CNT Assignment 3 Theory

Aim: Using a Network Simulator (e.g. packet tracer) Configure A router using router commands, Access Control lists – Standard & Extended.

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.

Access-list (ACL) is a set of rules defined for controlling the network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

ACL features –

1. The set of rules defined are matched serial wise i.e matching starts with the first line, then 2nd, then 3rd and so on.

2. The packets are matched only until it matches the rule. Once a rule is matched then no further comparison takes place and that rule will be performed.

3. There is an implicit deny at the end of every ACL, i.e., if no condition or rule matches then the packet will be discarded.

4. Once the access-list is built, then it should be applied to inbound or outbound of the interface:

   - **Inbound access lists –** When an access list is applied on inbound packets of the interface then first the packets will be processed according to the access list and then routed to the outbound interface.
   - **Outbound access lists –** When an access list is applied on outbound packets of the interface then first the packet will be routed and then processed at the outbound interface.

Types of ACL –

There are two main different types of Access-list namely:

1. **Standard Access-list –** These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, Https etc. By using numbers 1-99 or 1300-1999, router will understand it as a standard ACL and the specified address as source IP address.
2. **Extended Access-list –** These are the ACL which uses both source and destination IP address. In these type of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

Also there are two categories of access-list:

1. **Numbered access-list –** These are the access list which cannot be deleted specifically once created i.e if we want to remove any rule from an Access-list then this is not permitted in the case of the numbered access list. If we try to delete a rule from the access list then the whole access list will be deleted. The numbered access-list can be used with both standard and extended access lists.
2. **Named access list –** In this type of access list, a name is assigned to identify an access list. It is allowed to delete a named access-list, unlike a numbered access list. Like a numbered access-list, these can be used with both standard and extended access lists.

Rules for ACL –

1. The standard Access-list is generally applied close to the destination (but not always).
2. The extended Access-list is generally applied close to the source (but not always).
3. We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
4. We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule then whole ACL will be removed. If we are using named access lists then we can delete a specific rule.
5. Every new rule which is added into the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
6. As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.
7. Standard access lists and extended access lists cannot have the same name.

Advantages of ACL –

- Improve network performance.
- Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of network.

Standard Access-List

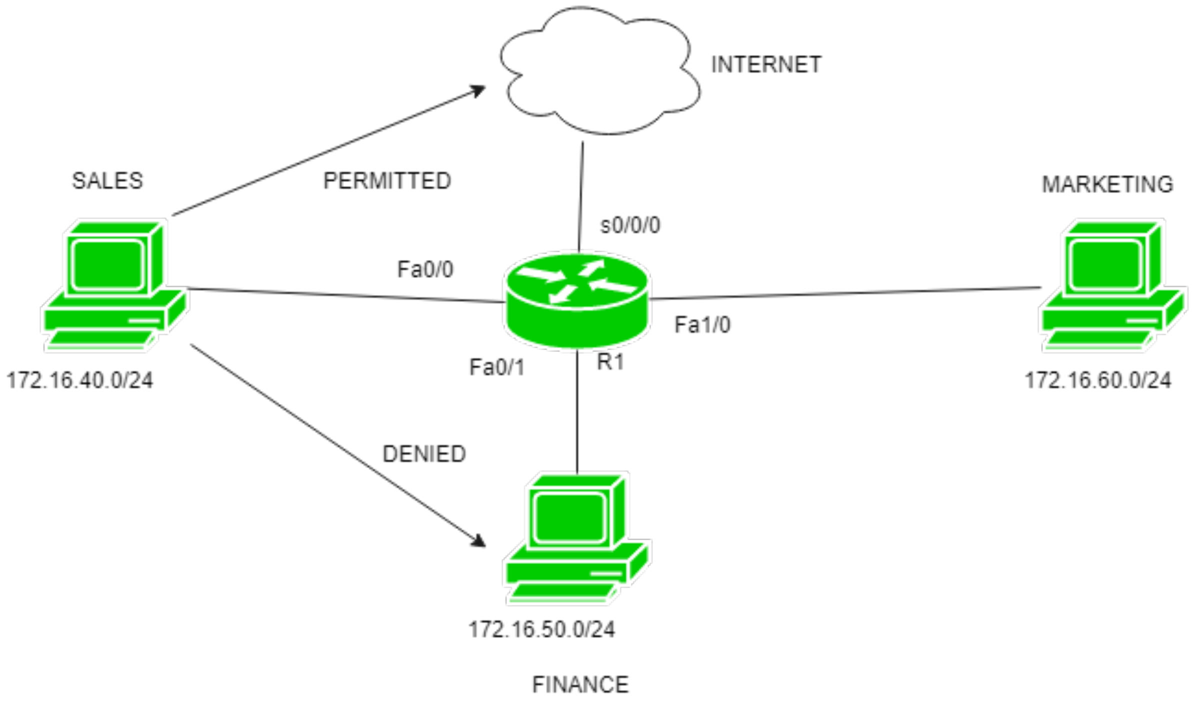
These are the Access-list which are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don’t distinguish between the IP traffic such as TCP, UDP, Https etc. By using numbers 1-99 or 1300-1999, router will understand it as a standard ACL and the specified address as source IP address.

Features –

1. Standard Access-list is generally applied close to destination (but not always).
2. In standard access-list, whole network or sub-network is denied.
3. Standard access-list uses the range 1-99 and extended range 1300-1999.
4. Standard access-list is implemented using source IP address only.
5. If numbered with standard Access-list is used then remember rules can’t be deleted. If one of the rule is deleted then the whole access-list will be deleted.
6. If named with standard Access-list is used then you have the flexibility to delete a rule from access-list.

Standard Access-lists are less used as compared to extended access-list as the entire IP protocol suite will be allowed or denied for the traffic as it can’t distinguish between the different IP protocol traffic.

Configuration:



Here is a small topology in which there are 3 departments namely sales, finance and marketing. Sales department having network 172.16.40.0/24, Finance department having network 172.16.50.0/24 and marketing department having network 172.16.60.0/24. Now, want to deny connection from sales department to finance department and allow others to reach that network.

Now, first configuring numbered standard access – list for denying any IP connection from sales to finance department.

```
R1# config terminal
R1(config)# access-list 10 deny 172.16.40.0 0.0.0.255
```

Here, like extended access-list, you cannot specify the particular IP traffic to be permitted or denied. Also, note that wildcard mask has been used (0.0.0.255 which means Subnet mask 255.255.255.0). 10 is used from the number standard access-list range.

```
R1(config)# access-list 110 permit ip any any
```

Now, as you already know there is an implicit deny at the end of every access-list which means that if the traffic doesn't match any of the rule of access-list then the traffic will be dropped.

By specifying any means that source having any ip address traffic will reach finance department except the traffic which it matches the above rules that you have made.

Now, you have to apply the access-list on the interface of the router:

```
R1(config)# int fa0/1
R1(config-if)# ip access-group 10 out
```

As you remember that the standard access-list is generally applied to the destination and here also if you apply access-list close to destination, it will satisfy our need, therefore, outbound to interface fa0/1 has been applied.

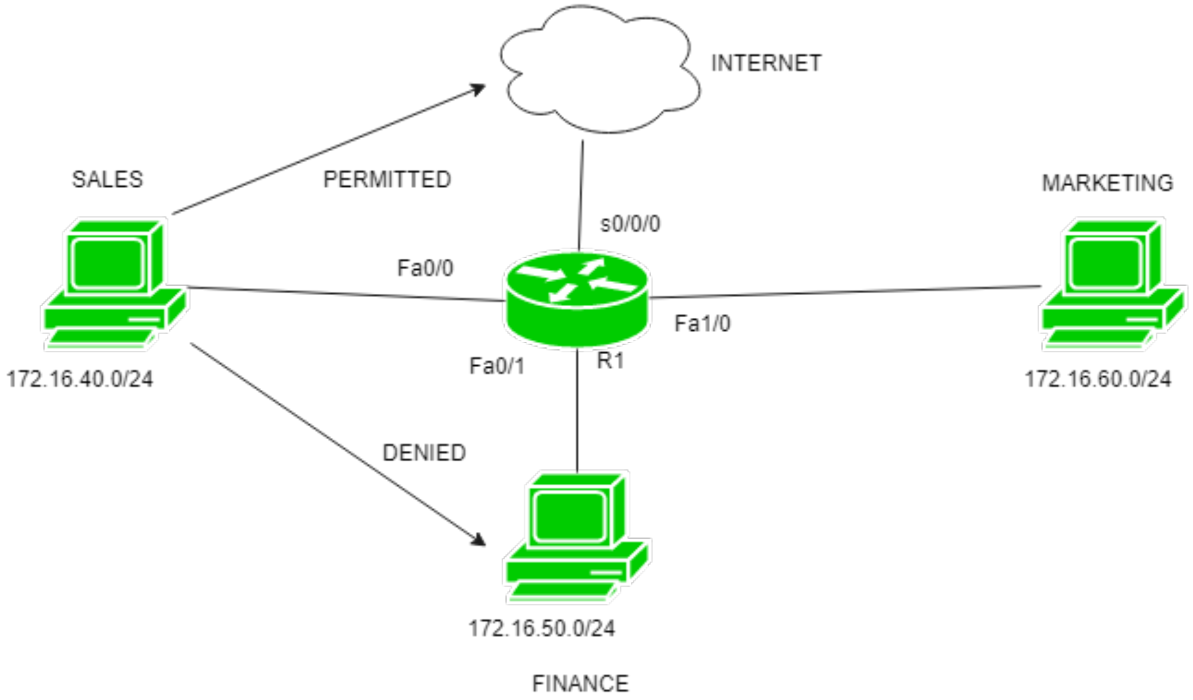
Named standard Access-list example –

Now, considering the same topology, you will make a named standard access-list.

```
R1(config)# ip access-list standard  blockacl
```

By using this command you have made an access-list named blockacl.

```
R1(config-std-nacl)# deny 172.16.40.0 0.0.0.255
```



```
R1(config-std-nacl)# permit  any
```

And then the same configuration you have done in numbered access-list.

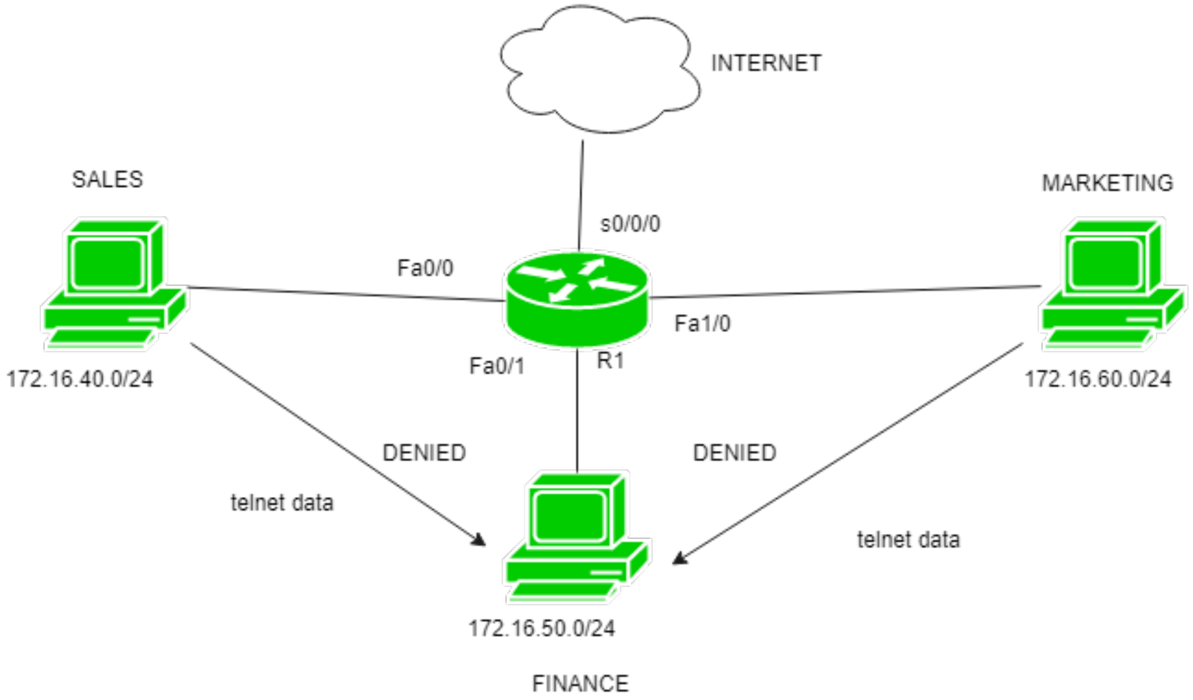
```
R1(config)# int fa0/1
R1(config-if)# ip access-group blockacl out
```

Standard access-list for Telnet example –

As you know, you cannot specify a particular IP traffic to be denied in standard access-list but telnet connection can be permitted or denied using standard access-list by applying access list on line vty lines.

Here, in the given figure, you want to deny telnet to Finance department from any network. Configuring for the same:

```
R1(config)# access-list 10 deny any
```



```
R1(config)# line vty 0 4

R1(config-line)# access-class 10 out
```

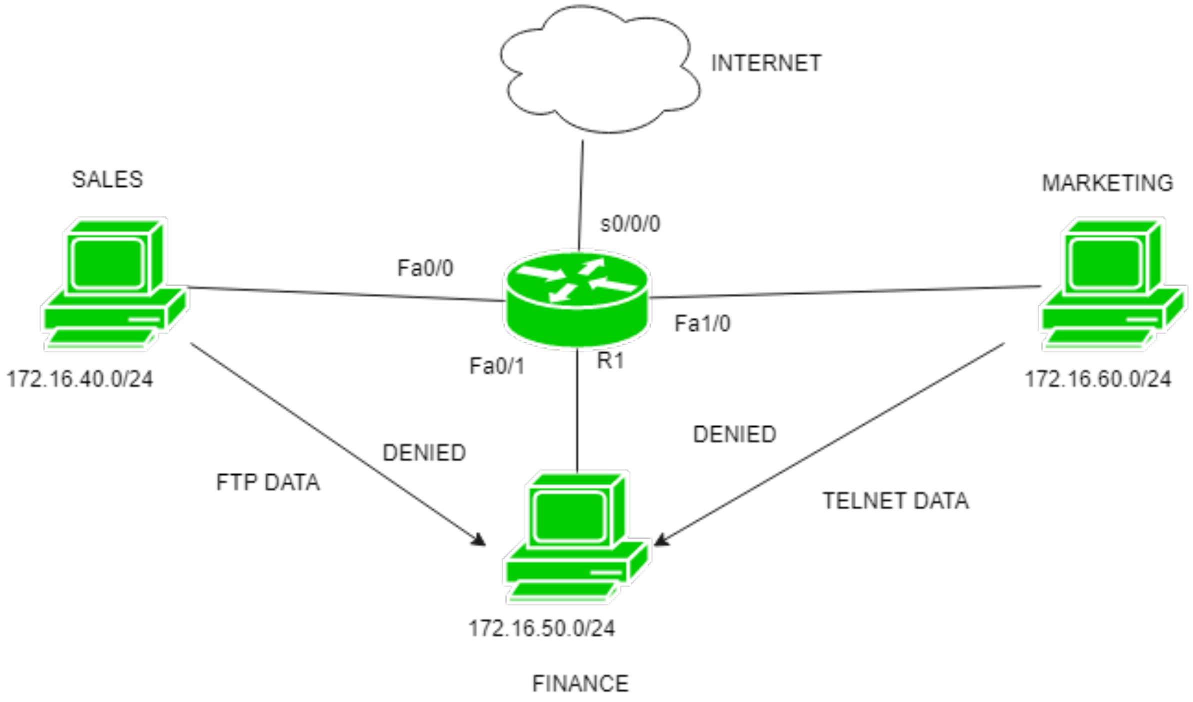
Extended Access-list –

It is one of the types of Access-list which is mostly used as it can distinguish IP traffic therefore the whole traffic will not be permitted or denied like in standard access-list . These are the ACL which uses both source and destination IP address and also the port numbers to distinguish IP traffic. In these type of ACL, we can also mention which IP traffic should be allowed or denied . These use range 100-199 and 2000-2699.

Features:

1. Extended access-list is generally applied close to the source but not always.
2. In Extended access-list, packet filtering takes place on the basis of source IP address, destination IP address, Port numbers.
3. In extended access-list, particular services will be permitted or denied .
4. Extended ACL is created from 100 – 199 & extended range 2000 – 2699.
5. If numbered with extended Access-list is used then remember rules can't be deleted. If one of the rule is deleted then the whole access-list will be deleted.
6. If named with extended Access-list is used then we have the flexibility to delete a rule from access-list.

Configuration –



Here is a small topology in which there are 3 departments namely sales, finance and marketing. Sales department having network 172.16.10.40/24, Finance department having network 172.16.50.0/24 and marketing department having network 172.16.60.0/24. Now, we want to deny FTP connection from sales department to finance department and deny telnet to Finance department from both sales and marketing department.

Now, first configuring numbered extended access – list for denying FTP connection from sales to finance department.

```
R1# config terminal

R1(config)# access-list 110 deny tcp 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255 eq 21
```

Here, we first create an numbered Access-list in which we use 110 (used from extended access-list range) and denying the sales network (172.16.40.0) to make FTP connection to finance network (172.16.50.0).

Here, as FTP uses TCP and port number 21. Therefore, we have to specify the permit or deny condition according to the need. Also, after eq we have use the port number for specified application layer protocol.

Now, we have to deny telnet connection to finance department from both sales and Marketing department which means no one should telnet to finance department. Configuring for the same.

```
R1(config)# access-list 110 deny tcp any 172.16.50.0 0.0.0.255 eq 23
```

Here, we have used the keyword any which means 0.0.0.0 0.0.0.0 i.e any ip address from any subnet mask. As telnet uses port number 23 therefore, we have to specify the port number 23 after eq .

```
R1(config)# access-list 110 permit ip any any
```

Now, this is the most important part. As we already know there is an implicit deny at the end of every access-list which means that if the traffic doesn't match any of the rule of Access-list then the traffic will be dropped.

By specifying **any, any** means that source having any ip address traffic will reach finance department except the traffic which it matches the above rules that we have made. Now, we have to apply the access-list on the interface of the router:

```
R1(config)# int fa0/1

R1(config-if)# ip access-group 110 out
```

As we remember, we have to apply the extended access-list as close as possible to source but here we have applied it to close to the destination because we have to block the traffic from both sales and marketing department, therefore, we have to apply it close to the destination here otherwise we have to make separate access-list for fa0/0 and fa1/0 inbound.

Named access-list example –

Now, considering the same topology, we will make a named extended access-list.

```
R1(config)# ip access-list extended blockacl
```

By using this command we have made an access-list named blockacl.

```
R1(config-ext-nacl)# deny tcp 172.16.40.0 0.0.0.255 172.16.50.0 0.0.0.255 eq 21
R1(config-ext-nacl)# deny tcp any 172.16.50.0 0.0.0.255 eq 23
R1(config-ext-nacl)# permit ip any any
```

And then the same configuration we have done in numbered access-list.

```
R1(config)# int fa0/1
R1(config-if)# ip access-group blockacl out
```

Conclusion: Thus I’ve studied the concept of ACL and their types and configured them using CLI.