Access Control List (ACL)

Theory

Defining who can/can’t access what is basically the gist of ACL. In our day-to-day lives, we apply the ACL concept in many areas. A simple example could be that you need to show your ID card to enter an office. There is a list of employees, and your ID is checked against that list to grant access. Similar access controls are in effect virtually everywhere, especially in places where security is critical. In the digital world, this access control is needed so that only the allowed ones can access a certain digital resource. For example, only admins would be allowed access to the backend of a web server, or only database admins would be allowed to access a database server, etc.

In networked devices, ACLs allow only authorized persons/devices to access a certain resource. For example, you can define that only a certain host device can access your webserver. You can also define ACLs so that hosts belonging to a particular network cannot communicate with hosts of certain other networks. More scenarios can be defined depending on the needs of an administrator.

In this part, we will learn about Cisco IP ACL, i.e., filtering network traffic based on IP address. Several ACL types can be configured on a Cisco device. However, we will only focus on Numbered Standard IPv4 ACL. There are two steps to implement an ACL. First, define the rule. Second, apply the rule to an interface.

The command format for defining a numbered standard IP ACL is:

```
Router(config)# access-list access_list_number {permit|deny}
{(source_address source_wildcard)|any}
```

You can either permit or deny a packet based on the source IP of the packet in numbered standard IP ACL. Like the OSPF configuration, you must specify a wildcard mask to permit/deny a range of source IP addresses based on the given pattern. You should remember that whenever you apply an ACL to an interface, all the traffic that does not match any ACL rule will be discarded by default. For example, you have defined an ACL to deny a certain source IP. Whenever you apply that rule to an interface, all packets other than the denied source will also be discarded because there is no matching rule for those packets. So, you must allow other traffic explicitly by defining another ACL. The any keyword is handy in this case. To permit (or deny) any packet other than the previously specified rules, you can add the keyword any in place of the source_address and source_wildcard like the following:

```
Router(config)# access-list 1 permit any
```

Another thing is you can only use numbers from 1 to 99 to specify the access list number. Other numbers are used for extended numbered ACLs. After defining the ACL rule, we must apply it to an interface. Remember that the ACL has no effect until you apply it. The command format for applying an ACL to an interface is:

```
Router(config-if)# ip access-group access_list_number {in|out}
```

The ACL is applied either for inbound or outbound traffic of an interface, and you need to specify the corresponding keyword, i.e., in or out for that. One best practice before applying an ACL to an interface is to verify the rule by using the following command:

```
Router# show access-lists
```