Cisco™ CCNA : Access-Lists

Access Lists

IP access lists are a sequential list of permit and deny conditions that apply to IP addresses or upper layer protocols. Access Control Lists are used in routers to identify and control traffic.

Purpose of Access Lists

1. Controlling traffic through a router, and
2. Controlling VTY access to a router's VTY ports
3. Filter incoming and outgoing packets
4. Restrict contents of routing updates
5. Trigger dial-on-demand routing (DDR) calls

Types of IP Access Lists

Standard IP Access Lists
Extended IP Access Lists
Named Access Lists

Wild Card Masking

Wild card masking is used to permit or deny a group of addresses.
For example, if we have a source address 185.54.13.2 and want all the hosts on the last octet to be considered, we use a wild card mask, 185.54.13.255.
The 32 bit wildcard mask consists of 1's and 0's
1 = ignore this bit
0 = check this bit

Special Case: Host 185.54.13.2 is same as 185.54.13.2 with a wild card mask of 0.0.0.0, considers only specified IP.
Any is equivalent to saying 0.0.0.0 with a wild card mask of 255.255.255.255. This means none of the bits really matter. All IP addresses need to be considered for meeting the criteria.

Standard Access List

1. These have the format, **access-list [number] [permit or deny] [source_address]**
Ex: access-list 1 permit 192.168.2.0 0.0.0.255
2. Place standard access lists as near the destination as possible and extended access lists as close to the source as possible.
3. Access lists have an implicit deny at the end of them automatically. Because of this, an access list should have at least one permit statement in it; otherwise the access list will block all remaining traffic.
4. Access lists applied to interfaces default to outbound if no direction is specified.

Extended Access Lists and Named Access Lists

Extended Access lists have the format,
access-list {number}{permit or deny} {protocol} {source}source-wildcard [operator [*port*]]{destination} destination-wildcard [operator [*port*]]
With extended IP access lists, we can act on any of the following:
- Source address
- Destination address
- IP protocol (TCP, ICMP, UDP, etc.)
- Port information (WWW, DNS, FTP, etc.)

Ex: access-list 101 permit icmp host 192.168.3.2 any

Named Access lists have the format, **ip access-list {standard /extended} name**
Ex: ip access-list extended denyping

Permitted numbers for access-lists

1-99: IP standard access list
100-199: IP extended access list
800-899: IPX standard access list
1000-1099: IPX SAP access list
1100-1199: Extended 48-bit MAC address access list
900-999: IPX extended access list