

INSTITUTE OF COMPUTER TECHNOLOGY
B. TECH COMPUTER SCIENCE AND ENGINEERING

Subject: Computer Networks[CN]

Name : Archita Gahoi

Enrollment_No. : 23162171002

SEM : 5

Class : A

Batch : 52 (CS)

Practical 4

Aim: To implement access control list (ACL) in network of an organization containing different departments.

Scenario:

There is an organization of the University having 3 different departments University, ICT and DCS. IPv4 addressing scheme is used for assigning the IP address to the device as shown in Table1. Each department has multiple employees, which have specific rights to communicate within the network.

The details of the rights are as mentioned below:

Access Rights:

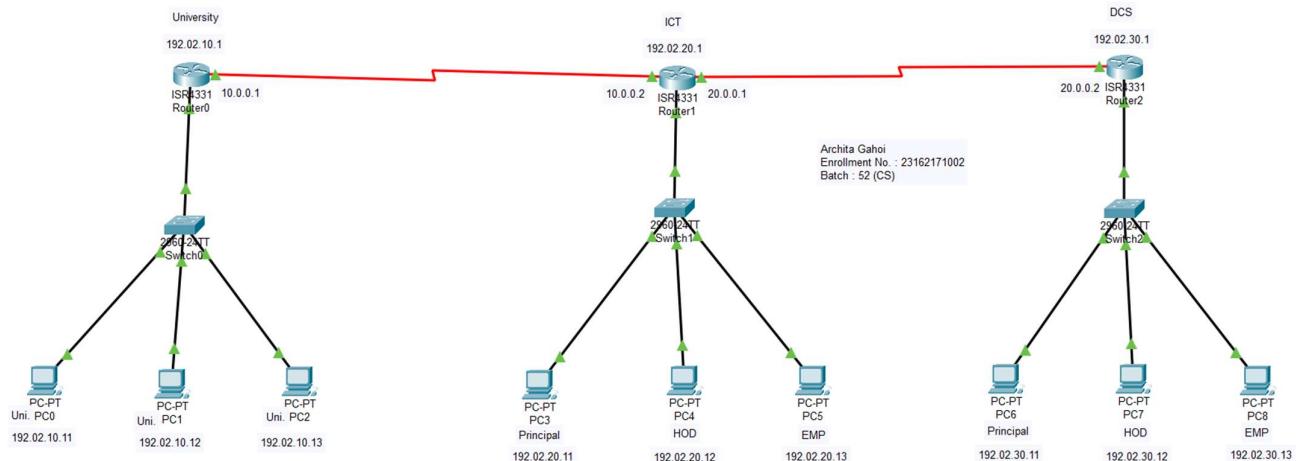
- University can contact all employees.
- Only Principal can contact University office.
- All Principals should contact each other
- All head of departments can contact each other

Configure Access Control List (ACL) at each router according to the specified access rights.

Procedure:

- 1) Create network as given below
- 2) Configure IP address (All Devices, Routers)
- 3) Configure dynamic routing table (RIP in routers)
- 4) Configure ACL on Router0
- 5) Configure ACL on Router1
- 6) Configure ACL on Router2

⇒ Main Circuit

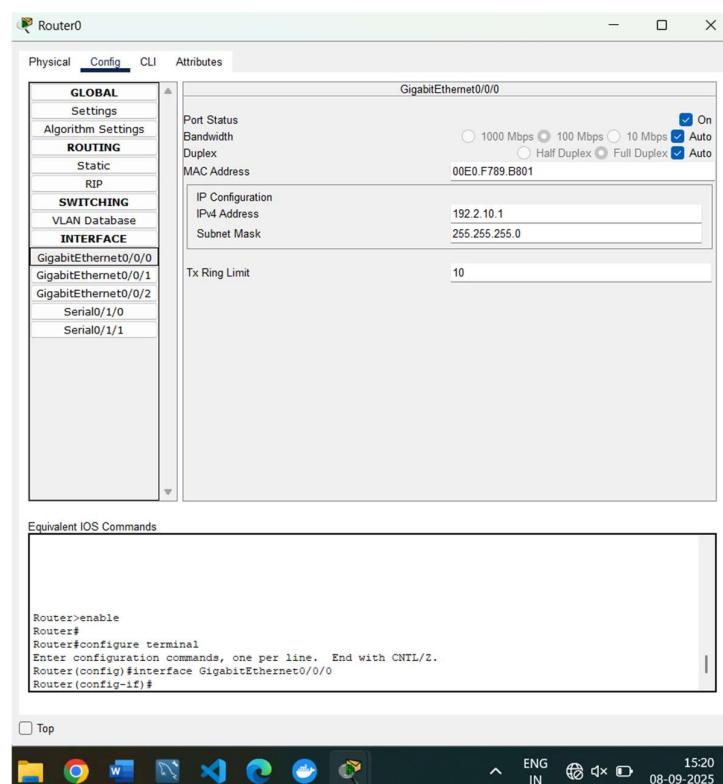
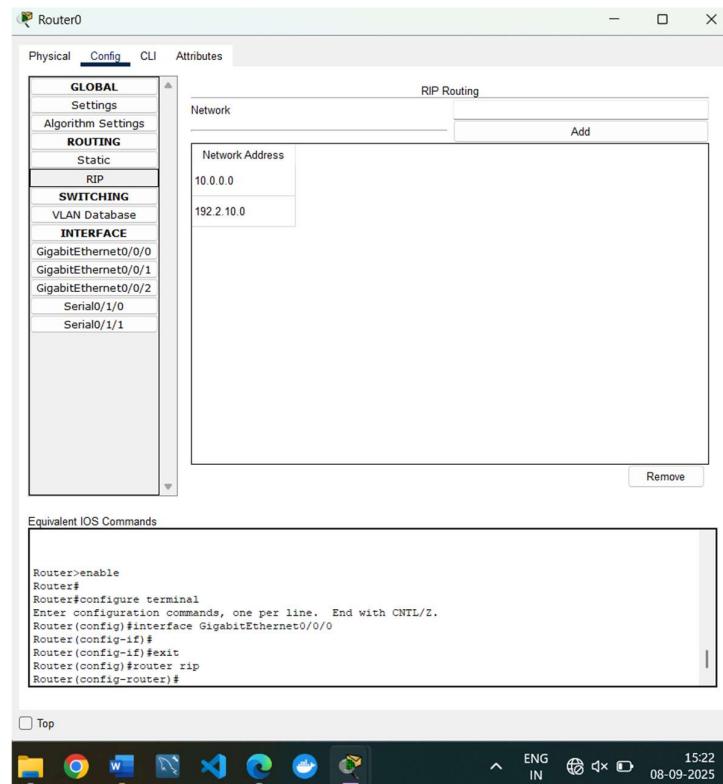


Configurations:

IP Address:

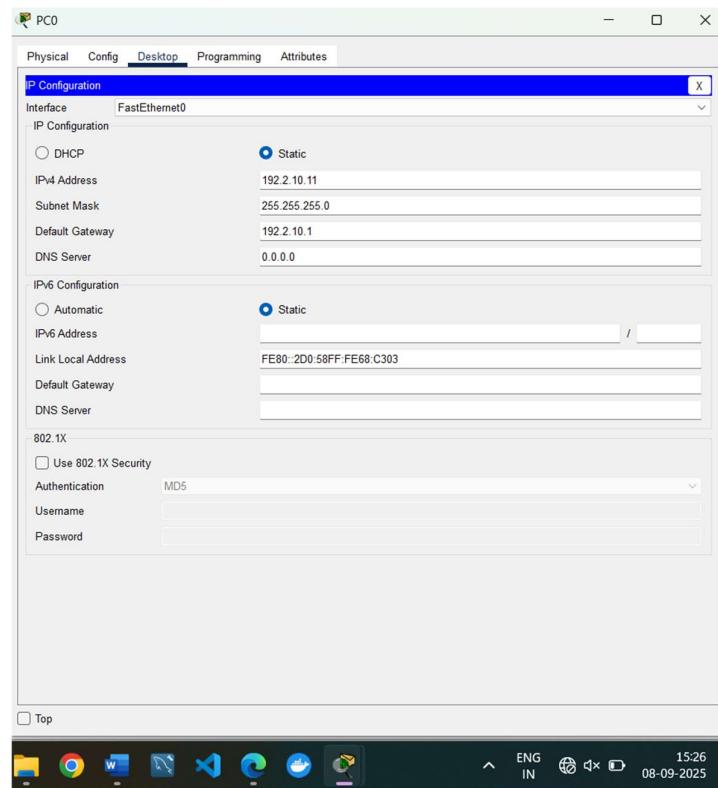
⇒ Routers

Router 0

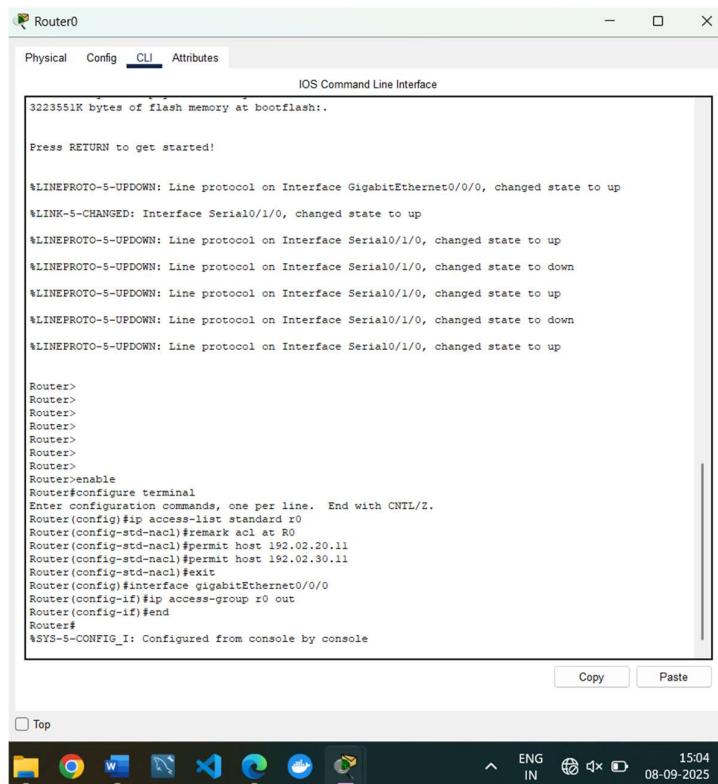


⇒ PCS

PC0



⇒ ACL on Router0



⇒ ACL on Router1

Router1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router con0 is now available

Press RETURN to get started.

Router>
Router>enable
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended rl
Router(config-ext-nacl)#exit
Router(config)#ip access-list extended rl
Router(config)#ip access-list extended rl
Router(config)#ip access-list extended rl
Router(config-ext-nacl)#permit ip 192.02.20.0 0.0.0.255 any
Router(config-ext-nacl)#permit ip host 192.02.30.11 host 192.02.20.11
Router(config-ext-nacl)#permit ip host 192.02.30.12 host 192.02.20.12
Router(config-ext-nacl)#exit
Router(config)#interface gigabitEthernet0/0/0
Router(config-if)#ip access-group rl out
Router(config-if)#end
Router#
SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

Top

16:12 08-09-2025

⇒ ACL on Router2

Router2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
3223551K bytes of flash memory at bootflash:.

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

Router>
Router>
Router>
Router>
Router>
Router>
Router>
Router>enable
Router>configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended r2
Router(config-ext-nacl)#permit ip 192.02.10.0 0.0.0.255 any
Router(config-ext-nacl)#permit ip host 192.02.20.11 host 192.02.30.11
Router(config-ext-nacl)#permit ip host 192.02.20.12 host 192.02.30.12
Router(config-ext-nacl)#exit
Router(config)#interface gigabitEthernet0/0
Router(config-if)#ip access-group r2 out
Router(config-if)#end
Router#
SYS-5-CONFIG_I: Configured from console by console
```

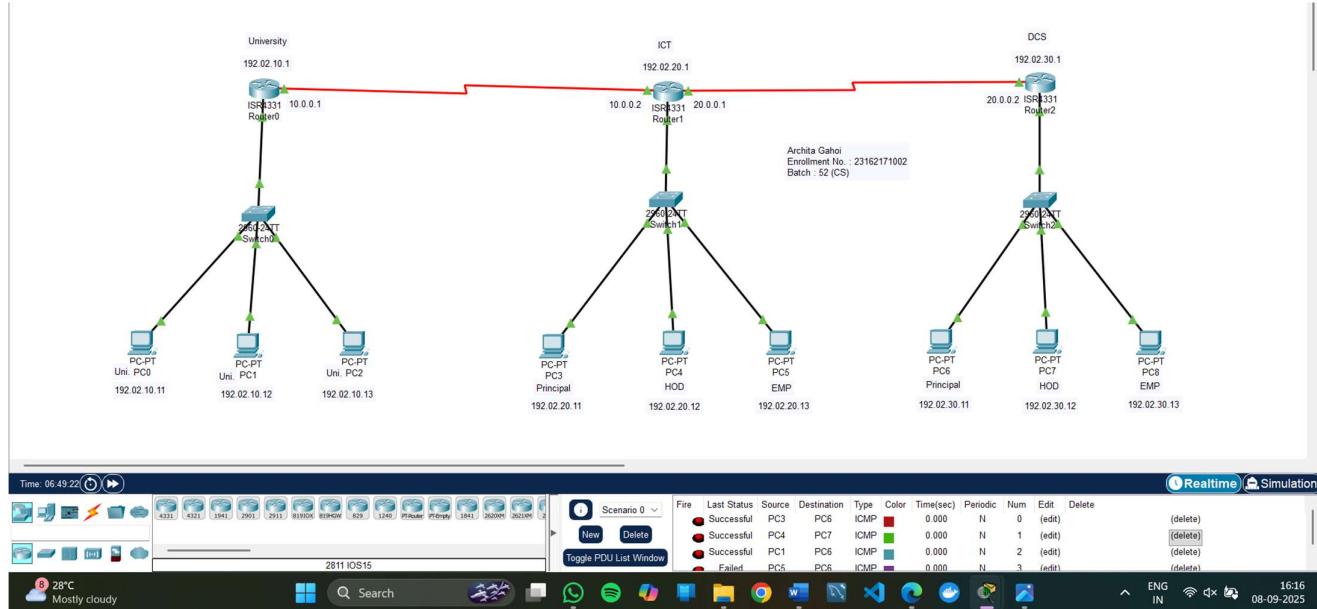
Copy Paste

Top

15:14 08-09-2025

PCs packet transfer

- : from principal to principal
- : from HOD to HOD
- : from Uni to principal
- : from EMP to principal



Conclusion:

In this practical, ACLs were successfully implemented on the routers to control communication between University, ICT, and DCS departments as per the given access rights. This ensured secure and authorized communication within the organization's network while restricting unauthorized access.