Access Control Lists Overview

- IPv4 Access Control Lists (ACLs) are packet filters that match layer 3 (IP) and layer 4 (TCP/UDP) fields to restrict traffic flows to or through the router.
- Traffic filtering is the main application of ACLs, but other applications exist such as route filtering (distribute-lists).
- IP ACLs are most common, but other types exist such as IPv6, MAC address, IPX, Appletalk, DECnet, MPLS, etc.
Types of IP ACLs

- IP ACLs fall into two categories, standard and extended
  - Standard ACLs
    - Defined by a name or number 1-99, 1300-1999
    - Match only on source IP address field
  - Extended ACLs
    - Defined by a name or number 100-199, 2000-2699
    - Match on source and destination IP address field along with details of Layer 3 and Layer 4 fields

Extended ACL Matches

- IP protocol number (ICMP, EIGRP, OSPF, IGMP, etc.)
- Source IP address
- Destination IP address
- Protocol fields
  - IP options (source route, timestamp, etc)
  - TCP / UDP ports (eq, neq, lt, gt, range)
  - TCP flags (SYN, ACK, FIN, PSH, etc.)
  - ICMP Type Code (echo, echo-reply, etc.)
  - Fragments
- QoS markings
  - DSCP
  - IP Precedence
  - Type of Service
- Time range
ACL Wildcards

- Both standard and extended ACLs use wildcard masks or inverse masks to decide which bits of the source or destination address to check or ignore
  - Wildcard mask is opposite of subnet mask
  - 0 bit in the wildcard means check
  - 1 bit in the wildcard means ignore
- Allows for flexible bit matching in the source or destination field

ACL Wildcard Examples

- Match no bits
  - 0.0.0.0 255.255.255.255
  - I.e. match “any” address
- Match all bits of address 1.2.3.4
  - 1.2.3.4 0.0.0.0
  - I.e. match “host” 1.2.3.4
- Match addresses with 1st octet of 10
  - 10.0.0.0 0.255.255.255
- Match addresses in subnet 192.168.0.0/24
  - 192.168.0.0 0.0.255.255
- Match addresses in subnet 150.1.0.0/18
  - 150.1.0.0 0.0.63.255
ACL Wildcard Examples (cont.)

- Match addresses with odd number in 1st octet
  - 1.0.0.0 254.255.255.255
- Match addresses with even number if 3rd octet
  - 0.0.0.0 255.255.254.255
- Match all class A addresses
  - 0.0.0.0 127.255.255.255
- Match all class B addresses
  - 128.0.0.0 63.255.255.255
- Match all class C addresses
  - 192.0.0.0 31.255.255.255
- Match all class D addresses
  - 224.0.0.0 15.255.255.255

ACL Wildcard Examples

<table>
<thead>
<tr>
<th>Addresses</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
<th>8</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wildcard</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating Standard ACLs

- Numbered standard ACLs
  - `access-list access-list-number {deny | permit} source [source-wildcard]`
- Named standard ACLs
  - `ip access-list standard {access-list-name | access-list-number}
    • [sequence-number] {deny | permit}
    source [source-wildcard]`

Creating Extended ACLs

- Numbered extended ACLs
  - `access-list access-list-number {deny | permit} protocol source
    source-wildcard destination
    destination-wildcard`
- Named extended ACLs
  - `ip access-list extended {access-list-name | access-list-number}
    • [sequence-number] {deny | permit}
    protocol source source-wildcard
    destination destination-wildcard`
**ACL Logging**

- Access-list hits can be logged to...
  - Console / Monitor / Buffer / Syslog
- Log options
  - “log” includes
    - List name / number
    - Permit / deny
    - Protocol name / number
    - Source / destination IP
    - Port numbers
  - “log-input” includes
    - All log options + source layer 2 address
      - MAC address
      - Input VC

**Applying ACLs**

- ACLs applied as a traffic filter use the `ip access-group` interface level command
  - Can also be applied to console, aux, or vty lines with `access-class` to filter management traffic
- ACLs can be applied both inbound and outbound
- Best practice is to apply ACL closest to the source of traffic being filtered
  - Saves bandwidth and resources
### ACL Caveats

- Only one ACL can be applied per interface, per protocol, per direction
  - E.g. only one inbound IPv4 ACL on Fa0/0
- ACLs are processed top down
  - Once match occurs, ACL loop exits
  - Implies more specific matches should be up top
- Last statement in ACL is always “implicit deny”
- Outbound ACLs can’t filter traffic locally generated by the router
  - E.g. can’t deny pings sourced from the router
- ACL names are case sensitive
  - To avoid confusion use all uppercase
- If an ACL is applied that doesn’t exist, no traffic is filtered

### ACL Examples

- Telnet
- SNMP
- DDoS
- Spoofing