CSC 402 – Internet Technology

Recap

- TCP/IP model
- Layers of TCP/IP model
- OSI & TCP/IP
- OSI vs. TCP/IP

Internetworking Terms

- **Circuit switching**: E.g. PSTN (Public Switched Telephone Network)
  - Dedicated communications path established between two sides through the nodes of the network for the duration of the conversation.
  - Path is a sequence of connected physical links between nodes.
  - Data generated by the source side is transmitted along the dedicated path as rapidly as possible (with the speed of the slowest link).
  - At each (transit) node incoming data are routed or switched to the appropriate outgoing channel without delay
- **Packet Switching**
  - Data sent out in small chunks (**packets**). No dedicated transmission capacity along a path.
  - Possible out of sequence delivery.
  - Each packet passed through the network from node to node between source and destination.
  - At each node the entire packet is received, stored and transmitted to the next node (store-and-forward).
  - Used for terminal to computer and computer to computer communications

Internetworking Terms

- **End system** – a device attached to a network that is used to support end-user applications and services E.g., a desktop PC, a Web server, a DNS server.
- **Intermediate system** – a device used to connect 2 or more networks and permit communication between end systems attached to different networks E.g., a bridge, a router, a gateway.
- **Communication network (network)** – a system of interconnected intermediate systems, end systems, and other equipment allowing information to be exchanged.
  - Basically, a network can be of any size, from 2 to thousands devices.
  - When networks get very large and are clearly comprised of smaller networks connected together, they are often no longer called networks but internetworks.

Internetworking Terms

- **Subnetwork (subnet)** – a part of a network (i.e. a network that is part of a larger internetwork).
  - Subnetwork can be quite large when it is a part of a network that is very large.
  - The abbreviated term ”subnet” refers generally to a subnetwork, but also has a specific meaning in the context of IP addressing
- **Network segment** – a small part of a network.
  - In some contexts, a segment is the same as a subnetwork and the terms are used interchangeably.
  - More often, however, the term ”segment” implies something smaller than a subnetwork.
  - The earliest forms of Ethernet used coaxial cables, and the coaxial cable itself was called a ”segment”.
- **TCP/IP network** – a network that uses the TCP/IP protocol suite.
- **Host** – a computer that is connected to a TCP/IP network, including the Internet

Internetworking Terms

- **Encapsulation:** Literally encapsulation is including data from an upper layer protocol into a lower layer protocol, gradually adding functionality.
  - Each PDU contains both payload data and control information.
  - Control information falls into:
    - address information
    - error-detecting code
    - protocol control
- **Sequencing**: In connection-oriented data transfer each PDU is given a unique number called sequencing.
- **Segmentation**: Usually, the data transfer between two entities can be characterized as consisting of a sequence of data blocks of some bounded size.
  - From the application point of view network interface is seen as pipe-like connection.
  - Application layer messages may be large, therefore lower-layer protocols may need to break the data into blocks of smaller size - this process is called segmentation (or **fragmentation in TCP/IP**).

Internetworking Terms

- **Advantages of fragmentation**:
  - Communication network may only accept blocks of data up to a certain size: e.g. Ethernet blocks (frames) size is limited up to 1526 bytes; Wi-Fi frame is limited by 2346 bytes.
  - Error control may be more efficient with a smaller PDU size.
  - Fairness of access to shared transmission facilities, with shorter delay, can be provided.
  - Smaller PDU size may require smaller buffers on the receiving side.
  - Restart/recovery operations easier to perform.
- **Disadvantages of fragmentation**:
  - Increased overhead - the smaller the block, the greater the overhead percentage
  - PDU arrival may generate an interrupt that must be served, smaller blocks result in more interrupts at receiver
  - More processing time

Internetworking Terms

- **Protocol Data Unit (PDU)**: In general, PDU is the combination of data from the next higher layer and some additional control information (header).
- **Transport layer PDU**: Control information is added to user data at each layer Transport Layer PDU (often referred to as **segment**, don't confuse with Network segment).
  - Transport layer may fragment or concatenate user data.
  - The header in each transport PDU contains control information to be used by the peer transport protocol at another side.
  - Examples of information that may be stored in the header:
    - Destination SAP (Service Access Point) allows each application individually accessing the services of the transport layer.
    - Sequence number to assure proper order of PDU sequence on receiving side.
    - Error detection code used to detect and (if possible) correct transmission errors

Internetworking Terms

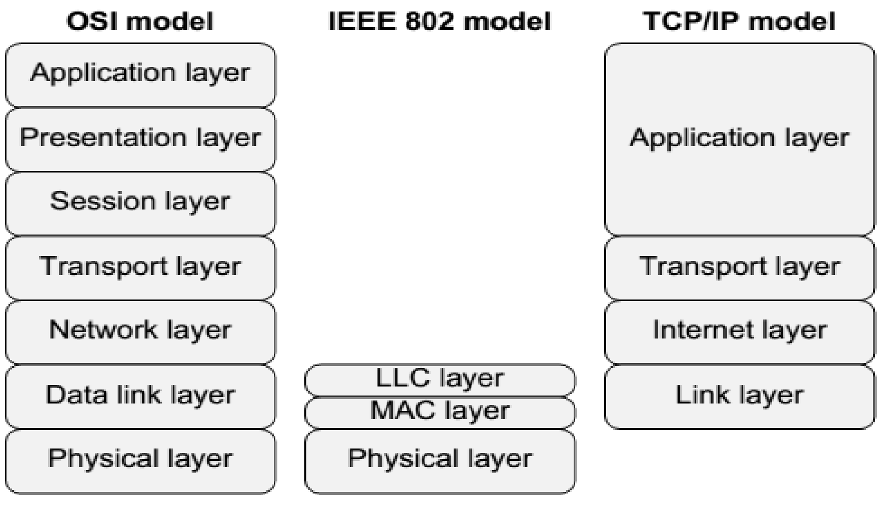
- **Network layer PDU**, often referred to as **datagram** or **packet**.
  - Used for data transmission to the destination side.
  - Also requires use of some control information, therefore network access protocol appends to the data it receives from the transport layer (creating a network access PDU):
    - Network address for destination computer.
    - Facilities requests.
    - The network access protocol might want the network to exercise certain facilities, such as priority
- **Connection-oriented mode** of operation includes the establishment of logical connection between 2 end systems.
  - The logical connection is set up first.
  - Then data are exchanged.
  - After the data transfer ends, the logical connection should be terminated
  - In a connection-oriented mode of operation, since all packets follow the same route, they arrive **in order**
  - They are reliable because they first gain a system's attention, prepare it to receive information, then send the information.
  - However, they require more system overhead, and are not always appropriate for certain networking tasks. E.g TCP, analogy: telephone call (establish connection before talking).

Internetworking Terms

- **Connectionless mode** of operation , data is just sent without a connection being created
  - Data is sent from one end system to another without prior arrangement.
  - Each packet is treated and routed independently of any other packets.
  - Since packets may travel different routes between the source and destination, they may arrive at the destination out of order.
  - In a connectionless mode of operation, each packet must contain complete routing information, since packets are routed individually.
  - Connectionless protocols rely on **the ”best-effort” approach**: they send the information, hoping that it will reach the other system. E.g. IP, analogy: sending postcard.

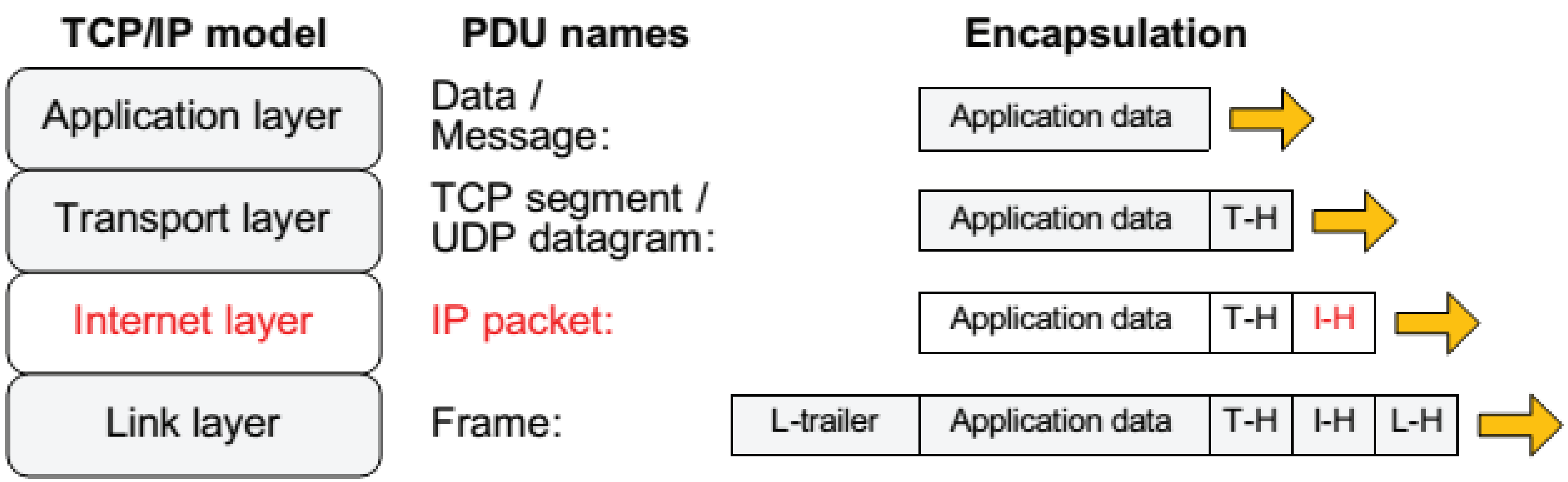
IEEE 802 Model

- The IEEE 802 model covers the physical and data link layers of the OSI reference model.
- The layers communicate using encapsulation/decapsulation of PDUs.
- The IEEE 802 model subdivides the data link layer of the OSI model into 2 layers:
  - The Logical Link Control (LLC) layer
  - The Media Access Control (MAC) layer



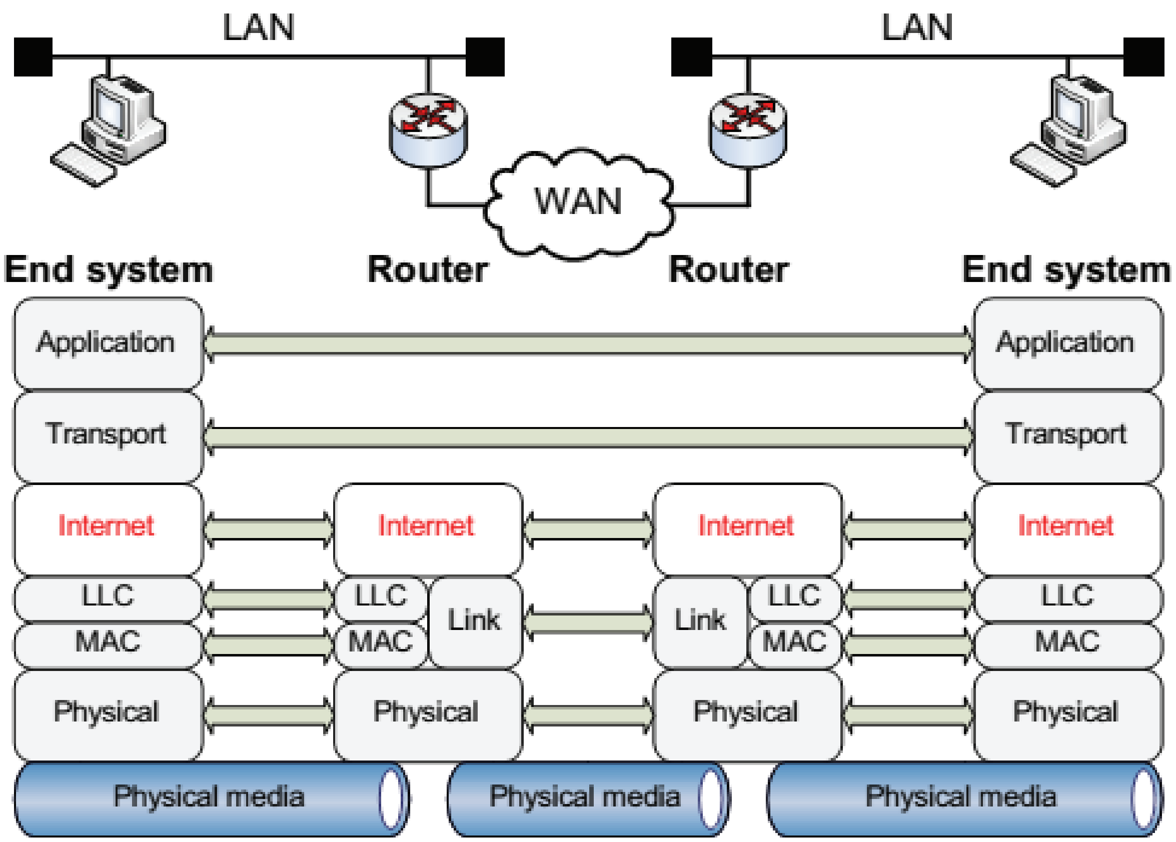
Internet Layer

- **The Internet layer** (**or IP Layer**, refer CSC-402_L4 for protocol suites in this layer) resides between the Transport and Link layers.
- Provides a connectionless best-effort delivery service for the Transport layer.
- Uses the services offered by the underlying Link layer.
- Hides the details of underlying networking from the higher layers



Internet Layer

- The Internet Protocol is a **hop-by-hop** protocol.



IP Overview

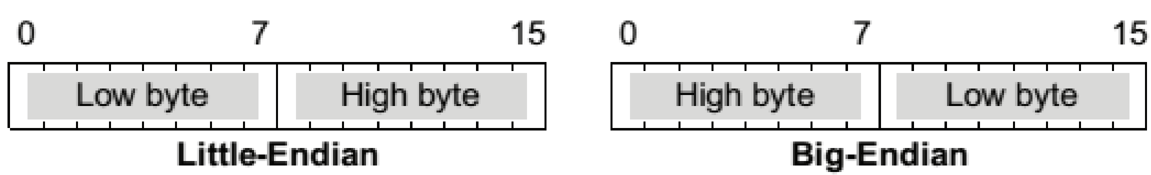
- **The Internet Protocol (IP)** is the heart of the TCP/IP protocol suite.
- IP corresponds to the Network layer of the OSI reference model.
  - The Network layer is primarily charged with the delivery of data, not between devices on the same physical network, but between devices that may be on different networks that are interconnected in an arbitrary manner.
- Why IP? Because, IP is said to be:
  - **Universally-addressed**: IP defines the addressing mechanism for internetworking and uses these addresses for delivery purposes.
  - **Underlying-protocol independent**: IP is designed to allow the transmission of data across any type of underlying network that is designed to work with the TCP/IP suite.
  - **Connectionless**: IP does not require a connection to be established before data transfer can begin.
  - **Unreliable (aka best-effort)**:
    - IP tries its best to forward packets to the destination, but does not guarantee that a packet will be delivered to the destination.
    - IP does not make any guarantee on the Quality of Service (QoS) and provides delivery without acknowledgements.
    - An application requiring reliability in packet delivery must implement the reliability function within a higher-layer protocol

IP Overview

- A bit is a **BI**nary digi**T**. So a bit is a zero or a one. A **byte** is a sequence of 8 bits i.e. $2^8 = 256$ possible values.
- A **word** is the number of bits that are manipulated as a unit by the particular CPU of the computer. Today most CPUs have a word size of 32 or 64 bits.
- The IPv4 "Total Length" header field has 16 bits to indicate the size of the packet in bytes.
- So we have 16 bits that can have a maximum value of 1111111111111111 = 65,535 bytes.
- The result that we received is just a "16 bit word" that gives us a certain indication on how big the packet is.
- Although RFC 791 states that “The Internet protocol provides for transmitting blocks of data called datagrams from sources to destinations. . . ”, technicians often use the term “packets” to avoid confusion with UDP datagrams.

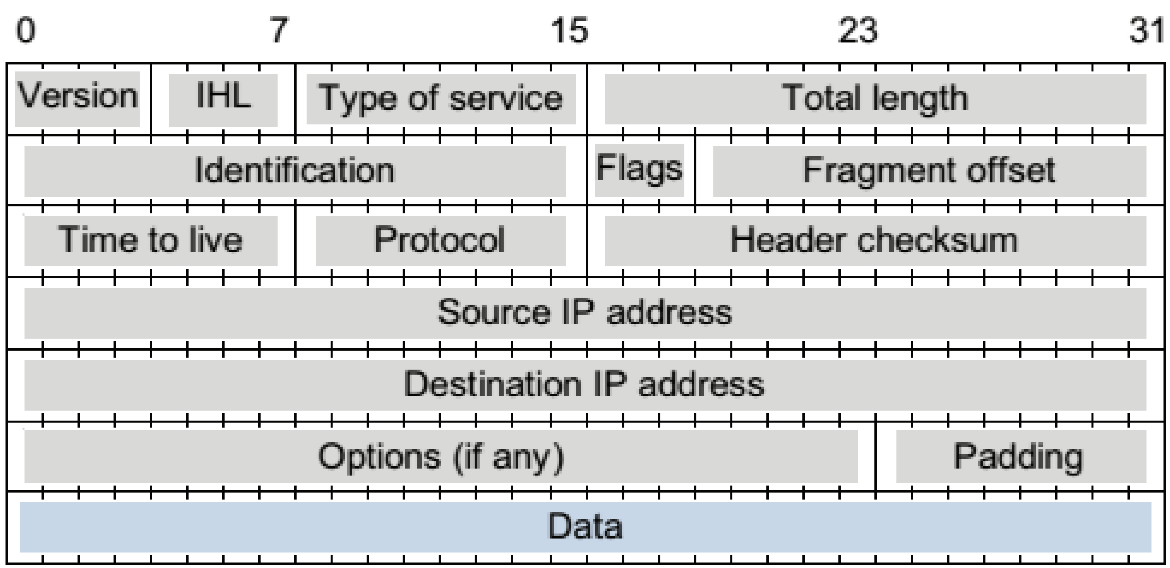
Endiannes

- Some human languages are read and written from left to right; others from right to left. Some countries use left driving; others use right driving.
- **Endianness** (origin Gulliver's Travel) is the attribute of a system that indicates whether integers are represented from left to right or right to left.
- Endianness comes in 2 variants: little and big
  - If the least significant byte is stored first (has the lowest memory address), it is known as **Little-Endian**.
  - If the most significant byte is stored first (has the lowest memory address), it is known as **Big-Endian** (Big-Endian does not mean "ending big", but "big end first").
- Analogy: difference between remembering the number "three hundred twenty-one" as 123 or 321).
- The Internet adopts **Big-Endian format**. This representation is also known as **network byte order**.



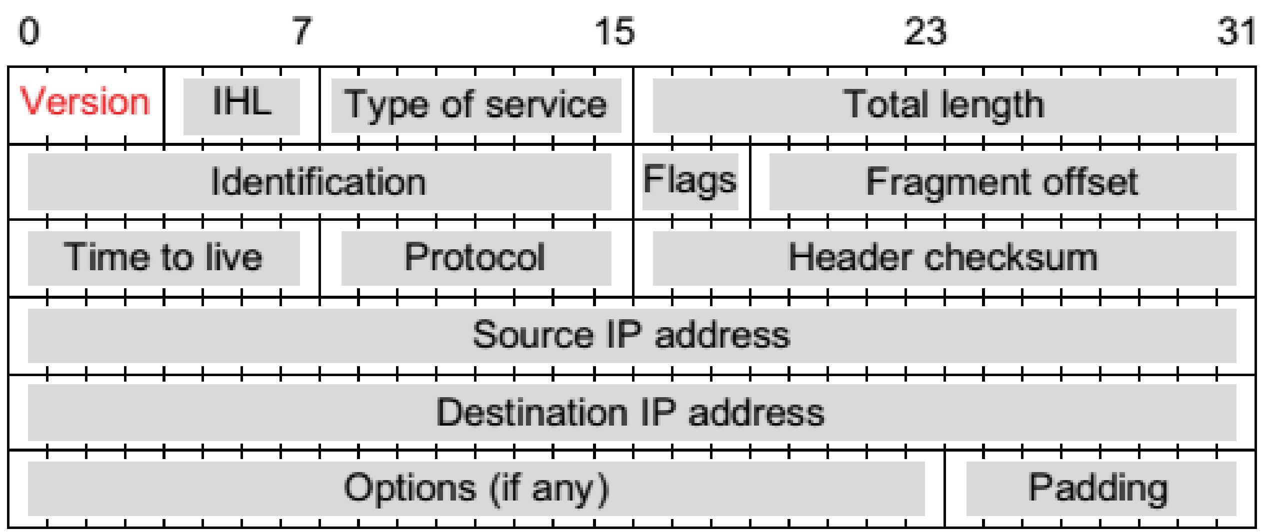
IPv4 – Packet Structure

- An IP packet consists of a header and a data part.
  - The header has a fixed-length component of 20 bytes plus a variable-length component consisting of options that can be up to 40 bytes.
  - Since the total length of the IP packet is measured in bytes, the Data field must contain an integer number of bytes.
  - IP packets are transmitted according to network byte order.



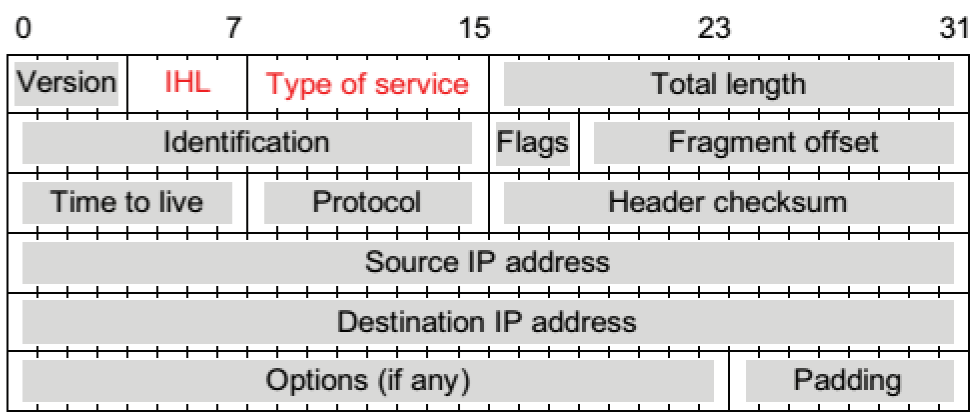
IPv4 – Packet Structure

- Version, 4 bits
  - Indicates version number, to allow evolution of the protocol.
  - The current IP version is 4.
  - Number 5 is reserved for the Internet Stream Protocol version 2 (ST2), defined in RFC 1819.
  - Number 6 is used for the next generation IP known as **IPv6** or **IPng**.



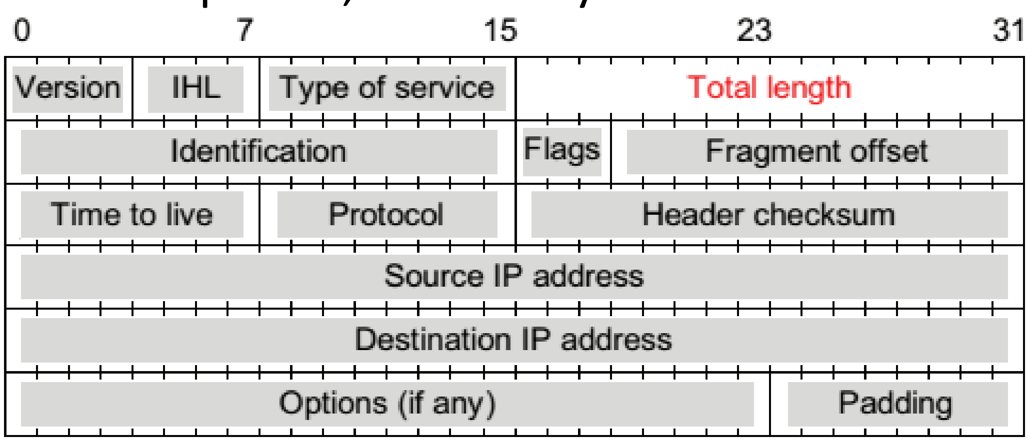
IPv4 – Packet Structure

- **Internet header length (IHL)**, 4 bits.
  - Specifies the length of the header in 32-bit words.
  - The minimum value is 5 (20 bytes), the maximum value is 15 (60 bytes).
  - If no options are present, IHL = 5.
  - The length of the Options field can be determined from IHL.
- **Type of service (TOS)**, 8 bits
  - Specifies priority, delay, throughput, reliability, and cost requirements.
  - 3 bits are assigned for priority levels (called ”**precedence**”) and 4 bits for specific requirements (Delay, Throughput, Reliability, and Cost). Default value is 0.



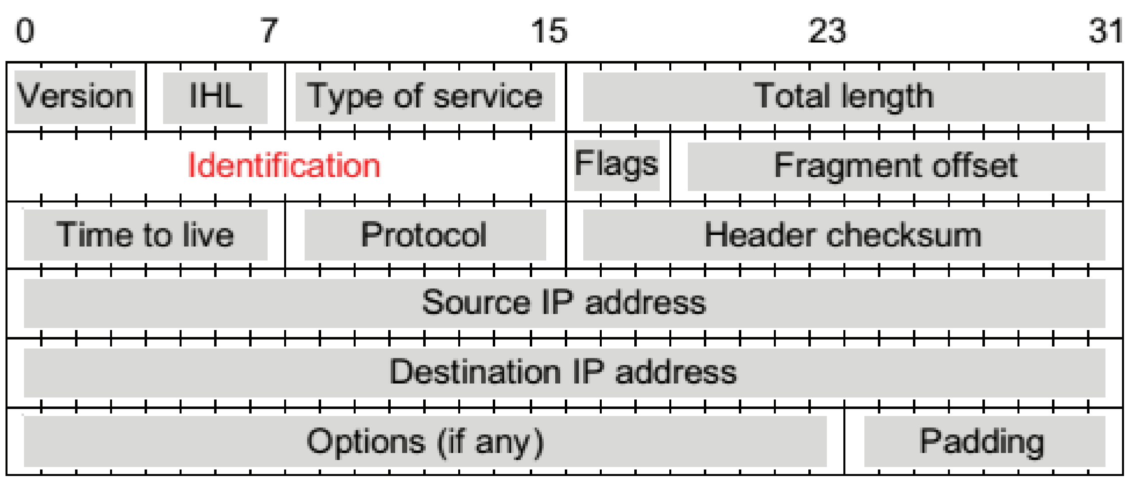
IPv4 – Packet Structure

- **Total length**, 16 bits
- Specifies the number of bytes of the IP packet including header and data.
- The minimum packet length is 28 bytes, using the minimum 20 bytes of header information, followed by the minimum of 8 bytes of data.
- The maximum packet length is 2^16 − 1 = 65535 bytes.
- However, most physical networks have their own length limitations. E.g., Ethernet II limits the payload length and, consequently, the maximum length of an IP packet, to 1500 bytes.



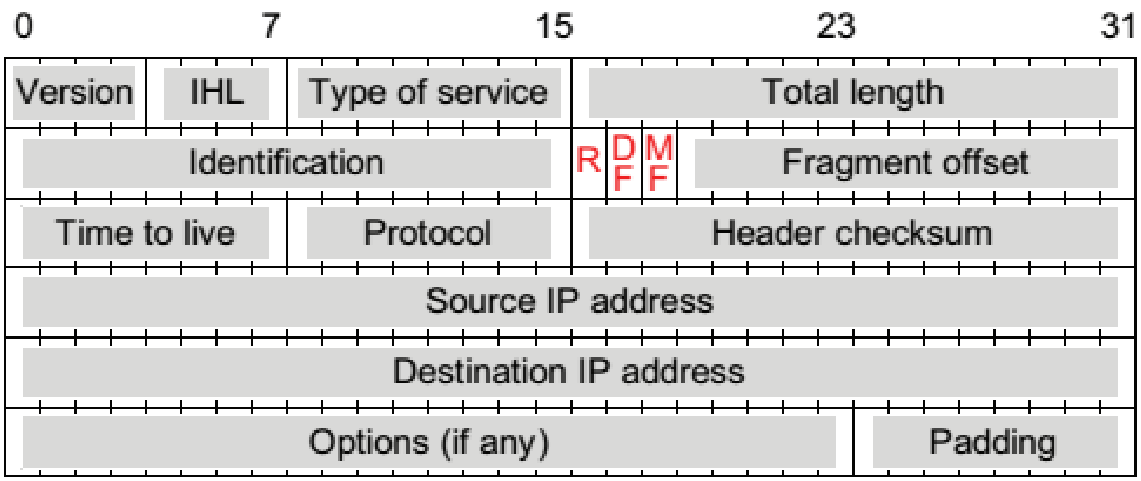
IPv4 – Packet Structure

- **Identification**, 16 bits
- A sequence number that, together with the source IP address, destination IP address, and the Protocol field, is intended to identify a packet uniquely for the time it will be active in the internetwork.
- A total of 216 = 65536 different identifiers can be used.
- The field is used by the destination host to reassemble fragmented packets.



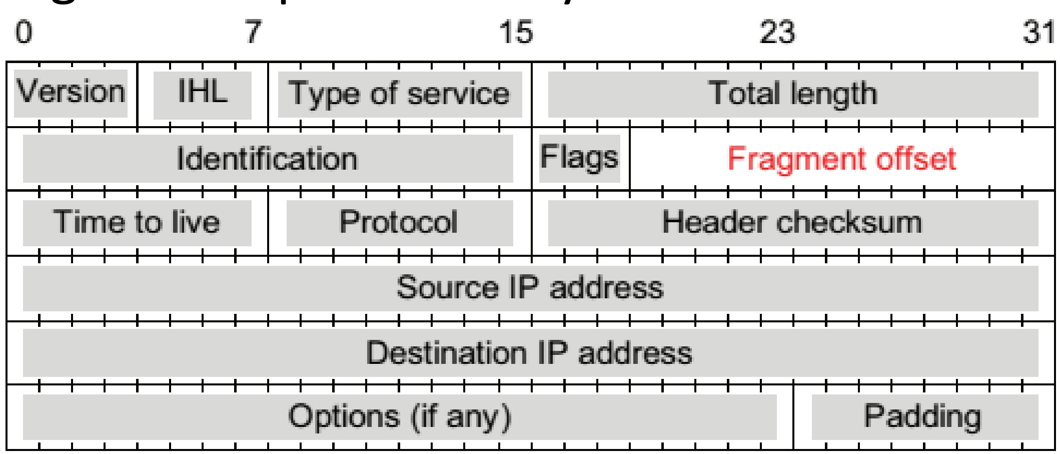
IPv4 – Packet Structure

- **Flags**, 3 bits
- There are 3 control flags, 2 of which are used to manage fragmentation and 1 is reserved.
- Bit R: Reserved, must be 0
- Bit DF: 1 = Don’t Fragment; 0 = may be fragmented
- Bit MF: 1 = More Fragments; 0 = last fragment



IPv4 – Packet Structure

- **Fragment offset**, 13 bits
- When fragmentation of a packet occurs, this field specifies the offset (position) in the overall massage where the data in this fragment goes.
- It is specified in units of 8 bytes.
- The first fragment has the offset of 0.
- An unfragmented packet always has an offset value of 0.



IPv4 – Packet Structure

- **Time to Live** (**TTL**), 8 bits
- Specifies how long, in seconds, the packet is allowed to travel. The maximum value is 28 − 1 = 255 seconds or 4.25 minutes.
- However, most routers in present day interpret this value as the number of hops the packet is allowed to traverse in the internetwork.
- Initially, the source host sets this field to some value. Each router along the path to the destination host decrements it by 1.
- If the value reaches 0 before the packet reaches the destination, the router discards the packet and sends an error message to the source.