ACCESS CONTROL LISTS

Advanced Systems Administration Course

Fred Msumeno
University computing Centre Ltd,
University of Dar es salaam,
E-mail: mfred@udsm.ac.tz
Website: www.udsm.ac.tz
What Access Lists Do

- Access lists filter 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, based on the criteria you specified within the access lists.
Why You Should Configure Access Lists

There are many reasons to configure access lists

- to provide security for your network
- to provide traffic flow control
- filter packets flow *in* or *out* of router interfaces
- restrict network use by certain users or devices

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.
When to Configure Access Lists

- 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.
Creating Access Lists

- 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.

- **Note** Access lists of some protocols must be identified by a name, and access lists of other protocols must be identified by a number. Some protocols can be identified by either a name or a number. When a number is used to identify an access list, the number must be within the specific range of numbers that is valid for the protocol.
Creating Access Lists

- Protocols with Access Lists Specified by Names

<table>
<thead>
<tr>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-route bridging NetBIOS</td>
</tr>
<tr>
<td>Apollo Domain</td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td>IPX</td>
</tr>
<tr>
<td>ISO CLNS</td>
</tr>
<tr>
<td>NetBIOS IPX</td>
</tr>
</tbody>
</table>
## Creating Access Lists

### Protocols with Access Lists Specified by Numbers

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>1 to 99</td>
</tr>
<tr>
<td>Extended IP</td>
<td>100 to 199</td>
</tr>
<tr>
<td>Ethernet type code</td>
<td>200 to 299</td>
</tr>
<tr>
<td>Ethernet address</td>
<td>700 to 799</td>
</tr>
<tr>
<td>Transparent bridging (protocol type)</td>
<td>200 to 299</td>
</tr>
<tr>
<td>Transparent bridging (vendor code)</td>
<td>700 to 799</td>
</tr>
<tr>
<td>Extended transparent bridging</td>
<td>1100 to 1199</td>
</tr>
<tr>
<td>DECnet and extended DECnet</td>
<td>300 to 399</td>
</tr>
<tr>
<td>XNS</td>
<td>400 to 499</td>
</tr>
<tr>
<td>Extended XNS</td>
<td>500 to 599</td>
</tr>
<tr>
<td>AppleTalk</td>
<td>600 to 699</td>
</tr>
<tr>
<td>Source-route bridging (protocol type)</td>
<td>200 to 299</td>
</tr>
<tr>
<td>Source-route bridging (vendor code)</td>
<td>700 to 799</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>IPX</td>
<td>800 to 899</td>
</tr>
<tr>
<td>Extended IPX</td>
<td>900 to 999</td>
</tr>
<tr>
<td>IPX SAP</td>
<td>1000 to 1099</td>
</tr>
<tr>
<td>Standard VINES</td>
<td>1 to 100</td>
</tr>
<tr>
<td>Extended VINES</td>
<td>101 to 200</td>
</tr>
<tr>
<td>Simple VINES</td>
<td>201 to 300</td>
</tr>
</tbody>
</table>
Defining Criteria for Forwarding or Blocking Packets

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

- Typical criteria you define in access lists are packet source addresses, packet destination addresses, or upper-layer protocol of the packet. However, each protocol has its own specific set of criteria that can be defined.

- Note that each additional criteria statement that you enter is appended to the 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.
Rules followed when comparing traffic with an ACL

- Is done in sequential order; line 1, line 2, line 3 etc
- Is done in the direction indicated by the keyword `in` or `out`
- Is compared with the access list until a match is made; then NO further comparisons are made
- There is an implicit “deny” at the end of each access list; if a packet does not match in the access list, it will be
Terms

- **Inbound**
  Traffic that a device receives through its interfaces

- **Outbound**
  Traffic that leaves the device through its interfaces

- **Standard IP access list**
  - ranges (1 - 99) & (1300-1999)
  - simpler address specifications
  - generally permits or denies entire protocol suite

- **Extended IP access list**
  - ranges (100 - 199) & (2000-2699)
  - more complex address specification
  - generally permits or denies specific protocols
Access list syntax

- Standard IP Access List Configuration Syntax
  - `access-list access-list-number {permit | deny} source {source-mask}`
  - `ip access-group access-list-number {in | out}`

- Extended IP Access List Configuration Syntax
  - `access-list access-list-number {permit | deny} protocol source {source-mask} destination {destination-mask}`
  - `ip access-group access-list-number {in | out}`

- Named IP Access List Configuration Syntax
  - `ip access-list {standard | extended} {name | number}`
Where to place Access lists

- Place **Standard IP** access list close to destination
- Place **Extended IP** access lists close to the source of the traffic you want to manage
What are Wild Card Masks?

- Are used with access lists to specify a host, network or part of a network.
- To specify an address range, choose the next largest block size e.g.
  - To specify a host (mask 255.255.255.255)
    - 196.200.220.1/32 -- 196.200.220.1 0.0.0.0
  - To specify a small subnet (mask 255.255..255.248)
    - 196.200.220.8 /29 -- 196.200.220.8 0.0.0.7
  - To specify all hosts on a /24 network:
    - 196.200.220.0/24 --- 196.200.220.0 0.0.0.255
- Short cut method to a quick calculation of a network subnet to wildcard:
  - 255 – {netmask bits on subnet mask}
  - Example: to create wild card mask for 196.200.220.160 255.255.255.240
    - 196.200.220.160 0.0.0.15 {255 – 240}
For a router with two interfaces, fastEthernet 0/0 (LAN interface) and FastEthernet0/1 (WAN interface) you configure as follows:

DUCE-RTR#config t

DUCE-RTR(config)#access-list 107 deny tcp any any eq 445

*This tells the router to block tcp packets on port 445 from any source to any destination*

DUCE-RTR(config)#access-list 107 permit ip 196.44.160.128 0.0.0.7 any

This tells the router to permit IP (any IP in this network) 196.44.160.128 with mask 255.255.255.248 (wildcard 0.0.0.7) to any IP (any network)
Instead of adding one-by-one access list you may create access list on a separate file and then apply them at once in the router

access-list 107 deny tcp any any eq 1236
access-list 107 deny udp any any eq 1236
access-list 107 deny tcp any any eq 1062
access-list 107 deny udp any any eq 1062
access-list 107 permit ip 196.44.168.8 0.0.0.7 any
access-list 107 permit ip 82.206.143.64 0.0.0.7 any
access-list 107 permit ip 196.44.160.0 0.0.7.255 any
access-list 107 permit ip 10.103.161.0 0.0.0.255 any
access-list 107 permit ip 196.44.160.128 0.0.0.7 any
access-list 107 deny ip any any
access-list 108 deny tcp any any range 135 139
access-list 108 deny udp any any range 135 netbios-ss
access-list 108 deny tcp any any eq 445
access-list 108 deny tcp any any eq 1434
access-list 108 deny udp any any eq 1434
access-list 108 deny tcp any any eq 6667
access-list 108 permit ip 196.44.160.128 0.0.0.7 any
access-list 108 deny ip any any
Then go to the router configuration mode and apply all access list at once.

After that apply the access control list 107 as inbound access list on the LAN interface and access control list 108 as outbound on the WAN interface.

DUCE-RTR(config)#interface fastEthernet 0/0
DUCE-RTR(config-if)#ip access-group 107 in

Exit from in LAN interface and go to the WAN interface
DUCE-RTR(config)#interface fastEthernet 0/1
DUCE-RTR(config-if)#ip access-group 108 out
Exit the interface and save the configuration
EXERCISE

1. Configure your router LAN interface with access list to do the following
   a. Deny tcp access to your network at ports 445, 135 to 139
   b. Deny udp access to your network at ports 445, 1236, 16384 to 16403
   c. Deny any access from your network to a host 196.44.161.110
   d. Deny access from one of the host in your network to internet
   e. Permit access from your network to 196.44.160.0 with mask 255.255.240.0
   f. Permit any access from your network to 82.206.143.64 with mask 255.255.255.248
2. Configure your router WAN interface with the following access control lists.
   a. permit your network to access any thing to the internet
   b. permit smtp service from two hosts(mail servers) to any server over the internet
EnD