**Source:** [**www.cisco.com**](http://www.cisco.com/)

**Access Control Lists**

# Lab Manual 11

**CLO4**

## **Router Configurations (Access Control Lists)**

* Access Control Lists used to implement security in routers
  + powerful tool for network control
  + filter packets flow in or out of router interfaces
  + restrict network use by certain users or devices
  + deny or permit traffic
* Rules Followed When Traffic Is Compared To An Access Control List
  + Is done in sequential order; line 1, line 2, line 3 e.t.c
  + 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 discarded
* Using Access Control Lists
  + Standard IP Access Lists (1 - 99)
    - simpler address specifications
    - generally permits or denies entire protocol suite
  + Extended IP Access Lists (100 - 199)
    - more complex address specification
    - generally permits or denies specific protocols
* Syntax of using access lists
  + 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}
* Where to place access control 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
* Using Wild Cards
  + Are used with access lists to specify a host, network or part of a network
* Wild Card Masks
  + Are used with the host/network address to tell the router a range of addresses to filter
* Examples:
* to specify a host: 81.199.108.1 0.0.0.0
* to specify a small subnet: 81.199.108.8 – 81.199.108.15 (would be a /29)
* Block size is 8, and wildcard is always one number less than the block size
* Cisco access list then becomes: 81.199.108.8 0.0.0.7
  + to specify all hosts on a Class C network: 81.199.108.0 0.0.0.255
* **What are wild card masks**
  + Short cut method to a quick calculation of a network subnet to wildcard:
* 255 – {netmask bits on subnet mask}
* to create wild card mask for 81.199.108.160 255.255.255.240
* 81.199.108.160 0.0.0.15 {255 – 240}
* to create wild card mask for 81.199.108.0 255.255.252.0 81.199.108.0 0.0.3.255
* **Examples**
  + Router(config)#Access-list access-list-number {permit|deny}{test conditions}
  + Router(config)#{protocol} access-group access-list-number
* e.g check for IP subnets 81.199.108.80 to 81.199.108.95 81.199.108.80,

Address and Wildcard Mask: **81.199.108.80 0.0.0.15**

* Wildcard bits indicate how to check corresponding address bit
  + 0=check or match
  + 1=ignore
* Matching Any IP Address
  + 255.255.255.255
  + or abbreviate the expression using the keyword any
* Matching a specific host
  + 81.199.108.8 0.0.0.0
  + or abbreviate the wildcard using the IP address preceded by the keyword host

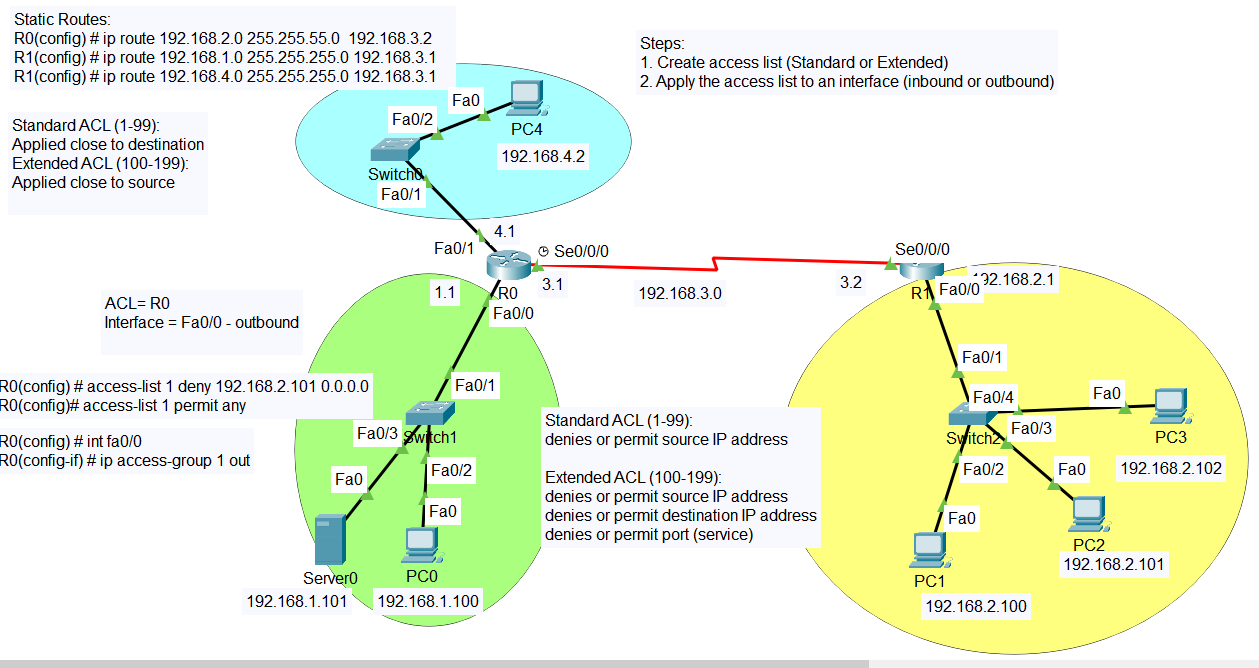
Lab Task

**Task 1:**

Use the topology created below and apply Standard ACL:

Assign valid IP address as shown in the topology

1. attach one webserver on a network
2. assign it a valid ip address from the pool and then deny one hosts of the other network to have an access to this webserver.



Task 2: Do Similar task for Extended ACL