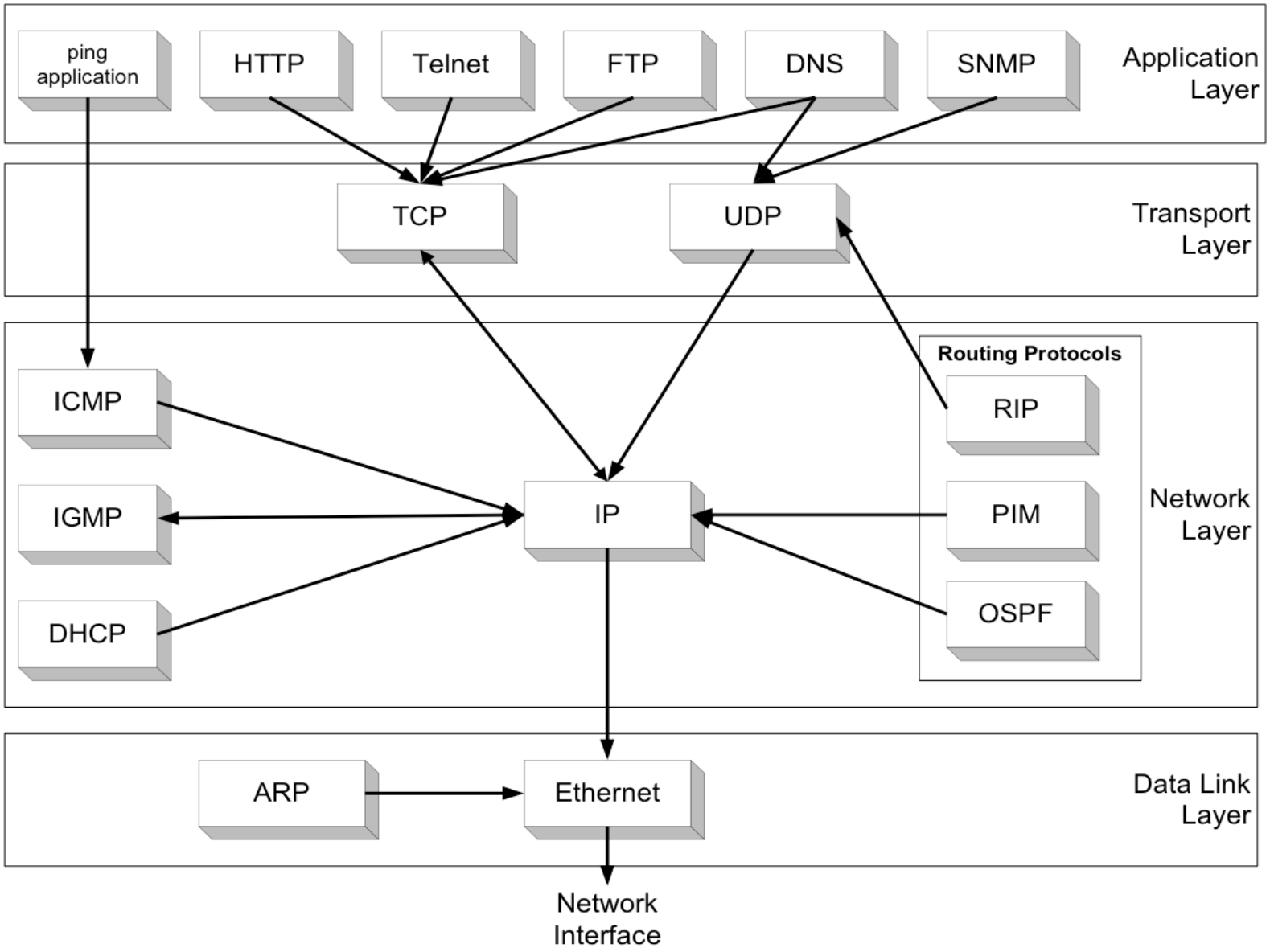
IP - The Internet Protocol

Content

1. Tasks of the network layer protocols
2. Classification and types of network layer protocols
3. IP services and header structure
4. IPv4 Features
   - Encapsulation
   - Addressing
   - Routing
   - Fragmentation
   - Identification
   - Parameterization

1.Tasks of the network layer protocols



1. Tasks of the network layer protocols

Network layer protocols are responsible for:

- assignment of logical addresses and their translation into physical ones;
- for switching and redirection;
- determination of the shortest route from sending to receiving system;
- for tracking network problems and shutters;
- for transfer from the sending system to the receiving system;
- for managing multicast data transmission over the Internet.

1.Switching in the local network is based on the MAC addresses, therefore the IP module uses the correspondence table of the type IP address - MAC address, which is filled in by the Address Resolution Protocol (ARP), the IP address itself can be assigned manually or automatically via DHCP (Dynamic Host Configuration Protocol).

2.To find the optimal route, the IP module uses the routing table (RT), which consists of routing protocols (RIP, OSPF) and other system components.

3.Routers and hosts notify each other of problems using the Internet Control Message Protocol (ICMP).

4.Group transmission is performed by group management protocols: in a local area network IGMP (Internet Group Management Protocol) and globally PIM (Protocol Independent Multicast).

2. Classification and types of network layer protocols

Network layer protocols redirect data from source to destination and can be divided into two classes:

1.Connection establishment protocols (for example, X.25) - begin data transfer from a call or setting the route of packets from the source to the recipient. Then they start serial transmission of data and then, at the end of the transfer, disconnect.

2.Protocols without establishing a connection (for example, IP) - send data containing complete address information in each packet.

- Each packet contains the address of the sender and receiver.
- Next, each intermediate network device reads the address information and makes a decision about data routing.
- A message or data packet is transferred from one intermediate device to another until it is delivered to the recipient.
- Protocols without establishing a connection do not guarantee the receipt of information to the recipient in the order in which it was sent, because different packages can go different routes.
- Transport protocols are responsible for restoring data order when using network protocols without establishing a connection.

2. Classification and types of network layer protocols

Types of network layer protocols:

- Interaction protocols
  - IP / IPv4 / IPv6 - Internet Protocol
  - IPX - Internetwork Packet Exchange (Internet Protocol)
  - X.25 (partially this protocol is implemented at level 2)
  - CLNP - Connection Less Network Protocol
- IPsec - Internet Protocol Security
- Routing Protocols
  - RIP - Routing Information Protocol
  - OSPF - Open Shortest Path First
  - IS-IS - Intermediate System to Intermediate System
  - BGP - Border Gateway Protocol
  - PIM - Protocol Independent Multicast
- Management Protocols
  - ICMP - Internet Control Message Protocol
  - IGMP - Internet Group Management Protocol
- Address resolution and assignment protocols (work at the boundaries of levels)
  - ARP - Address Resolution Protocol (in IPv6, it takes ICMPv6 functions)
  - DHCP - Dynamic Host Configuration Protocol
  - SLAAC - State-Less Address AutoConfiguration

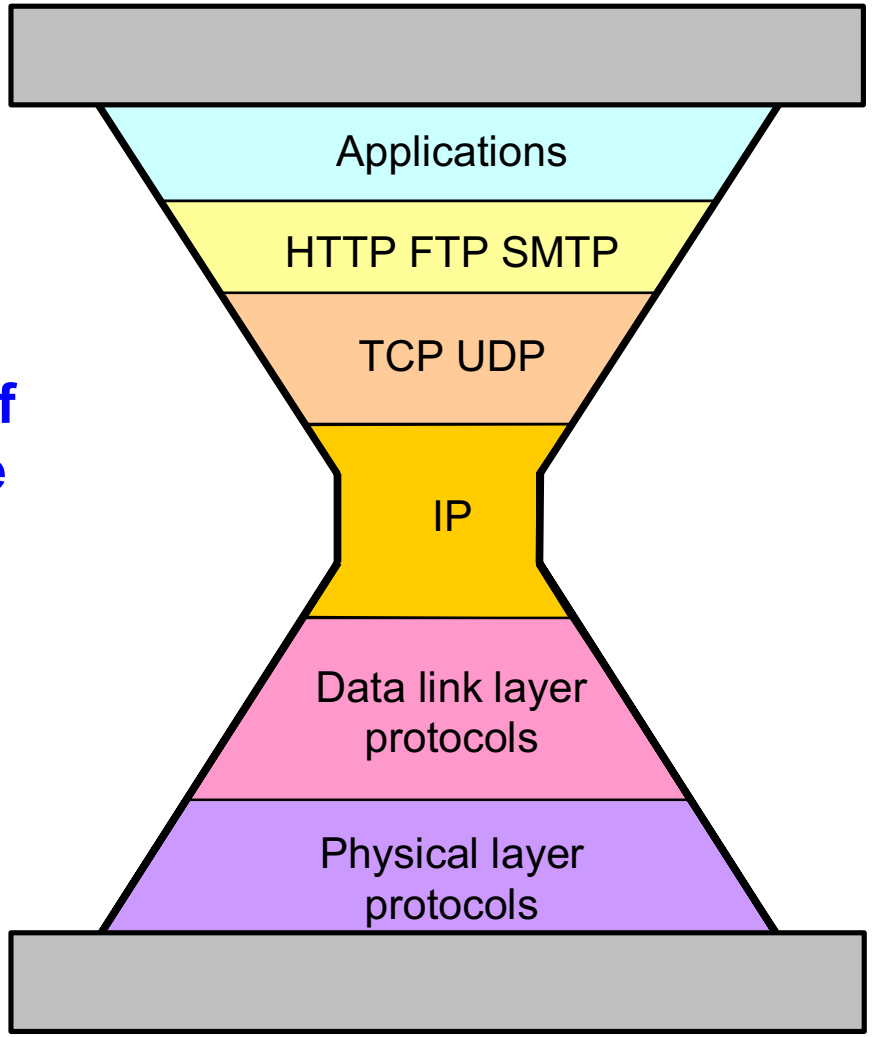
3. IP services and header structure

- IP (Internet Protocol) is a Network Layer Protocol.
- IP's current version is Version 4 (IPv4). It is specified in RFC 891.

- **IP is the waist of the hourglass of the Internet protocol architecture**

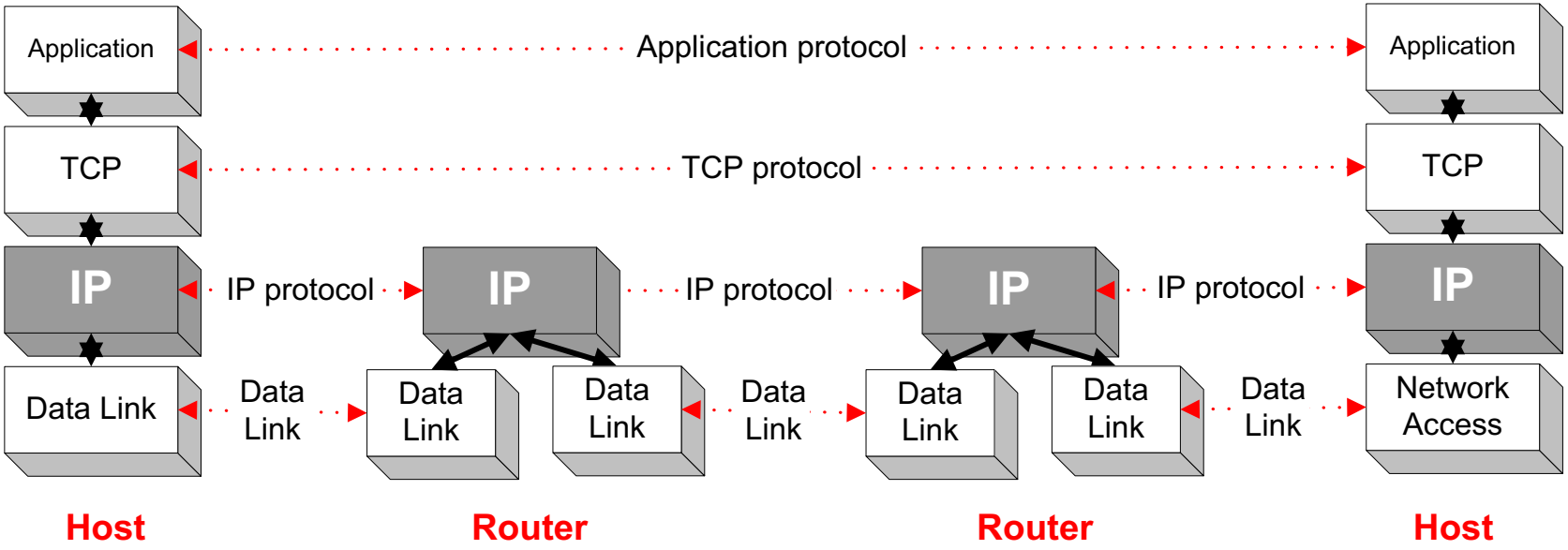
- Multiple higher-layer protocols
- Multiple lower-layer protocols

- Always IP protocol at the network layer.



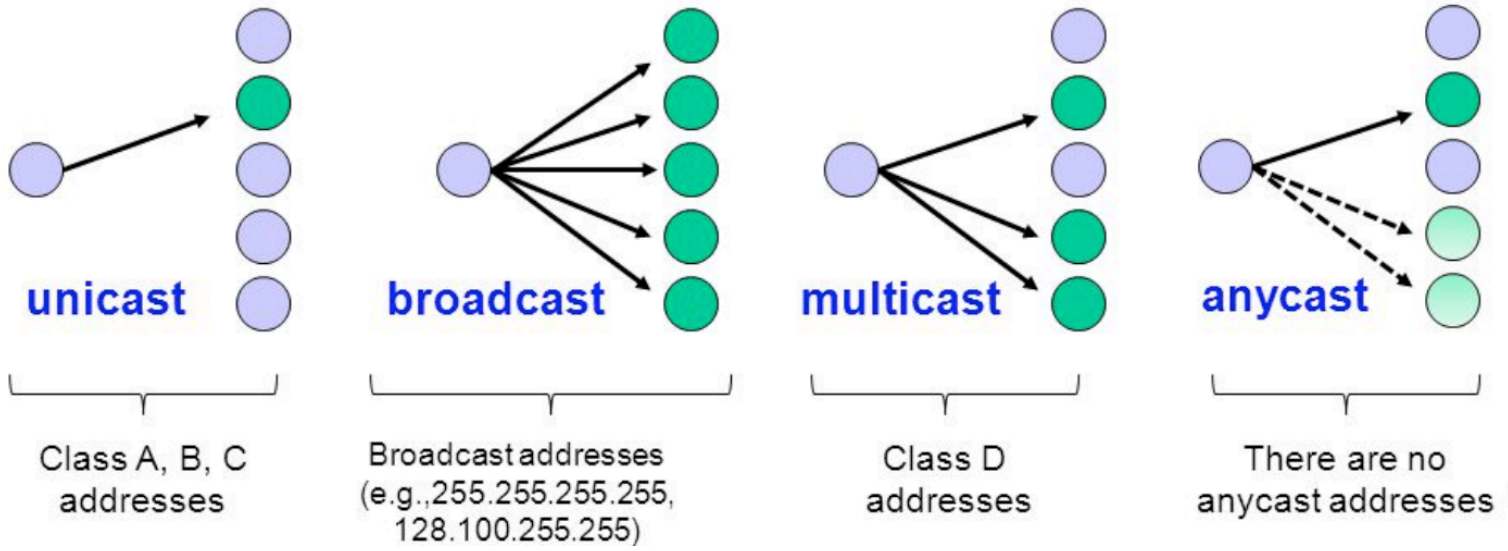
IP Implementation

- IP is the highest layer protocol which is implemented at both routers and hosts



IP Delivery Modes

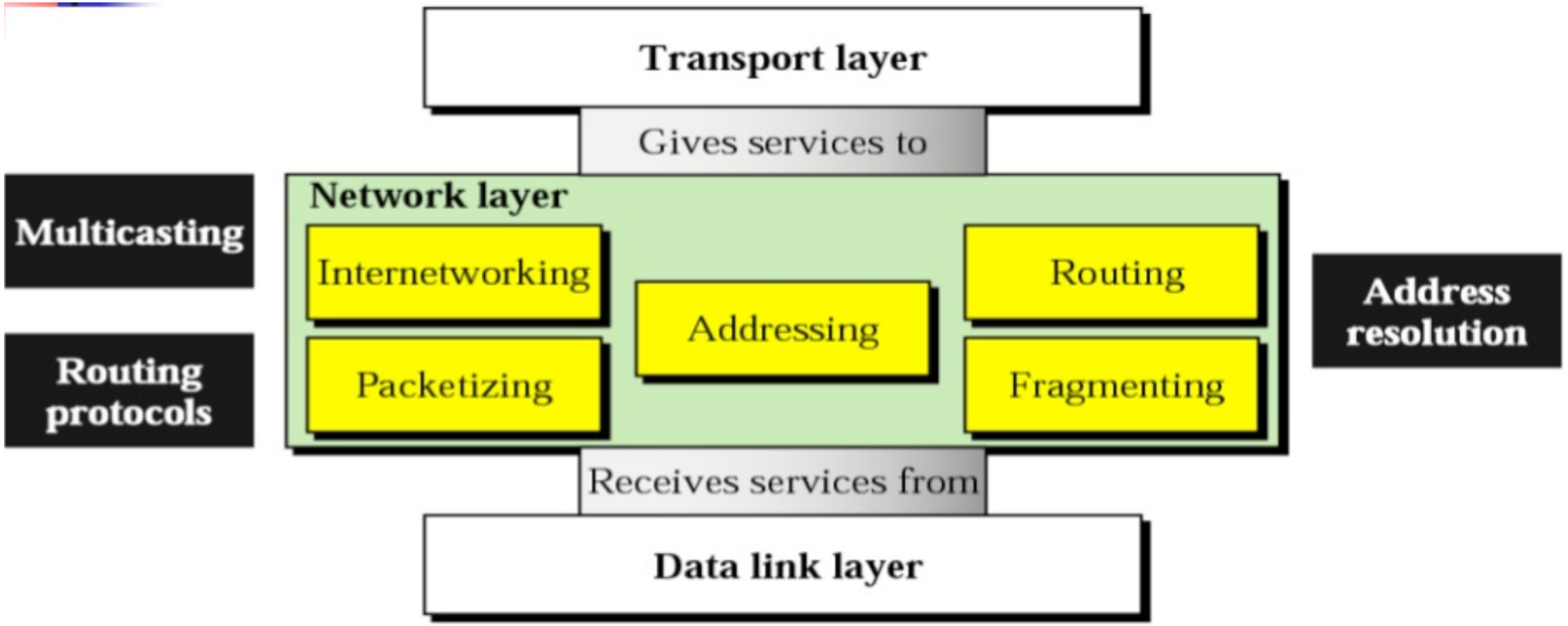
- IP supports the following delivery modes:
  - one-to-one (web, (unicast)
  - one-to-all (arp, dhcp) (broadcast)
  - one-to-several (ipTV) (multicast)
  - one-to-any (dns) (anycast)
- IP multicast also supports a many-to-many service.
- IP multicast requires support of other protocols (IGMP, multicast routing)
- Anycast (use IPv6) is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers, though it may be sent to several nodes, all identified by the same destination address.



IP Service

- Delivery service of IP is minimal
- IP provide provides an unreliable connectionless best effort service (also called: “datagram service”).
  - **Unreliable:** IP does not make an attempt to recover lost packets
  - **Connectionless:** Each packet (“datagram”) is handled independently. IP is not aware that packets between hosts may be sent in a logical sequence
  - **Best effort:** IP does not make guarantees on the service (no throughput guarantee, no delay guarantee,…)
- Consequences:
  - Higher layer protocols have to deal with losses or with duplicate packets
  - Packets may be delivered out-of-sequence

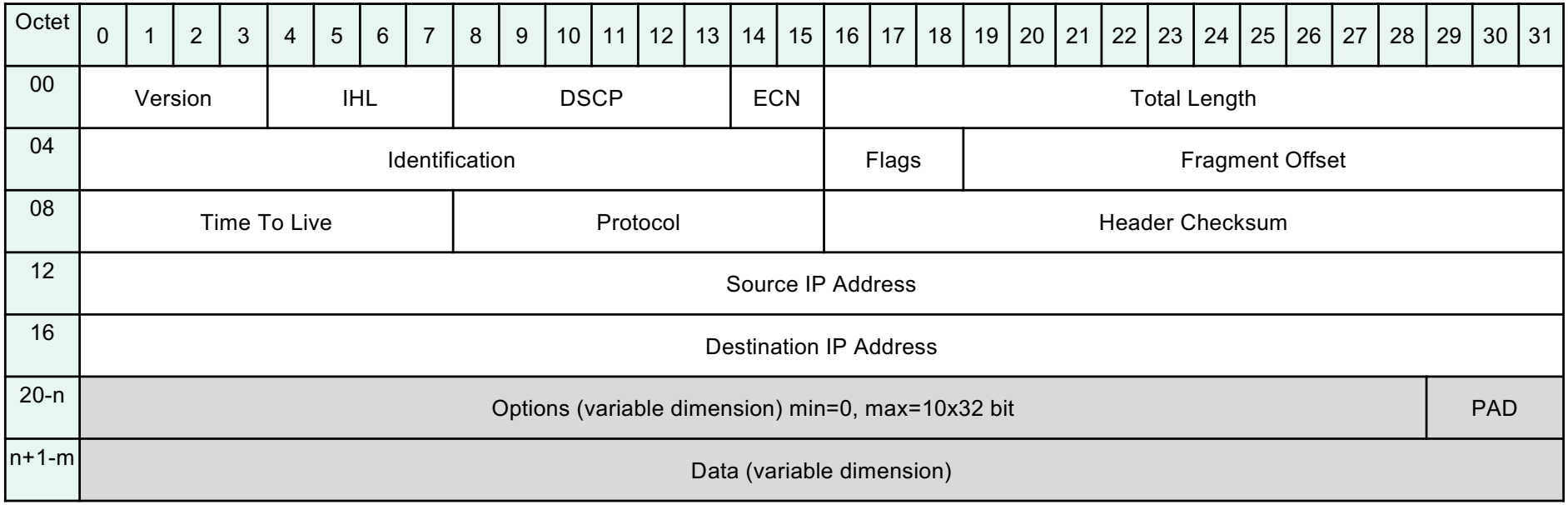
IP Service


Transport layer
Gives services to
Network layer
Multicasting
Routing protocols
Internetworking
Addressing
Routing
Address resolution
Packetizing
Fragmenting
Receives services from
Data link layer

IP Service

- TCP/IP protocols are described in RFCs (Requests For Comments) published by the Internet Engineering Task Force (IETF).
- TCP/IP specifications are available for general use and are available free of charge on the Internet at many sites, including on the IETF homepage at http://www.ietf.org. The IP protocol specification was published in RFC 791 (September 1981).
- IP performs several important network functions, including:
  1. Encapsulation - packing of a transport layer data packet into a datagram.
  2. Addressing - identification of systems on the network by their IP addresses.
  3. Routing - determining the most efficient path to the target system.
  4. Fragmentation - splitting data into fragments suitable for transmission over the network (MTU) in size.
  5. Identification of the upper layer protocol that generated the data for IP.
  6. Parameterization - setting IP options for specific tasks.

IP Datagram Format



- 20 bytes ≤ Header Size < 2^4 x 4 bytes = 64 bytes
- 20 bytes ≤ Total Length < 2^{16} bytes = 65536 bytes

IP Datagram Format

- **Question:** In which order are the bytes of an IP datagram transmitted?
- **Answer:**
    - Transmission is row by row
    - For each row:
        1. First transmit bits 0-7
        2. Then transmit bits 8-15
        3. Then transmit bits 16-23
        4. Then transmit bits 24-31
- This is called **network byte** order or **big endian** byte ordering.

- **Note:** some computers store 32-bit words in **little endian** format.

Fields of the IP Header

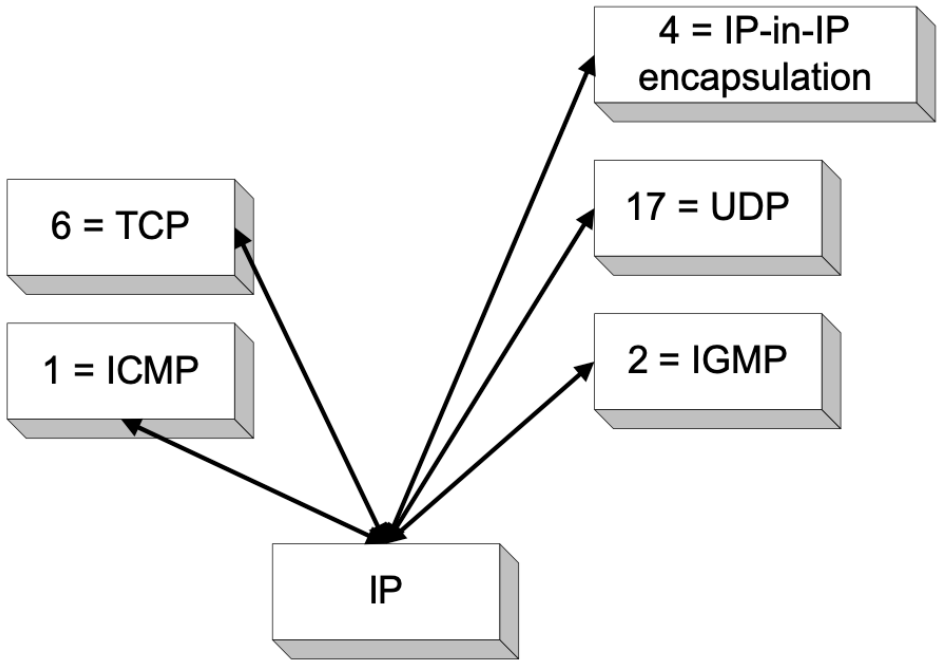
- **Version (4 bits)**: current version is 4, next version will be 6.
- **Header length (4 bits)**: length of IP header, in multiples of 4 bytes
- **DS/ECN field (1 byte)**
  - This field was previously called as Type-of-Service (TOS) field. The role of this field has been re-defined, but is "backwards compatible" to TOS interpretation
  - Differentiated Service (DS) (6 bits):
    - Used to specify service level (currently not supported in the Internet)
  - Explicit Congestion Notification (ECN) (2 bits):
    - New feedback mechanism used by TCP
- **Identification (16 bits):** Unique identification of a datagram from a host. Incremented whenever a datagram is transmitted
- **Flags (3 bits):**
  - First bit always set to 0
  - DF bit (Do not fragment)
  - MF bit (More fragments)

  Will be explained later→ Fragmentation

Fields of the IP Header

- **Time To Live (TTL) (1 byte):**
  - Specifies longest paths before datagram is dropped
  - Role of TTL field: Ensure that packet is eventually dropped when a routing loop occurs

  Used as follows:
  - Sender sets the value (e.g., 64)
  - Each router decrements the value by
  - When the value reaches 0, the datag
- **Protocol (1 byte):**
  - Specifies the higher-layer protocol.
  - Used for demultiplexing to higher layers.



Fields of the IP Header

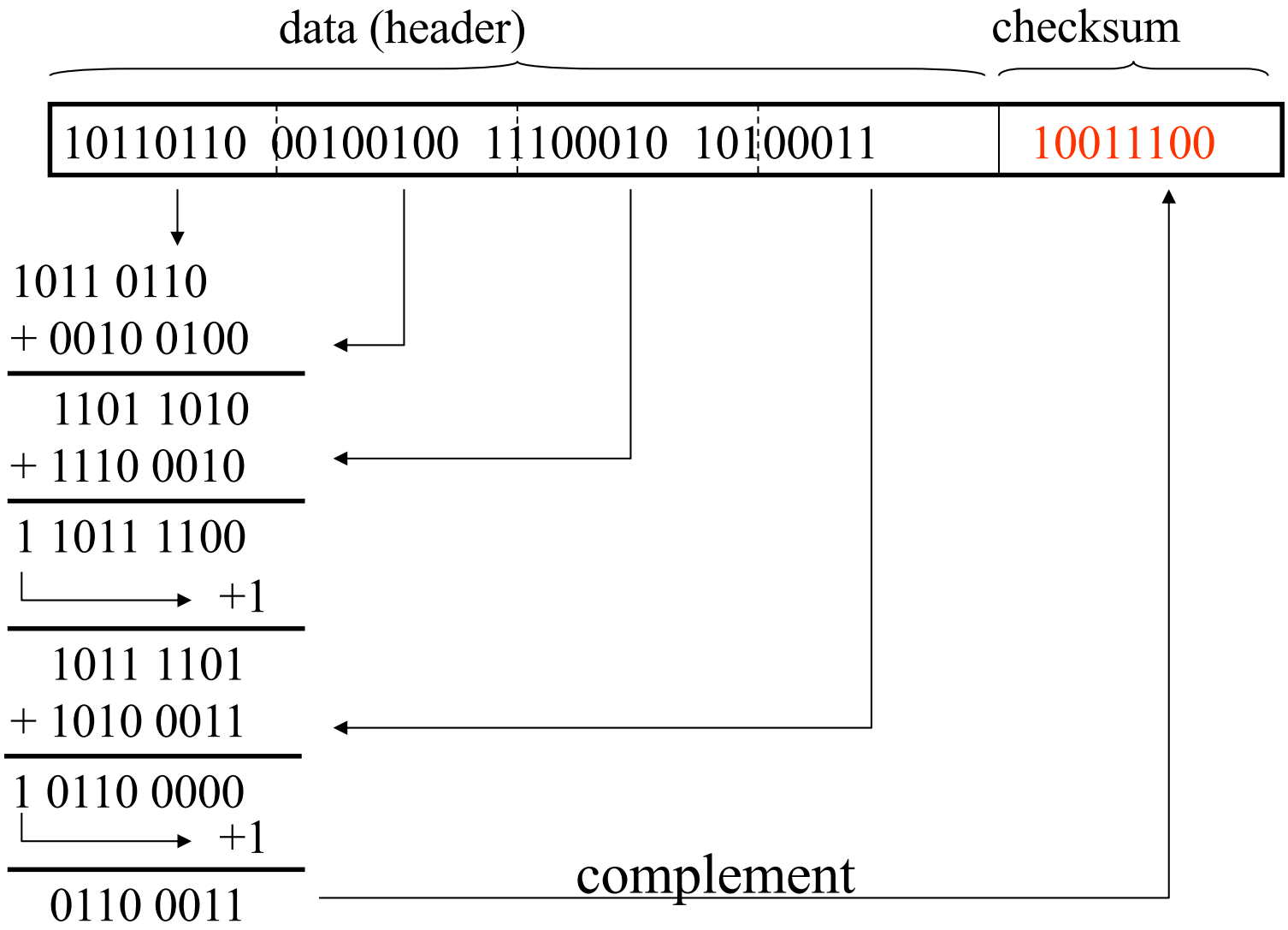
- **Header checksum (2 bytes):** A simple 16-bit long checksum which is computed for the header of the datagram.
- Checksum (16 bits)
  - Complement of the *one's-complement* sum of all 16-bit words in the IP **packet header**
- Each router computes ones-complement sum of entire header *including checksum* …
  - … should get 0 (or 0xffff)
  - If not, router discards packet as corrupted
    - So it doesn't act on bogus information

Fields of the IP Header

- Assume 8-bit numbers
  - Numbers starting with “0” are positive
    - E.g., 00001111 → 15;
  - Numbers starting with “1” are negative; negative number is obtained by inverting all bits of the positive number
    - E.g., 11110000 → -15
  - 00000000 and 11111111 both represent 0
- Addition: add carry-on to result

```
00001111      (15)
+ 11110111    (-8)
-------------------
1 00000110
  └──────→ + 1
-------------------
  00000111    (7)
```

Fields of the IP Header - Checksum Example



Fields of the IP Header

- **Options:**
  - Security restrictions
  - Record Route: each router that processes the packet adds its IP address to the header.
  - Timestamp: each router that processes the packet adds its IP address and time to the header.
  - (loose) Source Routing: specifies a list of routers that must be traversed.
  - (strict) Source Routing: specifies a list of the only routers that can be traversed.
- **Padding:** Padding bytes are added to ensure that header ends on a 4-byte boundary

Maximum Transmission Unit

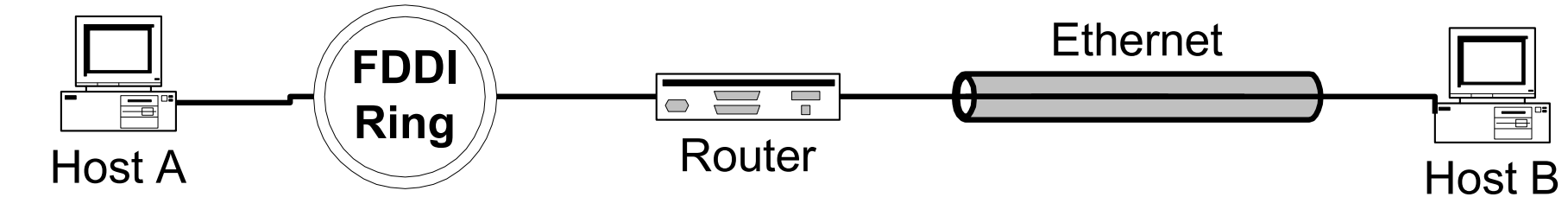
- Maximum size of IP datagram is 65535 (Bytes), but the data link layer protocol generally imposes a limit that is much smaller
- Example:
  - Ethernet frames have a maximum payload of 1500 bytes

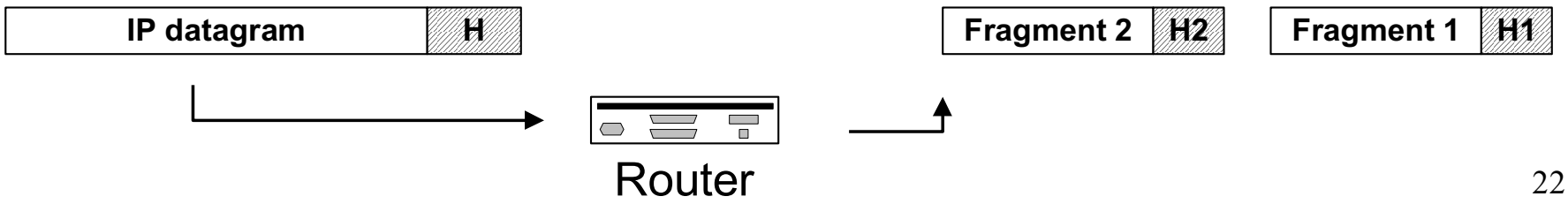
    → IP datagrams encapsulated in Ethernet frame cannot be longer than 1500 bytes
- The limit on the maximum IP datagram size (Bytes), imposed by the data link protocol is called **maximum transmission unit (MTU)**
- MTUs for various data link protocols:

  Ethernet: 1500
  802.3: 1492
  802.5: 4464
  X.25: 576
  FDDI: 4352
  ATM AAL5: 9180
  PPP: negotiated < 1492
  Hyperchannel: 65535
- **Jumbo-frames -** modern Ethernet adapters and switch's use Jumbo-frames include 1500<MTU<16000 bytes, real <9000 bytes, because CRC-32 not effective after 12000 bytes.
- **Jumbogram** - IPv6 packet that can transfer data up to 4 GB.

IP Fragmentation

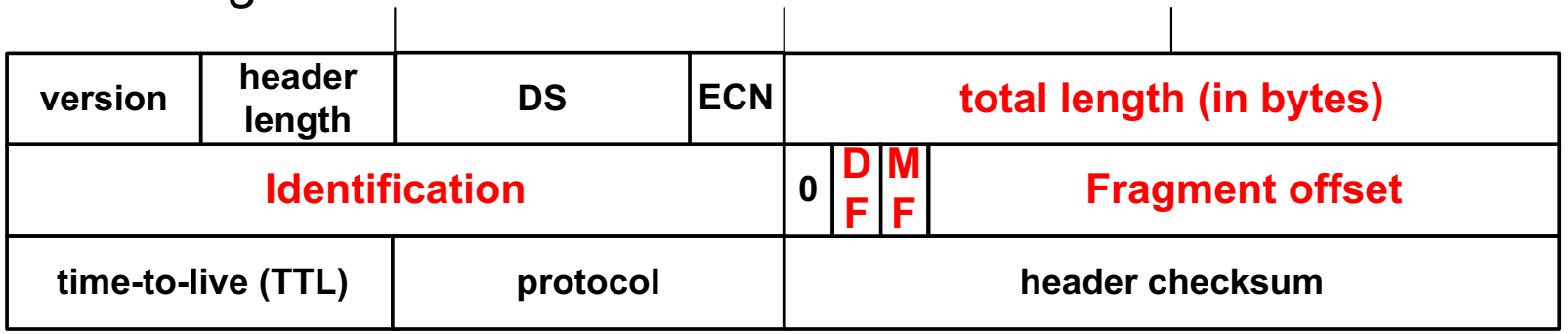
- What if the size of an IP datagram more then MTU?
  IP datagram is fragmented into smaller units.
- Why fragmentation is undesirable?
  If one fragment is lost, the datagram must be retransmitted as a whole.
- What if the route contains networks with different MTUs?
  - Fragmentation can be done at the sender or at intermediate routers
  - IP router splits the datagram into several datagram
  - The same datagram can be fragmented several times.
  - Reassembly of original datagram is only done at destination hosts !!





What's involved in Fragmentation?

- The following fields in the IP header are involved:



Identification:

- When a datagram is fragmented, the identification is the same in all fragments.

Flags:

- DF bit is set: Datagram cannot be fragmented and must be discarded if MTU is too small;
- MF bit set: This datagram is part of a fragment and an additional fragment follows this one.

Fragment offset:

- Offset of the payload of the current fragment in the original datagram

Total length of the all datagram or the current fragment after fragmentation.

Example of Fragmentation

- A datagram with size 2400 bytes must be fragmented according to an MTU limit of 1000 bytes