IP address:

- An IP address is a number that uniquely identifies every device (computer, smartphone, embedded device) on the network.
- 4 bytes e.g. 192.168.1.100.
- Devices connected on the network communicate with each other using their IP addresses as identities.

SOCIAL SECURITY
192.168.1.1
THIS NUMBER HAS BEEN ESTABLISHED FOR
INSERT ID THEFT VICTIMS NAME HERE
BOB'S COMPUTER
SIGNATURE

Image Source: http://www.darkreading.com/identity-and-access-management/the-problem-with-two-factor-authentication/d/d-id/1113697

Packet:

- A packet contains the information exchanged over the network.
- It also contains the details of the sending and receiving computers.

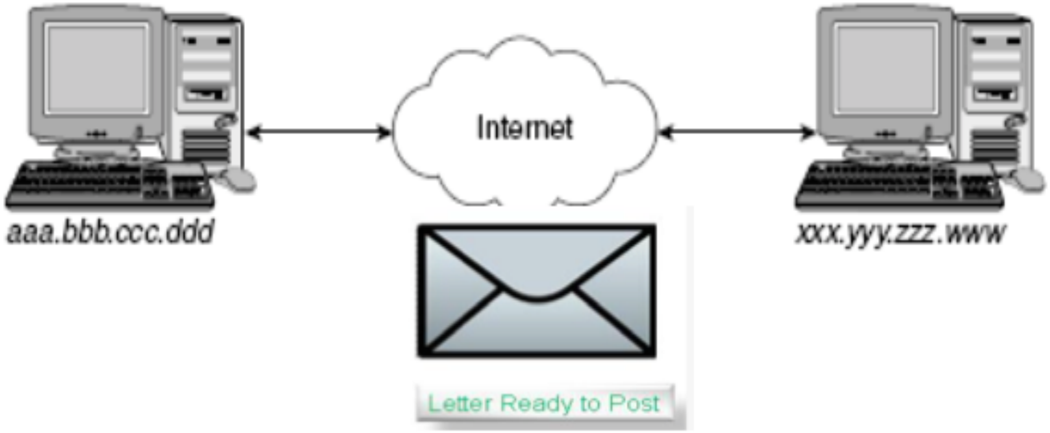
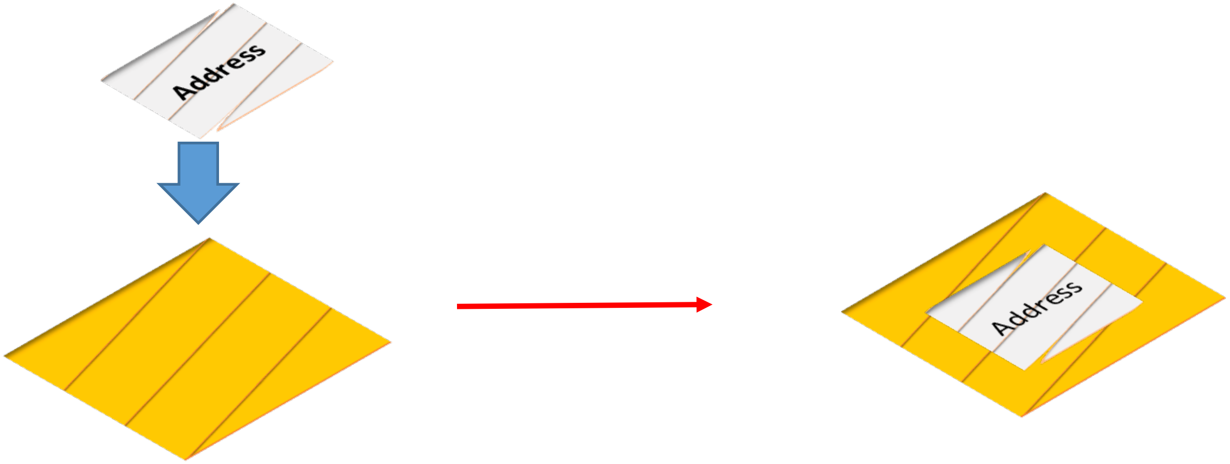


Image Source: http://www.webreference.com/programming/php_mysql/index.html

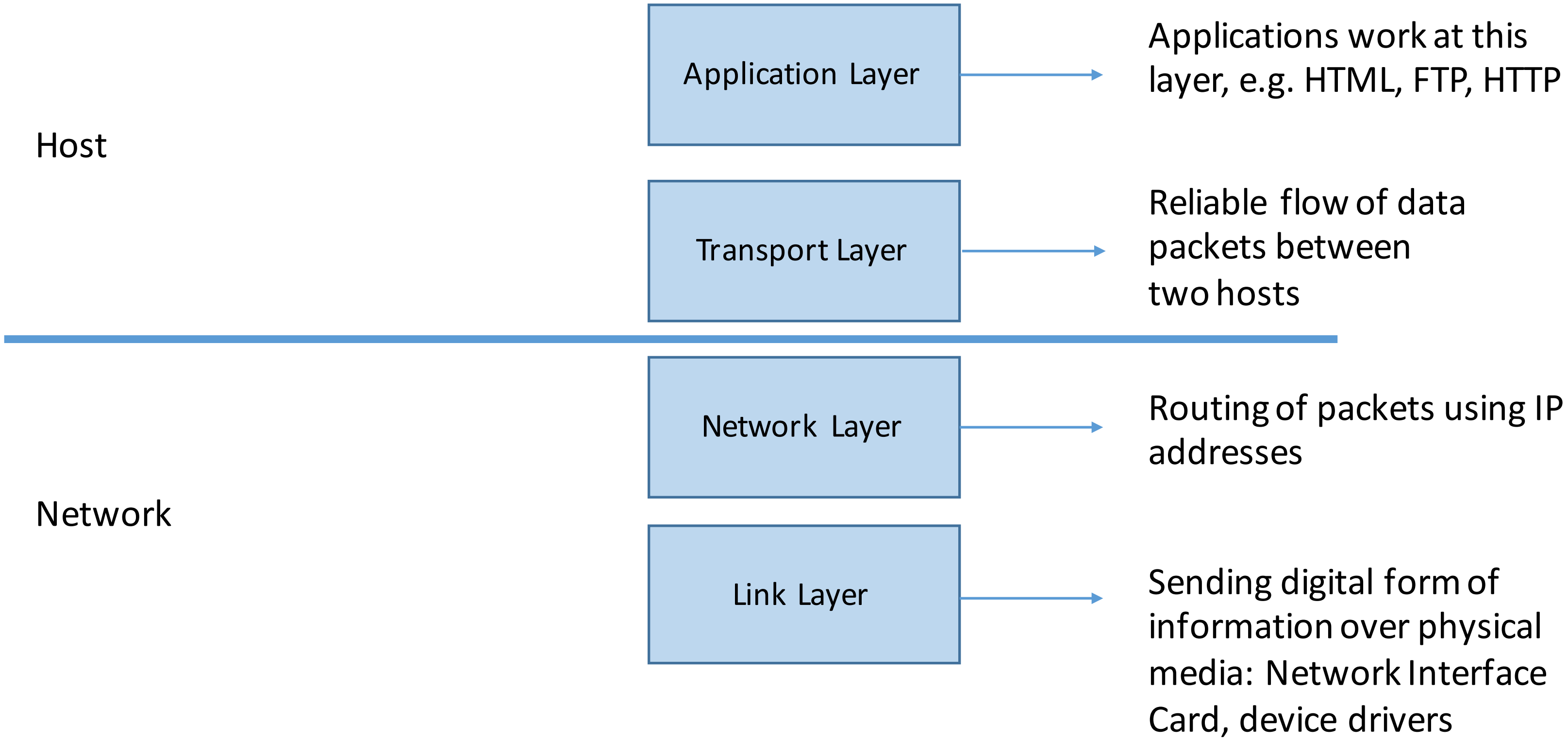
Packet Formation:

- When the information is sent (in form of a data packet) over the network, appropriate addressing information should be provided for the packet to reach the desired destination.
- The process of adding address information is similar to what is done for the letter mails. For example, the apartment number, street address and city information is required for the letter mail to reach the destination.



TCP/IP protocol suite

- System of rules that allows computers, smartphones and embedded devices to communicate with each other over the network.
- The process of taking the data from applications like web browser, segmenting it into small chunks if required, adding the addressing information (Port, IP and MAC), and sending out through the network interface card is performed as per the TCP/IP protocol suite.
- Combination of TCP & IP protocol suites:
  - TCP : Transmission Control Protocol
  - IP: Internet Protocol
- Based on four layer reference model.



Host

Application Layer

Applications work at this layer, e.g. HTML, FTP, HTTP

Transport Layer

Reliable flow of data packets between two hosts

Network

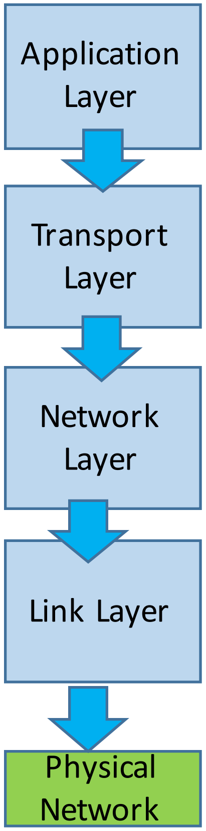
Network Layer

Routing of packets using IP addresses

Link Layer

Sending digital form of information over physical media: Network Interface Card, device drivers

Addressing Information is added in form of “**Headers**”



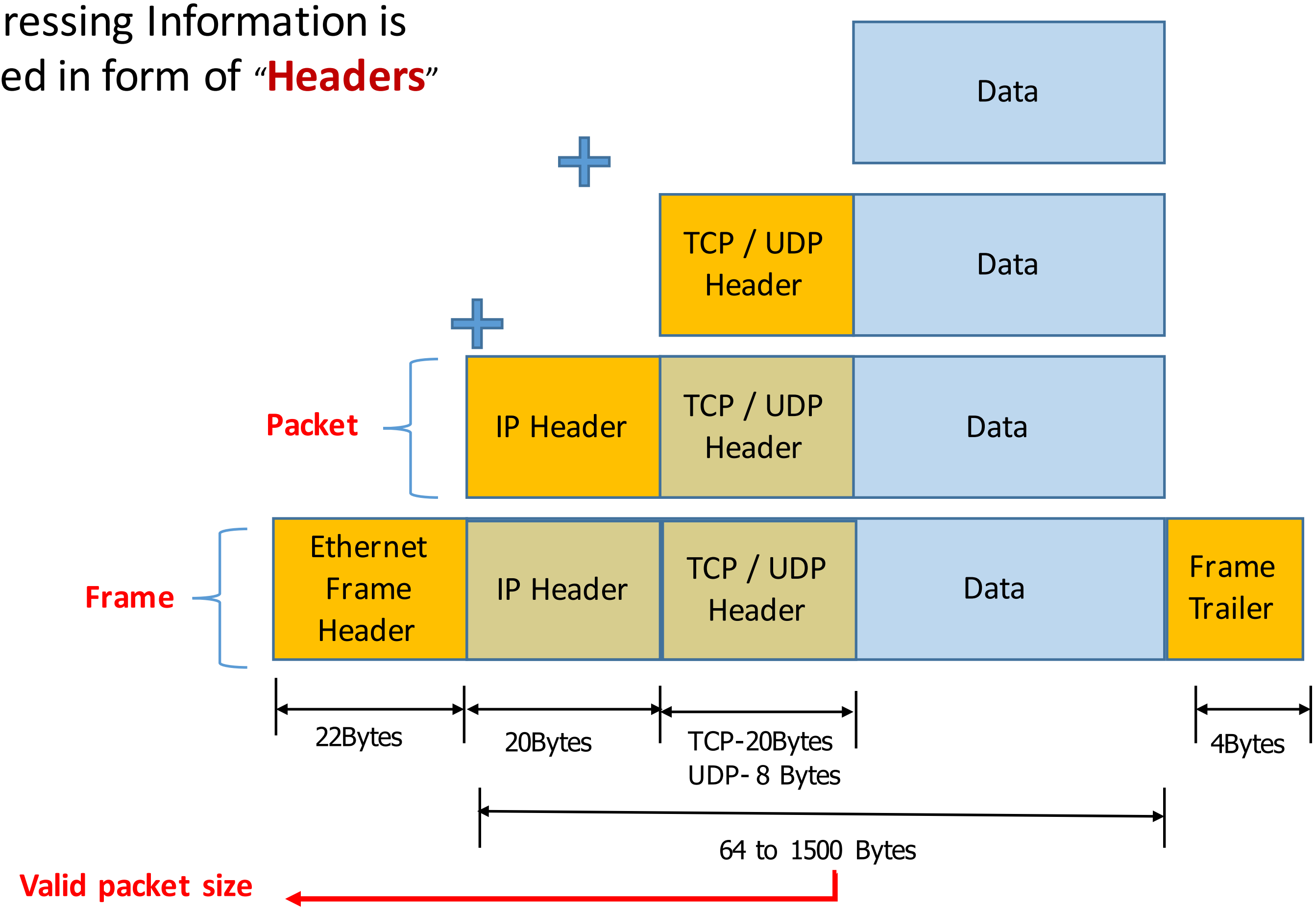
Application Layer

Transport Layer

Network Layer

Link Layer

Physical Network



Data

TCP / UDP Header | Data

Packet: IP Header | TCP / UDP Header | Data

Frame: Ethernet Frame Header | IP Header | TCP / UDP Header | Data | Frame Trailer

22Bytes

20Bytes

TCP-20Bytes
UDP- 8 Bytes

4Bytes

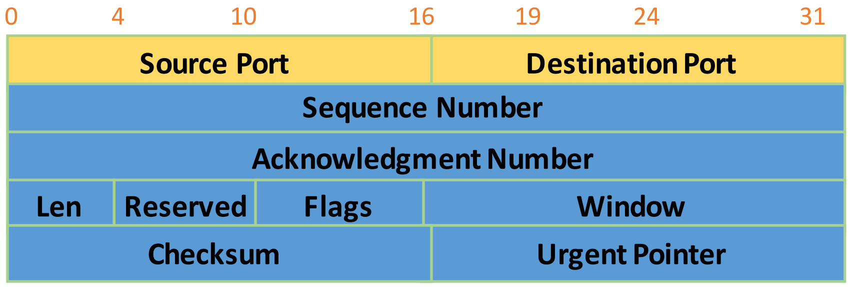
64 to 1500 Bytes

Valid packet size

Headers:

- Headers contain addressing information and other attributes necessary to route the frames in the network and process the packet at receiving host.

TCP Header



0 4 10 16 19 24 31

Source Port | Destination Port

Sequence Number

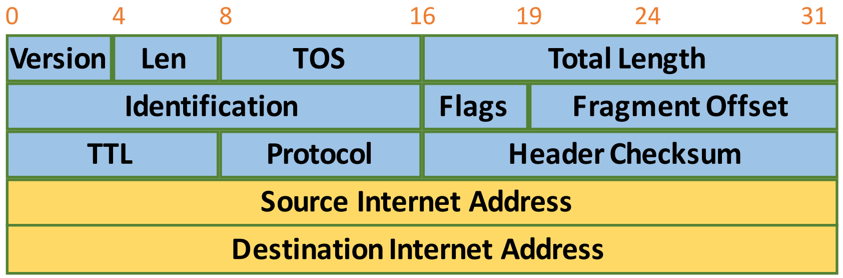
Acknowledgment Number

Len | Reserved | Flags | Window

Checksum | Urgent Pointer

Total Size = 20 Bytes

IP Header



0 4 8 16 19 24 31

Version | Len | TOS | Total Length

Identification | Flags | Fragment Offset

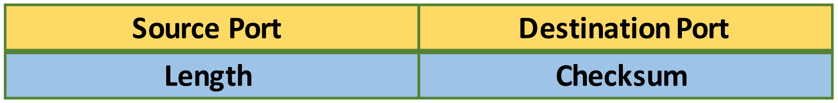
TTL | Protocol | Header Checksum

Source Internet Address

Destination Internet Address

Total Size = 20 Bytes

UDP Header



Source Port | Destination Port

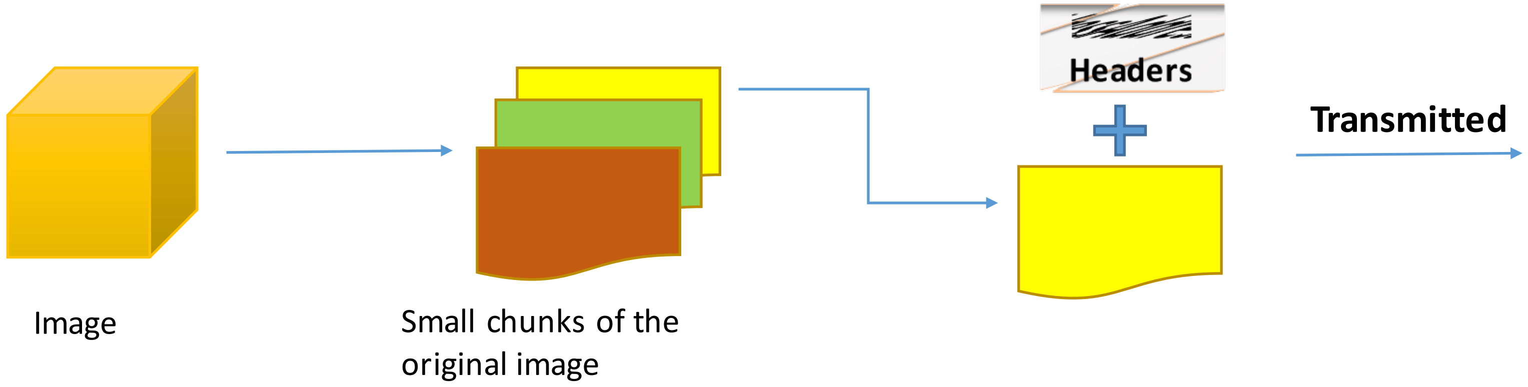
Length | Checksum

Total Size = 8 Bytes

Stream of packets:

- There is a maximum size limit for the packet to be transmitted over the network.
- For Ethernet (the most common network technology), it is 1500 bytes.
  - 1460 Bytes of data payload + 20 Bytes of TCP header + 20 Bytes of IP header.
- A TCP packet can take only 1460 Bytes of data as a payload over Ethernet network. Therefore, the communication typically requires exchange of multiple packets between the source and the destination

- The payload to be transmitted is broken into smaller pieces to keep the packet size within limits. For example, to send a picture of 4 MB i.e. 4096 bytes, the picture will be segmented into smaller pieces and it will take more than one packet to send the picture.
- For an investigator it is important to capture multiple packets in order to make complete sense of the content being sent or received over the network.


Headers
Transmitted
Image
Small chunks of the original image