Access Control Lists

Access lists are used as a form of firewall security on a router. Access lists are statements that a router will use to check traffic against, and if there is a match, the router can filter that traffic by either permitting or denying the packets based on the access list statement.

Cisco routers can be configured to utilize a variety of access lists with the most basic being the standard ACL, or access list. The standard access list number range is 1 to 99 and 2000 to 2699. The basic access lists in the Cisco CCNA curriculum are the standard access list, the extended access list and the named access list. The named access list is given a name instead of a number and is configured to be either a standard or extended access list.

Access lists are written and read line-by-line, each line in the access list is a statement or rule. At the end of the access list is an implicit "deny all" or "deny any," meaning even though you cannot see it, there is a "deny all" at the end of the access list. This can cause a problem because many people assume that by default an access list is permissive, and that you only have to write statements that deny the traffic you want to filter, and that everything else will be permitted, but this is in fact false.

Type of Access Control Lists (ACL):

1. Standard Access Control Lists
2. Extended Access Control Lists

Steps:

1. Create the access list (standard or extended)
2. Apply the access list to an interface (inbound or outbound)

1. Create the ACL

Standard ACL (1-99, and 2000-2699):

Denies or Permits:

1) Source IP address

Extended ACL (100-199):

Denies or Permits:

1) *Source IP address*
2) *Destination IP address*
3) *Port (service)* (optional)

Azim Uddin Chowdhury
Instructor, Dept of CSE & UIU CISCO Academy
United International University

2. Apply the ACL

- A *standard ACL* is applied *inbound or outbound* on the router interface that is *closest to the destination* of the traffic.
- An *extended ACL* is applied *inbound or outbound* on the router interface that is *closest to the source* of the traffic.

Cisco IOS CLI Commands

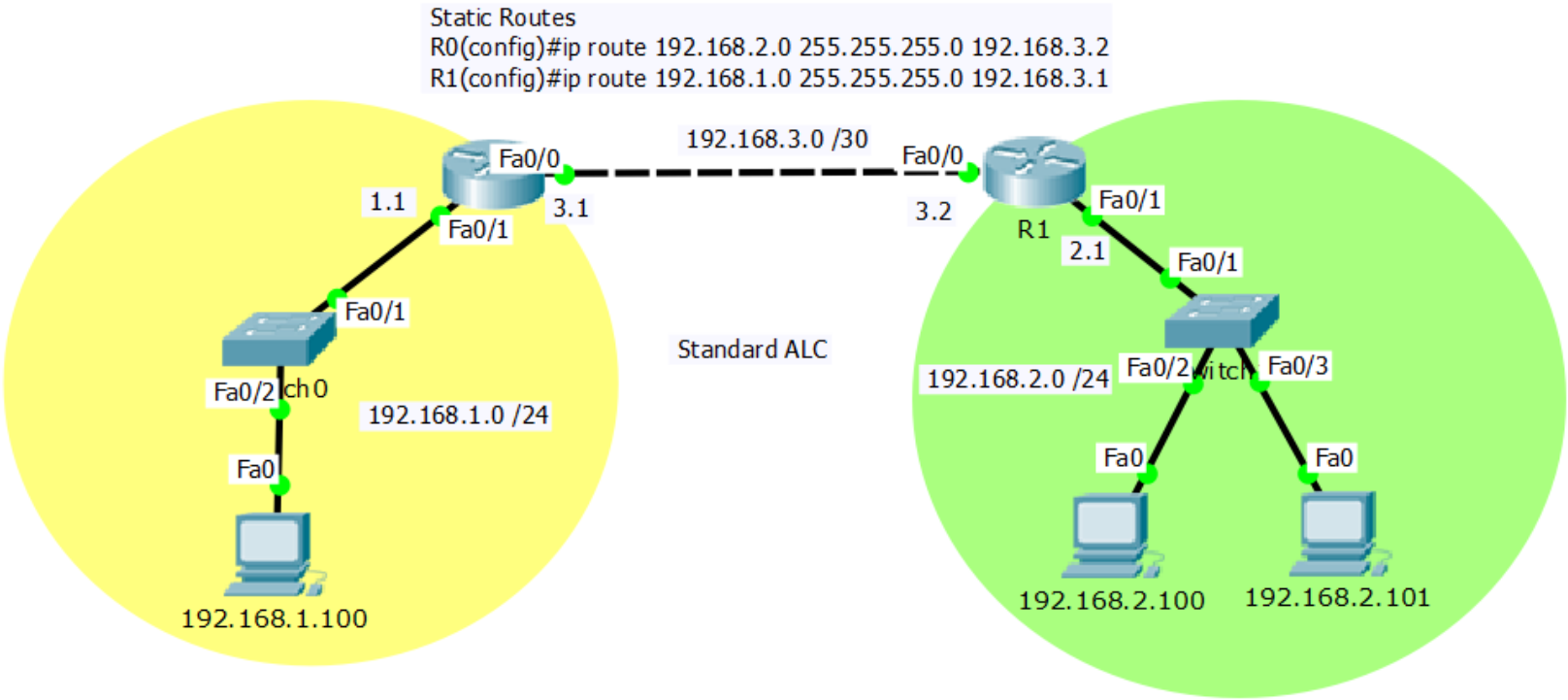
Standard ACL:

Standard access list command format:

#access-list <1-99> <deny | permit> <source ip address> <wildcard bits>

OR,

#access-list <1-99> <deny | permit> host <source ip address>



Examples:

Deny or permit a network:

`router` (config)#access-list 1 deny 192.168.1.0 0.0.0.255
`router` (config)#access-list 1 permit 192.168.2.0 0.0.0.255

Deny or permit a host:

```
router (config)#access-list 1 deny 192.168.1.100 0.0.0.0
router (config)#access-list 1 deny host 192.168.1.100
```

`router` (config)#access-list 1 permit 192.168.2.101 0.0.0.0
`router` (config)#access-list 1 permit host 192.168.2.101

Azim Uddin Chowdhury
Instructor, Dept of CSE & UIU CISCO Academy
United International University

Deny or permit all hosts:

```
router(config)#access-list 1 deny any
router(config)#access-list 1 permit any
```

Apply the access list to a router interface outbound and inbound

```
router(config)#interface fastEthernet 0/0
router(config-if)#ip access-group 1 out
```

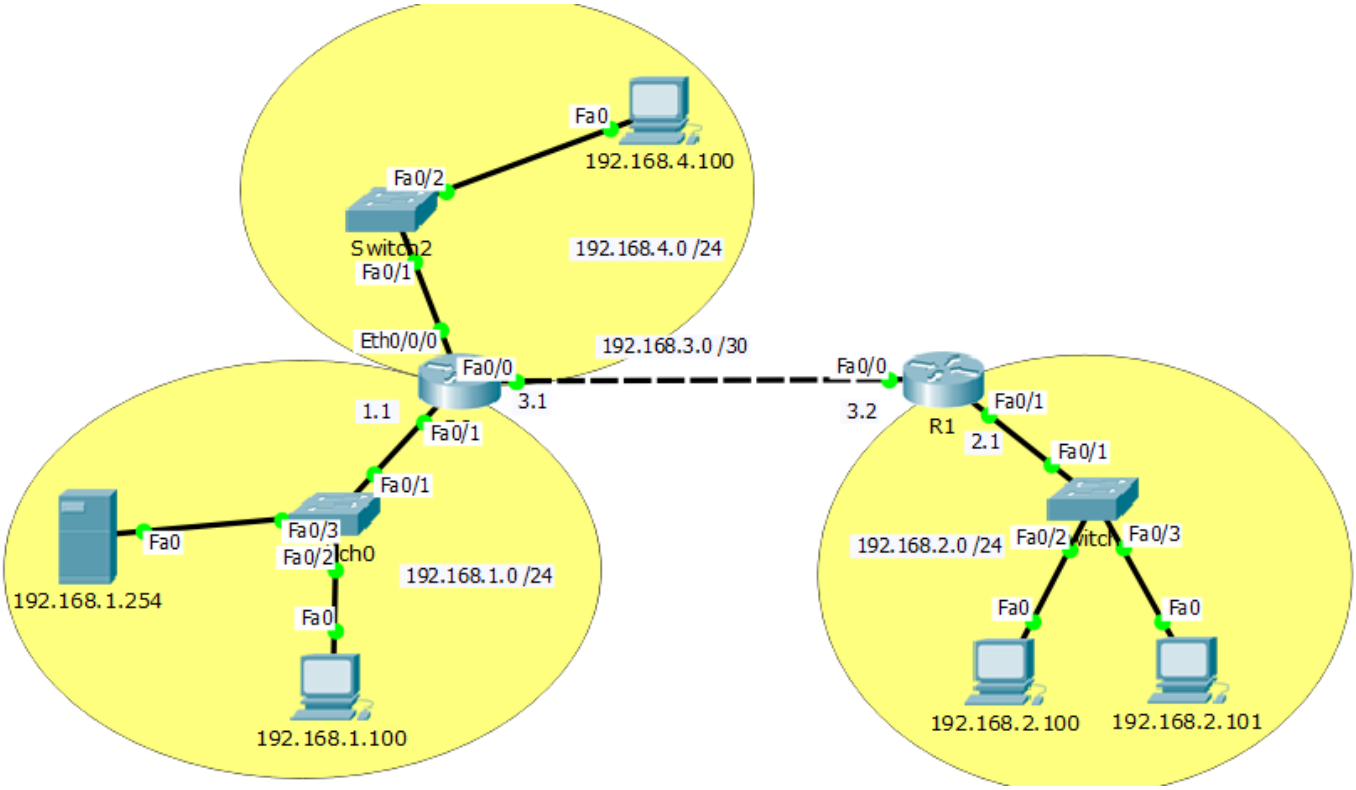
Extended access list

Extended access list command formats:

#access-list <100-199> <deny | permit> <protocol> <source ip address> <wildcard bits> <destination ip address> <wildcard bits> <operator> <port or service>

#access-list <100-199> <deny | permit> <protocol> host <source ip address> host <destination ip address> <operator> <port or service>

#access-list <100-199> <deny | permit> <protocol> <source ip address> <wildcard bits> <destination ip address> <wildcard bits>



Extended access list examples:

Deny and permit a source class c network to a destination class c network:

router(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

router(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

Azim Uddin Chowdhury
Instructor, Dept of CSE & UIU CISCO Academy
United International University

Deny or permit a source host to a destination /24 network:

router(config)#access-list 100 deny ip 192.168.1.100 0.0.0.0 192.168.4.0 0.0.0.255
router(config)#access-list 100 deny ip host 192.168.1.100 192.168.4.0 0.0.0.255
router(config)#access-list 100 permit ip 192.168.1.101 0.0.0.0 192.168.4.0 0.0.0.255
router(config)#access-list 100 permit ip host 192.168.1.101 192.168.4.0 0.0.0.255

Deny or permit any host to any destination on port 80 (http):

router(config)#access-list 100 deny tcp any any eq 80
router(config)#access-list 100 permit tcp any any eq 80

Deny or permit all hosts:

router(config)#access-list 100 deny any any
router(config)#access-list 100 permit any any

Apply the access list to a router interface outbound and inbound

router(config)#interface fastethernet 0/0
router(config-if)#ip access-group 100 out

router(config)#interface fastethernet 0/1
router(config-if)#ip access-group 100 in

Azim Uddin Chowdhury
Instructor, Dept of CSE & UIU CISCO Academy
United International University