

**كلية العلوم**

**قــســــــــــم الانـــظــــمــــة الــــطـبـيـة الـــذكــــــيـــة**

**Intelligent Medical Systems Department**

**محاضرة نظري وعملي لمنع وصول بيانات من راوتر الى اخر**

**Class: Third**

**Lecturer:** **Prof. Dr. Mehdi Ebady Manaa**

**Lecture: Implementing ACLs in Cisco Routers (Topology Scenario)**



In this lesson, we explore how to implement Access Control Lists (ACLs) in a given network topology. The goal is to block all traffic from PC-A (192.168.1.0/24) to PC-C (192.168.3.0/24) using extended ACLs on Router R1 and Router R2.

# Then;

- Understand and configure extended ACLs.
- Block specific inter-network traffic.
- Apply ACLs in the correct direction and interface.
- Verify and test ACL functionality.

# Topology details

Key IP Networks:
- PC-A: 192.168.1.0/24
- PC-C: 192.168.3.0/24
- Serial Link (R1-R2): 10.1.1.0/30
- Serial Link (R2-R3): 10.2.2.0/30

# Access Control List (ACL) Concept

An Access Control List is a set of rules that either permit or deny traffic. Extended ACLs allow filtering by source and destination IP, protocol, and port.

##  Configuration on R1

1. Enter global configuration mode:
 R1> enable
 R1# configure terminal

2. Create ACL 100 to block traffic from PC-A to PC-C:
 R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 R1(config)# access-list 100 permit ip any any

3. Apply the ACL to outbound traffic on the serial interface:
 R1(config)# interface s0/0/0
 R1(config-if)# ip access-group 100 out

**Where**

R1(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list [ACL\_NUMBER] [permit|deny] [PROTOCOL] [SOURCE\_IP] [WILDCARD\_MASK] [DEST\_IP] [WILDCARD\_MASK]



## Configuration on R2 (Optional Backup ACL)

1. Enter configuration mode:
 R2> enable
 R2# configure terminal

2. Create ACL 110:
 R2(config)# access-list 110 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 R2(config)# access-list 110 permit ip any any

3. Apply the ACL to inbound traffic:
 R2(config)# interface s0/0/1
 R2(config-if)# ip access-group 110 in

#  Testing the Configuration

On PC-A, try to ping PC-C:
 PC-A> ping 192.168.3.x

Expected result: Request timed out (due to ACL).

Try pinging other routers or PCs not affected by ACL to ensure traffic is still allowed.

You have successfully:???