ACCESS CONTROL LISTS

OUTLINE

- Introduction
- Wildcard Masks
- Types of ACLs
- Numbered ACL
- Named ACL
- Applying ACLs to Interfaces
- Where should one apply ACLs?

INTRODUCTION

- An access control list (ACL) is a list of rules that specifies which users or systems are granted or denied access to a particular device or system resource.
- Access control lists can be configured in routers or switches.
- Access control lists act as filters, managing which traffic can access the network.

WILDCARD MASKS

- Wildcard bit 0 means match the bit on IP address
- Wildcard bit 1 means do not match the bit on IP address
- For example 0.0.0.0 255.255.255.255 means any address
- 192.168.1.0 0.0.0.255 means any address in a network 192.168.1.0 (Match the first three octets and don't match the last octet) – *for this case means an entire class C network.*
- 192.168.1.15 0.0.0.0 means the exact host 192.168.1.15

TYPES OF ACCESS CONTROL LISTS

- Standard Access Control Lists
  - Check source address
  - Generaly permit or deny entire protocol suite
- Extended Access Control Lists
  - Check both source and destination addresses
  - Generally permits or denies specific protocols and applications

METHODS FOR IDENTIFYING ACL

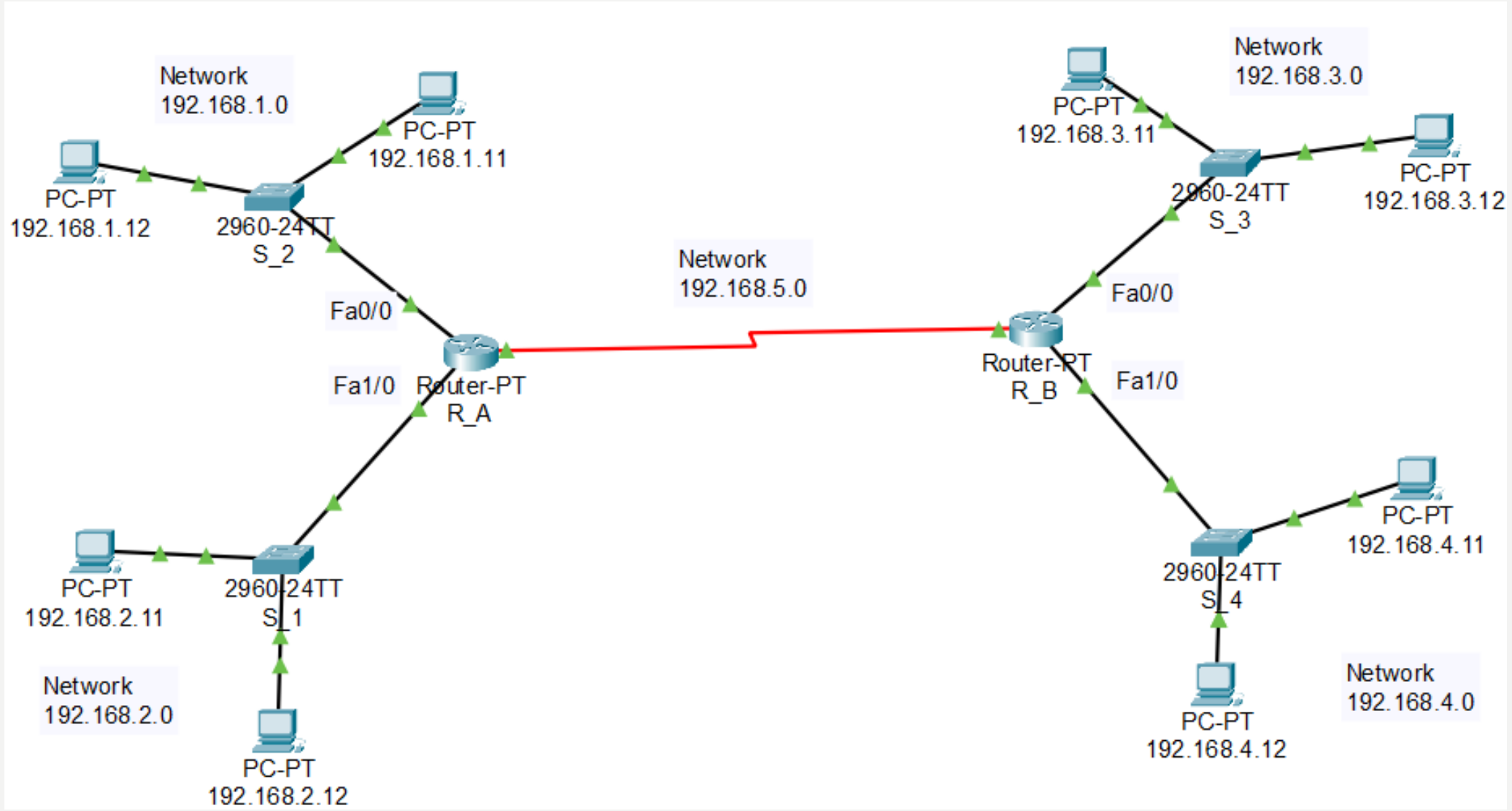
- Number identification
- Descriptive names identification

NUMBERED ACCESS CONTROL LISTS

- 1 – 99 used for standard ACLs (1300 – 1999 expanded range)
- 100 – 199 used for extended ACLs (2000 – 2699 expanded range)
- Create a numbered access control list by using command:

```
access-list 50 deny 192.168.1.5 0.0.0.0
access-list 150 deny ip 192.168.1.5 0.0.0.0 192.168.2.5 0.0.0.0
```

SAMPLE NETWORK DESIGN (2 COPIES)



PRACTICAL TASK 1 (FIRST COPY)

Based on given network design

- Create numbered standard access list preventing host 192.168.3.11 from accessing network 192.168.1.0
- Create numbered standard access list preventing network 192.168.4.0 from accessing network 192.168.1.0
- Create numbered extended access list preventing host 192.168.3.12 from accessing network 192.168.2.0
- Create numbered extended access list preventing network 192.168.4.0 from accessing network 192.168.1.0

PRACTICAL TASK 2 (SECOND COPY)

Based on given network design

- Create named standard access list preventing host 192.168.3.11 from accessing network 192.168.1.0
- Create named standard access list preventing network 192.168.4.0 from accessing network 192.168.1.0
- Create named extended access list preventing host 192.168.3.12 from accessing network 192.168.2.0
- Create named extended access list preventing network 192.168.4.0 from accessing network 192.168.1.0

NAMED ACCESS CONTROL LISTS

- Ip access-list standard ANameOfACL
- [sequence-number] {permit | deny} {ip access list test conditions}
- {permit | deny} {ip access list test conditions}
- For example

    ip access-list standard ICT
    10 permit 192.168.1.5 0.0.0.0
    20 deny 92.168.1.0 0.0.0.255
    30 permit any

APPLYING ACL TO INTERFACES

- ACL will perform its operations once applied to an interface.
- Use commands similar to the following in order to apply an ACL:

```
interface Fa0/0
ip access-group ICT out
exit
```

Alternatively

```
interface Se2/0
ip access-group ICT in
exit
```

WHERE TO APPLY ACL?

- Any router's interface in the complete path from source to destination an ACL can be applied.
- For an effective working of ACLs it is appropriate to:
  - Apply standard ACL to the interface that is very close to destination.
  - Apply extended ACL to the interface that is very close to the source.

ACL CONFIGURATION GUIDELINES

- Standard or extended indicates what can be filtered.
- Only one ACL per interface, per protocol, and per direction is allowed.
- The order of ACL statements controls testing, therefore, the most specific statements go at the top of the list.
- The last ACL test is always an implicit deny everything else statement, so every list needs at least one permit statement.

ACL CONFIGURATION GUIDELINES…

- ACLs are created globally and then applied to interfaces for inbound or outbound traffic.
- An ACL can filter traffic going through the router, or traffic to and from the router, depending on how it is applied.
- When placing ACLs in the network
  - Place extended ACLs close to the source
  - Place standard ACLs close to the destination