DATE 23/0/24
PAGE 40

Practical-6

* Aim → Router configuration Network Setup.

* Theory →
1) Create the network Topology →
→ Drag and drop devices:
a) Add two routers from the device list.
b) Add two switches, one for each router.
c) Add two PC's per switch (total of four PC(s).)

2) Connect the devices →
a) Use the appropriate cables: Ethernet Cables between the PC's and switches, and Serial or Ethernet cables between the routers, depending on the model.
b) Ensure connections are properly made each PC to the switch and each switch to the router.

3) Assign IP addresses to the PC's →
→ Go to each PC, click on it, and then go to the Desktop tab > IP configuration.

→ Configuration →
a) For PC1 (Connected to Router's 1s network)
i) IP address: 192.168.1.2
ii) Subnet Mask: 255.255.255.0
iii) Default Gateway: 192.168.1.1

b) For PC2 (Connected to Router 2's network) →

i) IP address → 192.168.2.2
ii) Subnet Mask → 255.255.255.0
iii) Default Gateway → 192.168.2.1

3) Configure IP Addresses on Routers →
→ Click on Router 1, go to CLI, and enter the following commands:

enable
Configure terminal
interface Gigabit Ethernet 0/0
IP address 192.168.1.1 255.255.255.0.
No shutdown
Exit.

→ Similarly, for Router 2 →
enable
Configure terminal
interface Gigabit Ethernet 0/0.
IP address 192.168.2.1 255.255.255.0
No shutdown
Exit

4) Configure Serial Interface for Router to Router connection →

* for Router 1 →
interface Serial 0/0/0
IP address 10.0.0.1 255.255.255.255
Clock rate 64000

no shutdown
exit

* For Router 2 →
Interface Serial 0/0/0
IP address 10.0.0.2 255.255.255.252
no shutdown
exit

* ~~Routing Configuration → 1) Configure Static Routing →~~
• On Router 1:
→ Ip Router 192.168.2.0 255.255.255.0 10.0.0.8

• On Router 2:
→ IP Router 192.168.1.0 255.255.255.0 10.0.0.1

2) Test Connectivity →
1) Use the ping command from PC1 (192.168.1.2) to ping PC2 (192.168.2.2).
2) On PC1, go to command prompt and type ping 192.168.2.2.
3) If every thing is configured correctly, you should receive successful replies.

3) Configure Dynamic Routing (Optional - RIP):
→ On Router 1:
Router rip
Version 2
network 192.168.1.0
network 10.0.0.0

no auto - summary
exit
=> On Router 2:
Router rip
Version 2
network 192.168.2.0
network 10.0.0.0
no auto-summary
exit
=> Verify Routing -> • On each router, check the routing table with show ip route
• You should see the router to other network listed.
=> With this setup, your routers are configured to forward traffic between the two network using either static routes or RIP as a dynamic routing protocol.

!! Warning Optional to Write A
Enable
Config t
Hostname Lab A
Enable Secret class
Line con 0
Passcode Cisco
Login
Line vty 0 4
Password Cisco

Login
Enit
Int e0
Ip add 192.5.5 L 255.255.255.0
No shut
Int e1
Ip add 205.7.5.1 255.255.255.0
No shut
Int s0
Ip add 201.100.11.1 255.255.255.0
Clock rate 56000
No shut
Exit
Router rip
Network 192.55.0
Network 205.7.5.0
Network 201.100.111)
Exit
IP host lab
IP host lab
IP host lab

- IP host lab A 192.5.5.1 205.7.5.1 201.100.11.1
- IP host lab B 219.17.100.1 199.6.18.) 201.100.11.2.
- IP host lab C 223.8.151.1 204.204.7.1 199.6.13.2
- IP host lab D 210.93.105.2 204.204.7.2

IP host Lab E 210.93.105.2
EXIT
EXIT
Copy num start

* Conclusion → In this we configured routers to establish connectivity between different network segments. By setting up interfaces, assigning IP addresses, and implementing routing protocols, we achieved seamless communication across the network!!

Practical-7

Aim → To study about Access Control Lept.

Theory → Introduction to ACL's →

1) Access control list (ACL) is a set of rules used to control network traffic and reduce network attacks.
2) Two main types → Standard ACL and Extended ACL.
3) Standard ACL's filter traffic based on source IP address only. They are generally used to permit or deny entire protocols.

2) Purpose of Standard ACL's →
Control Access to network resources by defining rules based on IP addresses. Help improve security and reduce unauthorized access.

3) Characteristics of Standard ACL's →
i) Identified by numbers 1-99 and 1300-1999
ii) Only considers source IP address for filtering.
iii) Placed closet to the destination network.

4) Syntax → Basic Command Structure →
Access-list <number> <permit/deny>
<source IP> <wildcard mask>.

* Example → Access-list to permit 192.168.1.0 0.0.0.255.

5) Wildcard Mask → Used to specify a range of IP's in ACL's. 0 means exact match, 1 means "any".

* Practical Configuration Example →
• Example Scenario →
⇒ Objective → Block access to the 192.168.1.0 network from a particular subnet (Eg → 192.168.2.0) while allowing other traffic.

* Network Setup → i) Router with interfaces on 192.168.1.0 and 192.168.2.0 networks.
ii) Applying ACL to Prevent 192.168.2.0 from accessing 192.168.2.0.

* Step by Step Configuration → 1) Enter Configuration Mode
Router > Enable
Router # Configure terminal

2) Create Standard ACL
⇒ Deny traffic from 192.168.2.0 and permit other traffic.
Router (Config) # Access-list 10 deny 192.168.2.0 0.0.0.255
Router (Config) # Access-list 10 permit any.

3) Apply ACL to an interface ⇒
⇒ Apply the ACL to an interface (ty ⇒ fast ethernet 0/0).
Router (Config) # interface fast ethernet 0/0.
Router (Config) # ip access-group 10 in

4) Verification ⇒ 1) Use show access lists to view ACL rules Router # show access lists. 2) Confirm that traffic from 192.168.2.0 is blocked.

3) Standard ACL's should be applied close to the destination.

4) Test ACL functionality to ensure it meets the requirements.

* Conclusion ⇒ In this we concluded the implementation of access control lists (ACL's) to regulate traffic flow in a network. By configuring standard and extended ACL's we effectively restricted unauthorized access while allowing permitted traffic