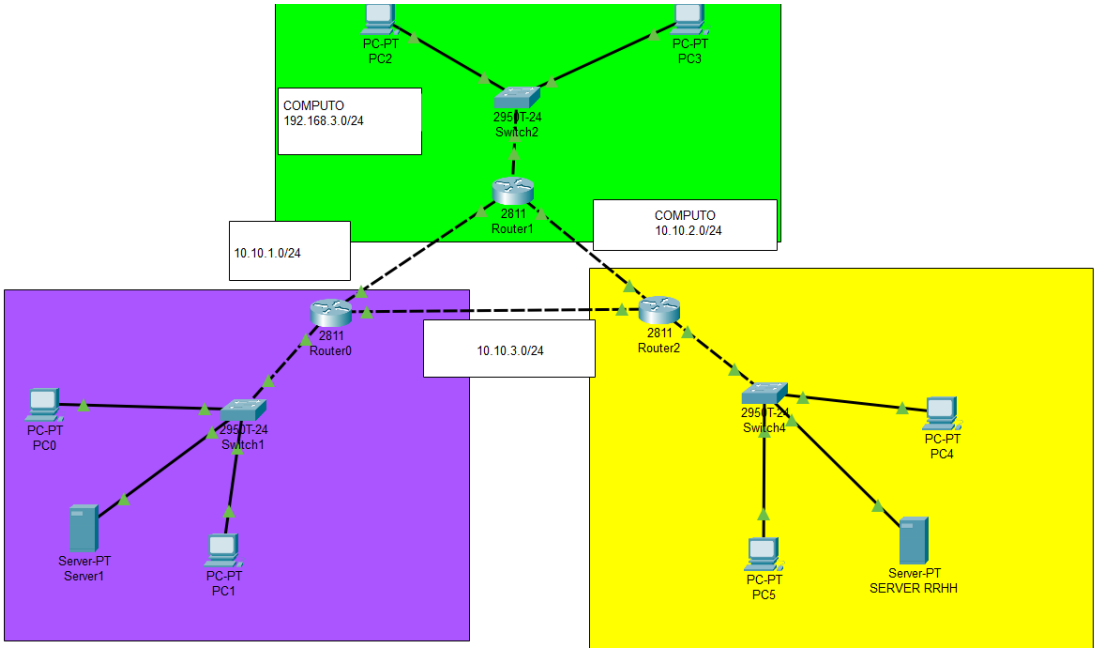
CONFIGURACIÓN DE RED CON ACLS EN ROUTERS CISCO

1. Objetivo

Implementar una red segmentada por áreas administrativas (Administración, Cómputo, Recursos Humanos), establecer rutas estáticas entre los routers y aplicar listas de control de acceso (ACL) para restringir o permitir tráfico según políticas establecidas.

2. Topología de Red



Subredes implementadas:

- **Administración**: 192.168.1.0/24 (Router0)
- **Cómputo**: 192.168.3.0/24 (Router1)
- **RRHH**: 192.168.2.0/24 (Router2)
- **Enlaces inter-routers**:
    - 10.10.1.0/24 (entre Router0 y Router1)
    - 10.10.2.0/24 (entre Router1 y Router2)
    - 10.10.3.0/24 (entre Router0 y Router2)

3. Configuración de Routers

Router0 - ADMINISTRACIÓN

```
interface fa0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface fa0/1
 ip address 10.10.1.1 255.255.255.0
 no shutdown
interface fa1/0
 ip address 10.10.3.1 255.255.255.0
 no shutdown
ip route 192.168.3.0 255.255.255.0 10.10.1.2
ip route 192.168.2.0 255.255.255.0 10.10.3.2
ip route 10.10.2.0 255.255.255.0 10.10.3.2
```

Router1 - CÓMPUTO

```
interface fa0/0
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface fa0/1
 ip address 10.10.1.2 255.255.255.0
 no shutdown
interface fa1/0
 ip address 10.10.2.1 255.255.255.0
 no shutdown
ip route 192.168.1.0 255.255.255.0 10.10.1.1
ip route 192.168.2.0 255.255.255.0 10.10.2.2
```

```
ip route 10.10.3.0 255.255.255.0 10.10.1.1
```

Router2 - RRHH

```
interface fa0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
interface fa0/1
 ip address 10.10.2.2 255.255.255.0
 no shutdown
interface fa1/0
 ip address 10.10.3.2 255.255.255.0
 no shutdown
ip route 192.168.1.0 255.255.255.0 10.10.3.1
ip route 192.168.3.0 255.255.255.0 10.10.2.1
ip route 10.10.1.0 255.255.255.0 10.10.3.1
```

4. Configuración de ACLs

ACL en Router1 (bloqueo de acceso de Cómputo a Administración)

```
access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 permit ip any any
interface fa0/0
ip access-group 100 in
```

Resultado esperado: Equipos de Cómputo **no deben comunicarse** con los de Administración.

ACL en Router2 (solo permitir tráfico HTTP/HTTPS hacia fuera)

```
access-list 101 permit tcp 192.168.2.0 0.0.0.255 any eq 80
```

```
access-list 101 permit tcp 192.168.2.0 0.0.0.255 any eq 443

access-list 101 deny ip any any

interface fa0/0

ip access-group 101 out
```

Resultado esperado: Equipos de RRHH **solo pueden acceder a internet por puertos 80 y 443**, y no pueden hacer ping ni comunicarse directamente con Cómputo ni Administración.

5. Pruebas de Conectividad

Desde Cómputo a Administración (bloqueado por ACL en Router1)

```
ping 192.168.1.2

Respuesta: Destination host unreachable (desde 192.168.3.1)


ping 192.168.1.3

Respuesta: Destination host unreachable (desde 192.168.3.1)
```

ACL aplicada correctamente. El acceso está denegado.

Desde Cómputo a RRHH (permitido)

```
ping 192.168.2.2

Respuesta exitosa


ping 192.168.2.3

Respuesta exitosa
```

Conectividad establecida entre Cómputo y RRHH.

Desde RRHH a Cómputo o Administración (bloqueado por ACL en Router2)

```
ping 192.168.3.2 → Timeout

ping 192.168.1.2 → Timeout
```

ACL de salida bloquea correctamente tráfico no HTTP/HTTPS.

6. Conclusiones

- La configuración de rutas estáticas permite el enrutamiento completo entre las subredes.
- Las ACL implementadas cumplen con las políticas de seguridad:
    - Cómputo no puede comunicarse con Administración.
    - RRHH solo puede usar puertos HTTP/HTTPS hacia fuera.
- El uso de ACLs en interfaces específicas (entrada/salida) permite un control granular del tráfico de red.