IPv6 Access Control Lists (ACLs)

Allow you to permit or deny traffic in your network

ACLs are a first line of defense in the real world, a firewall with protocol analyzers, IPS and IDS systems will be in place.

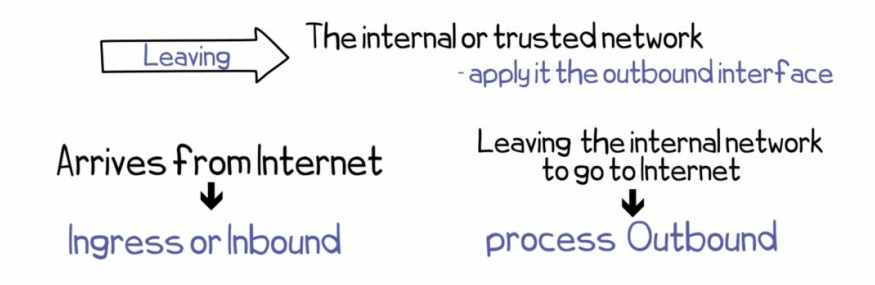
IPv6 ACLs share many of the same characteristics with IPv4
IPv6 ACLs can filter based on source/destination IPv6 address and they can also filter based on ICMP/TCP/UDP
Like IPv4 ACLs, IPv6 ACLs can implement QoS service policies.

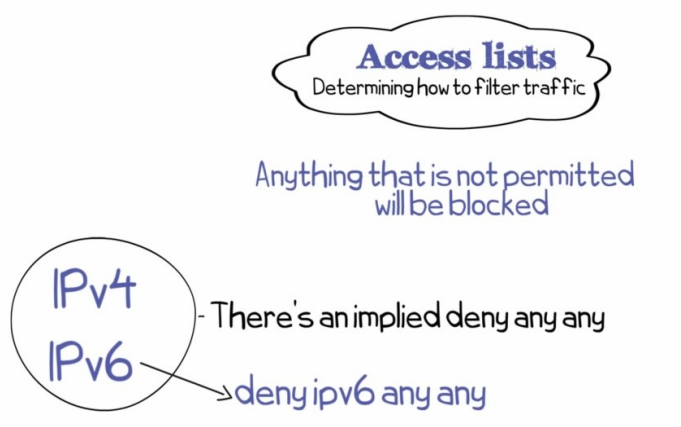
CCNA Course will focus on IPv6 ACLs to filter IPv6 packets being received or transmitted from router interfaces

Similarities
IPv4/IPv6 ACLs can match on the Source/Destination IP address in the protocol header
IPv4/IPv6 ACLs can match on individual host Addresses or subnets/prefixes
Both are Applied in an inbound or Outbound direction (on a router's interface or an SVI – Switch Virtual Interface)
Both can match on Transport Layer (Layer 4) protocol info – TCP / UDP / Source or Destination Port Number
Both can match on ICMP message types and codes
Both have an implicit deny statement at the end (that matches all remaining packets)
Both Support Time Based ACLs

Differences
IPv4 ACLs only match IPv4 packets and only match fields in IPv4 Headers
IPv6 ACLs are Independent and separate from IPv4 ACLs
IPv4 ACLs are identified by a name or a number
IPv6 ACLs are identified only by name
IPv4 ACLs identify whether an ACL is extended or standard 100-199 or 1-99
IPv6 ACLs uses standard or extended by are only differentiated by a Word (representing standard or extended) no #'s
IPv4 ACLs match on specific values unique to IPv4 (Precedence, ToS, TTL , fragments)
IPv6 ACLs match on specific values unique to IPv6 header (Flow Label, DSCP value, extensions, and option header values)
IPv6 ACLs have some implicit permit statements at the end of each ACL, just above the implicit deny all
IPv4 ACLs do not have implicit permit statements

IPv4/6 ACLs are applied to interfaces in either an inbound or outbound direction to router interfaces or to switch virtual interfaces (SVIs)
IPv4 ACLs and IPv6 ACLs are independent of each other and can be applied simultaneously with zero effect on the other
It makes sense to apply access lists on ingress (incoming) rather then egress (outgoing) interfaces
On an internet facing router, you want an inbound ACL denying access to the network and the router
You would rather deny packets before having to process them (save router overhead)
It is less secure to use on outbound ACL on a perimeter router's (internet facing) internal interface, rather put an ACL on the external interface and block traffic before it is processed by the router's routing table





Be careful when blocking Protocols in IPv6
ACLs
One protocol you will want to be specially careful with is ICMPv6
IPv4 used ARP to determine the IP address of a neighbor device, but ARP is no longer used in IPv6
NDP (Neighbor Discovery Protocol) is part of ICMPv6, so don't just deny ICMPv6
If you have a blanket deny of ICMPv6 inadvertently, it could effect the communication of devices in your IPv6 network
ICMPv6 also is used for path MTU Discovery.
You don't need to be as discerning when blocking ICMP in IPv4

IPv6 ACLs allow you to match on:

- Traffic Classes, Flow labels, IPv6 Next Header field,
- Source/Destination 128 bit IPv6 addresses,
- Upper-layer headers and Higher Layer Protocols (such as TCP / UDP at Layer 4)
- Protocols relevant port numbers and flags (such as SYN, ACK, SYNACK)
- ICMPv6 types and codes
- IPv6 extension header values and types

Limitations of IPv6 ACLs
IPv6 tends to have more tunnels than IPv4
(example IPv6 packets send over an IPv4 GRE tunnel (6to4 tunneling)
In IPv4 ACLs, wildcard masks don't have to be contiguous
In IPv6 ACL, you create ACLs using a prefix length number, that indicates the number of contiguous prefix mask bits

The Prefix length number represents the number of contiguous bits that will be matched for that IPv6 address prefix
We use a "slash" notation, where the number after the / indicates the number of bits of the prefix length

Meaning you can only match on an IPv6 address prefix and cannot use discontinuous masks with IPV6 ACLs

In addition, it is very common to have prefix mask lengths that are easily divisible by 4 (e.g. /48, /52, /56, /64)

Its not a standard practice to have a prefix length that doesn’t fall on a hex digit boundary

Its important to remember that Excessive Logging can impact router performance, therefore becareful using the logging keyword.

Just like an IPv4 ACL, IPv6 ACL don’t deny packets originating from a router

So a outbound ACL on router interface will not block router packets sent from that router