Network security

Nicolò Fornari

February 23, 2016

Chapter 1

Network protocols

1.1 Introduction

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).

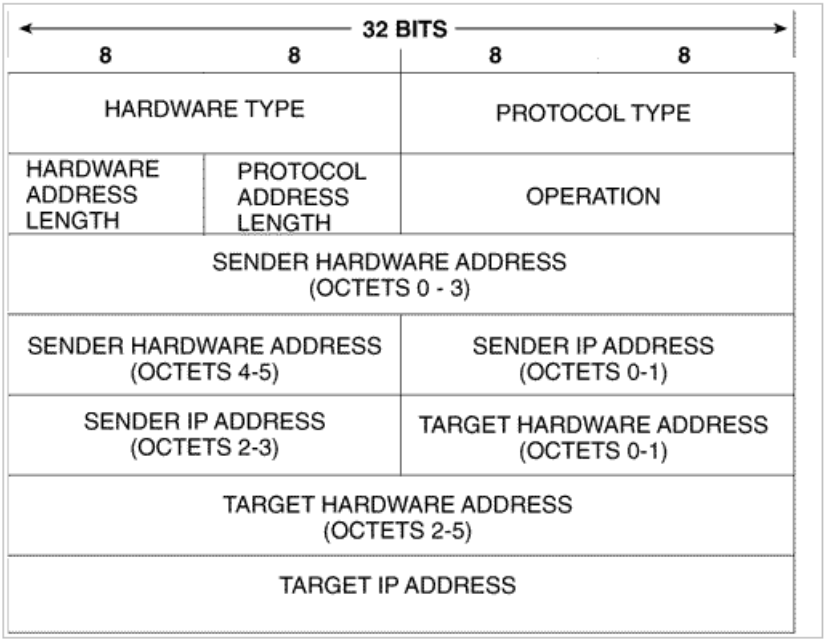
Stateful: communication starts, develops,ends. eg. TCP
Stateless: IP

1.2 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.

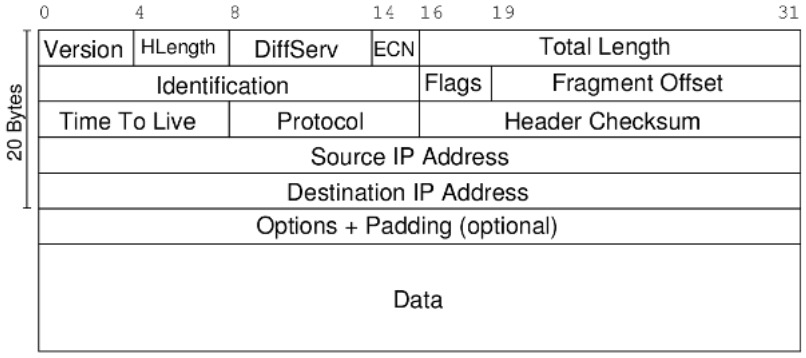
CIDR
Classless Inter Domain Routing, it is a synthetic way to represent subnet masks.
Example:

- 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)

1.3 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.

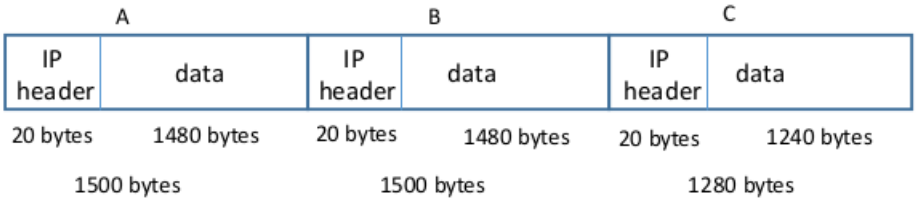
Def MTU maximum transmission unit

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

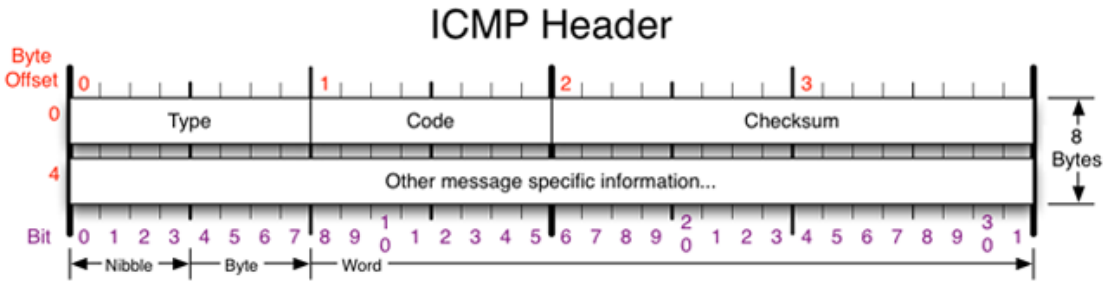


	A	B	C
Identification	4452	4452	4452
Flags	• DF=0 • MF=1	• DF=0 • MF=1	• DF=0 • MF=0
Offset	0	1480	2960

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.*

1.4 ICMP

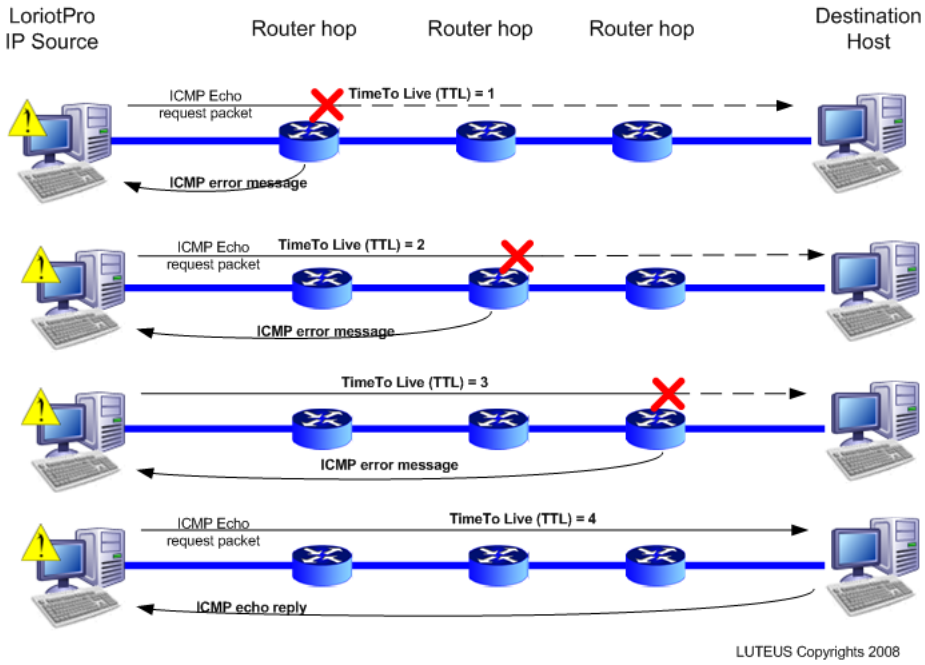
Internet control message protocol. It relies on IP and is and integral part of it.



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

1.5 Traceroute



1.6 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

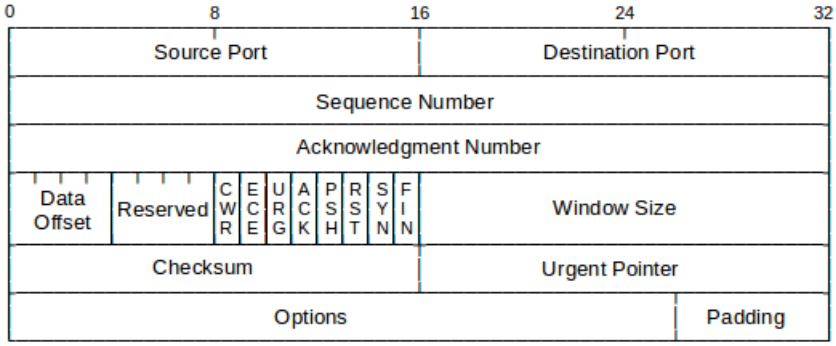
- Dos with IP fragmentation
- Ping Flooding (the attacker exploit his wider bandwidth)
- Ping of death

Chapter 2

Osi Transport Layer

2.1 TCP

The Transmission Control Protocol builds on top of IP the notion of state. Infact IP just delivers data while TCP manages the data segments by mean of checksums and re-delivery of unreceived/corrupted packets.

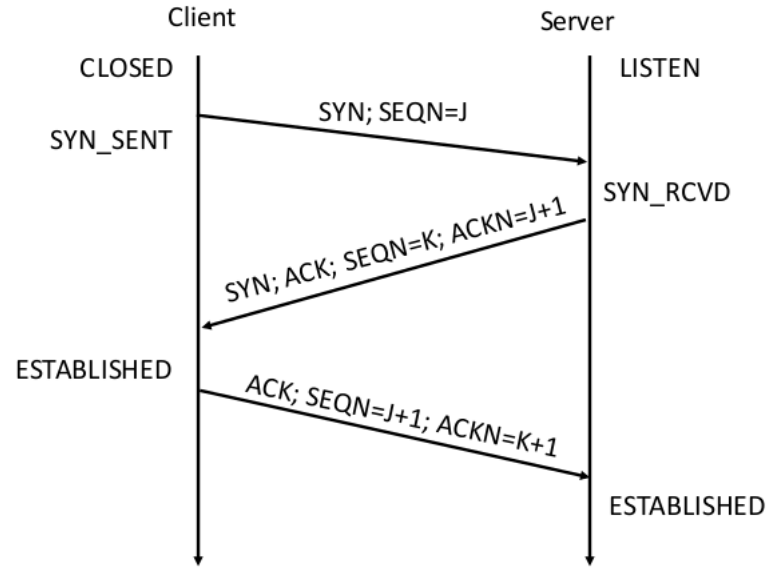


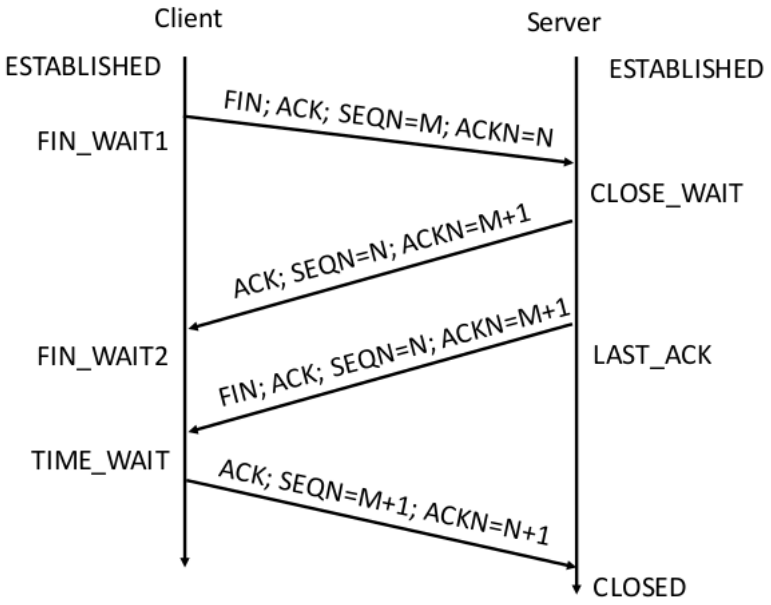
A server and a client that partecipate in a TCP connection open a *socket* which is a tuple (source-ip:source-port,destination-ip:destionation-port).
Note that a client generates a source port randomly.
TCP details - some flags:

- **SYN:** initializes the TCP session, it should be set to 1 only for the first datagram
- **ACK:** ackwnoledge the reception of the segment
- **FIN:** it signals the intention of closing the connection
- **RST:** drop the connection (reset)

Sequence number: it is a 32 bit generated by each end (note that the sequence number of the client is independent from the server's one).
Acknoledgement number: 32 bits

2.2 Handshakes





2.3 Some TCP specifics

Both client and server set up a TCB (Transmission control block) to keep track of connection. The TCB structure is freed from memory when connection reaches status CLOSED.

A packet with RST flag up does not receive an answer.
If the state is CLOSED any packet with no RST receives a RST.
If the state is LISTEN

- SYN flag up + no ACK opens a TCP session. Answer is SYN+ACK
- Only ACK receives a RST
- Drop with no answer otherwise

2.4 SYN DoS

When the server receives SYN J it answers back with SYN K, ACK J+1.
The server opens a new session in a separate threat/ allocates resources. Then the server waits for the ACK K+1 from the client, it waits for the MSL (maximum segment lifetime set by default to 2 minutes). The same mechanism is on the sender side but of course the attacker controls it and can bypass it.

The attacker drops all SYN ACKs with a firewall to avoid exhausting its own resources. Note that a server typically has more bandwidth than a single client.

Remark 2. *The attack currently works in $\mathcal{O}(2n)$ because for each SYN a SYN ACK is received $\rightarrow$ less bandwidth.*

However the attack can be improved by spoofing the source ip address, now the attacker is operating in $\mathcal{O}(n)$.
In theory the attack should not work because the server should receive a RST by each zombie, consequently free the TCB making the attack fail.
Still the attacker can choose a set of IPs which do not reply.

2.5 Dos mitigations

- Load balancing: distribute traffic loads evenly
- Rate limiter: deny traffic above a certain rate of SYN/sec
- Proof of work: require the source to solve a cryptopuzzle before allocating resources for the connection (note that this requires a protocol support).

2.6 TCP scans

It is possible to exploit specifications of a network protocol (TCP,UDP,..) to learn something about a system or a network.

SYN Scan: the attacker forges TCP packets with SYN=1. It is useful to see whether the remote system accepts incoming connections on a certain port.
Note that a polite way of scanning is performed in the following way: after the server's SYN ACK reply, the attacker sends a RST so that the 3-way handshake is never finished.

Host fingerprinting: different operating systems have their own independent implementation of the TCP stack.

Examples:

- FIN = 1
- all flags set to 0
- Xmas: FIN,URG,PSH = 1

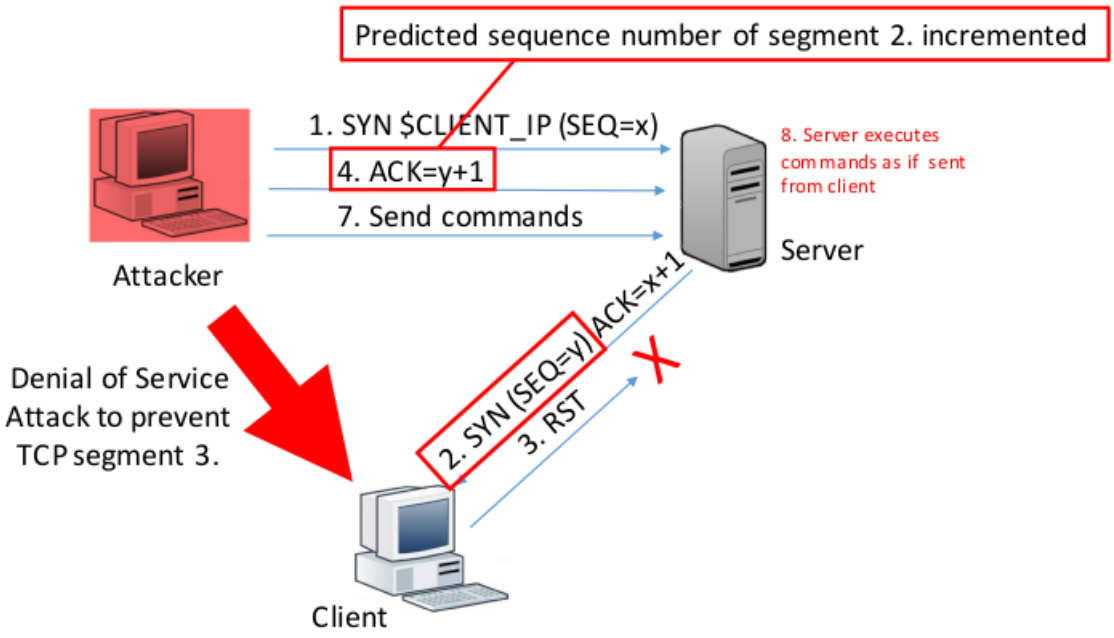
2.7 TCP Session hijacking - Mitnick attack

The attacker wants to send commands to a server they have no access to (eg. simple IP address authentication). The server has to think the attacker is the client, however the attacker does not sit in between client and server.

A TCP segment is identified and validated by:

- client ip → known
- destination ip → known
- port → known (if not standard, scan)
- client SEQ number → known(the attacker generates it)
- server SEQ number → *unknown*

Back in the old days algorithms for generating the SEQ number were really simple.



2.8 UDP

The User Datagram protocol is a stateless. It is designed for fast delivery of data

- Data integrity can be controlloed at application level
- It relies on the reliability of the underlying network link
- It does not guarantee delivery (there is no ACK mechanism)

Usage

- DNS servers
- NFS (network file systems)
- SNMP (simple network management protocol)
- DHCP (dinamic host configuration protocol)
- Most real time applications

2.9 UDP scans

It can be used to discover open ports on the network:

- CLOSE $\rightarrow$ ICMP port unreachable
- OPEN $\rightarrow$ no answer

However it is possible to configure a stealth system that does not reply to UDP requests to CLOSED ports by dropping ICMP packets with a firewall or router.