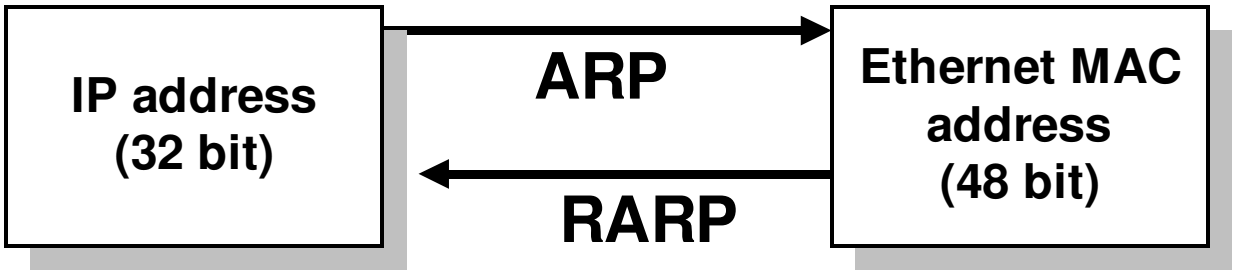
Dynamic Host Configuration Protocol (DHCP)

Dynamic Assignment of IP addresses

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

Solutions for dynamic assignment of IP addresses

- **Reverse Address Resolution Protocol (RARP)**
  - Works similar to ARP
  - Broadcast a request for the IP address associated with a given MAC address
  - RARP server responds with an IP address
  - Only assigns IP address (not the default router and subnetmask)



BOOTP

The Bootstrap Protocol (BOOTP) is a client/server protocol that configures a diskless computer or a computer that is booted for the first time. BOOTP provides the

IP address

net mask

the address of a default router

the address of a name server.

BOOTP is static. When a client workstation asks for the above info, it is retrieved from a fixed table. Every time the client asks for the info, it gets the same results.

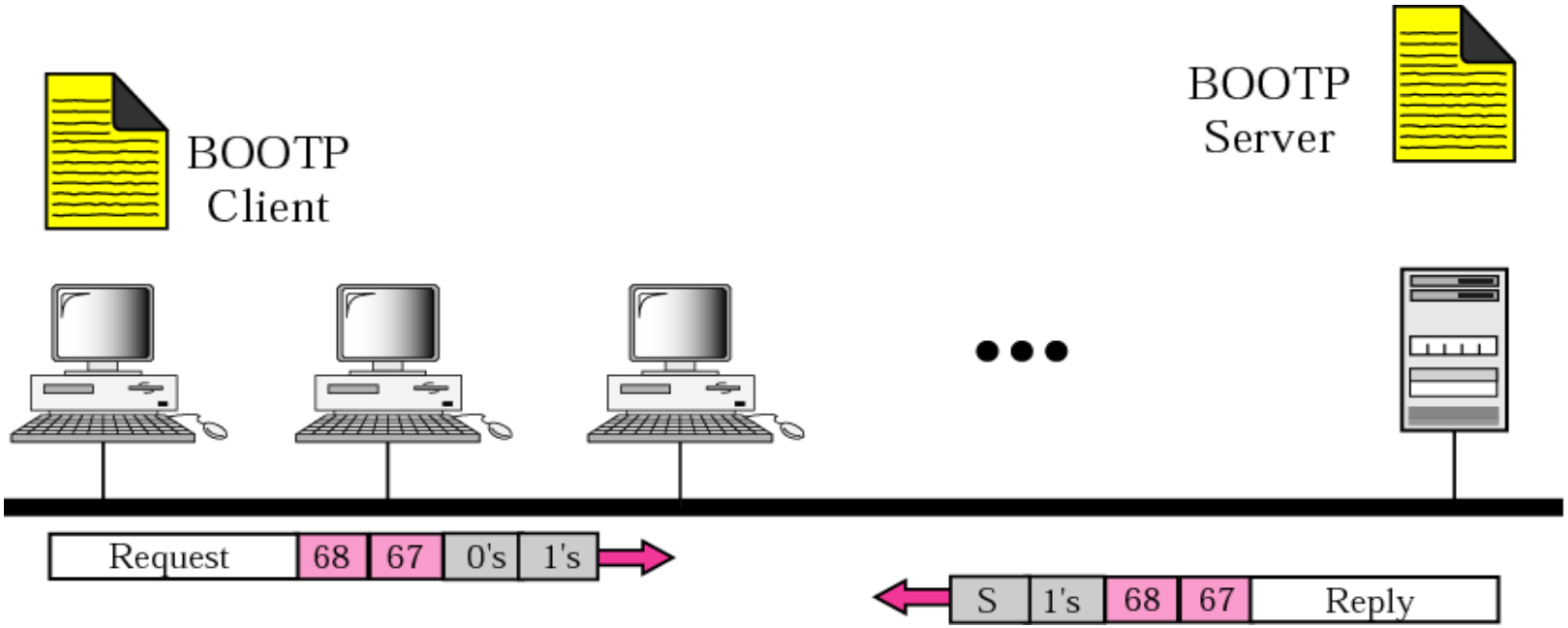
BOOTP

- **BOOTstrap Protocol (BOOTP)**
  - From 1985
  - Host can configure its IP parameters at boot time.
  - 3 services.
    - IP address assignment.
    - Detection of the IP address for a serving machine.
    - The name of a file to be loaded and executed by the client machine (boot file name)

  - Not only assigns IP address, but also default router, network mask, etc.
  - Sent as UDP messages (UDP Port 67 (server) and 68 (host))
  - Use limited broadcast address (255.255.255.255):
    - These addresses are never forwarded

BOOTP

The BOOTP server can be on the same network as the BOOTP client or on different networks.



BOOTP places its packet inside a UDP packet (note that BOOTP is an application layer program).

Client and Server on the Same Network

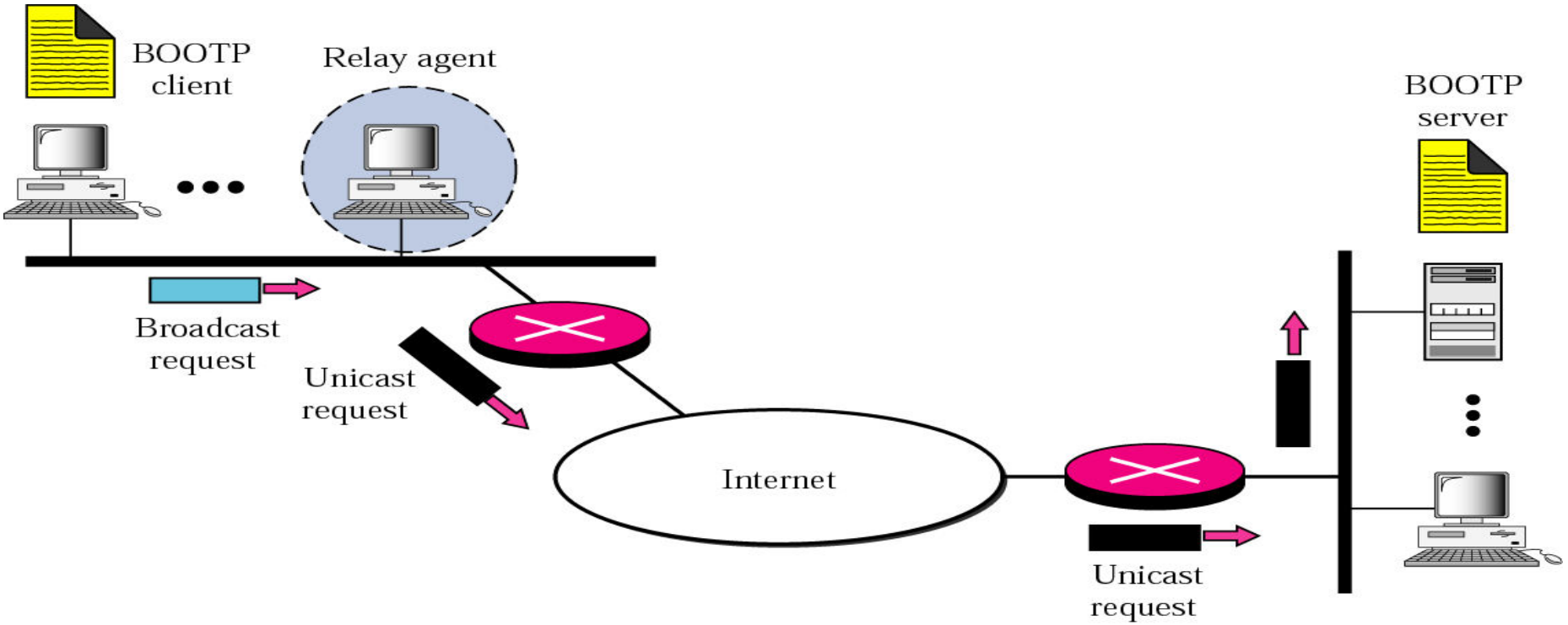
- **The BOOTP server issues a passive open command on UDP port number 67 and waits for a client.**

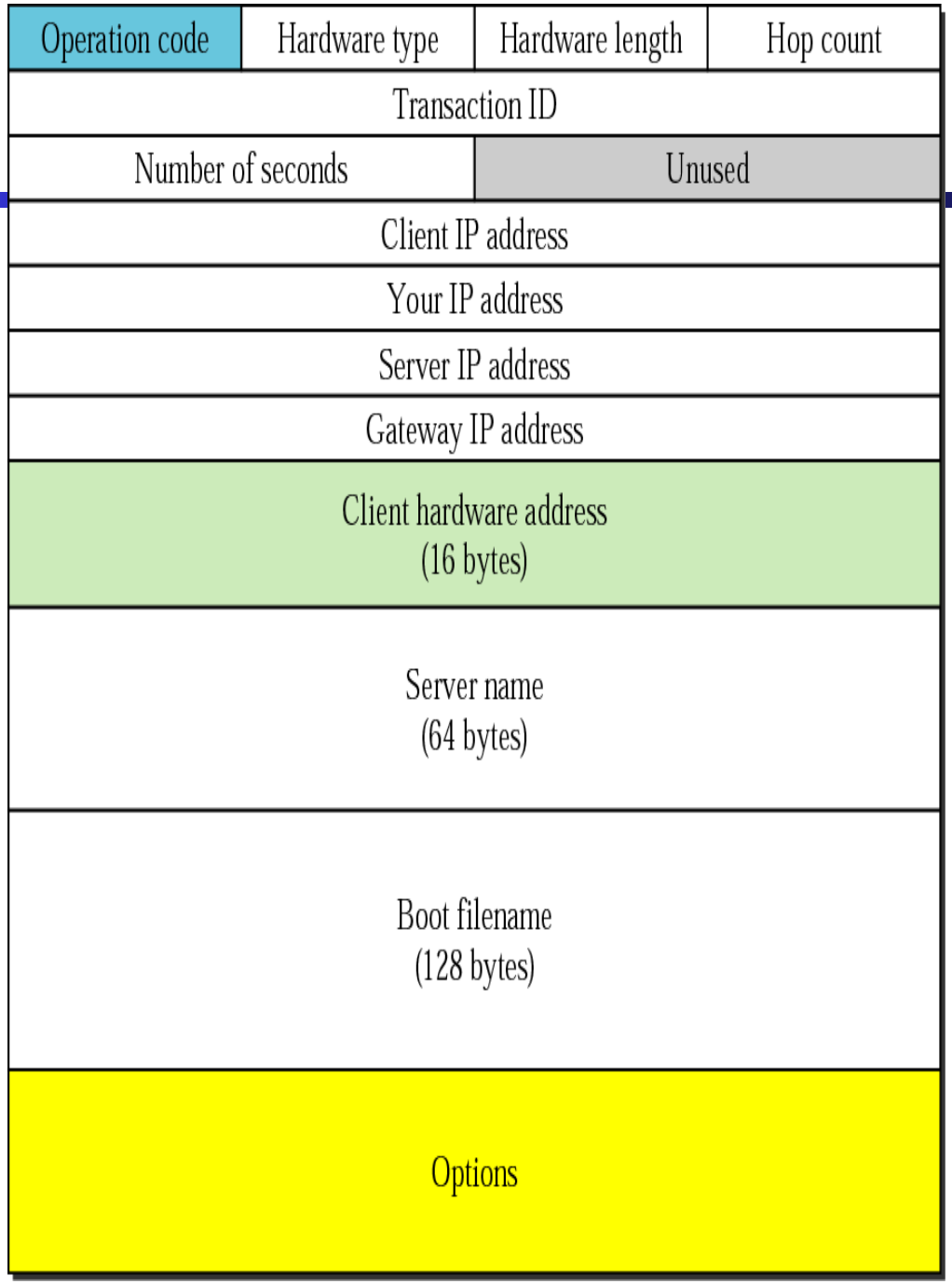
- **A booted client issues an active open command on port number 68. The message is encapsulated in a UDP user datagram and then in an IP packet. In the IP packet the source address is all 0s and the destination address is all 1s.**

- **Server responds with a UDP datagram source port 67 and destination port 68. Can also bypass ARP since server also knows the MAC address of the client.**

Client and Server on Different Network

When client and server are on different networks, we need a relay agent, because client does not know IP address of server, and a limited broadcast address gets dumped by the local router. Relay agent knows the IP addr of the server.





Operation code: request=1, reply=2
Hardware type: Ethernet=1
Hardware len: Ethernet=6
Transaction ID: identifies the BOOTP request/reply
Number seconds:how many seconds elapsed since the client started to boot.
Client hardware address: can be supplied by the client but is usually supplied by the server.
Server name: optional
Boot filename: optional, contains the full pathname of the boot file (contains other booting information).

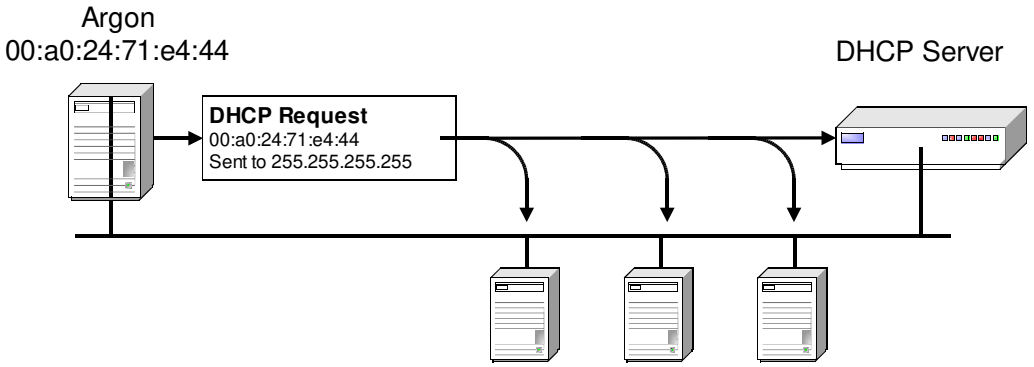
DHCP

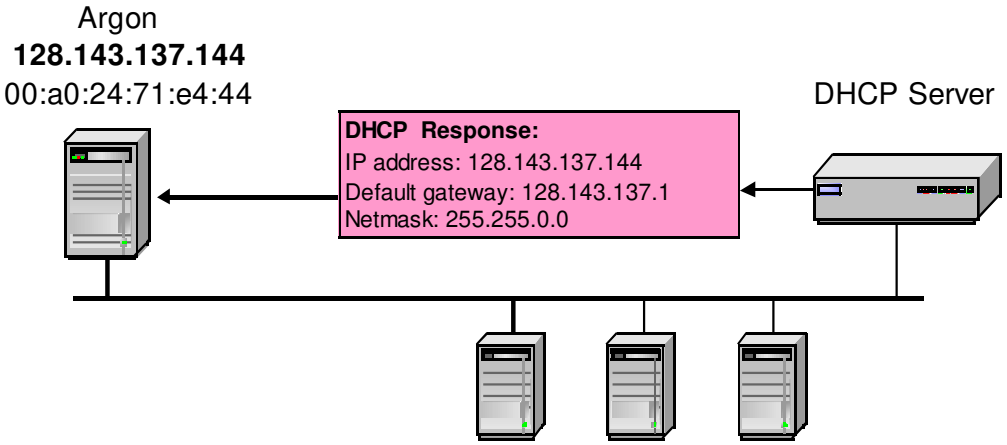
- **Dynamic Host Configuration Protocol (DHCP)**
  - From 1993
  - An extension of BOOTP
  - Same port numbers as BOOTP
  - Extensions:
    - Supports temporary allocation (“leases”) of IP addresses
    - DHCP client can acquire all IP configuration parameters needed to operate
  - DHCP is the preferred mechanism for dynamic assignment of IP addresses
  - DHCP can interoperate with BOOTP clients.

Key Ideas

- Broadcasting: when in doubt, shout!
  - Broadcast query to all hosts in the local-area-network
  - … when you don't know how to identify the right one
- Caching: remember the past for a while
  - Store the information you learn to reduce overhead
  - Remember your own address & other host's addresses
- Soft state: eventually forget the past
  - Associate a time-to-live field with the information
  - … and either refresh or discard the information
  - Key for robustness in the face of unpredictable change

DHCP Interaction (simplified)

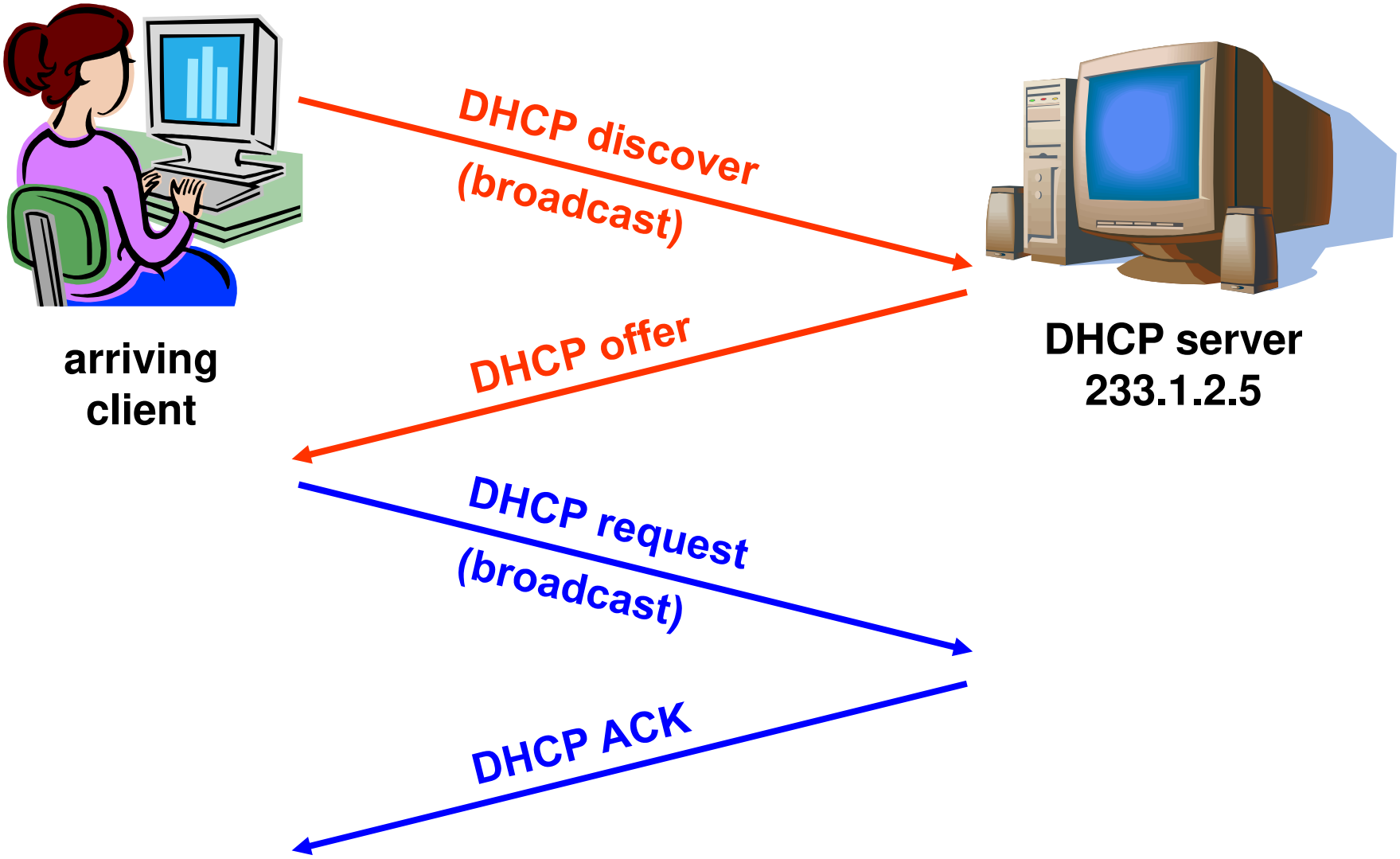




Response from DHCP Server

- DHCP “offer message” from the server
  - Configuration parameters (proposed IP address, mask, gateway router, DNS server, ...)
  - Lease time (the time the information remains valid)
- Multiple servers may respond
  - Multiple servers on the same broadcast media
  - Each may respond with an offer
  - The client can decide which offer to accept
- Accepting one of the offers
  - Client sends a DHCP request echoing the parameters
  - The DHCP server responds with an ACK to confirm
  - … and the other servers see they were not chosen

Dynamic Host Configuration Protocol



Deciding What IP Address to Offer

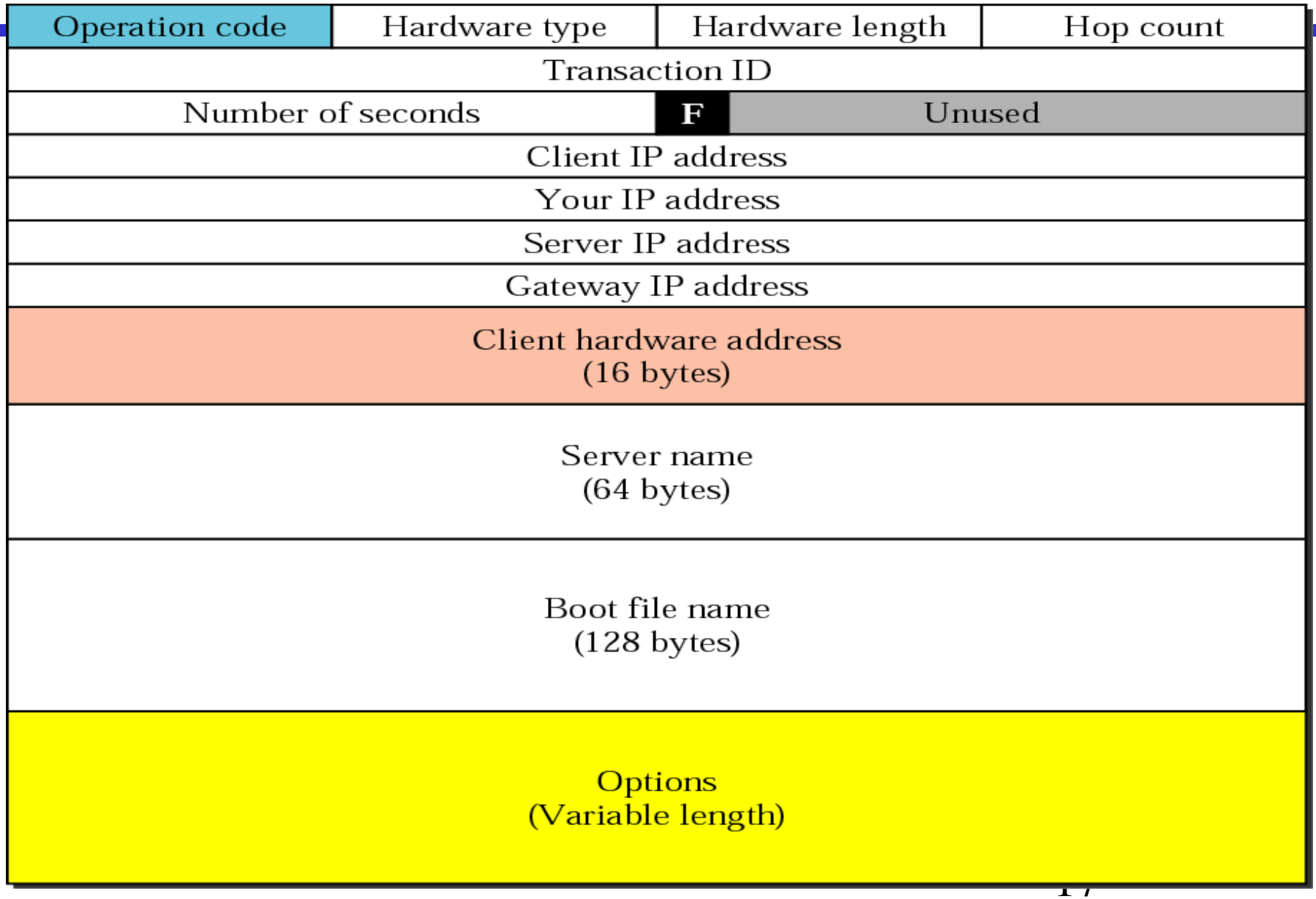
- Server as centralized configuration database
  - All parameters are statically configured in the server
  - E.g., a dedicated IP address for each MAC address
  - Avoids complexity of configuring hosts directly
  - … while still having a permanent IP address per host
- Or, dynamic assignment of IP addresses
  - Server maintains a pool of available addresses
  - … and assigns them to hosts on demand
  - Leads to less configuration complexity
  - … and more efficient use of the pool of addresses
  - Though, it is harder to track the same host over time

Soft State: Refresh or Forget

- Why is a lease time necessary?
  - Client can release the IP address (DHCP RELEASE)
    - E.g., “ipconfig /release” at the DOS prompt
    - E.g., clean shutdown of the computer
  - But, the host might not release the address
    - E.g., the host crashes
    - E.g., buggy client software
  - And you don’t want the address to be allocated forever

- Performance trade-offs
  - Short lease time: returns inactive addresses quickly
  - Long lease time: avoids overhead of frequent renewals

DHCP Message Format



Message Fields

- code: Indicates a request or a reply
  - 1 Request
  - 2 Reply
- HWtype: The type of hardware, for example:
  - 1 Ethernet
  - 6 IEEE 802 networks
- length: Hardware address length in bytes. E.g., Ethernet and token-ring both use 6 bytes.
- hops: The client sets this to 0. It is incremented by a router that relays the request to another server and is used to identify loops. RFC 951 suggests that a value of 3 indicates a loop.

Contd.

- Transaction ID: A random number used to match this boot request with the response it generates.
- Seconds: Set by the client. It is the elapsed time in seconds since the client started its boot process.
- Flags field: The most significant bit of the flags field is used as a broadcast flag. All other bits must be set to zero, and are reserved for future use.
  - Normally, DHCP servers attempt to deliver DHCP messages directly to a client using unicast delivery.
  - The destination address in the IP header is set to the DHCP "*your IP address"* and the MAC address is set to the DHCP *client hardware address*.
  - If a host is unable to receive a unicast IP datagram until it knows its IP address, then this broadcast bit must be set (=1) to indicate to the server that the DHCP reply must be sent as an IP and MAC broadcast. Otherwise this bit must be set to zero.

Contd.

- Client IP address: Set by the client. Either its known IP address, or 0.0.0.0.
- Your IP address: Set by the server if the client IP address field was0.0.0.0.
- Server IP address: Set by the server.
- Router IP address: This is the address of a BOOTP relay agent, *not* a general IP router to be used by the client. It is set by the forwarding agent when BOOTP forwarding is being used
- Client hardware address: Set by the client. DHCP defines a client identifier option that is used for client identification. If this option is not used the client is identified by its MAC address.

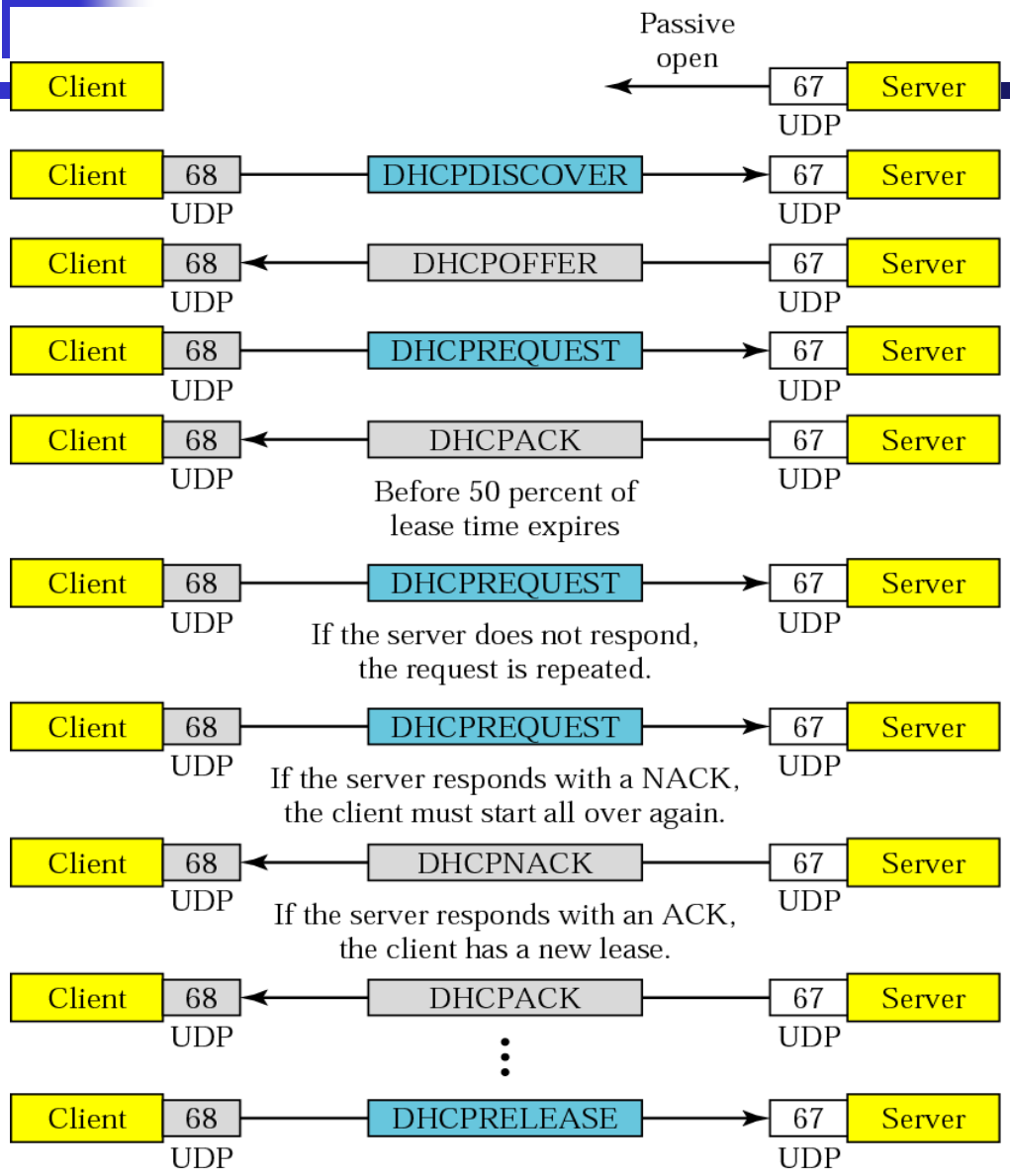
Contd.

- Server host name: Optional server host name terminated by X'00'.
- Boot file name: The client either leaves this null or specifies a generic name, such as router, indicating the type of boot file to be used. In a DHCPDISCOVER request this is set to null. The server returns a fully qualified directory path name in a DHCPOFFER request. The value is terminated by X'00'.
- Options: Subnet Mask, Name Server, Hostname, Domain Name, Forward On/Off, Default IP TTL, Broadcast Address, Static Route, Ethernet Encapsulation, X Window Manager, X Window Font, DHCP Msg Type, DHCP Renewal Time, DHCP Rebinding, Time SMTP-Server, SMTP-Server, Client FQDN, Printer Name, …

DHCP Message Type

- Message type is sent as an option.

Value	Message Type
1	DHCPDISCOVER
2	DHCPOFFER
3	DHCPREQUEST
4	DHCPDECLINE
5	DHCPACK
6	DHCPNAK
7	DHCPRELEASE
8	DHCPINFORM



Discover: client tries to find out what servers are out there.

Offer: those servers that can provide this service respond

Request: client selects one offer and makes a request

ACK: server acks the request

When 50% of the lease period is expired, client asks for a renewal.

If ACK received, reset timer. If NAK, go back to intializing state.

Message Types

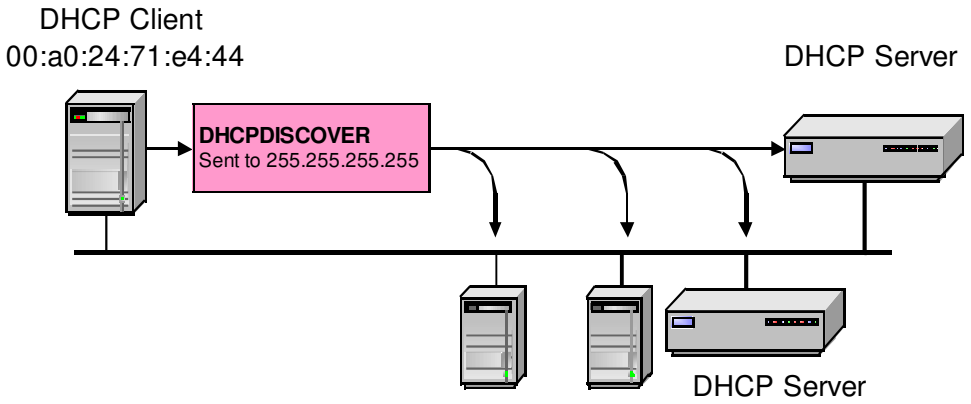
- DHCPDISCOVER: Broadcast by a client to find available DHCP servers.
- DHCPOFFER: Response from a server to a DHCPDISCOVER and offering IP address and other parameters.
- DHCPREQUEST: Message from a client to servers that does one of the following:
  - Requests the parameters offered by one of the servers and declines all other offers.
  - Verifies a previously allocated address after a system or network change (a reboot for example).
  - Requests the extension of a lease on a particular address.

Contd.

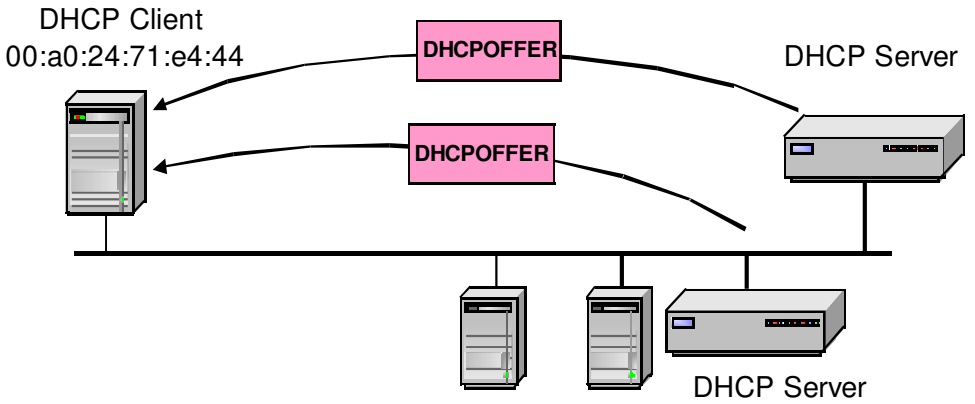
- DHCPACK: Acknowledgement from server to client with parameters,
- including IP address.
- DHCPNACK: Negative acknowledgement from server to client, indicating that the client's lease has expired or that a requested IP address is incorrect.
- DHCPDECLINE: Message from client to server indicating that the offered address is already in use.
- DHCPRELEASE: Message from client to server canceling remainder of a lease and relinquishing network address.
- DHCPINFORM: Message from a client that already has an IP address (manually configured for example), requesting further configuration parameters from the DHCP server.

DHCP Operation

- DCHP DISCOVER



- DCHP OFFER



The Discover Packet

- During the DHCP Discovery process, the client broadcasts a Discover packet that identifies the client's hardware address
- If the DHCP client was on the network before, the client also defines a preferred address—typically the client prefers the last address it used
- In the DHCP Discover packet, the Message Type value is one—this indicates that this packet is a DHCP Discover packet
- The Client Identifier field value is based on the client's hardware address

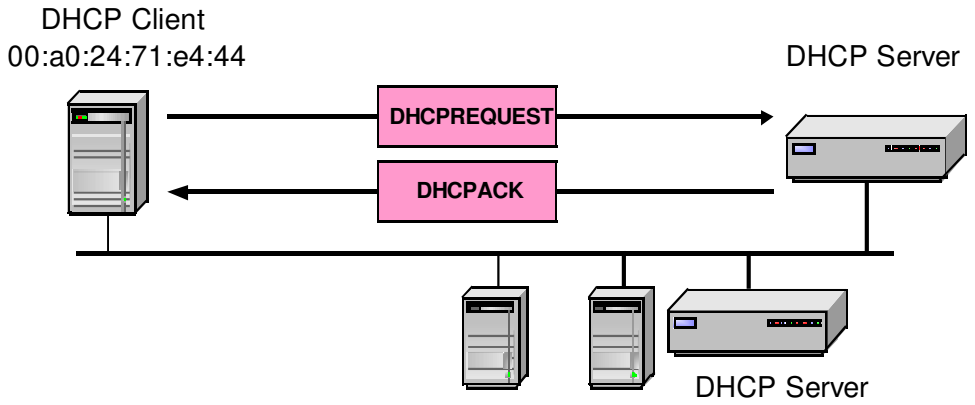
The Offer Packet

- The DHCP server sends the Offer packet to offer an IP address to the DHCP client
  - (your IP address)
- The Offer packet includes the IP address that is offered to the client, and sometimes answers to the requested options in the DHCP Discover packet
- The servers record the address as offered to the client to prevent the same address being offered to other clients in the event of further DHCPDISCOVER messages being received before the first client has completed its configuration.

DHCP Operation

- DCHP DISCOVER

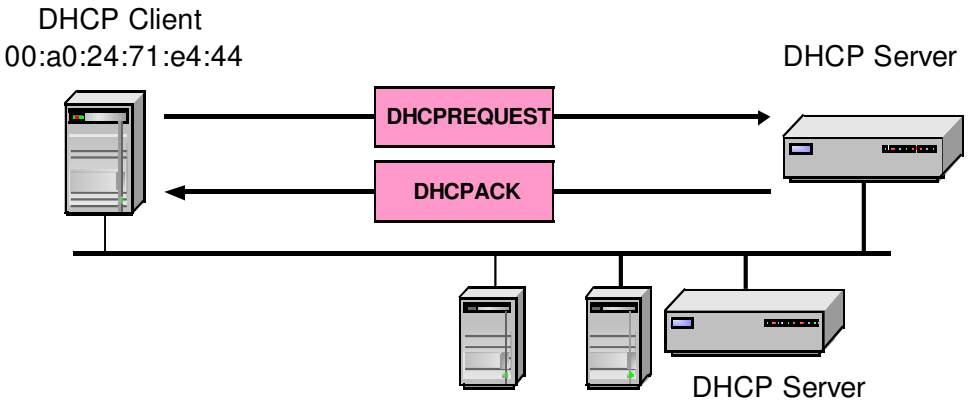
At this time, the DHCP client can start to use the IP address



- Renewing a Lease

(sent when 50% of lease has expired)

If DHCP server sends DHCPNACK, then address is released.



The Request Packet

- Once the Offer packet is received, the client can either accept the offer by issuing a DHCP Request packet, or reject the offer by sending a DHCP Decline packet

- The client chooses one based on the configuration parameters offered and broadcasts a DHCPREQUEST message that includes the server identifier option to indicate which message it has selected and the requested IP address option, taken from "your IP address" in the selected offer.

- In the event that no offers are received, if the client has knowledge of a previous network address, the client may reuse that address if its lease is still valid, until the lease expires.

The Request Packet

- The servers receive the DHCPREQUEST broadcast from the client.
- Those servers not selected by the DHCPREQUEST message use the message as notification that the client has declined that server's offer.
- The server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client.
- Typically, a client only sends a Decline if it received more than one Offer
- DHCP Client May list Additional Configuration Parameters in the DHCP Request Packet

The Acknowledgment Packet

- The Acknowledgement packet is sent from the server to the client to indicate the completion of the four-packet DHCP Discovery process
- This response contains answers to any options to which the DHCP server replies
- The Acknowledgement packet may include some answers to the client's request for information. For example:
  - The client subnet mask is 255.255.0.0
  - The client's default gateway address is 10.0.0.1
  - The client's DNS server address is 10.0.0.1

Contd.

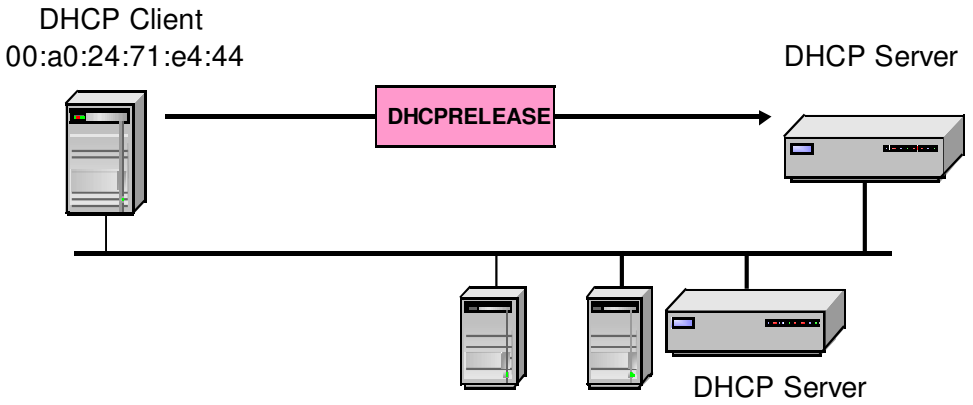
- The client receives the DHCPACK message with configuration parameters.
  - The client performs a final check on the parameters, for example with ARP for allocated network address, and notes the duration of the lease and the lease identification cookie specified in the DHCPACK message. At this point, the client is configured.
  - If the client detects a problem with the parameters in the DHCPACK message (the address is already in use on the network, for example), the client sends a DHCPDECLINE message to the server and restarts the configuration process.

Contd.

- The client should wait a minimum of ten seconds before restarting the configuration process to avoid excessive network traffic in case of looping.
- On receipt of a DHCPDECLINE, the server must mark the offered address as unavailable (and possibly inform the system administrator that there is a configuration problem).
- If the client receives a DHCPNAK message, the client restarts the configuration process.

DHCP Operation

- DCHP RELEASE



At this time, the DHCP client has released the IP address

Contd.

- The client may choose to relinquish its lease on a network address by sending a DHCPRELEASE message to the server.
- The client identifies the lease to be released by including its network address and its hardware address.

Lease Renewal

- When a server sends the DHCPACK to a client with IP address and configuration parameters, it also registers the start of the lease time for that address.
- This lease time is passed to the client as one of the options in the DHCPACK message, together with two timer values, T1 and T2.
- The client is rightfully entitled to use the given address for the duration of the lease time.

- T1 is the Renewal Time, i.e.
  - T1 is defined as the time that the client tries to renew its network address by contacting the DHCP server that sent the original address to the client
- T2 is the Rebinding Time, i.e.
  - T2 is defined as the time that the client begins to broadcast a renewal request hoping that another DHCP server can extend the lease time

Contd.

- On applying the receive configuration, the client also starts the timers T1 and T2. At this time, the client is in the BOUND state.

- Times T1 and T2 are options configurable by the server but T1 must be less than T2, and T2 must be less than the lease time.
- According to RFC 2132, T1 defaults to (0.5 * lease time) and T2 defaults to (0.875 * lease time).

Contd.

- When timer T1 expires, the client will send a DHCPREQUEST (unicast) to the server that offered the address, asking to extend the lease for the given configuration. The client is now in the RENEWING state
- The server would usually respond with a DHCPACK message indicating the new lease time, and timers T1 and T2 are reset at the client accordingly.
- The server also resets its record of the lease time.
- Under normal circumstances, an active client would continually renew its lease in this way indefinitely, without the lease ever expiring.

Contd.

- If no DHCPACK is received until timer T2 expires, the client enters the REBINDING state.
- Client now broadcasts a DHCPREQUEST message to extend its lease.
- This request can be confirmed by a DHCPACK message from any DHCP server on the network.
- If not confirmed, the DHCP client continues to retry the rebinding process until one minute from the lease expiration time
- If the client is unsuccessful in renewing the lease, it must give up the address at the expiration of the lease time, and reinitialize

Contd.

- The client may then return to the INIT state, issuing a DHCPDISCOVER broadcast to try and obtain any valid address.

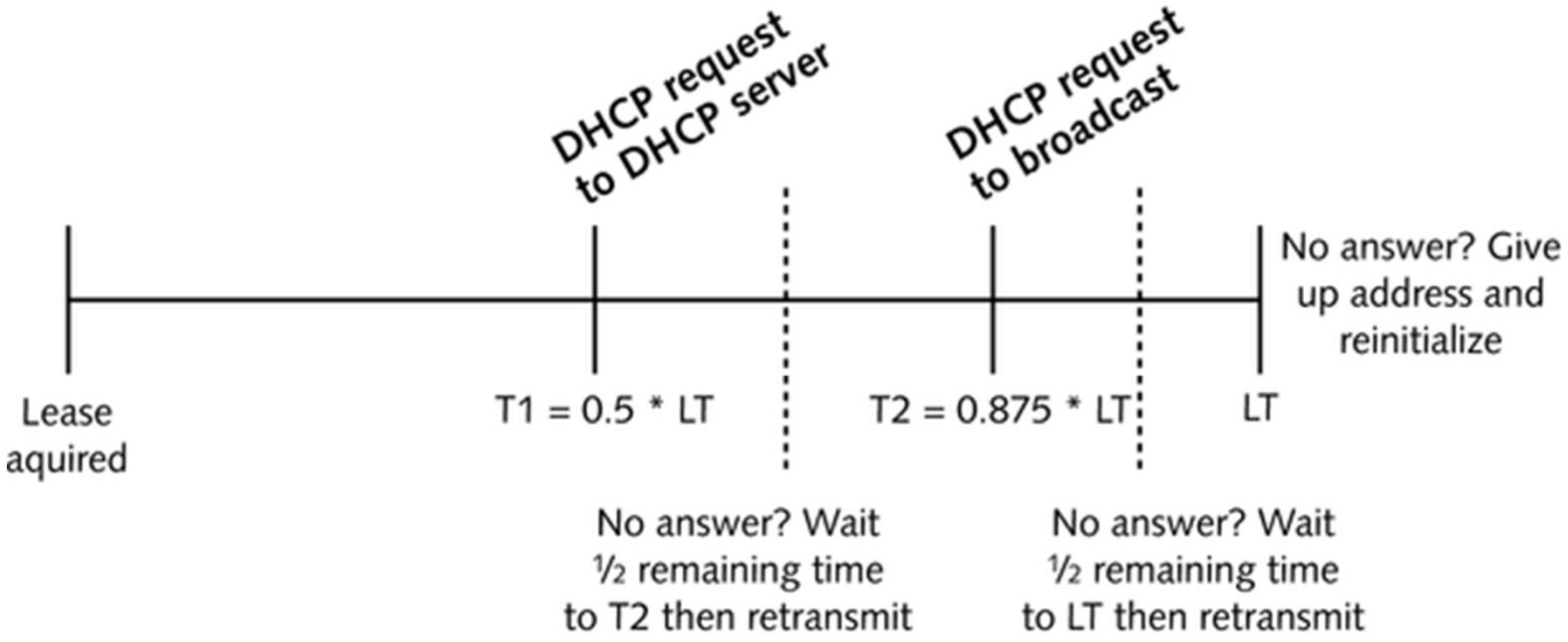


Figure 8-7 DHCP timeline includes the lease time (LT), renewal time (T1), and rebinding time (T2)

Packets: 7

Packet	Source	Destination	Dest. Port	Size	Protocol
1	IP-10.1.0.3	IP-10.1.0.1	bootps	346	UDP DHCP
2	IP-10.1.0.3	IP-10.1.0.1	bootps	346	UDP DHCP
3	IP-10.1.0.3	IP Broadcast	bootps	346	UDP DHCP
4	IP-10.1.0.3	IP Broadcast	bootps	346	UDP DHCP
5	IP-10.1.0.3	IP Broadcast	bootps	346	UDP DHCP
6	IP-10.1.0.3	IP Broadcast	bootps	346	UDP DHCP
7	IP-0.0.0.0	IP Broadcast	bootps	346	UDP DHCP

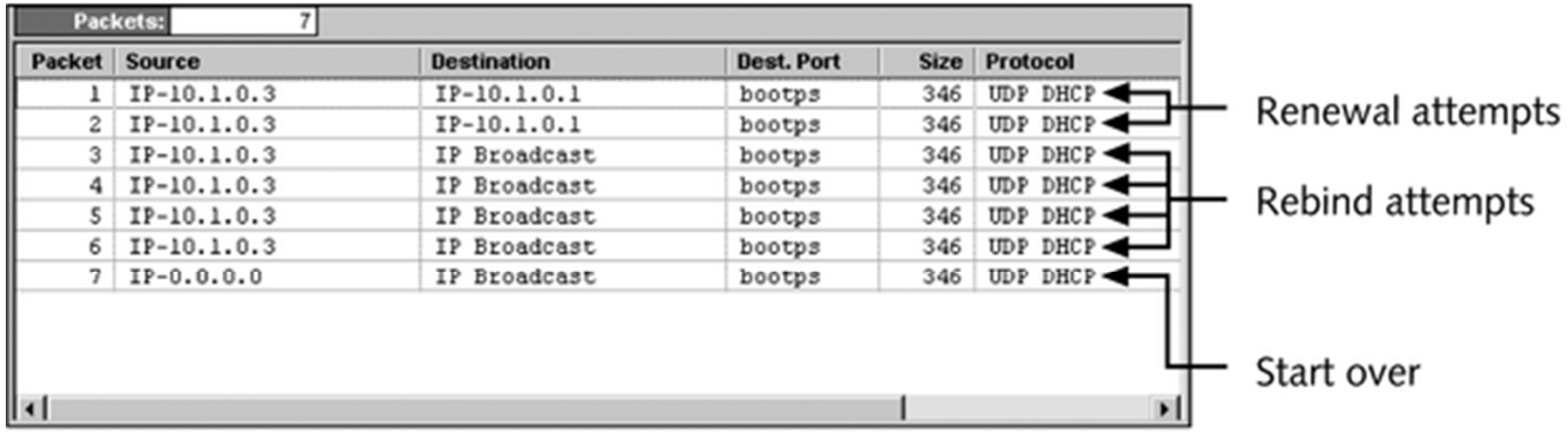


Figure 8-8 DHCP client begins advertising an address of 0.0.0.0 when it gives up its IP address

The DHCP Address Release Process

- Although not required by the specification, the client should release its address by sending a DHCP Release packet to the server (called the release process)

Reusing a Previously allocated address

- The client broadcasts a DHCPREQUEST message on its local subnet.
  - The DHCPREQUEST message includes the client's previously used network address.
- If the client's lease is still current, the server with knowledge of the client's configuration parameters responds with a DHCPACK message to the client, renewing the lease at the same time.
  - The client must then proceed to test for the IP address.
- If the client's lease has expired, the server with knowledge of the client responds with DHCPNACK.
  - The client then must initiate a new IP address allocation process.

Broadcast and Unicast in DHCP

- DHCP communications, use a strange mix of broadcast and unicast addressing
- DHCP clients must use broadcast until obtaining IP addresses through a successful completion of the Discovery, Offer, Request, and Acknowledgment processes

Table 8-3 DHCP Broadcast and Unicast Rules

Gateway IP Address Setting	Client IP Address Setting	Address Used
non-zero	N/A	Unicast packets from DHCP server to the relay agent
zero	non-zero	Unicast DHCP Offer and DHCP ACK messages to the client IP address
zero	zero	[Broadcast bit set] DHCP server broadcasts DHCP Offer and DHCP ACK messages to 0xFF.FF.FF.FF
zero	zero	[Broadcast bit not set] DHCP server unicasts DHCP Offer and DHCP ACK messages to the client IP address and the value contained in the Your IP Address field.

DHCP Relay Agents

- **The relay agent function is typically loaded on a router connected to the segment containing DHCP clients**
- **This relay agent device is configured with the address of the DHCP server, and can communicate unicast directly with that server**

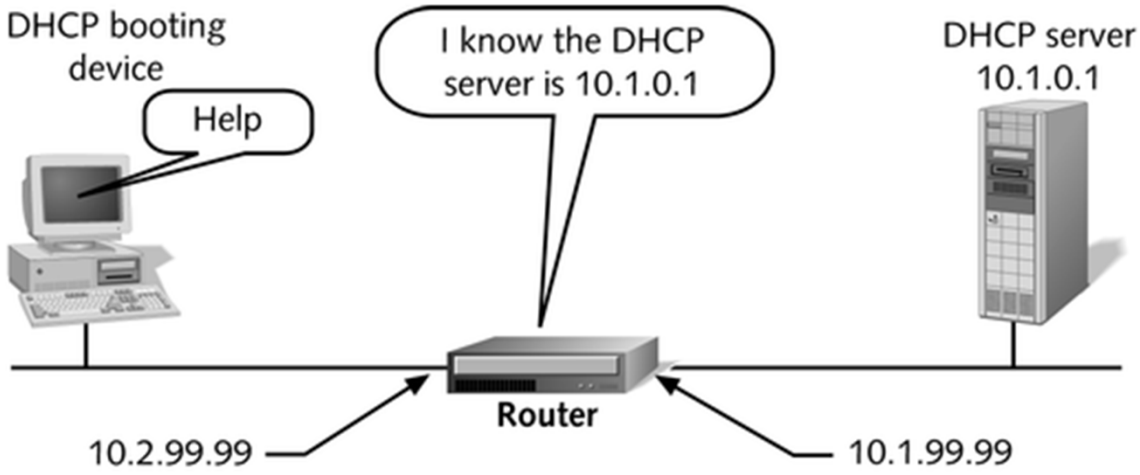


Figure 8-10 A network configuration using DHCP relay agent software on a router

DHCP Relay Agents

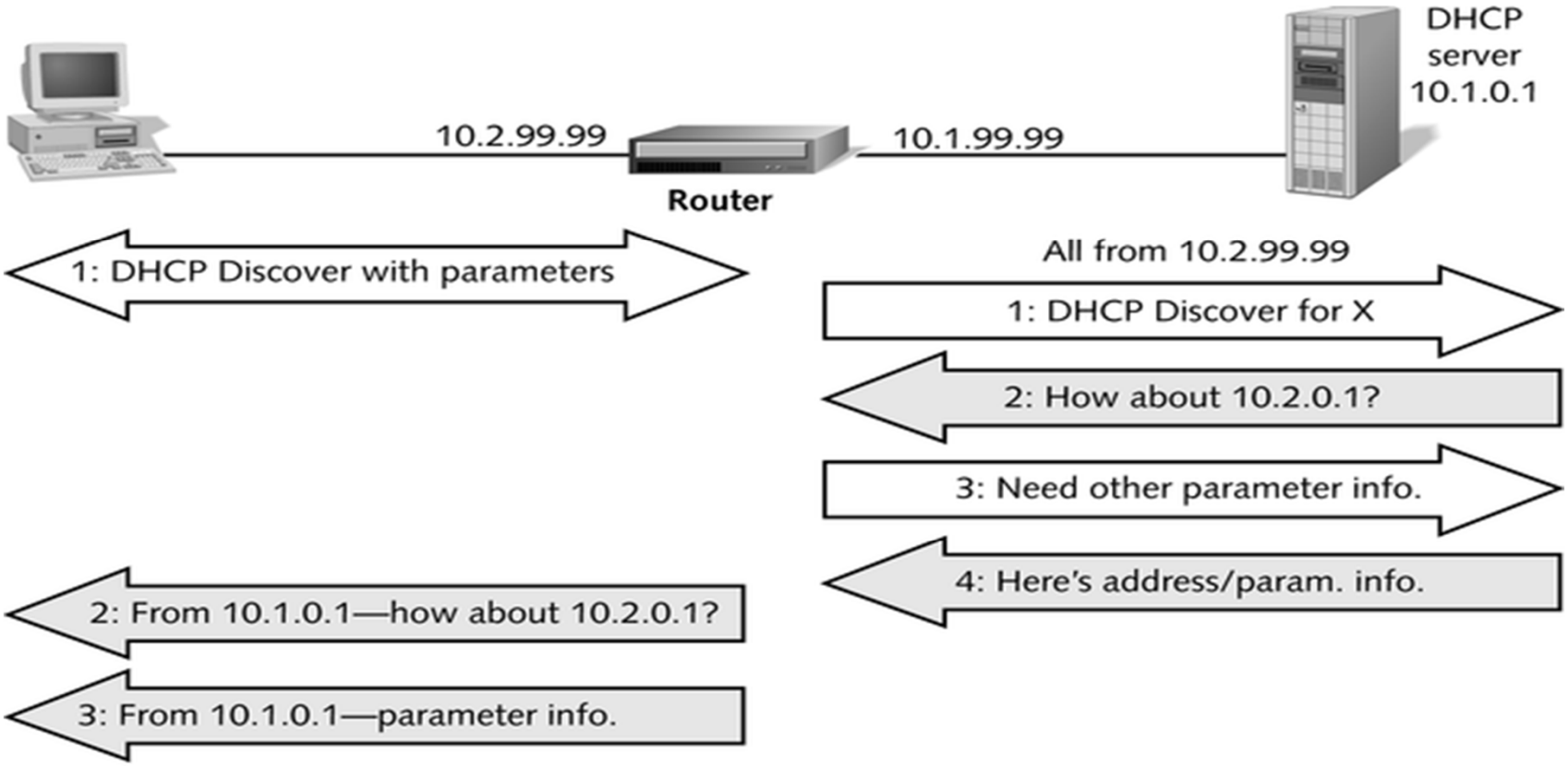


Figure 8-11 DHCP relay communications process

DHCP Pros

- It relieves the network administrator of a great deal of manual configuration work.
- The ability for a device to be moved from network to network and to automatically obtain valid configuration parameters for the current network can be of great benefit to mobile users.
- Because IP addresses are only allocated when clients are actually active, it is possible, by the use of reasonably short lease times and the fact that mobile clients do not need to be allocated more than one address, to reduce the total number of addresses in use in an organization.

The Future of DHCP

- As IPv6 development and deployment move forward, DHCP's role changes significantly

- One of the great advantages of IPv6 is autoconfiguration—IPv6 hosts can create local IP addresses using their hardware addresses and the Neighbor Discovery process

DHCP Cons

- Uses UDP, an unreliable and insecure protocol.
- DNS cannot be used for DHCP configured hosts.