ENCS4130
Computer Networks Laboratory

EXP#6 Access Control Lists (ACLs)

Slides By: Eng.Tariq Odeh

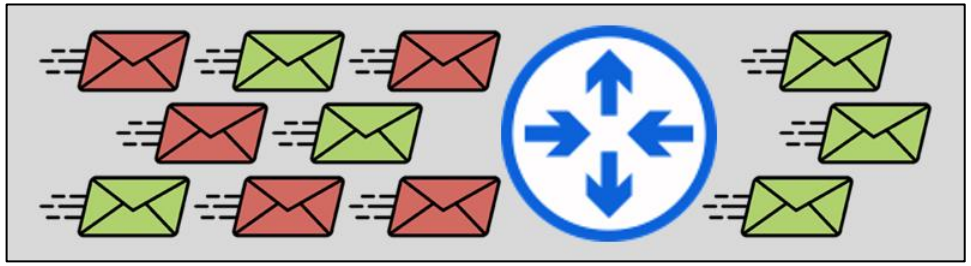
جامعة بيرزيت BIRZEIT UNIVERSITY

Objectives

- Learn how to configure and verify Access Lists with Cisco routers.
- Introducing to Standard ACL and Extended ACL.

Introduction to Access Control Lists (ACLs)

- **What is an ACL?**
  - ACL, or Access Control List, is a set of rules to control network traffic and enhance network security.
- **How ACLs Work?**
  - ACLs filter network traffic by determining whether routed packets are forwarded or blocked at router interfaces.
- **Access List Criteria**
  - Source Address
  - Destination Address
  - Upper-layer Protocols (e.g., TCP, UDP)



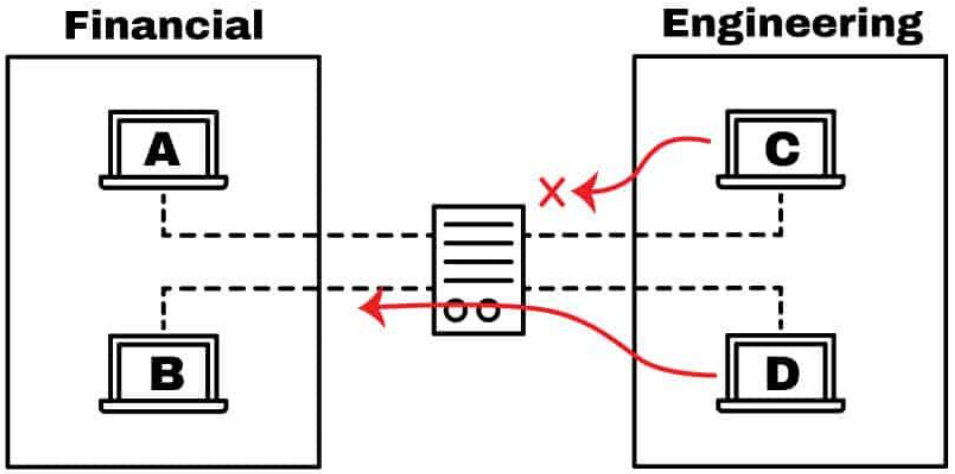
Uses & Creating ACLs

- **Why Use ACLs?**
  - Traffic Flow Control: Manages data flow within networks.
  - Routing Updates: Restricts the spread of specific route data.
  - Network Security: Prevents unauthorized access and controls traffic in/out of the network.

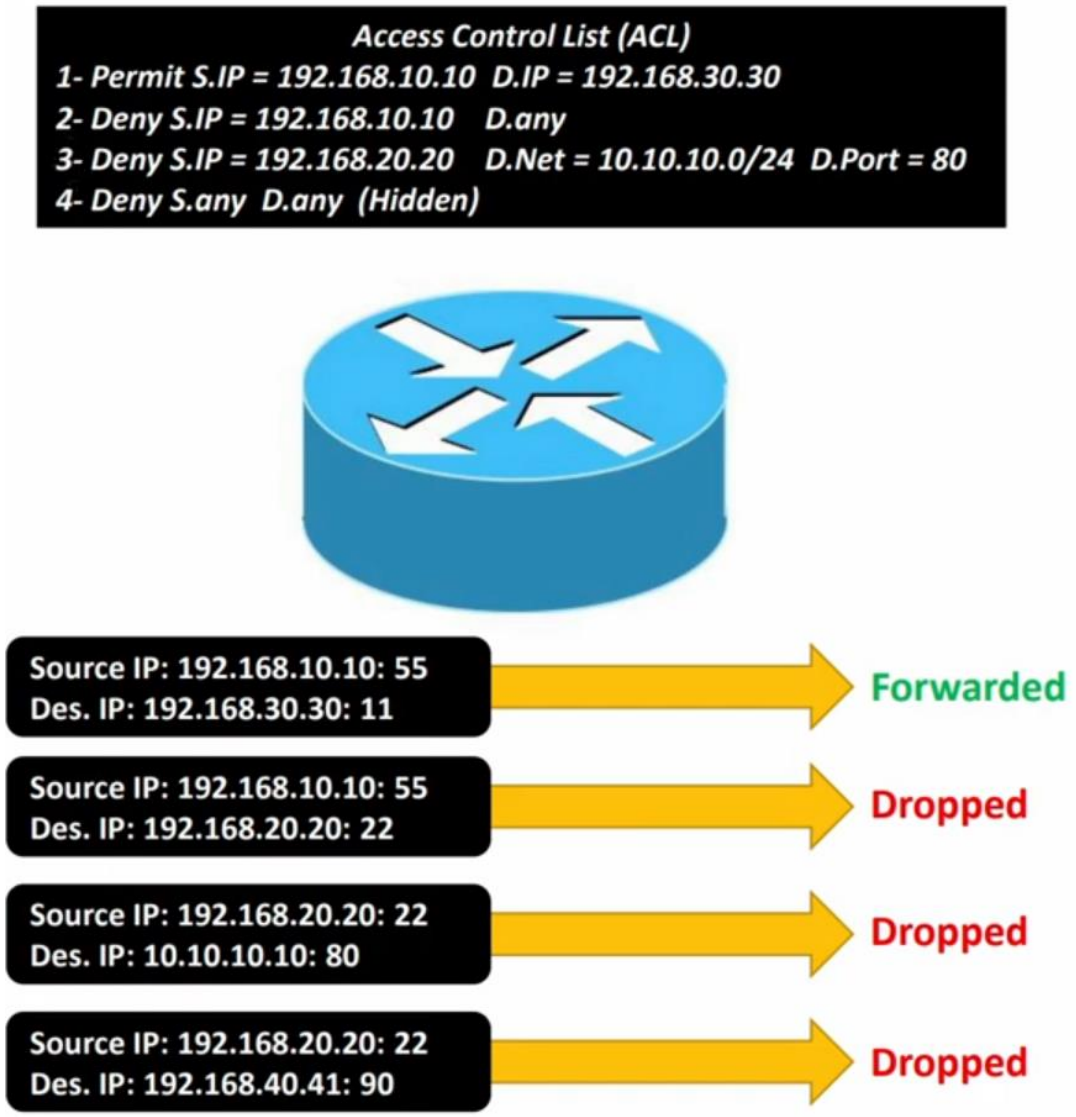
- **Creating an Access List:**
  1. Specify the Protocol: Choose the protocol to filter, like IP, TCP, or UDP.
  2. Assign a Unique Identifier: Each ACL has a unique name or number.
  3. Define Filtering Criteria:
     - Use multiple access control entries (ACEs) to specify source, destination, and ports.
     - Example: Allow TCP traffic from IP 192.168.1.1 to 10.0.0.1 on port 80.

Understanding ACLs Processing

- A packet is tested against the ACL statements in sequential order.
- When a statement matches, the rest of the ACL statements are ignored.
- There is an implicit deny any statement at the end of an ACL. If a packet does not match any of the statements in the ACL, it is dropped

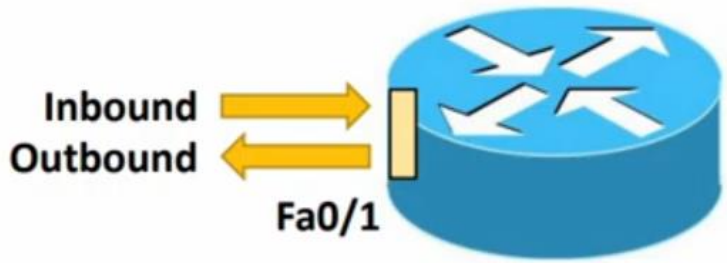


Example:



Applying ACLs on Interfaces

- **Directional Application:**
  - ACLs can be applied to an interface for **inbound** or **outbound** traffic.
  - Separate ACL needed for each direction.
- **Inbound Traffic:**
  - Router checks for inbound ACL on the interface before performing a route table lookup.
- **Outbound Traffic:**
  - Router verifies a route to the destination before applying outbound ACLs.



Named vs. Numbered Access Control Lists (ACLs)

Aspect	Named ACLs	Numbered ACLs
Identification	Referenced by a descriptive name (e.g., "BZU")	Identified by a number (e.g., 10, 101, 105)
Modification Flexibility	Individual rules can be deleted without affecting the entire list	Deleting a rule requires deleting the entire ACL (for extended numbered ACLs)
Management	Provides better management, ideal for extended access lists	Limited management options
Processing Requirements	Requires more processing	Requires less processing

Standard Access Control List (ACL)

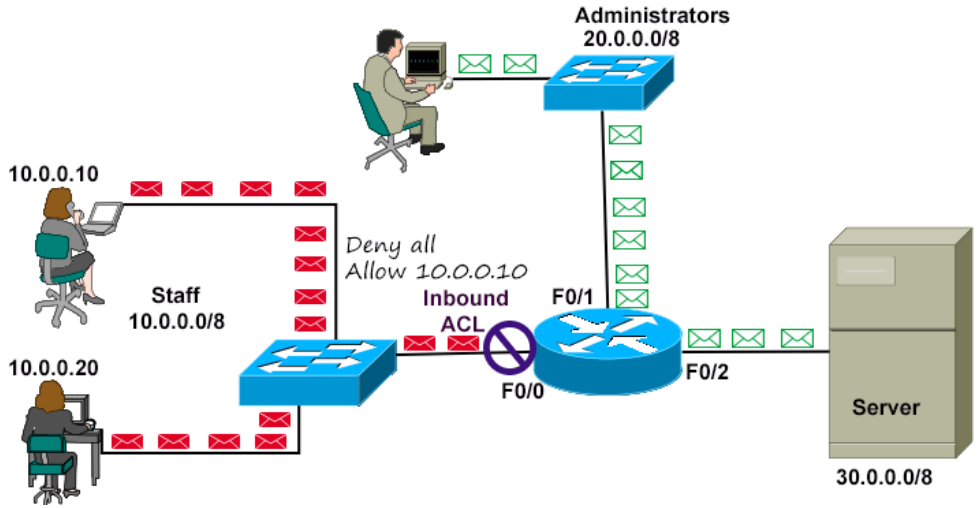
- **Purpose:**
  - Controls network traffic based solely on source IP address.
- **Key Points:**
  - Uses numbers (1-99, 1300-1999).
  - Applies to entire protocol suite (cannot distinguish between specific protocols like TCP, UDP).
  - Commonly applied close to the destination (not always mandatory).
- **Configuration Example:**
  - **Define the ACL:**
    - **Router(config)# access-list <ACCESS-LIST-NUMBER> <permit|deny> <host|source sourceWildCardMask|any>**
  - **Apply the ACL to an interface:**
    - **Router(config)# interface <INTERFACE-NUMBER>**
    - **Router(config-if)# ip access-group <ACCESS-LIST-NUMBER> <in|out>**

Extended Access Control List (ACL)

- **Purpose:**
  - Filters traffic using source and destination IP addresses, protocol, and port number.
- **Key Points:**
  - Uses numbers (100-199, 2000-2699).
  - Allows for granular control over specific traffic types (e.g., allowing HTTP but blocking FTP).
  - Commonly applied close to the source (though placement can vary).
- **Configuration Example:**
  - **Define the ACL:**
    - **Router(config)# access-list <ACCESS-LIST-NUMBER> <permit|deny> <TRANSPOT-LAYER-PROTOCOL> <host|source sourcewildcardmask|any> <host|destination destinationWildCardMask|any> eq <PORT-NUMBER>**
  - **Apply the ACL to an interface:**
    - **Router(config)# interface <INTERFACE-NUMBER>**
    - **Router(config-if)# ip access-group <ACCESS-LIST-NUMBER> <in|out>**

The Implied "Deny All Traffic" Criteria Statement

- **Overview:**
  - Every access list includes an implied rule at the end.
- **Key Point:**
  - "Deny All Traffic": If a packet does not match any of the criteria specified in the access list, it will be blocked.
- **Importance:**
  - This default behaviour ensures that all traffic not explicitly permitted by the access list is denied, enhancing network security.



Standard vs Extended ACLs

Standard Access Control List (ACL)

1- Permit S.IP = 192.168.10.10
2- Deny S.IP = 192.168.20.20
3- Deny S.Net = 192.168.10.10/24
4- Deny S.any (Hidden)

Extended Access Control List (ACL)

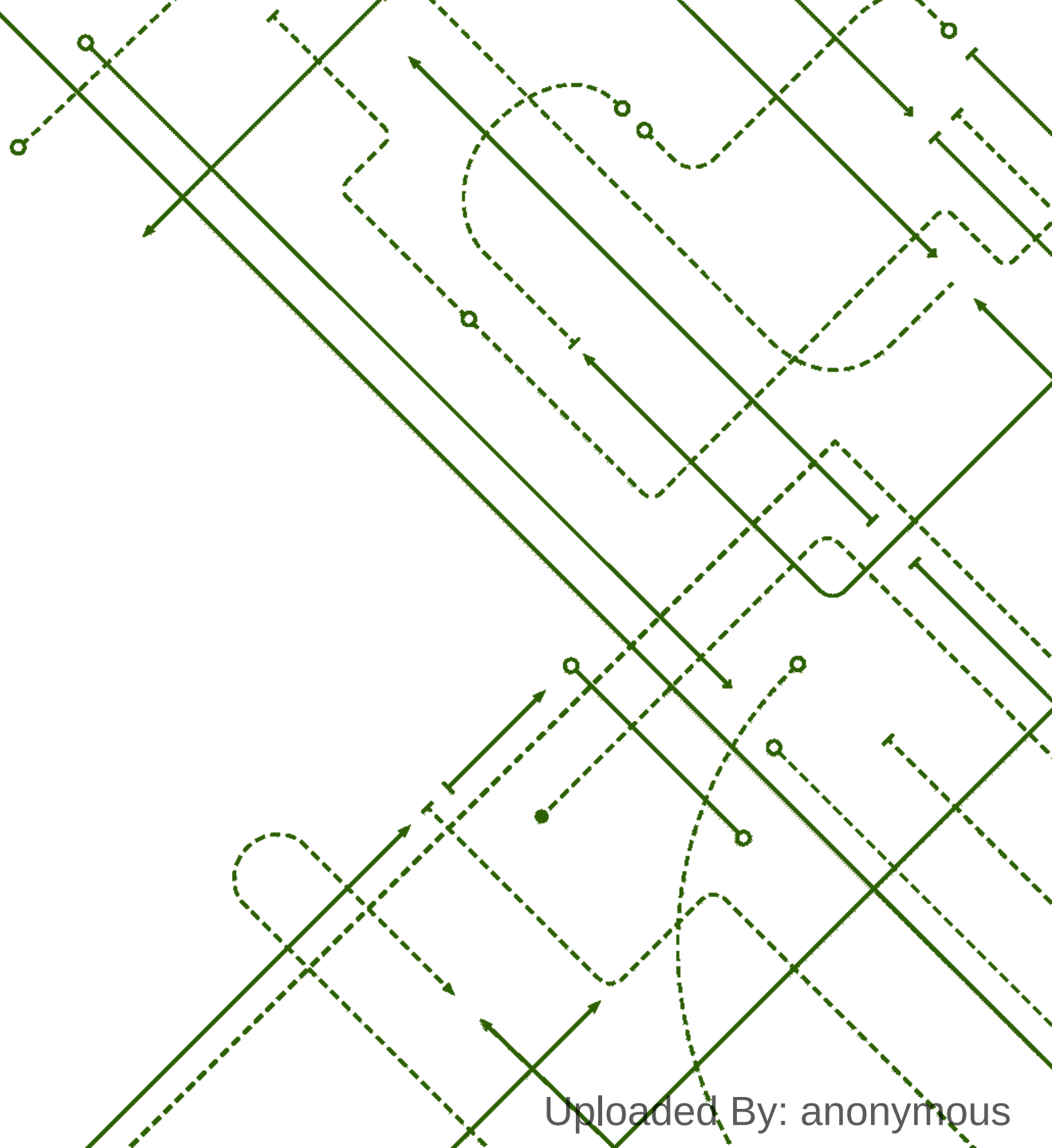
1- Permit S.IP = 192.168.10.10 D.Net = 192.168.5.0/24
2- Deny S.Net = 192.168.20.20/24 D.IP = 192.168.25.20
3- Deny S.Net = 192.168.10.10/24 D.any D.port 80
4- Deny S.any D.any (Hidden)

Wildcard Masks in ACLs

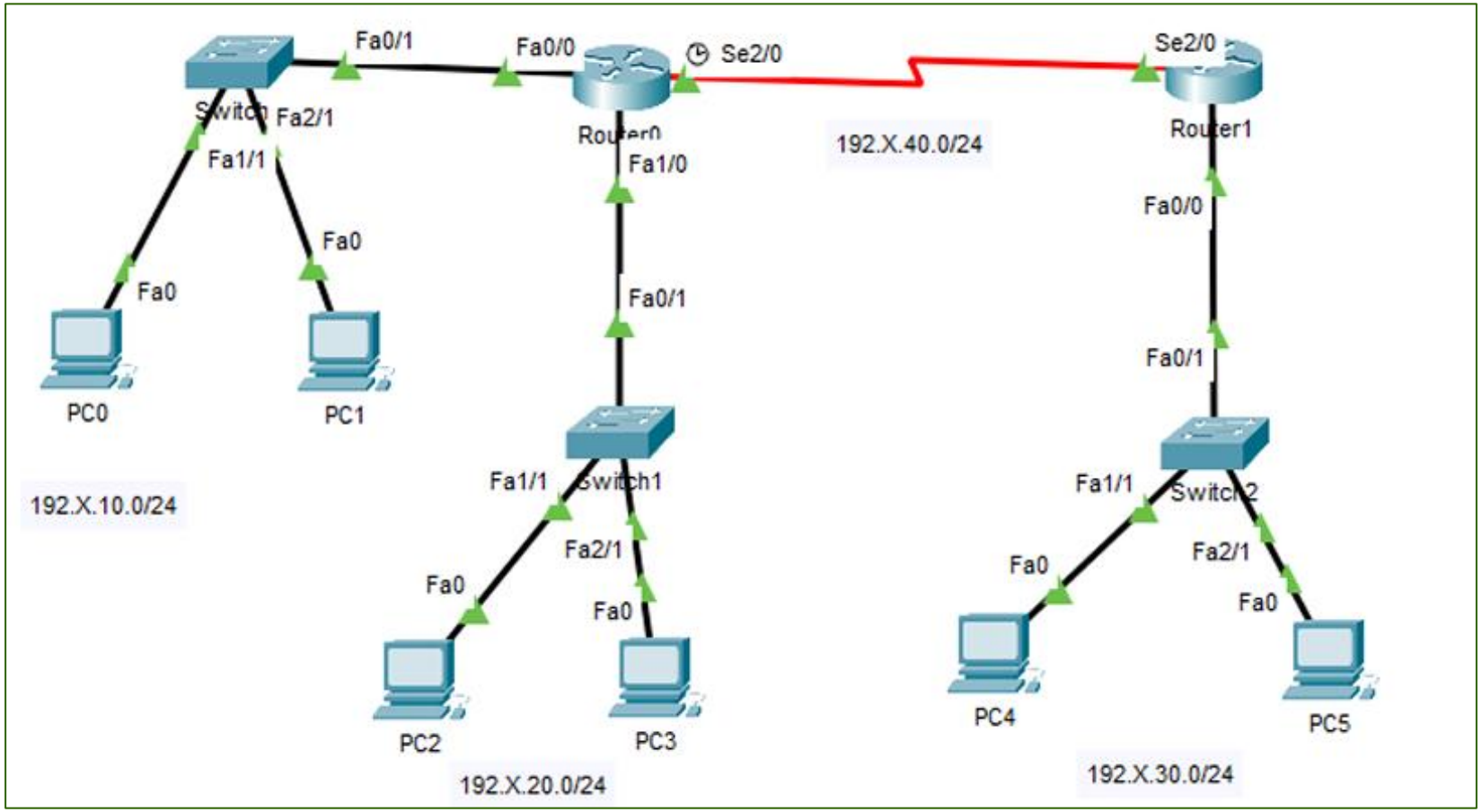
- **What is a Wildcard Mask?**
  - Used in ACLs to control which parts of an IP address to match or ignore.
  - Different from subnet masks: 0 = Match exactly, 1 = Ignore.

CIDR Notation	Subnet Mask	Wildcard Mask
/8	255.0.0.0	0.255.255.255
/16	255.255.0.0	0.0.255.255
/24	255.255.255.0	0.0.0.255
/25	255.255.255.128	0.0.0.127
/26	255.255.255.192	0.0.0.63
/27	255.255.255.224	0.0.0.31
/28	255.255.255.240	0.0.0.15
/29	255.255.255.248	0.0.0.7
/30	255.255.255.252	0.0.0.3
/32	255.255.255.255	0.0.0.0

Procedure



Topology



Networks IPS

Area	Network	Device	Interface	IP	Subnet Mask	Wildcard Mask
Area 0	192.X.40.0/24	Router 0	Se2/0	192.X.40.1	255.255.255.0	0.0.0.255
		Router 1	Se2/0	192.X.40.2	255.255.255.0	0.0.0.255
	192.X.10.0/24	Router 0	Fa0/0	192.X.10.1	255.255.255.0	0.0.0.255
		PC 0	Fa0	192.X.10.2	255.255.255.0	0.0.0.255
		PC 1	Fa0	192.X.10.3	255.255.255.0	0.0.0.255
	192.X.20.0/24	Router 0	Fa1/0	192.X.20.1	255.255.255.0	0.0.0.255
		PC 2	Fa0	192.X.20.2	255.255.255.0	0.0.0.255
		PC 3	Fa0	192.X.20.3	255.255.255.0	0.0.0.255
	192.X.30.0/24	Router 1	Fa0/0	192.X.30.1	255.255.255.0	0.0.0.255
		PC 4	Fa0	192.X.30.2	255.255.255.0	0.0.0.255
		PC 4	Fa0	192.X.30.2	255.255.255.0	0.0.0.255

Steps of Configurations

1. **Assign the IPs:** To Routers & PCs.

2. **Connectivity Check:** Ensure each PC can reach the Gateway and adjacent routers can communicate.

3. **Configuring OSPF Routing:** Make Sure that all PCs can ping each other
   - **Router(config)# router ospf <PROCESS-ID>**
   - **Router(config-router)# network <ID-ADDRESS> <WILDCARD-MASK> area <AREA-ID>**

4. **Create couple of copies from the .pkt file**

Steps of Configurations

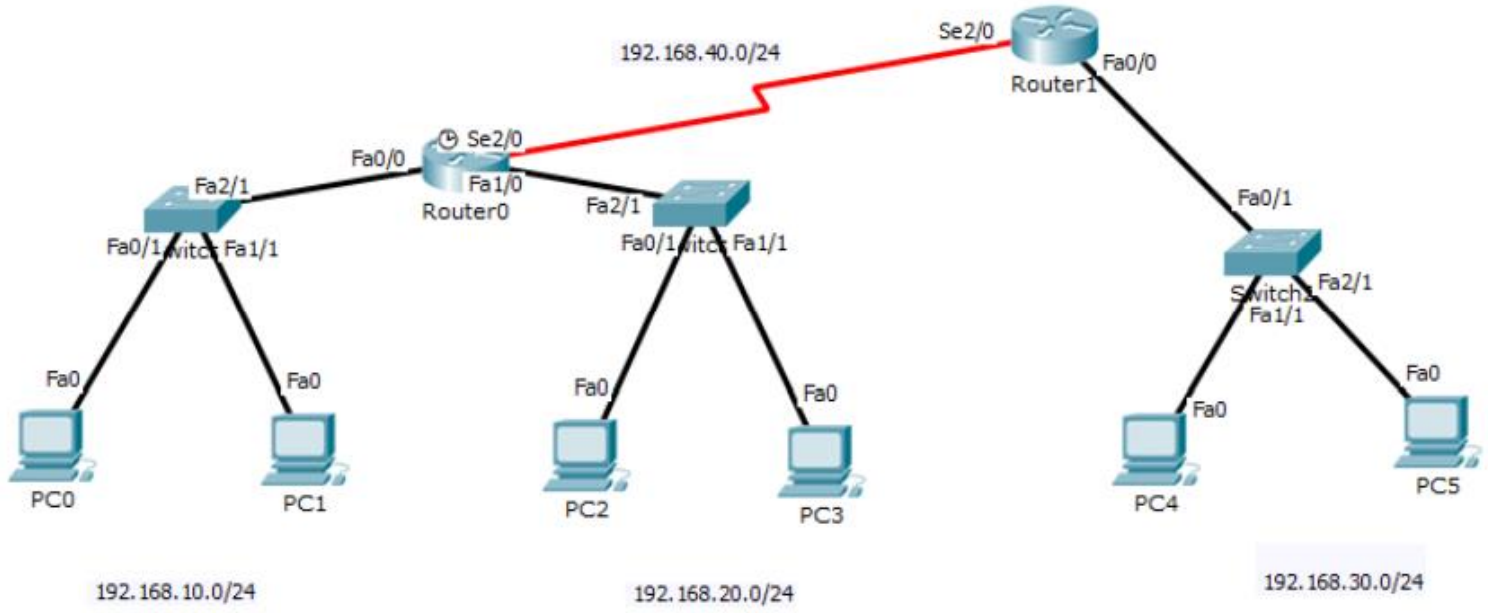
5. **Configuring Standard Access Lists**

6. **Configuring Extended Access Lists**

7. **Viewing Access Lists**
   - **Router# show access-list**

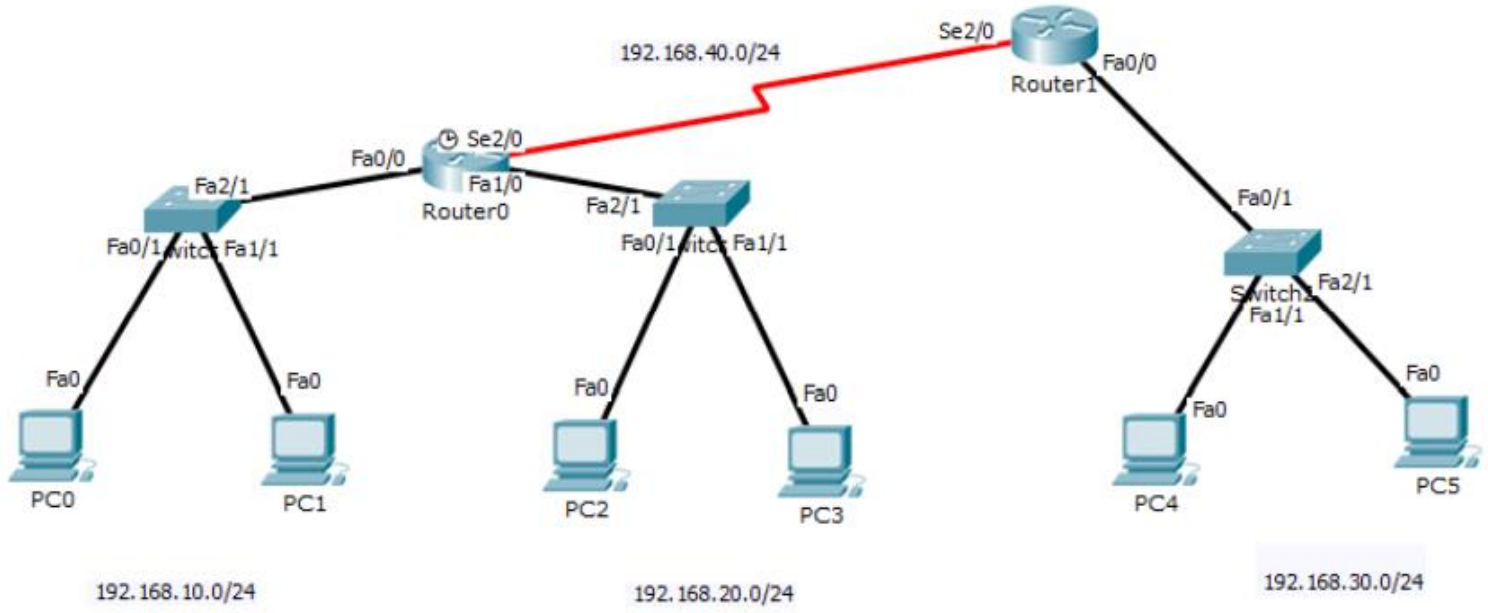
Standard Access Control List Example

- **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)?

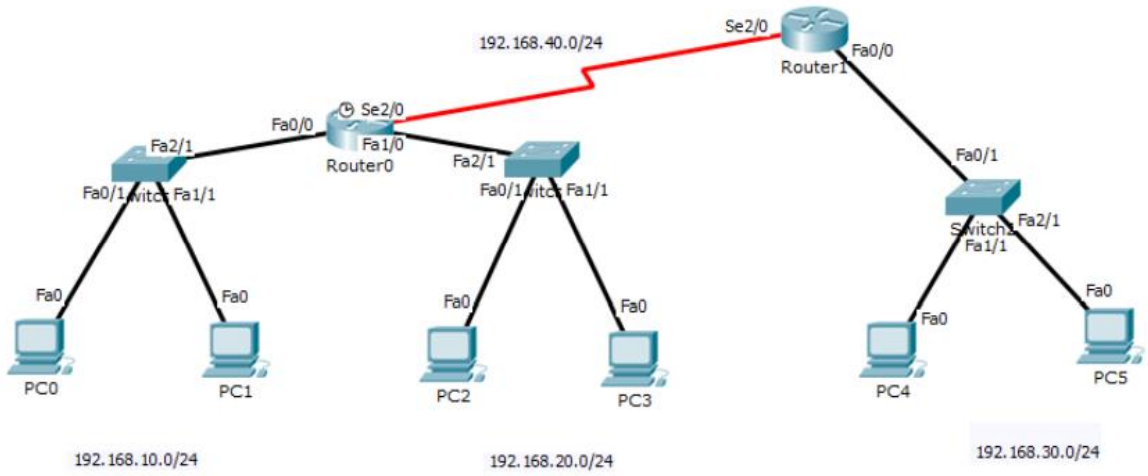


Standard Access Control List Example (Cont.)

- **Prevent PC0 to access network 192.x.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**

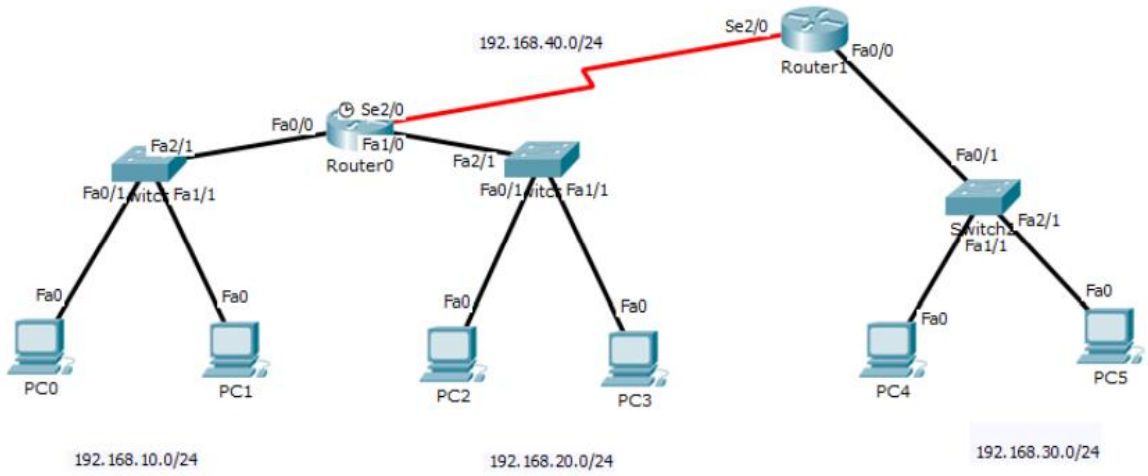


Standard Access Control List Example (Cont.)



- **Router0(config)#**
- **Router0(config)#**
- **Router0(config)#**
- **Router0(config-if)#**

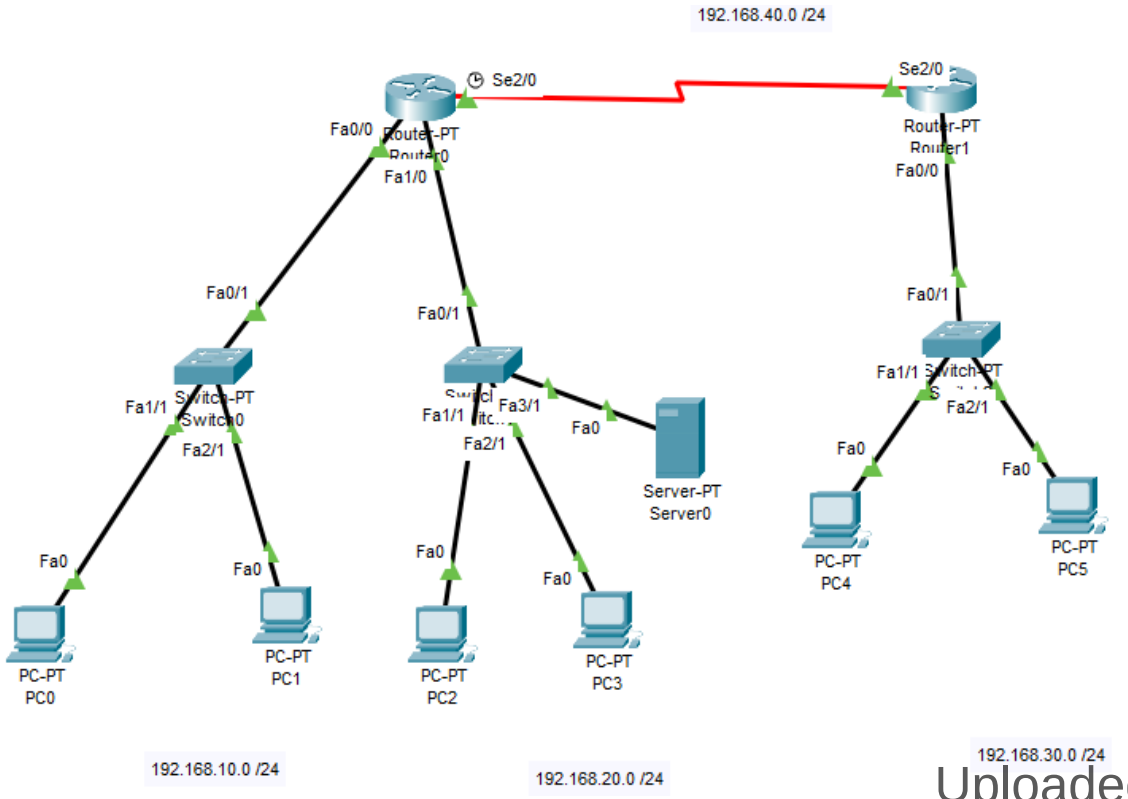
Standard Access Control List Example (Cont.)



- **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**

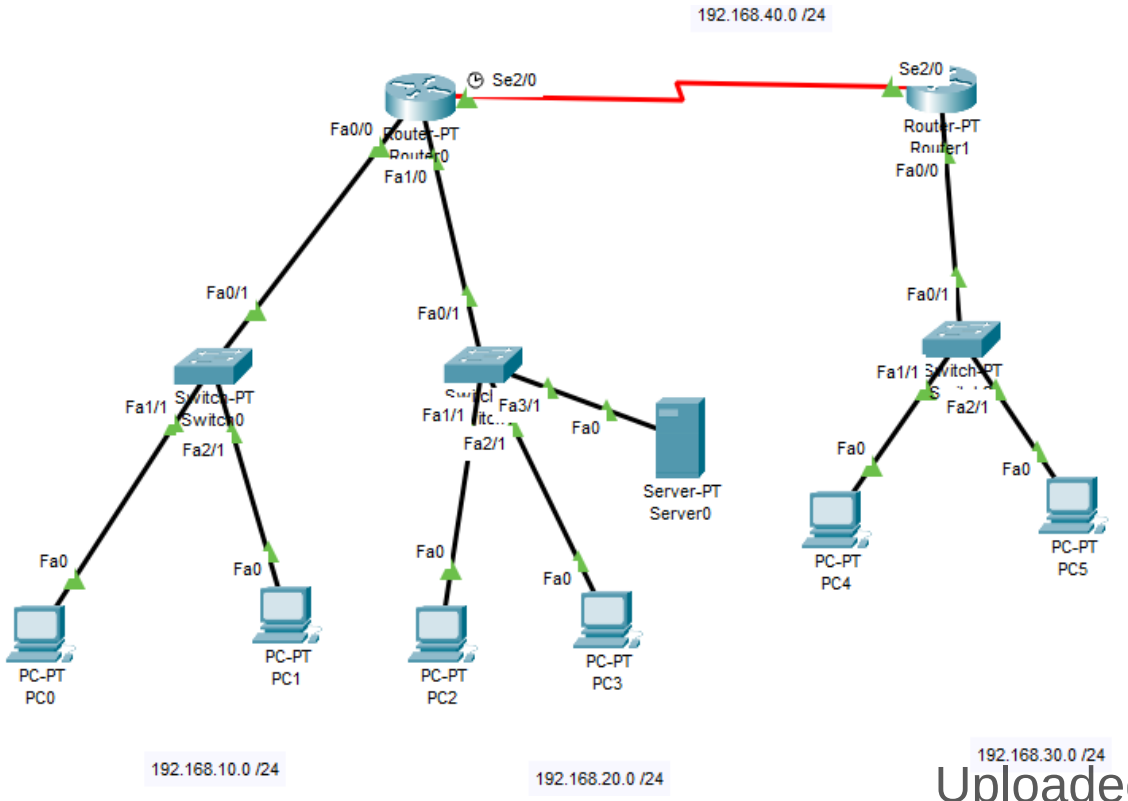
Extended Access Control List Example

- **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) ?



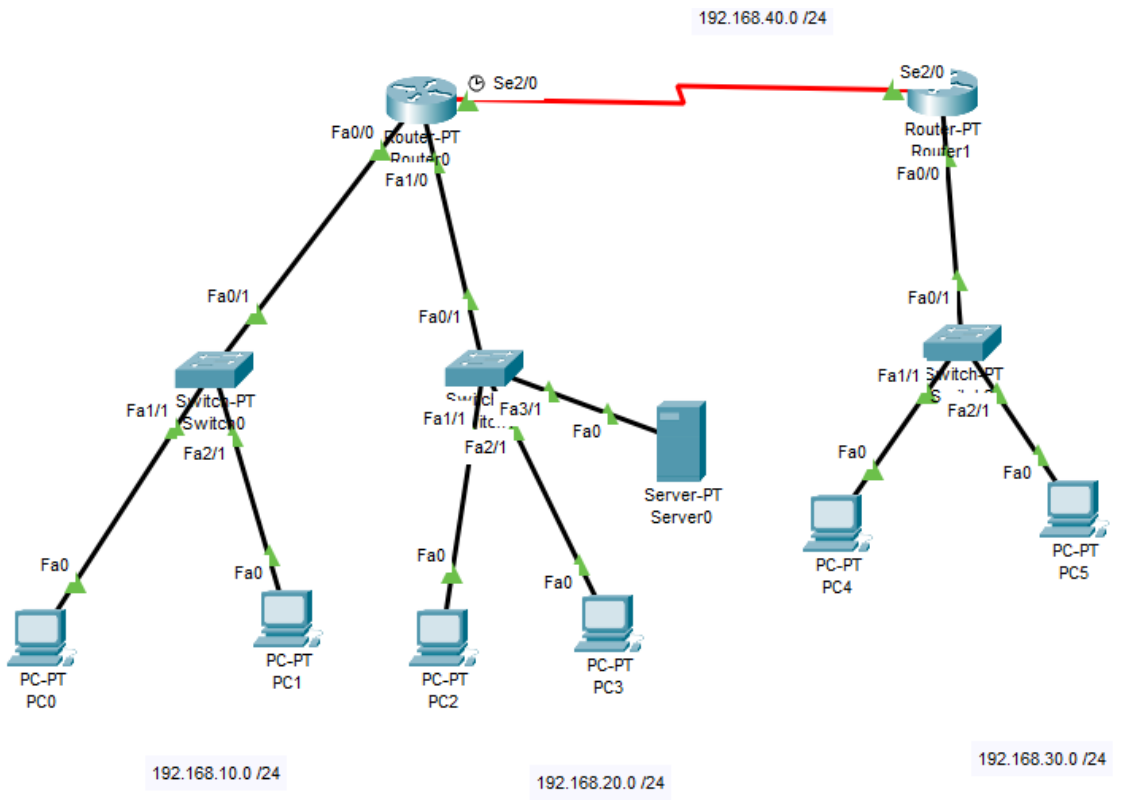
Extended Access Control List Example (Cont.)

- **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**



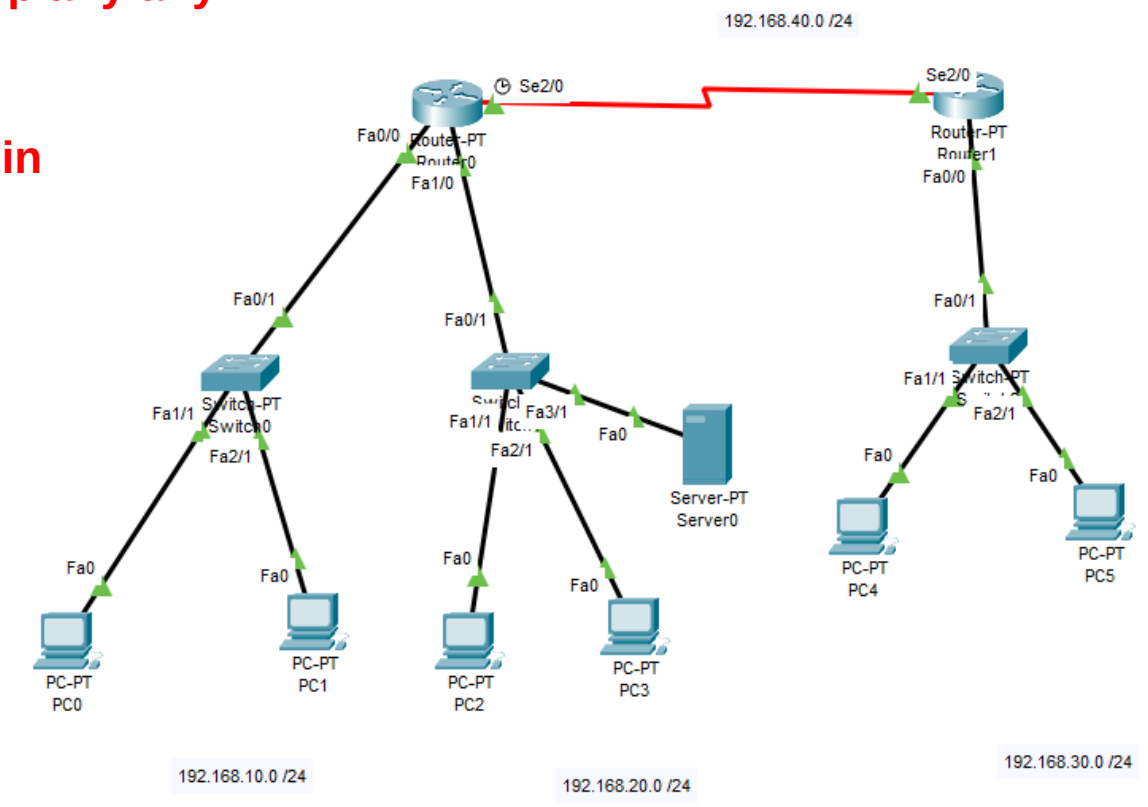
Extended Access Control List Example (Cont.)

- **Router0(config)#**
- **Router0(config)#**
- **Router0(config)#**
- **Router0(config-if)#**



Extended Access Control List Example (Cont.)

- **Router0(config)# access-list 101 deny tcp host 192.168.30.2 host 192.168.20.4 eq 80**
- **Router0(config)# access-list 101 permit ip any any**
- **Router0(config)# interface fa0/0**
- **Router0(config-if)# ip access-group 101 in**



Saving Configurations

- **Don't forget to save the configurations on your router.**

  → **Router# write**
  → **Router# copy run start**

Video explaining the experiment

--Soon--

References

- **Manual for ENCS4130 Computer Networks Laboratory.**