DHCP and NAT

Manas Ranjan Lenka
School of Computer Engineering,
KIIT University

Obtaining IP Address

- How does an organization get an address block?
  - From provider Internet Service Provider (ISP)
    India: Reliance, Tata

- How does an ISP get address blocks?
  - ICANN: Internet Corporation for Assigned Names and Numbers
    - allocates addresses
    - manages DNS
    - assigns domain names, resolves disputes

- How does a host get a specific IP address?
    - manually/automatically ?

Dynamic Assignment of IP Address

• Dynamic assignment of IP addresses is desirable for several reasons:
  – IP addresses are assigned on-demand
  – Avoid manual IP configuration
  – Support mobility of laptops

• Three Protocols:
  – RARP (until 1985, no longer used)
  – BOOTP (1985-1993)
  – DHCP (since 1993)

• Only DHCP is widely used today.

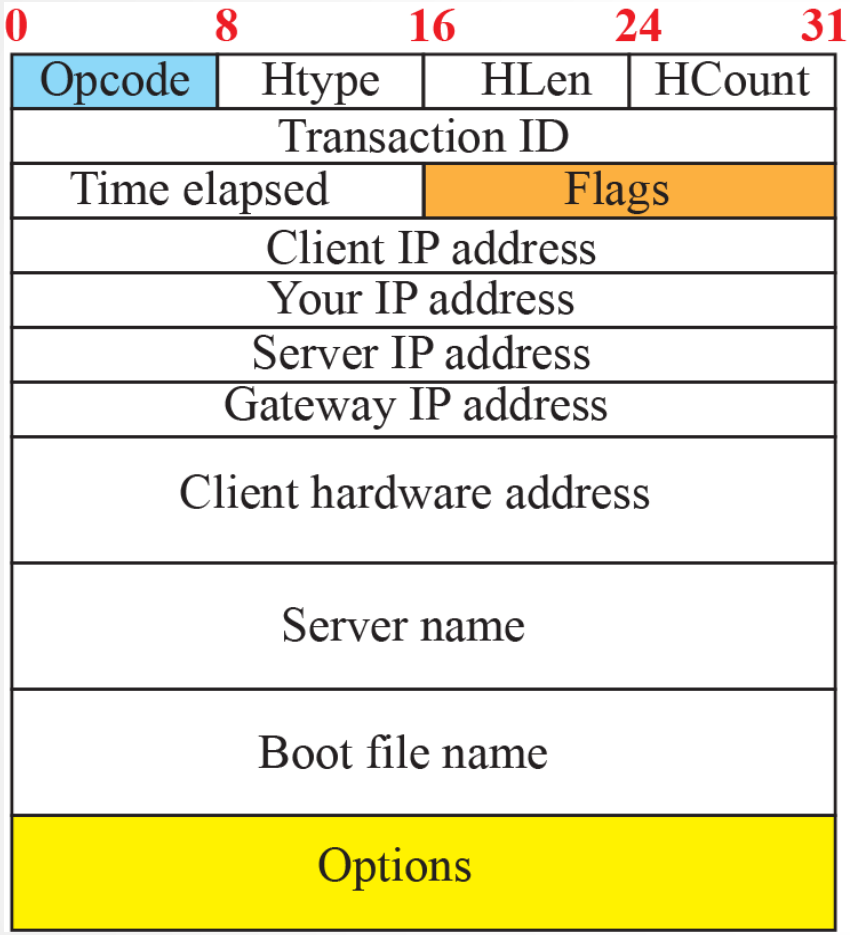
DHCP functionality

In addition to getting the IP Address, a computer may need the following informations

- network prefix
- address of a default router
- address of a Name Server

All these functionalities are provided by **DHCP** to the host.

DHCP Message Format



Fields:

Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Lengh of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by client and repeated by the server
Time elapsed: The number of seconds since the client started to boot
Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used
Client IP address: Set to 0 if the client does not know it
Your IP address: The client IP address sent by the server
Server IP address: A broadcast IP address if client does not know it
Gateway IP address: The address of default router
Server name: A 64-byte domain name of the server
Boot file name: A 128-byte file name holding extra information
Options: A 64-byte field with dual purpose described in text

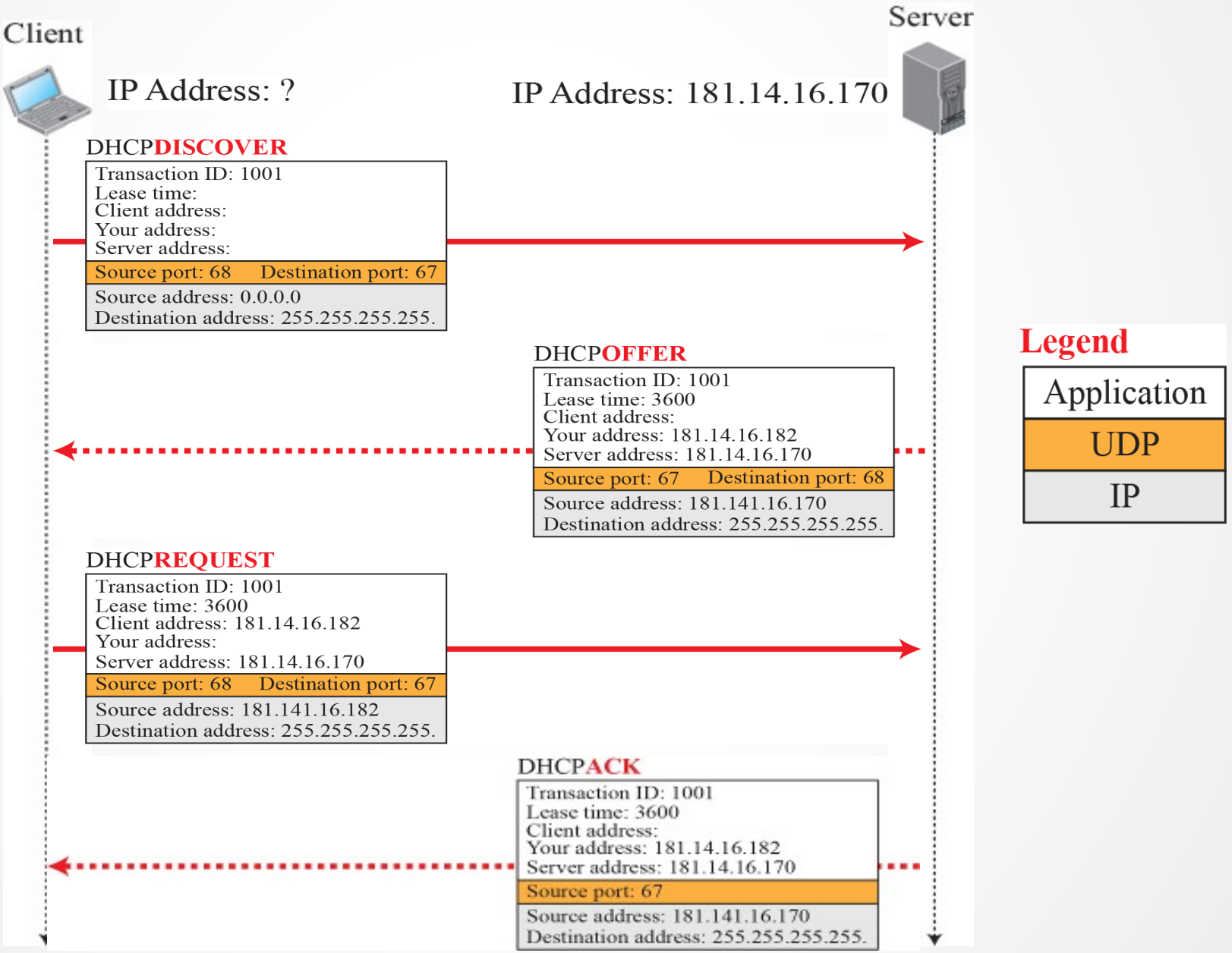
1 DHCPDISCOVER
2 DHCPOFFER
3 DHCPREQUEST
4 DHCPDECLINE
5 DHCPACK
6 DHCPNACK
7 DHCPRELEASE
8 DHCPINFORM

DHCP Operation

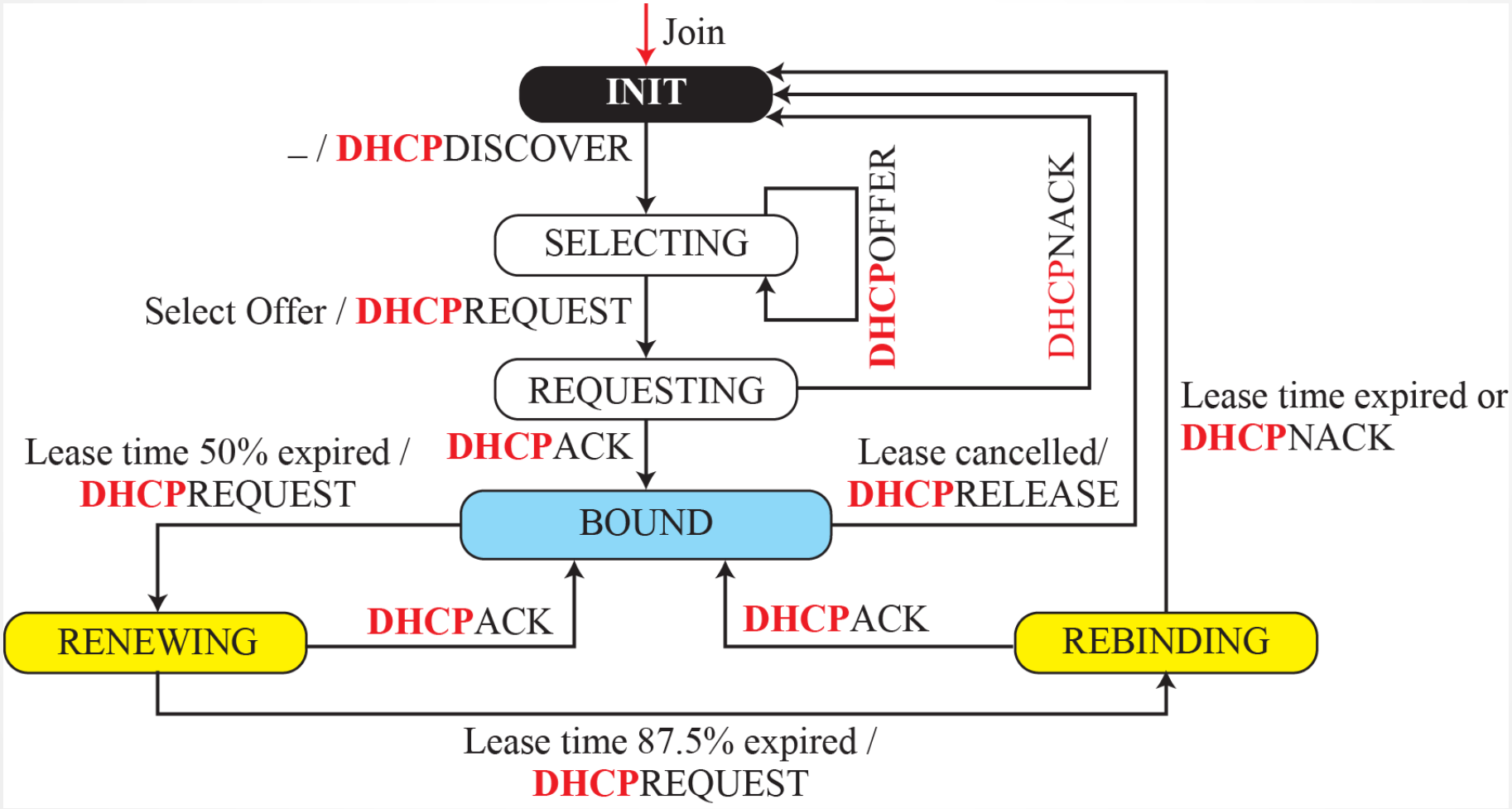
- Uses a client-server Architecture
- Operates at application layer using UDP protocol
- Uses 2 well-know ports (client port - 68 and server port - 67)
- A newly booted/attached host ‘broadcasts’ DHCP discover message
  - IP address: 255.255.255.255 known as **limited broadcast** (broadcasts only with in the local network) as opposed to the **directed broadcast** which send the broadcast message in the internet till it reaches the intended network.

- DHCP Server replies to host (others ignore message)

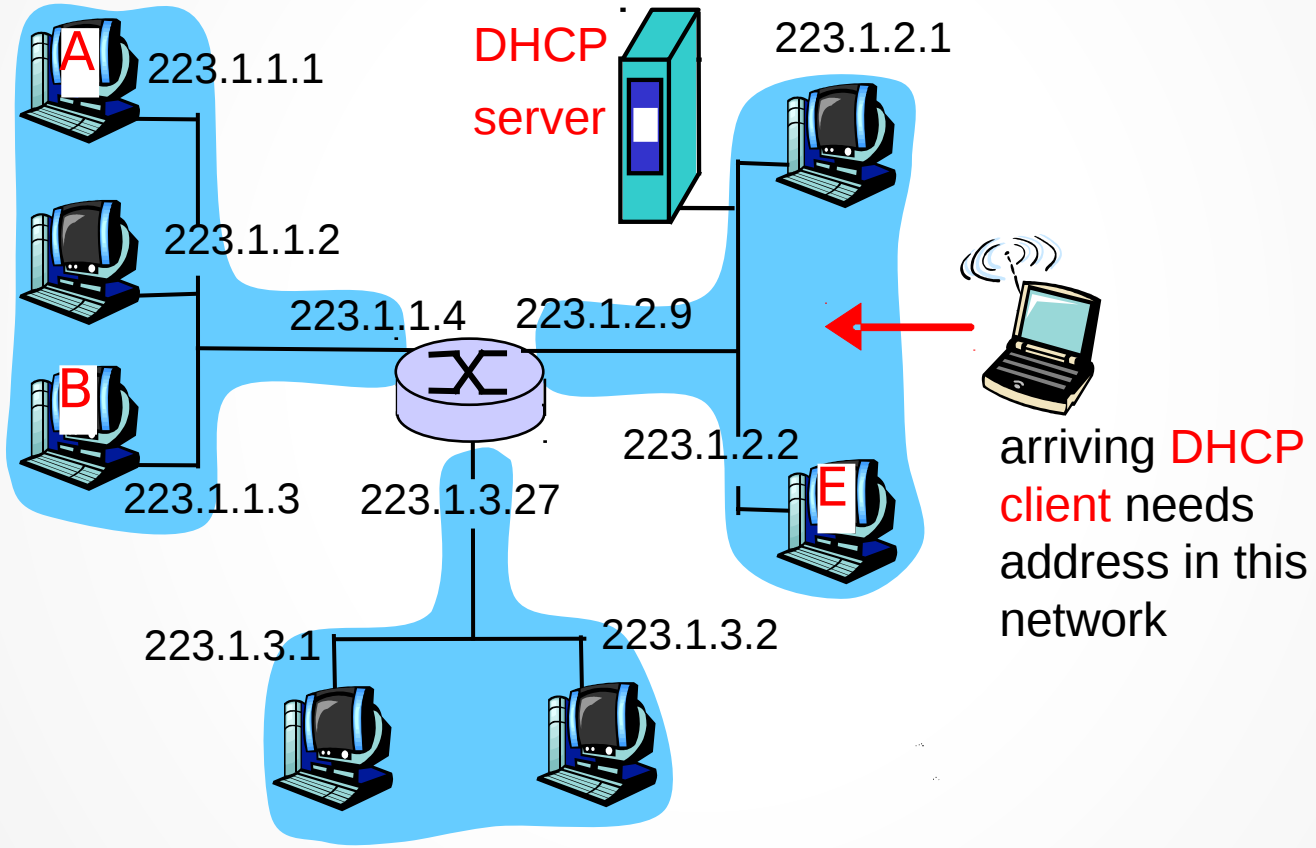
Message Exchanges



FSM : DHCP Client



DHCP Client-Server Scenario



NAT: Network Address Translation

- Private IP network is an IP network that is not directly connected to the Internet

- IP addresses in a private network can be assigned arbitrarily.
    - Not registered and not guaranteed to be globally unique

- Generally, private networks use addresses from the following experimental address ranges (non-routable addresses):

    10.0.0.0 – 10.255.255.255
    172.16.0.0 – 172.31.255.255
    192.168.0.0 – 192.168.255.255

NAT: Network Address Translation

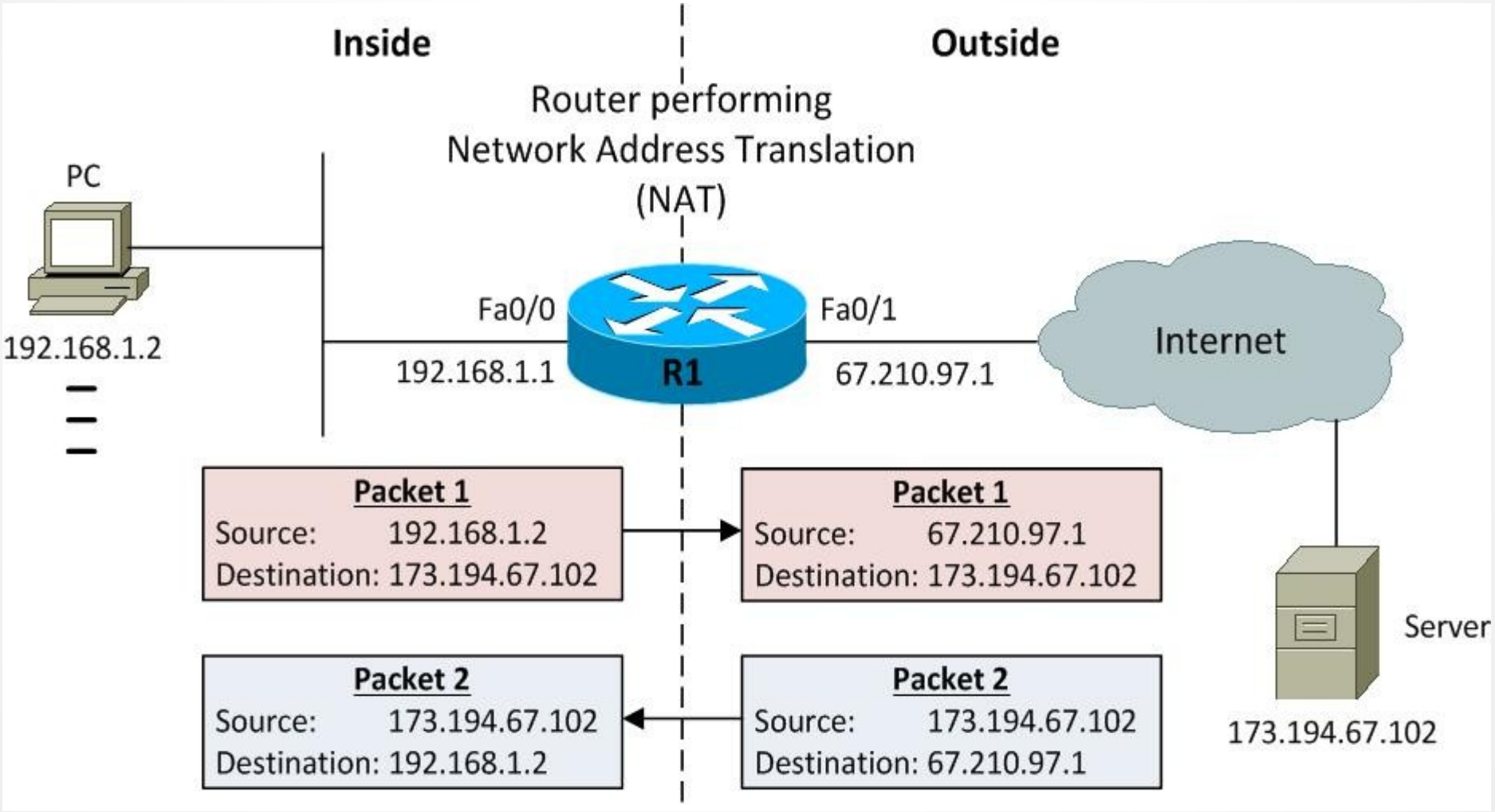
- NAT is a router function where IP addresses (and possibly port numbers) of IP datagrams are replaced at the boundary of a private network

- NAT is a method that enables hosts on private networks to communicate with hosts on the Internet

- NAT is run on routers that connect private networks to the public Internet, to replace the IP address-port pair of an IP packet with another IP address-port pair.

Basic operation of NAT

- NAT device has address translation table
- One to one address translation



IP masquerading

- Also called **Network Address and Port Translation** (NAPT), port address translation (PAT).

- Scenario: Single public IP address is mapped to multiple hosts in a private network.

- NAT solution:
  - Assign private addresses to the hosts of the corporate network
  - NAT device modifies the port numbers for outgoing traffic

IP masquerading