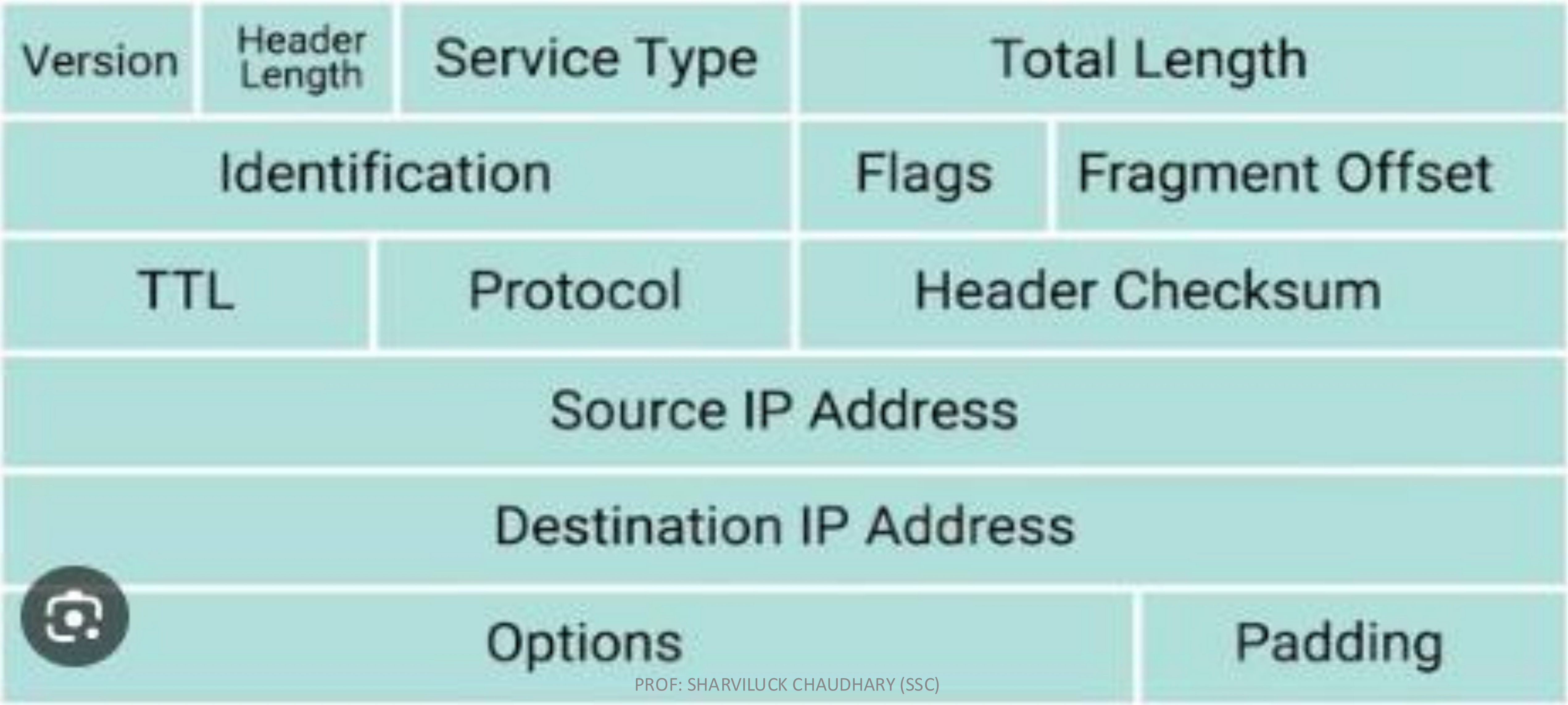
UNIT - 2

TCP/IP Protocol II

Internet Protocol (IP) Datagram

- IP Datagram. A datagram is “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

Structure of the IP Datagram



Version | Header Length | Service Type | Total Length

Identification | Flags | Fragment Offset

TTL | Protocol | Header Checksum

Source IP Address

Destination IP Address

Options | Padding

Characteristics of IP Datagram

- **Connectionless**: IP operates in a connectionless manner, meaning each datagram is handled independently and does not require prior setup of a dedicated connection.

- **Best Effort Delivery**: IP provides best-effort delivery, where it attempts to deliver datagrams to the destination without guarantees of reliability, sequencing, or error recovery. Higher layers such as TCP provide these features if needed.

- **Fragmentation and Reassembly**: IP allows for fragmentation of datagrams into smaller pieces to fit within the Maximum Transmission Unit (MTU) of the underlying network. Fragments are reassembled at the destination if they arrive out of order.

- **Routing**: IP uses routing tables and algorithms to determine the best path for forwarding datagrams from the source to the destination across interconnected networks.

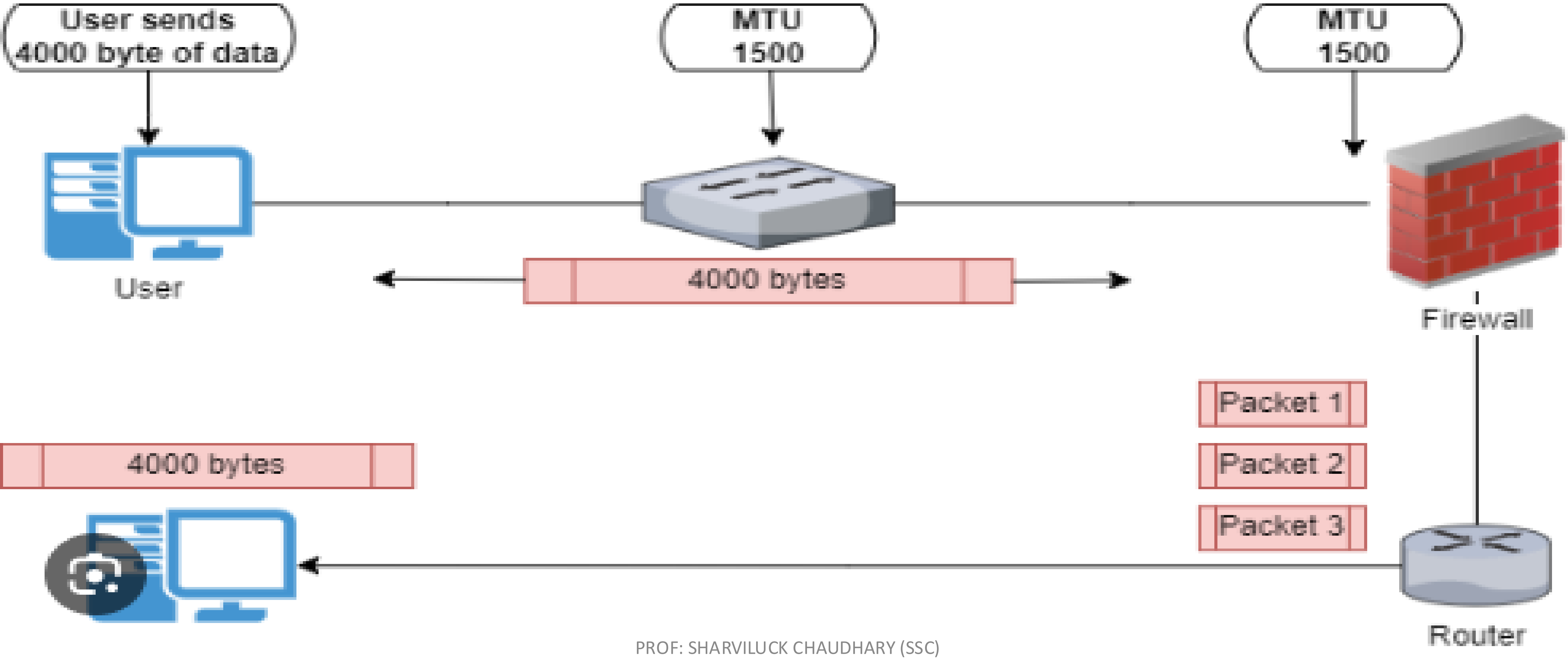
- **Version Support**: IPv4 and IPv6 are the two main versions of IP in use today, with IPv4 being the older and more widely deployed version, while IPv6 offers advantages like larger address space and improved security features.

Fragmentation

- The term fragmentation in computer networks refers to the breaking up of a data packet into smaller pieces in order to fit it through a network with a smaller maximum transmission unit (MTU) than the initial packet size.

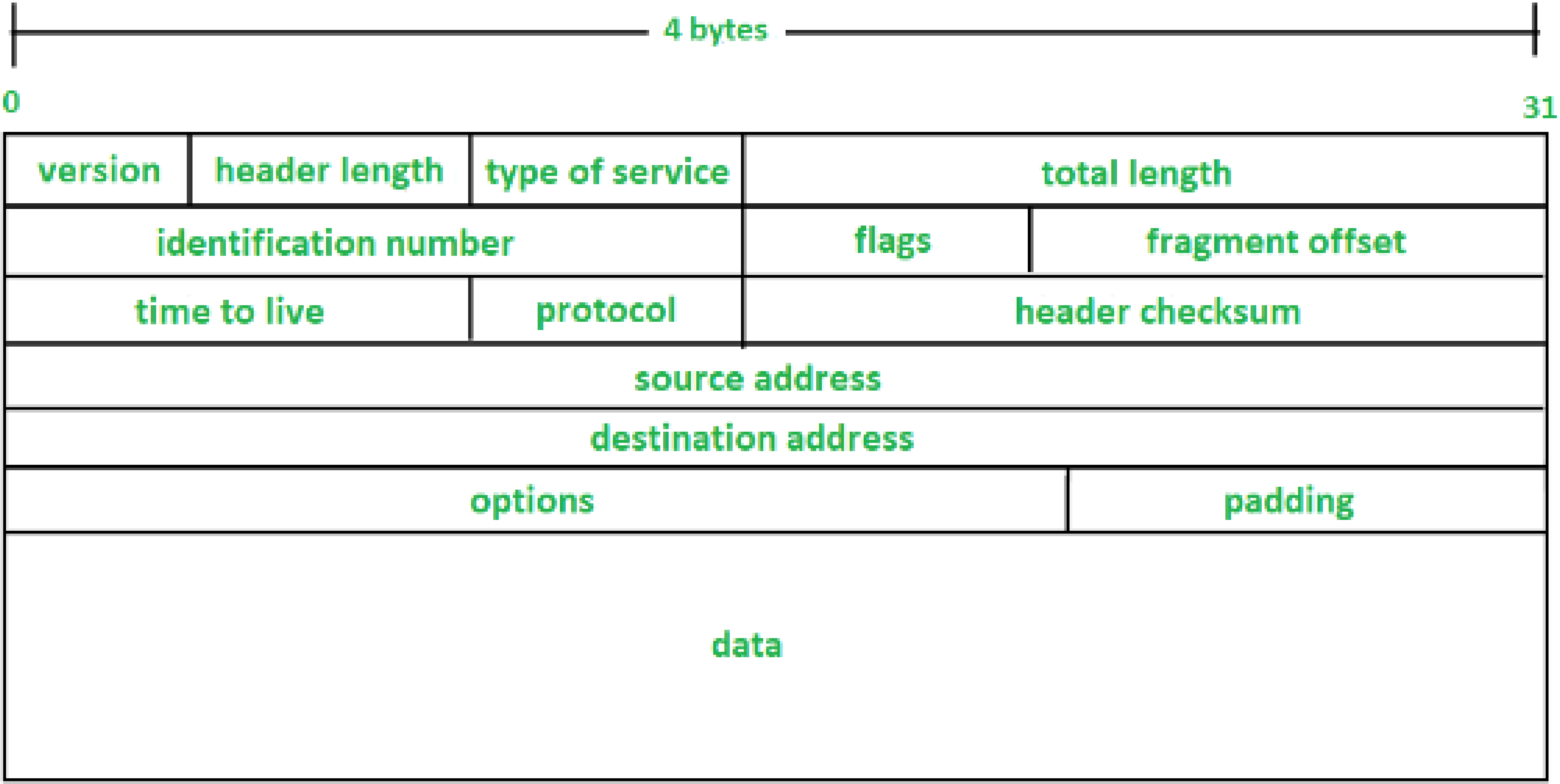
- Maximum Transmission Unit (MTU)

Structure of Fragmentation



(IP) Options

- IP Options provide a way to introduce special-handling services to the datagrams or packets, allowing a system to instruct a router to send the datagram through a predefined network, or to note that the path a datagram took should be



4 bytes

0 31

version | header length | type of service | total length

identification number | flags | fragment offset

time to live | protocol | header checksum

source address

destination address

options | padding

data

(IP) Checksum

- The Internet checksum, also called the IPv4 header checksum is a checksum used in version 4 of the Internet Protocol (IPv4) to detect corruption in the header of IPv4 packets.

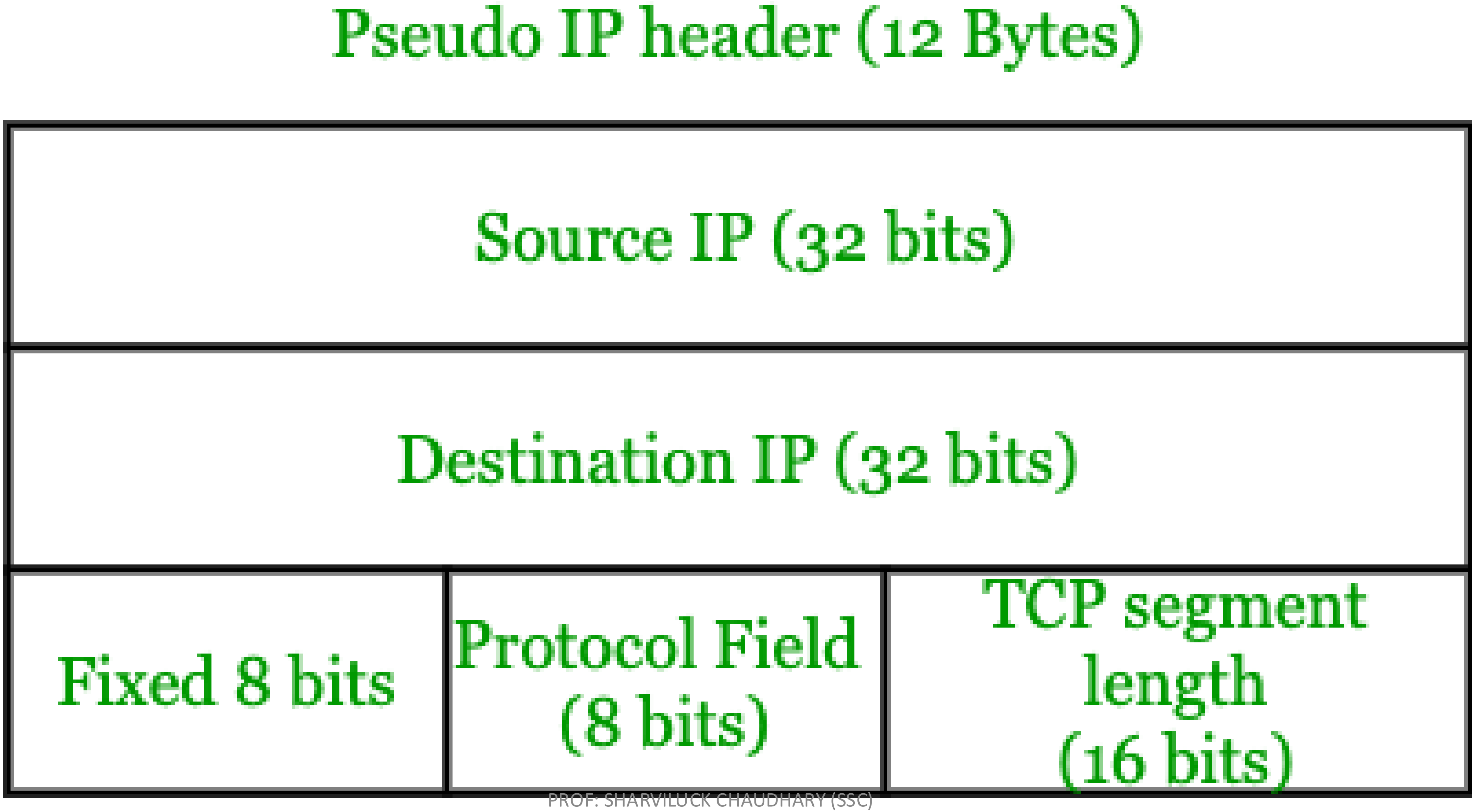
- It is carried in the IP packet header, and represents the 16-bit result of summation of the header words.

Characteristics of IP Checksum

- **Efficiency**: The checksum calculation is lightweight and adds minimal overhead to packet processing.

- **Coverage**: It covers both the IP header and the payload data (if present), ensuring comprehensive error detection.

- **End-to-End Principle**: The checksum verification is typically performed end-to-end, meaning the checksum is checked by the ultimate destination of the datagram.



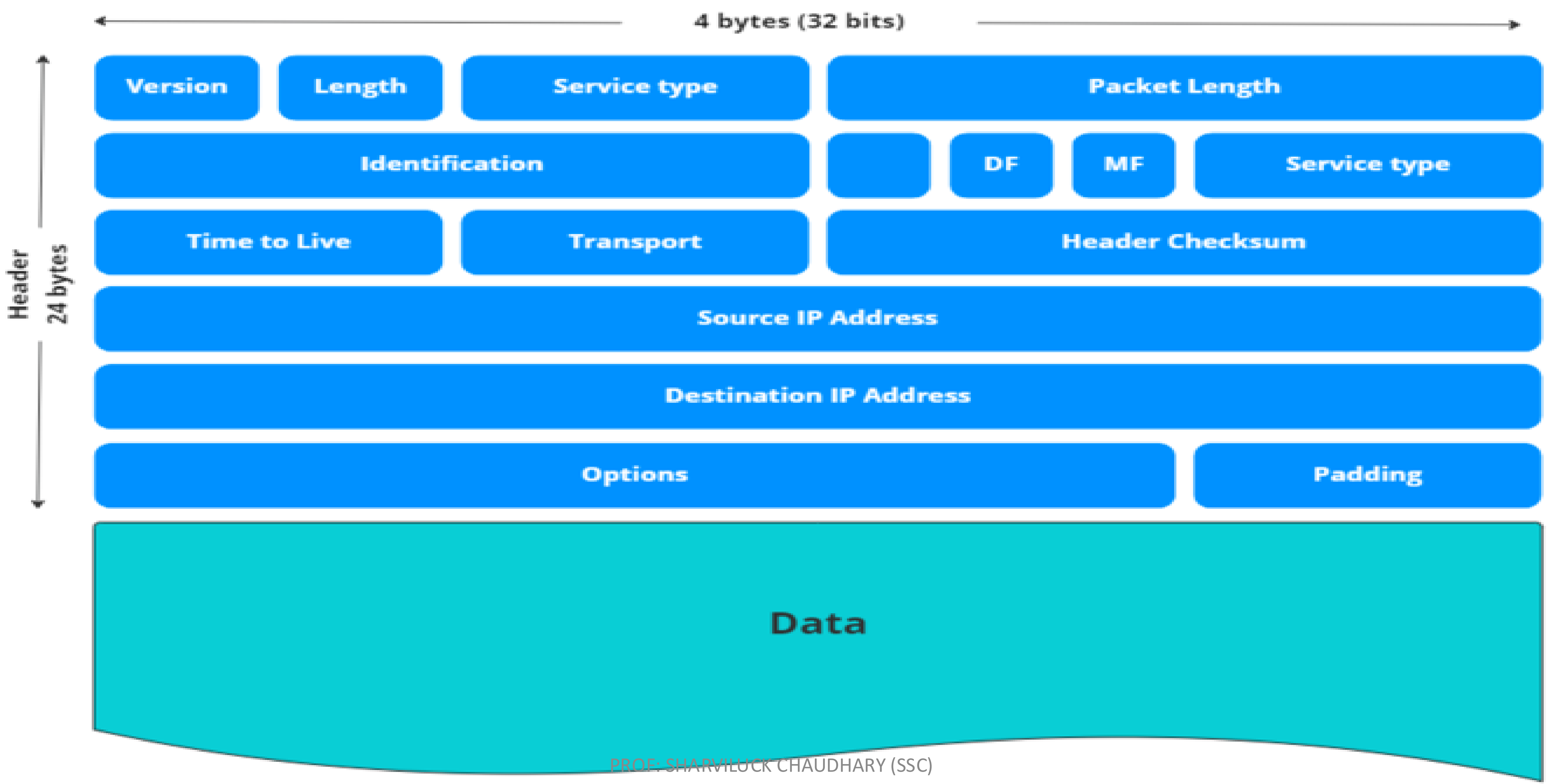
Pseudo IP header (12 Bytes)

Source IP (32 bits)		
Destination IP (32 bits)		
Fixed 8 bits	Protocol Field (8 bits)	TCP segment length (16 bits)

IP package

- An IP packet is a unit of data in a network that contains information about the source and destination addresses and other control information needed to transport the packet over a network.

The structure of an IP packet



4 bytes (32 bits)

Header 24 bytes

Version

Length

Service type

Packet Length

Identification

DF

MF

Service type

Time to Live

Transport

Header Checksum

Source IP Address

Destination IP Address

Options

Padding

Data

Components of an IP Packet

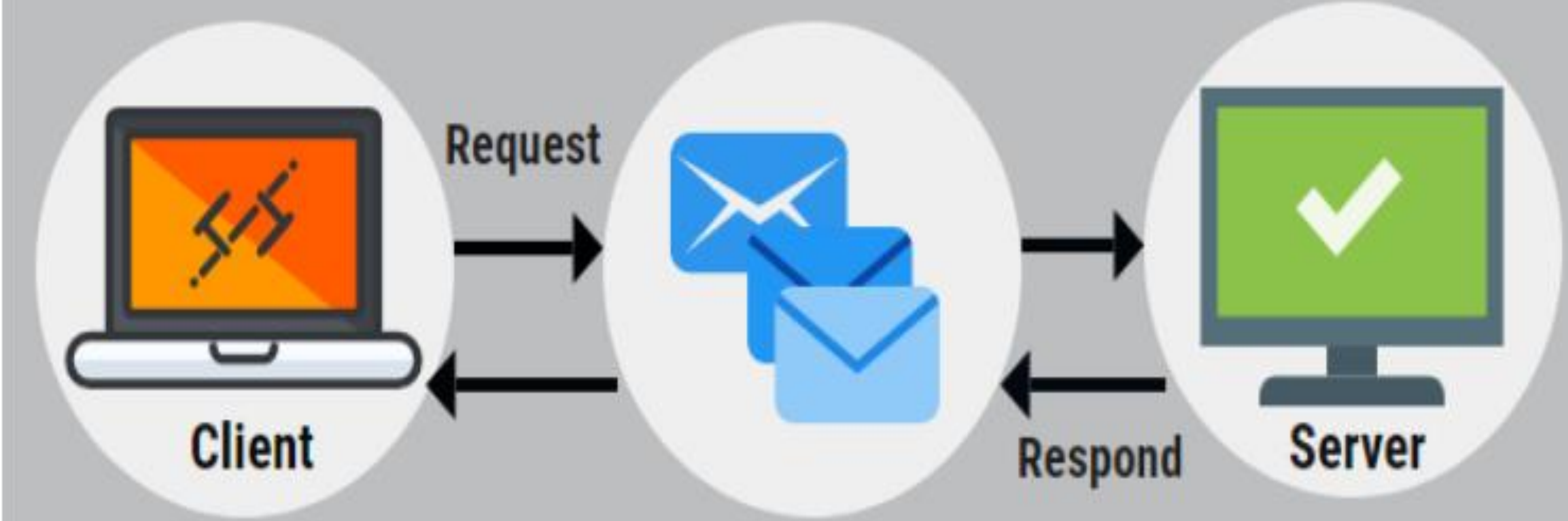
- **Version**: Specifies whether the packet is using IPv4 or IPv6.
- **Header Length**: Length of the IP header in 32-bit words.
- **Type of Service (TOS)**: Defines quality of service parameters such as priority and reliability.
- **Total Length**: Total length of the IP datagram including header and data payload.
- **Identification**: Unique identifier assigned by the sender to aid in reassembling fragmented packets.
- **Flags**: Control fragmentation and reassembly behavior.
- **Fragment Offset**: Position of the fragment in the original datagram for reassembly.
- **Time to Live (TTL)**: Limits the lifespan of the packet in seconds or hops to prevent indefinite circulation.
- **Protocol**: Specifies the protocol of the encapsulated data (e.g., TCP, UDP, ICMP).
- **Header Checksum**: Ensures the integrity of the header information.
- **Source IP Address**: IP address of the sender.
- **Destination IP Address**: IP address of the intended recipient.
- **Options**: Optional fields providing additional features or instructions (rarely used in practice).

User Datagram Protocol (UDP) Process To Process Communication

- User Datagram Protocol (UDP) is a communications protocol for time-sensitive applications like gaming, playing videos, or Domain Name System (DNS) lookups.

- UDP results in speedier communication because it does not spend time forming a firm connection with the destination before transferring the data

User Datagram Protocol



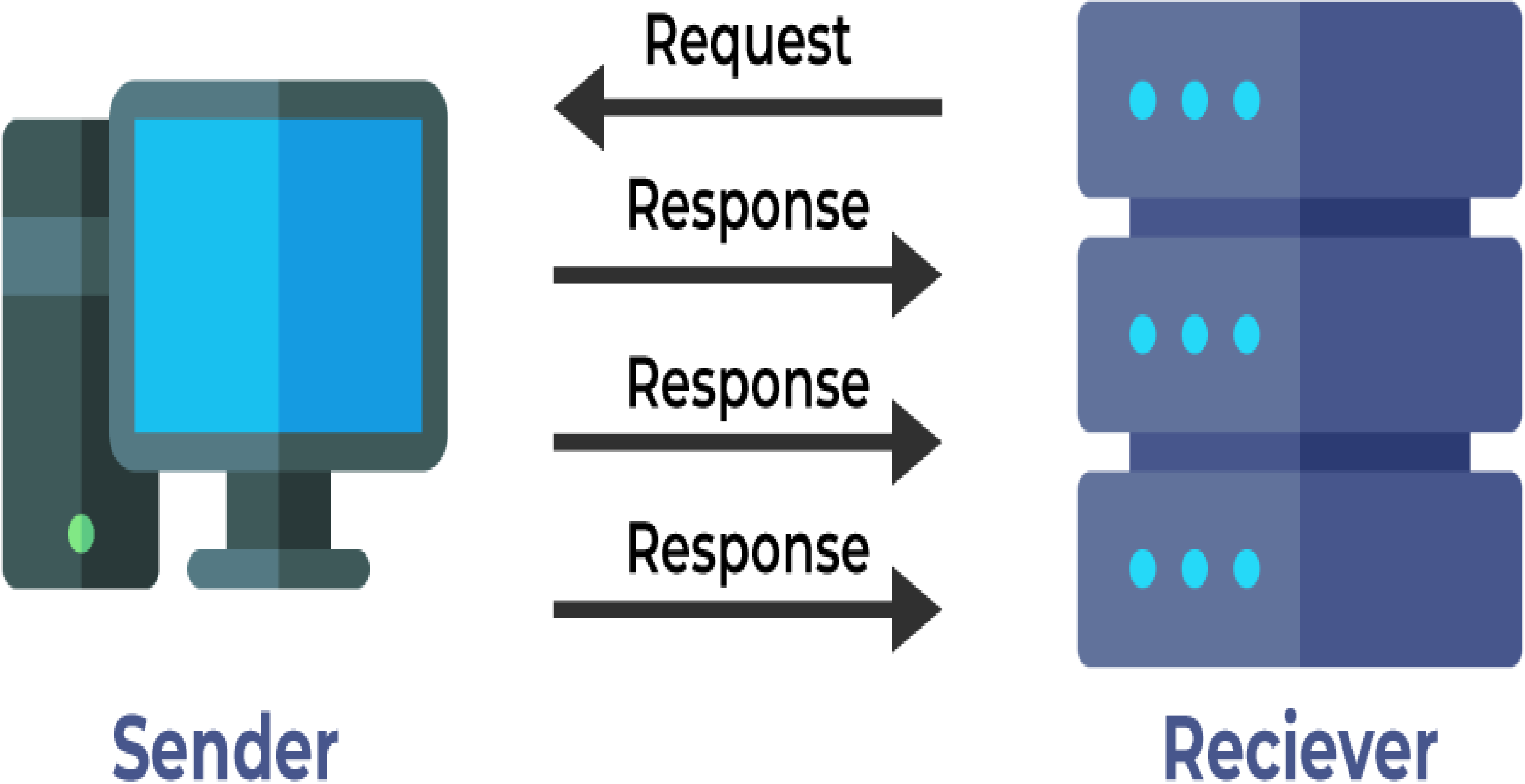
What is User Datagram Protocol (UDP)?

- is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite.

- Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer.

- The UDP helps to establish low-latency and loss-tolerating connections establish over the network.

- The UDP enables process-to-process communication



Request

Response

Response

Response

Sender

Reciever

Features of UDP

- Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.

- It is a suitable protocol for multicasting as UDP supports packet switching.

- UDP is used for some routing update protocols like RIP(Routing Information Protocol).

- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message

Application of UDP

- **Real-Time Multimedia Streaming**: UDP is ideal for streaming audio and video content. Its low-latency nature ensures smooth playback, even if occasional data loss occurs.

- **Online Gaming**: Many online games rely on UDP for fast communication between players.

- **DNS (Domain Name System) Queries**: When your device looks up domain names (like converting "www.example.com" to an IP address), UDP handles these requests efficiently.

- **Network Monitoring**: Tools that monitor network performance often use UDP for lightweight, rapid data exchange.

- **Multicasting**: UDP supports packet switching, making it suitable for multicasting scenarios where data needs to be sent to multiple recipients simultaneously.

- **Routing Update Protocols**: Some routing protocols, like RIP (Routing Information Protocol), utilize UDP for exchanging routing information among routers.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.

Disadvantages of UDP

- We can not have any way to acknowledge the successful transfer of data.

- UDP cannot have the mechanism to track the sequence of data.

- UDP is connectionless, and due to this, it is unreliable to transfer data.

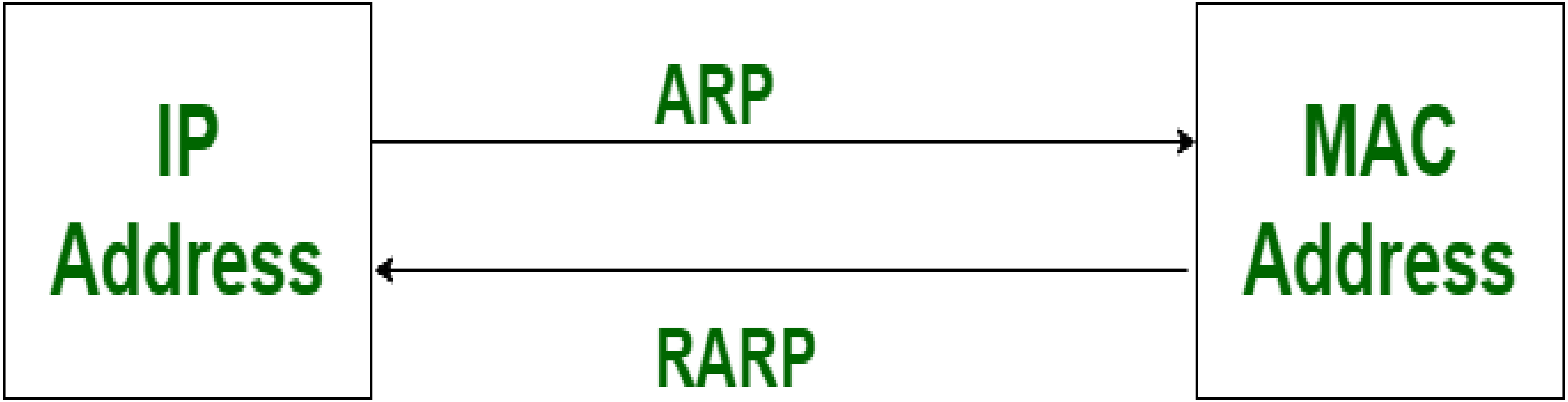
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.

- UDP can drop packets in case of detection of errors.

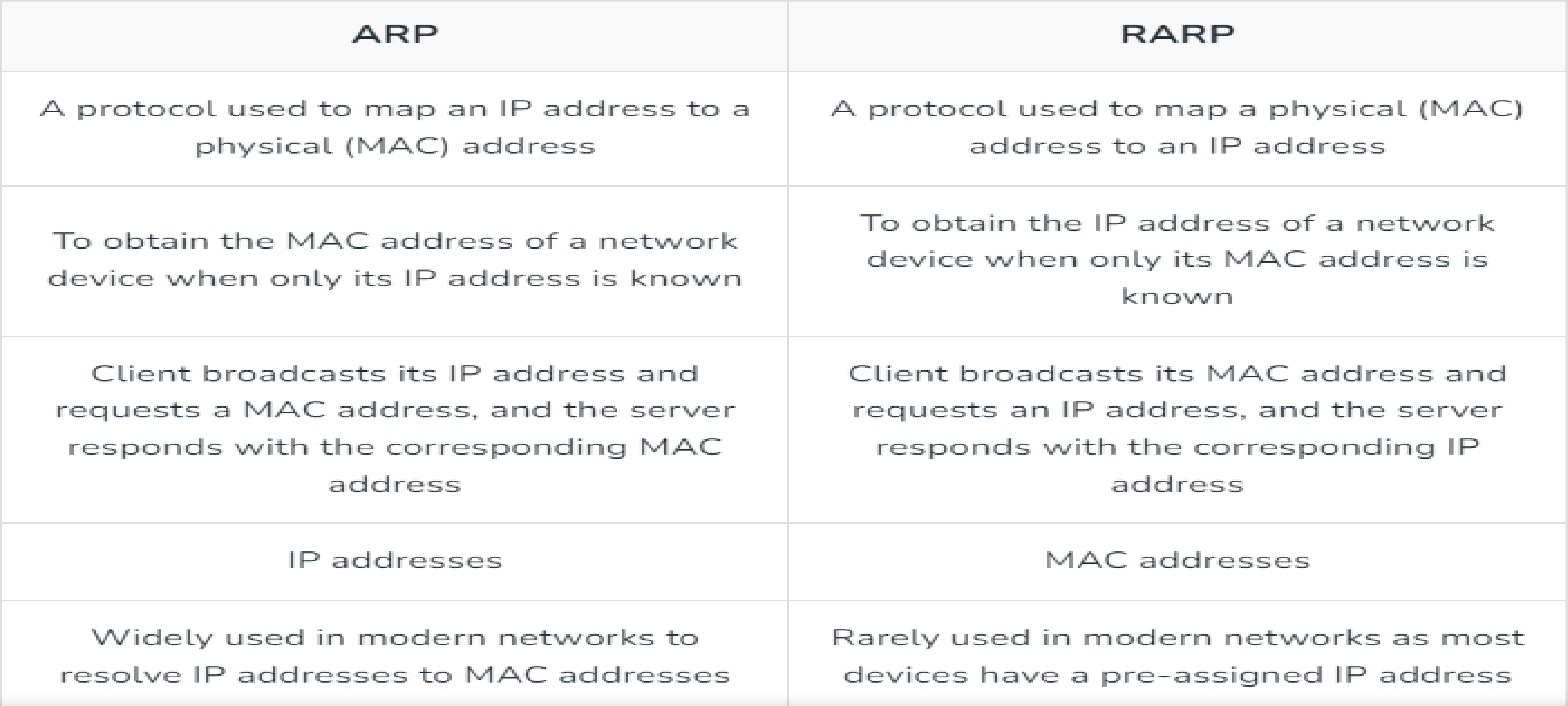
Where UDP is Used?

- Gaming
- Video Streaming
- Online Video Chats

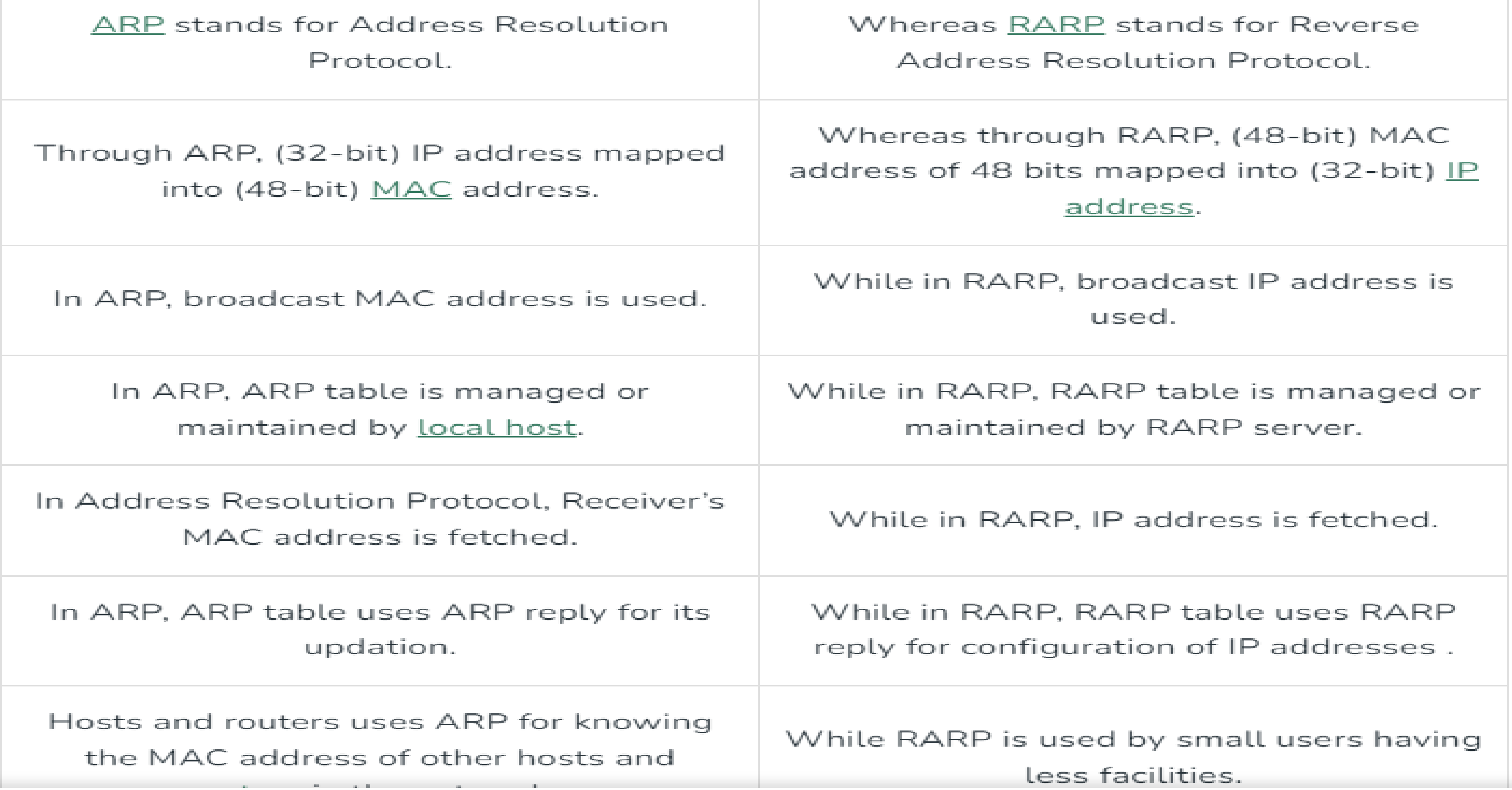
The Structure of ARP and RARP



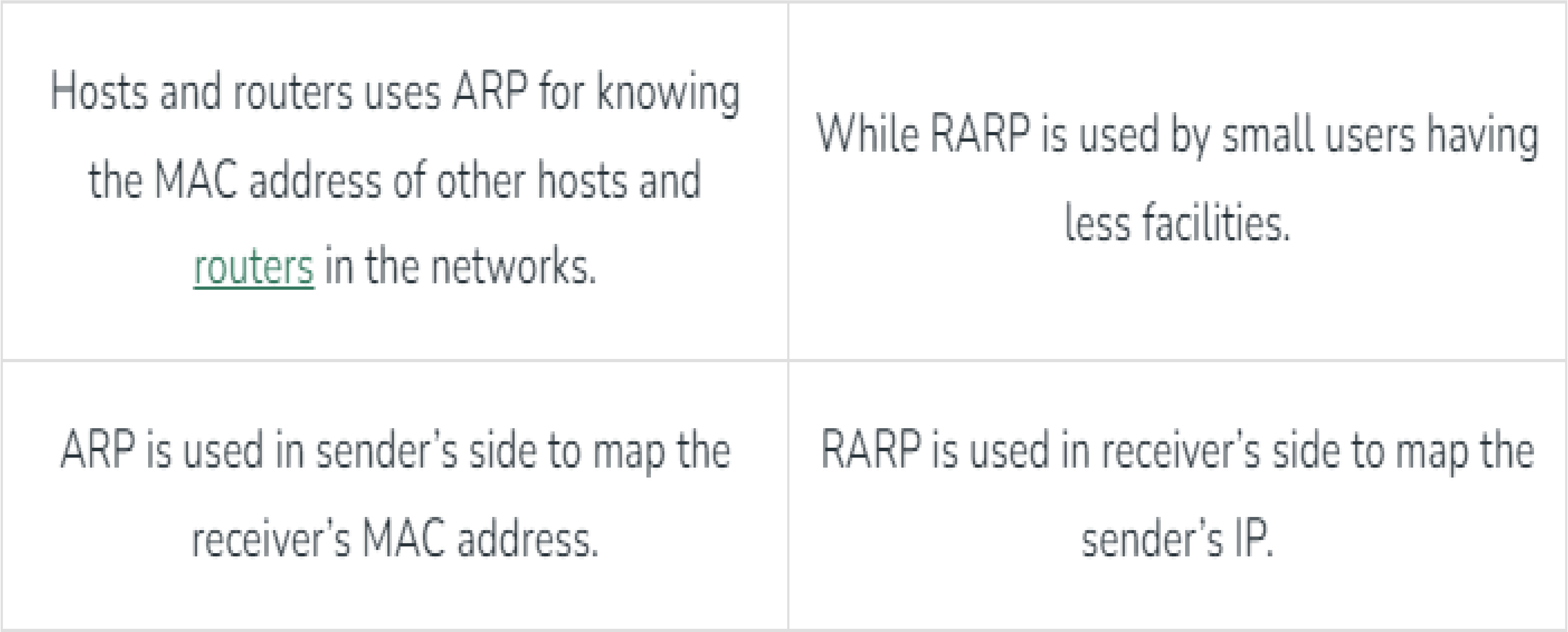
Difference Between ARP and RARP



ARP	RARP
A protocol used to map an IP address to a physical (MAC) address	A protocol used to map a physical (MAC) address to an IP address
To obtain the MAC address of a network device when only its IP address is known	To obtain the IP address of a network device when only its MAC address is known
Client broadcasts its IP address and requests a MAC address, and the server responds with the corresponding MAC address	Client broadcasts its MAC address and requests an IP address, and the server responds with the corresponding IP address
IP addresses	MAC addresses
Widely used in modern networks to resolve IP addresses to MAC addresses	Rarely used in modern networks as most devices have a pre-assigned IP address



ARP stands for Address Resolution Protocol.	Whereas RARP stands for Reverse Address Resolution Protocol.
Through ARP, (32-bit) IP address mapped into (48-bit) MAC address.	Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address.
In ARP, broadcast MAC address is used.	While in RARP, broadcast IP address is used.
In ARP, ARP table is managed or maintained by local host.	While in RARP, RARP table is managed or maintained by RARP server.
In Address Resolution Protocol, Receiver's MAC address is fetched.	While in RARP, IP address is fetched.
In ARP, ARP table uses ARP reply for its updation.	While in RARP, RARP table uses RARP reply for configuration of IP addresses .
Hosts and routers uses ARP for knowing the MAC address of other hosts and	While RARP is used by small users having less facilities.



Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks.	While RARP is used by small users having less facilities.
ARP is used in sender's side to map the receiver's MAC address.	RARP is used in receiver's side to map the sender's IP.

THANK YOU