# Network security

Nicolò Fornari

February 17, 2016

## 1 Network protocols

**Data link layer**
It is the lowest logical level, the data link interconnects physical interfaces. Each interface is identified by a MAC address (Media Access Control).
The MAC address is 48 bit long, it is usually represented in Hex notation and it is used to route packets in local networks.
It uniquely identifies a network interface. It is assigned by the producer according to the standard IEEE 802.

**Network Layer**
IP operates at this level. IP addresses are dynamically assigned by an authority (eg. ISP's DHCP server).

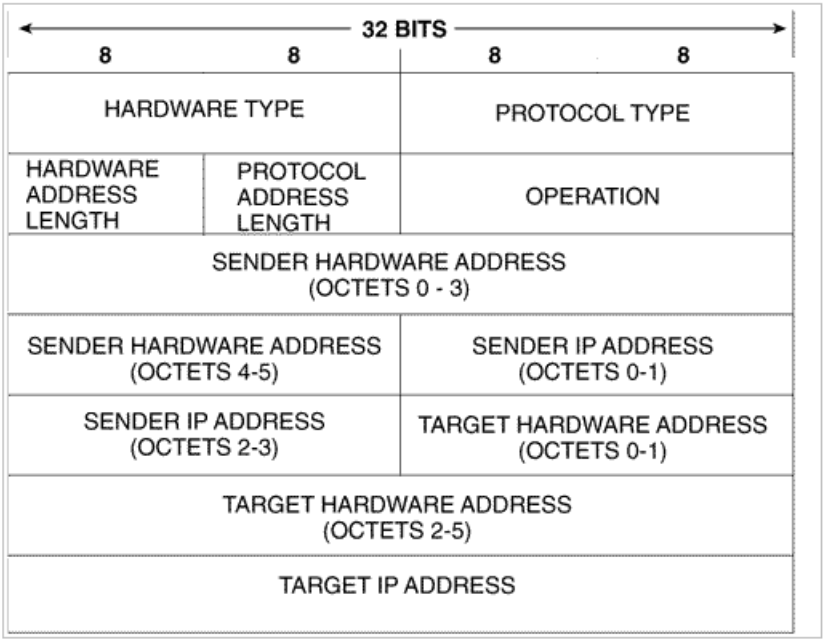
**Stateful:** communication starts, develops,ends. eg. TCP
**Stateless:** IP

## 1.1 ARP

ARP (address resolution protocol) allows systems to associate an ip address to a MAC address. All addresses in the ARP table are added by one of these mechanisms:

- ARP request-reply:
  who is 192.168.0.16 tell 192.168.0.1
  192.168.0.16 is at 00-10-BC-2c-11-56
- Gratuitous ARP
  192.168.0.16 is at 00-10-BC-2c-11-56

**ARP frame header**




**ARP poisoning**
The ARP protocol is declarative, it does not need an answer.
Nodes are not authenticated.
Limitations: it works only on LAN

**Subnets and CIDR**

Subnets are logical divisions of IP addresses. IP bits are partitioned as network,subnet,host.
A subnet mask indicates sections of IP addresses meant for network and subnet.
Eg. 255.255.255.0 means 24 bits for network and subnet and 8 bits for hosts.

**CIDR**

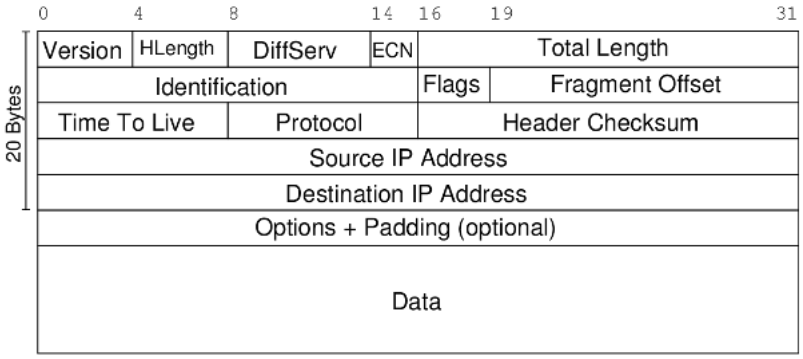
Classless Inter Domain Routing, it is a synthetic way to represent subnet masks.
*Example:*

- Network mask: 255.255.0.0.
- CIDR representation: 132.132.1.10/16
- Hosts = $2^{16}$

*Formulas:* (everything as binary)

- Network = Ip AND Subnet
- Host = Ip AND Not(Subnet)

## 1.2 IP




Some IPs are reserved for private networks:

- 10.0.0.0 → 10.255.255.255
- 192.168.1.1 → 192.168.255.255
- 172.16.0.0 → 172.16.255.255

**Def** A *datagram* is a basic transfer unit associated with a packet-switched network. The delivery, arrival time, and order of arrival need not be guaranteed by the network.

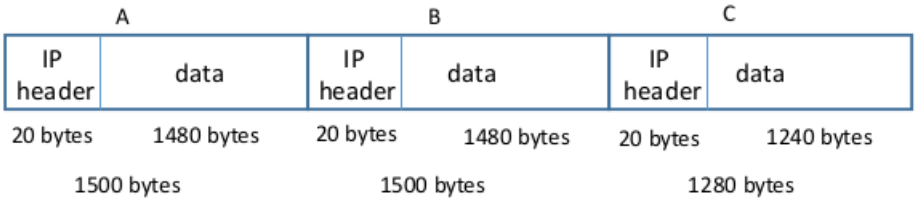
**Def** MTU maximum transmission unit

**IP fragmentation** *Identification:* 16 bit, is the unique identifier of the fragmented datagram. Note that all fragments have the same identification number.
*Flags:* 3 bits

- 0 Reserved, must be zero
- DF Don't fragment
  If set to 0 → there may be fragments
  If set to 1 → drop datagram if it has to be fragmented
- MF More fragments
  0 → last fragment
  1 → there are more fragments

*Offset* 13 bits, offset of this datagram wrt the first fragment with that ID

**Fragmentation example**

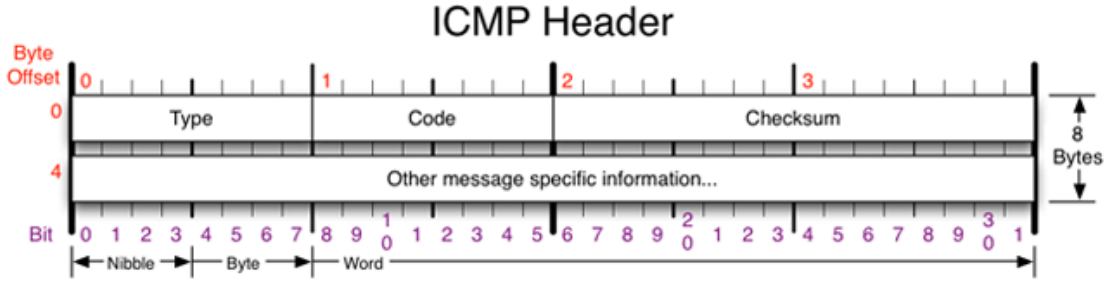



| | A | B | C |
|---|---|---|---|
| Identification | 4452 | 4452 | 4452 |
| Flags | • DF=0<br>• MF=1 | • DF=0<br>• MF=1 | • DF=0<br>• MF=0 |
| Offset | 0 | 1480 | 2960 |

**Remark 1.** ***DOS with IP fragments*** *You keep sending fragments without sending the first fragment, the router keeps waiting for it until it exhausts its memory.*

## 1.3 ICMP

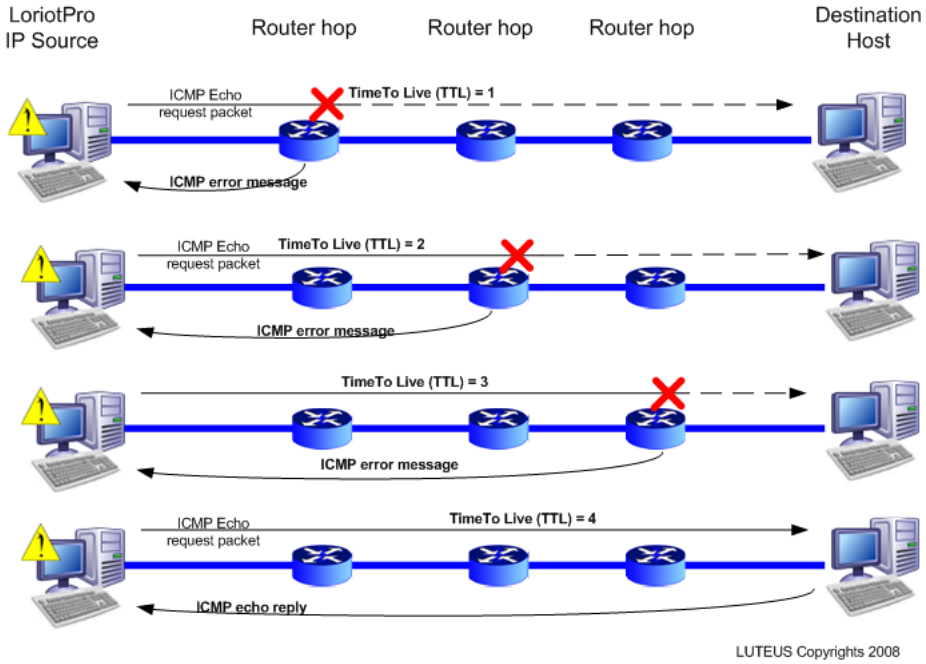
Internet control message protocol. It relies on IP and is and integral part of it.




**Some message types**

- 0 Echo Reply
- 3 Destination Unreachable
  Code 0 → Net unreachable
  Code 1 → Host unreachable
  Code 2 → Protocol unreachable
  Code 3 → Port unreachable
  Code 4 → Fragmentation needed and DF set
  Code 5 → Source route failed
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 11 Time Exceeded
  Code 0 → Net unreachable
  Code 1 → Host unreachable
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply

## 1.4 Traceroute



## 1.5 Denial of service

**Def** a Denial of Service is a type of attack that aims at congesting or overpowering a system's capacity by generating requests the system will have to answer.

**Examples**

- Dos with IP fragmentation
- Ping Flooding (the attacker exploit his wider bandwidth)
- Ping of death