Cisco CCNA (200-301)

Configuring and verifying Standard ACLs

Learning Objective: Configure and verify Standard 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.

Teaser

Intro

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 them?

- Standard ACLs
    - Identifies only the source IP address
    - permits / denies
    - must be applied on an interface
- Standard ACLs (configure ACL)
    - ```
      NYEDGE1#configure terminal
      NYEDGE1(config)#access-list 10 deny host 192.168.16.10
      NYEDGE1(config)#exit
      NYEDGE1#show access-lists
      NYEDGE1#configure terminal
      NYEDGE1(config)#access-list 10 permit any
      ```
    - Apply the ACL to the interface
    - ```
      NYEDGE1(config)#interface gigabitethernet 0/0
      NYEDGE1(config-if)#ip access-group 10 in
      NYEDGE1(config-if)#exit
      NYEDGE1(config)#exit
      NYEDGE1#
      ```
    - PLABCSCO01 and NYCORE1 to test
    - ```
      cmd
      ping 172.14.0.1
      ```
    - ```
      ping 172.14.0.1 (NYCORE1)
      ```

Outro

Endnotes, External and Etc.

5.6 Configure and verify access control lists