Sri Lanka Institute of Information Technology

IT2050 - Computer Networks
2nd Year, 1st Semester

Tutorial 9

---

1. Compare and contrast standard and extended Access Control Lists.

Standard ACL	**Extended ACL**
ACL number is in between 1-99	ACL number is in between 100-199
Checks only the source address	Checks both the source and destination address
Permits or denies entire protocol suite	Permits or denies specific protocols
Port numbers / services are not filtered	Filter the traffic using port number / service
Applied to the router(s) that is/are nearest to the destination	Applied to the router(s) that is/are nearest to the source

2. Explain what will happen if you apply an Access Control List without any statements to Fast Ethernet interface with inbound direction.
    - The implicit deny statement will be added to the list and will be applied – which states "deny any" – means that no inbound traffic will be allowed through that interface.

3. Design an IP access list that permits traffic from host 193.5.2.76, but denies all other IP traffic
    - Router(config)# access-list 13 permit 193.5.2.76 0.0.0.0 OR access-list 13 permit host 193.5.2.76

4. Design an IP access list that denies traffic from host 11.5.25.239, but permits all other IP traffic.
    - Router(config)# access-list 23 deny 11.5.25.239 0.0.0.0 OR access-list 23 deny host 11.5.25.239
    - Router(config)# access-list 23 permit any

5. Configure an IP access list that stops packets from subnet 134.141.7.0/24 from exiting serial 0 on a router. Allow all other packets.
    - Router(config)# access-list 33 deny 134.141.7.0 0.0.0.255
    - Router(config)# access-list 33 permit any
    - Router(config)# interface S0
    - Router(config-if)# ip access-group 33 out

6. Configure an IP access list that allows packets from subnet 101.100.45.32/27 from exiting serial 0 on a router. Deny all other packets.
    - Router(config)# access-list 43 permit 101.100.45.32 0.0.0.31

- Router(config)# interface S0
- Router(config-if)# ip access-group 43 out

7. Design an access list that denies IP traffic from hosts 152.5.35.83 and 104.2.64.33, permits IP traffic from all hosts on network 185.25.0.0/16, and denies all other IP traffic. Invoke your access list inbound on interface E2.
    - Router(config)# access-list 53 deny host 152.5.35.83 OR access-list 53 deny 152.5.35.83 0.0.0.0
    - Router(config)# access-list 53 deny host 104.2.64.33 OR access-list 53 deny 104.2.64.33 0.0.0.0
    - Router(config)# access-list 53 permit 185.25.0.0 0.0.255.255
    - Router(config)# interface E2
    - Router(config)# ip access-group 53 in

8. What will be the results for the following statements:

```
access-list 25 permit host 101.2.3.40
access-list 25 deny 203.45.0.0 0.0.255.255
access-list 25 permit any

interface  ethernet 1
 ip access-group 25 in
```

    - The above standard ACL will deny traffic from subnet 203.45.0.0/16 and allow traffic from 101.2.3.40 and any other hosts in the inbound direction of the Ethernet 1 interface

9. Configure an IP access list that allows only packets from subnet 193.7.6.0/24, going to hosts in network 128.1.0.0 And using web service in 128.1.0.0, to enter serial 0 on a router.
    - Router(config)# access-list 110 permit tcp 193.7.6.0 0.0.0.255 128.1.0.0 0.0.255.255 eq 80
    - Router(config)# interface S0
    - Router(config-if)# ip access-group 110 in

10. Configure and enable an IP access list that stops packets from subnet 10.3.4.0/24 from exiting from serial interface S0 and that stops packets from 134.141.5.4 from entering s0. Permit all other traffic.

    - Router(config)# access-list 20 deny 10.3.4.0 0.0.0.255
    - Router(config)# access-list 20 permit any
    - Router(config)# access-list 30 deny host 134.141.5.4 OR access-list 11 134.141.5.4 0.0.0.0
    - Router(config)# access-list 30 permit any
    - Router(config)# interface S0
    - Router(config-if)# ip access-group 20 out
    - Router(config-if)# ip access-group 30 in

11. Configure and enable an IP access list that allows packets from subnet 10.3.4.0/24, to any web server, to exit serial interface S0. Also allow packets from 134.141.5.4 going to all TCP-based servers using a well-known port to enter S0. Deny all other traffic.

    - Router(config)# access-list 113 permit tcp 10.3.4.0 0.0.0.255 any eq 80
    - Router(config)# access-list 114 permit tcp host 134.141.5.4 any lt 1024 OR access-list 114 permit tcp 134.141.5.4 0.0.0.0 any lt 1024
    - Router(config)# interface S0
    - Router(config-if)# ip access-group 113 out
    - Router(config-if)# ip access-group 114 in

12. what will be the results for given statements:

    access-list 164 deny tcp 14.3.6.234 0.0.0.0 host 6.5.4.1 eq 23
    access-list 164 deny udp any any eq tftp
    access-list 164 permit ip any any
    interface serial 0
    ip access-group 164 out

    - Deny telnetting (running in port 23) traffic from the host 14.3.6.234 (source) to the host 6.5.4.1 (destination) and also deny any tftp connections from the protocol udp and allow other traffic going out of the router's Serial 0 interface.