Мрежова сигурност I

http://training.iseca.org/

Ethernet 1/3

Boyan Krosnov

Acknowledgements

Some materials are based on work by

- Flickr users

  firas1, mrbill, studies_and_observations, eleaf, flocci, chrisdag

- Wikipedia users

  Inductiveload, Kju

План

- Преглед на Ethernet системата
- Топология на Ethernet мрежите
- Ethernet физически слой

  10BASE-x | 100BASE-x | 1000BASE-x | 10GBASE-x | Auto negotiation
- Ethernet логически слой

  Ethernet frame | MAC address | Type/Length | Jumbo | CRC

Преглед

- Слой по OSI reference model
  - 3. IP, ARP, MPLS
  - 2. Ethernet MAC/LLC
  - 1. Ethernet PHY
- Стандарт
  - IEEE 802.3 (както и 802.1, 802.2)
  - `http://standards.ieee.org/getieee802/`

Стандартът не е магия

- 802.3 стандарта е над 2500 страници
  - но е добре подреден и четим

34.1.4 Auto-Negotiation, type 1000BASE-X

Auto-Negotiation (Clause 37) provides a 1000BASE-X device with the capability to detect the abilities (modes of operation) supported by the device at the other end of a link segment, determine common abilities, and configure for joint operation. Auto-Negotiation is performed upon link startup through the use of a special sequence of reserved link codewords. Clause 37 adopts the basic architecture and algorithms from Clause 28, but not the use of fast link pulses.

34.1.5 Auto-Negotiation, type 1000BASE-T

Auto-Negotiation (Clause 28) is used by 1000BASE-T devices to detect the abilities (modes of operation) supported by the device at the other end of a link segment, determine common abilities, and configure for joint operation. Auto-Negotiation is performed upon link startup through the use of a special sequence of fast link pulses.

3.1.1 MAC frame format

Figure 3–1 shows the nine fields of a frame: the preamble, Start Frame Delimiter (SFD), the addresses of the frame's source and destination, a length or type field to indicate the length or protocol type of the following field that contains the MAC Client data, a field that contains padding if required, the frame check sequence field containing a cyclic redundancy check value to detect errors in a received frame, and an extension field if required (for 1000 Mb/s half duplex operation only). Of these nine fields, all are of fixed size except for the data, pad, and extension fields, which may contain an integer number of octets between the minimum and maximum values that are determined by the specific implementation of the CSMA/CD MAC. See 4.4 for particular implementations.

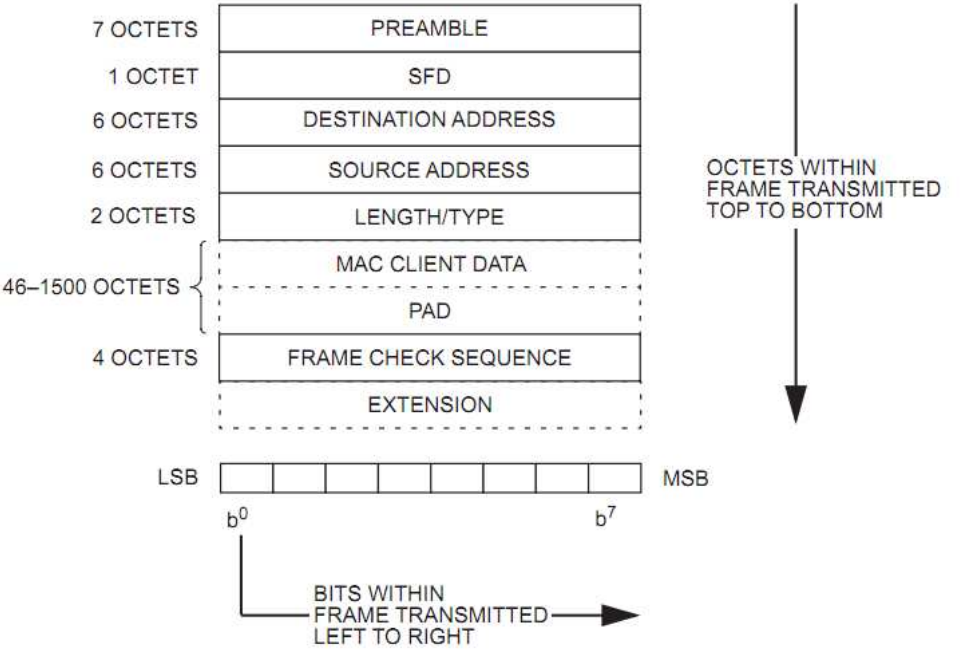
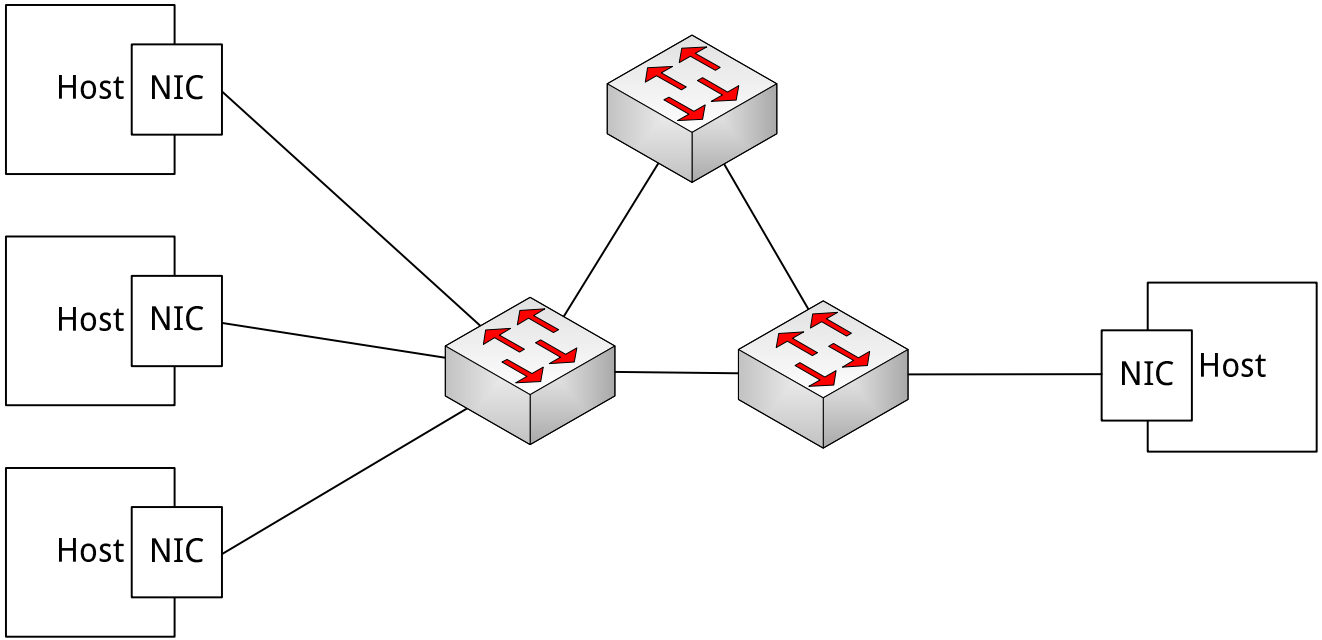


Figure 3–1—MAC frame format

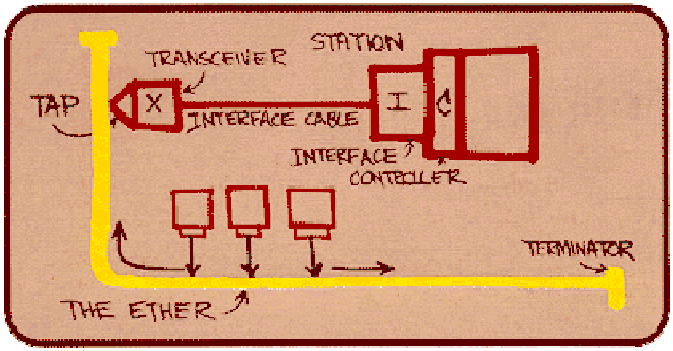
Топология

Физическа диаграма



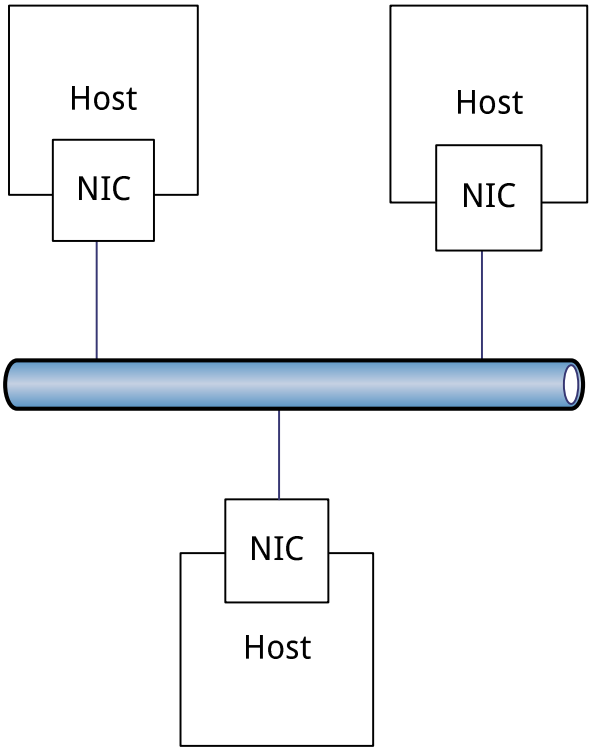
Споделена среда

- Коаксиалния кабел и “етера”
- Hub
- Колизии
- Switch
- Half duplex vs. Full duplex
- Flow control и half-duplex back-pressure



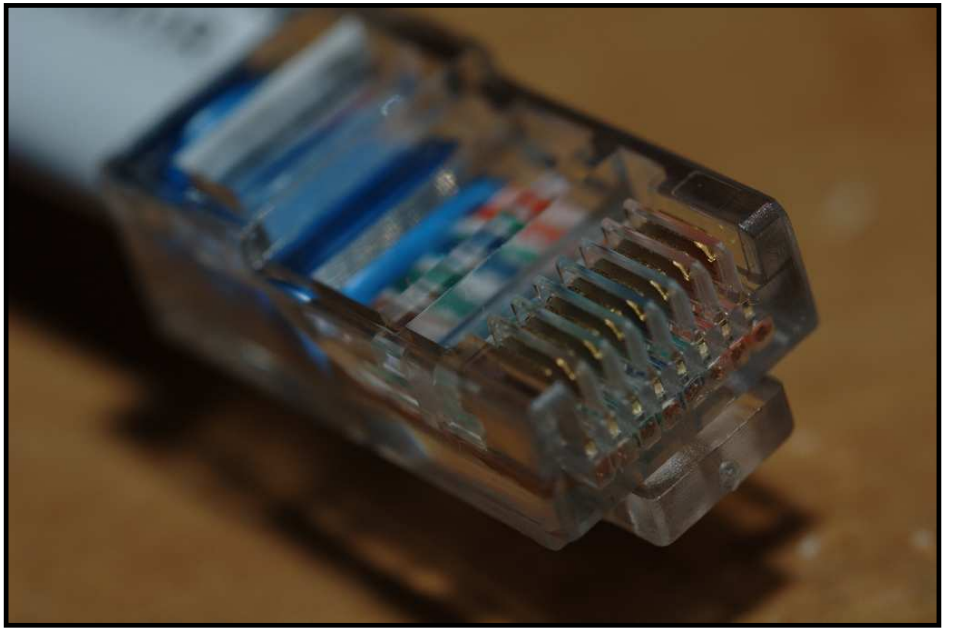
Топология

Логическа диаграма



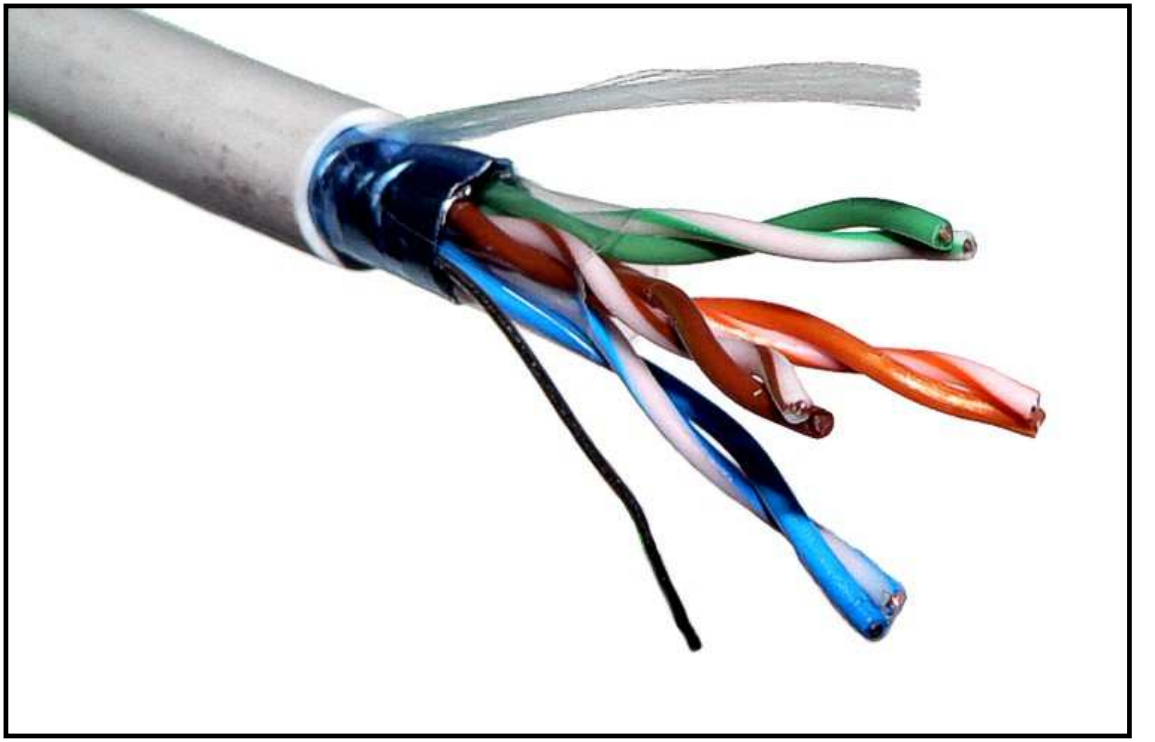
Физически слой

- 10BASE-T, 100BASE-TX, 1000BASE-T, 10GBASE-T

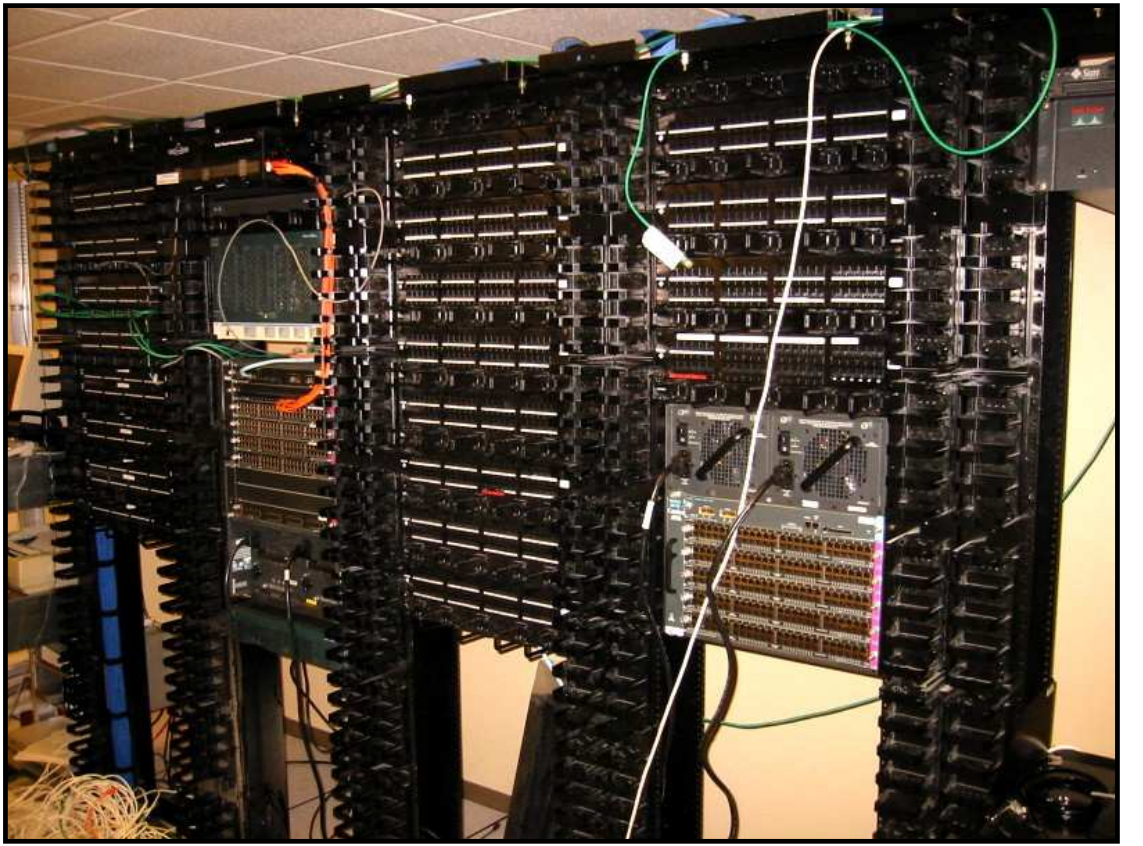


Физически слой – twisted pair

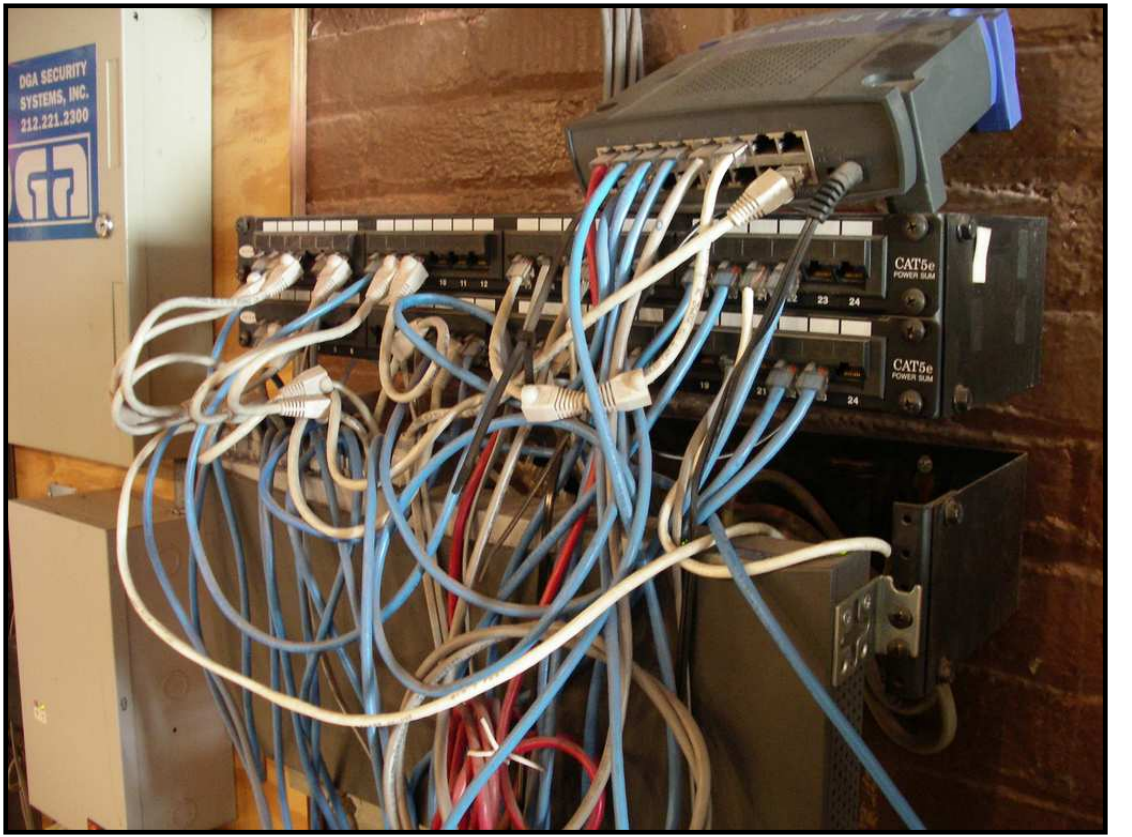
бо о бз с бс з бк к



Физически слой – twisted pair

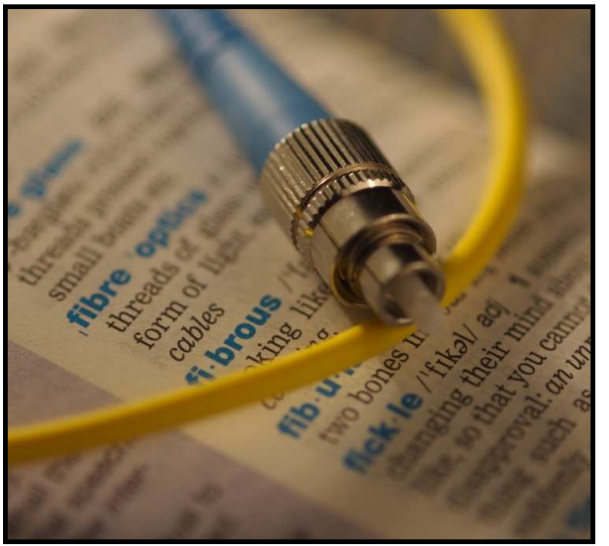


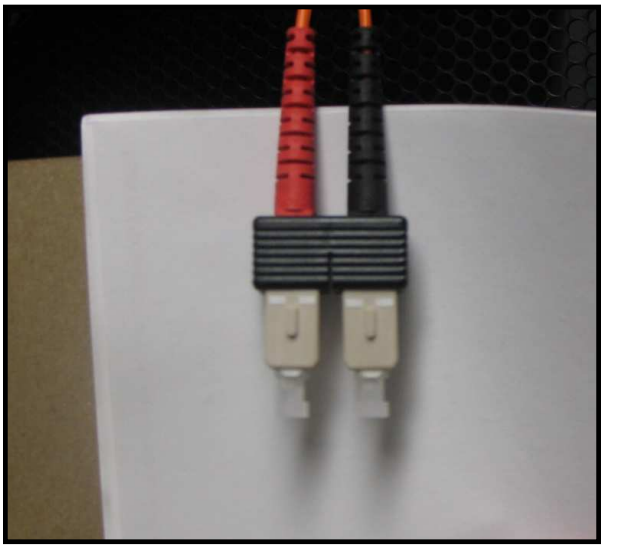
Физически слой – twisted pair



Физически слой – fibre

- По едно влакно или по две влакна
- Multimode vs. Singlemode





Физически слой – fibre

- 1000BASE-SX, 1000BASE-LX
- 10GBASE-SR, 10GBASE-LR
- други

- Baseband

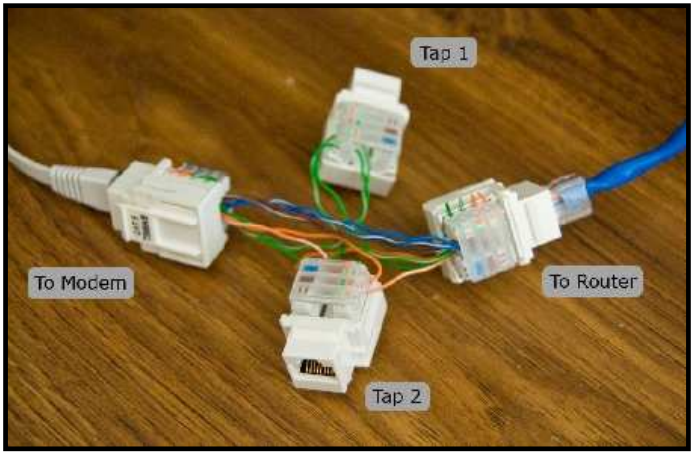
Autonegotiation

- Speed
- Duplex
- Flow Control

- MDI/MDI-X – кръстосаният кабел

Физически слой - атаки

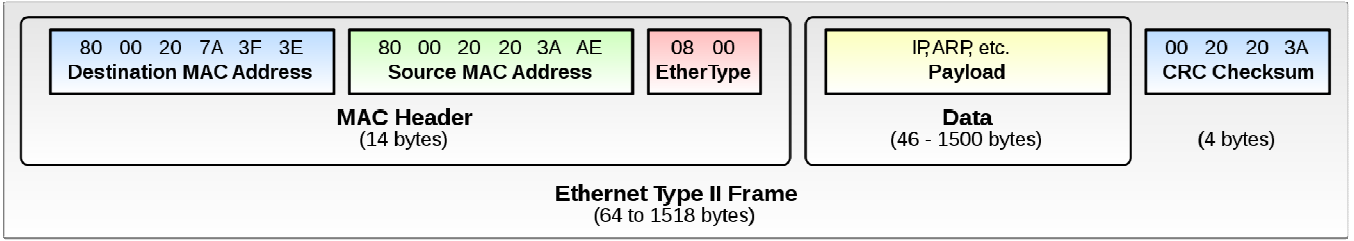
- DoS на споделената среда
- Пасивно подслушване - 10/100
- MITM



Въпроси

Логически слой

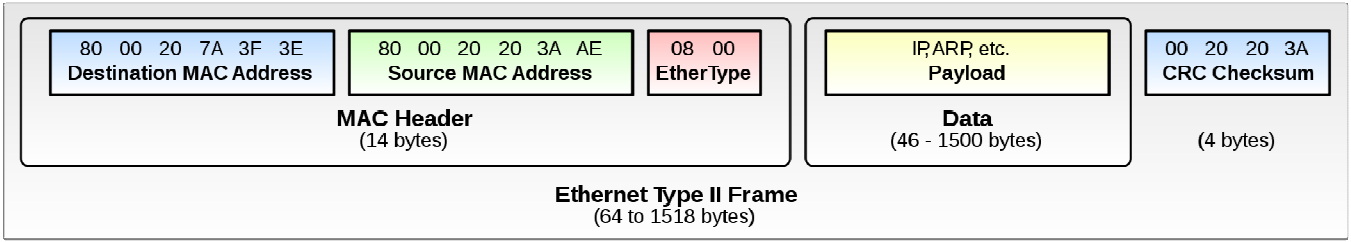
- Адресиране
- Идентифициране на носения протокол
- Защита от грешки от физическия слой
- Padding
- Полезен товар



Дължина на фрейма

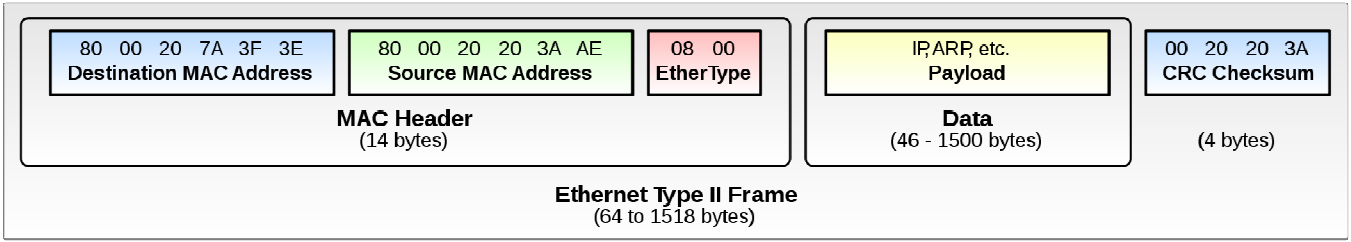
- 1500 байта полезен товар
- 14 MAC хедър + 4 CRC
- min frame size: 64
- max frame size: 1518
- preamble & interframe gap

- Допълнителни хедъри и място за тях
- Jumbo frames (9000B payload)



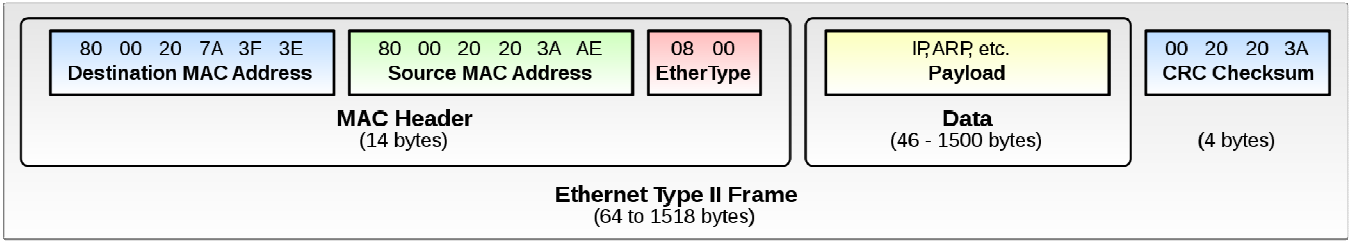
Фреймове в секунда

- 100 Mbps Ethernet – 150kpps
- GigE – 1.5 Mpps
- 10GE – 15Mpps



CRC

- Cyclic Redundancy Check (CRC)
- Защитава само от грешки във физическата среда



MAC address

- 48 bits
  - 24 bits OUI – `http://standards.ieee.org/regauth/oui/`
    - 1 bit global/local
    - 1 bit unicast/multicast
  - 24 bits NIC specific

- специални стойности
  - `ff:ff:ff:ff:ff:ff - broadcast`
  - `00:00:00:00:00:00` – unknown

MAC address

```
Ethernet adapter LAN:

Description . . . . . . . . . . . : Intel(R) 82567LM Gigabit Network Connection
Physical Address. . . . . . . . . : 00-21-6A-6A-0D-49
```

http://standards.ieee.org/regauth/oui/

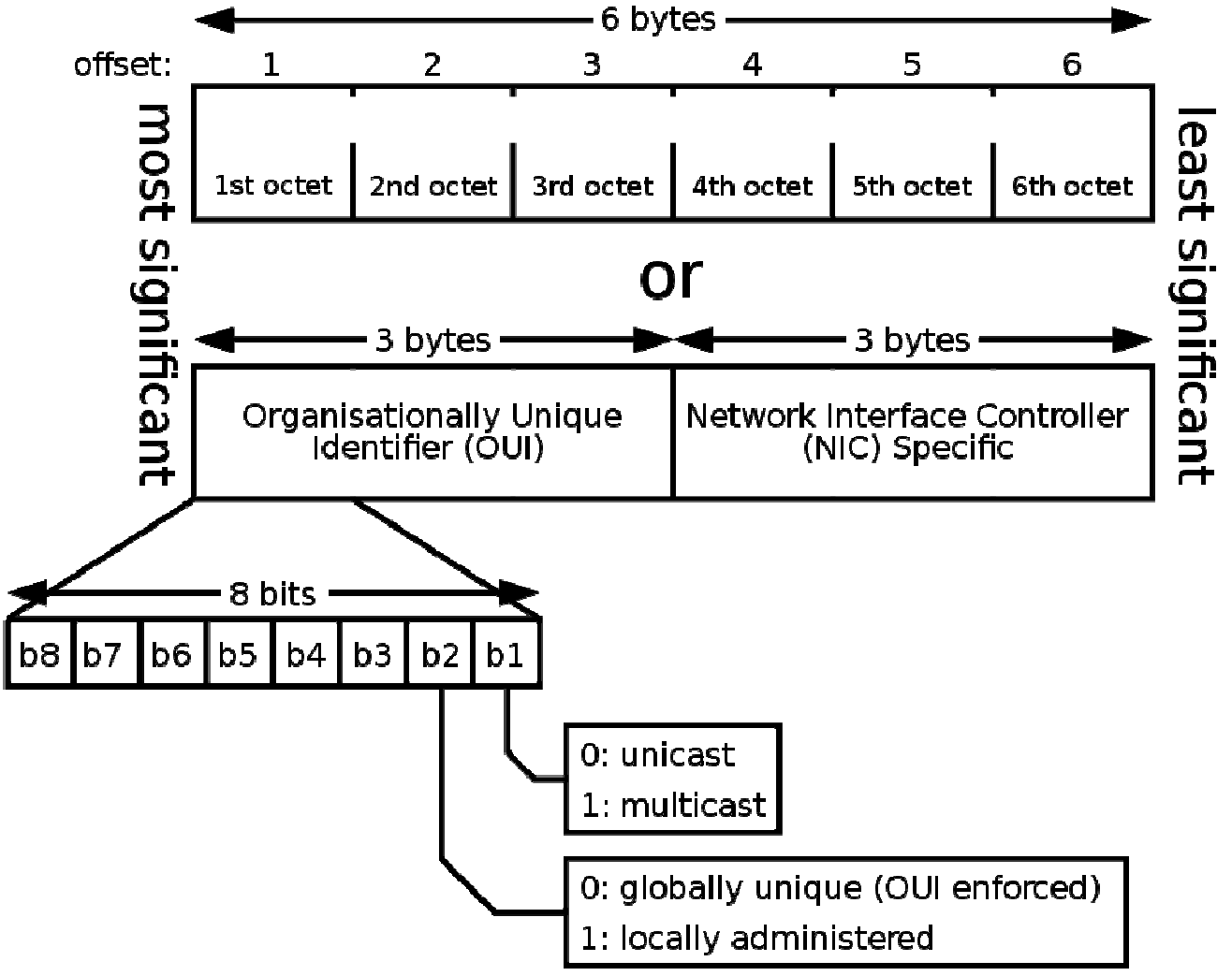
```
Here are the results of your search through the public section of the IEEE
Standards OUI database report for 00216a:
---------------------------------------------------------------------------
00-21-6A (hex)      Intel Corporate
00216A   (base 16)  Intel Corporate
                    Lot 8, Jalan Hi-Tech 2/3
                    Kulim Hi-Tech Park
                    Kulim Kedah 09000
                    MALAYSIA
---------------------------------------------------------------------------
Your attention is called to the fact that the firms and numbers listed may not
always be obvious in product implementation. Some manufacturers subcontract
component manufacture and others include registered firms' OUIs in their
products.
```

MAC address

```
gaia:~# ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
qlen 1000
    link/ether 00:11:d8:92:95:50 brd ff:ff:ff:ff:ff:ff
```

http://standards.ieee.org/regauth/oui/

```
Here are the results of your search through the public section of the IEEE
Standards OUI database report for 0011D8:
-----------------------------------------------------------------------
00-11-D8   (hex)              ASUSTek Computer Inc.
0011D8     (base 16)  ASUSTek Computer Inc.
                      No. 15, Li-Te Rd., Peitou
                      Taipei  112
                      TAIWAN, REPUBLIC OF CHINA
-----------------------------------------------------------------------
Your attention is called to the fact that the firms and numbers listed may not
always be obvious in product implementation. Some manufacturers subcontract
component manufacture and others include registered firms' OUIs in their
products.
```


6 bytes
offset:
1
2
3
4
5
6
most significant
least significant
1st octet
2nd octet
3rd octet
4th octet
5th octet
6th octet
or
3 bytes
3 bytes
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific
8 bits
b8
b7
b6
b5
b4
b3
b2
b1
0: unicast
1: multicast
0: globally unique (OUI enforced)
1: locally administered

Wireshark demo

Въпроси