Access Control Lists (ACLs):

- Sequential list of permit or deny rules that filter packets based on:

- Source and destination IP addresses

- Source and destination TCP/UDP ports

- ICMP message type and protocol

- Operates on either the network or transport layer of the OSI model

- Limited to one ACL per protocol, interface, and direction (inbound or outbound traffic)

- Serves as traffic flow control, security, network performance, and access control

- Operation process for an inbound ACL:

- If packet matches ANY of the rules, then it is allowed and sent to destination

- If packet matches NONE of the rules, then it is discarded

- Operation process for an outbound ACL:

- If there is no routing table entry for packet, then the packet is dropped

- If there is no ACL for a packet, then it is automatically forwarded by default

- If there is ACL and packet passes ANY of the rules, then it is forwarded

- If packet matches NONE of the rules, then it is dropped

- There are two types of ACLs:

- Standard -- only allow you to filter based on the source IP address

- Numbered from 1-99 and 1300-1999

- Extended -- can filter on source and destination IPs and ports, protocols, etc.

- Numbered from 100-199 and 2000-2699

- Can be identified by either numbers or names (ideally capitalized)

Process of ACL Operation:

- Note that all ACLs are processed from top to bottom in the list

- If the MAC address on the frame does not match that of router, then frame is dropped

- Apply inbound ACL to packet if it exists, drop packet is denied and forward if allowed

- If packet is forwarded, then the inbound packet goes to the outbound interface

- At the outbound interface, the outbound ACL is tested against the packet

- If denied, then the packet is dropped, otherwise it is forward to the outgoing interface

- Note: If packet is denied based on a rule, then it is a Deny, but if it matches no rules, then it is denied by default due to an Implicit Deny

Implementing ACLs on Networks:

- Every ACL should be placed to maximize efficiency and not waste network resources

- Extended ACLs should be placed as close as possible to the source of the traffic

- Standard ACLs should be placed close to the destination of the traffic

- Most frequently used ACL entries should be at the top of the list

Complex ACLs:

- Dynamic ACLs -- users who want to send packets through the network are blocked until they telnet into the router, and then a temporary ACL is added for a period of time that allows them to send packets through the router.

- Reflexive ACLs -- prevent packets from being received when no connection was setup

- when a packet is sent to a destination, a temporary ACL entry is added that allows the response to be received and forwarded back to the sender

- if no request was sent to the destination, then the response will be blocked

- Time-based ACLs -- enable and disable ACL entries based on the time of the day/week

IOS Commands:

- show access-lists -- shows all ACL entries in the router

- access-list [ID] [permit | deny] [?] -- adds an entry to the ACL that permits or denies

- any -- applies to all incoming and outgoing packets

- [tcp | udp] -- adds a protocol restriction

- [IPADDRESS] [WILDCARD] -- limit to source IP address and subnet mask

- any -- for some reason this is needed before adding port restrictions (?)

- [eq | lt | gt | neq | range] [ports] -- adds a source port restriction

- [IPADDRESS] [WILDCARD] -- limit to destination IP address and subnet mask

- [eq | lt | gt | neq | range] [ports] -- adds a destination port restriction

- established -- used for established TCP connections only

- ip access-list [standard | extended] [NAME] -- creates an ACL entry with a name

- then in (config-std-nacl) add permit and deny rules

- access-list [ID] permit host [IPADDRESS] -- allows a specific IP access to the network

- access-list [ID] remark [COMMENT] -- adds a comment for a specific ACL entry

- no access-list [ID] -- removes an entry from the ACL to eliminate the rule for it

- ip access-group [ACLID] [in | out] -- applies an ACL entry to a specific interface

- no ip access-group [ACLID] -- removes an ACL entry from a specific interface

- access-class [ACLID] [in | out] -- adds ACL entries for a connection in (config-line)