|  |  |
| --- | --- |
| **Practicum Case** |  |
| CPEN6247 | CPEN6247001  Computer Networks |
| **Computer Engineering** | **O221-CPEN6247-PH01-05** |
| ***Valid on*** *Odd Semester Year 2021/2022* | **Revision 00** |

## Learning Outcomes

* LO2 – concepts of create network environment

## Topic

* Session 5 – Access List

## Sub Topics

* Standard Access List
* Extended Access List
* Review

## Soal

*Case*

1. **Access List**

An access list is a rule for controlling the network traffic. These rules can be in a form of allowing or denying packets to a certain destination. This process will happen in the interface of a router. An access list is the same as a stateless firewall where it only allows or restricts a packet from going through from the source to the destination.

The reason we use an access list is to provide security to our network. Without an access list, any packet can be sent anywhere by anyone. Therefore, making it a lot more vulnerable to unwanted or dangerous traffic.

By the capability of the access list, access list can be divided into two types,

* **Standard Access List**

A standard access list is an access list that can only filter packets based on the source address. A standard access list cannot filter packets based on the destination or protocol used. For example, we have an access list that denies any packet from 192.168.0.10. Then any packet sent from 192.168.0.10 will be denied, but if another address sent a packet to 192.168.0.10 then that packet can still be received.

* **Extended Access List**

An extended access list is an access list that can filter not only from the source but also the destination. For example, we have an access list that denied packets where the source is 192.168.0.10 and the destination is 192.168.0.11. Any packet sent from 192.168.0.10 to 192.168.0.11 will not go through but if 192.168.0.10 send a packet to another address for example 192.168.0.12 it will still be sent.

To differentiate between the two access lists, we will be using numbers. To specify a standard access list, we will be using the numbers 1-99. Meanwhile, to specify an extended access list, we will be using the number 100-199.

There are two ways we can put an access list in an interface of a router, Inbound and Outbound. Inbound is when we want the access list to filter packets when the packet is entering the interface. Meanwhile, outbound is when the packet is exiting the interface.

1. **Standard Access List**

To demonstrate a standard access list, we will have the following case.

Diagram

Description automatically generated

First, we need to set the IP address for each device in our topology.

**PC:**

* **PC 1** = 192.168.100.2/24
* **PC 2** = 192.168.100.3/24
* **PC 3** = 192.168.101.2/24
* **PC 4** = 192.168.101.3/24

**Router:**

* **Fa0/0** = 192.168.100.1
* **Fa1/0** = 192.168.101.2

After we are done setting IP for each device, we can proceed to make a new access list. For example, we want to block all packets coming from PC 2. Therefore, we can do the following steps:

* 1. First, we will be **making a new access list**. The command that will be used is:

***access-list [number] [type] [ip address]***

|  |  |
| --- | --- |
| Parameter | Description |
| number | The number of our access list, in this case, we will be using an extended access list so the number that will be used is 100-199 |
| type | type of access list that we want to make |
| IP address | The source IP address that we want to permit or deny |

Therefore, we can type the following command:

access-list 5 deny 192.168.100.3

access-list 5 permit any

The command above will first deny any packet coming from 192.168.100.3. Then, the next line will permit any address because the default is to deny any, meaning every packet from all sources will be blocked.

* 1. After the access list has been made, you can use the command **show access-lists** to check the access list that has been made.



* 1. Then, we need to **set our access list on the interface** that we want. For example, we will put this access list in the interface fa0/0. To do so, we will go to the corresponding interface and type in the command:

***ip access-group [access-list number] [type]***

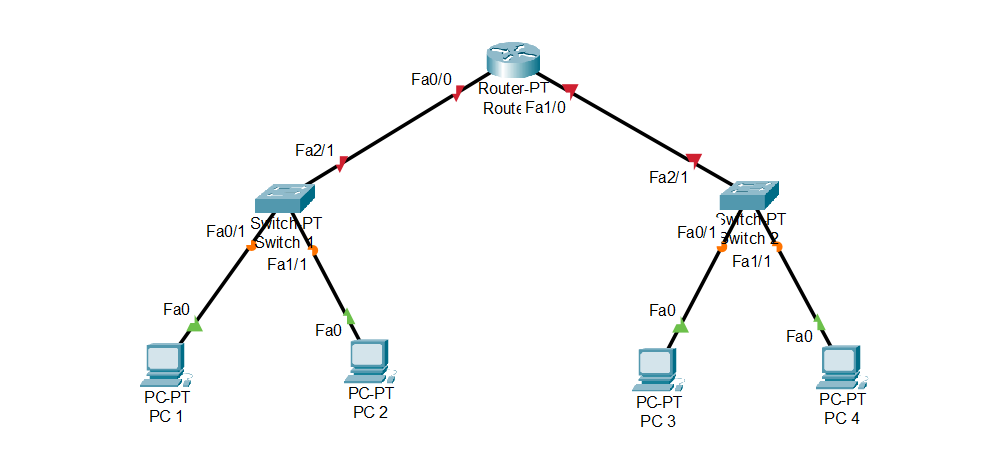
The access-list number will be the number that we previously used when we made our access list and the type will be whether we want to set it as **inbound** or **outbound**.

ip access-group 5 in

* 1. Now, when we try to send a packet from PC 2 to PC 3, the packet should fail. But, if we try to send from PC 1 to PC 3, the packet should be successfully sent.

1. **Extended Access List**

To demonstrate an extended access list, we will be using the previous case.



We will also be using the same IP address from the standard access list. For example, we want to block packets coming from PC-1 to PC-4. To do so, we can do the following steps,

* 1. First, we will be **making a new access list**. The command that will be used is

***access-list [number] [type] [protocol] [source] [destination]***

|  |  |
| --- | --- |
| Parameter | Description |
| number | The number of our access list, in this case, we will be using an extended access list so the number that will be used is 100-199 |
| type | type of access list that we want to make |
| protocol | type of protocol that we want to permit or deny |
| source | The source IP address that we want to permit or deny |
| destination | The destination IP address that we want to permit or deny |

Therefore, we can type the following command

access-list 105 deny ip host 192.168.100.2 host 192.168.101.3

access-list 105 permit ip any any

The command above will create an access list that will deny the packet from 192.168.100.2 to 192.168.101.3. Then, the second command will permit packet from any IP to any IP

* 1. Same as before, we can check the access list that we have made by typing in the command **show access-lists**.



* 1. Then, we need to **set the access list to the interface** that we want. For example, we will put this access list in the interface fa0/0 of Router 1. We will use the previous command to do so,

ip access-group 105 in

* 1. Now, if we try to send a packet from PC-1 to PC-4 the packet should fail. But, if we send it to a different PC for example PC-3, the packet should be successfully sent.

1. **Case**

After building a two-floor office and implementing static routing for that building, Quantum & Clock realized because all devices can communicate with each other. Therefore, the security of each division is significantly lower. So, you as a network engineer are asked to implement an access list inside the two-floor office. Below are the network topology asked by Quantum & Clock.

