Intro to Router configurations. - Lab 3

* Modes

-> User mode (mainly checking for router status)
-> Privileged mode (Perform additional status monitoring and entering into configuration mode.)
-> Global configuration mode.
(To configure global configurations which will affect the router as a whole and to enter into specific configuration modes.

* Help command

- ?
-> You can use this in any mode to view all the supported commands in that particular mode.

- show?
-> Use to issue this as a way of finding the additional options of a command.

* Set a message of the day banner
-> You should be in global configuration mode.

name (config) # banner motd @ message @

* Remove the privilage mode password.

name (config) # no enable password.

* Saving running config to startup-config.
-> You should be in Privilage mode.

name # copy running-config startup-config

* View the routing table with diredly connected networks.

name # show ip route.

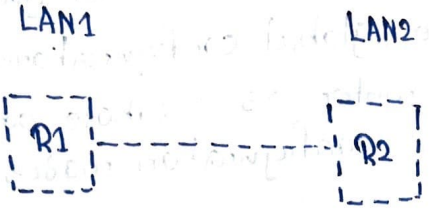
Lab-3

* Enable inter LAN communication by configuring static routing and default routing

-> global configuration mode

-> name(config)# ip route <Destination network address> <Des net subnetmask> <exit interface name/next hop ip address>

In ex :-



-> Above R1 and R2 each one is connected to a separate LAN. In order for devices on LAN 1 to communicate with device on LAN 2 we need to configure routing on both devices.

-> One way to configure routing is to use static routing. With static routing, we manually configure the routes that each route will be use to reach the other LAN. for example, we could configure R1 to use the following static route to reach LAN 2

ip route 192.168.2.0 255.255.255.0 192.168.1.2

This tells R1 that in order to reach the 192.168.2.0/24 network (which represents ~~R2~~ Lan2) it should ~~use~~ send Packets to the next hop address 192.168.1.2 (which is the Ip address of R2's interface on R1

We could configure R2 to use a static route to reach LAN 1

ip route 192.168.1.0 255.255.255.0 192.168.2.2

-> Another way is default route, default route is a route that is used when there is no specific route in the routing table for a particular destinations network. in other way, if a router doesn't know how to reach a particular network, it will send the Packet to the next hop address specified in the default route. we could configure R1 to use the following defant route to reach any network that it doesn't have a specific route.

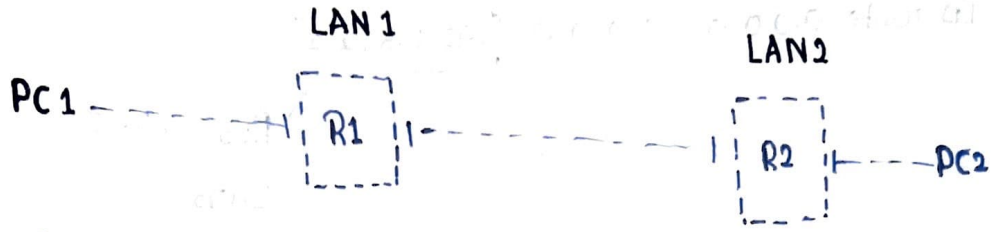
ip route 0.0.0.0 0.0.0.0 192.168.1.2 ← R2's interface on LAN1

We could configure R_2 to use a default route to reach any network that it doesn't have a specific route,

Ip route 0.0.0.0 0.0.0.0 192.168.2.2

↖ R_1's interface on LAN_2

Lab 4 - RIP routing configuration.



-> We have two LANs connected by two routers, we want to use RIP routing to enable communication between PC1 and PC2

- First we need to enable routing on both routers

```
name (config)# router rip
```

- Next, we need to configure the interface on both routers that ~~participate~~ participate in RIP routing. For example on R1,

```
R1 (config)# interface FastEthernet0/0
R1 (config-if)# ip address 192.168.1.1 255.255.255.0
                # ip rip send version 2
                # ip rip receive version 2
                # ip rip authentication mode text
                # ip rip authentication string mypassword.
                # ip rip enable.
```

-> Configure the Ip address of the interface as 192.168.8.1 with Subnet mask of 255.255.255.0

-> Configure the router to ~~rip version~~ send and receive RIP version 2 packets on this interface.

-> Enable authentication for RIP packets using a Plain text password of "mypassword".

-> Enables RIP routing on the interface.

after update, update should be propagated.

```
name (config-router)# default-information originate
```

-> Now RIP is enabled on the interfaces. now need to configure the network statement for RIP routing These statement tell the routers which networks should be advertised via RIP.
on R1,

```
R1(config-if router)# network 192.168.1.0
                    # network 192.168.2.0
```

- This configuration tells R1 to advertise the 192.168.1.0/24 and 192.168.2.0/24 networks via RIP.

on R2,

```
R2(config-router)# network 192.168.2.0
                  # network 192.168.1.0
```

*Why should disable auto summerization?

When communication is happenning from one network to another this router 1 should get summerized details about every network it encounters.
If we enable auto summerization sometimes in would be get over traffic

This is because auto-summerization can conse routing issue in networks withe discontiguous subnets or variable length subnet mask (VLSMs)

Auto summarization is a feature that is enabled by default in RIPv1 and can enabled in RIPv2. It allows a route to summarize networks with different subnet mask into a single network entry in the routing table.

```
name(config)# router rip
     (config-router)# version 2
                    # no auto-summary
```

Lab 5 - Switch Security

→ observe the ip configuration of the router, switch and PCs using the

```
name#show ip interface brief
```

→ Assign the ip address 192.168.50.111 to the switch and connect the switch to the Router's fa0/0 interface. configure the default gateway of the switch and PC.s using

```
name#(config)# interface vlan1
    (config-if)# ip address 192.168.50.111 255.255.255.0
    (config-if)# no shutdown
    (config)# ip default-gateway 192.168.50.1
```

→ Observe the switch Mac address table using

```
name# show mac-address-table
```

→ Security policy of the switch

There are three violation mode

- shutdown (shutdow the port by violate rules. discard transmission and disable the port)
- ~~sticky~~
- ~~stic~~ protect (Drop unauthorized packets. without any notificati
- restrict (discard unauthorized mac addresses and not disable the port) (notify user to using syslog message is generated to notify the network administrator)

→ Disable all unuse ports in fa0/6-24 interface range

```
name(config)# interface rang fastEthernet 0/6-24
(config-if-range)# shutdown.
```

-> Configure fastEthernet 0/3 as an access port security enable and set a maximum of 2 MAC address allowed. Allowed only one specific MAC address (0004:9A 47.8113) to be connected to the interface. set violation mode shutdown.

```
name (config)# interface fa0/3
    (config-if)# switchport mode access
        # switchport port-security
        # switchport port-security maximum 2
        # switchport port-security mac-address 0004.9A47.81
        # switchport port-security violation shutdown.
```

-> Configure fa0/4 use sticky learning method for MAC address and set the violation mode to "restrict"

```
name (config)# interface fa0/4
    (config-if)# switchport port-security mac-addres sticky
    (config-if)# switchport port-security violation restrict
```

-> Verify the port security configuration using

```
name# show port-security interface <interface-name>
```

Lab-6 - VLAN

→ To create a VLAN we have to give an ID and a name.

- Create VLAN in switch0

```
(config)# vlan <VLAN ID>
(config-vlan)# name <vlan name>
(config-vlan)# exit
```

→ Go back to the privileged mode and run the command below to view information of the created VLANs.

```
name#show vlan brief.
```

→ Configure VTP (Virtual Trunk Protocol)

- At the first change the switch port mode of the interface of the switch 1 which is connected with switch 2 to TRUNK.

```
(config)# interface <name>
(config-if)# switchport mode trunk
```

When using VTP, between interface network devices (Router, switch) should be in TRUNK mode and interface connected with end devices (PCs) should be in access mode. When changed a port mode of an interface the other end will automatically change its port mode.

- To transfer the VLANS in switch 1 to switch 2 should act as a server and client. Switch2 should act as a client
- To show status.

```
name#show VTP status.
```

- The domain name of the both switches also have to be same because then only these switches will exchange VLAN information among them using VTP since they are in the same domain.

```
(config)# vtp mode server          → switch 1
         # vtp domain name1

(config)# vtp mode client          → switch 2
         # vtp domain name1
```

→ Now run

Show vlan brief

command in Switch 2 and check weather the VLANs created in Switch 1 are now available in switch 2

→ VLANs are now available in both switches but still the PCs are not assigned to VLANs.
This can be done by assiging the interfaces of the switch to VLANs.

→ Assign ports to VLANs

Now the connected PCs must be allocated to VLANs and the port mode of interfaces which is connected with end devices should be change to access

```
name(config)# interface <interface name>
(config-if)# switchport mode access
(config-if)# switchport access vlan <VLAN ID>
```

→ Assign Ip address for the router's sub interfaces.

To create sub interface, assign dot1q encapsulation and to assign Ip addresses, Enter the global configuration mode in Router and follow the below command.

```
(config)# interface fa0/0.50
(config-subif)# encapsulation dot1Q 50
(config-subif)# ip address 192.168.50.1 255.255.255.0

(config)# interface fa0/0.100
(config-subif)# encapsulation dot1Q 100
(config-subif)# ip address 192.168.100.1 255.255.255.0
```

→ After configure the sub interfaces, go inside the main interface and run no shutdown comand to turn on the main interface.

```
(Config)# interface fa0/0
# no shutdown
```

→ ~~Next~~ Next you have to update the default gateway of the PCs in the network according to the VLAN.

PC1 - default gateway - 192.168.100.1

PC2 - " - 192.168.50.1

PC3 - " - 192.168.150.1

Lab Sheet7- ~~TCP~~ ACL

-> Apply the standard Access control list configuration for the following

1) PC2 is allowed to access network 172.16.0.0
2) PC3 in not allowed to access network 172.16.00
3) Only PC4 of lan_R can transmit data to Lan-S

1) access-list 1 permit 172.16.0.0 0.0.255.255
   access-list 1 permit any
   interface <interface name>
   ip access-group 1 in

2) access-list 2 deny 172.16.0.0 0.0.255.255
   access-list 2 permit any
   interface <interface name>
   ip access-group 2 in.

3) access-list 3 permit host <PC4 IP>
   access-list 3 deny any
   interface <interface name>
   ip access-group 3 in

-> Extend access control list configuration.

- PC1 is not allowed to access the web service in Server1
- PC3 is not allowed to access the ~~se~~ ftp service in Server1
- PC2 is not allowed to access the ftp service in Server1
- Any other traffic will be allowed.

access-list 110 deny tcp host 172.16.0.10host 172.17.0.100 eq 80
access-list 110 deny tcp host 172.16.0.20 host 172.17.0.100 eq ftp
access-list 110 permit ip any any
interface fa0/0
ip access-group 110 in

Lab 8 - DHCP

→ Configure a Router as a DHCP Server.

- Configure the excluded ipv4 addresses.

```
(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
(config)# ip dhcp excluded-address 192.16.30.1 192.168.30.10
```

- Create a DHCP Pool on R2 for the R1 LAN.

```
(config)# ip dhcp pool R1-LAN (Create DHCP pool)
```

Configure the DHCP Pool to include the network address, the default gateway and the IP address of the DNS server.

```
(dhcp-config)# network 192.168.10.0 255.255.255.0
(dhcp-config)# default-router 192.168.10.1
              # dns-server 192.168.20.254
```

→ Configure DHCP Relay

Configure R1 and R3 as a DHCP relay agent.

```
(config)# int g0/0
(config-if) ip helper-address 10.1.1.2
```

→ Configure R2 as a DHCP client

```
(config)# interface g0/1
(config-if)# ip address dhcp
           # no shutdown

name# show ip interface brief
```

→ Verify DHCP and connectivity

```
name# show ip dhcp binding
```