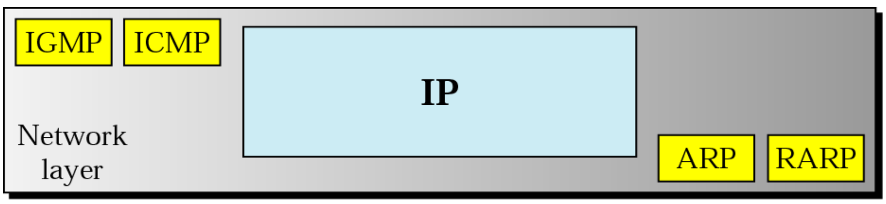
Data Communication & Computer Networks

8. Network Layer Protocols

ARP
IPv4
ICMP
IPv6

Protocols at network layer



ARP

IP-MAC mapping

- Packet delivery to a host or a router requires two levels of addressing
  - IP address
  - MAC address
- IP-MAC mapping is needed
- IP-MAC mapping can be …
  - Static mapping
  - Dynamic mapping

IP-MAC mapping

Static mapping

- A table associates all IP addresses on a network to their MAC addresses
- The table is stored in each machine
- Requires periodic updates

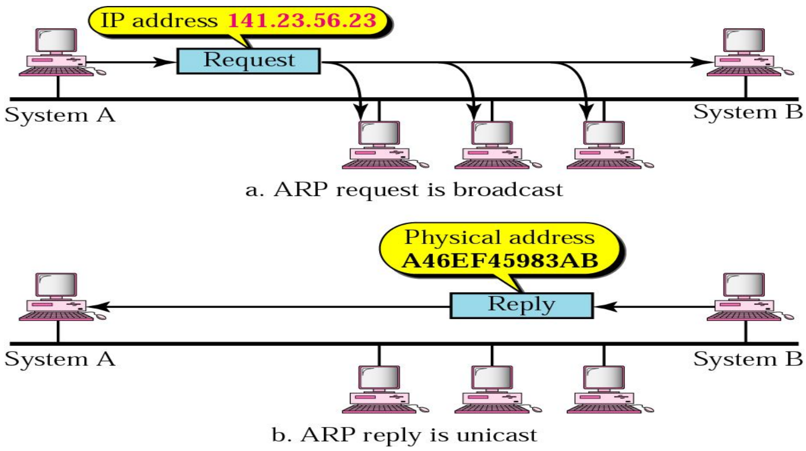
Dynamic mapping

- If a machine knows one of the two addresses, it can use a protocol to find the other
- ARP: IP->MAC
- RARP: MAC->IP

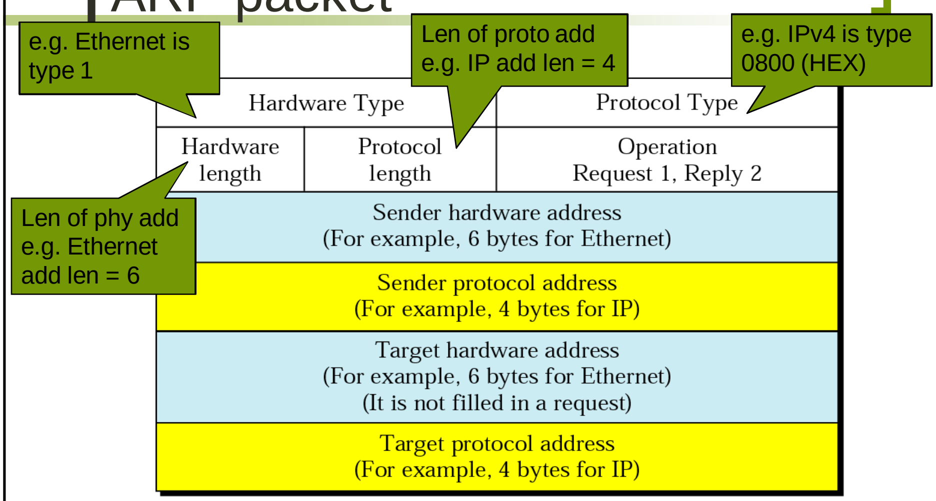
Address Resolution Protocol (ARP)

- ARP (RFC 826) provides dynamic IP to Ethernet address mapping
  - source broadcasts ARP request
  - destination replies with ARP response

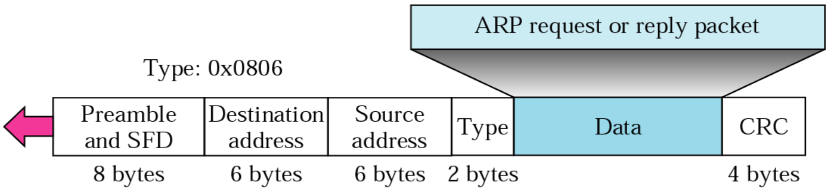
ARP operation



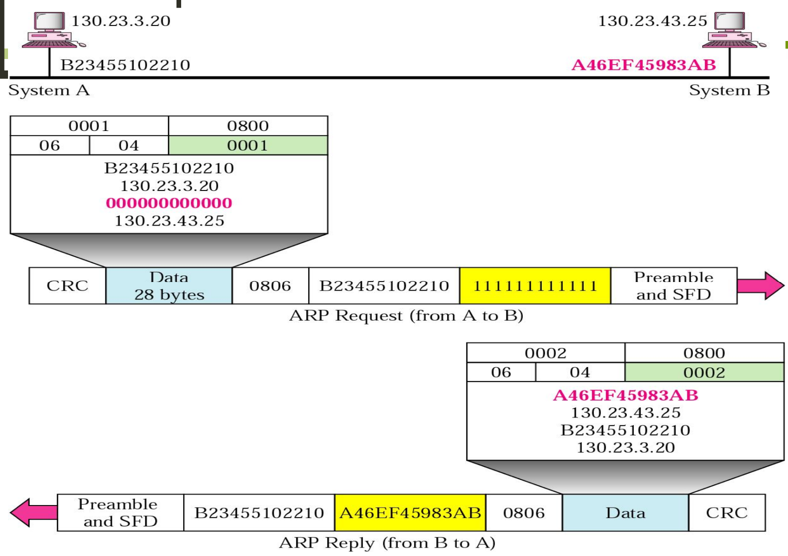
ARP packet



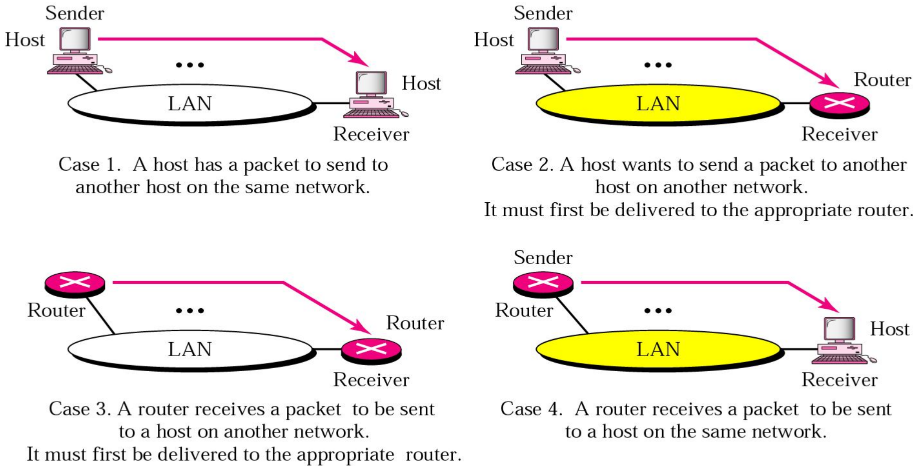
Encapsulation of ARP packet



ARP operation



ARP use case



IPv4

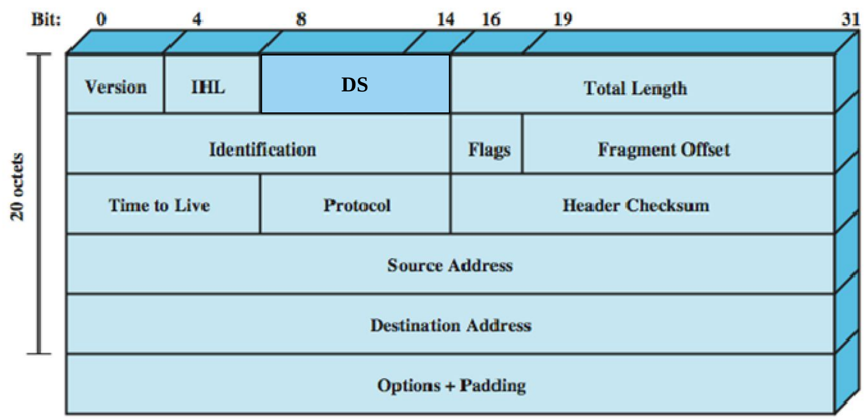
Internet Protocol (IP) v4

- IP version 4
- defined in RFC 791
- part of TCP/IP suite
- two parts
  - specification of interface with a higher layer
    - e.g. TCP
  - specification of actual protocol format and mechanisms
- will (eventually) be replaced by IPv6

IP

- Used for host-to-host delivery
- Unreliable
- Connection less
- Best Effort delivery
  - IP does to best to deliver a packet to destination … no guarantees
- If reliability is required, use it with TCP
- IP layer packets are called datagrams

IPv4 Header



Header Fields (1)

- Version
  - currently 4
  - IP v6 - see later
- Internet header length
  - in 32 bit words
  - including options
- DS (was type of service)
- total length
  - of datagram, in octets (data+header)

Header Fields (2)

- Identification
  - sequence number
  - identify datagram uniquely with addresses / protocol
- Flags
  - More bit
  - Don’t fragment
- Fragmentation offset
- Time to live
- Protocol
  - Next higher layer to receive data field at destination

Header Fields (3)

- Header checksum
  - reverified and recomputed at each router
  - 16 bit ones complement sum of all 16 bit words in header
  - set to zero during calculation
- Source address
- Destination address
- Options
- Padding
  - to fill to multiple of 32 bits long

Data Field

- carries user data from next layer up
- integer multiple of 8 bits long (octet)
- max length of datagram (header plus data) is 65,535 octets

Checksum calculation

- Set checksum to zero
- Divide header into 16-bit sections
- Add all sections
- Take 1's compliment of the sum
- Result is inserted in checksum field

4	5	0	28
1		0	0
4	17	0	
10.12.14.5			
12.6.7.9			

4, 5, and 0 →	0100010100000000
28 →	0000000000011100
1 →	0000000000000001
0 and 0 →	0000000000000000
4 and 17 →	0000010000010001
0 →	0000000000000000
10.12 →	0000101000001100
14.5 →	0000111000000101
12.6 →	0000110000000110
7.9 →	0000011100001001
Sum →	0111010001001110
Checksum →	1000101110110001

Fragmentation

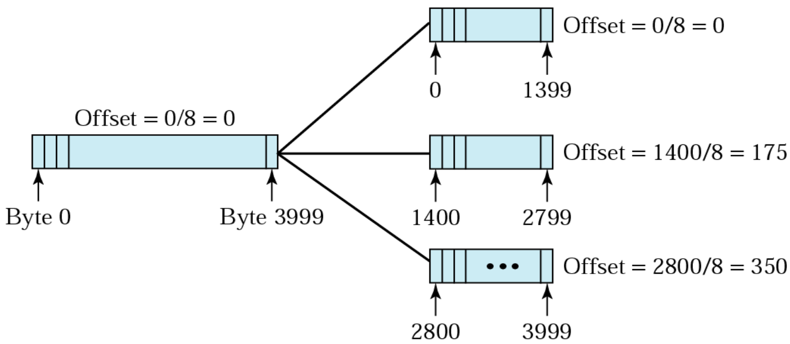
- Each data link protocol has its own limitation on maximum data size
  - Maximum Transfer Unit (MTU)
- If an IP packet is larger than MTU of its underlying L2 protocol, it must be divided to match the MTU
  - fragmentation

Fragmentation

- Can happen at every router
- Each fragmented part has its own IP header
  - Independent datagram
- Reassembly done only at destination

Fragmentation

- IP fields concerned with fragmentation
  - Identification, Flags, Fragmentation offset



ICMP

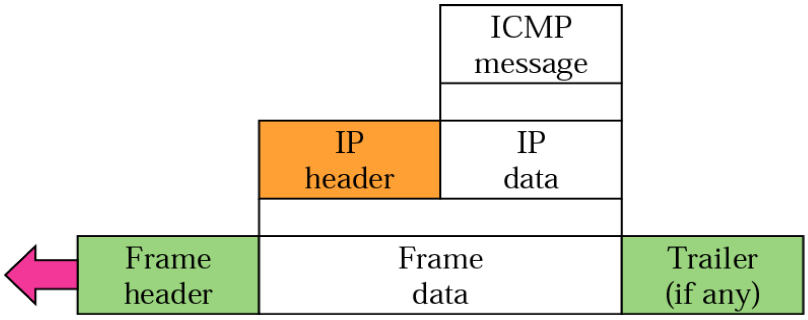
ICMP

- IP is a best-effort delivery service
  - No error control or assistance method
- What if something goes wrong?
  - e.g. a router has to drop a packet etc.
- What if a device needs some info?
  - e.g. is next-hop router alive?
- Solution: ICMP

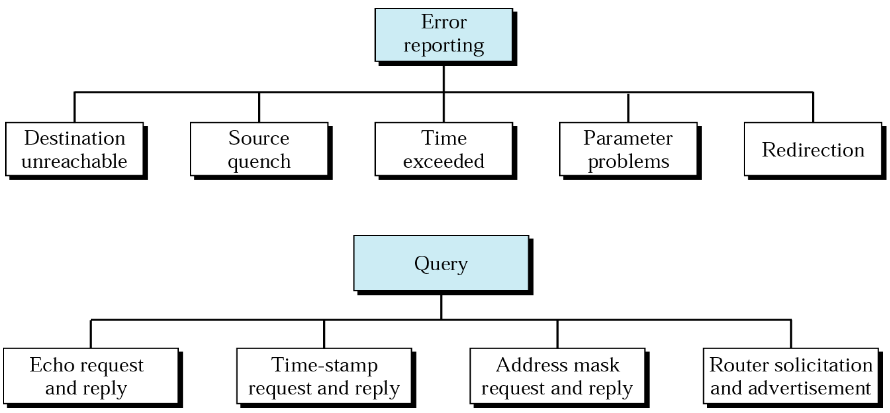
ICMP

- Internet Control Message Protocol
- RFC 792 (study it)
- transfer of (control) messages from routers and hosts to hosts
- feedback about problems
  - e.g. time to live expired
- encapsulated in IP datagram
  - hence not reliable

ICMP encapsulation



ICMP messages



IPv6

IP Versions

- IP v1-3 defined and replaced
- IP v4 - current version
- IP v5 - streams protocol
- IP v6 - replacement for IPv4
  - during development it was called IPng (IP Next Generation)

RQ 30

Why Change IP?

- Address space exhaustion
  - two level addressing (network and host) wastes space
  - network addresses used even if not connected
  - growth of networks and the Internet
  - extended use of TCP/IP
- requirements for new types of service
- Requirements for security features by some applications

IPv6 RFCs

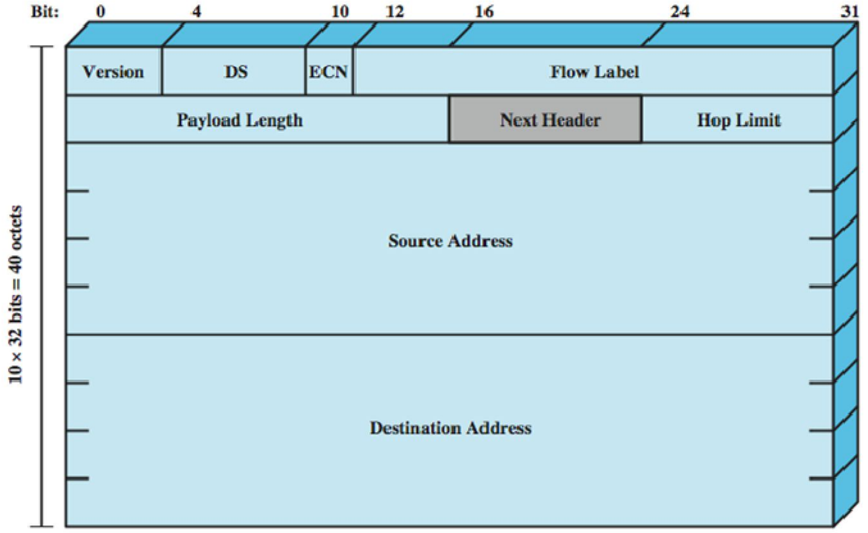
- RFC 1752 - Recommendations for the IP Next Generation Protocol
  - requirements
  - PDU formats
  - addressing, routing security issues
- RFC 2460 - overall specification
- RFC 2373 - addressing structure
- many others

IPv6 Enhancements

- expanded 128 bit address space
- improved option mechanism
  - most not examined by intermediate routes
- allows extensions
- support for security
- support for resource allocation
  - labeled packet flows

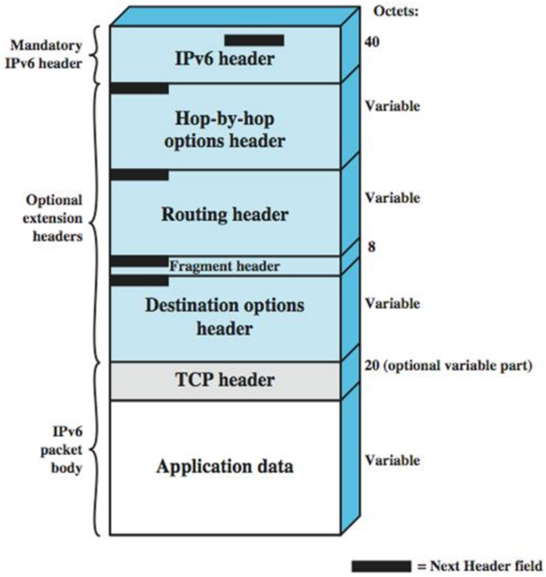
RQ 33

IPv6 Header



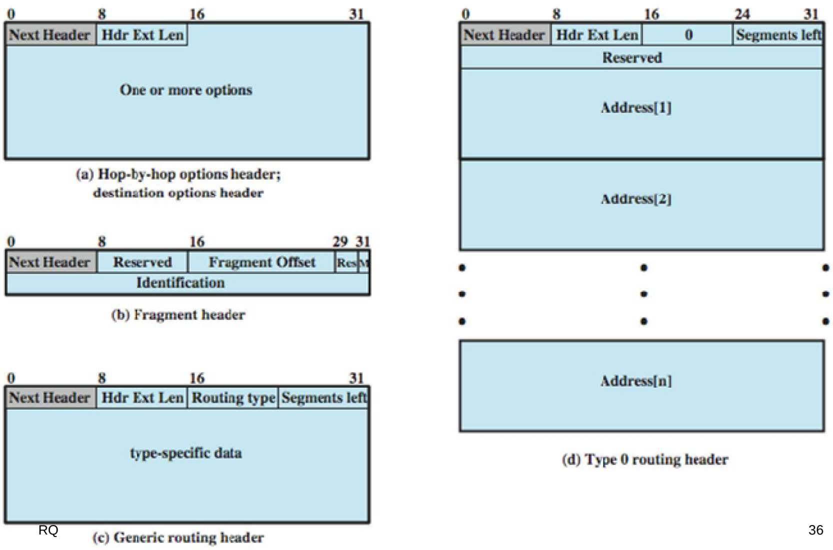
RQ 34

IPv6 PDU (Packet) Structure



RQ

IPv6 Extension Headers



RQ

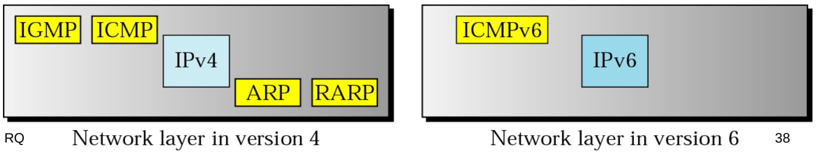
Fragmentation Header

- fragmentation only allowed at source
- no fragmentation at intermediate routers
- node must perform path discovery to find smallest MTU of intermediate networks
- set source fragments to match MTU
- otherwise limit to 1280 octets
- header includes
  - fragment offset
  - more fragments bit
  - identification

RQ 37

ICMPv6

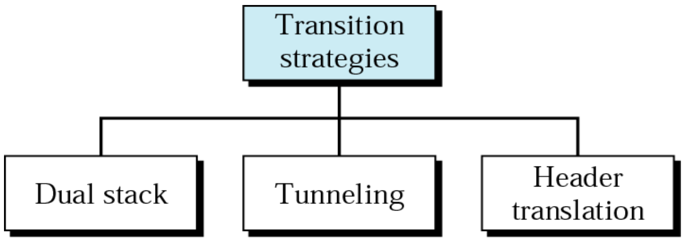
- ICMPv6 follows the same strategy and purposes of ICMPv4 but modified to make it more suitable for IPv6.
- Some protocols that were independent in version 4 are now part of Internet Control Message Protocol (ICMPv6).



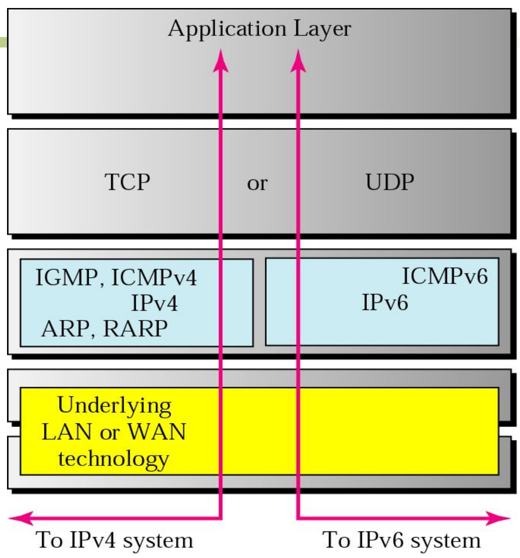
RQ 38

Transition from IPv4 to IPv6

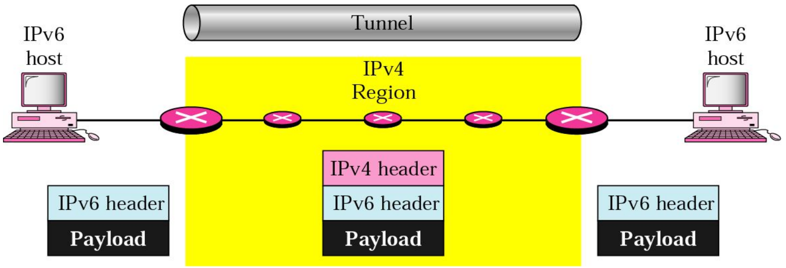
- Transition can not take place overnight
- Transition should be smooth, allowing both versions to coexist before complete transition



Dual stack



Tunnelling



Header translation