DIVINE WORD COLLEGE OF CALAPAN

SCHOOL OF INFORMATION AND TECHNOLOGY

DATA COMMUNICATION AND NETWORKING 2

EXERCISE 13

NAME ____________________________ **SCORE** _________ **RATING** _________%
ID# ____________________________ **COURSE**__________________________

COMPLEX LAYERED ACL CONFIGURATION

OBJECTIVE

This laboratory activity requires students to design, configure, and validate **multi-layer Access Control Lists (ACLs)** applied across several interfaces and networks. Students must implement combined **standard**, **extended**, and **named ACLs**, apply them strategically (inbound/outbound), and test network behavior using different services (HTTP, SSH, ICMP, DNS, and FTP). The exercise emphasizes the use of **hierarchical ACL logic**, **network management restriction**, and **inter-VLAN traffic control**.

NETWORK TOPOLOGY

- **Routers:** R1, R2, R3
- **Switches:** SW1, SW2 (Layer 3 capable)
- **End Devices:** PC1, PC2, PC3, PC4, Server1

Connections:

- R1 ↔ SW1 ↔ VLAN 10 (PC1, PC2)
- R2 ↔ SW2 ↔ VLAN 20 (PC3, PC4)
- R3 ↔ Server1 (central services)
- R1 ↔ R2 ↔ R3 (serial links)

NETWORK DETAILS

Device	Network / Interface	Subnet	Remarks
VLAN 10 (PC1, PC2)	172.30.10.0	/26	User Network A
VLAN 20 (PC3, PC4)	172.30.20.0	/26	User Network B
Server1	192.168.100.10	/28	Web/FTP/DNS Server
R1–R2 link	10.1.1.0	/30	Serial Link
R2–R3 link	10.1.2.0	/30	Serial Link
Loopback Interfaces	Configured by student	—	Testing only

*Verify **full connectivity** before applying ACLs.*

TASK REQUIREMENTS

Task 1: Standard ACL on R1 (VLAN Access Restriction)

- Deny all hosts in **VLAN 10 (172.30.10.0/26)** from accessing **VLAN 20 (172.30.20.0/26)**.
- Permit all other traffic.
- Apply in the **outbound** direction on the correct interface toward R2.

Sample Pattern:

```
R1(config)# access-list 25 deny 172.30.10.0 0.0.0.63 172.30.20.0 0.0.0.63
R1(config)# access-list 25 permit any
R1(config)# interface g0/1
R1(config-if)# ip access-group 25 out
```

Task 2: Extended ACL on R2 (Service-Level Control)

Implement the following rules in one **extended ACL (No. 140):**

Source	**Destination**	**Service**	**Action**
172.30.10.0/26	192.168.100.10	HTTP (80)	Permit
172.30.20.0/26	192.168.100.10	FTP (21)	Permit
172.30.20.0/26	192.168.100.10	SSH (22)	Deny
any	any	ICMP	Deny
any	any	All other traffic	Permit

*Apply in the **inbound** direction on the interface facing R1.*

Sample Pattern:

```
R2(config)# access-list 140 permit tcp 172.30.10.0 0.0.0.63 host 192.168.100.10 eq 80
R2(config)# access-list 140 permit tcp 172.30.20.0 0.0.0.63 host 192.168.100.10 eq 21
R2(config)# access-list 140 deny tcp 172.30.20.0 0.0.0.63 host 192.168.100.10 eq 22
R2(config)# access-list 140 deny icmp any any
R2(config)# access-list 140 permit ip any any
R2(config)# interface g0/0
R2(config-if)# ip access-group 140 in
```

TASK 3: Named ACL on R3 (Management Security)

Create a **named extended ACL** called MGMT-ACCESS that enforces the following:

- Permit only **PC1 (172.30.10.5)** and **PC3 (172.30.20.5)** to access R3 via **SSH (port 22)**.
- Deny all other SSH attempts.
- Permit all other IP traffic for normal routing operations.
- Apply inbound on the management interface of R3.

Sample Pattern:

```
R3(config)# ip access-list extended MGMT-ACCESS
R3(config-ext-nacl)# permit tcp host 172.30.10.5 any eq 22
R3(config-ext-nacl)# permit tcp host 172.30.20.5 any eq 22
R3(config-ext-nacl)# deny tcp any any eq 22
R3(config-ext-nacl)# permit ip any any
R3(config)# interface g0/0
R3(config-if)# ip access-group MGMT-ACCESS in
```

TASK 4: DNS and Ping Testing

- Ensure Server1 acts as a **DNS and Web server**.
- PC1 and PC3 should successfully resolve and reach Server1’s web service (HTTP).
- All ICMP (ping) requests should be **denied** based on ACL rules.
- Record results with screenshots.

Documentation:

1. Screenshot of **show running-config** for each router.
2. Screenshot of **successful/failed pings, Telnet/SSH attempts, and HTTP/FTP tests**.
3. Table summarizing **which protocols are permitted or denied** per VLAN.