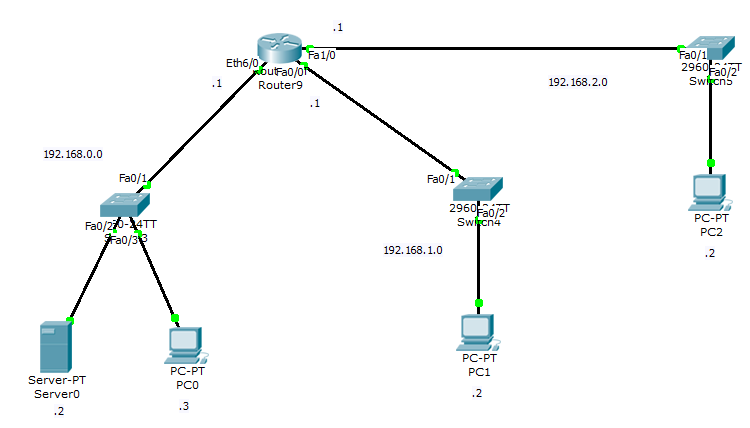
**ACL Extendida**



**Requerimientos**

1. **Situacion1**: Bloquear el tráfico entre la PC0 y las subredes externas, pero que permita el acceso al servidor desde todas las PC.

***access-list 101 deny ip******192.168.1.0 0.0.0.255******192.168.0.3 0.0.0.0***

***access-list 101 permit ip any any***

Ingresar a la interfcaz: eth6/0

***ip access-group 101 out***

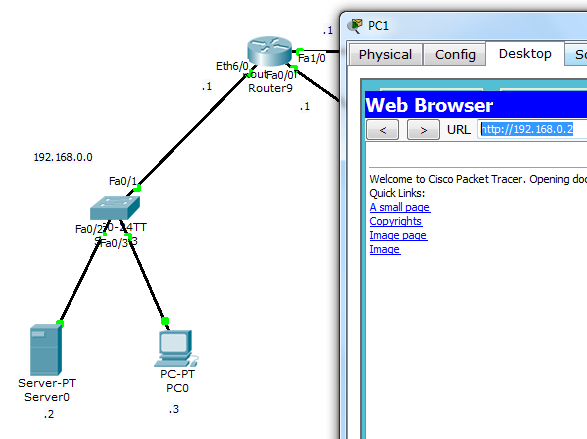
1. **Situacion2**: Se requiere bloquear sólo el tráfico de la subred S1 hacia PC0 asignando la access-list a la interfaz eth6/0
2. **Situacion3**: Bloquear los paquetes ICMP que circulen hacia el servidor

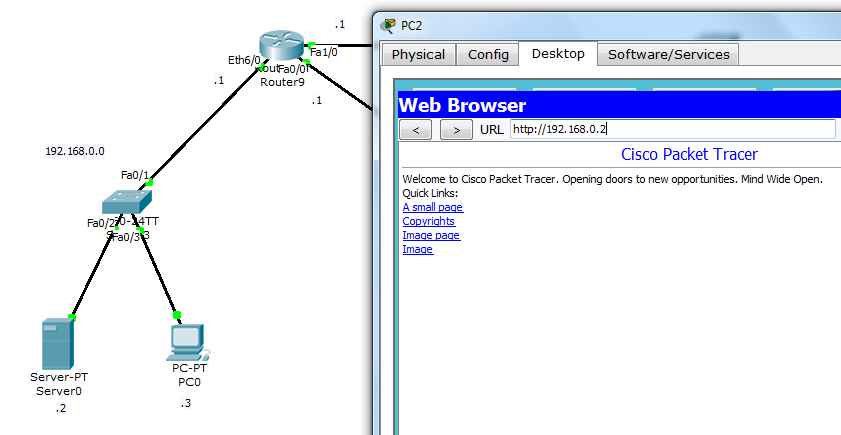
**access-list 102 deny icmp any 192.168.0.2 0.0.0.0**

**access-list 102 permit ip any any**

Ingresar a la interfcaz: eth6/0

***ip access-group 102 out***





1. **Situacion4**: Limitar solo el tráfico HTTP entre la subred 2 y el servidor

HTTP = TCP puerto 80

**access-list 103 deny tcp 192.168.2.0 0.0.0.255 192.168.0.2 0.0.0.0 eq 80**

**access-list 103 permit ip any any**

**OBS: Eliminar las access list anteriores para que se pueda ver la solucion de la situacion 4**

**(config)#no access-list 101**

**(config)#no access-list 102**

**APLICANDO:**

**int fa1/0**

**ip access-group 103 in**

1. **Comandos de monitoreo**

**#show access-lists**

1. x