Packet Filtering

Access lists can be configured to permit or deny incoming and outgoing packets on an interface. By following a set of conventions, the network administrator can exercise greater control over network traffic by restricting network use by certain users or devices.

Applications of an IP Access List

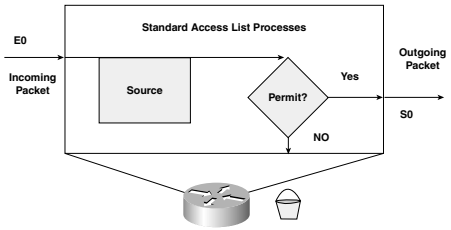
To establish an access list, you must define a sequential list of permit and deny conditions that apply IP addresses or IP protocols. Access lists filter only traffic going through the router; they do not filter traffic originated from the router. Access lists can also filter Telnet traffic in to or out of the router's vty ports.

Access List Type		Number Range/Identifier
IP	Standard Extended Named	1-99 100-199 Name (Cisco IOS 11.2 and later)
IPX	Standard Extended SAP filters Named	800-899 900-999 1000-1099 Name (Cisco IOS 11.2 F and later)

Other Access List Uses

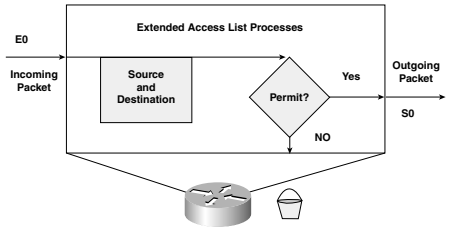
- Access lists allow finer granularity of control when you're defining priority and custom queues.
- Access lists can be used to identify "interesting traffic," which triggers dialing in dial-on-demand routing (DDR).
- Access lists filter and in some cases alter the attributes within a routing protocol update (route maps).

Types of Access Lists



There are two general types of access lists:

- Standard access lists check the source address of packets. Standard access lists permit or deny output for an entire protocol suite based on the source network/subnet/host IP address.
- Extended IP access lists check both source and destination packet addresses. Extended lists specify protocols, port numbers, and other parameters, giving administrators more flexibility and control.



Standard	Extended
Filter based on source	Filter based on source and destination
Permit or deny the entire TCP/IP protocol suite	Specify a specific IP protocol and port number
Range: 1 to 99	Range: 100 to 199

Access List Process Options

- **Inbound access lists**—Incoming packets are processed prior to being sent to the outbound interface. If the packet is to be discarded, this method reduces overhead (no routing table lookups). If the packet is permitted, it's processed in the normal way.
- **Outbound access lists**—Outgoing packets are processed by the router first and then are tested against the access list criteria.

Permit or Deny Process

Access list statements are operated on one at a time from top to bottom. After a packet header match is found, the packet is operated on (permitted or denied), and the rest of the statements are skipped.

If no match is found, the packet is tested against the next statement until a match is found or the end of the list is reached. An implicit **deny** statement is present at the end of the list. (All remaining packets are dropped.)

Unless there is at least one **permit** statement in an access list, all traffic is blocked.