CMPD414 Data and Computer Security

Chapter 7:
Access Control Lists
ACL: Network

Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router.

**Purpose:** To prevent certain traffic from entering or exiting a network.
What Access Lists Do

- It filters network traffic by controlling whether routed packets are forwarded or blocked at the router’s interfaces.

- Your router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists.

- Access list criteria could be the source address of the traffic, the destination address of the traffic, the upper-layer protocol, or other information.

- Note that sophisticated users can sometimes successfully evade or fool basic access lists because no authentication is required.
Why You Should Configure ACL?

• There are many reasons to configure access lists; for example, you can use access lists to restrict contents of routing updates or to provide traffic flow control.

• One of the most important reasons to configure access lists is to provide security for your network.

• You should use access lists to provide a basic level of security for accessing your network. If you do not configure access lists on your router, all packets passing through the router could be allowed onto all parts of your network.
• Access lists can allow one host to access a part of your network and prevent another host from accessing the same area.
• In Figure below, host A is allowed to access the HR network, and host B is prevented from accessing the HR network.

![Diagram showing network access]

• You can also use access lists to decide which types of traffic are forwarded or blocked at the router interfaces. For example, you can permit e-mail traffic to be routed, but at the same time block all Telnet traffic.
When to Configure ACL?

• Access lists should be used in “firewall” routers, which are often positioned between your internal network and an external network such as the Internet. You can also use access lists on a router positioned between two parts of your network, to control traffic entering or exiting a specific part of your internal network.

• To provide the security benefits of access lists, you should at a minimum configure access lists on border routers—routers situated at the edges of your networks. This provides a basic buffer from the outside network, or from a less controlled area of your own network into a more sensitive area of your network.
• On these routers, you should configure access lists for each network protocol configured on the router interfaces. You can configure access lists so that inbound traffic or outbound traffic or both are filtered on an interface.

• Access lists must be defined on a per-protocol basis. In other words, you should define access lists for every protocol enabled on an interface if you want to control traffic flow for that protocol.
Overview of ACL Configuration

- Each protocol has its own set of specific tasks and rules that are required in order for you to provide traffic filtering. In general, most protocols require at least two basic steps to be accomplished.
  - The first step is to create an access list definition,
  - The second step is to apply the access list to an interface.
Creating ACL

• Create access lists for each protocol you wish to filter, per router interface.

• For some protocols, you create one access list to filter inbound traffic, and one access list to filter outbound traffic.

• To create an access list, you specify the protocol to filter, you assign a unique name or number to the access list, and you define packet filtering criteria.

• A single access list can have multiple filtering criteria statements.
Assigning a Unique Name or Number to Each ACL

- When configuring access lists on a router, you must identify each access list uniquely within a protocol by assigning either a name or a number to the protocol’s access list.

- You can specify access lists by names for the following protocols:
  - Apollo Domain
  - IP
  - IPX
  - ISO CLNS
  - NetBIOS IPX
  - Source-route bridging NetBIOS
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>1–99, 1300–1999</td>
</tr>
<tr>
<td>Extended IP</td>
<td>100–199, 2000–2699</td>
</tr>
<tr>
<td>Ethernet type code</td>
<td>200–299</td>
</tr>
<tr>
<td>Ethernet address</td>
<td>700–799</td>
</tr>
<tr>
<td>Transparent bridging (protocol type)</td>
<td>200–299</td>
</tr>
<tr>
<td>Transparent bridging (vendor code)</td>
<td>700–799</td>
</tr>
<tr>
<td>Extended transparent bridging</td>
<td>1100–1199</td>
</tr>
<tr>
<td>DECnet and extended DECnet</td>
<td>300–399</td>
</tr>
<tr>
<td>XNS</td>
<td>400–499</td>
</tr>
<tr>
<td>Extended XNS</td>
<td>500–599</td>
</tr>
<tr>
<td>AppleTalk</td>
<td>600–699</td>
</tr>
<tr>
<td>Source-route bridging (protocol type)</td>
<td>200–299</td>
</tr>
<tr>
<td>Source-route bridging (vendor code)</td>
<td>700–799</td>
</tr>
</tbody>
</table>
Defining Criteria for Forwarding or Blocking Packets

• When creating an access list, you define criteria that are applied to each packet that is processed by the router; the router decides whether to forward or block each packet on the basis of whether or not the packet matches the criteria.

• Typical criteria you define in access lists are packet source addresses, packet destination addresses, and upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be defined.
• For a single access list, you can define multiple criteria in multiple, separate access list statements.

• Each of these statements should reference the same identifying name or number, to tie the statements to the same access list. You can have as many criteria statements as you want, limited only by the available memory.

• Of course, the more statements you have, the more difficult it will be to comprehend and manage your access lists.
The Implied “Deny All Traffic” Criteria Statement

• At the end of every access list is an implied “deny all traffic” criteria statement. Therefore, if a packet does not match any of your criteria statements, the packet will be blocked.

• For most protocols, if you define an inbound access list for traffic filtering, you should include explicit access list criteria statements to permit routing updates. If you do not, you might effectively lose communication from the interface when routing updates are blocked by the implicit “deny all traffic” statement at the end of the access list.
The Order in Which You Enter Criteria Statements

• Note that each additional criteria statement that you enter is appended to the \textit{end} of the access list statements. Also note that you cannot delete individual statements after they have been created. You can only delete an entire access list.

• \textit{The order of access list statements is important!} When the router is deciding whether to forward or block a packet, the software tests the packet against each criteria statement in the order in which the statements were created. After a match is found, no more criteria statements are checked.
• If you create a criteria statement that explicitly permits all traffic, no statements added later will ever be checked. If you need additional statements, you must delete the access list and retype it with the new entries.
Creating and Editing Access List Statements on a TFTP Server

- The first command of an edited access list file should delete the previous access list (for example, type a `no access-list` command at the beginning of the file).

- If you do not first delete the previous version of the access list, when you copy the edited file to your router you will merely be appending additional criteria statements to the end of the existing access list.
Applying Access Lists to Interfaces

- For some protocols, you can apply up to two access lists to an interface: one inbound access list and one outbound access list.

- With other protocols, you apply only one access list which checks both inbound and outbound packets.
• If the access list is inbound, when the router receives a packet, the software checks the access list’s criteria statements for a match. If the packet is permitted, the software continues to process the packet. If the packet is denied, the software discards the packet.

• If the access list is outbound, after receiving and routing a packet to the outbound interface, the software checks the access list’s criteria statements for a match. If the packet is permitted, the software transmits the packet. If the packet is denied, the software discards the packet.

• Access lists that are applied to interfaces do not filter traffic that originates from that router.