**Aim**

The aim of this experiment is to **configure and verify Dynamic Network Address Translation (NAT)** on a Cisco router to allow hosts from a **private (internal) network** (using non-routable IP addresses) to access services on a **public (external) network** (like the internet), using a single public IP address assigned to the router's interface.

**Algorithm**

1. **Topology Setup:** Design a simple network with a **private LAN**, a **router**, and a **public server/network**.
2. **IP Configuration:** Configure all devices with appropriate IP addresses, distinguishing between the private and public segments.
3. **Define NAT Scope:** Create a **Standard Access Control List (ACL)** to identify the source IP addresses (the private network) that need NAT.
4. **Create NAT Pool:** Define an **IP Pool** containing the public IP address(es) that the internal traffic will be translated to.
5. **Link ACL and Pool:** Create the **NAT translation rule** using the ip nat inside source list [ACL number] pool [Pool Name] command.
6. **Interface Designation:** Mark the router interfaces as either **"inside"** (private network) or **"outside"** (public network).
7. **Verification:** Test connectivity from the internal host to the external server and check the NAT translation table.

**Result**

The experiment is successful when PC-A can successfully communicate with Server-B, and the NAT configuration is visible in the translation table.

 