Ganpat University | Institute of Computer Technology

॥ विद्यया समाजोत्कर्षः ॥

Name: Tushar Panchal

En.No: 21162101014

Sub: CN (Computer Networks)

Branch: CBA

Batch:51

----------PRACTICAL 04----------

- **AIM :** Implement an access control list in a network of an organization containing different departments.
- **Scenario :**

There is an organization named CORPUS having 6 different departments Admin, HR, Support, Development, Testing and Design. IPv4 addressing scheme is used for assigning the IP address to the device. Each department has multiple employees, which have specific rights to communicate within the network. The details of the rights are as mentioned below:

The Admin Department can access all the devices in the organization. The Testing Department can only communicate with the Admin, HR and Development department. Only the head of the development department can communicate with the support department. Two members of the support department out of five members can contact the design department.

Implement the network in Cisco packet tracer, as per the requirement. As the number of the end devices are not mentioned in the requirement, you can take as per your requirement.

- ✓ **Procedure :**

1. Create a network department as follows :

ADMIN DEPARTMENT – 200.0.0.0

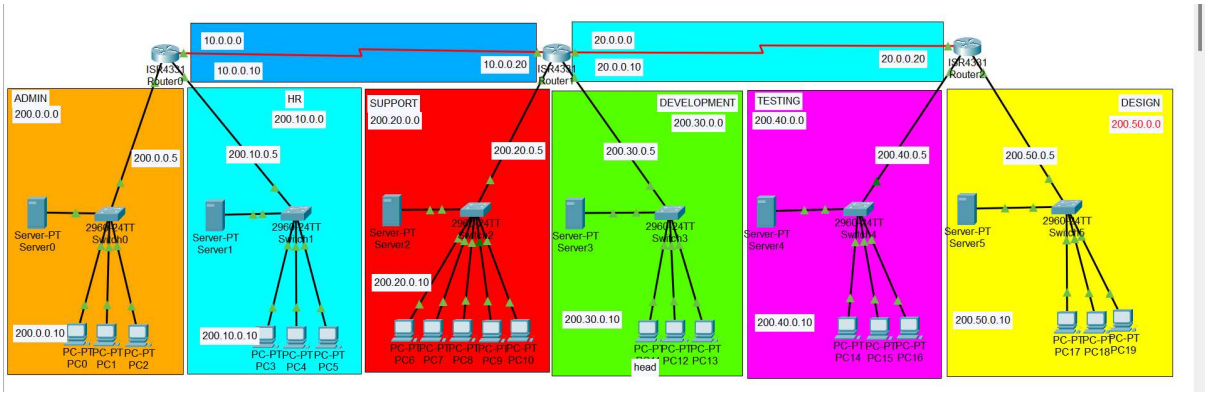
HR DEPARTMENT – 200.10.0.0

SUPPORT DEPARTMENT - 200.20.0.0

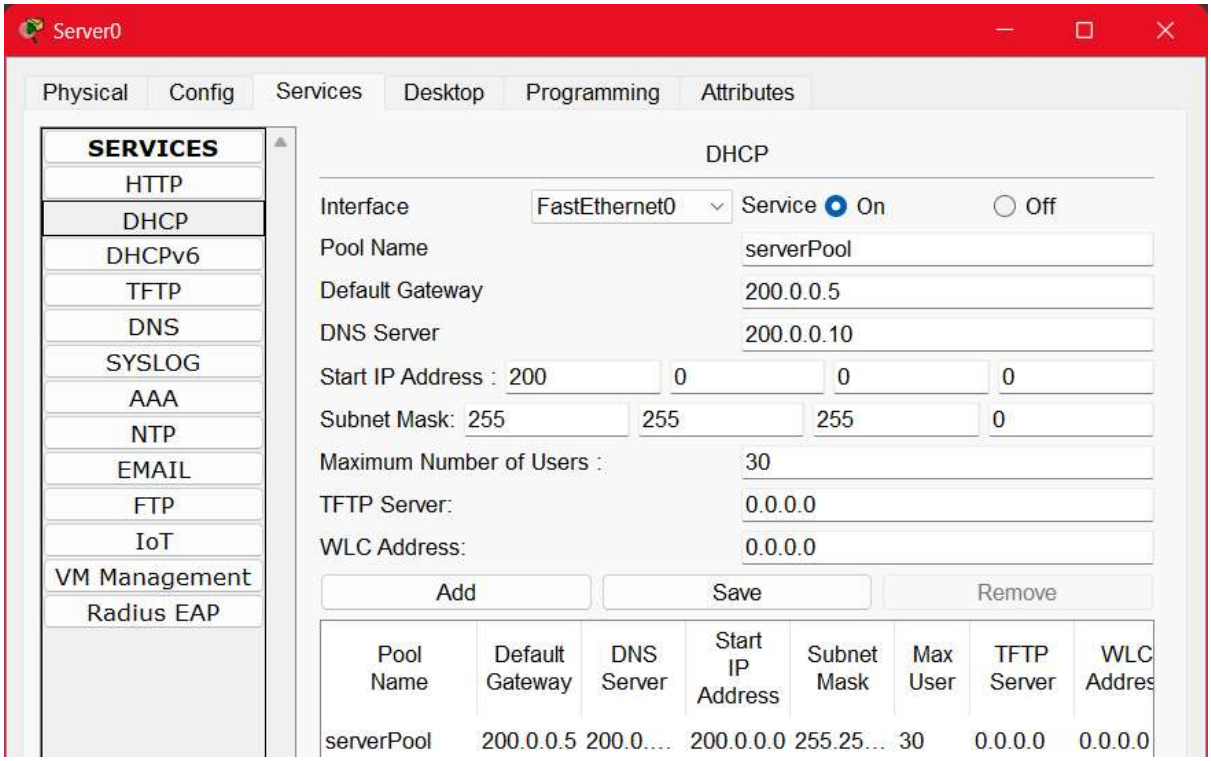
DEVLOPMENMT DEPARTMENT - 200.30.0.0

TESTING DEPARTMENT – 200.40.0.0

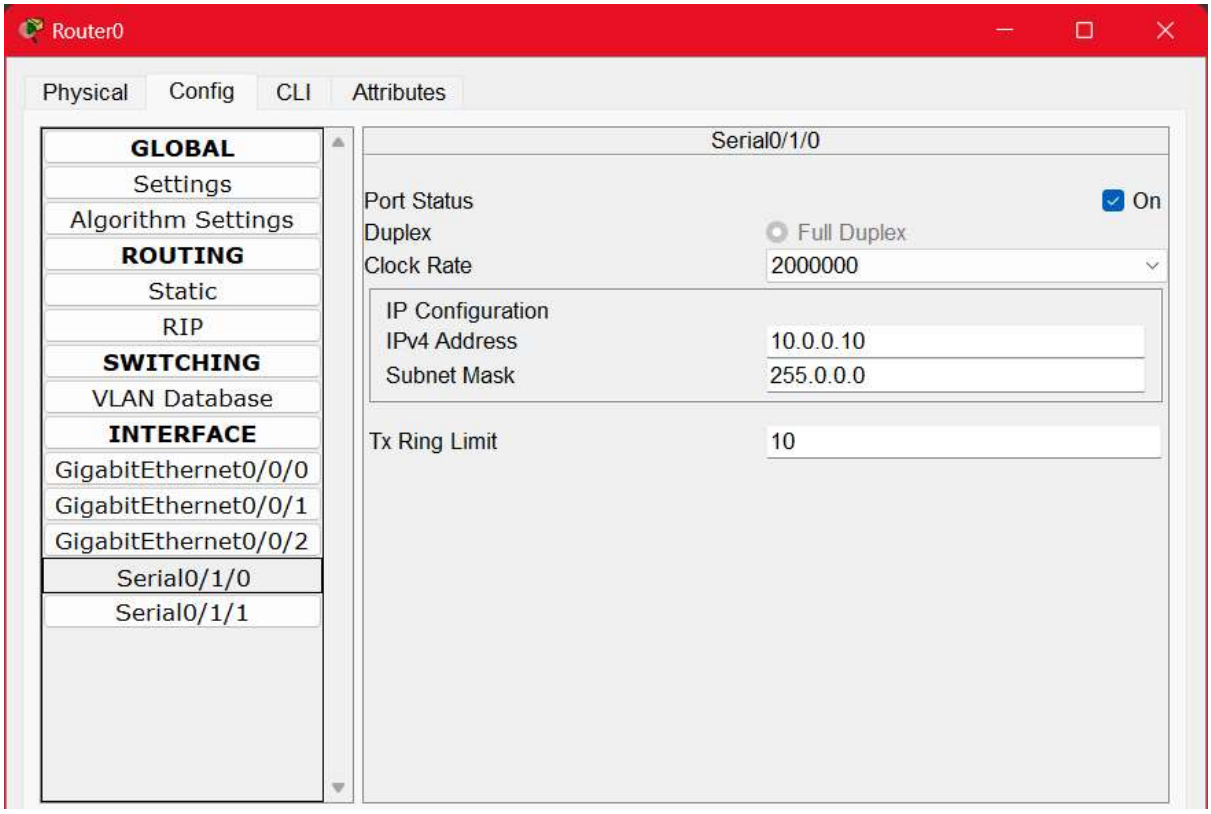
DESIGN DEPARTMENT – 200.50.0.0

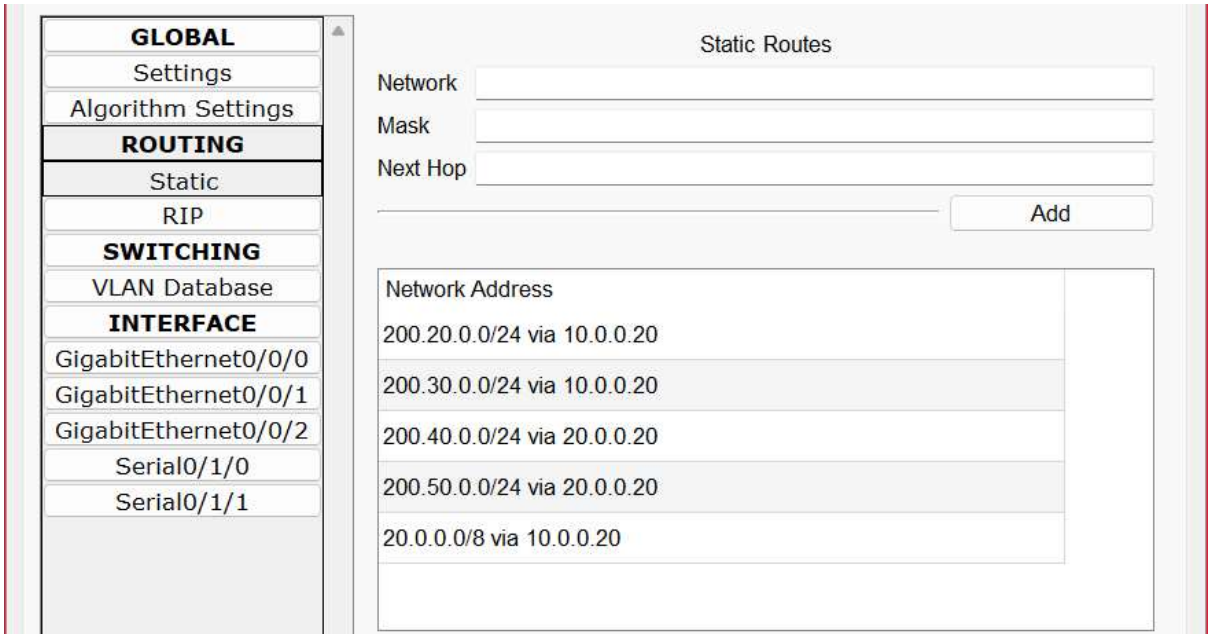


2. Configure DHCP in each server and assign IP to PCs of each network/department:



3. Configure each route and its routings :





4. Set up ACL for each router as per the given scenario's conditions:

Restrict the Testing Department from communicating with Support & Design Department.

Only permit the head of the Development Department to communicate with the Support Department.

Only permit 2 out of 5 members of the Support Department to communicate with the Design Department.

Router1 Config :

```
deny 200.40.0.0 0.0.0.255   # deny Testing Department permit
host 200.30.0.3             # allow Developer Head deny
200.30.0.0 0.0.0.255        # deny rest of Developer user permit
any                         # allow rest
```

```
Router(config)#ip acce
Router(config)#ip access-list ?
  extended  Extended Access List
  standard  Standard Access List
Router(config)#ip access-list sta
Router(config)#ip access-list standard 7
Router(config-std-nacl)#?
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
Router(config-std-nacl)#deny 200.40.0.0 0.0.0.255
Router(config-std-nacl)#permit host 200.30.0.3
Router(config-std-nacl)#deny 200.30.0.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#in
Router(config)#interface gig 0/0/0
Router(config-if)#ip acc
Router(config-if)#ip access-group 7 out
Router(config-if)#
```

Router2 config :

deny 200.40.0.0 0.0.0.255 # deny Testing Department

permit host 200.20.0.3 # allow user1 of Support Department

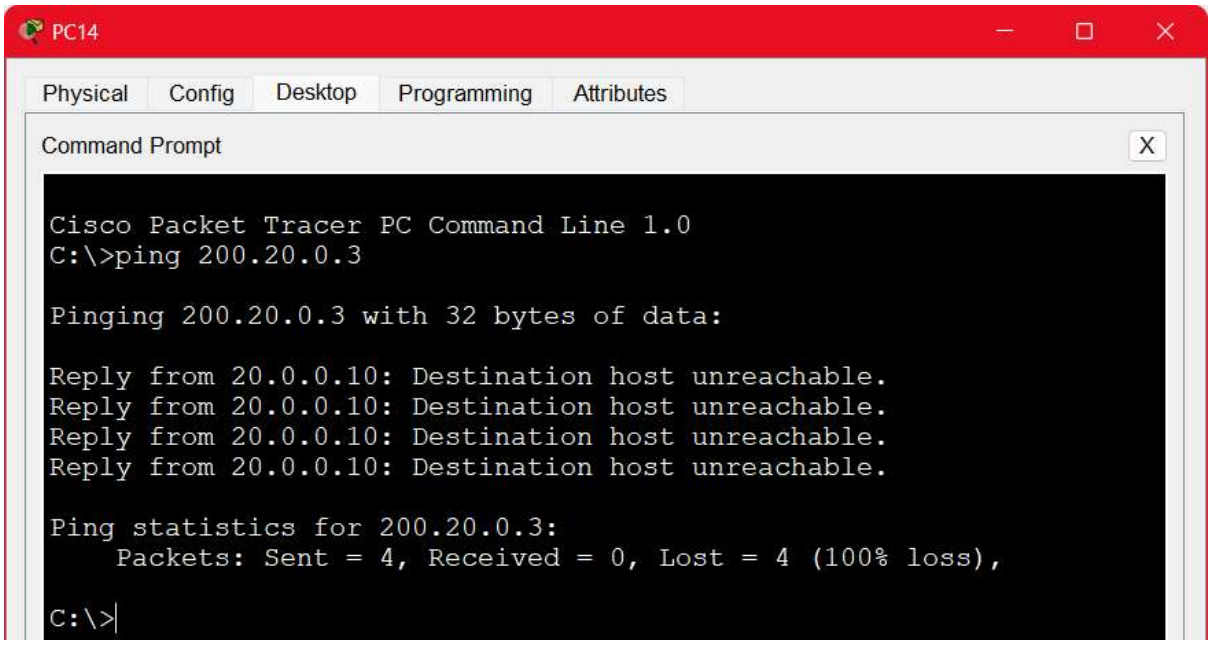
permit host 200.20.0.4 # allow user2 of Support Department

deny 200.20.0.0 0.0.0.255 # deny rest of Support Department

permit any # allow rest

```
Router(config)#ip access-
Router(config)#ip access-list stanb=
Router(config)#ip access-list stan
Router(config)#ip access-list standard 7
Router(config-std-nacl)#deny 200.40.0.0 0.0.0.255
Router(config-std-nacl)#permit host 200.20.0.3
Router(config-std-nacl)#permit host 200.20.0.4
Router(config-std-nacl)#deny 200.20.0.0 0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#interface
Router(config)#interface gig
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip ac
Router(config-if)#ip access-group 7 out
Router(config-if)#
```

➡ Lastly , Let's check [Sending packet from Testing to Support]:



» **Conclusion :** Thus , hereby performing this practical we understood how to implement an Access Control List in a network of an Organization.