

120.0.0.0/13

#	ID	Broadcast	#	ID	Broadcast
0	120.0.0.0	120.7.255.255	16	120.128.0.0	120.135.255.255
1	120.8.0.0	120.15.255.255	17	120.136.0.0	120.143.255.255
2	120.16.0.0	120.23.255.255	18	120.144.0.0	120.151.255.255
3	120.24.0.0	120.31.255.255	19	120.152.0.0	120.159.255.255
4	120.32.0.0	120.39.255.255	20	120.160.0.0	120.167.255.255
5	120.40.0.0	120.47.255.255	21	120.168.0.0	120.175.255.255
6	120.48.0.0	120.55.255.255	22	120.176.0.0	120.183.255.255
7	120.56.0.0	120.63.255.255	23	120.184.0.0	120.191.255.255
8	120.64.0.0	120.71.255.255	24	120.192.0.0	120.199.255.255
9	120.72.0.0	120.79.255.255	25	120.200.0.0	120.207.255.255
10	120.80.0.0	120.87.255.255	26	120.208.0.0	120.215.255.255
11	120.88.0.0	120.95.255.255	27	120.216.0.0	120.223.255.255
12	120.96.0.0	120.103.255.255	28	120.224.0.0	120.231.255.255
13	120.104.0.0	120.111.255.255	29	120.232.0.0	120.239.255.255
14	120.112.0.0	120.119.255.255	30	120.240.0.0	120.247.255.255
15	120.120.0.0	120.127.255.255	31	120.248.0.0	120.255.255.255

Directions:

If you need more room to write the ACLs that are required in the answers below, please use the back of this sheet and be sure to number each one correctly. When writing commands, start each line with the appropriate router prompt. You may use the help features on a router to complete the last

portion of this test.

Write an ACL that allows telnet from subnet 1 to subnet 30.

```
Router(Config)# access-list 101 permit tcp 120.8.0.0 0.7.255.255 120.240.0.0  
0.7.255.255 eq 23
```

Using the fewest lines possible, write an ACL that blocks all ip traffic from subnets 1 and 2 to subnets 16 and 17, but allows anything else. (3 lines minimum.)

```
Router (config)# access-list 101 deny 120.8.0.0 0.7.255.255 120.128.0.0 0.15.255.255  
Router (config)# access-list 101 deny 120.16.0.0 0.7.255.255 120.128.0.0 0.15.255.255  
Router (config)# access-list 101 permit any any
```

Using the fewest lines possible, write an ACL that allows tftp from subnets 2-7 to host 120.208.12.5, but blocks everything else. (2 lines minimum)

```
Router (config)# access-list 101 permit 120.16.0.0 0.15.255.255 host 120.208.12.5  
Router (config)# access-list 101 permit 120.32.0.0 0.31.255.255 host 120.208.12.5
```

What is the general rule for placing Standard ACLs in a network?

Standard ACLs go closest to the destination of filtered traffic.

What is the general rule for placing extended Acls in a network?

Extended ACLs go closest to the source of filtered traffic

If you had Access-list 101, how would you apply it to an interface such that it filtered traffic that came from a LAN to the router on interface F0/1?

```
Router (config) int f0/1
```

```
Router (config-if)# ip access-group 101 in
```