[UNIVERSIDAD TECNOLOGICA NACIONAL]
FRD
[FACULTAD REGIONAL DELTA]

Carrera: Ing. Sistemas de información

Materia: Redes de datos

Profesor: Ing. Juan Antonio González

Docente Laboratorio: Ing. Carlos José Alberto Carrizo


# TP N° 10

# Seguridad - ACL

Alumna:

| Apellido y Nombre | legajo |
|---|---|
| | |

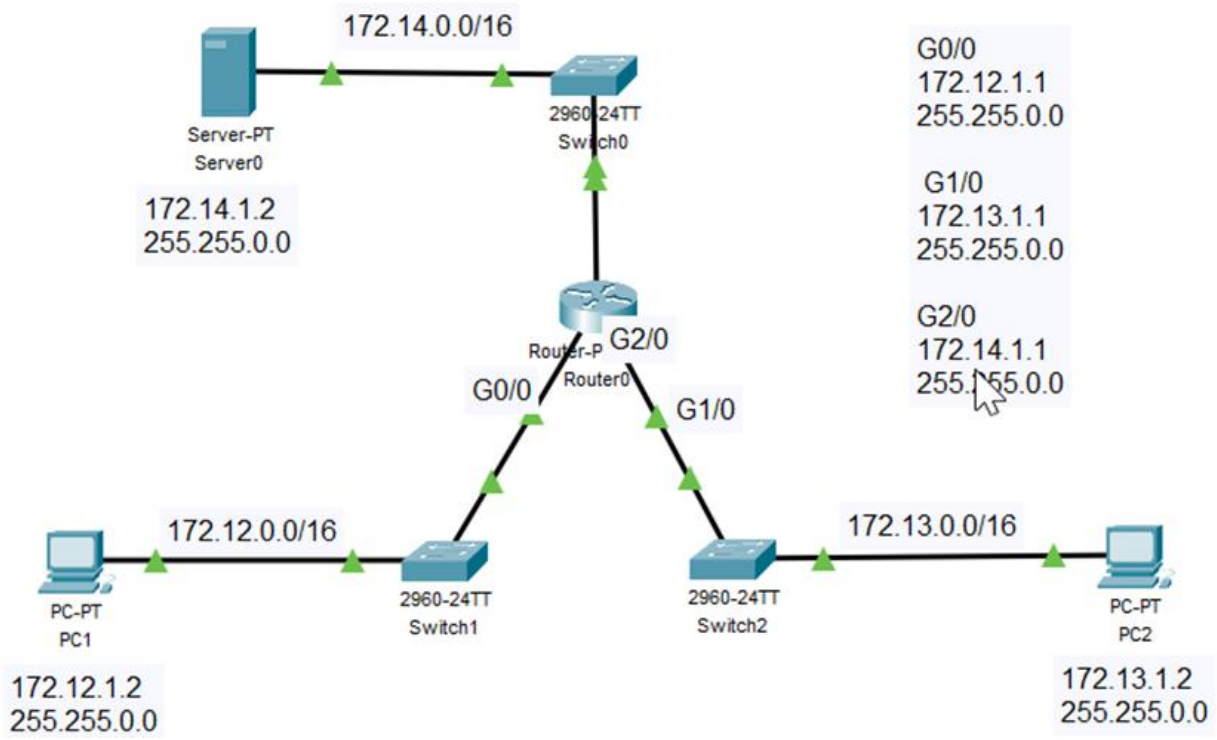
Curso: 2025

CONSIGNA TRABAJO PRÁCTICO 9

# Seguridad

Tema: **Seguridad**

Dado el siguiente diagrama de red y tabla de direccionamiento:



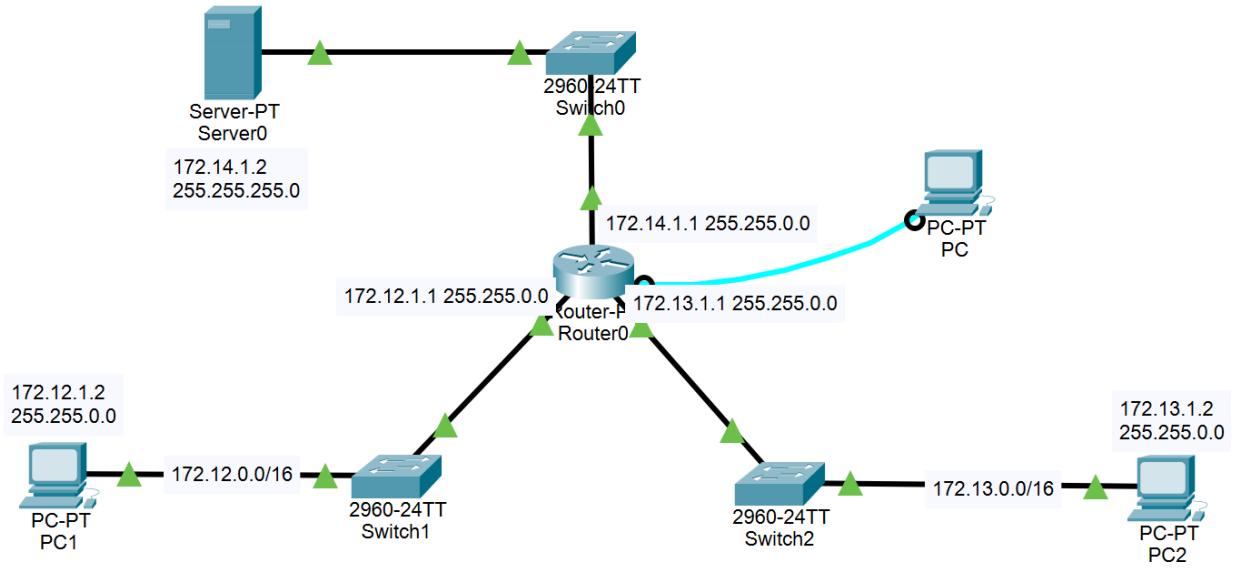

- Permitir todo el tráfico desde la PC1 a cualquier destino
- Permitir el tráfico de la PC2 a cualquier destino excepto para la PC1
- Permitir el tráfico HTTP en el Server desde cualquier destino
- Bloquear el tráfico FTP en el servidor para la PC1.

**Adjunte el archivo Packet tracer funcional.**

## Desarrollo del trabajo práctico 10

# Seguridad

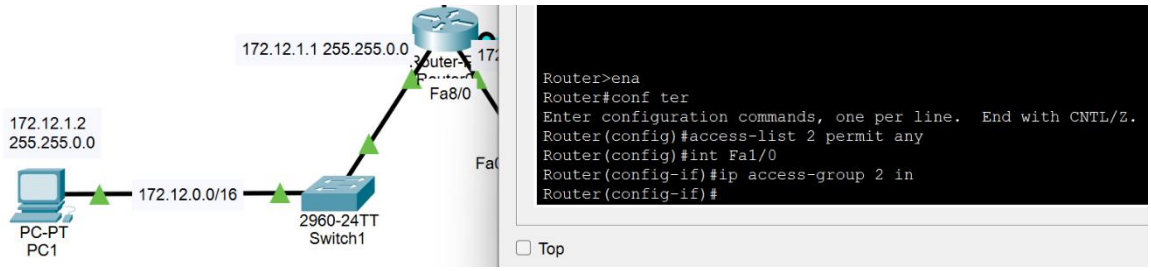
Diagrama del desarrollo de este trabajo práctico:




- **Permitir todo el tráfico desde la PC1 a cualquier destino**

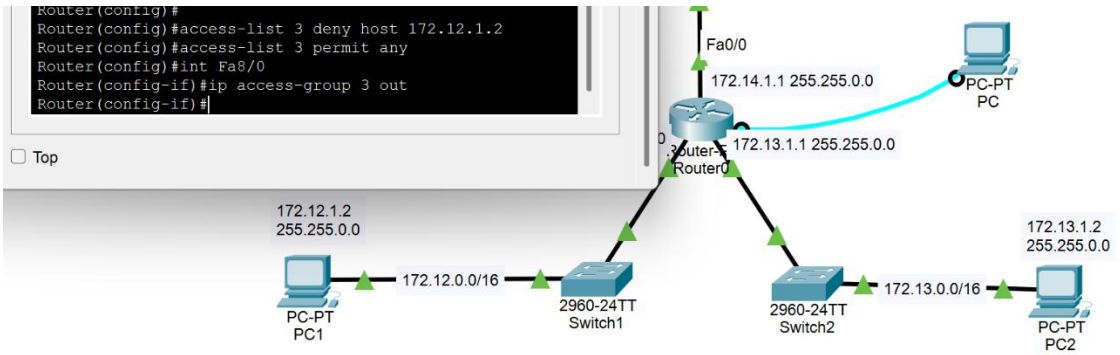
  Para cumplir este objetivo creo una lista de acceso (ACL) tipo standard, pues solo voy a trabajar con las direcciones IP. En este caso, utilizo el comodín “any” para indicar que permita “cualquier” dirección.

  Luego activo en la interfaz con IP 172.12.1.1 la ACL creada, como “in” (entrada)

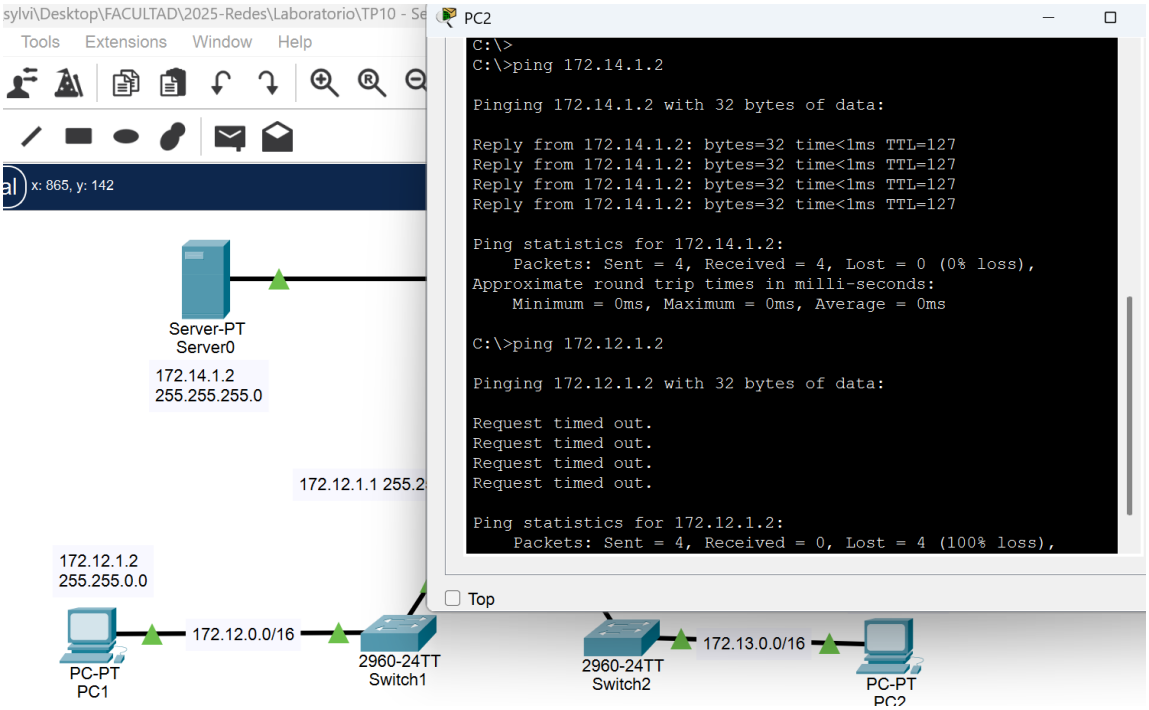



- **Permitir el tráfico de la PC2 a cualquier destino excepto para la PC1**

  En este caso también creo una ACL pero denegando el acceso a la PC1 y lo activo en la interfaz con IP 172.13.1.1, como “out” (salida). Siempre recordando permitir el pasaje de paquetes hacia cualquier dirección (permit any) como última regla:



Se intenta una conexión con el server (IP 172.14.1.2) y se tiene éxito y se realiza un intento de conexión con la PC1 (IP 172.12.1.2) y no se logra la misma.

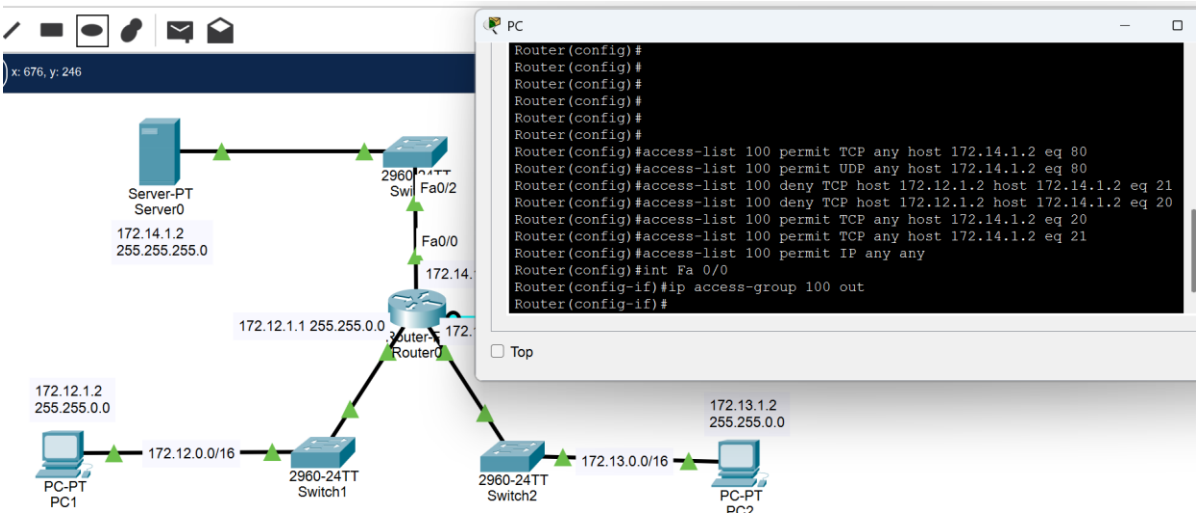



- **Permitir el tráfico HTTP en el Server desde cualquier destino y bloquear el tráfico FTP en el servidor para la PC1**

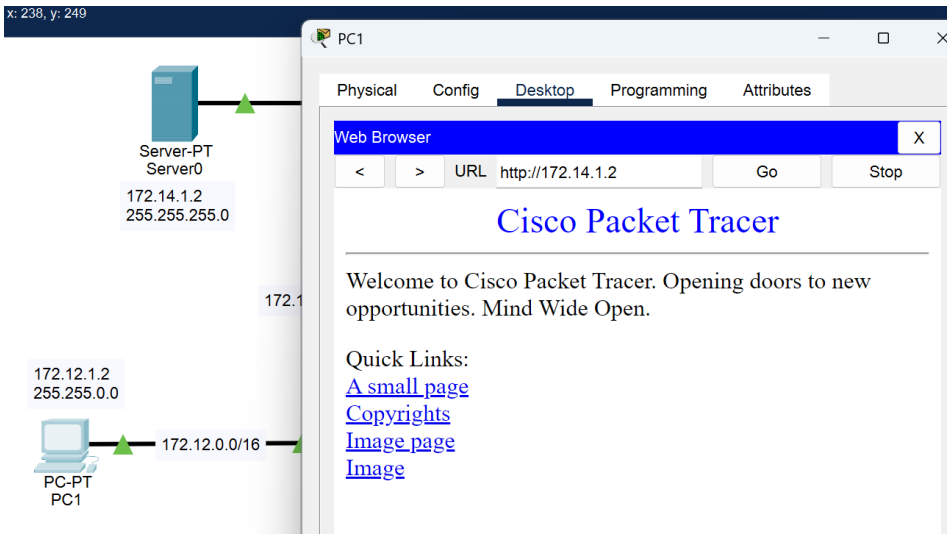
Para realizar esta parte del trabajo práctico uso una lista de acceso “extendida” pues necesito utilizar protocolos (no una dirección IP).

El protocolo http utiliza, principalmente, TCP. Eso no quita que pueda llegar a utilizarse UDP, por lo que se activarán los dos protocolos.

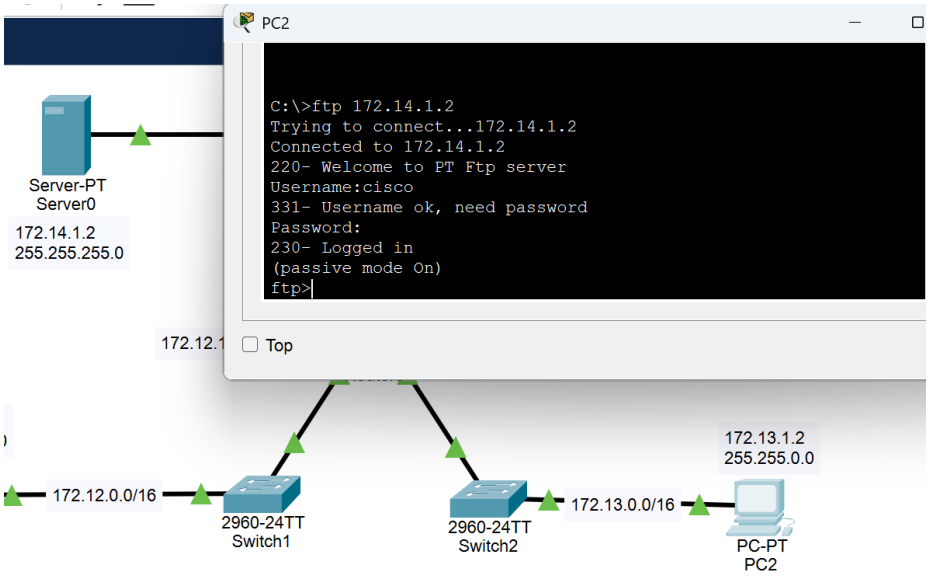
También anexo una regla que deniegue el tráfico FTP desde la PC1 hacia el servidor.



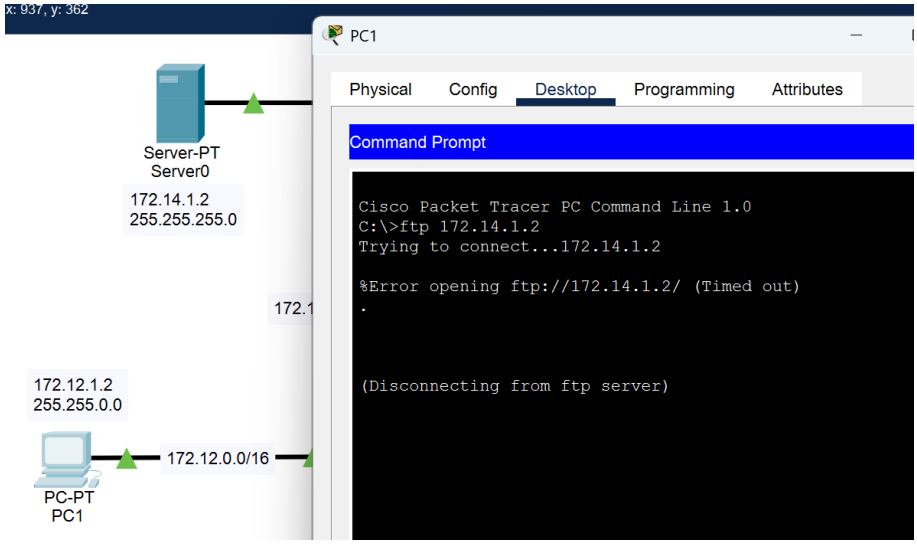
Uso del servicio http desde PC1:




Uso del servicio FTP desde la PC2 (exitoso):




Uso del servicio FTP desde la PC1 (no exitoso, pues está denegado por ACL):



Las listas quedaron configuradas de la siguiente manera:

```
Router#show access-lists
Standard IP access list 2
    10 permit any (38 match(es))
Standard IP access list 3
    10 deny host 172.12.1.2 (4 match(es))
    20 permit any (12 match(es))
Extended IP access list 100
    10 permit tcp any host 172.14.1.2 eq www (5 match(es))
    20 permit udp any host 172.14.1.2 eq www
    30 deny tcp host 172.12.1.2 host 172.14.1.2 eq ftp (12 match(es))
    40 deny tcp host 172.12.1.2 host 172.14.1.2 eq 20
    50 permit tcp any host 172.14.1.2 eq 20
    60 permit tcp any host 172.14.1.2 eq ftp (14 match(es))
    70 permit ip any any
```

**Adjuntar el archivo Packet tracer funcional.**

## Conclusiones

Con el desarrollo de este trabajo práctico pude observar, con mayor claridad, cuándo asignar una lista de acceso como entrada o como salida.