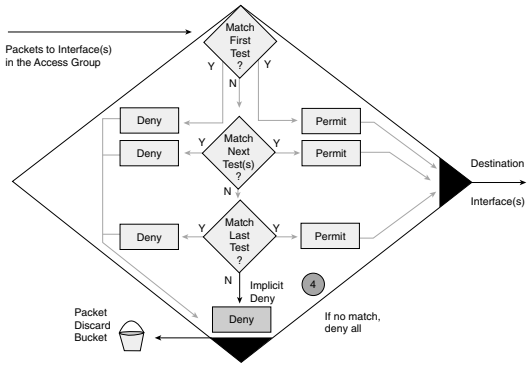


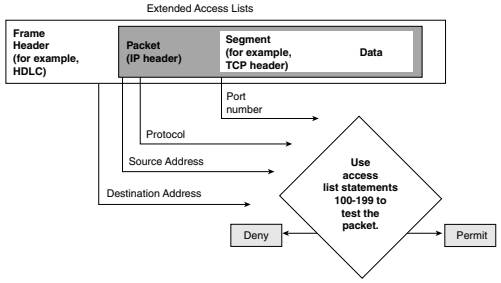
Guidelines for Implementing Access Lists

- Be sure to use the correct numbers for the type of list and protocols you want to filter.
- You can use only one access list per protocol, direction, and interface. A single interface can have one access list per protocol.
- Put more-specific statements before more-general ones. Frequently occurring conditions should be placed before less-frequent conditions.
- Additions are always put at the end of the access list. You cannot selectively add or remove statements in the middle of an access list.
- Without an explicit **permit any** statement at the end of a list, all packets not matched by other statements are discarded. Every access list should include at least one **permit** statement.
- An interface with an empty access list applied to it allows (permits) all traffic. Create your statements before applying the list to an interface.
- Access lists filter only traffic going through the router.

Protocol Access List Identifiers

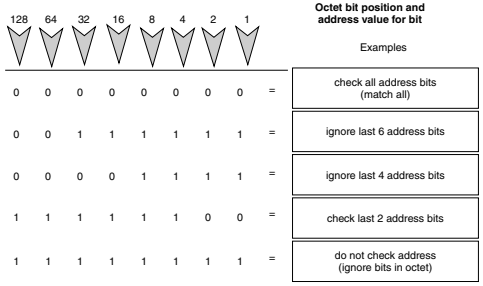
The access list number entered by the administrator determines how the router handles the access list. The arguments in the statement follow the number. The types of conditions allowed depend on the type of list (defined by the access list number). Conditions for an access list vary by protocol. You can have several different access lists for any given protocol, but only one protocol is allowed on any access list (one protocol per direction per interface).

TCP/IP Packet Tests



For TCP/IP packets, access lists check the packet and upper-layer headers for different items (this depends on the type of access list, standard or extended). Standard access lists are assigned a number in the range 1 to 99. Extended access lists use the range 100 to 199. As soon as a packet is checked for a match with the **access list** statement, it is either permitted to an interface or discarded.

Wildcard Masking



It is not always necessary to check bytes within an address. Wildcard masking identifies which bits should be checked or ignored. Administrators can use this tool to select one or more IP addresses for filtering. Wildcard masking is exactly opposite of subnet masking.