CS3103: Computer Networks Practice

ARP, DHCP

ARP

DHCP

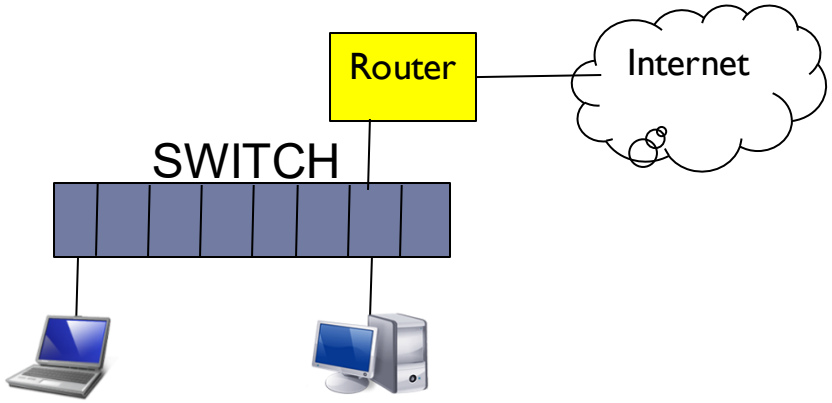
Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

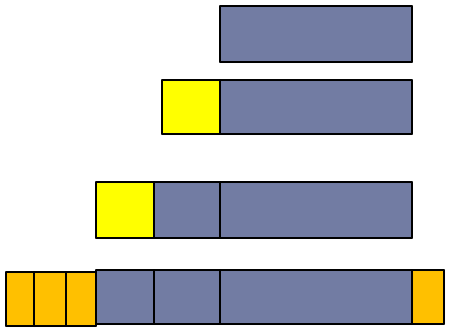
ARP

Address Resolution Protocol

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

ARP - Address Resolution Protocol





Client
TCP
IP
Ethernet

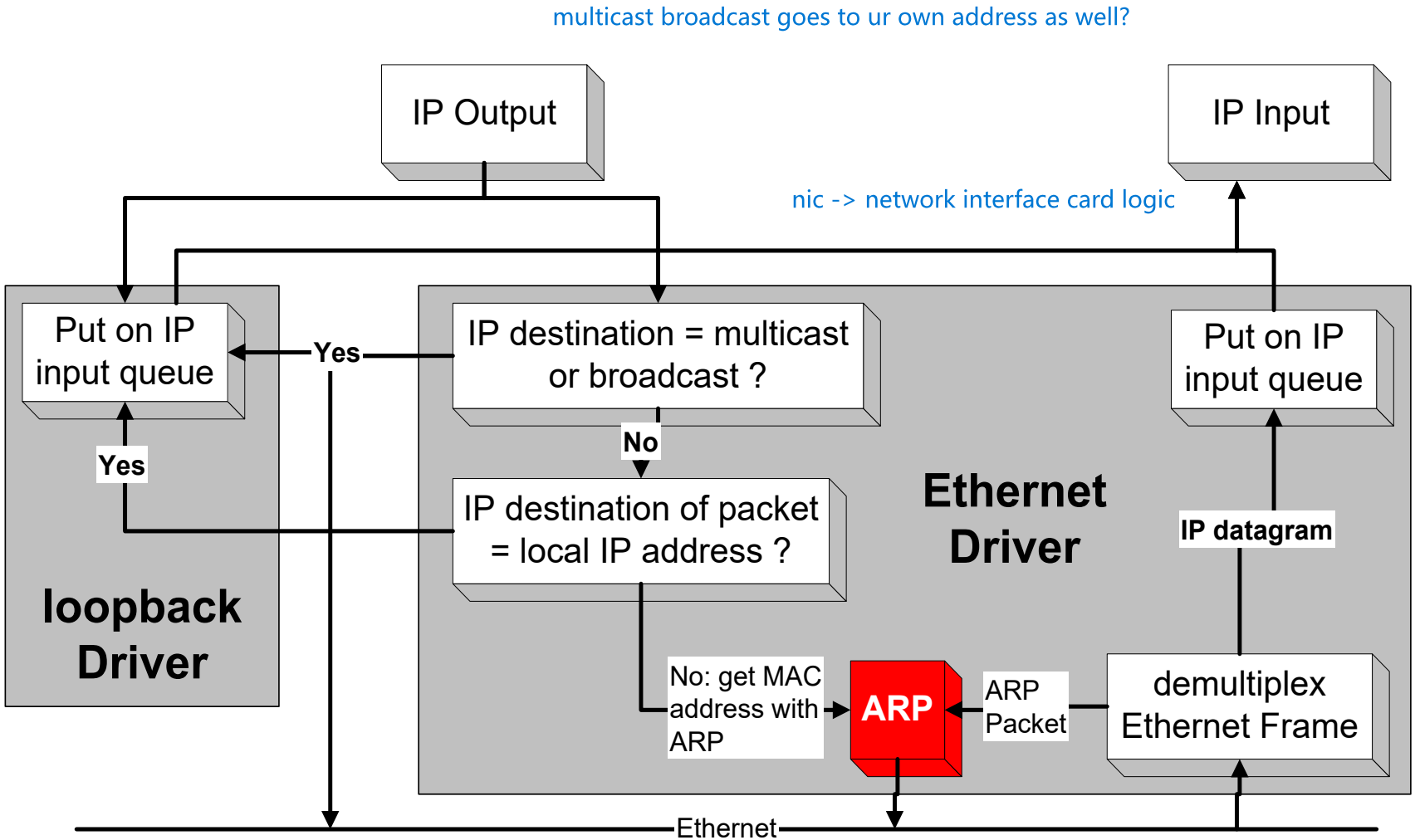
Server
TCP
IP
Ethernet

Application
Transport
Network
Data Link

Motivation:

- End-to-End delivery involves hop-to-hop-delivery.
- How to deliver a packet to the next hop?

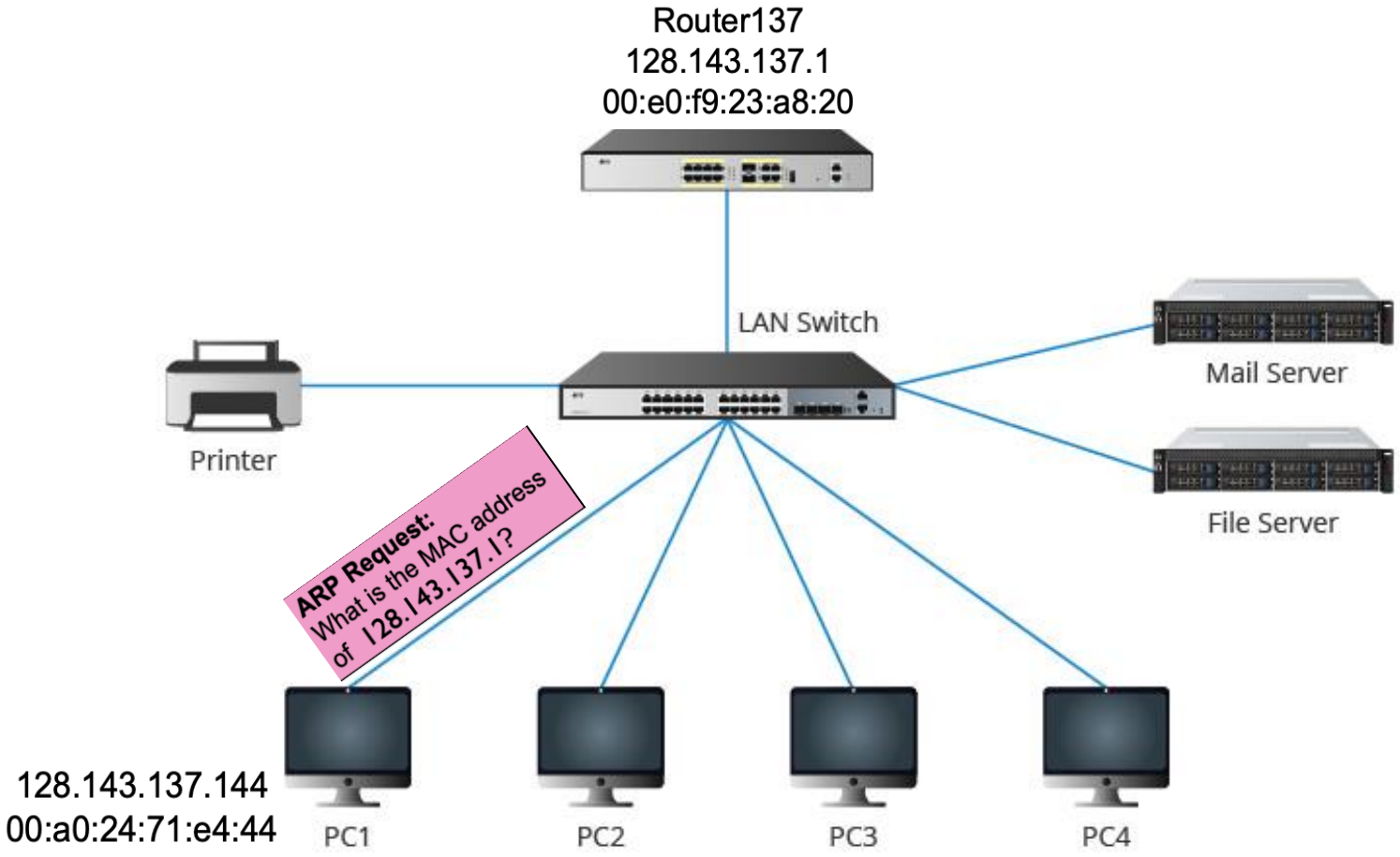
Processing of IP packets by network device drivers



Address Translation with ARP

ARP Request: [Broadcast]

PC1 broadcasts an ARP request to all stations on the network: **"What is the hardware address of Router137?"**

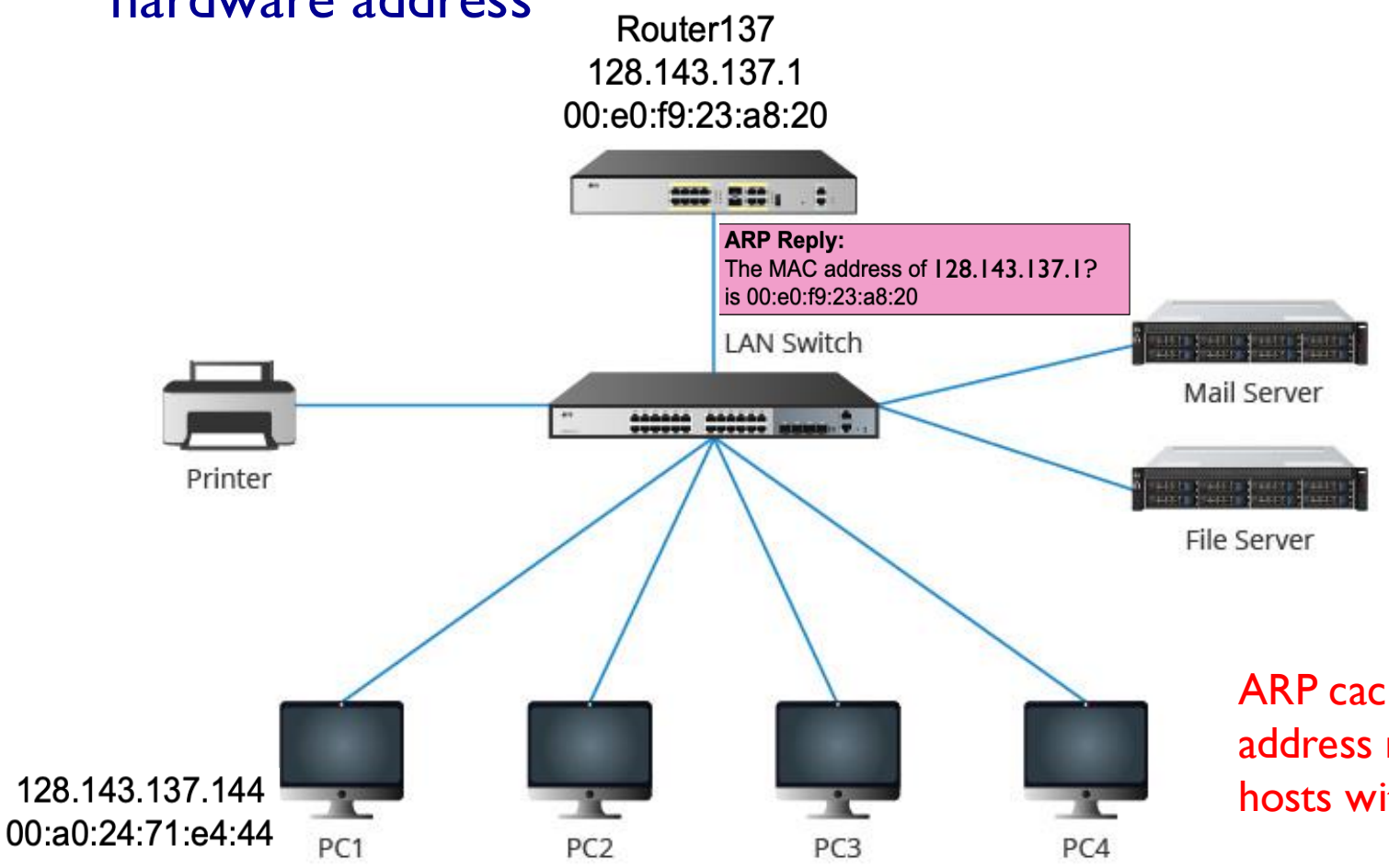


ARP broadcast is restricted to within a LAN.

Address Translation with ARP

ARP Reply: **[Unicast]**

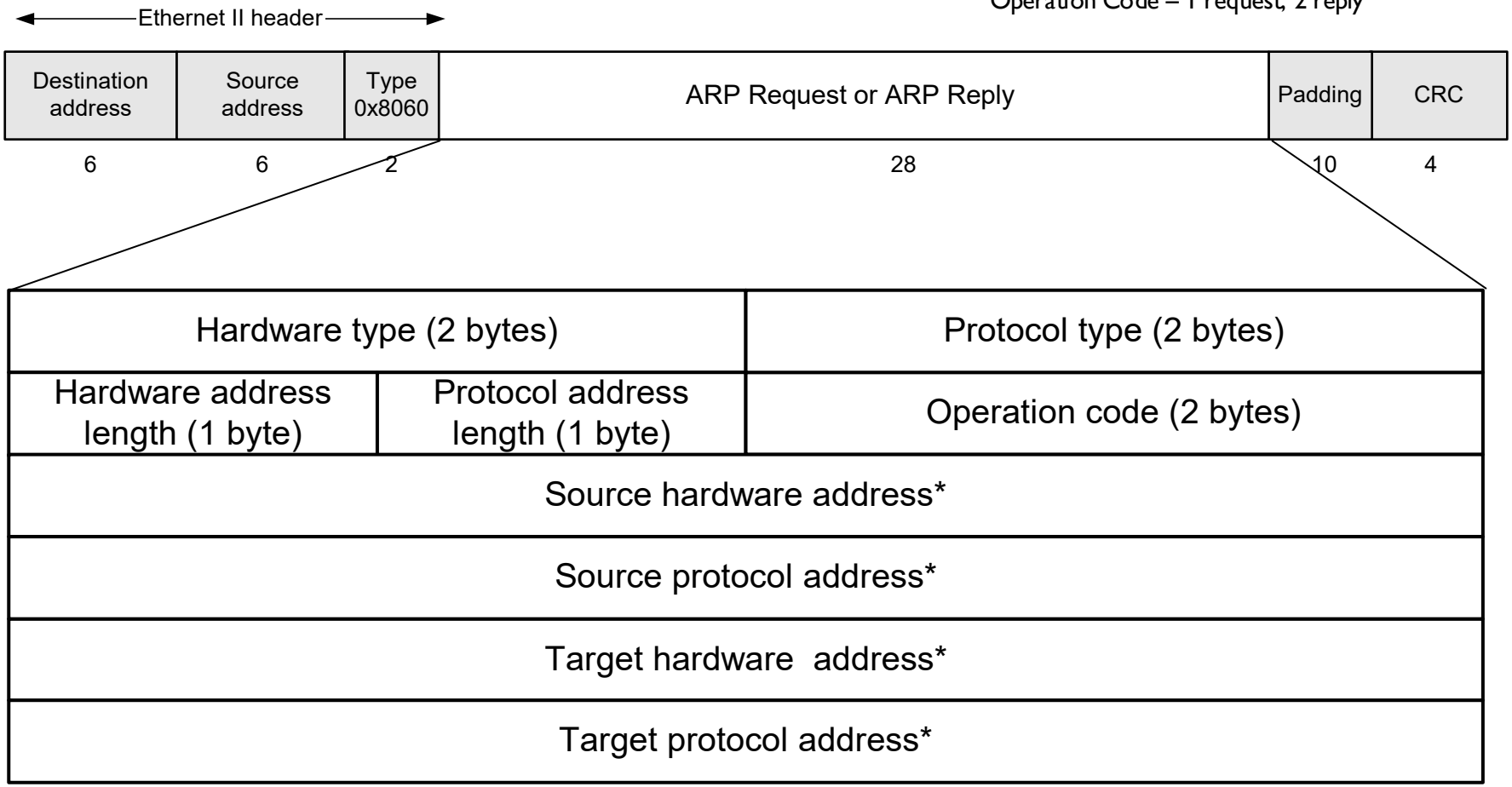
Router 137 responds with an ARP Reply which contains the hardware address



ARP cache contains address mapping for all hosts within a single LAN.

ARP Packet Format

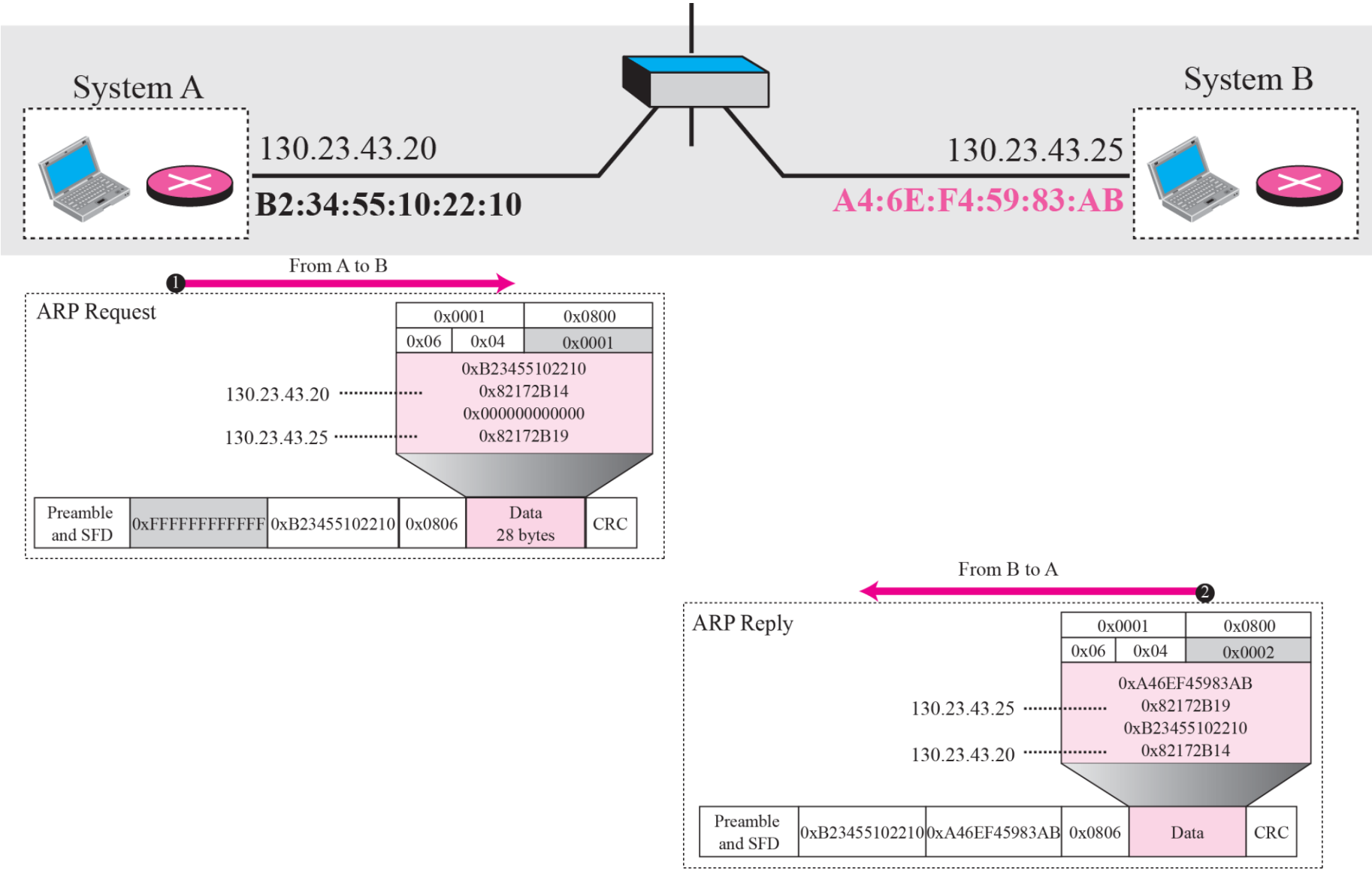
0x8060 – ARP
HW Type for Ethernet = 0x0001
Protocol Type IPv4 – 0x0800
Operation Code – 1 request, 2 reply



* Note: The length of the address fields is determined by the corresponding address length fields

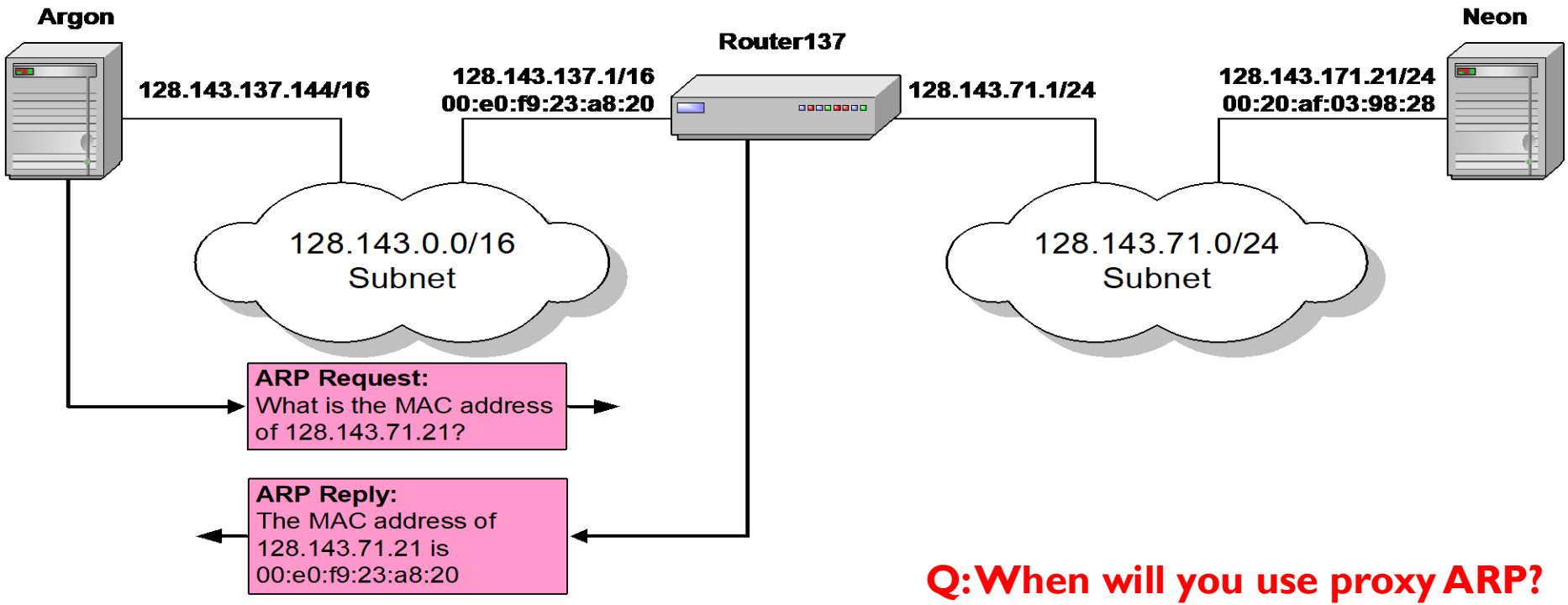
Q:What will be the target H/W address in a ARP request message?

ARP eg


System A
130.23.43.20
B2:34:55:10:22:10
System B
130.23.43.25
A4:6E:F4:59:83:AB
From A to B
1
ARP Request
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
Preamble and SFD
0xFFFFFFFFFFFF
0xB23455102210
0x0806
Data 28 bytes
CRC
From B to A
2
ARP Reply
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
130.23.43.25
130.23.43.20
Preamble and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC

Proxy ARP

- **Proxy ARP:** Host or router responds to ARP Request that arrives from one of its connected networks for a host that is on another side of its connected networks.



Q: When will you use proxy ARP?

Things to know about ARP

- What happens if an ARP Request is made for a non-existing host?
  - Several ARP requests are made with increasing time intervals between requests. Eventually, ARP gives up.

- On some systems (including Linux) a host periodically sends ARP Requests for all addresses listed in the ARP cache. This refreshes the ARP cache content, but also introduces traffic.

- Gratuitous ARP Requests: A host sends an ARP request for its own IP address:
  - Useful for detecting if an IP address has already been assigned.
  - To update ARP caches about its IP to MAC, mapping. (for eg, when a MAC address is changed)

Vulnerabilities of ARP

1. Since ARP does not authenticate requests or replies, ARP Requests and Replies can be forged
2. ARP is stateless: ARP Replies can be sent without a corresponding ARP Request
3. According to the ARP protocol specification, a node receiving an ARP packet (Request or Reply) must update its local ARP cache with the information in the source fields, if the receiving node already has an entry for the IP address of the source in its ARP cache. (This applies for ARP Request packets and for ARP Reply packets)

Questions to ponder:

Q: How the above vulnerabilities can be exploited?

Q: What is **ARP poisoning**?

Q: Discuss Mechanisms to Defend ARP vulnerabilities.

https://pollev.com/banand

REMEMBER TO LOGIN
for PARTICIPATION marks

ARP Defenses – Questions to ponder… Discuss in Discord forum

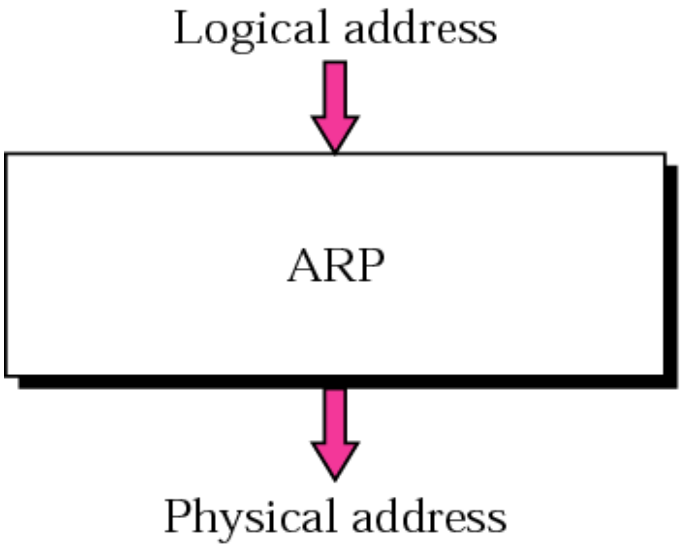
- What is Dynamic ARP Inspection (DAI)? How it works in conjunction with DHCP snooping?
- What is Neighbour Discovery Protocol (NDP) in IPv6? How is it better than ARP?
- In SDN, ARP can be centralised. What are the advantages of centralising?

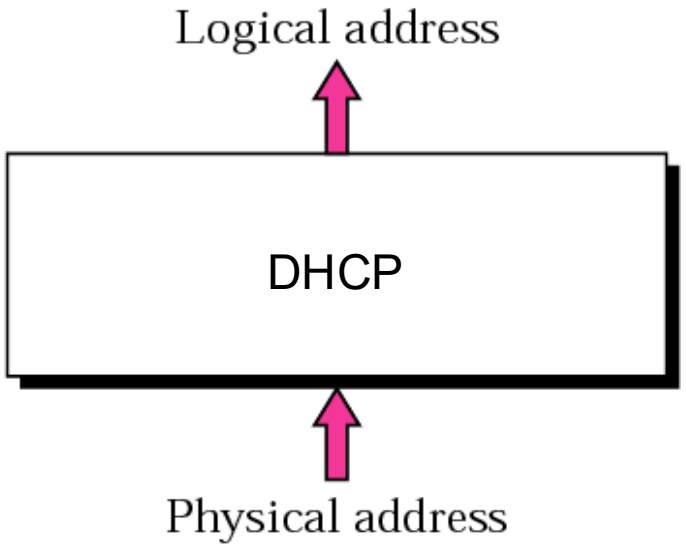
DHCP

Dynamic Host Configuration Protocol

Dr. Anand Bhojan
COM3-02-49, School of Computing
banand@comp.nus.edu.sg ph: 651-67351

ARP and DHCP



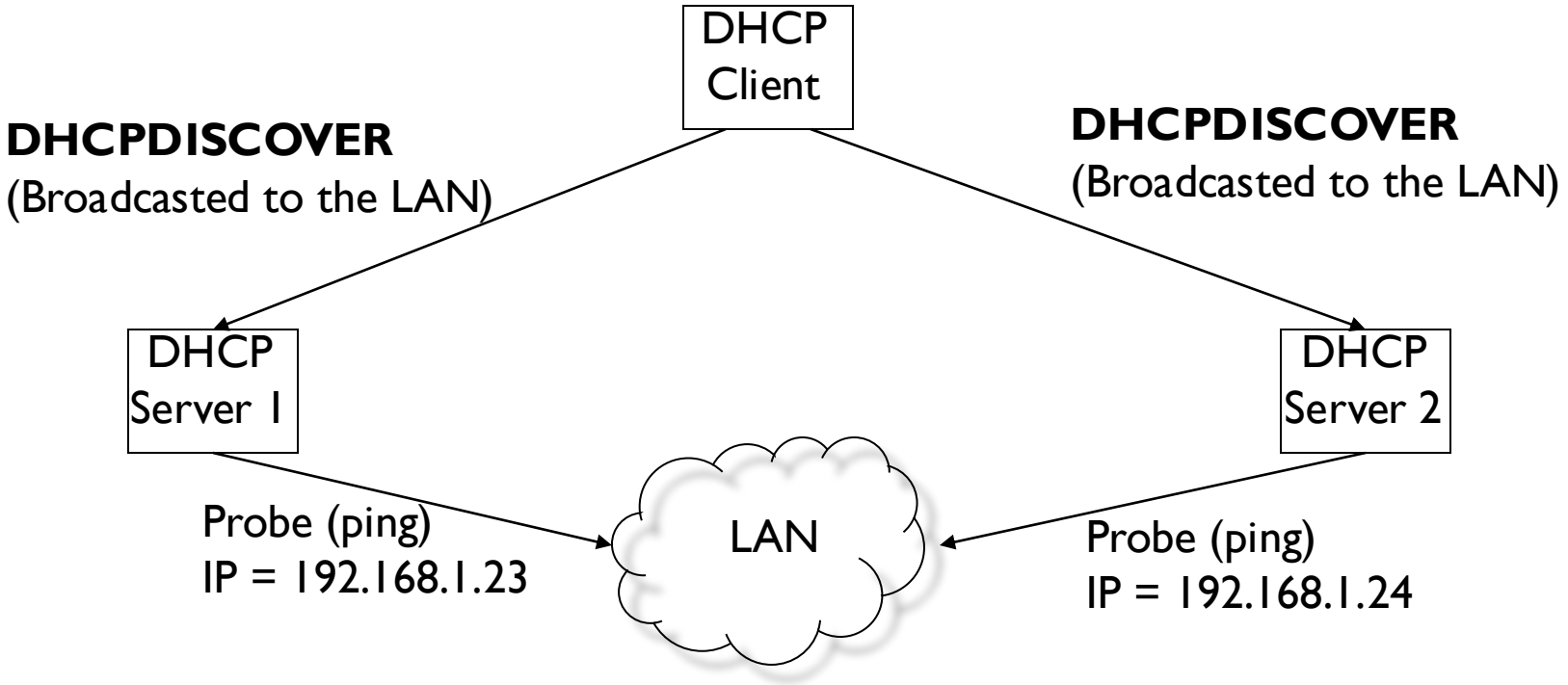


- ARP associates an IP address (logical address) with its physical address (Ethernet address).
- DHCP associates a physical address (Ethernet address) with an IP address (logical address).

DHCP

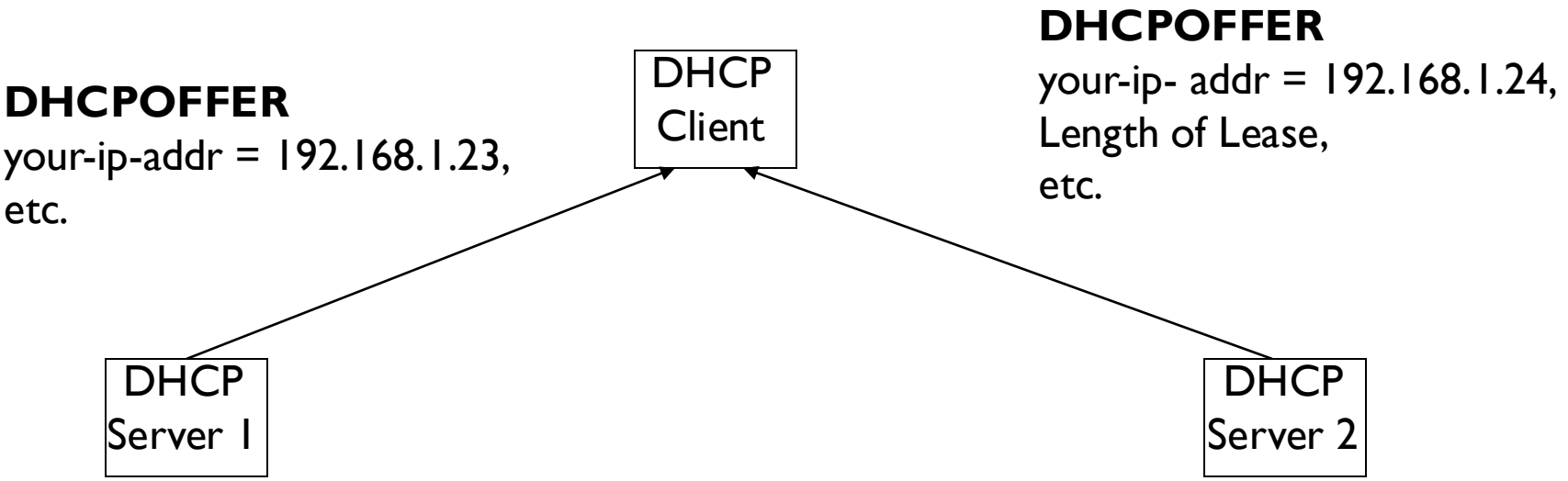
- DHCP allows allocation of IP addresses from a pool through,
  - Static configuration (specific address for indefinite time)
    - (eg., routers, servers)
  - Automatic configuration (for indefinite time)
  - Dynamic configuration (for specific duration)
    - DHCP server loans IP addresses for a limited time
  - DHCP is a Application Layer Protocol.
  - Defined in RFC 2131 and RFC 2132
  - Server waits on UDP port 67, client communicates on UDP port 68.

DHCP – Client-server Interaction (Step 1)

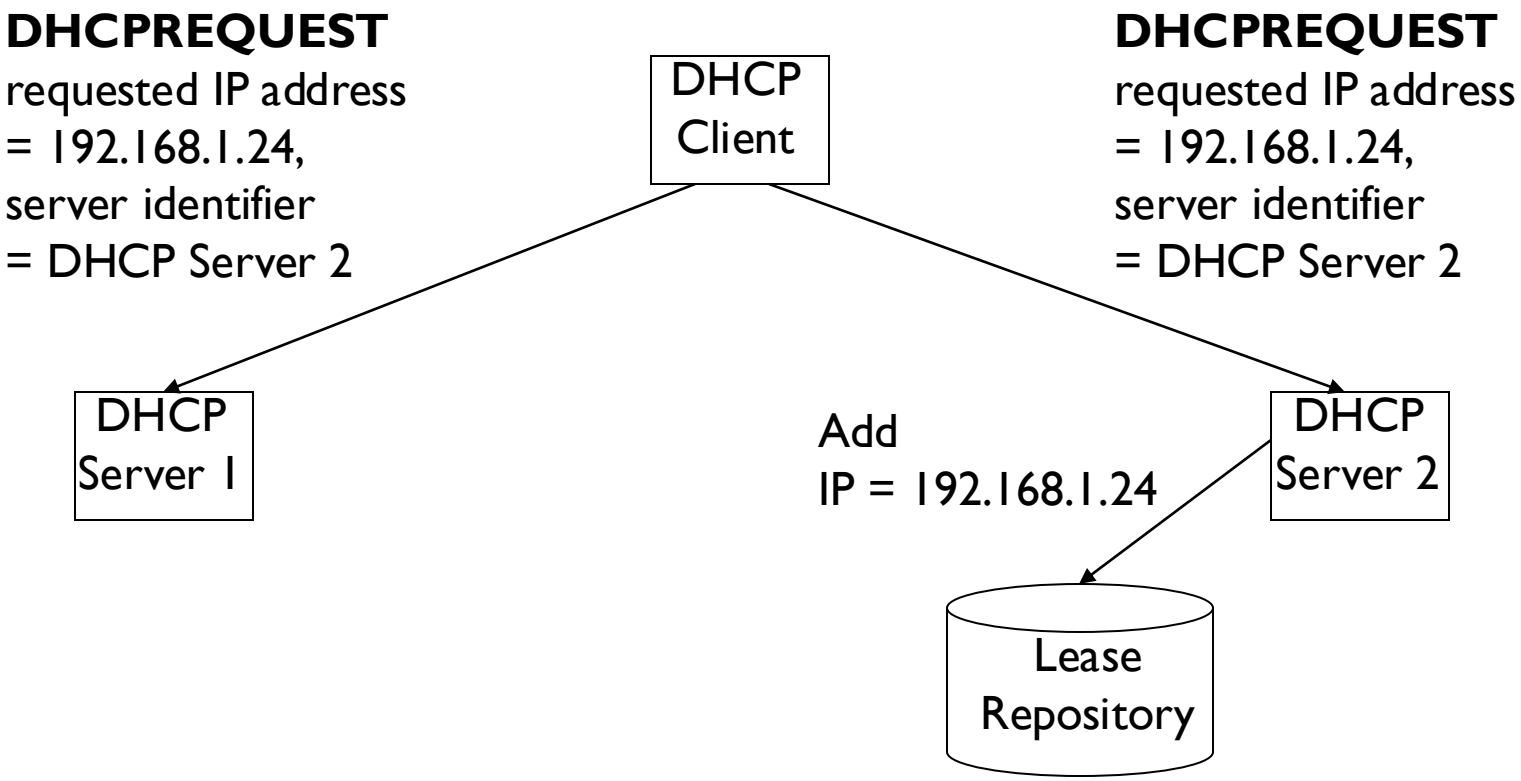


- Q: What is the use of the ping probe?

DHCP – Client-server Interaction (Step 2)

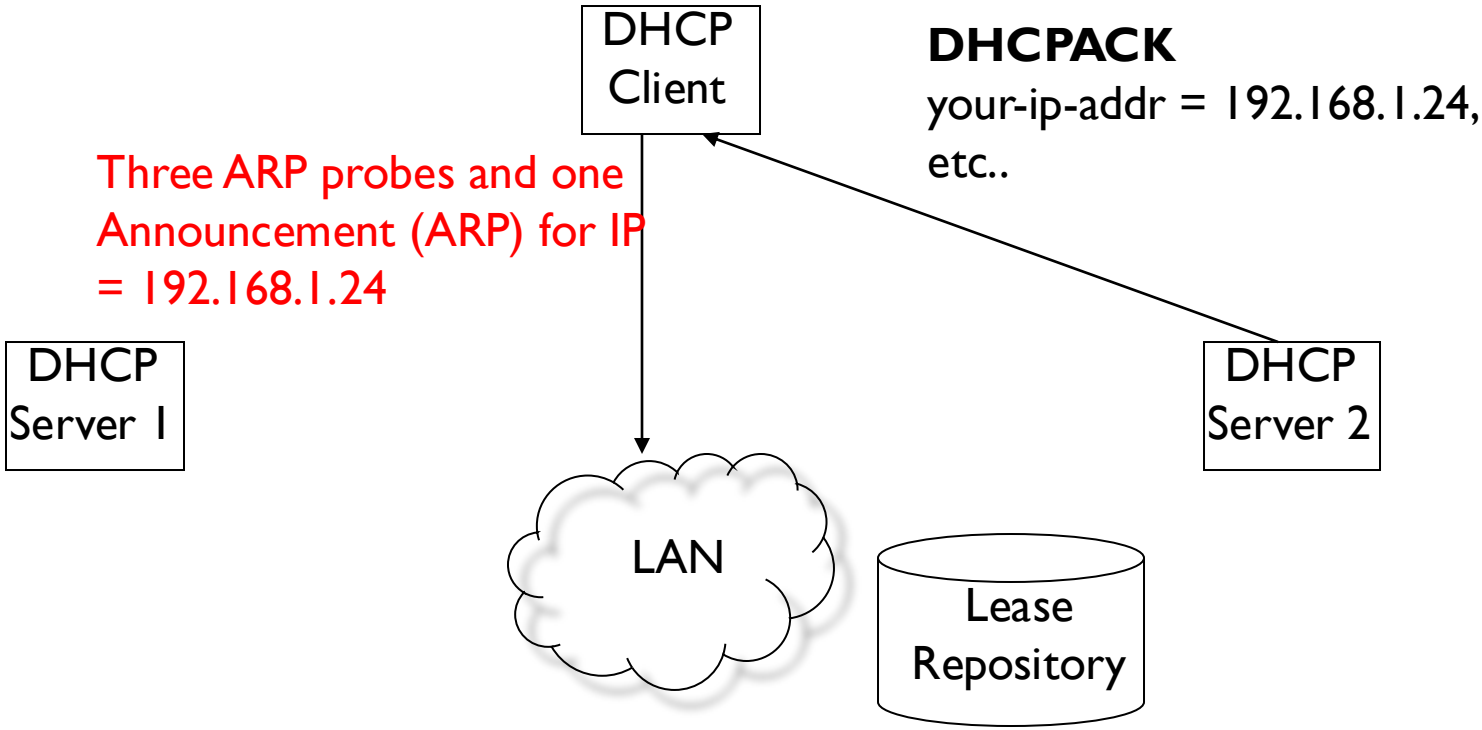


DHCP – Client-server Interaction (Step 3)



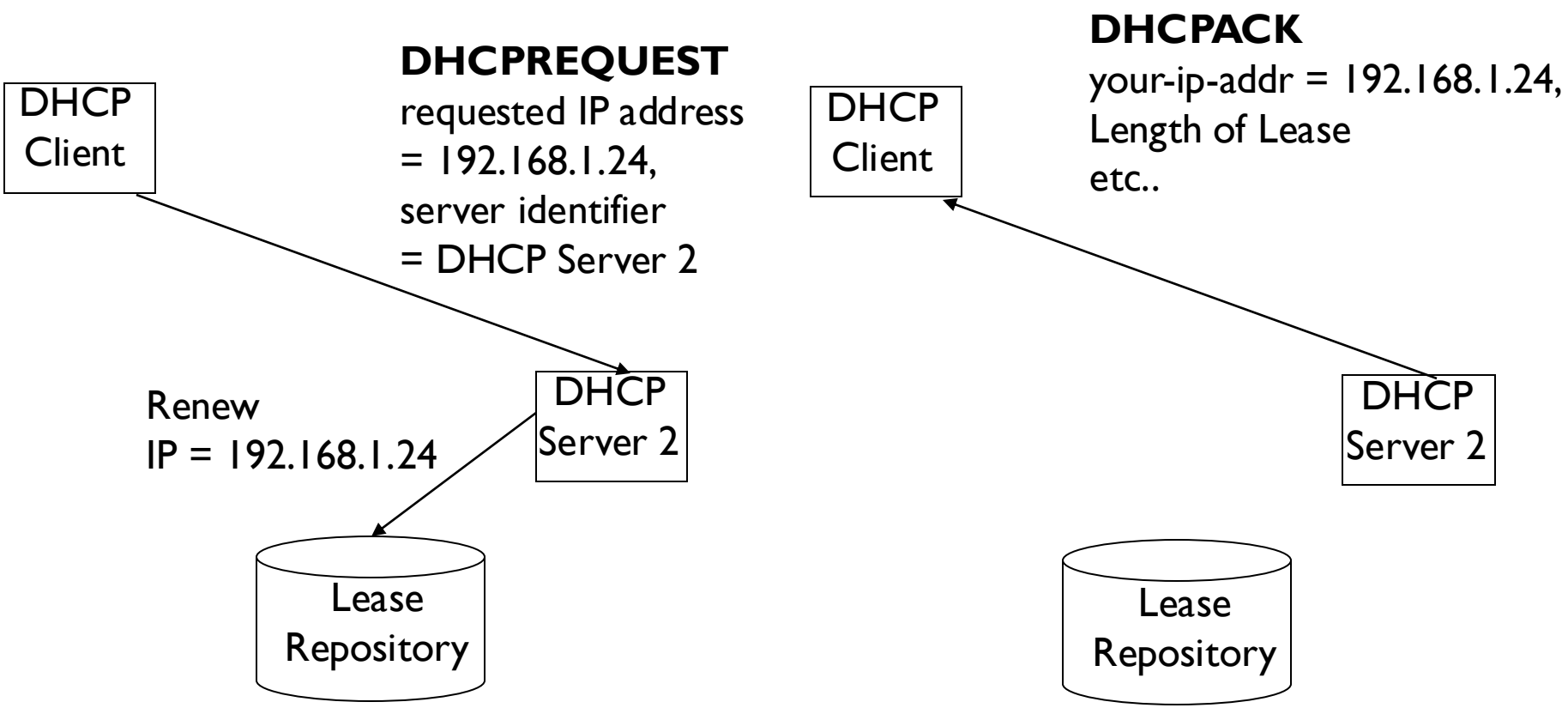
Q: Why is DHCPREQUEST a Broadcast?

DHCP – Client-server Interaction (Step 4)



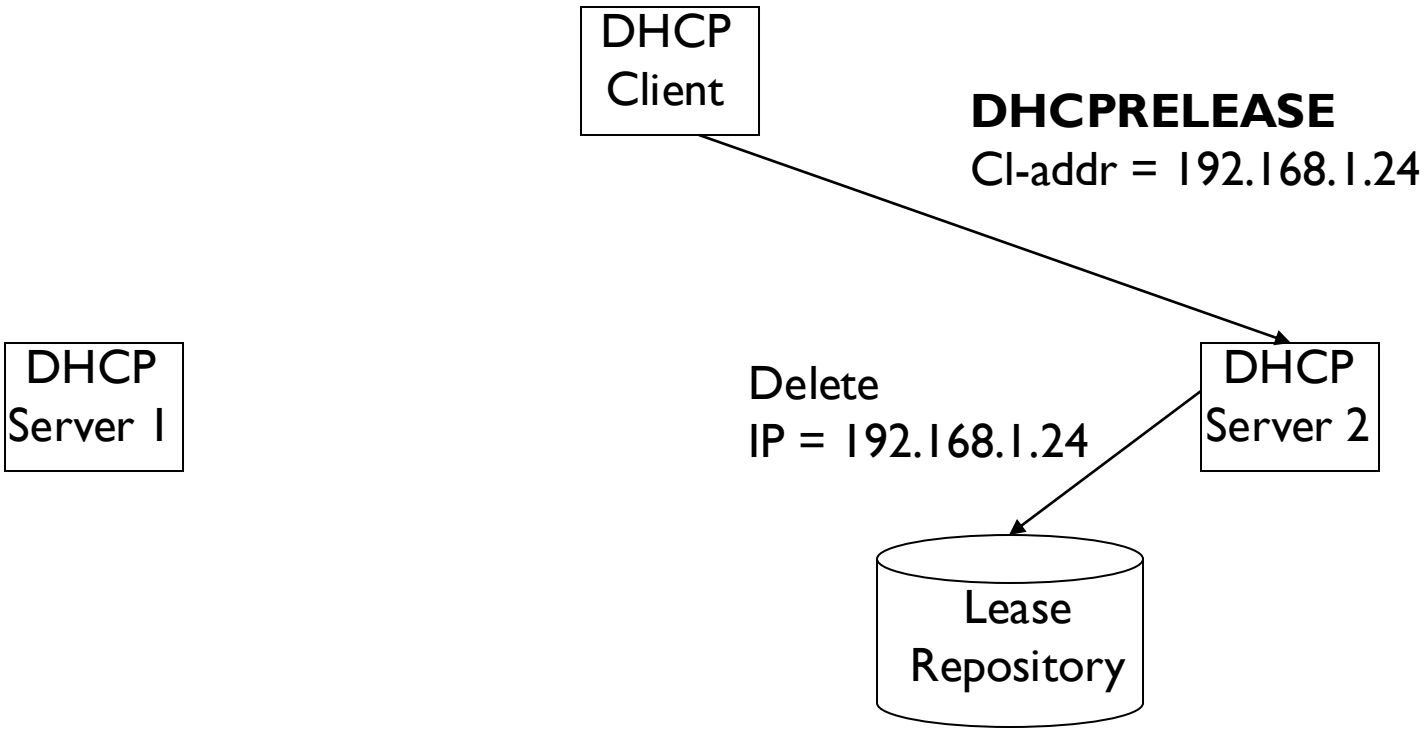
DHCP – Client-server Interaction (Step 5)

- DHCP renew before the Lease Expiry



DHCP – Client-server Interaction (Step 6)

- DHCP release

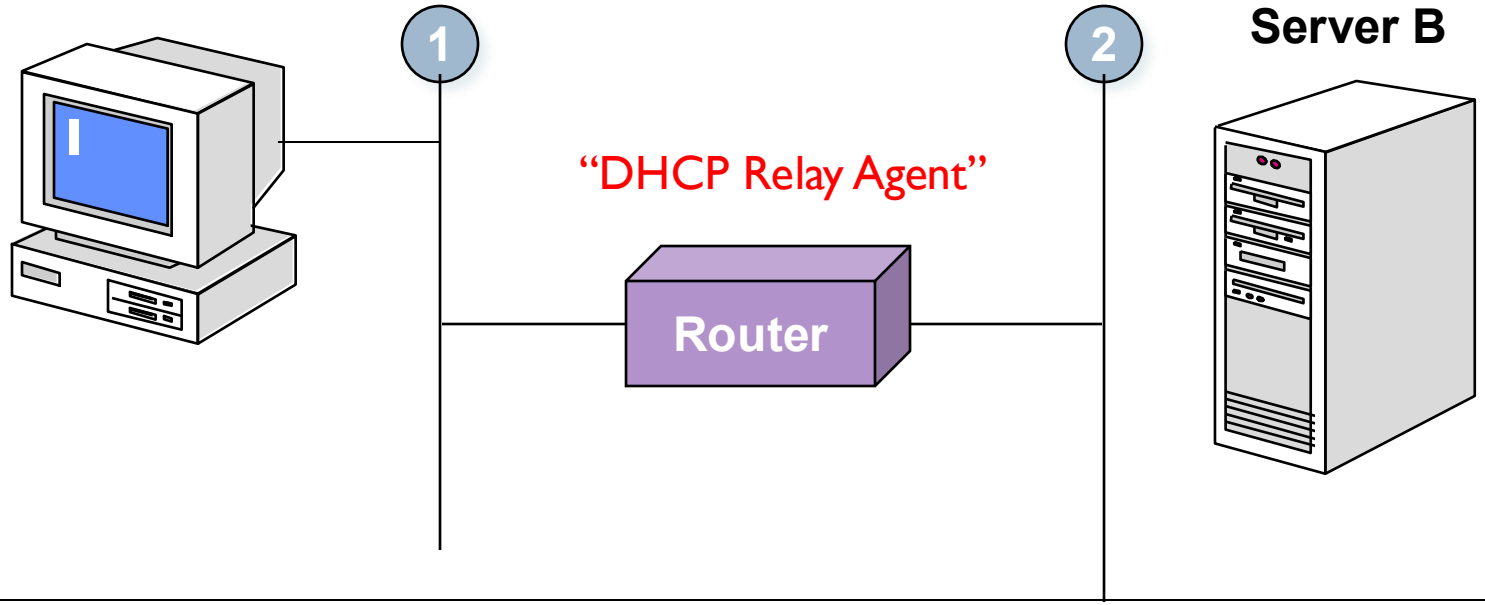


DHCP – Typical TCP/IP Info Returned

- Subnet 192.168.1.0
- Netmask 255.255.255.0
- IP Address 192.168.1.20
- Router 192.168.1.1
- Domain mydomain.com
- DNS #1 192.168.1.2
- DNS #2 192.168.5.2

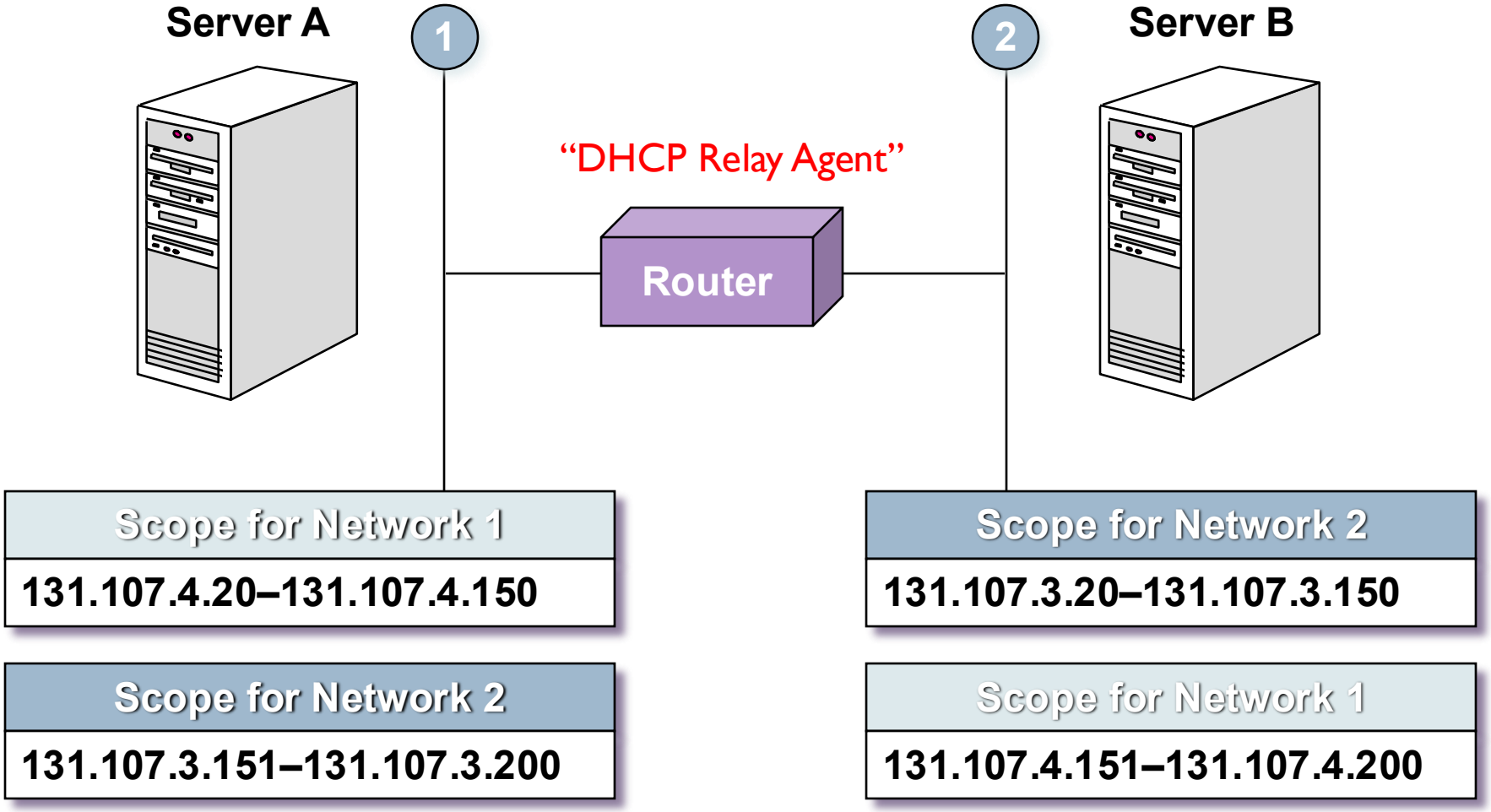
- Does it mean we need one DHCP server for every IP subnet?
- What happens if DHCP Server is not functioning?

DHCP through a Relay Agent



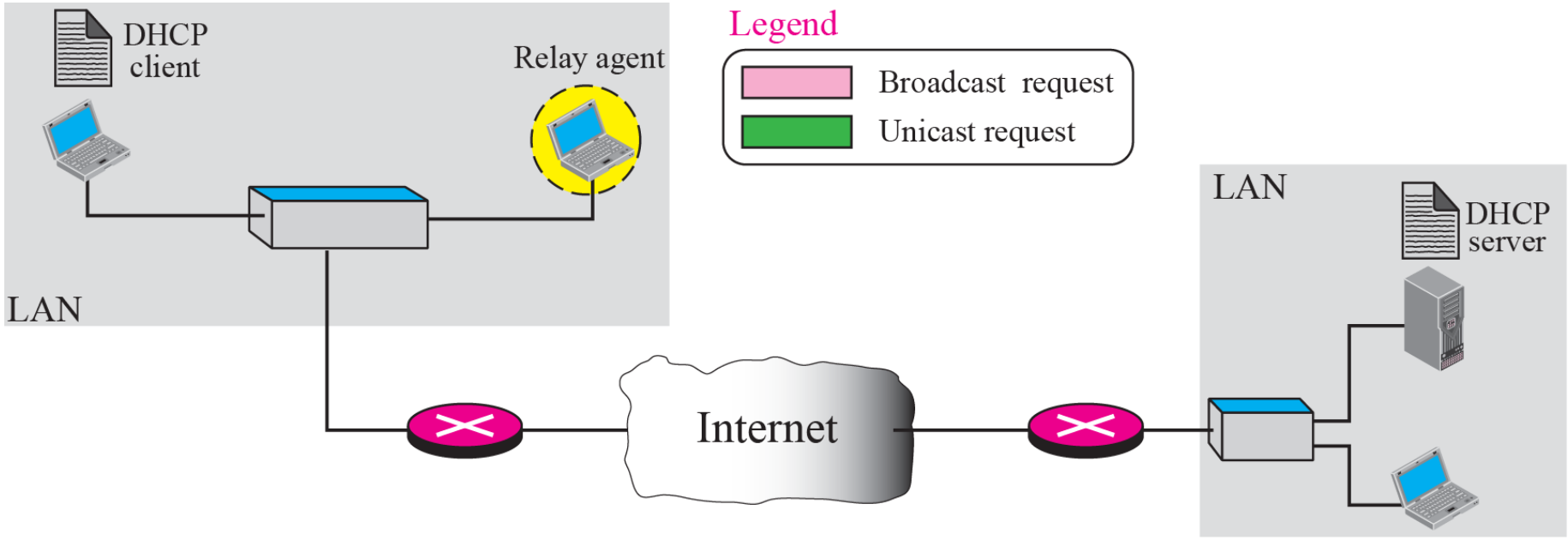
- Router listens on port 67, intercepts DHCP Discover message and forwards (**unicast**) the request to one or more DHCP servers.
  - places Router incoming IP address in the Router-address field
  - increments hop-count by 1
- DHCP server recognizes this request is coming from Router & not-the-client
  - sends **unicast** reply to the router
  - router replies to the client

Implementing Multiple DHCP Servers



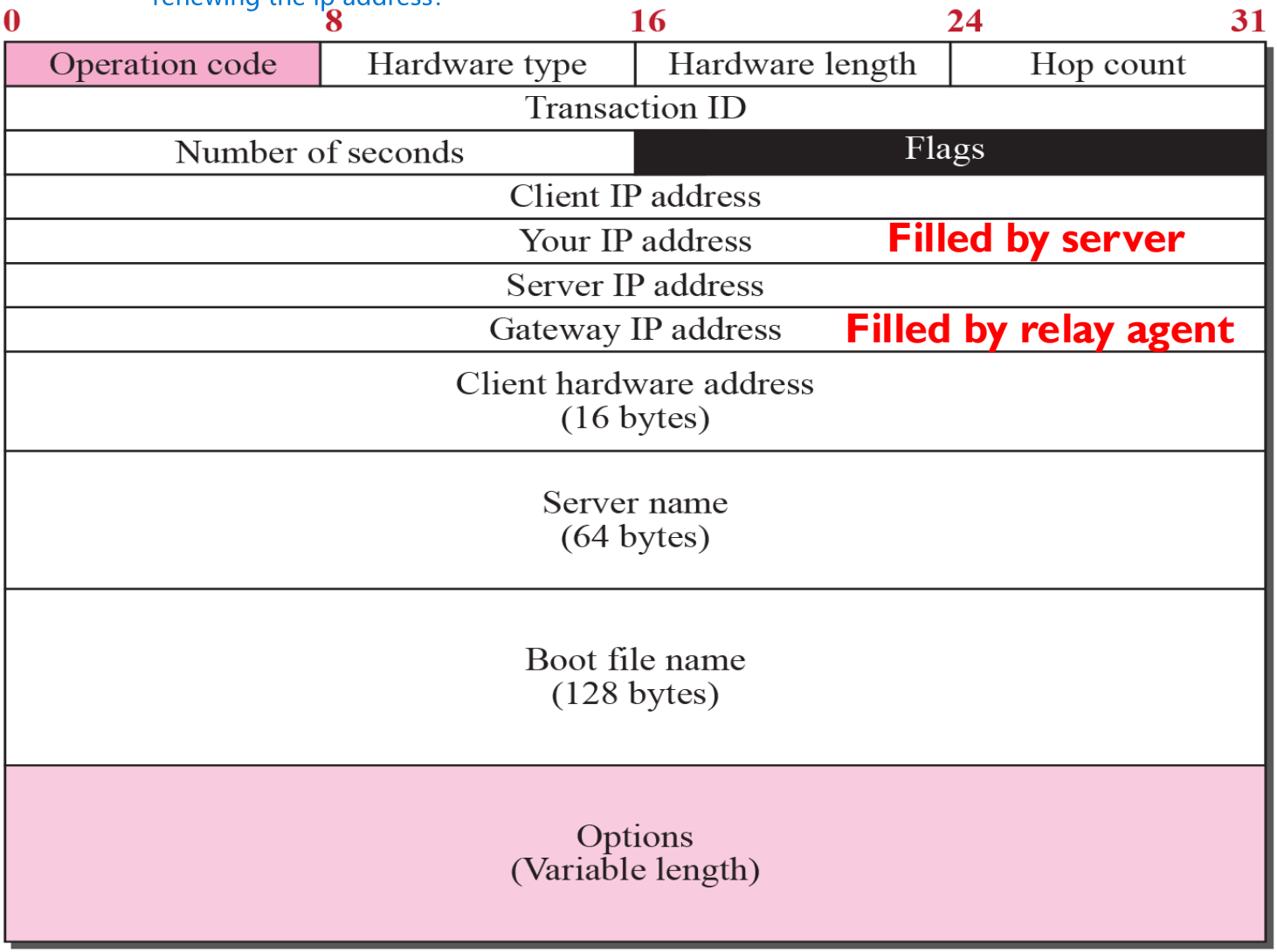
- Why do we need multiple DHCP servers?

DHCP through a Relay Agent – another eg.



DHCP packet format

renewing the ip address?



- HW: Find the purpose of the fields and the flags?

DHCP – Message format

- Field OP
  - Specifies whether the message is a request (1) or a reply (2).
- HTYPE and HLEN
  - Specify the network hardware type and length of the hardware address (e.g., Ethernet has type 1 and length 6).
- HOPS
  - Client places 0 in the HOPS field. The DHCP server increments the HOPS count by 1 if it decides to pass it to another server across a Router.
- Xid - Transaction ID
  - Contains an integer that machines use to match responses with requests.
- Seconds
  - number of seconds since the client started to boot.
- Flags
  - Flags for indicating **broadcast** and other reserved use

DHCP – Message format

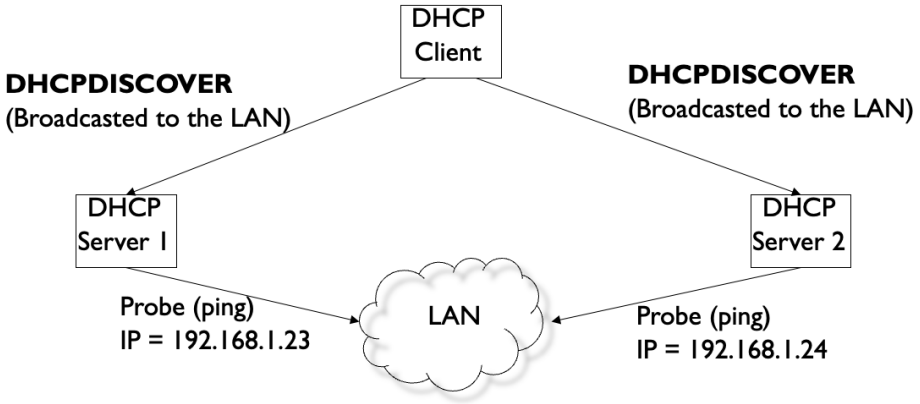
- Remaining fields:
  - To allow the greater flexibility, clients fill in as much information as they know and leave remaining fields set to zero.
  - e.g., if Server IP Address or Server Host Name are nonzero, only the server with matching address/name will answer the request; if they are zero, any server that receives the request will reply.

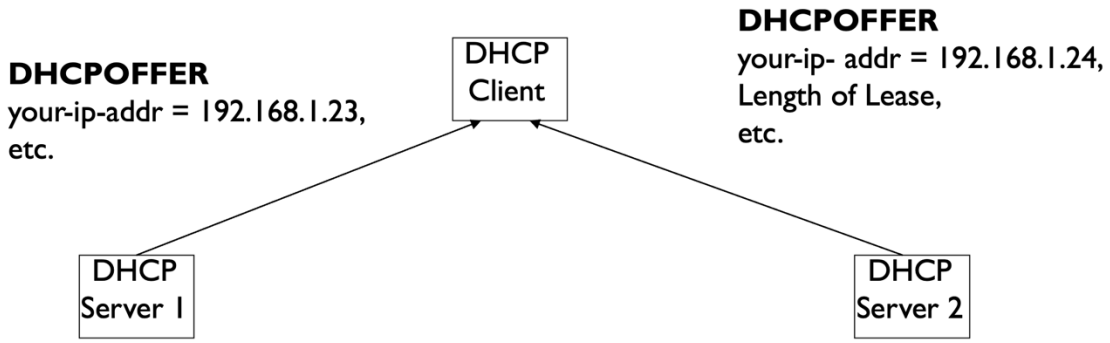
- Q: Why are there fields for Client IP and Your IP?

Question in Discussion Forum…

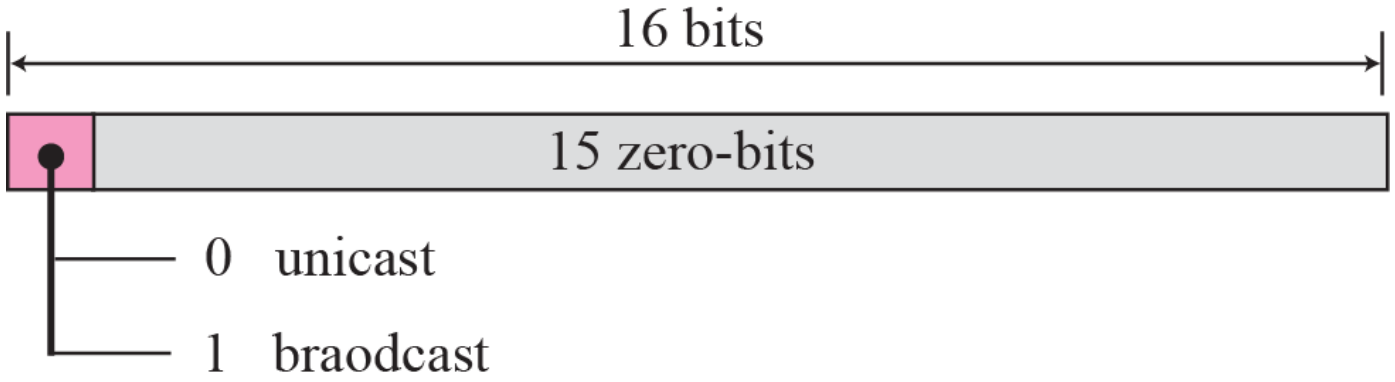
- Q: Should DHCP OFFER be a limited broadcast message or a unicast message? [Also applies to, DHCP ACK of the DHCP REQUEST]
  - Why is this question?

usually broadcast as At this stage, the client has no valid IP and might n yet be able to receive unicast frames addressed to its "offered" IP.At thi stage, the client has no valid IP and might not yet be able to receive un frames addressed to its "offered" IP.





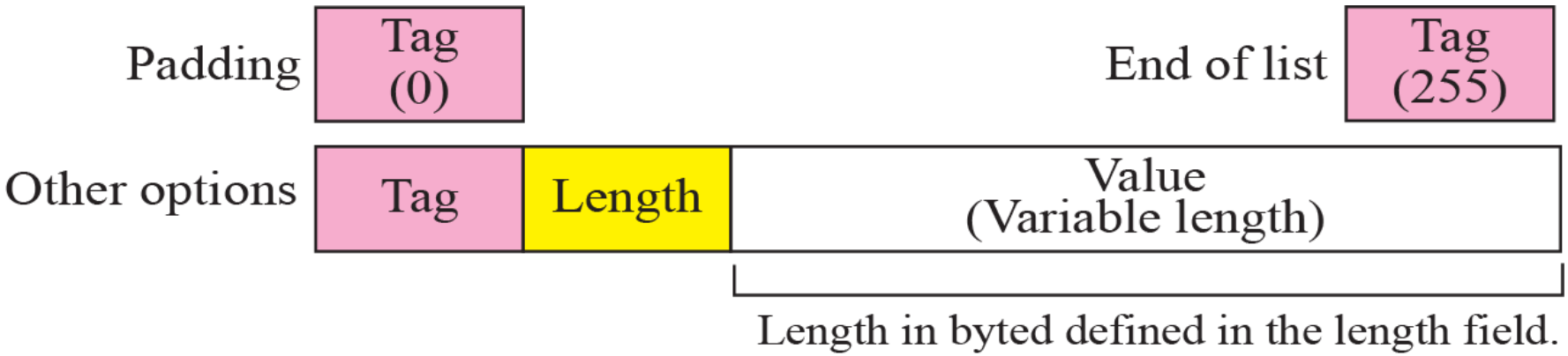
Flag format



- Only the left most bit is used. [for, Forced broadcast].
- When a client cannot accept unicast, it can ask the server to Broadcast reply by setting this bit to 1. [most clients set this bit to 1 by default]
- The remaining bits are 0's

Option format

- Used mostly in Reply message
- For "additional information to client" and "vendor specific information"



Tag = 0 → Is used for padding purposes.
Tag = 255 → Indicates end of **an option**.
For other Tag values refer:
https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml

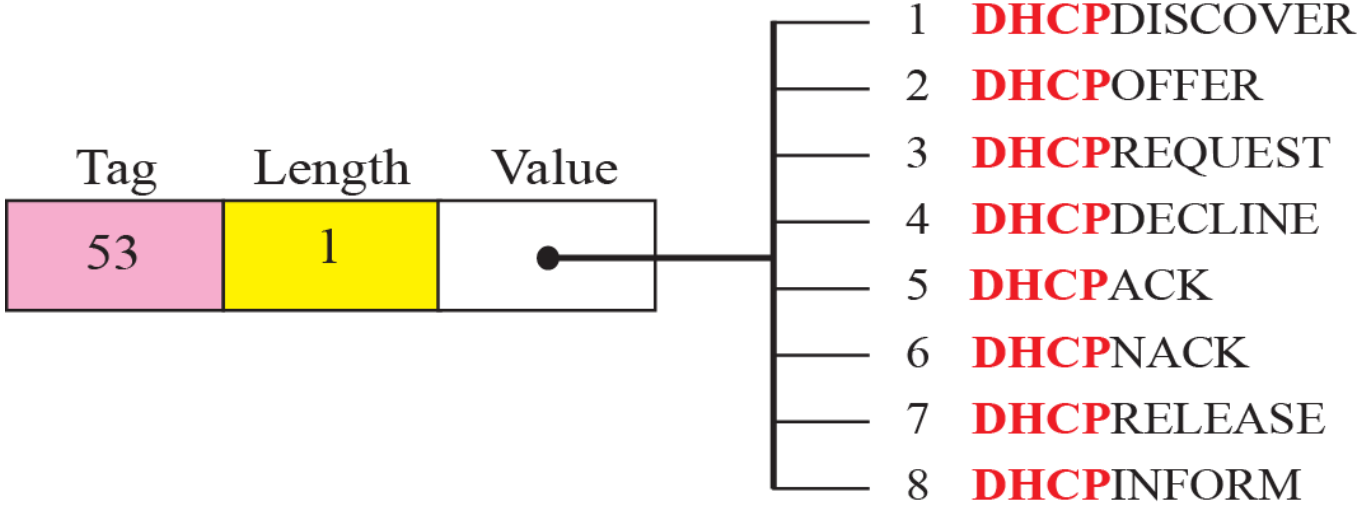
Option format – Padding Example. [for 8 byte word]

Tag	Len	Data	End	Pad	Pad	Pad	Pad
53	1	01	255	0	0	0	0

Explanation:

- **Tag (53)** = DHCP Message Type.
- **Len (1)** = 1 byte of data.
- **Data (01)** = e.g., Discover.
- **End (255)** = marks the end of options.
- **Pad (0)** = padding until the next 8-byte word boundary.

Option format



Tag = 1	Len = 4	Subnet Mask
1 byte	1 byte	4 bytes

Tag = 2	Len = 4	Time
1 byte	1 byte	4 bytes

Tag = 3	Len = 4	IP address of preferred GW
1 byte	1 byte	4 bytes

What is the value of Tag field that gives IP address lease time?

http://www.iana.org/assignments/bootp-dhcp-parameters/

DHCP – Server Design

- DHCP server stores a (key, value) pair for each client.
- Key used to identify a client.
- Default key = (IP- subnet number, hardware- address)

Key		Value	
IP-Subnet	**MAC-Address**	**IP-address assigned**	**Lease time**

- Address Conflict Avoidance
  - Servers may assign an address previously used by another client (address reuse).
    - Servers may choose the least recently used address.
    - Server should perform conflict detection using ICMP echo requests (ping).
    - Client should probe received address (e. g., with ARP).

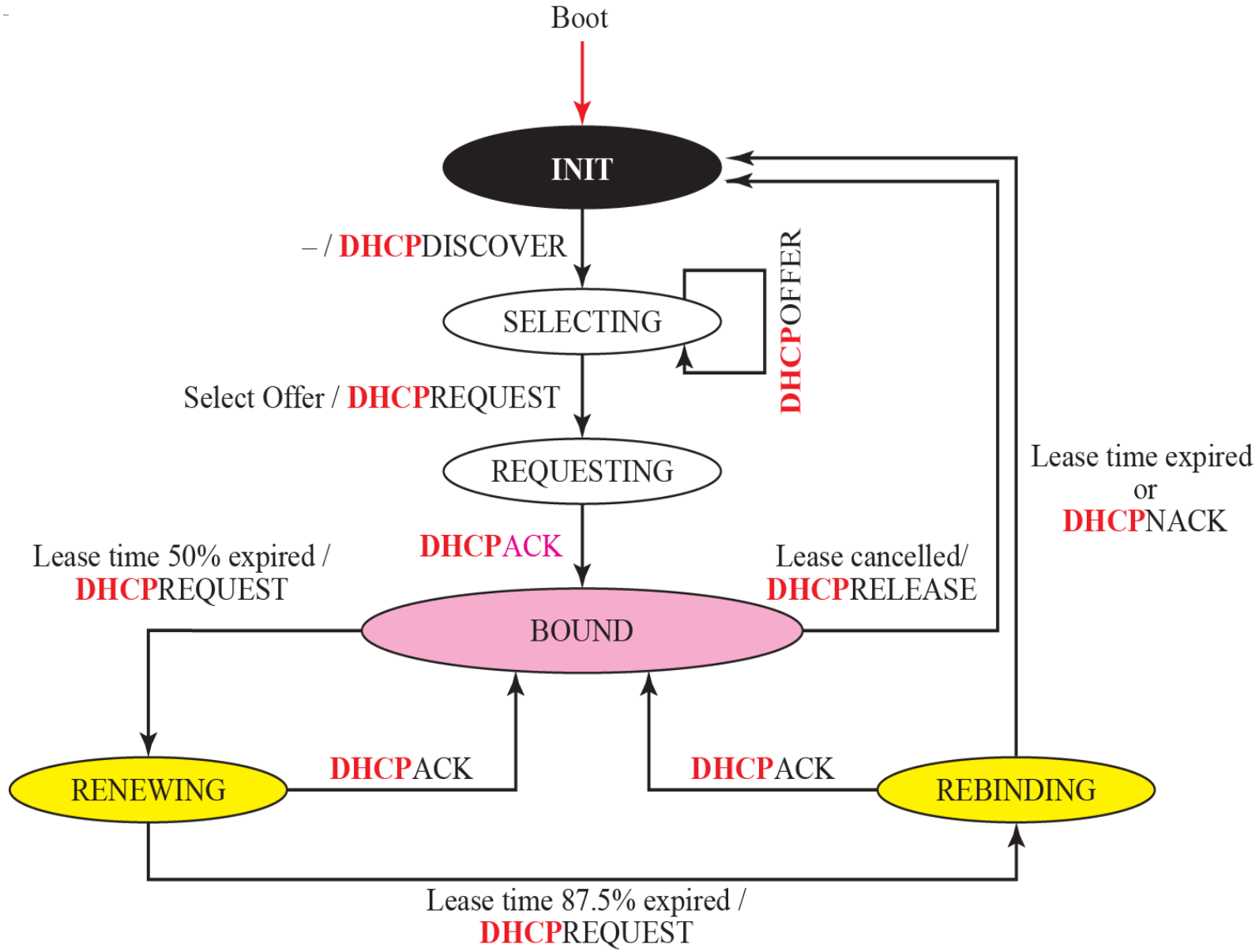
DHCP – Server Design

- TIME
  - Time represented in units of seconds.
  - 0xFFFFFFFF represents infinite time.
  - Time always expressed in relation to client's clock.
  - Client lease expiration time =

    Time when client sent DHCPREQUEST

    + lease duration in DHCPACK.

DHCP Client Design – Transition Diagram



DHCP Client – When does it renew?

- Timer Values
  - Renewal timer: → 50% of lease timeer Values
    - (DHCPREQUEST will be sent to Renew)
  - Rebinding timer: → 87.5% of lease time
    - (DHCPREQUEST will be sent to Renew)
  - Expiration timer: → 100% of lease time

Questions to Ponder

- When you are connected to the plug and play network (SPnP) and/or to the SoC network through a PC in the programming lab and/or to NUSNET wireless network, find out the following.
  - The DHCP server address
  - The lease time given by the DHCP server

- Is really DHCP required? Mac address (48 bits) is unique. Why can't we use this itself as IP address or derive a 32 bit IP address from this.
- What is DHCP FORCERENEW? What is the use of it? Refer to RFC 3203

DHCP Snooping– Discuss in Discord forum

DHCP snooping is a security feature implemented on network switches that helps prevent unauthorized or rogue DHCP servers from assigning IP addresses to devices within a network. It acts as a firewall between untrusted hosts and the DHCP server, ensuring that only legitimate DHCP transactions occur.

- Q: How DHCP Snooping Works?
- Q: What are the advantages of enabling DHCP Snooping in switches?

Activities ….. Next Week

- Lab Sessions Starts – Next Week @ **COM1-B1-02 (Data Comm Lab 1)**
- Read the "Labs Intro" and familiarise yourself with the Lab Setting.
- Read the "Lab Sheet" at least once before you come to each Lab session.
- Assignment 1 will be out today.
- Learning Activities (Every Week) –
  - In-class online quiz **[Pls login to Pollev**, before answering questions]
  - Discord discussion forum for clarifications & to discuss new topics

THE END

Attendance

- https://inetapps.nus.edu.sg/ctr/