INSTITUTE OF COMPUTER TECHNOLOGY

B-TECH COMPUTER SCIENCE ENGINEERING 2025-26

SUBJECT:COMPUTER NETWORKS

NAME: Rahul Prajapati

ENRLL. NO: 23162171020

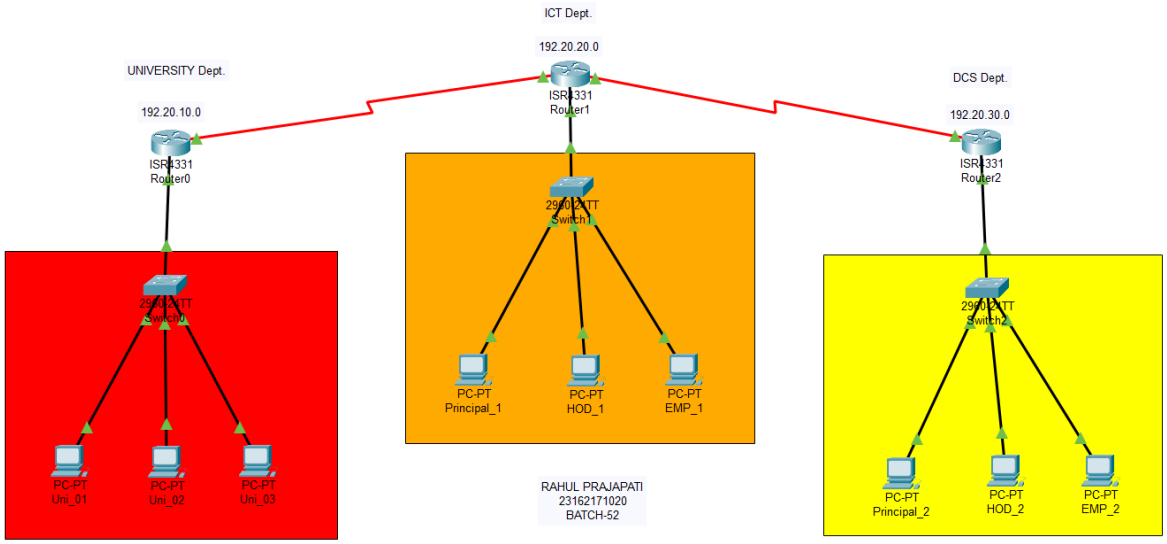
BRANCH: CYBER SECURITY

BATCH: 52

PRACTICAL_04

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

Network Design:



NETWORK'S PCs IP Configuration

DEPARTMENT	DEVICE	IP ADDRESS	SUBNET MASK	DEFAULT GATEWA
UNIVERSITY	UNI_01	192.20.10.11	255.255.255.0	192.20.10.1
	UNI_02	192.20.10.12	255.255.255.0	
	UNI_03	192.20.10.13	255.255.255.0	
ICT	PRINCIPAL_1	192.20.20.11	255.255.255.0	192.20.20.1
	HOD_1	192.20.20.12	255.255.255.0	
	EMP_1	192.20.20.13	255.255.255.0	
DCS	PRINCIPAL_2	192.20.30.11	255.255.255.0	192.20.30.1
	HOD_2	192.20.30.12	255.255.255.0	
	EMP_2	192.20.30.13	255.255.255.0	

NETWORK'S ROUTERs IP Configuration

DEVICE	ROUTER_0	ROUTER_1	ROUTER_2
IP ADDRESS	192.20.10.0	192.20.20.0	192.20.30.0
SUBNET MASK	255.255.255.0	255.255.255.0	255.255.255.0
DEFAULT GATEWAY	192.20.10.1	192.20.20.1	192.20.30.1
RIP	10.0.0.0	10.0.0.0	10.0.0.0
	20.0.0.0	20.0.0.0	20.0.0.0
	192.20.10.0	192.20.20.0	192.20.30.0

Router0 (university dept) ACL configuration:

```
Router>enable
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-li
Router(config)#ip access-list standard R0
Router(config-std-nacl)#remark ACL on Router0
Router(config-std-nacl)#permit host 192.20.20.11
Router(config-std-nacl)#permit host 192.20.30.11
Router(config-std-nacl)#interface g0/0/0
Router(config-if)#ip access-group R0 out
Router(config-if)#do write
Building configuration...
[OK]
```

```
ip access-list standard R0
 remark ACL on Router0
 permit host 192.20.20.11
 permit host 192.20.30.11
```

Router1 (ICT dept) ACL configuration:

```
Router#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended R1
Router(config-ext-nacl)#remark ACL on Router1
Router(config-ext-nacl)#permit ip 192.20.10.0 0.0.0.255 any
Router(config-ext-nacl)#permit ip host 192.20.30.13 host 192.20.20.13
Router(config-ext-nacl)#permit ip host 192.20.30.11 host 192.20.20.11
Router(config-ext-nacl)#permit ip host 192.20.30.12 host 192.20.20.12
Router(config-ext-nacl)#interface g0/0/0
Router(config-if)#ip access-group g0/0/0
% Incomplete command.
Router(config-if)#ip access-group R1 out
Router(config-if)#do write
Building configuration...
[OK]
```

```
ip access-list extended R1
 permit ip 192.20.10.0 0.0.0.255 any
 permit ip host 192.20.30.11 host 192.20.20.11
 permit ip host 192.20.30.12 host 192.20.20.12
 permit ip 192.20.30.0 0.0.0.255 host 192.20.20.13
 remark ACL on Router1
 permit ip host 192.20.30.13 host 192.20.20.13
```

Router2 (DCS dept) ACL configuration:

```
Router>enable
Router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip access-list extended R2
Router(config-ext-nacl)#remark ACL on Router2
Router(config-ext-nacl)#permit ip 192.20.10.0 0.0.0.255 any
Router(config-ext-nacl)#permit ip host 192.20.20.11 host 192.20.30.11
Router(config-ext-nacl)#permit ip host 192.20.20.12 host 192.20.30.12
Router(config-ext-nacl)#permit ip host 192.20.20.13 host 192.20.30.13
Router(config-ext-nacl)#interface g0/0/0
Router(config-if)#ip access-group R2 out
Router(config-if)#do write
Building configuration...
[OK]
Router(config-if)#do show run
```

```
ip access-list extended R2
 remark ACL on Router2
 permit ip 192.20.10.0 0.0.0.255 any
 permit ip host 192.20.30.11 host 192.20.20.11
 permit ip 192.20.20.0 0.0.0.255 host 192.20.30.13
 permit ip 192.20.30.0 0.0.0.255 host 192.20.30.13
 permit ip host 192.20.20.12 host 192.20.30.12
 permit ip host 192.20.20.11 host 192.20.30.11
 permit ip host 192.20.20.13 host 192.20.30.13
```

Communication between different Department

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	D
	Successful	Uni_01	Principal_1	ICMP		0.000	N	0	(edit)	
	Successful	Uni_02	Principal_2	ICMP		0.000	N	1	(edit)	
	Failed	Uni_03	HOD_1	ICMP		0.000	N	2	(edit)	
	Failed	Uni_03	HOD_2	ICMP		0.000	N	3	(edit)	
	Successful	Principal_1	Uni_02	ICMP		0.000	N	4	(edit)	
	Successful	Principal_2	Uni_01	ICMP		0.000	N	5	(edit)	
	Successful	Principal_1	Principal_2	ICMP		0.000	N	6	(edit)	
	Successful	Principal_2	Principal_1	ICMP		0.000	N	7	(edit)	
	Successful	HOD_1	Principal_1	ICMP		0.000	N	8	(edit)	
	Failed	HOD_2	Principal_1	ICMP		0.000	N	9	(edit)	
	Successful	HOD_1	HOD_2	ICMP		0.000	N	10	(edit)	
	Failed	HOD_1	EMP_2	ICMP		0.000	N	11	(edit)	

Conclusion:- In this practical, access control lists (ACLs) are used to manage and restrict communication between different departments based on their roles. It ensures that only authorized users, like principals and department heads, can communicate as needed while keeping the network secure and organized. This helps in controlling access and protecting sensitive information.