DIVINE WORD COLLEGE OF CALAPAN

SCHOOL OF INFORMATION AND TECHNOLOGY

DATA COMMUNICATION AND NETWORKING 2

EXERCISE 12

NAME ____________________________ **SCORE** __________ **RATING** __________%
ID# _____________________________ **COURSE**___________________________

ADVANCED ACCESS CONTROL LIST CONFIGURATION

OBJECTIVE

This exercise challenges students to design, configure, and troubleshoot **multiple Access Control Lists (ACLs)**—both **standard** and **extended**—to enforce network segmentation, service-level restrictions, and security policies. By the end of this activity, students should demonstrate mastery of ACL logic, wildcard masks, interface direction, and correct placement.

NETWORK TOPOLOGY

- **Routers:** R1, R2, R3
- **Switches:** SW1, SW2
- **End Devices:** PC1, PC2, PC3, PC4

Connections:

- R1 ↔ SW1 ↔ PC1, PC2
- R1 ↔ R2
- R2 ↔ R3
- R3 ↔ SW2 ↔ PC3, PC4

NETWORK DETAILS

Device	Network / Interface	Subnet	Remarks
PC1	172.16.10.5	/27	Connected to SW1
PC2	172.16.10.10	/27	Connected to SW1
PC3	192.168.20.5	/28	Connected to SW2
PC4	192.168.20.10	/28	Connected to SW2
R1–R2 link	10.0.10.0/30		Serial link
R2–R3 link	10.0.20.0/30		Serial link
Loopback Interfaces	Assigned by student		For verification

All devices must initially be fully reachable (basic connectivity verified) ***before applying ACLs****.*

TASK REQUIREMENTS

Task 1: Standard ACL on R1 (Basic Filtering)

- Deny **PC1 (172.16.10.5/27)** from accessing any **network behind R3 (192.168.20.0/28)**.
- Allow all other traffic.
- Apply the ACL in the **outbound direction** on the correct interface.

Sample Pattern:

```
R1(config)# access-list 15 deny host 172.16.10.5
R1(config)# access-list 15 permit any
R1(config)# interface g0/1
R1(config-if)# ip access-group 15 out
```

Task 2: Extended ACL on R2 (Multiple Protocol Control)

Implement the following rules in **one extended ACL (No. 120):**

Source	Destination	Service	Action
172.16.10.10/27	192.168.20.10/28	Telnet (port 23)	Deny
172.16.10.0/27	192.168.20.5/28	FTP (port 21)	Deny
172.16.10.0/27	any	HTTP (port 80)	Permit
any	any	All other traffic	Deny

Apply the ACL on R2 in the correct direction where traffic passes **from R1 to R3**.

Sample Pattern:

```
R2(config)# access-list 120 deny tcp 172.16.10.10 0.0.0.31 host 192.168.20.10 eq 23
R2(config)# access-list 120 deny tcp 172.16.10.0 0.0.0.31 host 192.168.20.5 eq 21
R2(config)# access-list 120 permit tcp 172.16.10.0 0.0.0.31 any eq 80
R2(config)# access-list 120 deny ip any any
R2(config)# interface g0/1
R2(config-if)# ip access-group 120 in
```

Task 3: Extended ACL on R3 (ICMP and Mixed Conditions)

- Deny **ICMP (ping)** packets from **PC2 (172.16.10.10)** to any host on **192.168.20.0/28**.
- Deny **any SSH (port 22)** attempt from **192.168.20.0/28** to **R2’s 10.0.20.1**.
- Permit all other traffic.

Sample Pattern:

```
R3(config)# access-list 130 deny icmp host 172.16.10.10 192.168.20.0 0.0.0.15
R3(config)# access-list 130 deny tcp 192.168.20.0 0.0.0.15 host 10.0.20.1 eq 22
R3(config)# access-list 130 permit ip any any
R3(config)# interface g0/0
R3(config-if)# ip access-group 130 in
```

Task 4: Mixed Verification

1. Ping Testing:
   a. Verify which PCs can or cannot ping each other.
2. Telnet and FTP Testing:
   a. Attempt sessions between PC1–PC3, PC2–PC4.
3. HTTP Testing:
   a. Use a browser from PC1 or PC2 to reach PC3 or PC4.
4. SSH Testing:
   a. Attempt SSH connections to confirm they are properly denied.

Documentation

1. Screenshot of the **final routing table** of each router.
2. Full ACL configurations used.
3. Summary table of test results (Allowed / Denied).