Computer Networks
2nd Year, 1st Semester

ACL Tutorial Sample Answers

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 source address	Checks source and destination address
Generally permits or denies entire protocol suite	Generally permits or denies specific protocols

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 apply which is 'deny any'

3. Design an IP access list that permits traffic from host 193.5.2.76, but denies all other IP traffic
   R1(config)# access-list 10 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.
   R1(config)# access-list 11deny host 11.5.25.239
   R1(config)# access-list 11 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.
   R1(config)# access-list 12 deny 134.141.7.0 0.0.0.255
   R1(config)# access-list 12 permit any

   R1(config)# interface s0
   R1(config-if)# ip access-group 12 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
   R1(config)# access-list 13 permit 101.100.45.32 0.0.0.62

   R1(config)# interface s0
   R1(config-if)# ip access-group 10 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.
   R1(config)# access-list 14 deny host 152.5.35.83
   R1(config)# access-list 14 deny host 104.2.64.33
   R1(config)# access-list 14 permit 185.25.0.0 0.0.255.255

   R1(config)# interface E2
   R1(config-if)# ip access-group 14 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
```

*It will deny access of subnet 203.45.0.0/16 and will allow 101.2.3.40 and rest of the host in the direction in 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.

```
R1(config)# access-list 101 permit tcp 193.7.6.0 0.0.0.255 193.7.6.0 0.0.255.255 eq 80

R1(config)# interface s0
R1(config-if)# ip access-group 101 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.

```
R1(config)# access-list 10 deny 10.3.4.0 0.0.0.255
R1(config)# access-list 10 permit any
R1(config)# access-list 11 deny host 134.141.5.4
R1(config)# access-list 11 permit any

R1(config)# interface s0
R1(config-if)# ip access-group 10 out
R1(config-if)# ip access-group 11 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.

```
R1(config)# access-list 101 permit tcp 10.3.4.0 0.0.0.255 any eq 80
R1(config)# access-list 102 permit tcp host 134.141.5.4 any lt 1023

R1(config)# interface s0
R1(config-if)# ip access-group 101 out
R1(config-if)# ip access-group 102 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 the host 6.5.4.1 from host 14.3.3.234.And also deny any tftp connections from the protocol udp and allow other traffic going out of the router's serial 0 interface.