Cisco CCNA (200-301)

Configuring and Verifying Access Control Lists

Learning Objective: Configure and Verify Extended ACLs

Description: Routers look at destination IP address to make a routing decision on how packets will leave that router. You will learn how to use the IOS Access Control List to identify traffic to either permit or deny it towards its destination.

Q: What is the purpose of ACLs on Cisco Devices?

- Help to identify traffic via IP address, Protocol that we want to allow or deny
- These examine every packet by the IP address according to configuration to control access
- There are 2 types access control lists: Standard and Extended. Today we are looking specifically deeper in configuring extended ACLs.

Q: How do they work?

- List is evaluated from top to bottom--Most specific rule to generic
    - It is evaluated until a match, then it stops.
- There is an implicit deny any traffic at the end of every list
    - If traffic does match any other rule in the list it will be *implicity denied.*

Q: How do we configure extended ACLs?

- Extended ACLs
    - Identifies source IP address, destination IP Address and Protocol
    - permits / denies
- Extended ACLs
    - ```
      NYEDGE1#configure terminal
      Enter configuration commands, one per line.  End with CNTL/Z.
      NYEDGE1(config)#access-list 110 permit tcp host 192.168.16.10 any eq ftp
      NYEDGE1(config)#access-list 110 permit tcp host 192.168.16.10 any eq ftp-data
      NYEDGE1(config)#access-list 110 deny icmp host 192.168.16.10 host 172.15.0.10
      NYEDGE1(config)#exit
      NYEDGE1#NYEDGE1#show access-lists 110
      ```
- Apply the ACL to the interface
    - ```
      NYEDGE1#configure terminal
      Enter configuration commands, one per line.  End with CNTL/Z.
      NYEDGE1(config)#interface GigabitEthernet 0/0
      NYEDGE1(config-if)#ip access-group 110 in
      NYEDGE1(config-if)#exit
      NYEDGE1(config)#
      ```
    - ```
      ping www.practice-labs.com
      ftp www.practice-labs.com
      ```

Endnotes, External and Etc.

5.6 Configure and verify access control lists
      ```