Access Control List (ACL) Implementation

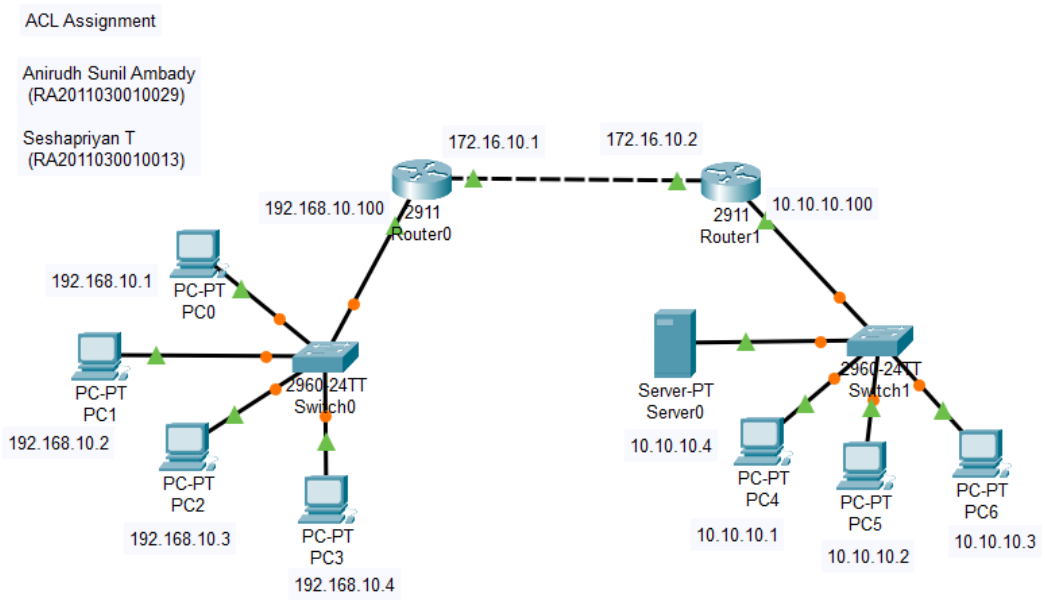
Aim:

To implement Access Control List (ACL) in Cisco Packet Tracer.

Abstract:

A set of rules known as an access control list (ACL) defines which users or systems are allowed or denied access to a specific object or system resource. Additionally, access control lists are implemented in switches and routers, where they serve as filters to govern which traffic is allowed access to the network. A security attribute on each system resource identifies the access control list for that resource. Every person who has access to the system has a place on the list. The most typical privileges for a file system ACL are the capacity to read a file or all the files in a directory, to write to the file or files, and, if the file is an executable file or programme, to run it.

Architechure and Design:



Implementation:

a) **IP Address Table:**

Serial No.	Device	IP Address
1.	PCs	198.168.10.1-192.168.10.4
2.	Router0	Gig0/0-172.16.10.1 Gig0/1-192.168.10.100
3.	Router1	Gig0/0-172.16.10.2 Gig0/1-10.10.10.100
4.	Server0	10.10.10.4

Connection:

```
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time=1ms TTL=126
Reply from 10.10.10.1: bytes=32 time<1ms TTL=126
Reply from 10.10.10.1: bytes=32 time=10ms TTL=126

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Result:

ACL is implemented with the help of Cisco Packet Tracer.