

Access-List Wildcards KEY KEY KEY KEY KEY KEY KEY

1. Copy the definition of a wildcard here.

A wildcard mask is a 32-bit quantity that is divided into four octets, with each octet containing 8 bits. A wildcard mask bit 0 means "check the corresponding bit value" and a wildcard mask bit 1 means "do not check (ignore) that corresponding bit value".

2. In a wild card a 0 means CHECK and a 1 means IGNORE

3. What range of IP addresses would the following statements allow?

A. Access-list 17 permit 175.25.26.0 0.0.0.255 175.25.26.0 - 175.25.26.255

B. Access-list 89 permit 190.12.0.0 0.0.255.255 190.12.0.0 - 190.12.255.255

C. Access-list 10 permit 10.10.10.0 0.0.0.255 10.10.10.0 - 10.10.10.255

4. For each of the following networks indicate the wildcard mask that would be used to ensure that no traffic from this network is transmitted.

12.0.0.0 0.255.255.255 199.34.25.0 0.0.0.255

145.16.0.0 0.0.255.255 205.34.23.0 0.0.0.255

5. Convert the following values into binary and then indicate what values will be permitted.

Access-list 24 permit 172.16.16.0 0.0.7.255

16 = 00010 000

7 = 00000 111 - indicates that the first 5 digits must match – last 3 digits are ignored so the range is from 00010 000 which equals 16 to 00010 111 which equals 23 (16 + 7) . In dotted decimal the range is 172.16.16.0 – 172.16.23.255

6. What is another way of writing 0.0.0.0 255.255.255.255 in an access list? ANY

7. What is another way of writing 125.42.7.25 0.0.0.0 in an access list? Host 125.42.7.25

8. List several wise practices you should employ when working with access-lists.

A. Two Approaches:

1. List the traffic you know you want to permit

Deny all other traffic

2. List the traffic you want to deny

Permit all other traffic (permit any)

B. Document your Access-list

After each line indicate exactly what that line is supposed to do.

C. Verifying Your Access-list

Show Access-lists

Show IP Interfaces

D. Revisit your access-list after a few days

Routers keep track of the number of packets that match each statement in an access-list

Use this information to reorder your access-list and thus improve its efficiency

E. Never remove an access-list that is applied to a port - this can crash a router