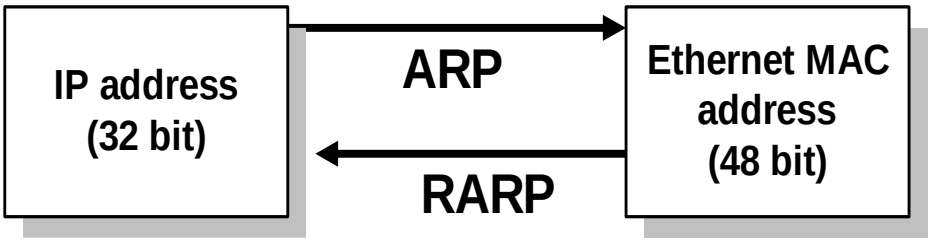
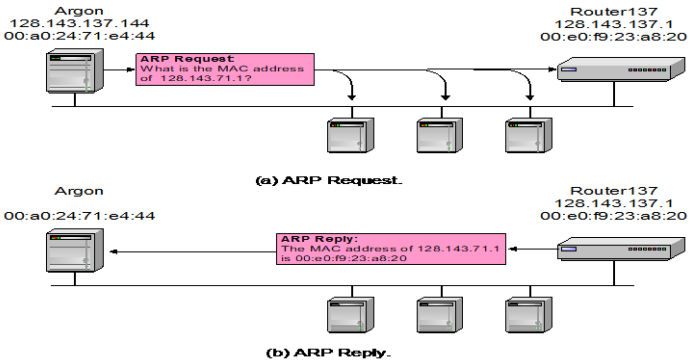
Address Resolution Protocol (ARP) & Reverse Address Resolution Protocol (RARP)

- The ARP and RARP protocols perform the translation between IP addresses and MAC layer addresses
- We will discuss ARP for broadcast LANs, particularly Ethernet LANs



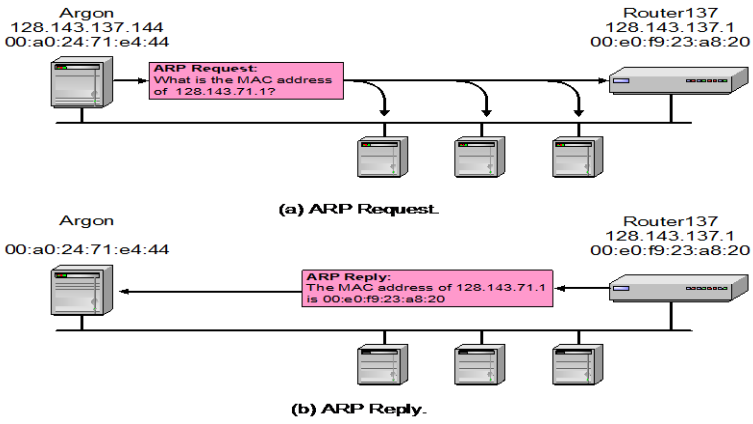
ARP Request:

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



ARP Reply:

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



ICMP - INTERNET CONTROL MESSAGE PROTOCOL

➢ICMP is a network-layer protocol.

➢It is a companion to the IP protocol.

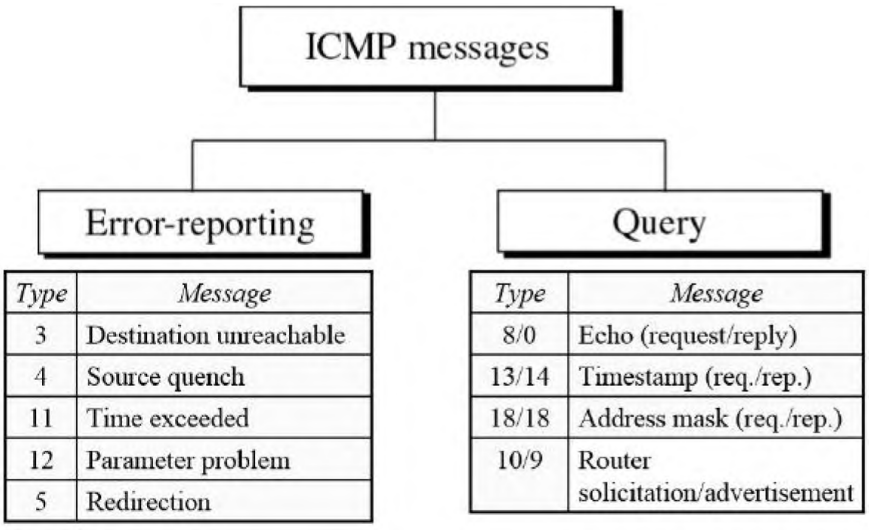
➢Internet Control Message Protocol (ICMP) defines a collection of error messages that are sent back to the source host whenever a router or host is unable to process an IP datagram successfully

ICMP MESSAGE TYPES

➢ICMP messages are divided into two broad categories: *error-reporting messages* and *query messages.*

➢The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

➢The query messages help a host or a network manager get specific information from a router or another host



Type	*Message*
3	Destination unreachable
4	Source quench
11	Time exceeded
12	Parameter problem
5	Redirection

Type	*Message*
8/0	Echo (request/reply)
13/14	Timestamp (req./rep.)
18/18	Address mask (req./rep.)
10/9	Router solicitation/advertisement

ICMP Error – Reporting Messages

➢***Destination Unreachable—***When a router *cannot route* a datagram, the datagram is discarded and sends a destination unreachable message to source host.

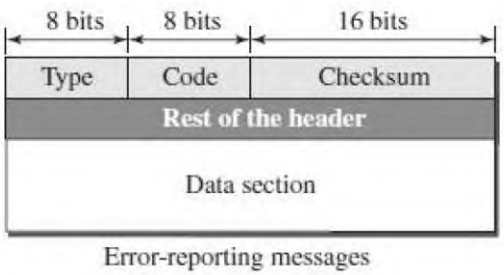
➢***Source Quench—***When a router or host discards a datagram due to *congestion*, it sends a source-quench message to the source host. This message acts as flow control.
➢***Time Exceeded—***Router discards a datagram when TTL field becomes 0 and a time exceeded message is sent to the source host.
➢***Parameter Problem—***If a router discovers ambiguous or *missing* value in any field of the datagram, it discards the datagram and sends parameter problem message to source.
➢***Redirection—***Redirect messages are sent by the default router to inform the source host to *update* its forwarding table when the packet is routed on a wrong path.

ICMP Query Messages

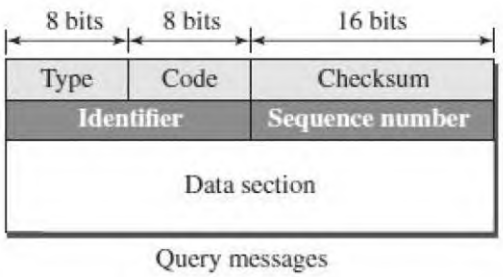
➢***Echo Request & Reply—***Combination of echo request and reply messages determines whether two systems communicate or not.
➢***Timestamp Request & Reply—***Two machines can use the timestamp request and reply messages to determine the round-trip time (RTT).
➢***Address Mask Request & Reply—***A host to obtain its subnet mask, sends an address mask request message to the router, which responds with an address mask reply message.
➢***Router Solicitation/Advertisement—***A host broadcasts a router solicitation message to know about the router. Router broadcasts its routing information with router advertisement message.

ICMP MESSAGE FORMAT

➢An ICMP message has an 8-byte header and a variable-size data section.



Error-reporting messages



Query messages

Type	Defines the type of the message
Code	Specifies the reason for the particular message type

Checksum	Used for error detection
Rest of the header	Specific for each message type
Data	Used to carry information
Identifier	Used to match the request with the reply
Sequence Number	Sequence Number of the ICMP packet

DHCP – DYNAMIC HOST CONFIGURATION PROTOCOL

➢The dynamic host configuration protocol is used to simplify the installation and maintenance of networked computers.

➢DHCP is derived from an earlier protocol called BOOTP.

➢Ethernet addresses are configured into network by manufacturer and they are unique.

➢IP addresses must be unique on a given internetwork but also must reflect the structure of the internetwork

➢Most host Operating Systems provide a way to manually configure the IP information for the host

➢**Drawbacks of manual configuration :**

1. A lot of work to configure all the hosts in a large network
2. Configuration process is error-prune

➢It is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address.

➢For these reasons, automated configuration methods are required.

➢The primary method uses a protocol known as the *Dynamic Host Configuration Protocol* (DHCP).

➢The main goal of DHCP is to minimize the amount of manual configuration required for a host.

➢If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network. ➢DHCP is based on a client/server model.

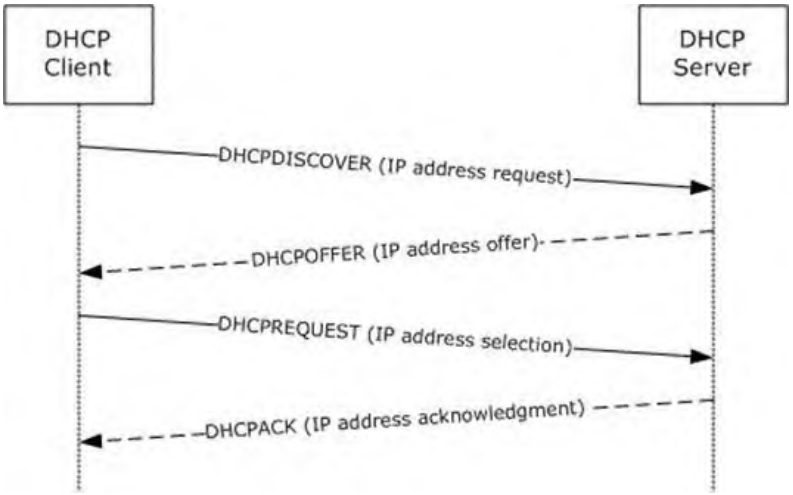
➢DHCP clients send a request to a DHCP server to which the server responds with an IP address

➢DHCP server is responsible for providing configuration information to hosts.

➢There is at least one DHCP server for an administrative domain.

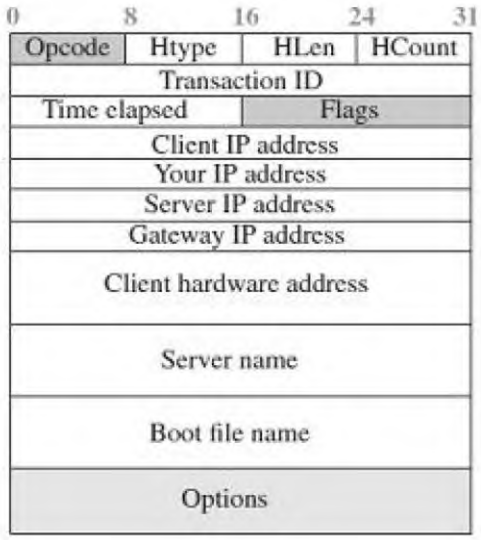
➢The DHCP server can function just as a centralized repository for host configuration information.

➢The DHCP server maintains a pool of available addresses that it hands out to hosts on demand.



DHCP Message Format

A DHCP packet is actually sent using a protocol called the *User Datagram Protocol* (UDP).



Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Length of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by the 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