Experiment-3

Aim → Creating and implementing a user access list for permit and deny the remote hosts.

Objective 1 → An overview on standard and extended access list.

Access Control Lists (ACLs) are used in networking to control packet flow based on defined rules. They help in filtering traffic for security, performance and access management.

1) Standard ACLs → It filters traffic based only on IP address. They do not differentiate between protocols or destination addresses.

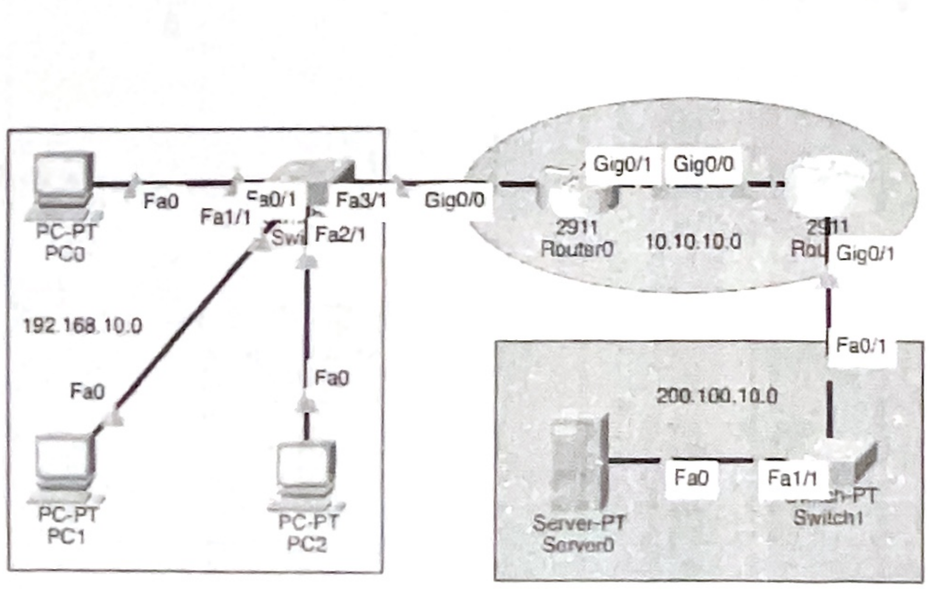
Features → i) Uses ACL numbers 1-99 and 1300-1999 (expanded range).
ii) Can permit or deny entire traffic from a source IP.
iii) Should be placed as close to the destination as possible to avoid unnecessary filtering.

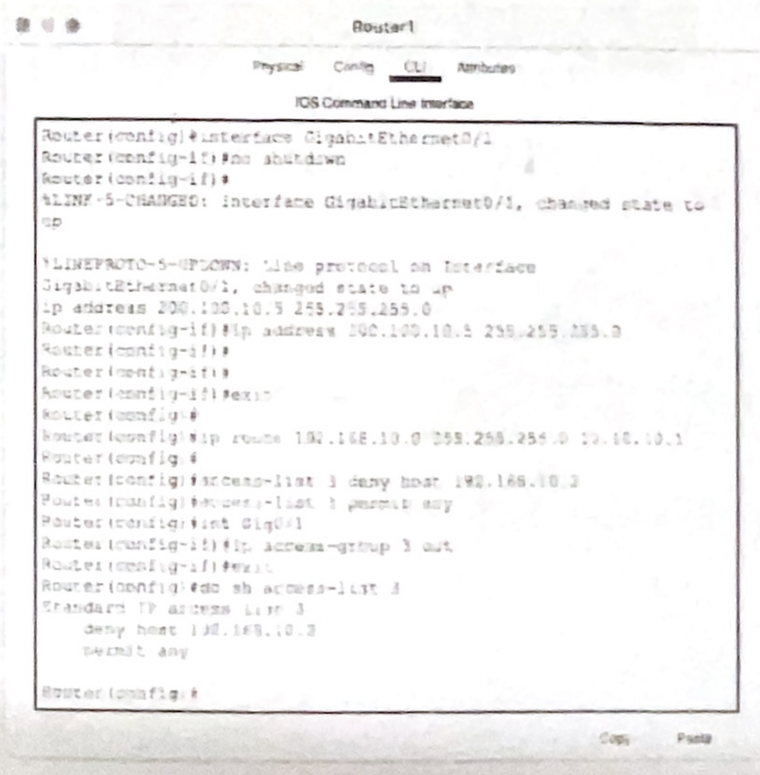
2) Extended ACLs → It filter traffic based on source IP, destination IP, protocol (TCP, UDP, ICMP) and port numbers.

Features → i) Uses ACL number 100-199 and 2000-2699 (~~expanded~~ expanded range)
ii) More granular control over traffic filtering.
iii) Should be placed as ~~above~~ close to the source as possible to prevent unnecessary traffic flow.

Objective 2 → Configuration and verification of a standard access list for permit and deny to a remote server.

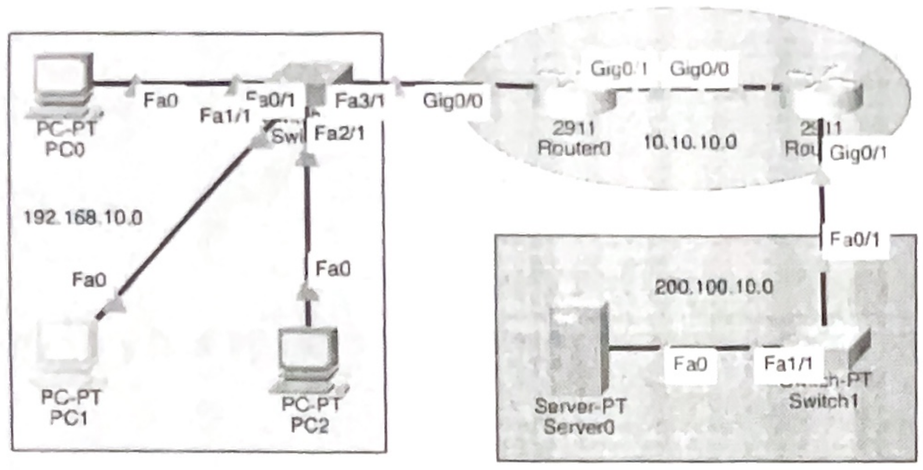
Configuring router 1 to deny PC1 for access and permitting all other.

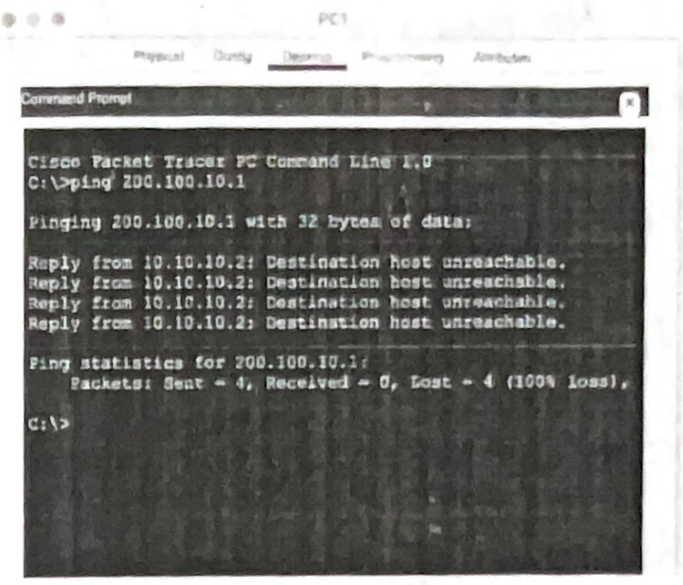




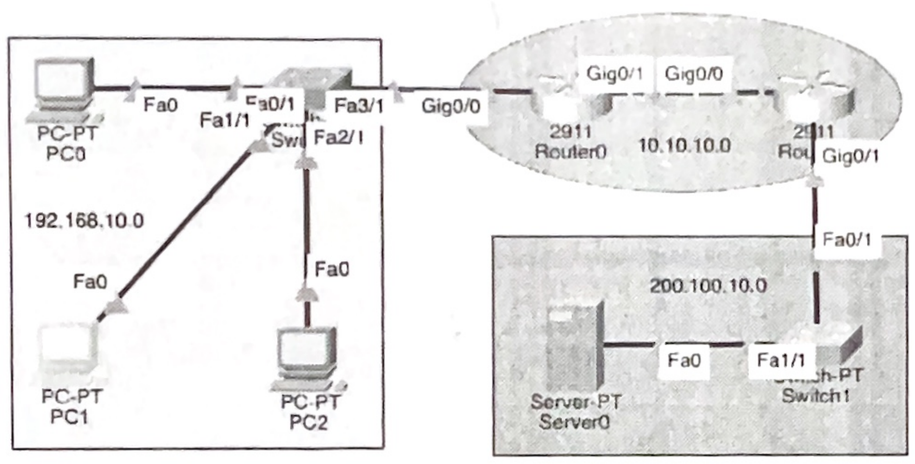
Name: _____ Regd No: _____

As we can see, PC1 cannot access Server.



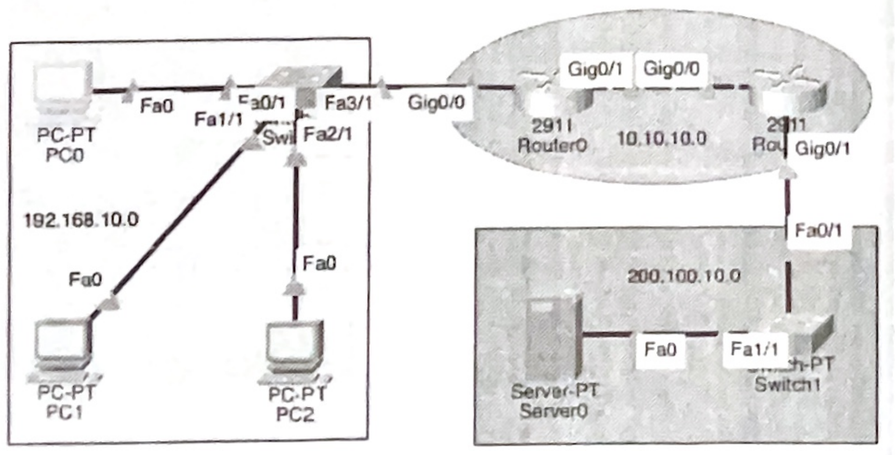


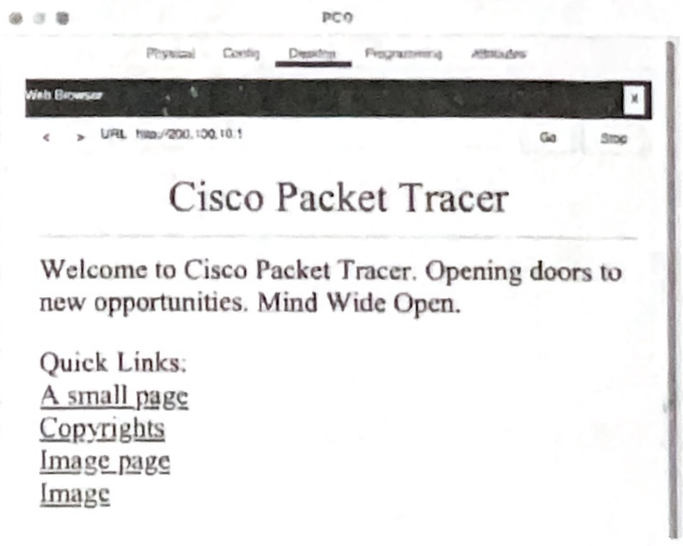
But PC0 remains the same and still access the server.



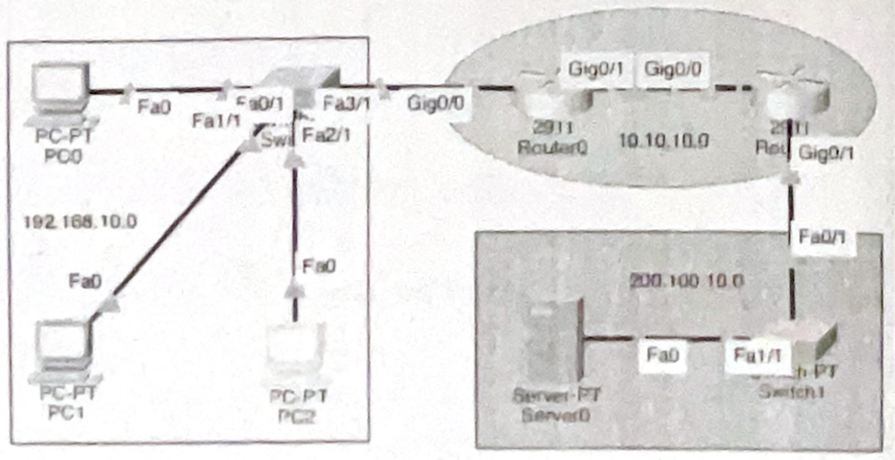
Objective 3 → Configuration and verification of an extended access list for permit and deny to a remote servers (HTTP/FTP).

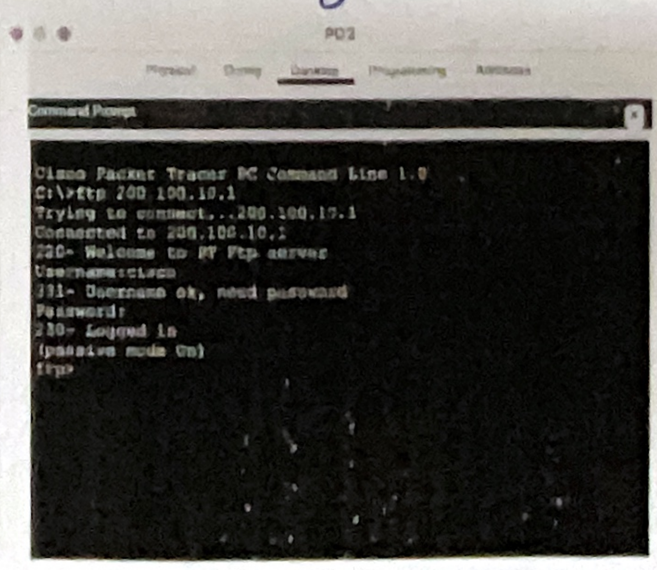
Before configuration PC0 can access Server0 through HTTP.





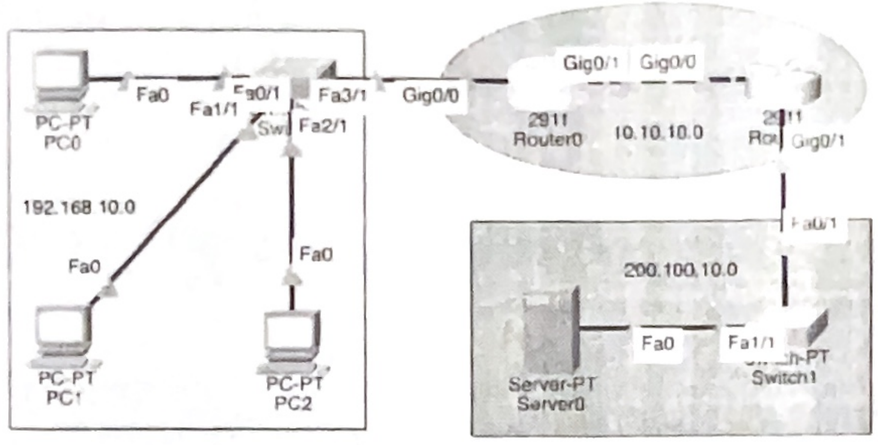
PC2 as well can access Server0 through FTP.

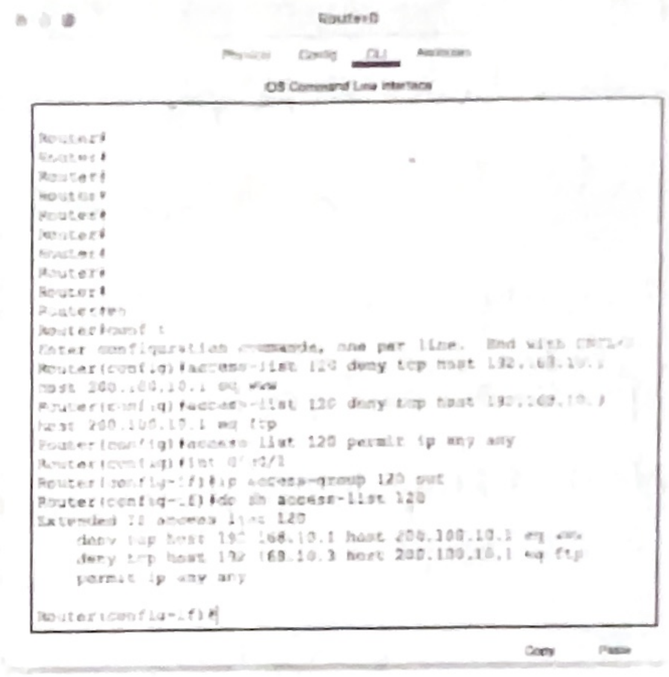




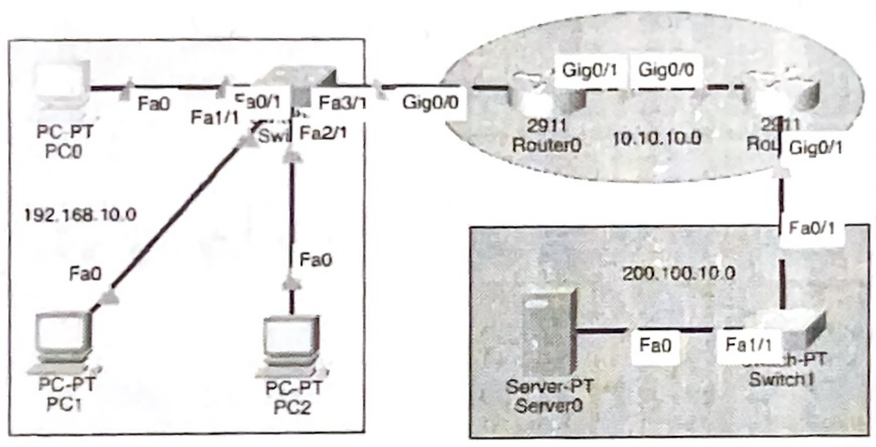
Name: _____ Regd No: _____

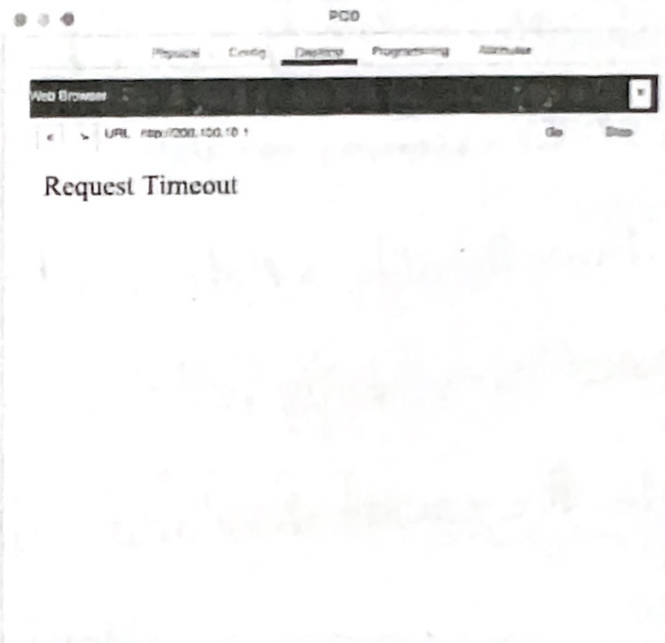
Configuring Router 0 to deny HTTP and FTP for PC0 and PC2 respectively, and permitting remaining.



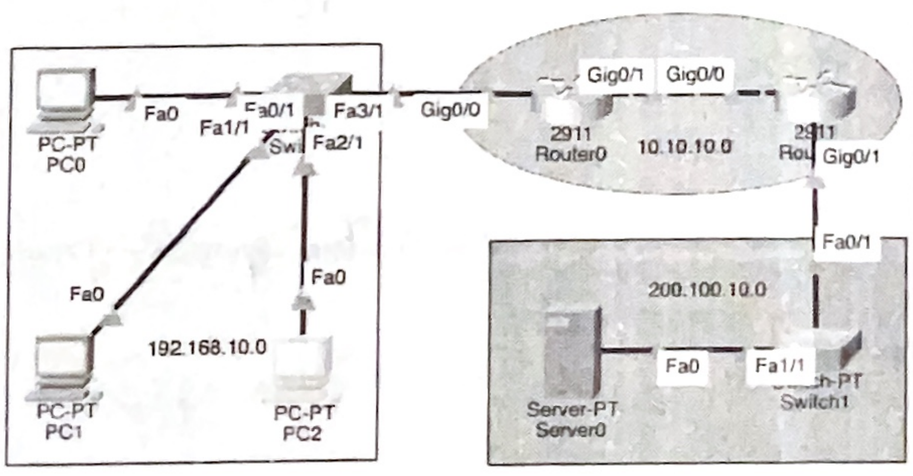


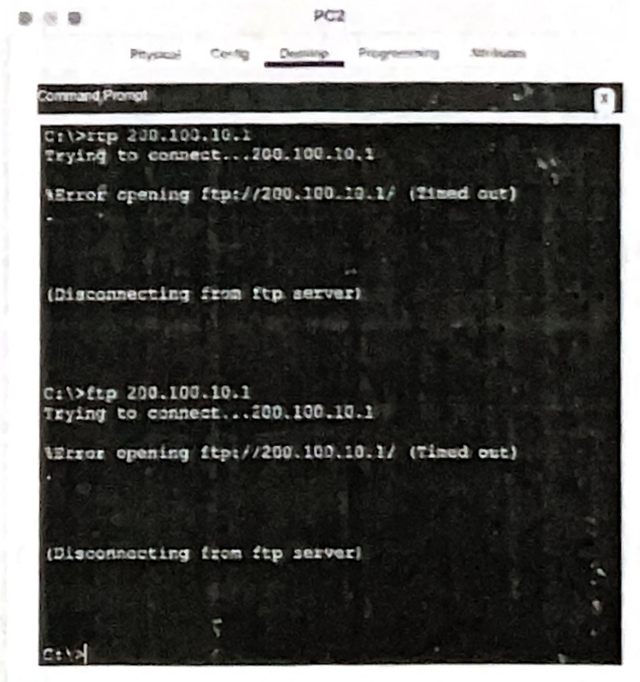
Now, PC0 cannot access Server0 through HTTP.





PC2 as well cannot access Server0 through FTP.





Conclusion →

The experiment demonstrated the implementation of both standard and extended Access Control Lists (ACLs) to control network traffic by permitting or denying access to remote hosts. Standard ACLs were used to filter traffic based on source IP addresses, while extended ACLs provided more granular control by filtering traffic based on source and destination IPs, protocols and port numbers.

Name: _____ Regd No: _____

Exercises →

1) State the importance of Access Control Lists (ACL) in Computer networking.

Ans→ Access Control Lists (ACLs) play a crucial role in network security and traffic management by filtering packets based on defined rules.

i) Enhanced Security → ACLs prevent unauthorised access by allowing or denying traffic based on IP addresses, protocols and ports.

ii) Traffic Control → Helps in managing network congestion by permitting only necessary traffic, improving efficiency.

iii) Network Performance Optimisation → Reduces unwanted traffic, conserving bandwidth and improving response times.

iv) Access Restriction → Limit access to sensitive resources, ensuring only authorised users can connect to critical services.

v) Firewall Functionality → Acts as a basic firewall by filtering inbound and outbound traffic based on security policies.

2) Differentiate the use of standard and extended ACL.

Ans→

Feature	Standard ACL	Extended ACL
Filtering based on	Source IP address only	Source IP, Destination IP, Protocol and Port number.
ACL Number Range	1-99, 1300-1999	100-199, 2000-2699
Granularity	Basic filtering	Fine-grained control
Protocol Control	Cannot specify protocols	Can filter specific protocols
Placement recommendation	Near the destination	Near the source
Usage	Allow or deny traffic from specific hosts/networks	Allow or deny specific services like HTTP, FTP, SSH.
Configuration	access-list 10 deny 192.168.10.1	access-list 110 deny tcp 192.168.1.1 any eq 80

3) How does an ACL process traffic in a router? How would you apply an ACL to filter OSPF traffic?

Ans→ An Access Control List (ACL) processes traffic in a router by analyzing incoming or outgoing packets against predefined rules and deciding whether to permit or deny them.

i) Packet Arrival → When a packet reaches an interface, the router checks if an ACL is applied.

ii) Sequential Rule Matching → The router examines the ACL rules line by line, from top to bottom.

iii) First-Match Logic → The router stops checking once a match is found and executes the action.

iv) Implicit Deny rule → If no rules match, the packet is denied by default.

v) Packet Forwarding or Dropping → If permitted, the packet is processed; if denied it is discarded.

Applying an ACL to filter OSPF traffic →

i) Create an Extended ACL to deny OSPF traffic

```
access-list 120 deny OSPF any any
access-list 120 permit ip any any
```

ii) Apply the ACL to an interface

```
int GigO/1
ip access-group 120 in
```

4) What is the purpose of a "wildcard mask" in ACLs and how does it differ from a subnet mask?

Ans→ A wildcard mask is used in ACLs to specify a range of IP addresses. It determines which bits of an IP address should be checked and which should be ignored when applying ACL rules.

Name:_____ Regd. Number:_____

Difference between Wildcard Mask and Subnet Mask →

Feature	Wildcard Mask	Subnet Mask
Purpose	Used in ACLs, OSPF and route filtering to match IP address ranges.	Defines network and host portions of an IP address
Bit Representation	0 = Match the bit exactly, 1 = Ignore the bit	1 = Network bit, 0 = Host bit
Usage	ACLs, OSPF, EIGRP, logging	IP addressing and subnetting
Example (for 192.168.1.0/24)	0.0.0.255 (matches all 192.168.1.x)	255.255.255.0 (defines subnet)

Name:_____ Regd. Number:_____