

Introduction to Routers

TEL-335
Week 9 – Access Control Lists
Part 1

Access Control Lists

- ACLs are a way to tell a router which traffic it should find “interesting”
- Common misconception that ACLs only filter traffic
- Filtering is the most common use, however ACLs are used for several other purposes, such as:
 - Specifying traffic to undergo NAT or PAT
 - Filtering routing information
 - Designating priority traffic for QoS

ACL Overview

- An ACL causes the router to discard some packets based on criteria defined by the network engineer.
- The goal of an ACL is to prevent unwanted traffic in the network
- To prevent rouge users from penetrating the network
- To prevent employees from using network resources they should not be using

ACL Features

- Packets can be filtered as they enter an interface, before the routing decision.
- Packets can be filtered before they exit an interface, after the routing decision.
- “Deny” is the term used in Cisco IOS software to imply that the packet will be filtered.
- “Permit” is the term used in Cisco IOS software to imply that the packet will not be filtered.
- The filtering logic is configured in the access list.
- At the end of every access list is an implied “deny all traffic” statement.

ACL Features, continued

- Access lists have two major steps in their logic
1. Matching
 - Examines each packet and determines whether it matches the access-list statement
 2. Action
 - Deny or Permit

ACL Logic

- Access lists are a series of statements with matching criteria and resulting actions.
- Each statement is evaluated in sequence.
- Step 1 – The matching parameters of the first access-list statement are compared with the packet
- Step 2 – If a match is made, the action defined in this access-list statement is performed
- Step 3 – If a match is not made in Step 2, Step 1 is repeated using the next sequential access-list statement
- Step 4 – If no match is made with an entry in the access list, the deny action is performed

ACL Logic, continued

- The matching criteria available to access lists is based on fields inside the IP, TCP, and UDP headers.
- There are two types of access lists:
 1. Standard
 - Examines the source IP address only
 2. Extended
 - Can examine source and destination IP addresses, source and destination port numbers, along with several other fields

ACL Wildcards

- You can configure an ACL to permit or deny an individual IP address
- You can configure the portion of the IP address that is checked by the ACL
- ACL wildcard masks
 - 0 indicates that a bit is examined
 - 1 indicates a “don’t care”

Standard IP Access List Configuration

- Configuration commands
 - Interface subcommand to enable access lists
ip access-group {number|name [**in**|**out**]}
 - Global command for standard IP access list
access-list access-list-number (**deny**|**permit**)
source [source-wildcard]

Standard IP Access List Configuration, continued

- Example

```
configure terminal
interface ethernet 0
ip address 192.168.5.1 255.255.255.0
ip access-group 1 out
exit
access-list 1 deny 192.168.5.200 0.0.0.0
access-list 1 permit 0.0.0.0
255.255.255.255
```

Standard IP Access List Configuration, continued

- Example, modified

```
configure terminal
interface ethernet 0
ip address 192.168.5.1 255.255.255.0
ip access-group 1 out
exit
access-list 1 deny host 192.168.5.200
access-list 1 permit any
```

Standard IP Access List Configuration, continued

- EXEC Commands

```
show ip interface
show access-lists [access-list-number|access-list-name]
show ip access-list [access-list-number|access-list-name]
```

Standard IP Access List Configuration, continued

- Standard IP access lists use a number between 1 and 99
- The access-list command is a global configuration command, not a subcommand under an interface.

Extended IP Access Lists, continued

- What can be matched:
 - Source IP address
 - Portions of the source IP address
 - Destination IP address
 - Portions of the destination IP address
 - Protocol type (TCP, UDP, ICMP, IGRP, GMP, and others)
 - Source port
 - Destination port
 - Established – matches all TCP flows except the first
 - IP TOS
 - IP precedence

Extended IP Access List Configuration

- Configuration commands

```
access-list access-list-number
{deny|permit}
protocol source source-wildcard
destination
destination-wildcard
```

Extended IP Access List Configuration, continued

- Examples

```
access-list 101 deny tcp any host
192.168.1.1 eq 23
any source address, destination 192.168.1.1,
TCP header, destination port 23
access-list 101 deny ip 10.10.10.0
0.0.0.255 20.20.0.0 0.0.255.255
source address in 10.10.10.0 subnet,
destination in 20.20.0.0 subnet
```

Extended IP Access List Configuration, continued

- Extended IP access lists use a number between 100 and 199 inclusive

Named IP Access Lists

- Named IP access lists allow the same logic to be configured as with numbered standard and extended access lists.
 - A name is a more intuitive reminder of the list's function
 - Names allow for more access lists than 99 standard and 100 extended
 - Named access lists allow individual statements to be deleted.
 - The actual names used must be unique across all named access lists of all protocols and types on an individual router

Named IP Access Lists, continued

- Creating a named access list places the user into a named access list submode
- Configuration command

```
ip access-list {standard|extended}  
name
```

Today's Lab

- Using your local workstations for the first time!
- IIS (web) and Mail server services will be installed (unless they are install already).
- Once we've connected and played with those, we'll apply ACLs (all four types covered in the lecture) and see them in action!

LAB!
