# ACL Extendida

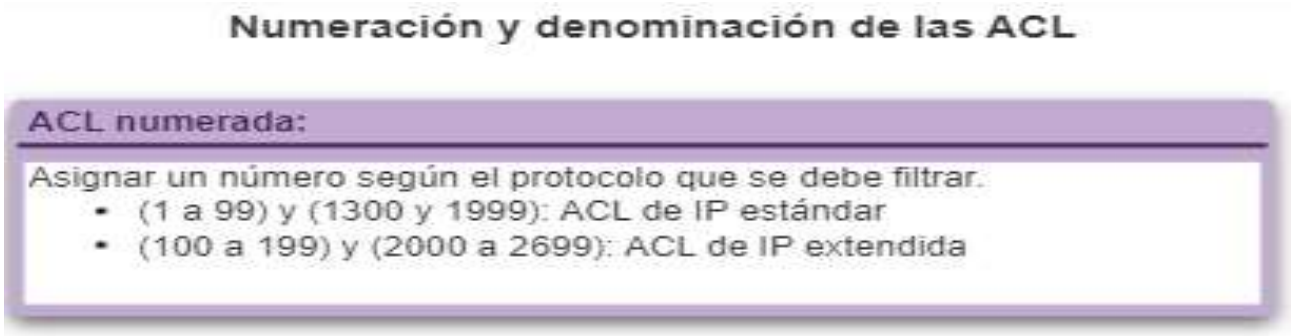
# Propósitos de las ACL

Proporcionar seguridad para el acceso a la red y pueden bloquear un host o una red.

Filtrar el tráfico según su tipo, como el tráfico de Telnet.

Controlar los hosts para permitir o denegar el acceso a servicios de red como FTP, HTTP, SMTP, ICMP, etc..

Recordando la numeración del rango de las listas de Acceso:



# ACL extendida

En su sintaxis aparece el protocolo, una dirección de origen y de destino.

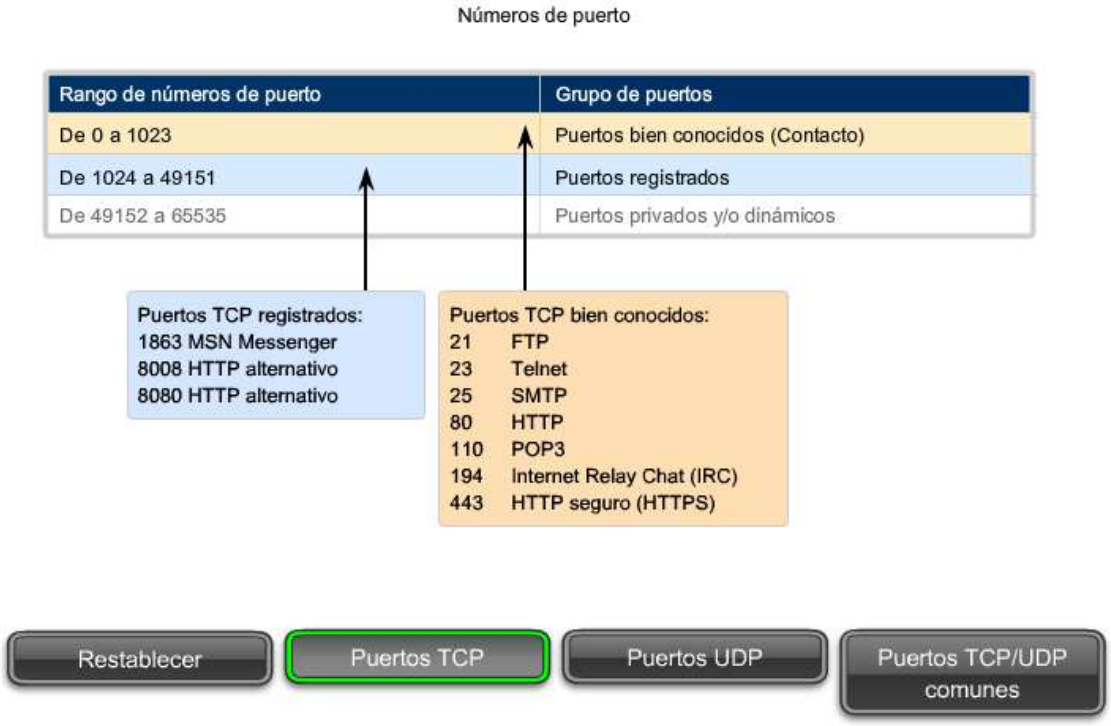
**(config)#access-list n {permit | deny} *protocol* source {source-mask}**

**destination {destinationmask} [eq destination-port]**

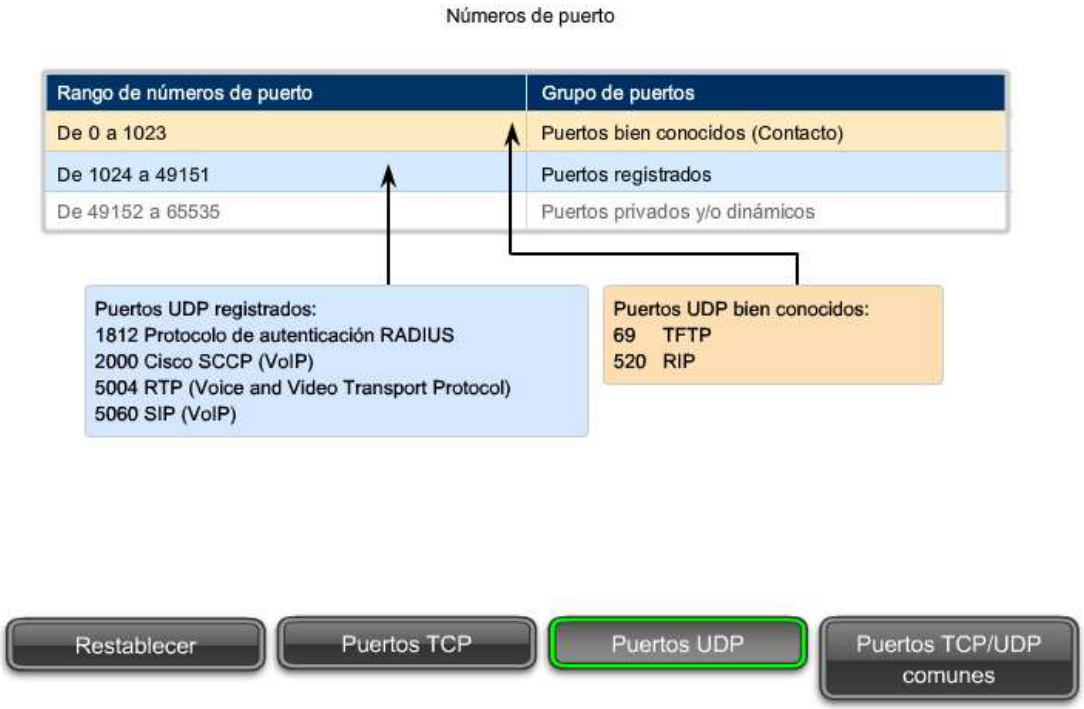
Ejemplo:

(config)# access-list **105** permit **tcp** **192.168.10.0** 0.0.0.255 host **192.168.31.12** **eq** 80

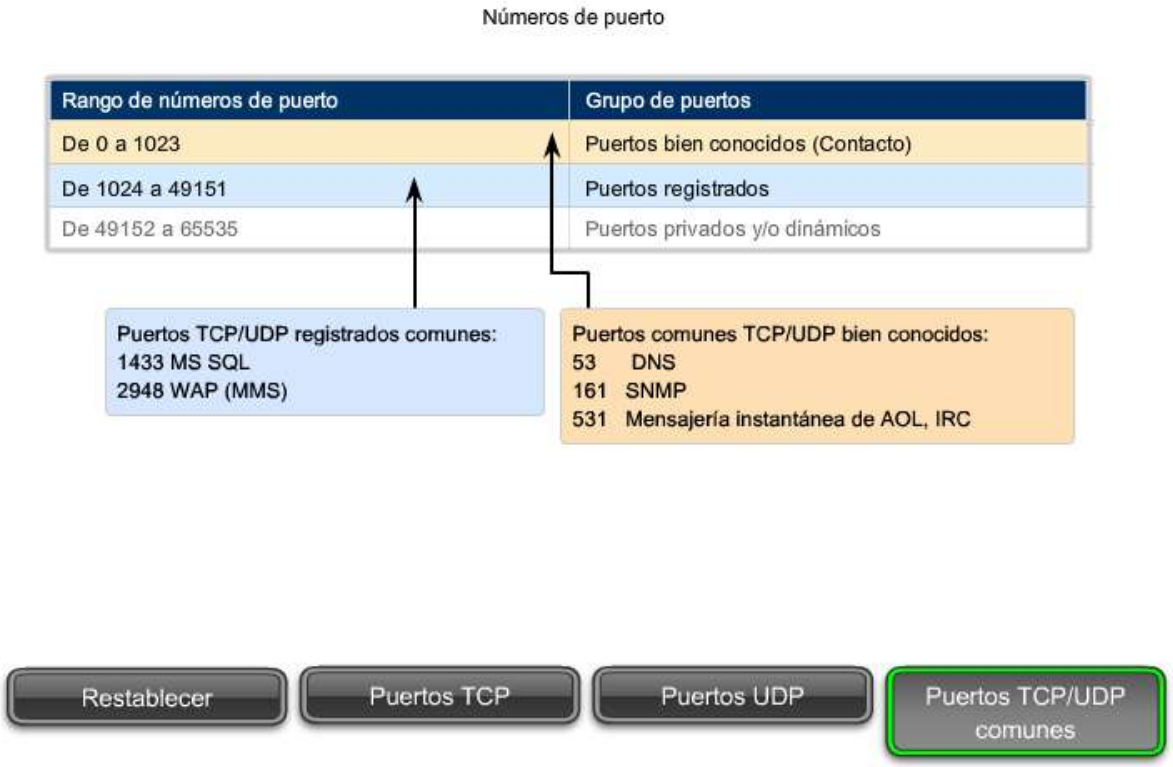
# Números de puerto



# Números de puerto UDP



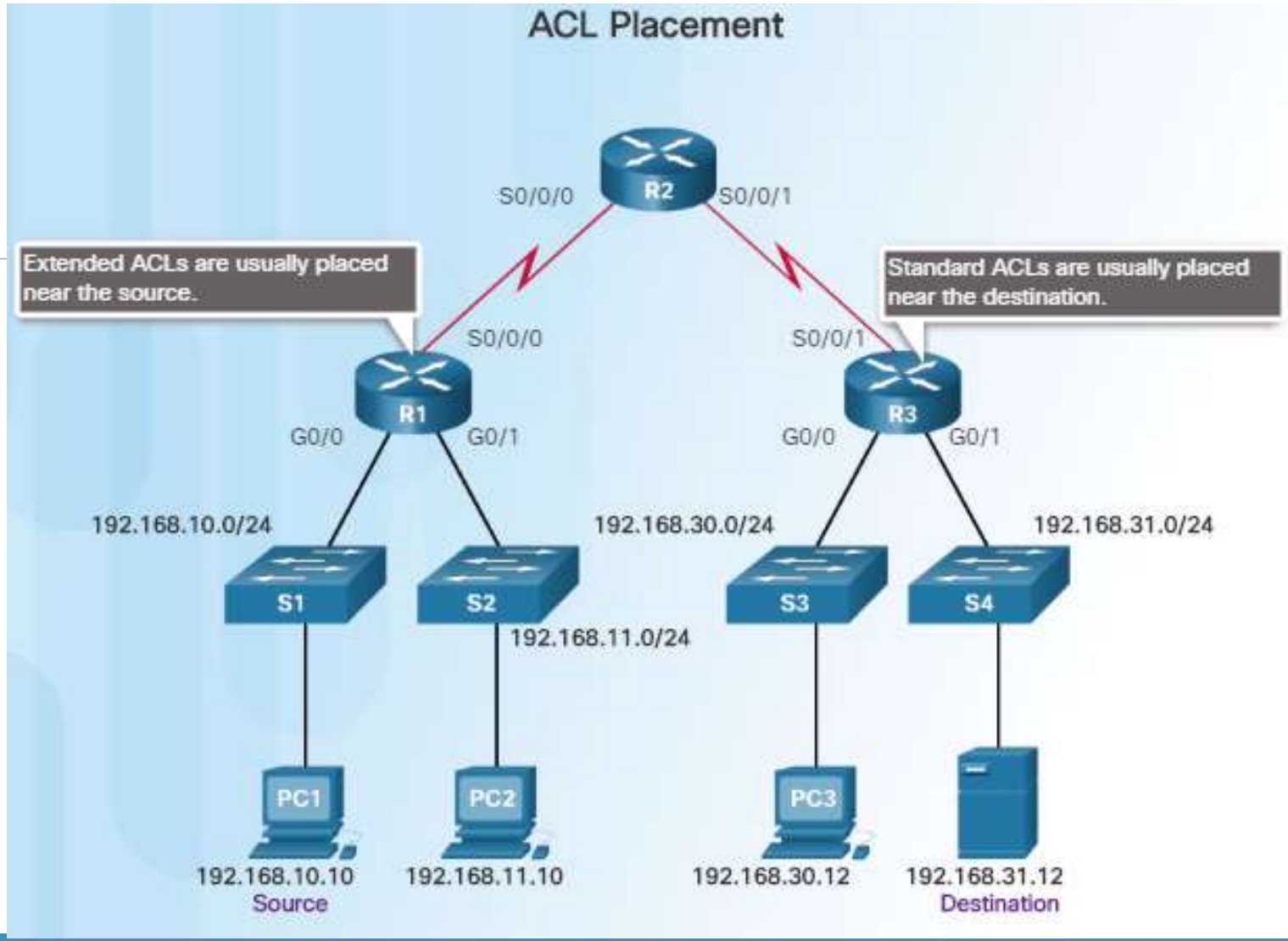
# Números de puerto TCP/UDP



# Recuerda…aplicar la ACL

Pero… ¿dónde se aplican?


- Las listas de acceso extendidas se deben colocar cerca de la fuente u origen.


ACL Placement
R2
S0/0/0
S0/0/1
Extended ACLs are usually placed near the source.
Standard ACLs are usually placed near the destination.
S0/0/0
S0/0/1
R1
R3
G0/0
G0/1
G0/0
G0/1
192.168.10.0/24
192.168.30.0/24
192.168.31.0/24
S1
S2
S3
S4
192.168.11.0/24
PC1
PC2
PC3
192.168.10.10
Source
192.168.11.10
192.168.30.12
192.168.31.12
Destination

# Aplicar la lista a un interface

Ejemplo:

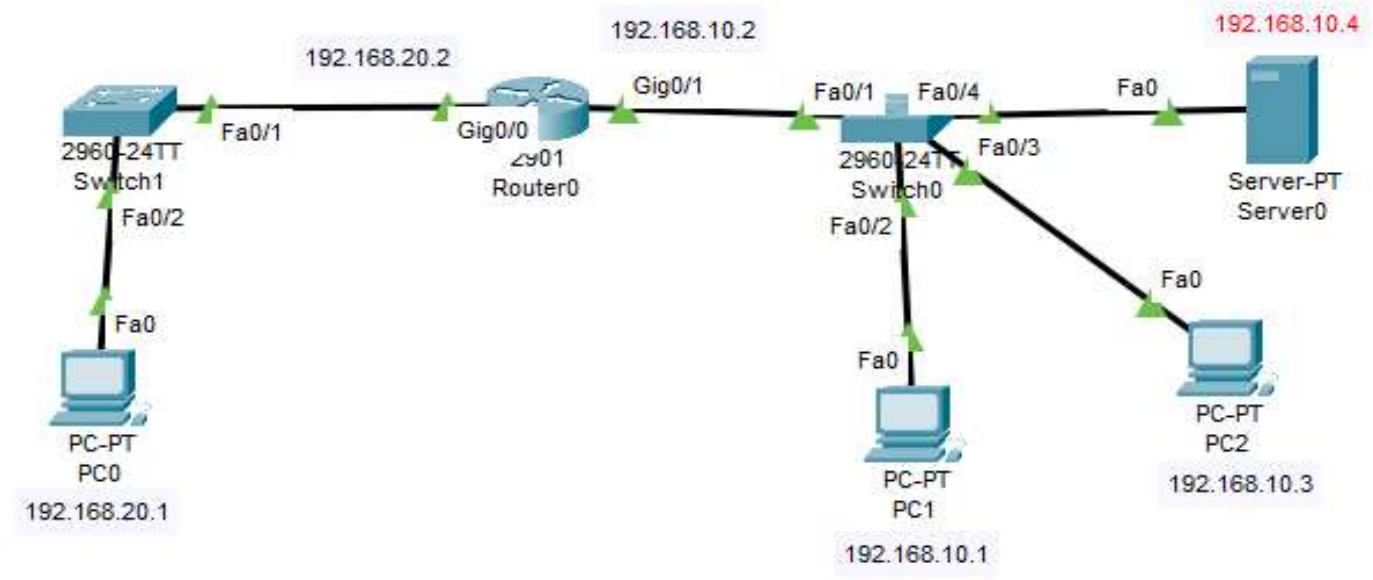
R1(config) #interface gi0/0

R1(config-if)#ip access-group 105 in

# Ejemplo 1

Crear una ACL 101 que :

- Deniegue el trafico de telnet del host 192.168.20.1 al router, pero permitir trafico IP.



# Solución

Ejercicio 1

Solución 1

access-list 101 deny tcp host 192.168.20.1 host 192.168.20.2 eq telnet

access-list 101 permit ip any any

Solución 2

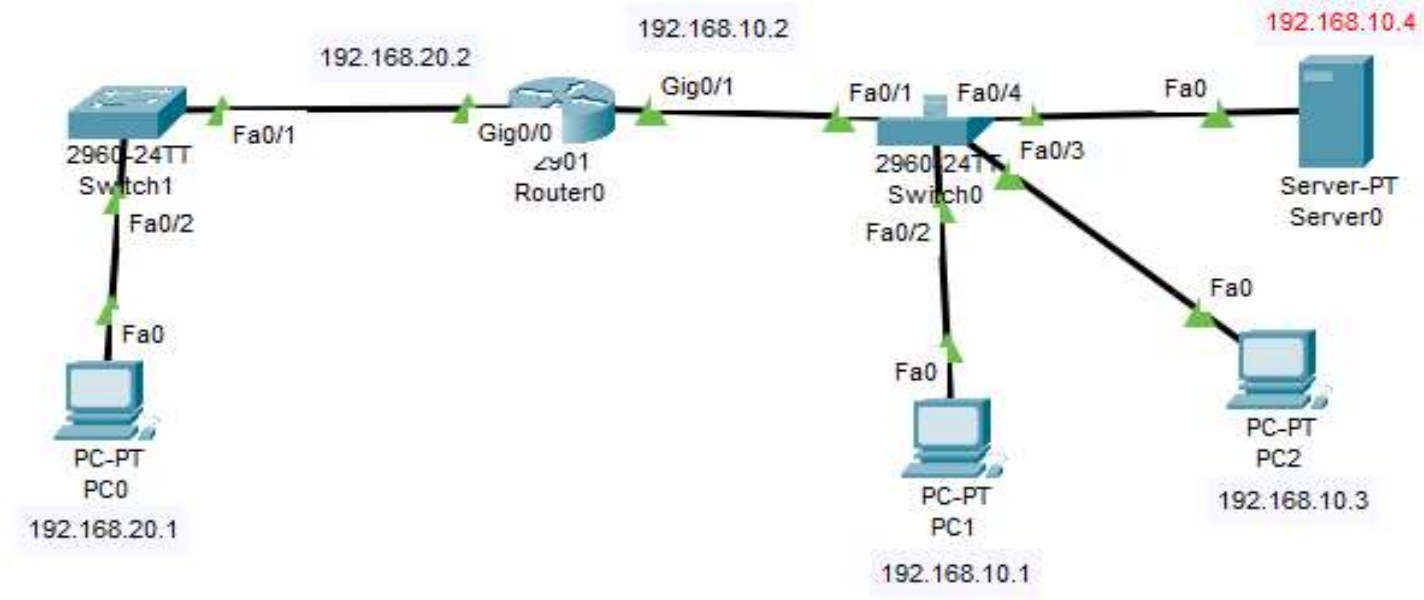
access-list 101 deny tcp any any eq telnet

access-list 101 permit ip any any

# Ejemplo 2

Crear una ACL 102 que:

- Denegar el trafico de FTP del host 192.168.20.1 al server 192.168.10.4 y permitir el trafico IP



# Solución

Ejercicio 2

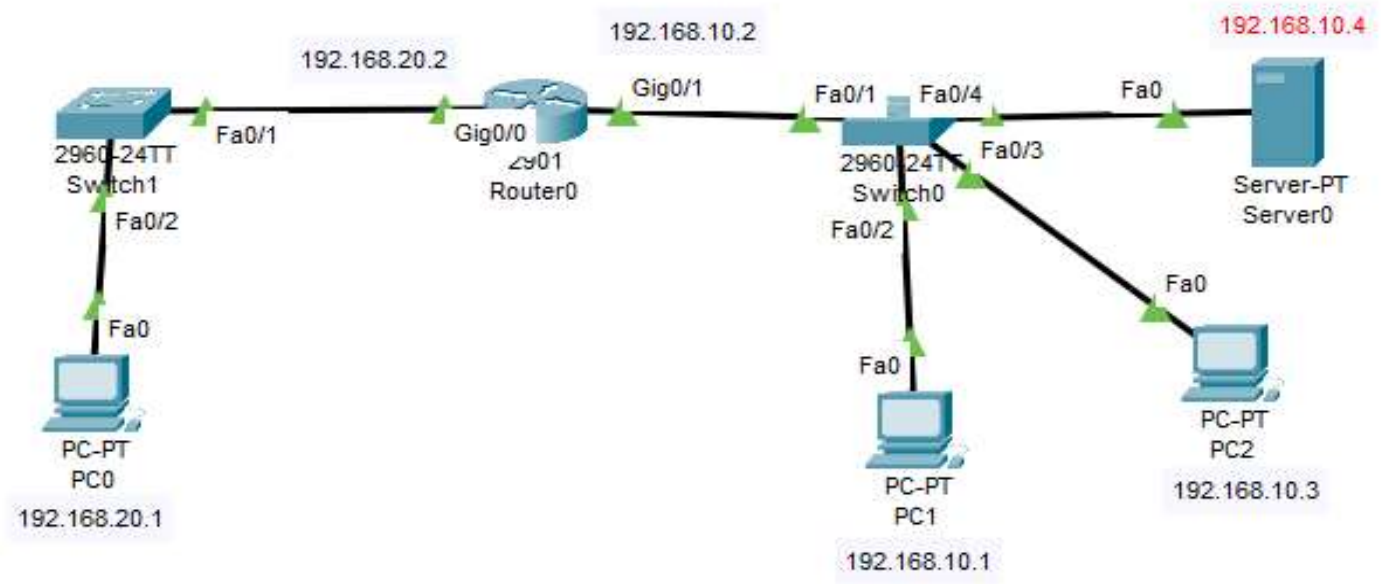
access-list 102 deny tcp host 192.168.20.1 host 192.168.10.4 eq ftp

access-list 102 permit ip any any

# Ejemplo 3

Crear una ACL 103 que:

- Deniegue el ping del host 192.168.20.1 al host 192.168.10.3 y si permita el ping a otros hosts.



# Solución

Ejercicio 3

Solución 1

access-list 103 deny icmp host 192.168.20.1 host 192.168.10.3 echo

access-list 103 permit icmp any any

Solución 2

access-list 103 deny ip host 192.168.20.1 host 192.168.10.3

access-list 103 permit ip any any

# Comandos ACL

Mostrar las listas de acceso:

Router#show access-list

```
Router#sh access-lists
Extended IP access list 101
    10 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 (108 match(es))
Extended IP access list 102
    10 deny tcp any any eq ftp (12 match(es))
    20 permit ip any any (53 match(es))
Extended IP access list 103
    9 deny icmp host 192.168.20.1 host 192.168.10.3 (4 match(es))
    10 permit icmp any any (12 match(es))
```

Borrar una ACL:

Router(config)#no access-list n