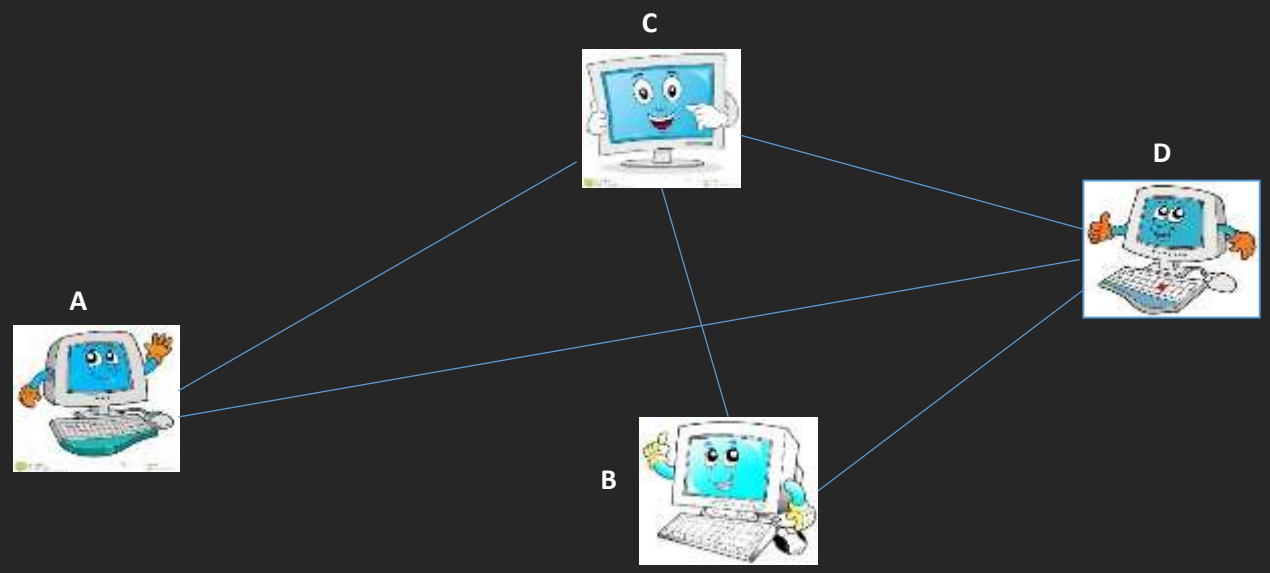
Protocol Review
(TCP, IP, UDP, ICMP, and Ethernet)

Hosts on a Network

Hosts on a network communicate:

- By exchanging ***data packets***
- Through ***protocols***



The Protocol Stack (TCP/IP Model)

Protocol layers

Application
Transport
Network
Data Link/Link
Physical

Layer-specific protocols

- **APPLICATION**

  HTTP, HTTPS, FTP, SMTP, Telnet, SSH, etc.
- **TRANSPORT**

  TCP, UDP
- **NETWORK**

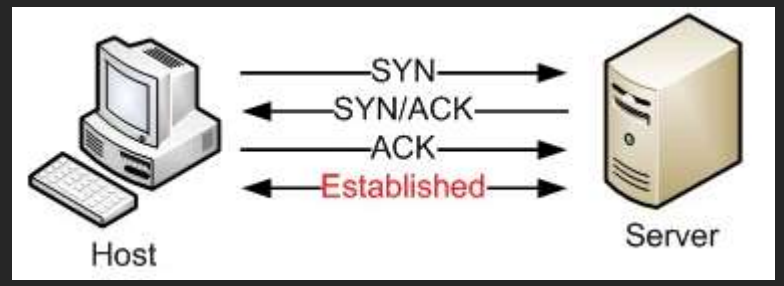
  IP (IPv4, IPv6), ICMP
- **DATA LINK**

  Ethernet
- **PHYSICAL**

  IEEE 802.3u

TCP (Transmission Control Protocol)

- Required for connection between two communicating computers for exchange of data
- Connection-oriented: analogous to a telephone conversation
- Delivery of data is guaranteed
- Handshake process: SYN-SYN/ACK-ACK
- Works with the Internet protocol (IP) over the TCP/IP Internet protocol suite

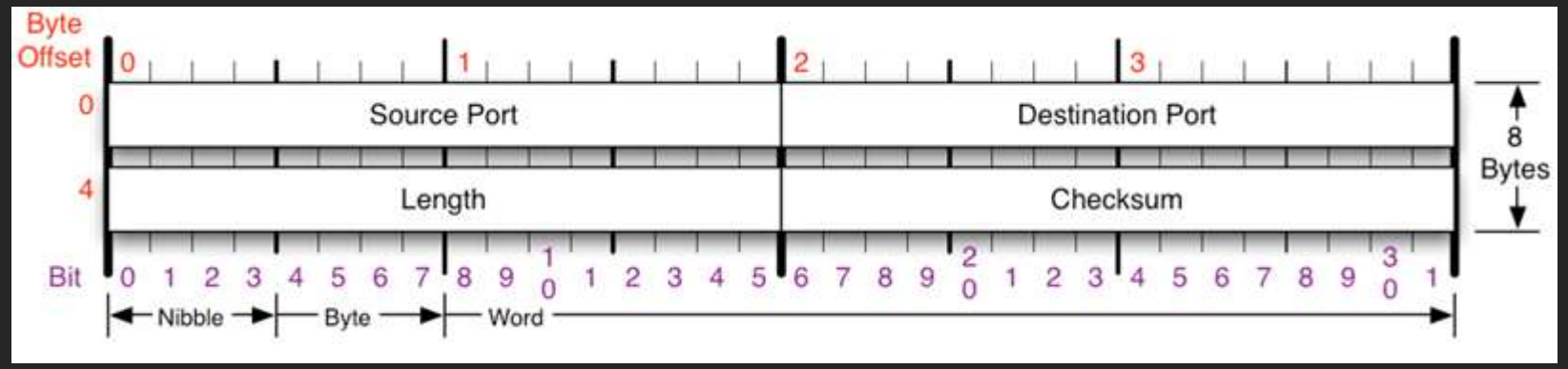


IP (Internet Protocol)

- Internet/Network layer protocol
- Responsible for routing of data units (datagrams) across network boundaries
- Delivery of data packets from source host to destination host based on source and destination IP addresses in packet headers
- Versions: IPv4, IPv6

UDP (User Datagram Protocol)

- Connectionless: unlike TCP, no hand-shake process
- Analogous to a mail delivery system
- Faster transmission than with TCP
- Suitable for time-sensitive applications where the trade-off between timely transmission and loss of packets is not a major concern



UDP header information. Source: http://wiki.smallroom.net

ICMP (Internet Control Message Protocol)

- Not typically used for data exchange between network hosts in the way that TCP and UDP are used
- Network devices (e.g. routers) use this protocol for sending error messages on network faults
- Works for diagnostic purposes over a network; such as when determining if a network device can be reached or not
- The protocol over which the ***ping*** and ***traceroute*** programs work (run these programs at the command line and view the output on Wireshark.)

Ethernet

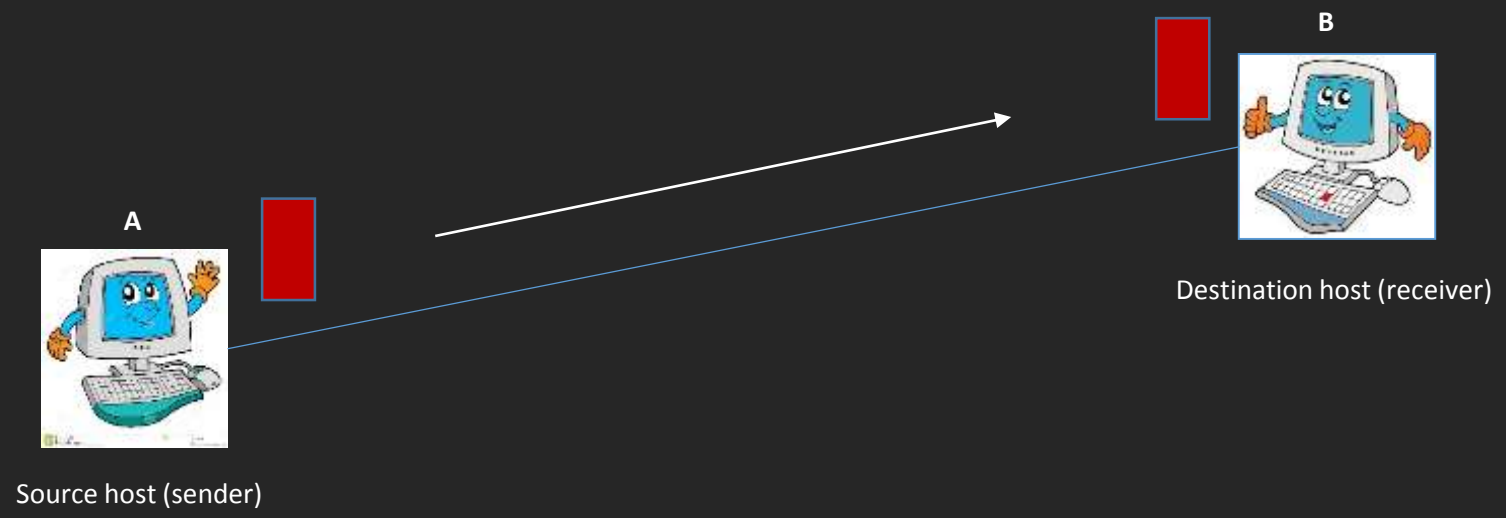
- Works at the Data Link layer
- Data framing in readiness for encoding onto the physical transmission medium as bits (0's and 1's)
- Frames: 48-bit MAC addresses, error-checking

Preamble	Destination MAC address	Source MAC address	Type	PayLoad	CRC/FCS

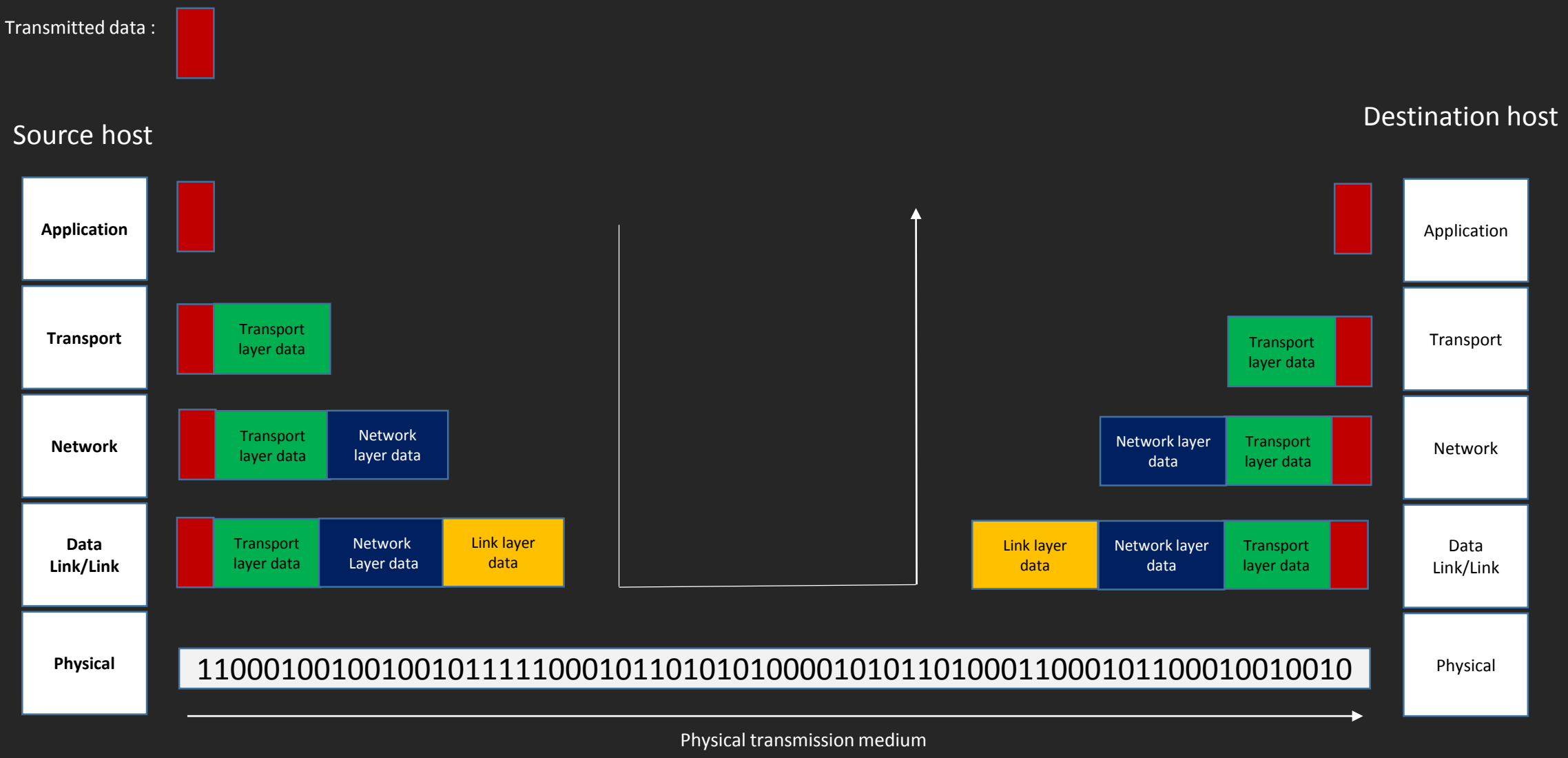
Ethernet frame information. Source: http://wiki.mikrotik.com

The Network Communication Process

- Send packet (from Source)
- Receive packet (at Destination)



Packet Communication: Encapsulation



Layer-specific Header Data Components

- **Transport layer data(TCP/UDP)**

  Header information: source port, destination port, sequence number, acknowledgement number, flags/control bits, checksum, etc.

- **Network layer data (IP)**

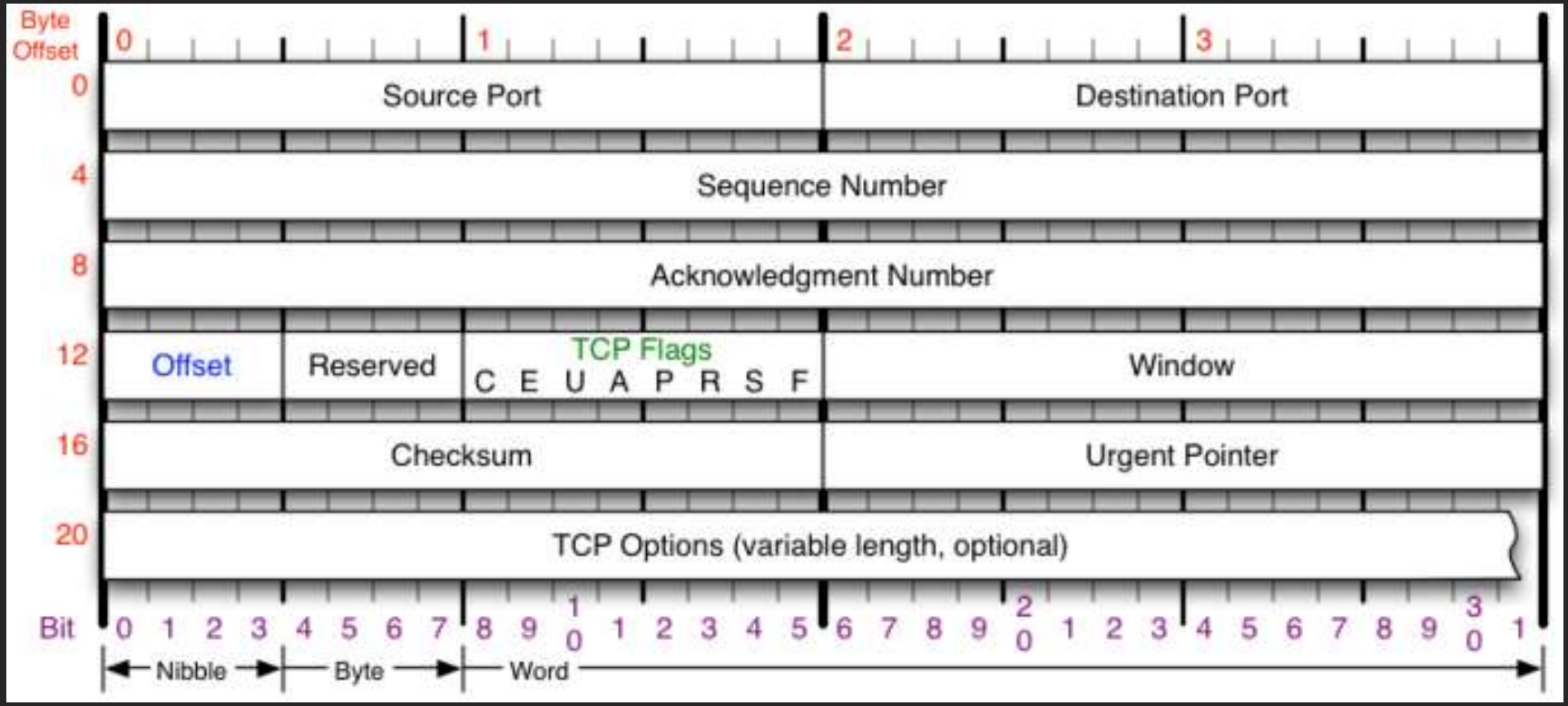
  Header information: source address, destination address, length, TTL, header checksum, etc.

- **Link layer data**

  Frame header information: source MAC address, destination MAC address, error checking, payload, etc.

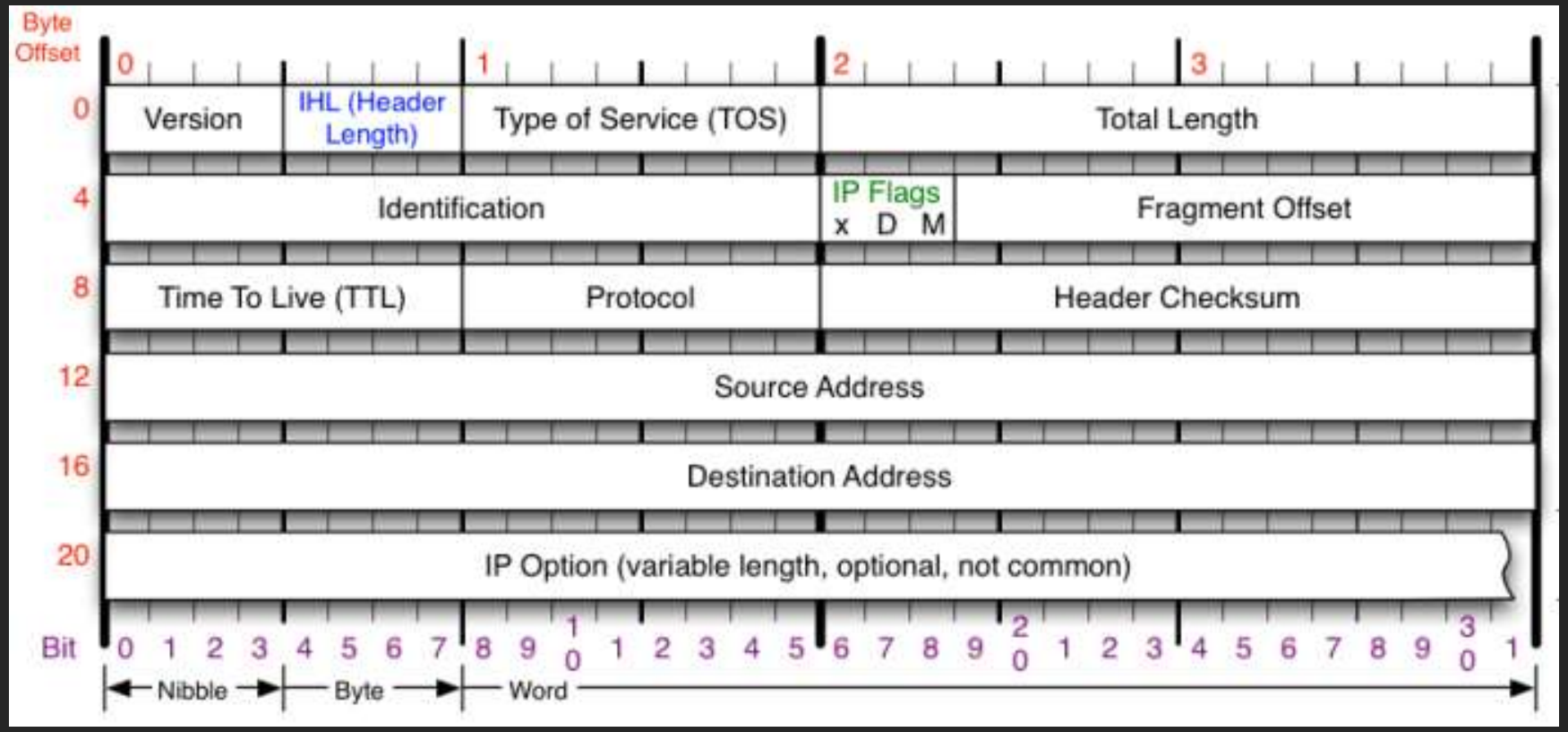
- On the physical layer (frames are encoded into bit streams for transmission over a physical channel

The TCP Header



TCP header information. Source: nmap.org

The IP Header



IP header information. Source: nmap.org

Simple Demonstration of the Network Communication Process Between two Hosts: launching a browser and visiting a webpage

- We view specific TCP and IP packet information over communication across a network.
  1. Run Wireshark
  2. Note the IP address of host A (ipconfig/ifconfig). Host A is our test system and is connected to the Internet.
  3. Filter the Wireshark output by entering: ip.addr == the IP address of our computer
  4. While the Wireshark output window is clear, launch a browser (Mozilla Firefox or IE) and go to a website (e.g. microsoft.com, ucalgary.ca, etc.)
  5. Observe the Wireshark output for TCP and IP header data (search for the string "microsoft" or "calgary" and view the TCP and IP data for the packet.

     (**To find a packet that has a particular string**: Click the **Find a packet …** icon; Select the **String** option; Enter the string - e.g. "microsoft" - and click **Find**.

- Our simple network consists of two network hosts (A and B) as follows: