DATE : ....

CN Lab

ACL (Access control list)

Standard ACL

* Router (config)#

access-list <1-99> <permit/deny>
<1300-1999>
<net addr> <wild card mask>

* (config)# interface <port>

* (config-if)#

ip access-group <1-99> (inbound/out)
<1300-1999>

Scenerio:

I. If src_ip = 192.10.1.0/24, permit

II. " " " = 192.10.2.0/24 deny

III. " " " = any, permit

apply for (gig 0/0/0) pin {assume}

Solution:

```
* access-list 10 permit 192.10.1.0 0.00.255
* access-list 10 deny 192.10.2.0 0.0.0.255
* access-list 10 permit any
```

```
* interface gig0/0/0
* ip access-group 10 outbound.
```

Standard ACL should be applied as close to the destination as possible.

operation: <eq, gt, lt, neq, range>

DATE : ....

Extended ACL

number= <100-199> <2000-2699>

protocol = tcp, udp, icmp, ip

codes:

```
* Router (config)#
access-list <num> <permit/deny> <protocol>
        <src_ip_addr> <src_wildcard_mask>
        <dst_ip_addr> <dst_wildcard_mask>
```

with port numbers:

```
*access-list <num> <permit/deny> <protocol>
 <src_ip_addr> <src_wild_card_mask> <op> <port>
 <dst_ip_addr> <dst_wildcard_mask> <op> <port>
```

Scenerio

1. Allow all traffic

⇒
```
access-list 110 permit ip any any
```

2. Prevent 10.0.0.0/16 from sending udp traffic to 192.168.1.1/32

⇒
```
access-list 115 deny udp
 10.0.0.0    0.0.255.255
 192.168.1.1    0.0.0.0
```

3. prevent 172.16.1.1/32 from pinging host in 192.168.0.0/24

⇒
```
access-list 120 deny icmp
 172.16.1.1    0.0.0.0
 192.168.0.0    0.0.0.255
```

4. prevent all host using source Udp port numbers from (2000- 3000) from accessing the server at 3.3.3.3/32

⇒
```
access-list 120 deny udp any
range 2000 3000   3.3.3.3   0.0.0.0
```

5. Allow hosts in 172.16.1.0/24 using a TCP source port greater than 9999 to access all TCP ports on server 4.4.4.4/32 except port 23

⇒
```
access-list 125 permit tcp
172.16.1.0  0.0.0.255  gt 9999
4.4.4.4  0.0.0.0  neq 23
```

DATE : ....

* Host in 190.160.1.0/24 can't use HTTPs to access 10.0.0.0/24

```
=> access-list 110 deny tcp
190.160.1.0 0.0.0.255 eq 443
10.0.0.0 0.0.0.255
```

* Hosts in 190.168.2.0/24 can't access 15.0.2.0/24

```
=> access-list 120 deny ip
190.168.2.0 0.0.0.255
15.0.2.0 0.0.0.255
```

* None of the host in 190.160.1.0/24 can ping 15.0.1.0/24

```
=> access-list 130 deny icmp
190.160.1.0 0.0.0.255
15.0.1.0 0.0.0.255
```

Last step:
* access-list <num> permit ip any any.

* interface gig0/0/0

* ip access-group <num> inbound.

Extended ACL should be apply as close to the source as possible.

Inbound ↓

Outbound ↑