Dynamic Address Configuration

- Each computer that is attached to the internet must have the following information:
  - IP address
  - Subnet mask
  - IP address of a router
  - IP address of a name server
- This information is usual stored in a configuration file and accessed by the computer during bootstrap process.

Q: How does a *host* get IP address?

- hard-coded by system admin in a file
  - Windows: control-panel->network->configuration->tcp/ip->properties
  - UNIX: /etc/rc.config

- DHCP: Dynamic Host Configuration Protocol: dynamically get address from as server
  - "plug-and-play

DHCP – Dynamic Host Configuration Protocol

- DHCP is a protocol design to provide the information dynamically.
- DHCP assign address to a host dynamically.
- DHCP is client server program
- Basically DHCP has two databases
  - Database statically binds physical addresses to IP addresses.
  - Database dynamically makes DHCP dynamic
- When a DHCP client request temporary IP address the DHCP server goes to the pool of available unused IP addresses and assign an IP for a negotiable period of time.
- DHCP server first check its static database

DHCP – Dynamic Host Configuration Protocol

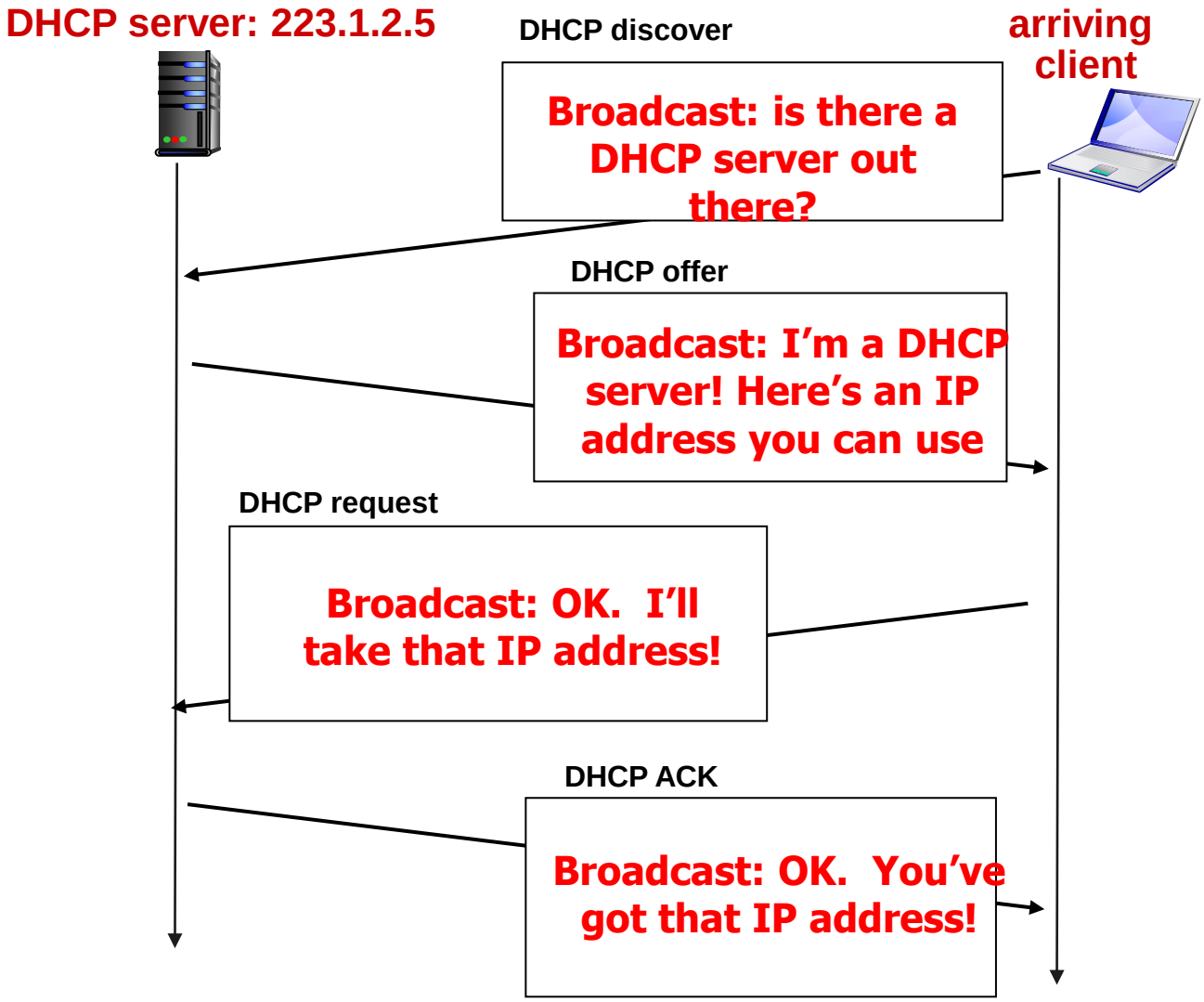
goal: allow host to *dynamically* obtain its IP address from network server when it joins network

- can renew its lease on address in use
- allows reuse of addresses (only hold address while connected/"on")
- support for mobile users who want to join network (more shortly)

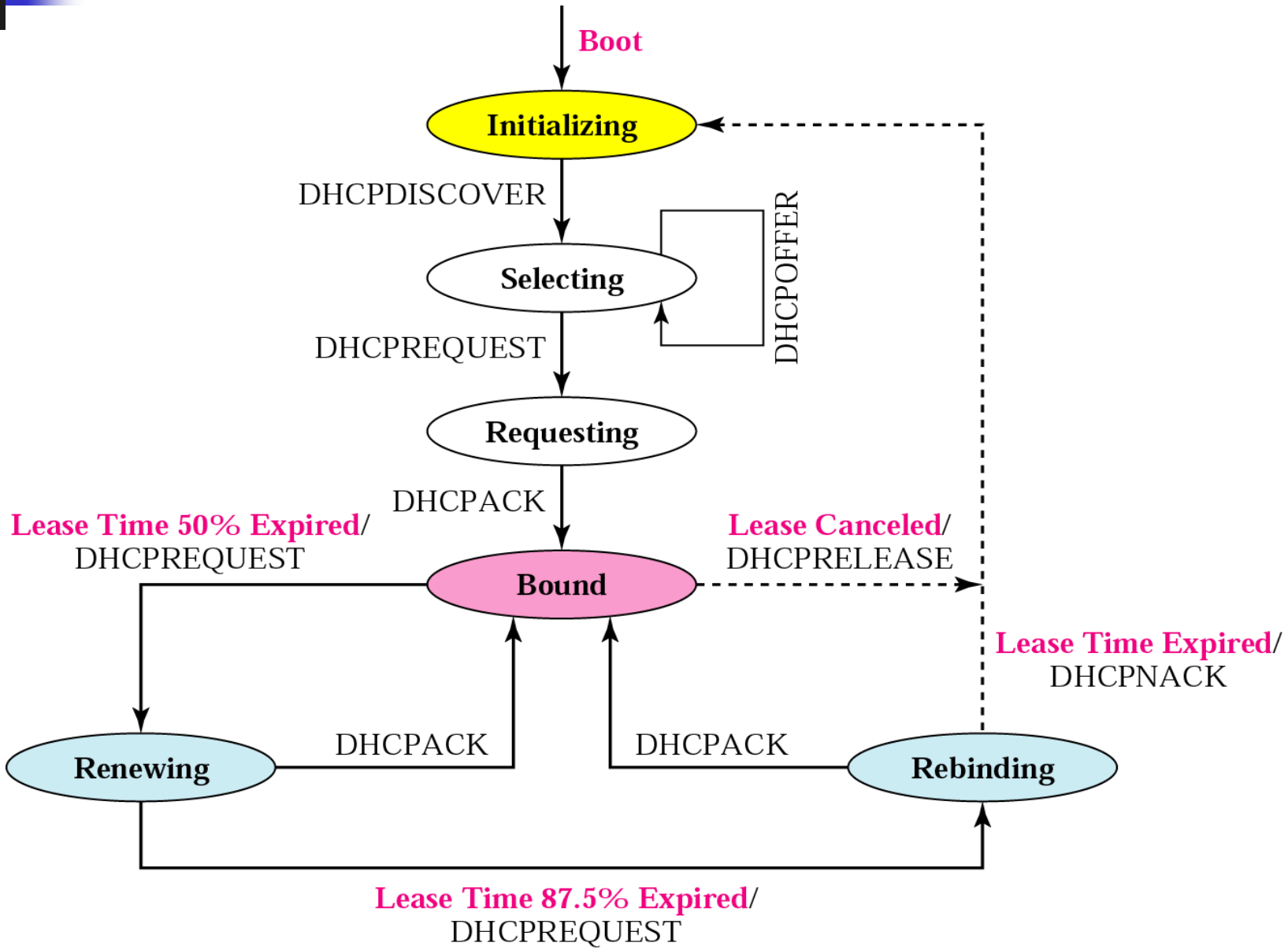
DHCP overview:

- host broadcasts "DHCP discover" msg [optional]
- DHCP server responds with "DHCP offer" msg [optional]
- host requests IP address: "DHCP request" msg
- DHCP server sends address: "DHCP ack" msg

DHCP client-server scenario



DHCP transition diagram



DHCP States

- 1. **Initializing state:**
  - The client broadcasts a DHCP_DISCOVER message on its local physical subnet.
  - The DHCP_DISCOVER message may include options that suggest values for the network address and lease duration.
  - BOOTP relay agents may pass the message on to DHCP servers not on the same physical subnet.

- 2. **Selecting State**
  - Each server may respond with a DHCP_OFFER message that includes an available IP address and a lease duration (default 1hour).
  - The server that sends a DHCP_OFFER lock the offered IP address so that it is not available to any other clients.
  - The client chooses one of the offers and sends DHCP_REQUEST message to the selected server.
  - If the client receive no DHCP_OFFER message it tries fore more times, each with a span of 2 sec.
  - If there is no reply to any of these DHCP_DISCOVER the client sleep for 5 min before trying again.

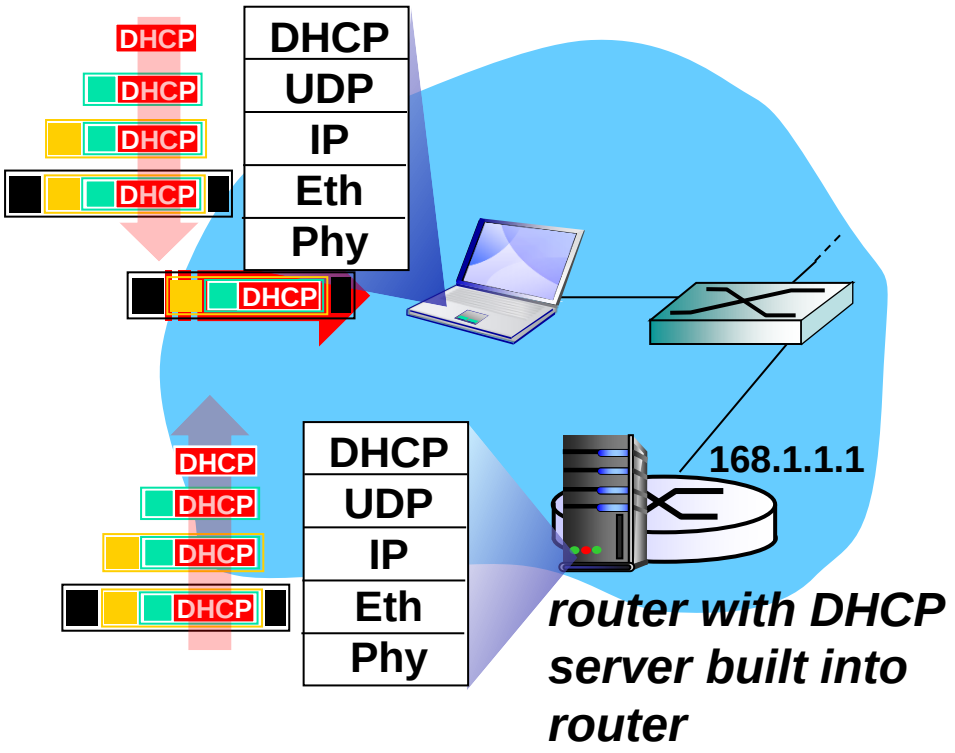
DHCP States cont'

- **3 Requesting State**
  - The client remains in the requesting state until it receives a DHCP_ACK message from the server which creates the binding between the client's physical address and its IP address.
- **4 Bound State**
  - The client use the IP address until the lease expire. When 50% of the lease period is reached the client sends another DCHP_REQUEST to ask for renewal.
- **5 Renewing State**
  - The client remains in the renewing state
  - If receives a DHCP_ACK renew the lease agreement. Reset the timer and goes back to the bound state
  - If DHCP_ACK is not received and 87.5% of the lease time expire the client goes to the rebinding state
- **6 Rebinding State**
  - If receives DHCP_NACK or the lease time expires , the client goes back to the Initializing State
  - IF receives DHCP_ACK it goes to the bound state and reset the timer.

DHCP messages

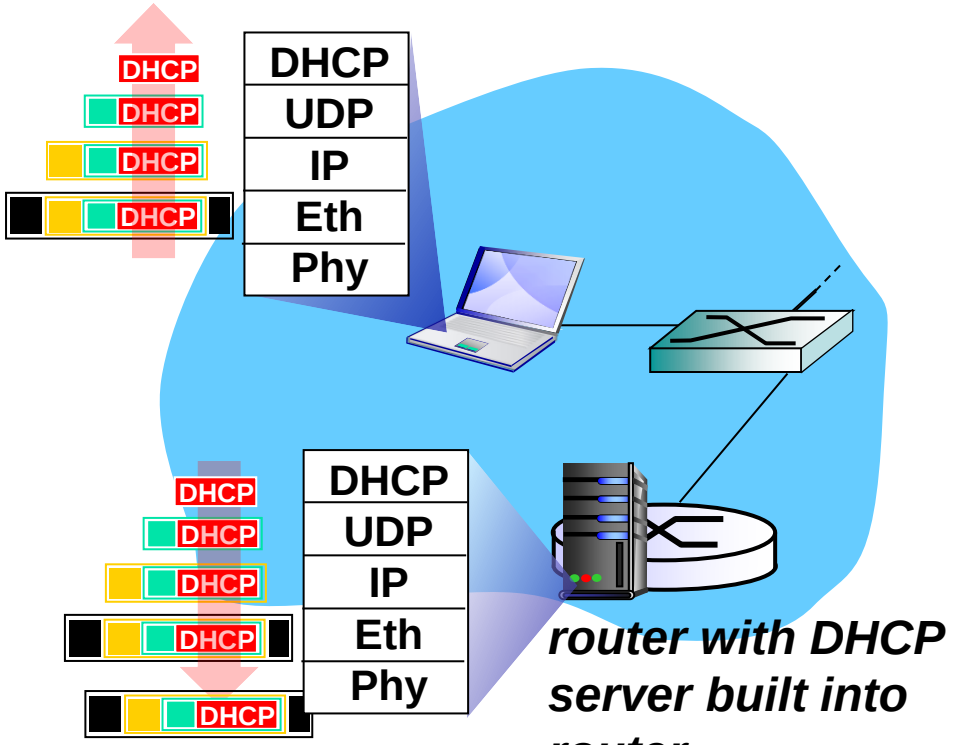
- DHCP_DISCOVER - Client broadcast to locate available servers.
- DHCP_OFFER - Server to client in response to DHCP_DISCOVER with offer of configuration parameters.
- DHCP_REQUEST - Client broadcast to servers requesting offered parameters from one server and implicitly declining offers from all others.
- DHCP_ACK - Server to client with configuration parameters, including committed network address.
- DHCP+NACK - Server to client refusing request for configuration parameters (e.g., requested network address already allocated).
- DHCP_DECLINE - Client to server indicating configuration parameters (e.g., network address) invalid.
- DHCP_RELEASE - Client to server relinquishing network address and canceling remaining lease.

DHCP: example



- connecting laptop needs its IP address, addr of first-hop router, addr of DNS server: use DHCP
- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.1 Ethernet
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server
- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

DHCP: example



- DCP server formulates DHCP ACK containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
  - encapsulation of DHCP server, frame forwarded to client, demuxing up to DHCP at client
  - client now knows its IP address, name and IP address of DSN server, IP address of its first-hop router

DHCP: Wireshark output (home LAN)

request

Message type: Boot Request (1)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0 (0.0.0.0)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 0.0.0.0 (0.0.0.0)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP Request
Option: (61) Client identifier
    Length: 7; Value: 010016D323688A;
    Hardware type: Ethernet
    Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Option: (t=50,l=4) Requested IP Address = 192.168.1.101
Option: (t=12,l=5) Host Name = "nomad"
Option: (55) Parameter Request List
    Length: 11; Value: 010F03062C2E2F1F21F92B
    1 = Subnet Mask; 15 = Domain Name
    3 = Router; 6 = Domain Name Server
    44 = NetBIOS over TCP/IP Name Server
    ……

reply

Message type: Boot Reply (2)
Hardware type: Ethernet
Hardware address length: 6
Hops: 0
Transaction ID: 0x6b3a11b7
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.101 (192.168.1.101)
Your (client) IP address: 0.0.0.0 (0.0.0.0)
Next server IP address: 192.168.1.1 (192.168.1.1)
Relay agent IP address: 0.0.0.0 (0.0.0.0)
Client MAC address: Wistron_23:68:8a (00:16:d3:23:68:8a)
Server host name not given
Boot file name not given
Magic cookie: (OK)
Option: (t=53,l=1) DHCP Message Type = DHCP ACK
Option: (t=54,l=4) Server Identifier = 192.168.1.1
Option: (t=1,l=4) Subnet Mask = 255.255.255.0
Option: (t=3,l=4) Router = 192.168.1.1
Option: (6) Domain Name Server
    Length: 12; Value: 445747E2445749F244574092;
    IP Address: 68.87.71.226;
    IP Address: 68.87.73.242;
    IP Address: 68.87.64.146
Option: (t=15,l=20) Domain Name = "hsd1.ma.comcast.net."

Internet Assigned Number Authority

- The commercialization of the Internet, however, has consumed nearly all of the unique TCP/IP address space. The fact that nearly all private and public entities are moving to establish an Internet connection has created a serious IP address shortage.
- The Internet Assigned Number Authority (IANA), the organization responsible for resolving the problem, proposed to conserve the unique addressing space by blocking out (reserving) a large addressing space (private space) that may be replicated in multiple private local area networks (LANs).
- This pool of set-aside addresses would also be non-routable on the Internet.