इरिसेट

नेटवर्क प्रयोगशाला

प्रयोग नं: एन डब्लू एल - 06

IRISET

NETWORK LABORATORY

EXPERIMENT NO.: NWL-06

नाम
Name : ---

अनुक्रमांक
Roll No : --

प्राप्त अंक
Marks Awarded **:**

पाठ्यक्रम
Course : --

दिनांक
Date : --

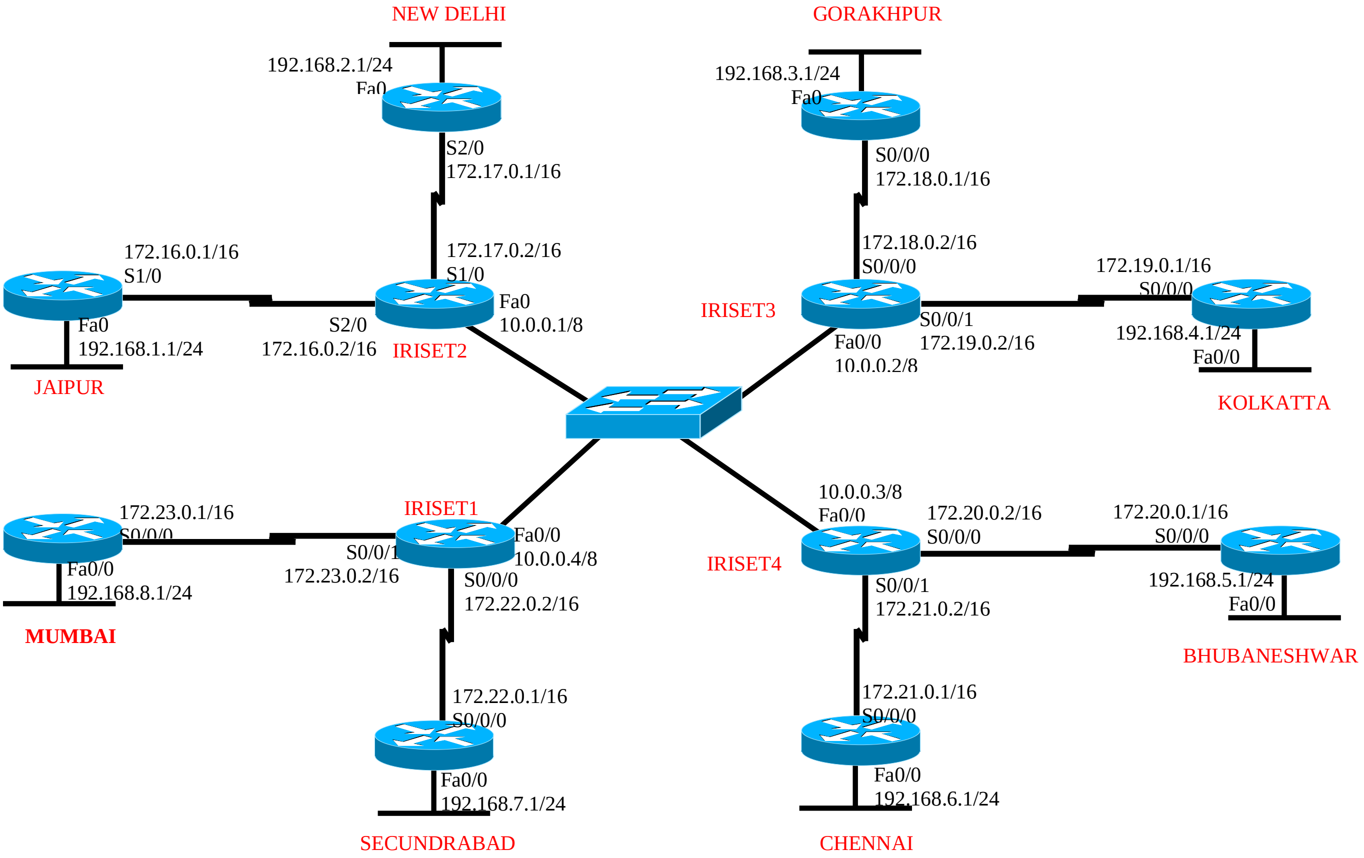
अनुदेशक का हस्ताक्षर :
Instructor Initial

Name of Experiment: **Configuration of Access list**

Object

Configuring Access lists as per the network connectivity diagram shown below.

Network Connectivity diagram



S0/0/1

Introduction

Access Control List (ACL):

- Earliest method of providing network security
- Provides Layer3 & Layer4 security
- Controls the flow of traffic from one network to another network
- It is called as packet filtering firewall

Terminology:

Deny: Blocking a network/subnet/host/service
Permit: Allowing a network/subnet/host/service
Source Address: The address from where the request starts
Destination address: The address from where the request ends
In bound: Traffic coming into the interface with respect to the router
Out bound: Traffic going out of the interface with respect to the router

Protocols:

TCP: Transmission Control Protocol
UDP: User datagram protocol
ICMP: Internet Control Messaging Protocol

Operators:

Eq: equal to
Neq: not equal to
Lt: less than
Gt: greater than

Service (Port number):

HTTP (80): Hyper text transfer protocol
FTP (20,21): File transfer protocol
Telnet (23)

Wild card mask:

- Tells the router which addressing bits must match to the addressing given in the ACL statement
- It is the inverse of the subnet mask
- Wild card mask (or) Inverse mask (Global subnet mask – subnet mask)
- A bit value of ‘0’ indicates must match (check bits)
- A bit value of ‘1’ indicates ignore (ignore bits)
- Wild card mask for a host will be always 0.0.0.0

Working of access list:

- Works in sequential order from top to bottom
- If a match is found it does not check further
- All deny statements should be given first
- There should be at least one permit statement
- An implicit deny block all traffic by default when there is no match (an invisible statement)
- New entries are automatically added to the bottom
- Can have one access-list per interface per direction
- Removing of specific statement in a access list is not possible

Types of Access list

- Standard access control list
    - Named
    - Numbered
- Extended access control list
    - Named
    - Numbered

Apparatus Required

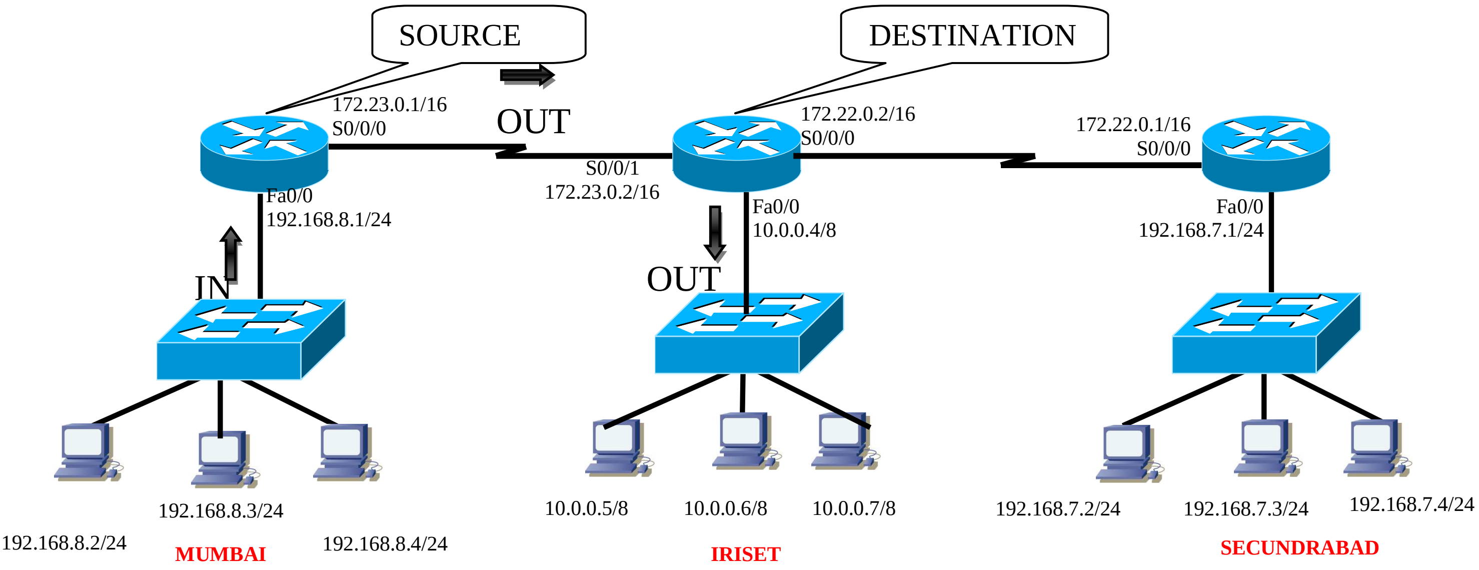
1. Desktop PCs with NIC card
2. Patch card (straight cable, both ends terminated with RJ 45 connectors)
3. Router (CISCO 1845)
4. Switch (DAX)
5. Null modem cable with connectors on both ends

Procedure

Configure standard access control list (ACL) for the given connectivity diagram

Standard access control list:

- The access-list number range is 1-99
- Can filter a network, subnet, or host
- Two way communication is stopped
- All services are blocked or allowed
- Filters traffic based only on the source address
- Implemented closest to the destination [Guide lines]



Criteria :

a. **192.168.8.2 & 192.168.8.3 should not communicate with 10.0.0.0 network**

Syntax:

```
Router(config)#access-list <no.> permit/deny  <source ip><source wildcard mask>↵
```

Access-list no: *any number between 1 to 99 (standard access-list)*

Configuration:

```
Router(config)#access-list 1 deny  192.168.8.2  0.0.0.0↵
Router(config)#access-list 1 deny  192.168.8.3  0.0.0.0↵
Router(config)#access-list 1 permit any ↵
Router(config)#exit↵
```

Implementation:

Implement access-list (ACL) on an interface

Syntax:

```
Router(config)#interface <type> <no.>↵
Router(config-if)#ip access-group <no.> in/out↵
```

Access-group no: *same as access-list number*
In / out: *in bound traffic / out bound traffic moving through the interface with respect to source IP address*

Configuration:

```
Router(config)#interface fa0/0↵
Router(config)#ip access-group 1 out↵
Router(config)#exit↵
```

Verification of access-list

To verify the output of access-list

Syntax:

```
Iriset1# show ip access-list↵
```

To verify the implementation of access-list

Syntax:

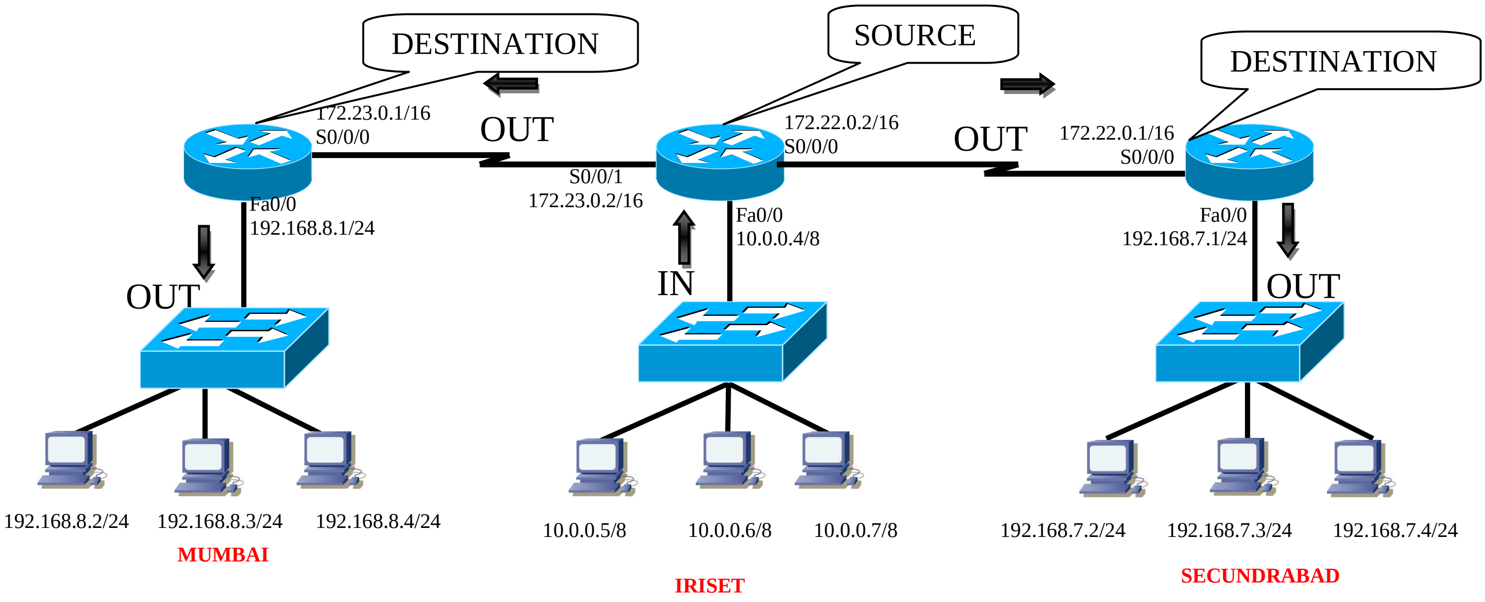
```
Iriset1# show interface <type> <no.>↵
```

Extended access control list:

- The access-list number range is 100-199
- Can filter a network, subnet, host & service
- One way communication is stopped
- Selected service can be blocked or allowed
- Filters traffic based on the source address, destination address & service
- Implemented closest to the source [Guide lines]

<u>Procedure</u>

Configure extended access control list (ACL) for the given connectivity diagram



Criteria :

a. **10.0.0.0 should not access web services on 192.168.7.2**
b. **10.0.0.0 should not ping 192.168.8.0**

<u>Syntax:</u>

Router(config)#*access-list <no.> permit/deny <protocol> <source ip> <source wildcard mask> <destination ip> <destination wildcard mask> [operator] [port no.]*↵

Access-list no: *any number between 100 to 199 (extended access-list)*
Protocol: *like TCP, UDP, ICMP*
Operator: *like eq =*
Port no: *like port no. 80 for http service*

Configuration:

```
Iriset1(config)#access-list 101 deny  TCP 10.0.0.0  0.255.255.255 192.168.7.2  0.0.0.0 EQ=80↵
Iriset1(config)#access-list 101 deny  ICMP 10.0.0.0  0.255.255.255 192.168.8.0  0.0.0.255 ECHO↵
Iriset1(config)#access-list 101 ip permit any any ↵
Iriset1(config)#exit↵
```

Implementation:

Implement access-list (ACL) on an interface

Syntax:

```
Router(config)#interface <type> <no.>↵
Router(config-if)#ip access-group <no.> in/out↵
```

Access-group no: *same as access-list number*
In / out: *in bound traffic / out bound traffic moving through the interface with respect to source IP address*

Configuration:

```
Router(config)#interface fa0/0↵
Router(config)#ip access-group 101 in↵
Router(config)#exit↵
```

Verification of access-list

To verify the output of access-list

Syntax:

```
Iriset1# show ip access-list↵
```

To verify the implementation of access-list

Syntax:

```
Iriset1# show interface <type> <no.>↵
```

Exercise:

1. What is the difference between access control-list & firewall?

2. What is the difference between standard access control-list & extended access control list?

3. What is the difference between in-bound & out-bound traffic?