ASSIGNMENT-3

AIM : ACCESS CONTROL LISTS

PROBLEM STATEMENT: Using a N/W simulator, Configure a router using router commands, and ACLs.

THEORY:

- ACCESS CONTROL LISTS:

- ACLs are basically a set of commands, grouped together by a no. or name that is used to filter traffic entering or leaving an interface.

- When activating an ACL on an interface, you must specify in which direction the traffic should be filtered.
  - Inbound (as traffic enters interface)
  - Outbound (before traffic exits interface)

- Inbound ACLs:
  Incoming packets are processed before they are routed to an outbound interface. An inbound ACL is efficient because it saves the overhead of routing lookups if the packet will be discarded after it is denied by the filtering tests. If the packet is permitted by tests, it is processed for routing.

- Outbound ACLs:
  Incoming packets are routed to the outbound interface & then processed through outbound ACL

- ACL LIST RANGES:

TYPE	RANGE
IP Standard	1 - 99
IP Extended	100 - 199
IP Standard Expanded Range	1300 - 1999
IP Extended Expanded Range	2000 - 2699

- STANDARD ACCESS LISTS :

- Because a standard access list filters only traffic based on source traffic, all you need is IP address of host or subnet you want to permit or deny.

- ACLs are created in global configuration mod & then applied on an interface.

- Syntax :

```
access-list {1-99 |1300-1999} {permit | deny} src-add
[wildcard mask]
```

- Steps to configure Standard ACLs:

i. Use access-list global configuration command to create an entry in a standard ACL

ii. Use interface configuration command to select an interface to which to apply the ACL.

iii. Use the IP access grp interface configuration command to activate existing ACL on an interface.

• EXTENDED ACCESS LISTS:

- An extended ACL gives you much more power than just a standard ACL.

- Extended ACLs check both source & destination packet addresses. They can also check for specific protocols, port numbers, & other parameters that allow administrators more flexibility & control.

- Steps to configure Extended ACLs:

i. Use access-list global configuration command to create an entry in an extended ACL.

ii. Use the interface configuration command to select an interface to which to apply the ACL.

iii. Use IP access group interface configuration command to activate existing ACL on an interface.

- CONCLUSION :

In this assignment, we successfully configured router using router commands & configured ACL using a N/W simulator.