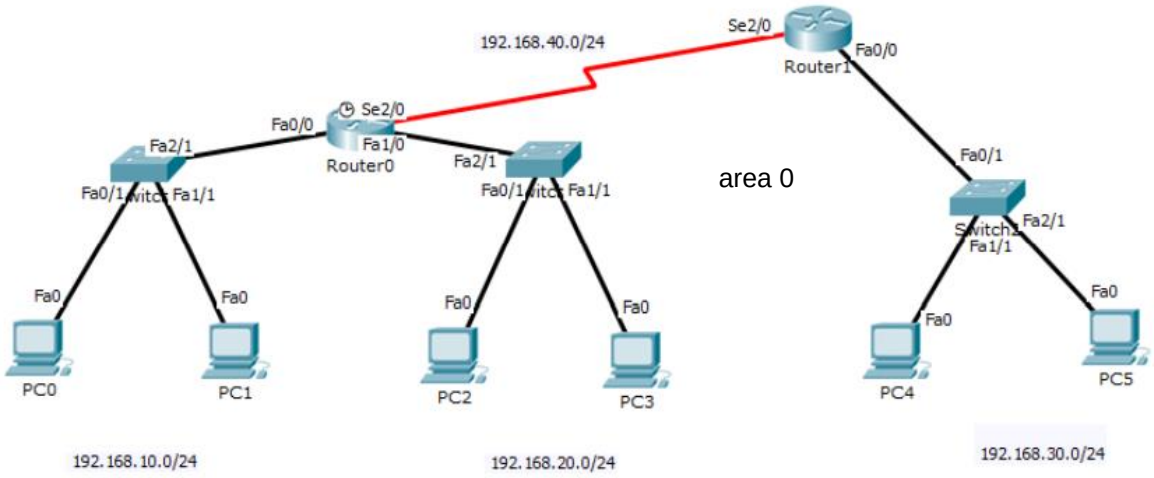
Computer Network Lab– ENCS4130
EXP. No. 6. Access Lists

Prepared by: **Ayham Hashesh**
Modified by: **Ibrahim Nemer**

1

Build the Topology:

Insert the devices & Wiring them.



2

Assign the IPs:

To Routers & PCs.

3

Connectivity Check:

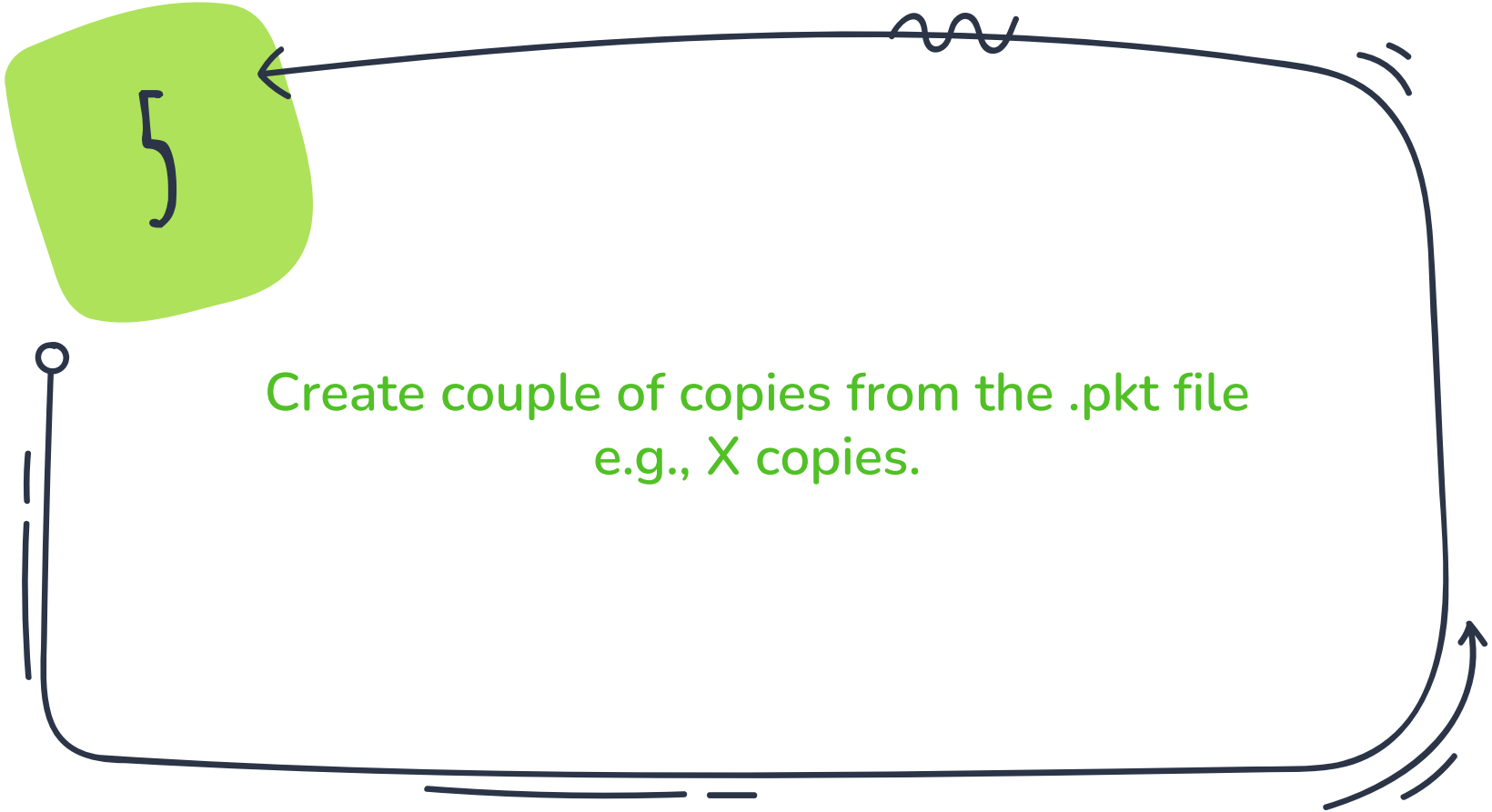
Make sure that each PC can reach the GW.
In addition, you need to make sure that
each adjacent routers can reach each other.

4

Routing:

Configure OSPF on the Routers

Make Sure that all PCs can ping each other


5
Create couple of copies from the .pkt file
e.g., X copies.

ACL Access Control List

- Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces to provide security for your network.

- **IMPORTANT NOTE:**
  After creating the ACL and attaching it to an interface. At the end of every access list there is an implied **"deny all traffic"** criteria statement.

Standard Access Control List

- **Permit** or **deny** traffic based on the **source IP address.**
- Range **1-99**
- It don't distinguish between the IP traffic: TCP, UDP, HTTPs, etc.

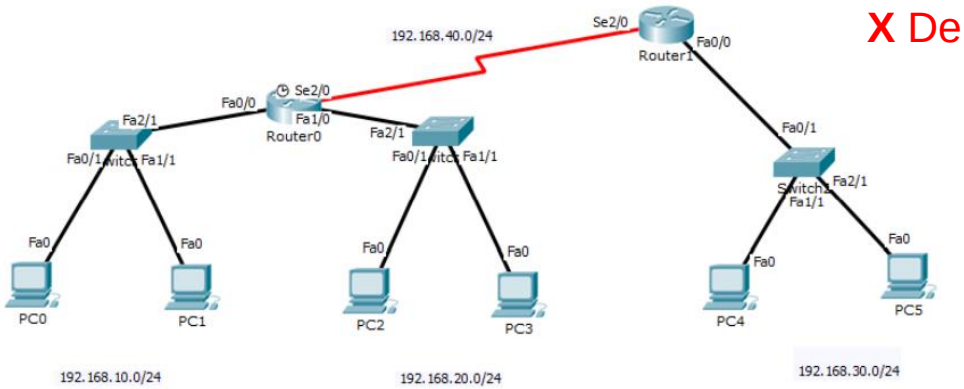
Syntax:

$ access-list <ACL-NUM> <permit | deny> < host | source sourceWildCardMask | any>

Standard Access Control List

A. Prevent PC0 to access network **192.x.20.0 /24**

- On which Router we need to create the Access List?
- On Which Interface we need to put the Access List?
- Type (Input or output) ?

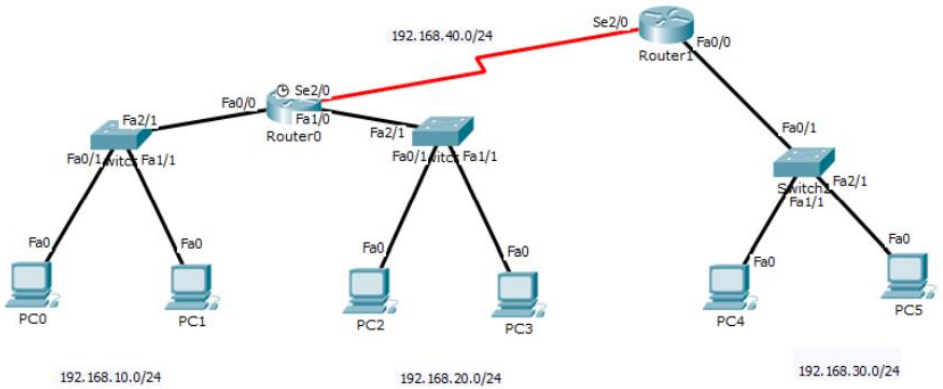


X Depend on your UID.

Standard Access Control List

A. Prevent PC0 to access network **192.168.20.0 /24**

- On which Router we need to create the Access List? **Router0**
- On Which Interface we need to put the Access List? **Fa1/0**
- Type (Input or output) ? **out**



Standard ACL

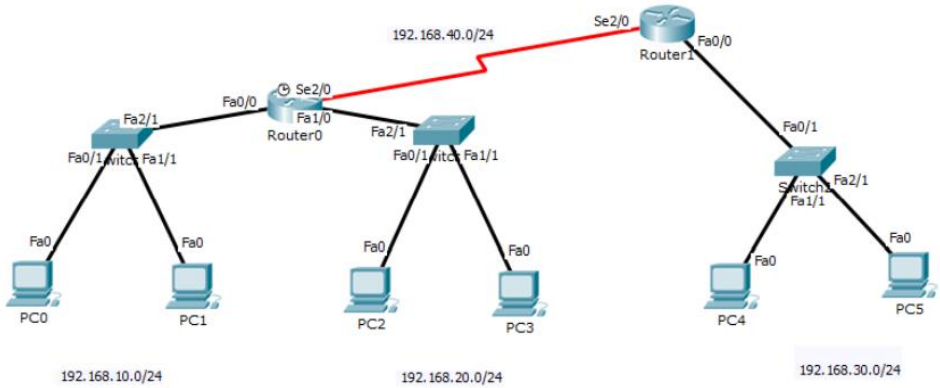
OPTIOMAL SOLUTION

We Put the ACL on the interface that is closet to the destination with the type out

Be aware: You can come with other solution.

SACL

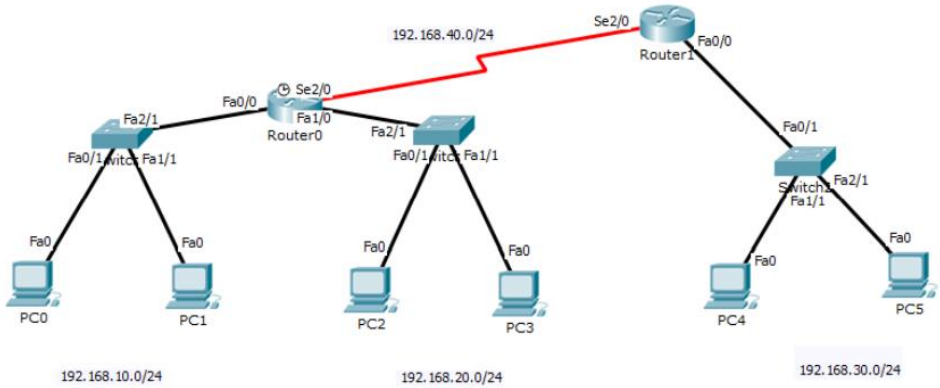
A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.



Router0(config)# access-list ?

SACL

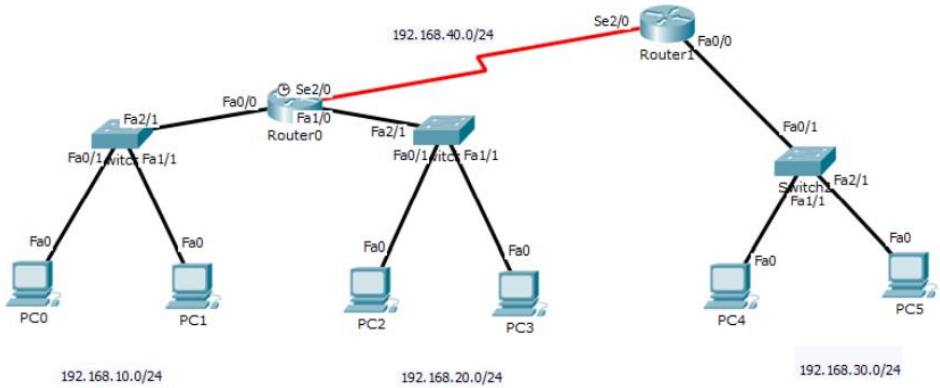
A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.



Router0(config)# access-list 10 ?

SACL

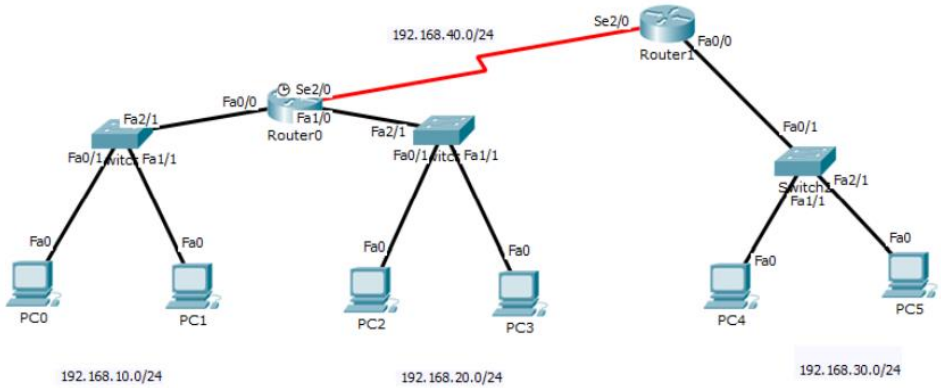
A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.



Router0(config)# access-list 10 deny ?

SACL

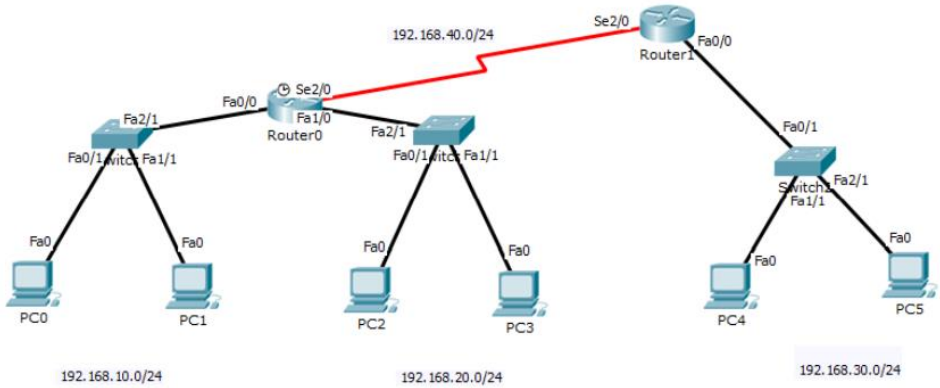
A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.



Router0(config)# access-list 10 deny host ?

SACL

A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.



Router0(config)# access-list 10 deny host 192.168.10.2

SACL

A. Prevent PC0 to access network 192.168.20.0/24 using standard access control list.

COPY 1

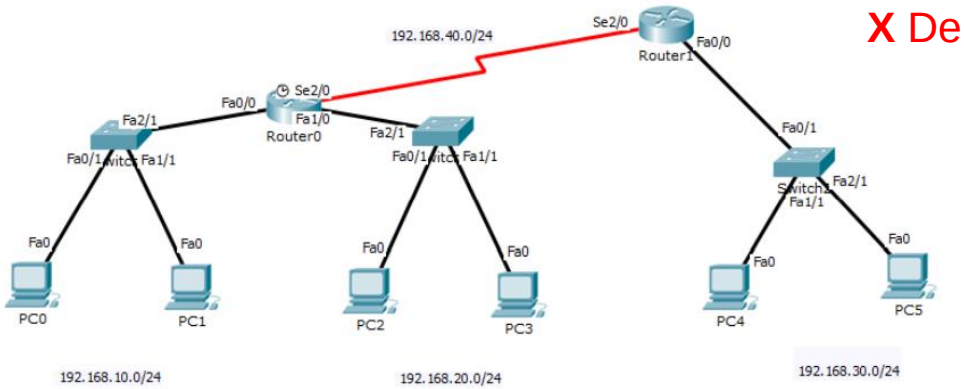
All CMDs:

```
Router0(config)# access-list 10 deny host 192.168.10.2
Router0(config)# access-list 10 permit any
Router0(config)# interface fa1/0
Router0(config-if)# ip access-group 10 out
```

Standard Access Control List

B. Allow just PC3 to access network 192.**x**.30.0 /24 using the Standard ACLs and deny any other traffic.

- On which Router we need to create the Access List?
- On Which Interface we need to put the Access List?
- Type (Input or output) ?

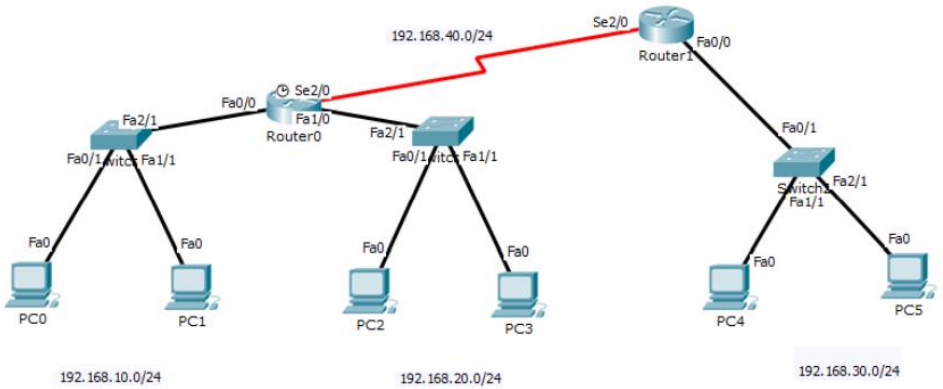


X Depend on your UID.

Standard Access Control List

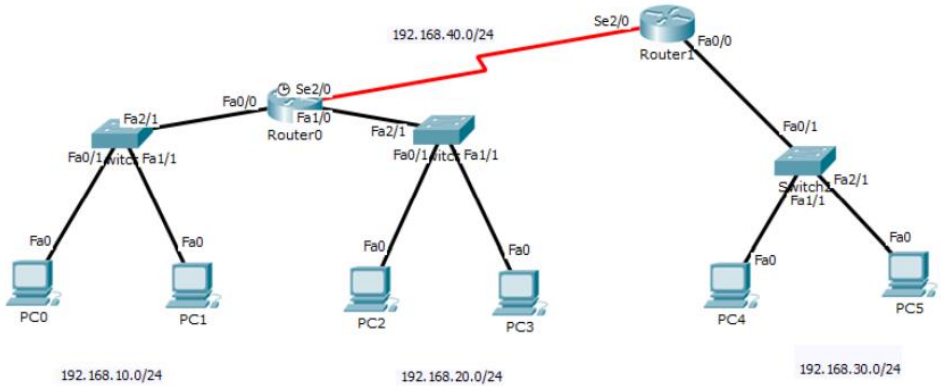
B. Allow just PC3 to access network 192.**x**.30.0 /24 using the Standard ACLs and deny any other traffic.

- On which Router we need to create the Access List? **Router1**
- On Which Interface we need to put the Access List? **Fa0/0 or Se2/0**
- Type (Input or output) ? **Out (Fa0/0) or In (Se2/0)**



SACL

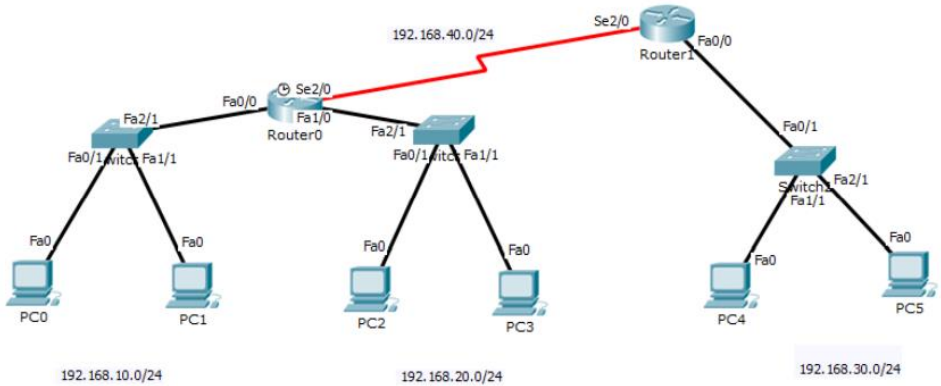
B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.



Router1(config)# access-list ?

SACL

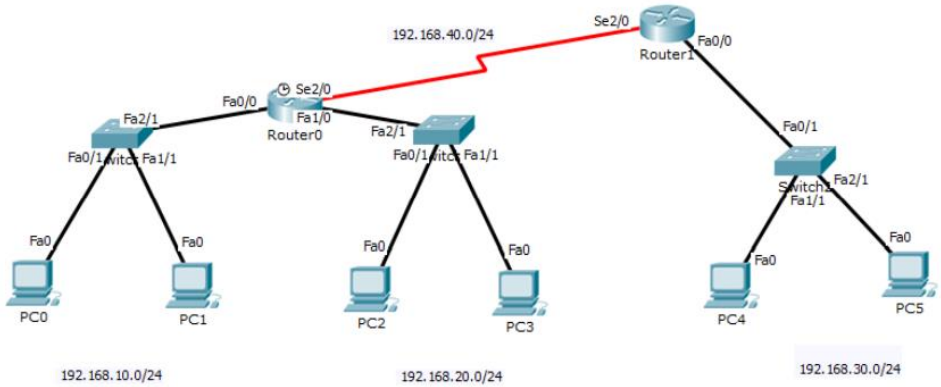
B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.



Router1(config)# access-list 15 ?

SACL

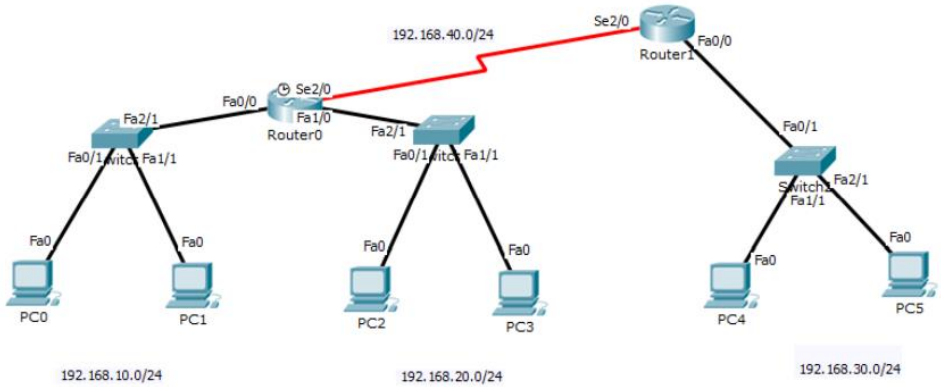
B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.



Router1(config)# access-list 15 permit ?

SACL

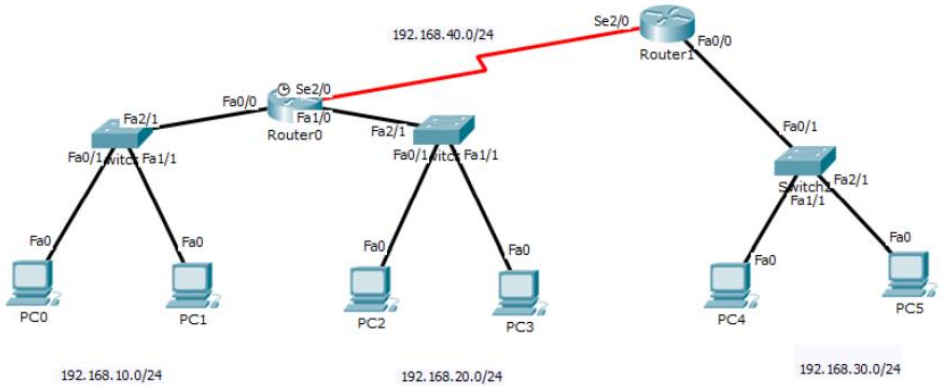
B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.



Router1(config)# access-list 15 permit host ?

SACL

B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.



Router1(config)# access-list 15 permit host 192.168.20.3 ?

SACL

B. Allow just PC3 to access network 192.168.30.0/24 using the Standard ACLs and deny any other traffic.

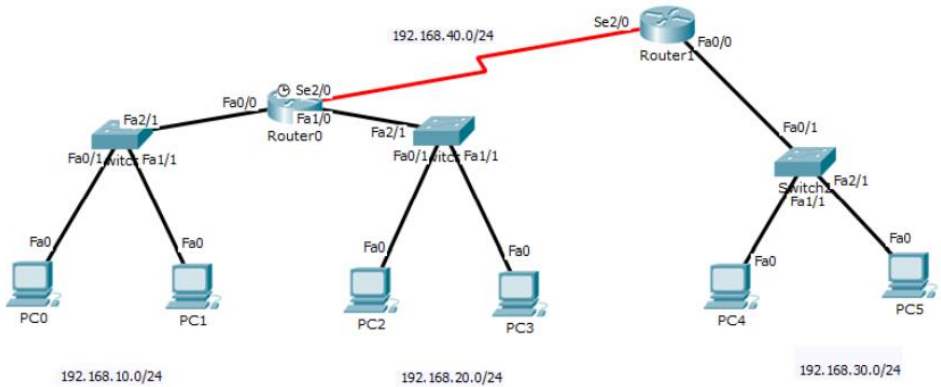
COPY 2

All CMDs:

```
Router1(config)# access-list 15 permit host 192.168.20.3
Router1(config)# interface fa0/0
Router1(config-if)#ip access-group 15 out
```

SACL

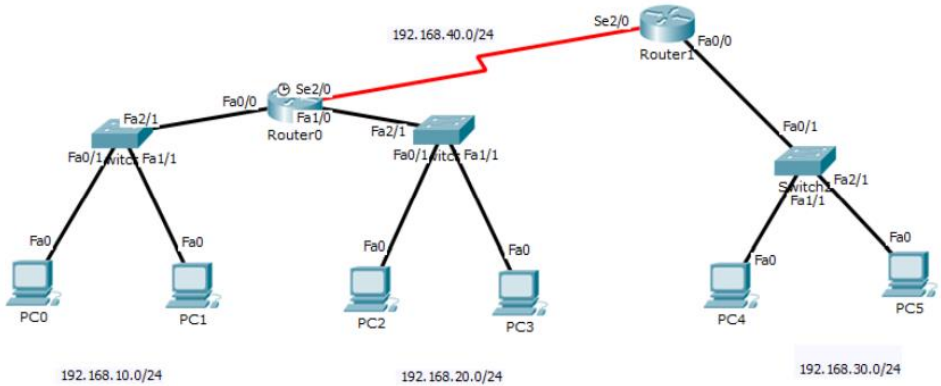
C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).



Router0(config)# access-list ?

SACL

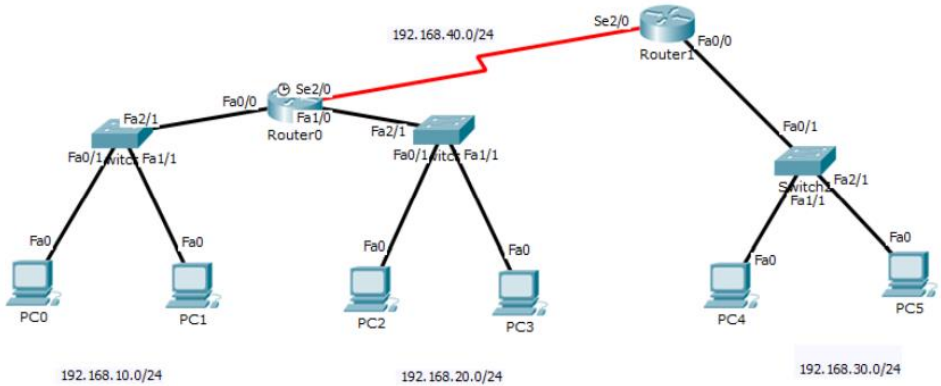
C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).



Router0(config)# access-list 20 ?

SACL

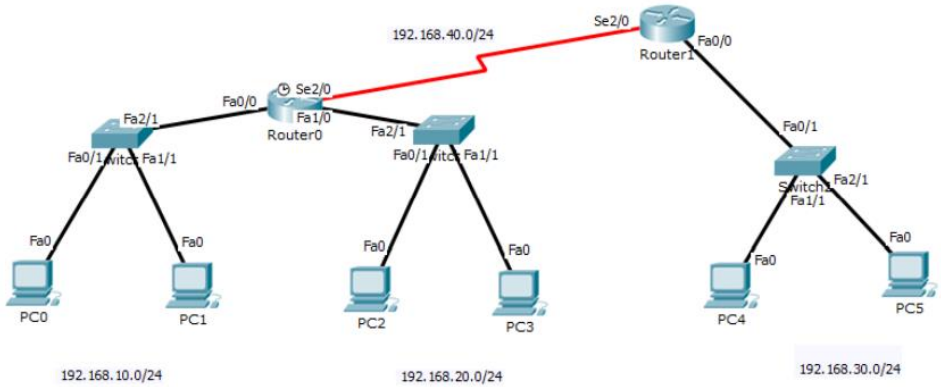
C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).



Router0(config)# access-list 20 deny ?

SACL

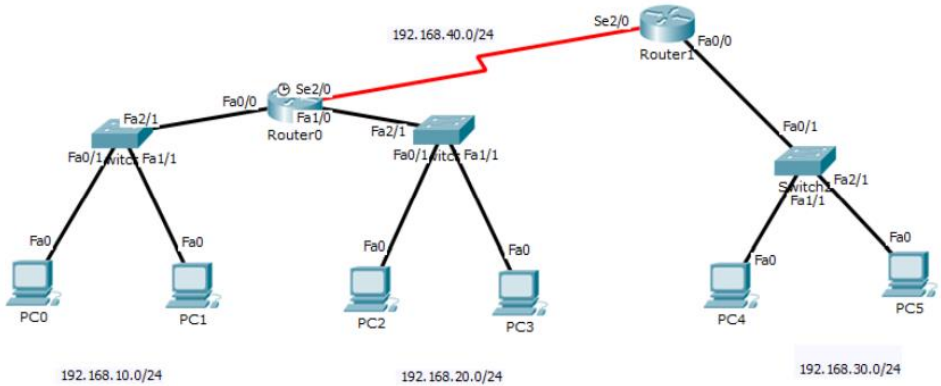
C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).



Router0(config)# access-list 20 deny 192.168.10.0 ?

SACL

C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).



Router0(config)# access-list 20 deny 192.168.10.0 0.0.0.255

SACL

C. Prevent network 192.168.10.0 from accessing network 192.168.20.0 only (use the wild card, not ‘any’ option).

COPY 3

All CMDs:

```
Router0(config)# access-list 20 deny 192.168.10.0 0.0.0.255
Router0(config)# access-list 20 permit any
Router0(config)# interface fa1/0
Router0(config-if)#ip access-group 20 out
```

Extended Access Control List

- Permit or deny traffic based on the Source and the Destination IP address.
- Range **100-199**
- Distinguish between the IP traffic TCP, UDP, HTTPs, etc.
- We can use the port number.

Syntax:

$ access-list <ACL-NUM> <permit | deny> <Protocol> < host | source sourceWildCardMask | any> < host | destination destinationWildCardMask | any> eq <portNumber>

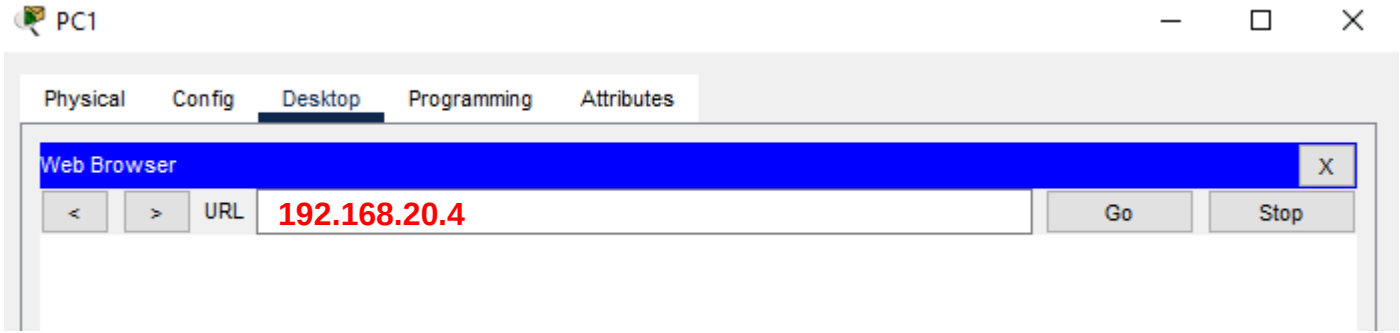
TODO

Add server device to the network 192.x.20.0 /24

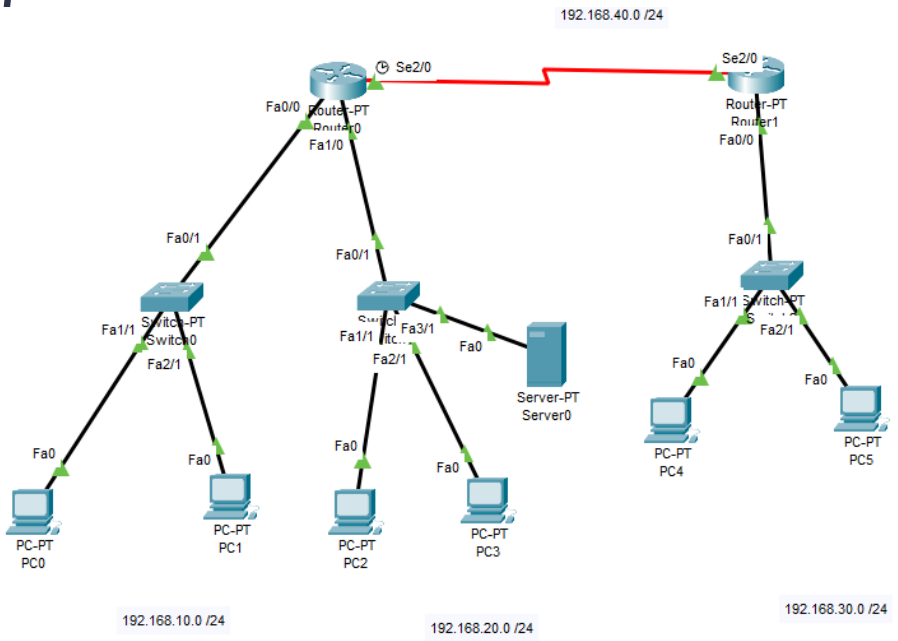
Extended Access Control List

How to make HTTP Request?

Press on the PC → Desktop → Web Browser → Type Server/PC IP address in URL → Press Go



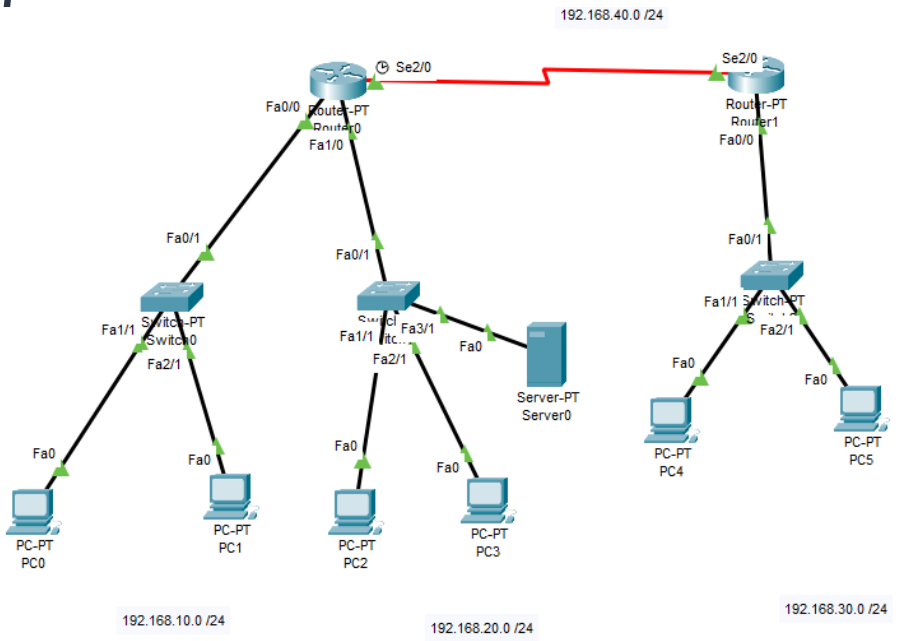
Extended Access Control List



A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).

- On which Router we need to create the Access List?
- On Which Interface we need to put the Access List?
- Type (Input or output) ?

Extended Access Control List



A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).

- On which Router we need to create the Access List? **Router 1**
- On Which Interface we need to put the Access List? **Fa0/0**
- Type (Input or output) ? **IN**

Extended ACL

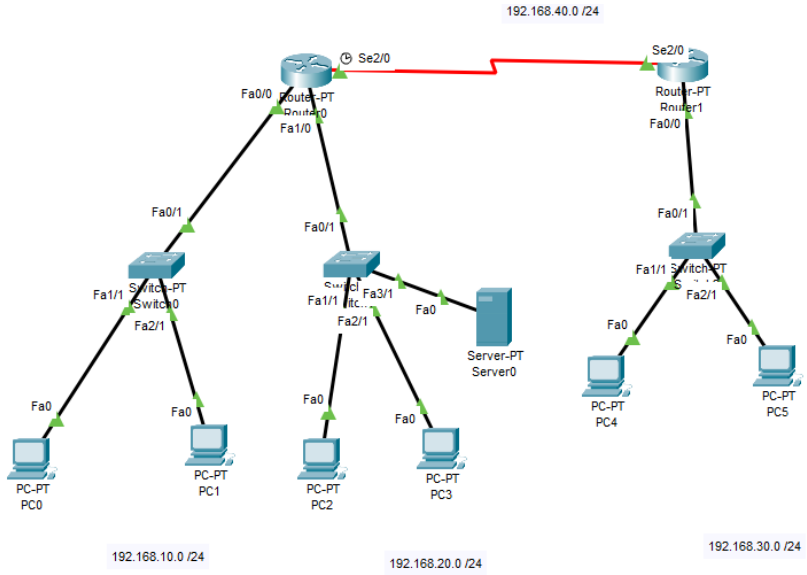
OPTIMAL SOLUTION

We Put the ACL on the interface that is closet to the source with the type in

Be aware: You can come with other solution.

EACL

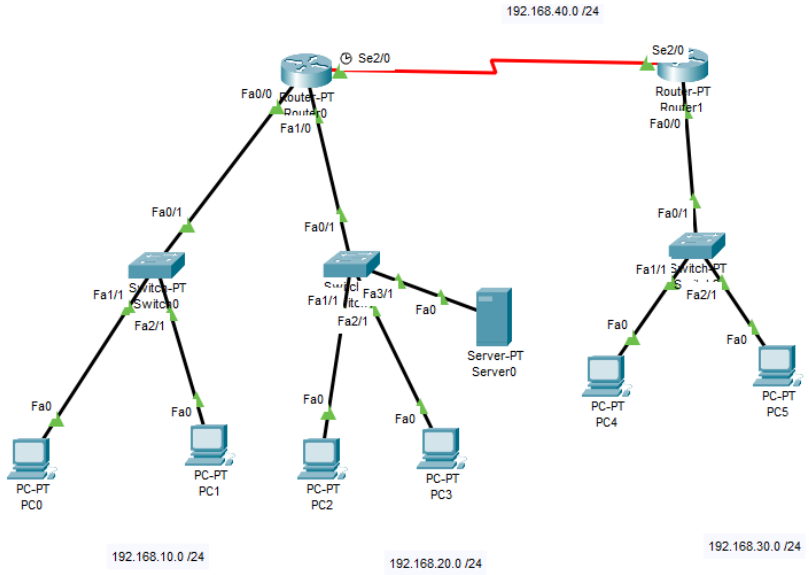
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list ?

EACL

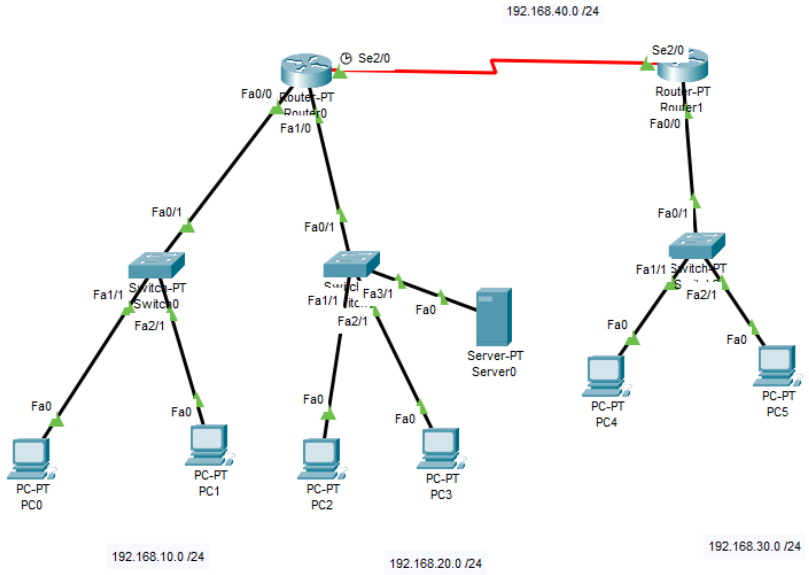
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 ?

EACL

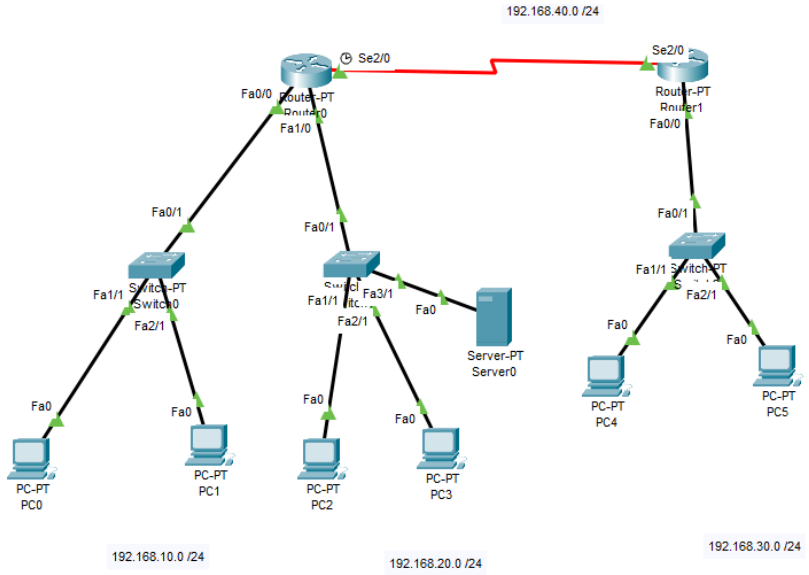
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny ?

EACL

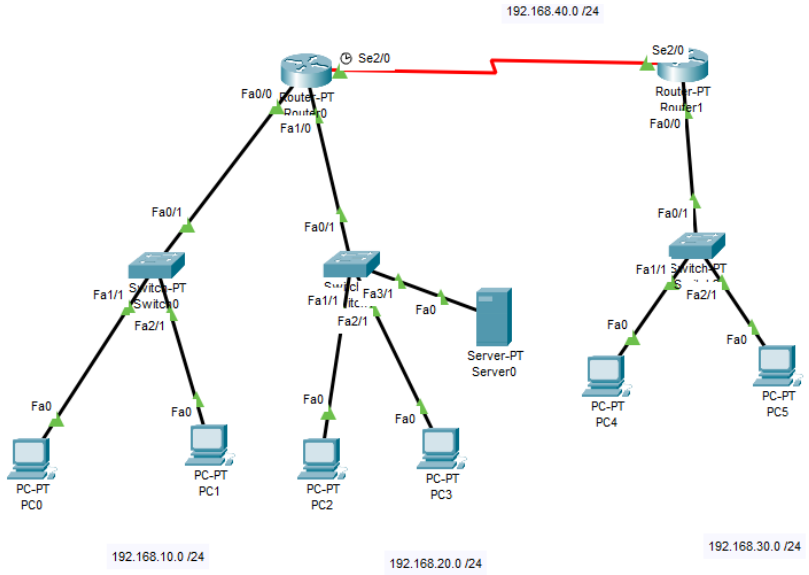
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp ?

EACL

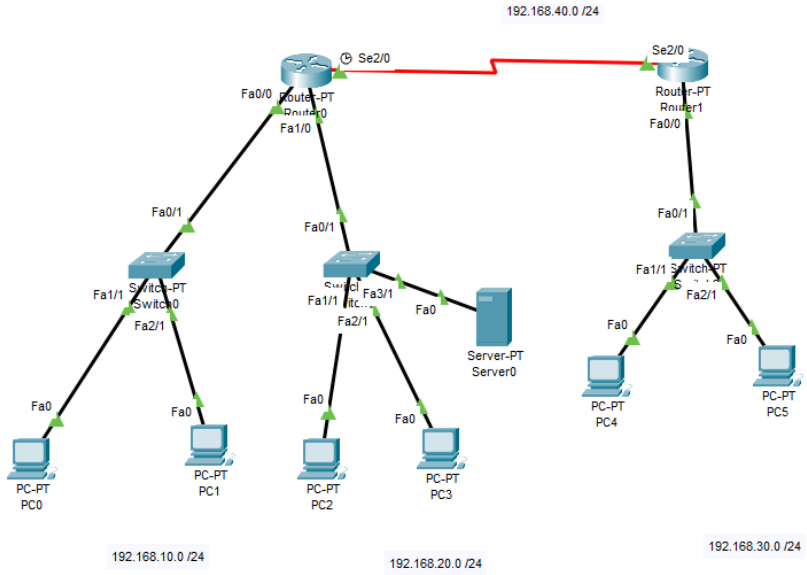
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host ?

EACL

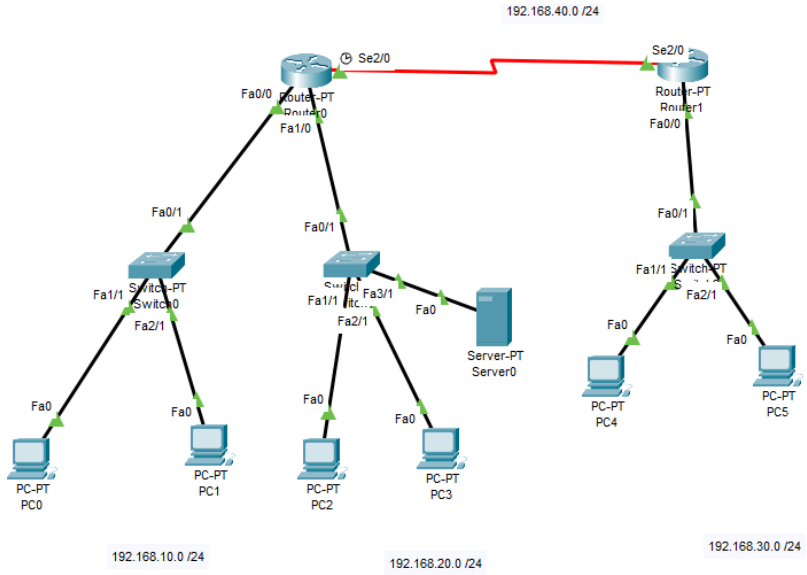
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host 192.168.30.2 ?

EACL

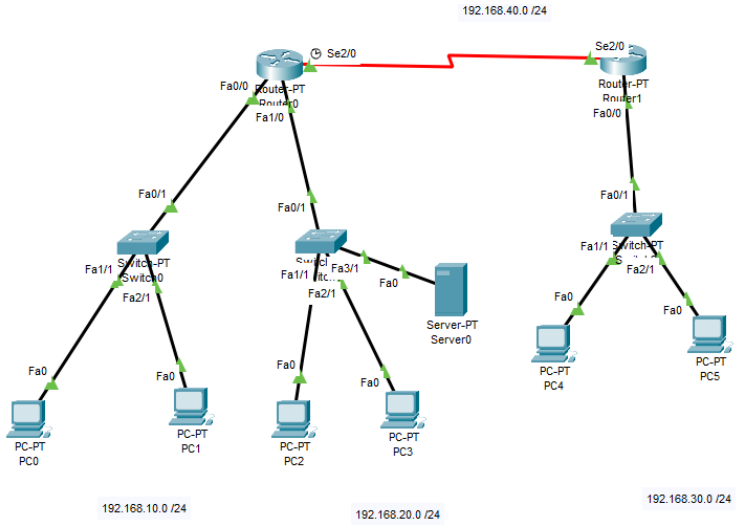
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host 192.168.30.2 host ?

EACL

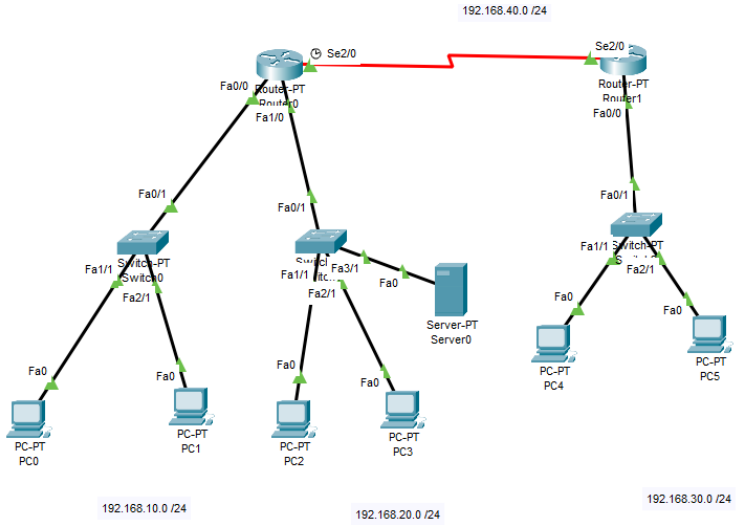
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host 192.168.30.2 host 192.168.20.4 ?

EACL

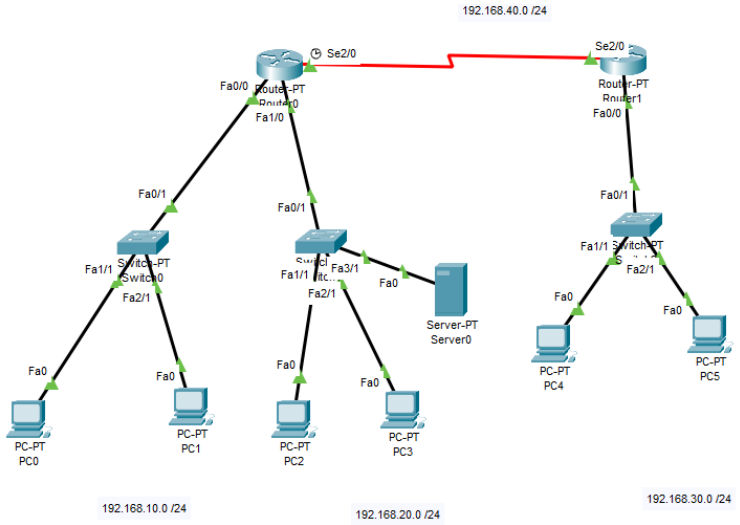
A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host 192.168.30.2 host 192.168.20.4 eq ?

EACL

A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).



Router1(config)# access-list 101 deny tcp host 192.168.30.2 host 192.168.20.4 eq 80

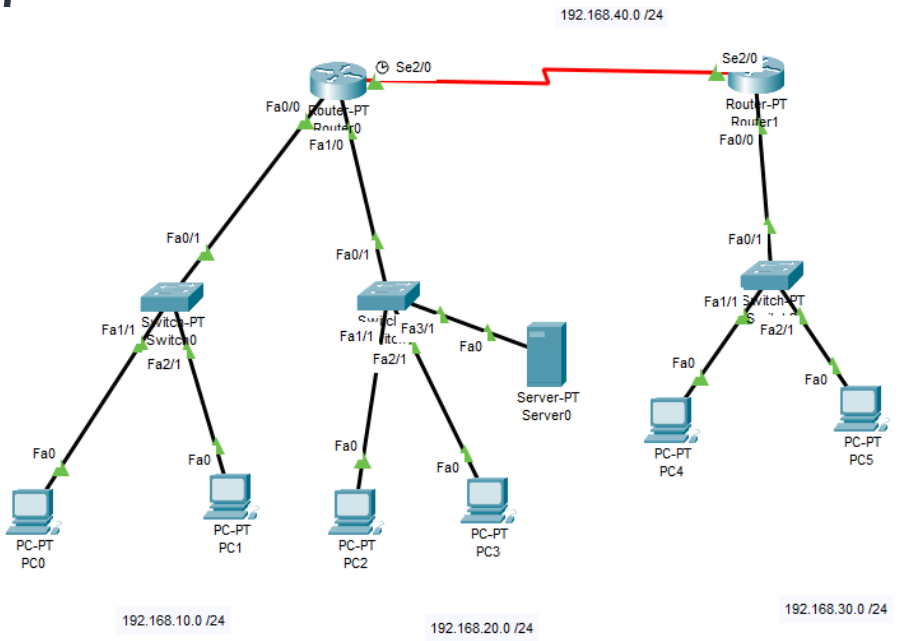
EACL

A. Deny PC4 to make HTTP request via TCP to the Server. (all other traffic is allowed).

All CMDs:

```
Router1(config)# access-list 101 deny tcp host 192.168.30.2 host 192.168.20.4 eq 80
Router1(config)# access-list 101 permit ip any any
Router1(config)# interface fa0/0
Router1(config-if)# ip access-group 101 in
```

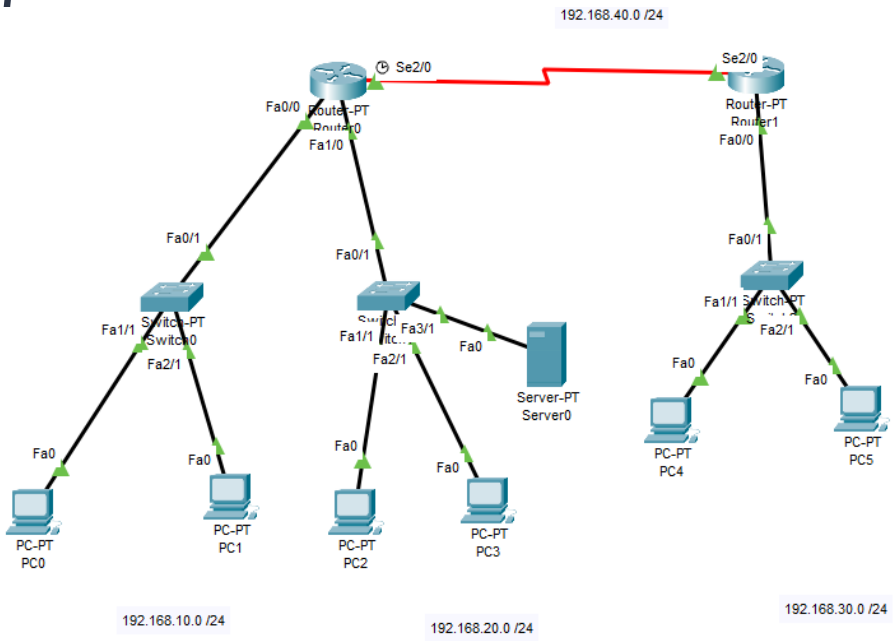
Extended Access Control List



B. Prevent PC0 from accessing PC2 (All other traffic is allowed)

- On which Router we need to create the Access List?
- On Which Interface we need to put the Access List?
- Type (Input or output) ?

Extended Access Control List

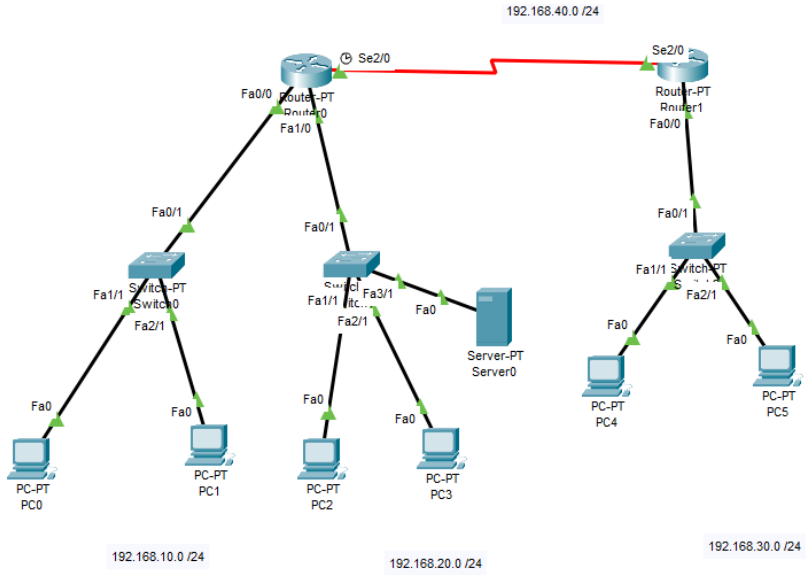


B. Prevent PC0 from accessing PC2 (All other traffic is allowed)

- On which Router we need to create the Access List? **Router 0**
- On Which Interface we need to put the Access List? **Fa0/0**
- Type (Input or output) ? **IN**

EACL

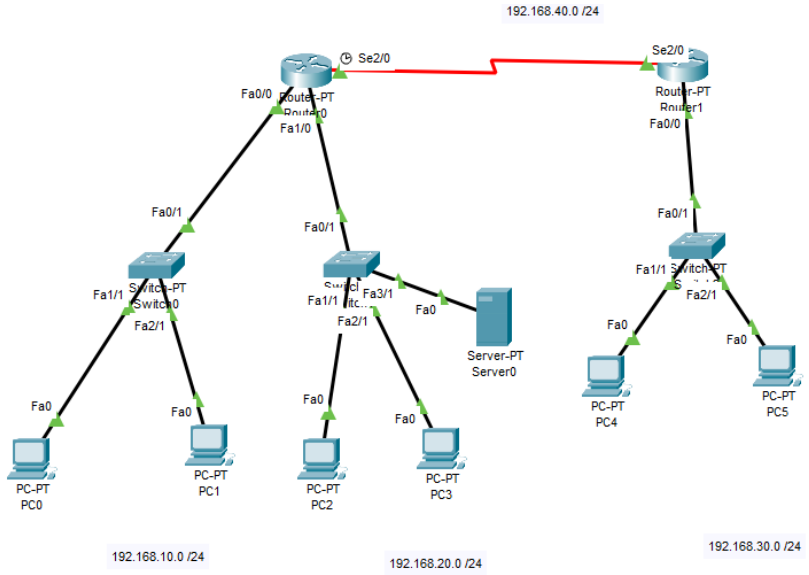
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list ?

EACL

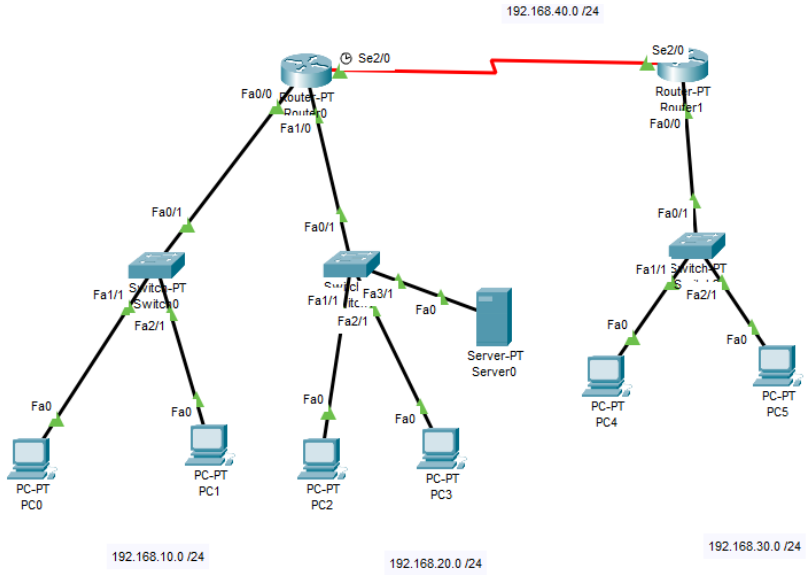
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 ?

EACL

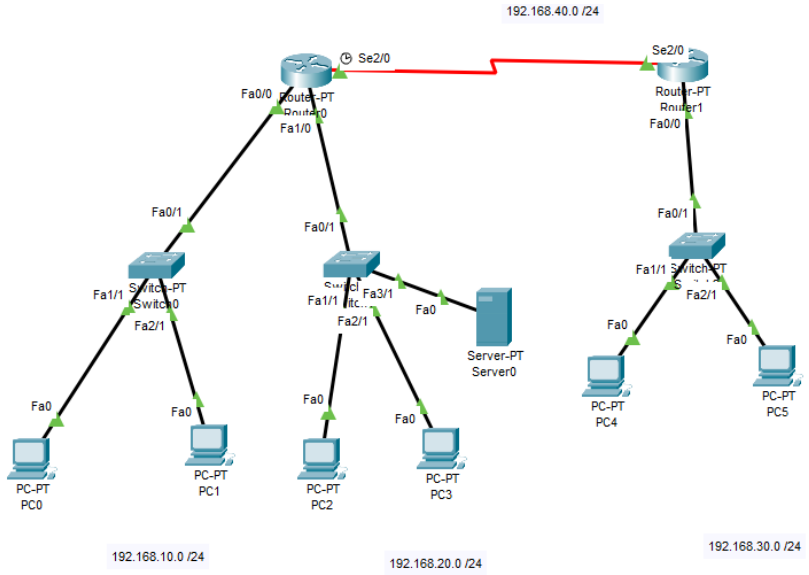
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ?

EACL

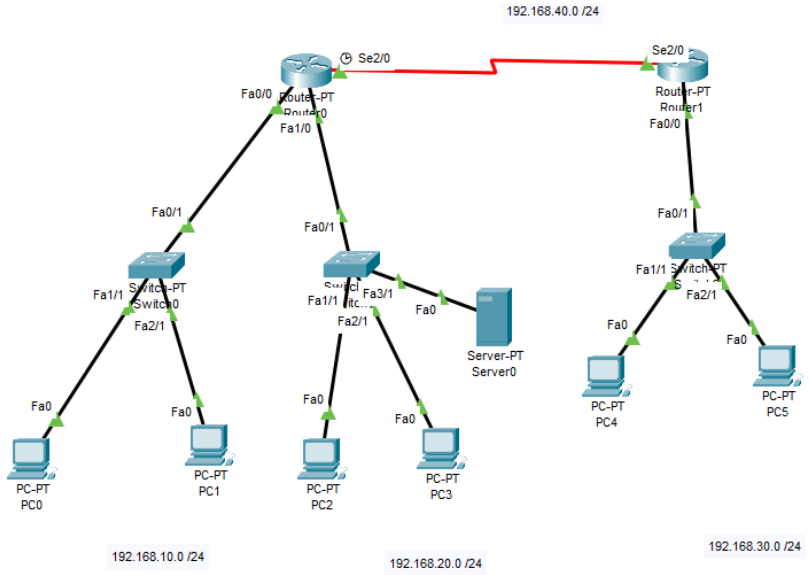
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ip ?

EACL

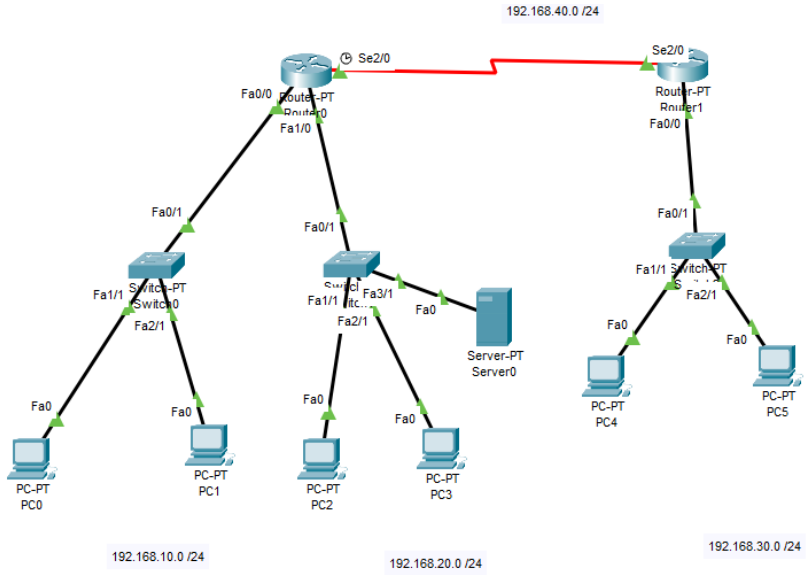
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ip host ?

EACL

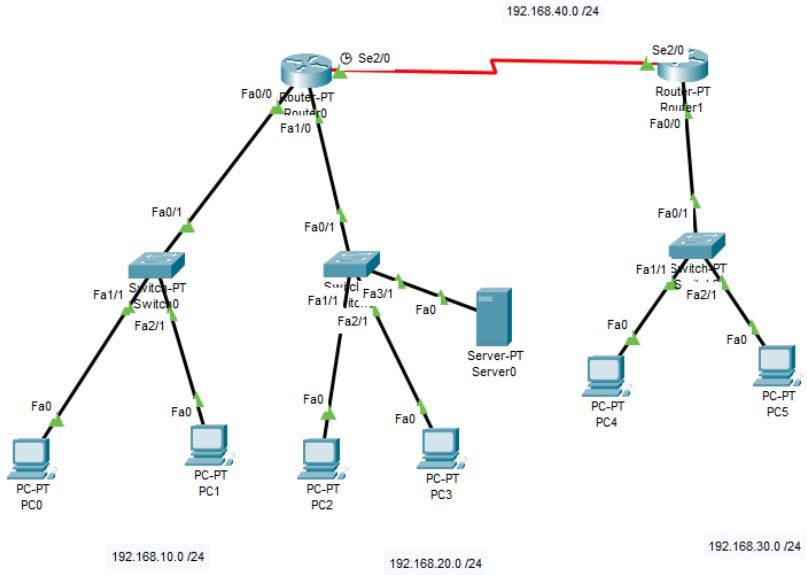
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ip host 192.168.10.2 ?

EACL

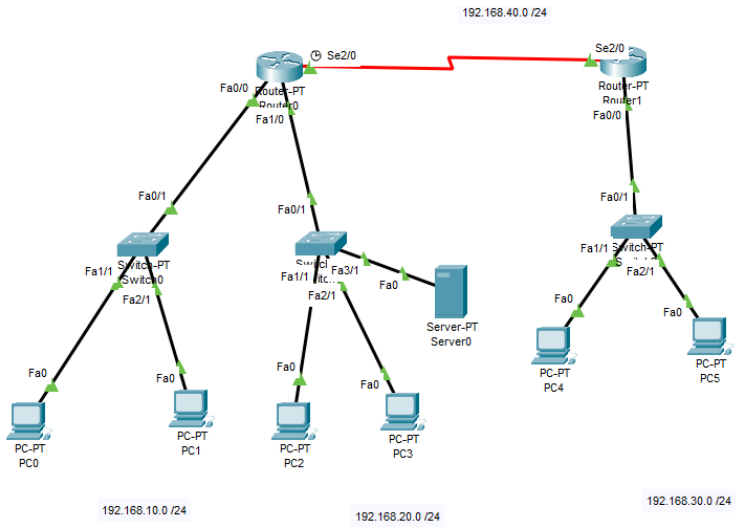
B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ip host 192.168.30.2 host ?

EACL

B. Prevent PC0 from accessing PC2 (All other traffic is allowed)



Router0(config)# access-list 101 deny ip host 192.168.30.2 host 192.168.20.2 ?

EACL

B. Prevent PC0 from accessing PC2 (All other traffic is allowed)

All CMDs:

```
Router0(config)# access-list 101 deny ip host 192.168.10.2 host 192.168.20.2
Router0(config)# access-list 101 permit ip any any
Router0(config)# interface fa0/0
Router0(config-if)# ip access-group 101 in
```


END