Student Name_____ Student Roll Num_____

LAB # 12: ACCESS CONTROL LIST Part-I

- **Introduction to ACL**
- **Standard ACL Implementation**

Access Control List

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 conditions applied on entrance work as inbound filter. ACL conditions applied on exit work as outbound filter.

The three general rules of configuring ACLs:

There are three cardinal rules that should always be observed when configuring ACLs. These rules determine how traffic on a network will flow.

1 ACL per protocol – this is to control each of the protocols that you may have configured on your router.

1 ACL per direction – there are two directions in this case; inbound traffic is the traffic that is coming into the router whilst outbound traffic is traffic that is leaving the router.

1 ACL per interface – this is meant to control traffic from leaving the router through a specified interface.

There are two directions in which ACLs can be configured.

Inbound ACLs- with this type of ACL, the router checks the traffic that it receives from an interface against the configured ACLs before it can determine whether to route the traffic or not. This type of ACL is important since the router does not waste CPU cycles by processing packets that would eventually be dropped.

Outbound ACLs– with this type of ACL, the packets are usually processed and forwarded to the outward ACL for filtering. In this ACL, the router first checks in its routing table to see if the packet has a destination, if the destination is not in the routing table the packet is dropped. The second thing the router inspects is whether the outbound interface has an ACL, if the interface does not have an ACL for the packet, it is forwarded. Finally, for packets that have an ACL that is bound to the outbound interface, they are inspected by the ACL group statements to see if they match any criteria. If they match any criteria, the router decides whether to forward or drop the packet. If they do not match any criteria and the ACL does not permit them, they are dropped.

Types of ACLs

There are two types of ACLs:

Standard ACLs (1 – 99 and 1300 - 1999)

Extended ACLs (100 – 199 and 2000 – 2699) *will be discussed in next Lab*

There are also Named ACLs; Named ACLs are the extended version of existing ACLs. Named standard ACL is the extended version of standard ACL. Named extended ACL is the enhanced version of extended ACL. Existing ACLs (Standard and Extended) assign a unique number among all the ACLs. While Named ACLs assign a unique name among all the ACLs.

Standard ACLs (1 – 99 and 1300 - 1999)

ACLs are the part of Cisco IOS from its beginning. In earlier days simple filtering was sufficient. Standard ACLs are used for normal filtering. Standard ACLs filter the packet based on its source IP address.

Command to Configure Standard ACL

```
access-list access-list-number {permit|deny}
{host|source source-wildcard|any}
```

Example:

Suppose we want to permit traffic only from the host address 10.0.0.2 255.0.0.0 to Marketing LAN and blocking traffic from all other LAN and hosts in the topology see Figure 12.1.

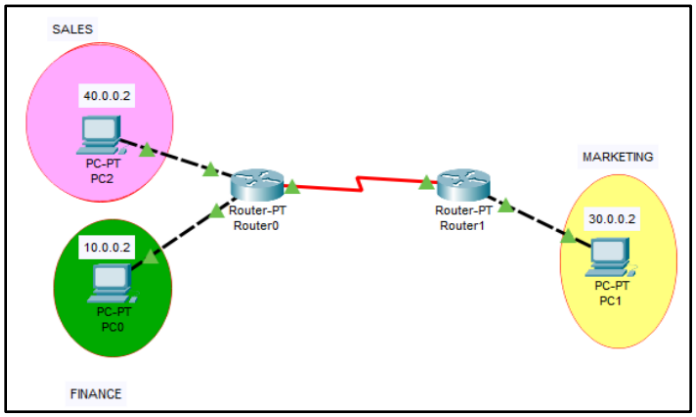


Figure 12.1

To meet with this requirement, we need to create two ACL conditions.

1. Permit 10.0.0.2 255.0.0.0.0

2. Block All

Configuration:

```
Router(config)#access-list 10 permit 10.0.0.2 0.0.0.0

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

For single host entry we can use both 0.0.0.0 wildcard mask or host keyword.

Applying ACL:

Once the access list is created, it needs to be applied to an interface by using the ip access-group ACL_NUMBER in|out interface subcommand. *in* and *out* keywords specify in which direction you are activating the ACL. in means that ACL is applied to the traffic coming into the interface, while the out keyword means that the ACL is applied to the traffic leaving the interface.

The command to apply the ACL to an interface:

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

As in our example following commands will activate Standard ACL number 10 on Fa0/0 interface in outbound direction

```
Router(config)#int Fa0/0
```

```
Router(config-if)#ip access-group 10 out
```

It is recommended to place the standard access lists as close to the destination as possible. In our case, this is the Fa0/0 interface on Router1. Since we wanted to evaluate all packets trying to exit out Fa0/0, we specified the outbound direction with the out keyword.

To check Access-lists, use the following command:

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

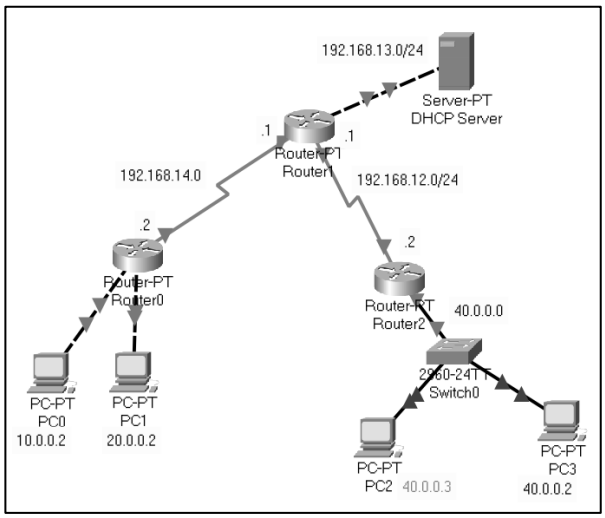
NOTE

At the end of each ACL there is an implicit deny all statement. This means that all traffic not specified in earlier ACL statements will be forbidden.

Student Name_____ Student Roll Num_____

LAB TASKs:

Considering following network topology:



1) Create an ACL 1 to deny traffic only from host 20.0.0.2/24 to DHCP server. Permit traffic from all other users of the network 20.0.0.0 and 10.0.0.0
2) Create another ACL 2 to permit traffic only from network 10.0.0.0 to network 40.0.0.0.