Universidad Nacional de La Matanza

Departamento de Ingeniería e Investigaciones Tecnológicas

Redes de Computadoras (3643)
Trabajo Final Integrador

Docentes:

Carlos Binker

Diego Fernandez

Martín Vilariño

Eliseo Zurdo

Maximiliano Frattini

Alumnos:

Brizzolara César	34728140
Barcia Matías Alejandro	43975241
Cáceres Olguin Facundo	45747823
Mangalaviti Sebastián	45233238
Rodríguez Gonzalo	46418949
Sanz Eliseo Tomas	44690195
Serra Leandro Emanuel	43516473

Cuatrimestre: Primero

Año lectivo: 2025

Lineamientos del Trabajo Práctico Integrador

Objetivo del TP: demostrar las competencias adquiridas durante el cuatrimestre

Elementos a utilizar: Packet Tracer. Postman. Vscode con scripts de Python

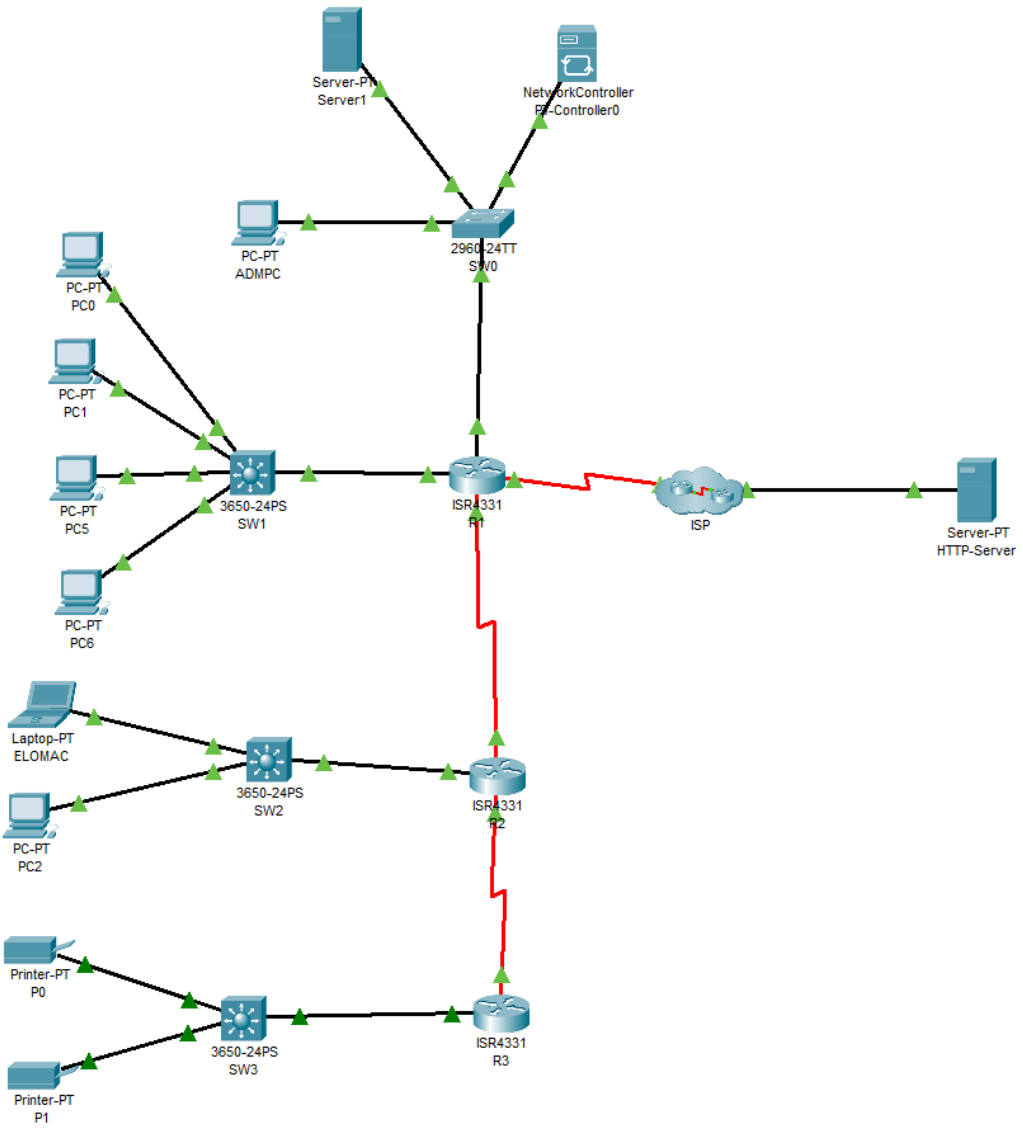
Topología a diseñar: La topología será definida por el grupo, la misma debe contar con:

- 1 Network controller
- 6 routers totales (usar 3650 y 4331)
- Switches 2960
- 1 Servidor DNS
- 1 Servidor FTP
- 1 Servidor HTTP
- 1 Servidor NTP
- 1 servidor DHCP en un 3650 y otro en un 4331 (no vale configurar desde la solapa services de un servidor)
- Direccionamiento tipo classles para IPv4 (proponer direccionamiento basado en la RFC 1918 para la intranet, definir máscaras, etc.)
- Direccionamiento público para el servidor http (inventar una IP pública y un dominio)
- Direccionamiento IPv6 (definir IP globales y link local estáticas para las líneas punto a punto, máscaras, ULA optativo, etc.)
- Rutas por default en el router de borde (en IPv4 e IPv6)
- Simular un router ISP para su conexión a internet dual stack
- Propagar rutas por default a todos los dispositivos del sistema autónomo
- Ruteo dinámico (a elección RIP, EIGRP, OSPF con sus variantes para IPv6)
- Vlans (definir las mismas a elección). Al menos un router 4331 ruteando en 802.1q con switches 2960 (método router on a stick)
- Hosts (laptops, PC desktop, impresoras, servers, etc. Todos conectados por medio de Fast/ Gigabit Ethernet).

Actividad a desarrollar

1. Con los elementos indicados desplegar una topología de manera tal que todos los dispositivos tengan plena conectividad entre sí y que sea dual stack.
2. Todo el management de la red deberá estar supervisado por un network controller (sólo en IPv4).
3. A partir de la documentación de la API del controlador (*Cisco Packet Tracer Northbound API for Network Controller Device*), tomar 4 *endpoints* que se correspondan con el esquema CRUD, es decir que utilicen los métodos *post, get, put y delete* y comprobar su funcionamiento mediante *Postman*. Documentar su utilización, y verificar los resultados en base a la documentación dada por cisco. Comprobar también la verificación de la API utilizando los scripts de Python suministrados.

Topología propuesta:



A lo largo de todo el trabajo práctico, y para cada uno de los elementos utilizados en la topología, se aplicaron las mismas **configuraciones de seguridad**, las cuales son las siguientes:

```
hostname <HOSTNAME>
line console 0
password tpfinal
login
line vty 0 4
password tpfinal
login
logging synchronous
exit
no ip domain-lookup
enable secret grupo8
```

Cada vez que en el trabajo se mencionen **“Configuraciones de seguridad”**, se refiere a los comandos previamente mostrados.

Switch 0 (SW0)

El **Switch 0** opera como un **switch tradicional de Capa 2**, encargado de interconectar hosts pertenecientes a distintas VLANs y reenviar tráfico a través de un enlace trunk hacia el router R1, el cual realiza el ruteo inter-VLAN mediante la técnica de **router-on-a-stick**.

Configuración realizada en SW0
- **VLAN 50**: asignada a los puertos FastEthernet 0/1 al 0/10.
- **VLAN 60**: asignada a los puertos FastEthernet 0/11 al 0/20.
- **Puerto G0/2**: configurado como access en VLAN 60, utilizado probablemente para conectar una PC administrativa o un servidor.
- **Puerto G0/1**: configurado en modo trunk, permitiendo el transporte del tráfico etiquetado de las VLANs 50 y 60 hacia R1.

Este dispositivo no tiene configurado *ip routing* ni interfaces VLAN con direcciones IP, por lo tanto:
- No realiza funciones de enrutamiento.
- No participa en el proceso de OSPF.
- No brinda servicio DHCP.

En resumen, **SW0 no cuenta como router**. Su función es esencial como elemento de acceso y segmentación, ya que permite que el router R1 actúe como gateway de las VLANs al recibir el tráfico etiquetado y enrutarlo entre ellas mediante subinterfaces configuradas con encapsulación dot1Q.

Los comandos utilizados para su configuración son los siguientes:

1. Configuraciones de seguridad
2. VLANS SW0

```
configure terminal

interface range F0/1-10
switchport mode access
switchport access vlan 50
exit

interface range F0/11-20
switchport mode access
switchport access vlan 60
exit

interface G0/2
switchport mode access
switchport access vlan 60
exit

interface G0/1
switchport mode trunk
switchport trunk allowed vlan 50,60
exit

exit
write
```

Switch 1 (SW1) – Grupo Ingeniería

El **Switch 1** se encuentra configurado con las VLAN 10 (Piso 1) y VLAN 20 (Piso 2). Sus direcciones IP asignadas son:

- 10.0.10.254 para VLAN 10
- 10.0.20.254 para VLAN 20
- 10.1.0.2 para la interfaz de enlace con R1

Se encuentra habilitado con *ip routing* y configurado como participante en **OSPFv2 e IPv6 OSPFv3**. Asimismo, funciona como **servidor DHCP** para ambas VLANs y tiene direccionamiento IPv6 configurado tanto en sus interfaces VLAN como en la interfaz de enlace con R1.

En síntesis, SW1 realiza funciones de enrutamiento inter-VLAN, participa en el enrutamiento dinámico del sistema autónomo y proporciona direccionamiento IP mediante DHCP.

Los comandos utilizados para su configuración son los siguientes:

1. Configuraciones de seguridad
2. SSH

```
configure terminal

ip domain-name sw1.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. VLANS SW1

```
configure terminal
ip routing

vlan 10
name INGPISO1

interface range G1/0/1-10
switchport mode access
switchport access vlan 10
no shutdown
exit

interface vlan 10
ip address 10.0.10.254 255.255.255.0
no shutdown
exit

vlan 20
name INGPISO2
```

```
interface range G1/0/11-20
switchport mode access
switchport access vlan 20
no shutdown
exit

interface vlan 20
ip address 10.0.20.254 255.255.255.0
no shutdown
exit

interface G1/0/24
no switchport
ip address 10.1.0.2 255.255.255.252
no shutdown
exit
```

4. OSPF

```
configure terminal
router ospf 8
router-id 11.11.11.11
passive-interface vlan 10
passive-interface vlan 20
network 10.0.10.254 0.0.0.255 area 0
network 10.0.20.254 0.0.0.255 area 0
network 10.1.0.2 0.0.0.3 area 0
```

5. DHCP SW1

```
configure terminal
ip dhcp excluded-address 10.0.10.254
ip dhcp excluded-address 10.0.20.254

ip dhcp pool VLAN10
network 10.0.10.0 255.255.255.0
default-router 10.0.10.254
dns-server 10.0.50.254
exit

ip dhcp pool VLAN20
network 10.0.20.0 255.255.255.0
default-router 10.0.20.254
dns-server 10.0.50.254
exit
```

Switch 2 (SW2) – Grupo Administración

El **Switch 2** gestiona las VLAN 30 (Piso 1) y VLAN 40 (Piso 2). Las direcciones IP configuradas son:

- 10.0.30.254 para VLAN 30
- 10.0.40.254 para VLAN 40
- 10.2.0.2 en la interfaz de enlace con R2

Cuenta con ip routing habilitado y está configurado en **OSPFv2 y OSPFv3**. Además, actúa como **servidor DHCP** para ambas VLANs y posee direccionamiento IPv6 en sus interfaces VLAN y en la interfaz de enlace.

Por lo tanto, SW2 cumple funciones de ruteo inter-VLAN, enrutamiento dinámico y asignación de direcciones IP en un entorno dual stack.

Los comandos utilizados para su configuración son los siguientes:

1. Configuraciones de seguridad
2. SSH

```
configure terminal

ip domain-name sw2.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. VLANS SW2

```
configure terminal

ip routing

vlan 30
name ADMPISO1

interface range G1/0/1-10
switchport mode access
switchport access vlan 30
no shutdown
exit

interface vlan 30
ip address 10.0.30.254 255.255.255.0
no shutdown
exit

vlan 40
name ADMPISO2

interface range G1/0/11-20
switchport mode access
switchport access vlan 40
no shutdown
exit

interface vlan 40
ip address 10.0.40.254 255.255.255.0
no shutdown
exit
```

```
interface G1/0/24
no switchport
ip address 10.2.0.2 255.255.255.252
exit
```

4. OSPF
```
configure terminal

router ospf 8
router-id 22.22.22.22
passive-interface vlan30
passive-interface vlan40
network 10.0.30.254 0.0.0.255 area 0
network 10.0.40.254 0.0.0.255 area 0
network 10.2.0.2 0.0.0.3 area 0
```

5. DHCP SW2
```
configure terminal

ip dhcp excluded-address 10.0.30.254
ip dhcp excluded-address 10.0.40.254

ip dhcp pool VLAN30
network 10.0.30.0 255.255.255.0
default-router 10.0.30.254
dns-server 10.0.50.254
exit

ip dhcp pool VLAN40
network 10.0.40.0 255.255.255.0
default-router 10.0.40.254
dns-server 10.0.50.254
exit
```

SW3 – Grupo Impresoras

El **Switch 3** gestiona la VLAN 70 destinada al segmento de impresoras. Las direcciones IP configuradas son:

- 10.0.70.254 para VLAN 70
- 10.3.0.2 en la interfaz de enlace con R3

Tiene habilitado *ip routing* y está configurado en **OSPFv2 y OSPFv3**. No brinda servicio DHCP, pero participa activamente en el enrutamiento dinámico y cuenta con direccionamiento IPv6.

En resumen, SW3 actúa como router de acceso para el segmento de impresoras en un entorno IPv4 e IPv6.

Los comandos utilizados para su configuración son los siguientes:

1. Configuraciones de seguridad
2. VLANS SW3
```
configure terminal
```

```
ip routing

vlan 70
name IMPRESORAS

interface range G1/0/1-22
switchport mode access
switchport access vlan 70

interface vlan 70
ip address 10.0.70.254 255.255.255.240
no shutdown
exit

interface G1/0/24
no switchport
ip address 10.3.0.2 255.255.255.252
no shutdown
exit
```

3. OSPF

```
configure terminal

router ospf 8
router-id 33.33.33.33
passive-interface vlan70
network 10.0.70.254 0.0.0.255 area 0
network 10.3.0.2 0.0.0.3 area 0
```

Configuración IPv4

Para los routers R1, R2 y R3 se realizó la configuración de acceso remoto seguro mediante SSH. Los aspectos relevantes son:

- SSH permite acceso remoto cifrado, brindando mayor seguridad en comparación con Telnet, que transmite credenciales y datos en texto plano.
- El comando *login local* configura la autenticación con usuarios locales previamente definidos mediante username.
- *crypto key generate rsa* genera las claves necesarias para cifrar el tráfico SSH.
- *ip ssh version 2* fuerza la utilización de la versión 2 del protocolo SSH, más segura que la versión anterior.
- *transport input ssh* limita el acceso a las líneas VTY exclusivamente a SSH, evitando conexiones Telnet.

Interfaces configuradas en R1, R2 y R3

Enlaces punto a punto entre routers:

Enlace	IPs asignadas	Máscara
R1 ↔ R2	10.0.1.1 / 10.0.1.2	255.255.255.252 (/30)
R2 ↔ R3	10.0.2.1 / 10.0.2.2	255.255.255.252 (/30)

Interfaces hacia switches y VLANs

- R1 cuenta con subinterfaces configuradas para las VLAN 50 y VLAN 60, utilizando la IP terminada en **.1** como gateway predeterminado de cada VLAN.
- Las subinterfaces (por ejemplo, G0/0/1.50 y G0/0/1.60) están configuradas con encapsulación dot1Q, implementando la técnica de **router-on-a-stick**.

Configuración de DHCP en R1

En R1 se configuró el servicio DHCP desde CLI para asignar direcciones IP dinámicamente a los hosts de las VLANs. La configuración incluyó:

- Exclusión de direcciones reservadas (gateways y servidores)
- Creación de pools DHCP para cada VLAN
- Configuración de default-router y servidor DNS para los clientes

Rutas por defecto y OSPF

En R1 se configuró:

- Una ruta estática por defecto apuntando hacia el ISP a través de la interfaz Serial 0/1/1.
- El proceso de OSPF para propagar dicha ruta por defecto al resto de los routers mediante el comando *default-information originate*.

Configuración general de OSPF

- Cada router cuenta con un router-id único para su identificación en el área.
- Las instrucciones network indican qué interfaces participan en el proceso de enrutamiento dinámico.
- Toda la configuración se realizó en el área 0, correspondiente al backbone de OSPF.

Los comandos utilizados para la configuración de los tres routers son los siguientes:

R1

1. Configuraciones de seguridad
2. SSH

```
configure terminal

ip domain-name r1.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. Interfaces R1

```
configure terminal

interface S0/1/0
ip address 10.0.1.1 255.255.255.252
clock rate 4000000
no shutdown
exit

interface S0/1/1
ip address 11.0.1.1 255.255.255.252
no shutdown
exit

interface G0/0/0
ip address 10.1.0.1 255.255.255.252
no shutdown
exit

interface G0/0/1
no ip address
no shutdown
exit

interface G0/0/1.50
encapsulation dot1Q 50
ip address 10.0.50.1 255.255.255.0
no shutdown
exit

interface G0/0/1.60
encapsulation dot1Q 60
ip address 10.0.60.1 255.255.255.0
no shutdown
exit
```

4. Ruta estatica por defecto

```
configure terminal
ip route 0.0.0.0 0.0.0.0 S0/1/1
```

5. OSPF
```
configure terminal

router ospf 8
router-id 1.1.1.1
default-information originate
passive-interface g0/0/1
passive-interface s0/1/1
network 11.0.1.1 0.0.0.3 area 0
network 10.0.1.1 0.0.0.3 area 0
network 10.1.0.1 0.0.0.3 area 0
network 10.0.50.1 0.0.0.255 area 0
network 10.0.60.1 0.0.0.255 area 0
```

6. DHCP R1
```
configure terminal

ip dhcp excluded-address 10.0.50.1
ip dhcp excluded-address 10.0.60.1
ip dhcp excluded-address 10.0.50.254

ip dhcp pool VLAN50
network 10.0.50.0 255.255.255.0
default-router 10.0.50.1
dns-server 10.0.50.254
exit

ip dhcp pool VLAN60
network 10.0.60.0 255.255.255.0
default-router 10.0.60.1
dns-server 10.0.50.254
exit
```

R2

1. Configuraciones de seguridad
2. SSH
```
configure terminal
ip domain-name r2.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. Interfaces R2
```
configure terminal

interface S0/1/0
```

```
ip address 10.0.1.2 255.255.255.252
no shutdown
exit

interface S0/1/1
ip address 10.0.2.1 255.255.255.252
clockrate 4000000
no shutdown
exit

interface G0/0/0
ip address 10.2.0.1 255.255.255.252
no shutdown
exit
```

4. OSPF

```
configure terminal

router ospf 8
router-id 2.2.2.2
network 10.0.1.2 0.0.0.3 area 0
network 10.0.2.1 0.0.0.3 area 0
network 10.2.0.1 0.0.0.3 area 0
```

R3

1. Configuraciones de seguridad
2. SSH

```
configure terminal

ip domain-name r3.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. Interfaces R3

```
configure terminal

interface S0/1/1
ip addresss 10.0.2.2 255.255.255.252
no shutdown
exit

interface G0/0/0
ip address 10.2.0.1 255.255.255.252
no shutdown
exit
```

4. OSPF

```
configure terminal
```

```
router ospf 8
router-id 3.3.3.3
network 10.0.2.2 0.0.0.3 area 0
network 10.3.0.1 0.0.0.3 area 0
```

Configuración ISP:

Interfaces configuradas (IPv4)

A continuación, se detallan las interfaces configuradas en el router ISP:

Interfaz	IP asignada	Observaciones
G0/0/0	100.100.100.1	IP pública que simula la conexión a Internet.
S0/1/1	11.0.1.2	Enlace serial hacia R1, interconectando el ISP con el sistema autónomo interno.

El router ISP se encuentra conectado al entorno simulado de Internet mediante la interfaz G0/0/0, mientras que la interconexión con el sistema autónomo interno se realiza a través de la interfaz Serial0/1/1.

Tabla de enrutamiento (IPv4)

El comando ***show ip route*** evidencia la siguiente tabla de enrutamiento:

- C 11.0.1.0/30 → conectado directamente (enlace con R1)
- C 100.100.100.0/24 → conectado directamente (Internet simulado)
- S* 0.0.0.0/0 → ruta por defecto vía Serial0/1/1

Esto indica que el router ISP tiene configurada una ruta estática por defecto, reenviando todo tráfico destinado a redes no conocidas hacia la interfaz **Serial0/1/1 (R1).** De esta manera, el ISP puede recibir y reenviar tráfico hacia el sistema autónomo y hacia la red simulada de Internet.

Configuración de enrutamiento IPv6

De manera similar a IPv4, el ISP cuenta con una ruta estática por defecto en IPv6, configurada para apuntar hacia R1 utilizando su dirección link-local (FE80::) como next-hop. Esto permite la salida de tráfico IPv6 desde el sistema autónomo a Internet y el reingreso de paquetes desde la red simulada hacia la red interna.

Participación en protocolos de enrutamiento dinámico

El router ISP no participa en protocolos de enrutamiento dinámico (OSPF, RIP o EIGRP). Según la revisión de su configuración (show running-config), se observa que:

- No existen procesos configurados de OSPF, RIP o EIGRP.
- No se encuentra configurado default-information originate.
- Todas sus rutas son estáticas.

Esto es consistente con su rol, ya que, al actuar como proveedor de servicios de

Internet en esta práctica, no forma parte del sistema autónomo interno y no intercambia rutas dinámicas con los routers del AS.

Resumen

El router ISP simula un proveedor de Internet. Cuenta con:
- Una IP pública en la interfaz G0/0/0 (100.100.100.1).
- Una IP privada en la interfaz Serial0/1/1 (11.0.1.2) para conexión con R1.
- Rutas estáticas configuradas tanto para IPv4 como IPv6.
- Uso de dirección link-local (FE80::) como next-hop en IPv6.

No participa en protocolos de enrutamiento dinámico, cumpliendo exclusivamente funciones de tránsito y salida a Internet para el sistema autónomo.

Los comandos utilizados para la configuración son los siguientes:

1. Configuraciones de seguridad
2. SSH
```
configure terminal
ip domain-name isp.grupo8.com
crypto key generate rsa
line vty 0 4
transport input ssh
login local
exit
username grupo8 privilege 15 password tpfinal
ip ssh version 2
```

3. Interfaces ISP
```
configure terminal

interface S0/1/1
ip address 11.0.1.2 255.255.255.252
clock rate 4000000
no shutdown
exit

interface G0/0/0
ip address 100.100.100.1
255.255.255.0
no shutdown
exit
```

4. Ruta estatica por defecto
```
configure terminal
ip route 0.0.0.0 0.0.0.0 Serial0/1/1
```

Configuración IPv6

Se habilitó el enrutamiento IPv6 en los routers mediante el comando ***ipv6 unicast-routing***. Este comando es obligatorio, ya que permite que el router reenvíe paquetes IPv6 entre sus interfaces. Sin esta configuración, el router actuaría únicamente como host IPv6 y no como enrutador.

Direccionamiento IPv6 configurado

Tipos de direcciones utilizadas:

Tipo de dirección	Ejemplo	Función
Global Unicast	2001:DB8:...	Direcciones únicas en la red, utilizadas para comunicación global en la topología de práctica (RFC 3849).
Link-local	fe80::, fe80::1	Direcciones locales al enlace, necesarias para la comunicación entre vecinos y protocolos de enrutamiento como OSPFv3.

Las direcciones 2001:DB8::/32 se utilizan exclusivamente para documentación y prácticas de laboratorio, como en este trabajo.

Método de asignación

- **Interfaces punto a punto:** se utilizaron prefijos /127, optimizando el uso de direcciones y eliminando la posibilidad de ataques de escaneo en enlaces de dos equipos.
- **Interfaces VLAN (subinterfaces):** se asignaron direcciones globales únicas. Si bien en redes LAN la práctica recomendada es utilizar /64, en entornos controlados como este TP se implementaron /127 para simplificación y consistencia con los enlaces p2p.

Se configuró una ruta estática por defecto hacia el ISP con el siguiente formato:
ipv6 route ::/0 2001:db8:0:2::1

Posteriormente, esta ruta por defecto se propagó al resto del sistema autónomo mediante OSPFv3 utilizando los comandos:

- `redistribute static`
- `default-information originate`

Esto permitió que los routers conocieran la salida hacia redes externas en IPv6.

Configuración de OSPFv3 (enrutamiento dinámico para IPv6)

En OSPFv3, la activación del protocolo se realiza directamente en cada interfaz participante, a diferencia de OSPFv2 que utiliza el comando network. Por ejemplo:

- `interface G0/0/0`
- `ipv6 ospf 8 area 0`

Configuración global del proceso OSPFv3:

- `ipv6 router ospf 8`
- `router-id X.X.X.X`

El router-id mantiene el formato de dirección IPv4, ya que funciona como identificador

lógico dentro del proceso de enrutamiento. Las rutas se propagan automáticamente entre las interfaces participantes en el área configurada.

Conclusión

Se configuró IPv6 en todos los routers del sistema autónomo, asignando direcciones ***global unicast*** en enlaces punto a punto y subinterfaces para VLANs, utilizando /127 para enlaces p2p y direcciones ***link-local*** (fe80::) requeridas por OSPFv3. Se habilitó ipv6 *unicast-routing* para el reenvío de paquetes, y se propagó la ruta por defecto desde R1 al resto de la red mediante OSPFv3 con *default-information originate* y *redistribute static*. Cada router fue configurado como participante en el área 0.

Los comandos utilizados para la configuración son los siguientes:

Activar Routing IPV6:

```
configure terminal
ipv6 unicast-routing
```

R1

1. Interfaces R1

```
configure terminal
interface S0/1/1
ipv6 address 2001:DB8:0:2::/127
ipv6 address fe80:: link-local
exit

interface S0/1/0
ipv6 address 2001:DB8:0:1::/127
ipv6 address fe80:: link-local
exit

interface G0/0/0
ipv6 address 2001:DB8:0:1::4/127
ipv6 address fe80:: link-local
exit

interface G0/0/1.50
ipv6 address 2001:DB8:0:50::/127
exit

interface G0/0/1.60
ipv6 address 2001:DB8:0:60::/127
exit
```

2. Ruta estática por defecto

```
configure terminal
ipv6 route ::/0 2001:db8:0:2::1
exit
```

3. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 1.1.1.1
```

```
default-information originate
redistribute static
passive-interface G0/0/1
passive-interface S0/1/1
exit

interface G0/0/0
ipv6 ospf 8 area 0
interface S0/1/0
ipv6 ospf 8 area 0
```

R2

1. Interfaces R2

```
configure terminal

interface S0/1/0
ipv6 address 2001:DB8:0:1::1/127
ipv6 address fe80::1 link-local
exit

interface S0/1/1
ipv6 address 2001:DB8:0:1::2/127
ipv6 address fe80:: link-local
exit

interface G0/0/0
ipv6 address 2001:DB8:0:1::6/127
ipv6 address fe80:: link-local
exit
```

2. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 2.2.2.2
exit

interface G0/0/0
ipv6 ospf 8 area 0
interface S0/1/0
ipv6 ospf 8 area 0
interface S0/1/1
ipv6 ospf 8 area 0
```

R3

1. Interfaces R3

```
configure terminal

interface S0/1/1
ipv6 address 2001:DB8:0:1::3/127
ipv6 address fe80::1 link-local
exit

interface G0/0/0
```

```
ipv6 address 2001:DB8:0:1:8/127
ipv6 address fe80:: link-local
exit
```

2. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 3.3.3.3
exit

interface G0/0/0
ipv6 ospf 8 area 0
interface S0/1/1
ipv6 ospf 8 area 0
```

SW1

1. Interfaces SW1

```
configure terminal

interface vlan10
ipv6 address 2001:db8:0:10::/64
ipv6 address fe80:: link-local
exit

interface vlan20
ipv6 address 2001:db8:0:20::/64
ipv6 address fe80:: link-local
exit

interface G1/0/24
ipv6 address 2001:DB8:0:1::5/127
ipv6 address fe80::1 link-local
exit
```

2. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 11.11.11.11
exit

interface G1/0/24
ipv6 ospf 8 area 0
interface vlan10
ipv6 ospf 8 area 0
interface vlan20
ipv6 ospf 8 area 0
```

SW2

1. Interfaces SW2

```
configure terminal

interface vlan30
```

```
ipv6 address 2001:db8:0:30::/64
ipv6 address fe80:: link-local
exit

interface vlan40
ipv6 address 2001:db8:0:40::/64
ipv6 address fe80:: link-local
exit

interface G1/0/24
ipv6 address 2001:DB8:0:1::7/127
ipv6 address fe80::1 link-local
exit
```

2. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 22.22.22.22
exit

interface G1/0/24
ipv6 ospf 8 area 0
interface vlan30
ipv6 ospf 8 area 0
interface vlan40
ipv6 ospf 8 area 0
```

SW3

1. Interfaces SW3

```
configure terminal

interface vlan70
ipv6 address 2001:db8:0:70::/64
ipv6 address fe80:: link-local
exit

interface G1/0/24
ipv6 address 2001:DB8:0:1::9/127
ipv6 address fe80:: link-local
exit
```

2. OSPF ipv6

```
configure terminal

ipv6 router ospf 8
router-id 33.33.33.33
exit

interface G1/0/24
ipv6 ospf 8 area 0
interface vlan70
ipv6 ospf 8 area 0
```

ISP

1. Interfaces ISP

```
configure terminal

interface S0/1/1
ipv6 address 2001:db8:0:2::1/127
ipv6 address fe80::1 link-local
exit

interface G0/0/0
ipv6 address 2800:110:1010::/64
ipv6 address fe80:: link-local
exit
```

2. Ruta estática por defecto

```
configure terminal
ipv6 route ::/0 Serial 0/1/1 FE80::
exit
```

Controller

Nos da acceso a una **API RESTful** (en `http://localhost:58000/api`) con la cual podemos:

- Consultar el estado de la red (interfaces, dispositivos, topología, etc.)
- Automatizar configuraciones (por ejemplo, asignar IPs, crear VLANs)
- Observar tráfico o monitorear cambios en tiempo real
- Usar scripts desde Python, Postman, o el propio sistema

Es el punto central que expone los datos y permite enviar configuraciones. Cuando el controlador está encendido y conectado a los dispositivos se puede:

- Hacer `GET` para consultar información (como interfaces, routing tables)
- Hacer `POST`, `PUT` o `DELETE` para cambiar configuraciones
- Interactuar con **hosts, routers, switches**, etc., sin necesidad de usar CLI
- El Network Controller tiene una **IP propia dentro de la topología**.
- Los dispositivos deben estar **conectados al mismo dominio de administración** (vía OSPF).
- La API escucha por defecto en el **puerto 58000**, que actúa como una puerta de entrada HTTP/REST.

Configuraciones Network Controller Desde el navegador de ADMPC ir a http://10.0.60.2
username: grupo8
password: tpfinal
Ir a provisioning solapa credentials
add credential
username: grupo8
password: tpfinal
enable password: tpfinal
description: SSH
solapa discovery
name: SW1
ip address: 10.1.0.2
CLI credential list: grupo8 - SSH

Accedimos al **Network Controller** desde el navegador de la PC administrativa (ADMPC), ingresando la dirección `http://10.0.60.2` con el usuario `grupo8` y la contraseña `tpfinal`. Una vez dentro, fuimos a la sección **Provisioning** para comenzar a ges

Primero, en la solapa **Credentials**, cargamos las credenciales necesarias para que el controlador pueda conectarse por **SSH** a los equipos. Ingresamos el usuario, la contraseña y el enable password, todos como `tpfinal`, y lo etiquetamos como "SSH".

Luego, en la solapa **Discovery**, agregamos el switch **SW1**, indicando su IP (`10.1.0.2`) y asociando las credenciales previamente creadas. Esto le permitió al controlador conectarse con el switch y comenzar a gestionarlo.

Este proceso simula cómo en redes reales un controlador central como **Cisco DNA Center** descubre y administra los dispositivos mediante protocolos seguros como SSH, permitiendo automatización y monitoreo desde una única interfaz.

Python
Usamos la API REST del Network Controller de Packet Tracer para consultar datos de red desde Python. Creamos un entorno virtual, instalamos dependencias y ejecutamos scripts que obtienen un token de acceso, y luego listan dispositivos y hosts en tiempo real. Esto demuestra cómo podemos automatizar el monitoreo de red y aplicar conceptos modernos de programación y redes.

1. **Creamos un entorno virtual** para trabajar ordenadamente y aislar dependencias.

2. **Instalamos librerías** desde `requirements.txt`, probablemente incluyendo `requests` y `tabulate`.

3. **Ejecutamos scripts que interactúan con la API REST del Network Controller**, usando autenticación tipo *ticket* (token) y luego consultando:

    - Dispositivos de red

    - Hosts conectados

    - Y presentando los datos en tabla

1. **`/api/v1/ticket`**
   Solicita un token de autenticación válido (tipo session-token).

2. **`/api/v1/network-device`**
   Devuelve todos los dispositivos descubiertos por el controlador.

3. **`/api/v1/host`**
   Muestra los hosts activos en la red, incluyendo IPs y direcciones MAC.

4. **`tabulate`**
   Es una forma de mostrar la salida en formato tabla, más clara para análisis visual.

Link al repositorio: https://github.com/LeanSerra/redes-tp-integrador/tree/main