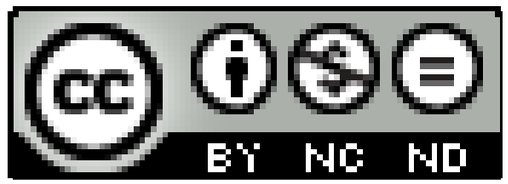
Мрежова сигурност I

http://training.iseca.org/

Recap



Boyan Krosnov

План на курса

- Увод в мрежовата сигурност
- Криптография
- Увод в мрежите
- Ethernet
- Wi-Fi
- IP
- UDP, DHCP, ARP, Атаки върху IP
- IP routing protocols, IPv6
- TCP

→ **Лекция преговор – 16-ти Ноември**

- Тест – 18-ти Ноември
- Демо
- …

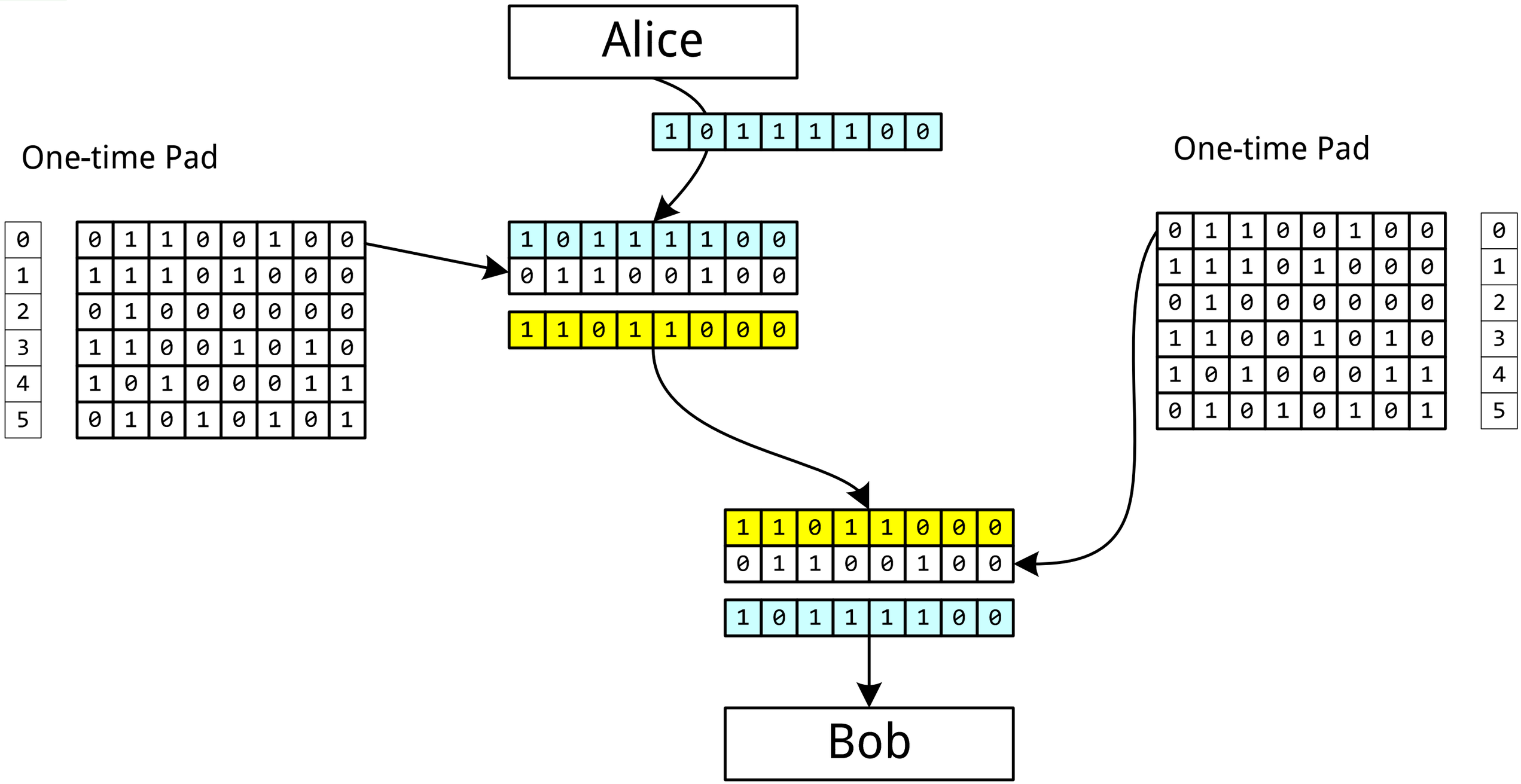
Crypto

- One-time pad
- Крипто алгоритъм vs. крипто система

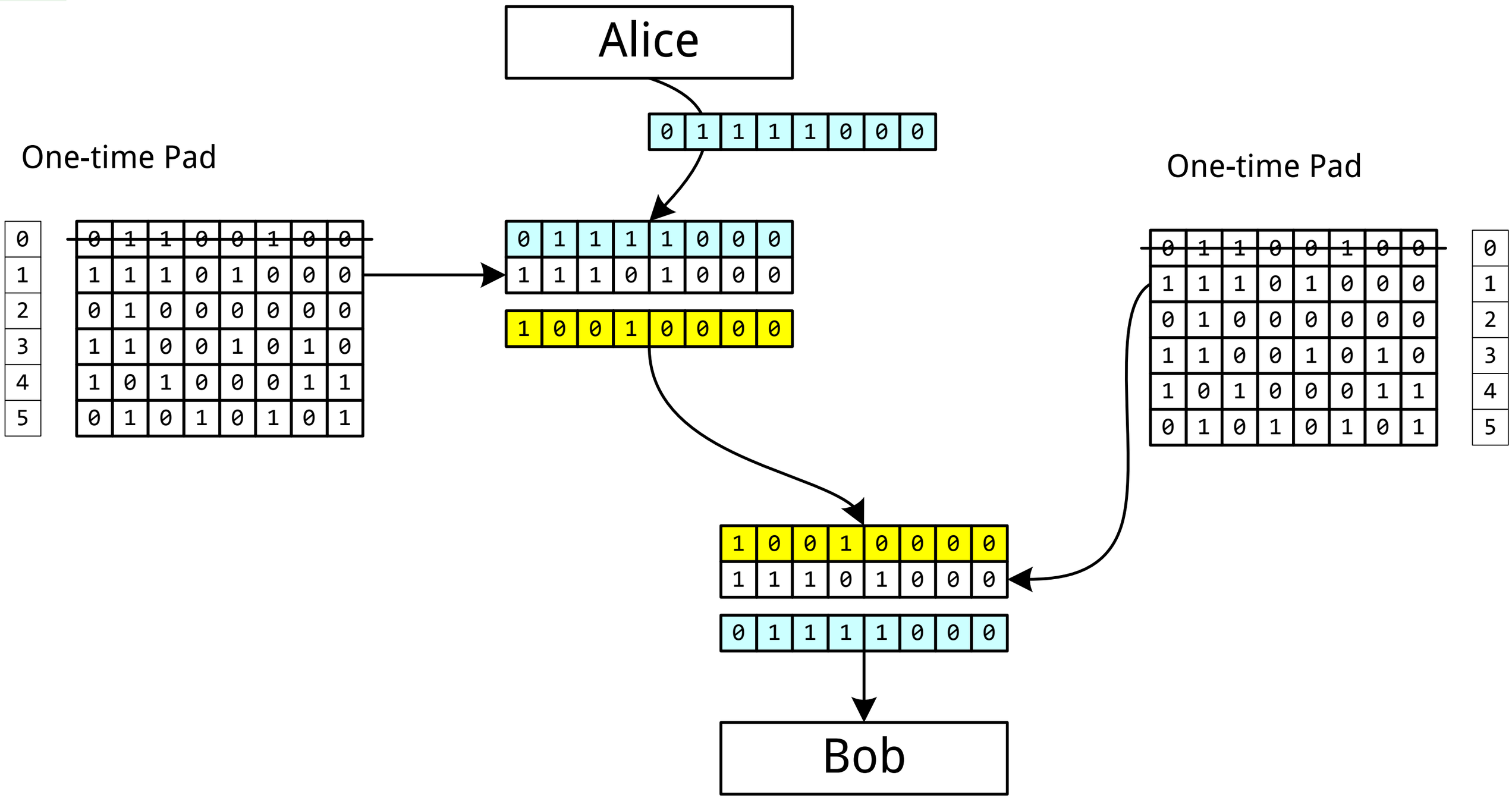
- Асиметричен алгоритъм – e.g. RSA
- Симетричен алгоритъм – e.g. AES, DES

- Поточен алгоритъм – e.g. RC4
- Блоков алгоритъм – e.g. AES, DES
  - режими на работа – e.g. CBC, ECB

One-time Pad


Alice
1 0 1 1 1 1 0 0
One-time Pad
0 1 1 0 0 1 0 0
1 1 1 0 1 0 0 0
0 1 0 0 0 0 0 0
1 1 0 0 1 0 1 0
1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1
0 1 2 3 4 5
1 0 1 1 1 1 0 0
0 1 1 0 0 1 0 0
1 1 0 1 1 0 0 0
One-time Pad
0 1 1 0 0 1 0 0
1 1 1 0 1 0 0 0
0 1 0 0 0 0 0 0
1 1 0 0 1 0 1 0
1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1
0 1 2 3 4 5
1 1 0 1 1 0 0 0
0 1 1 0 0 1 0 0
1 0 1 1 1 1 0 0
Bob

One-time Pad

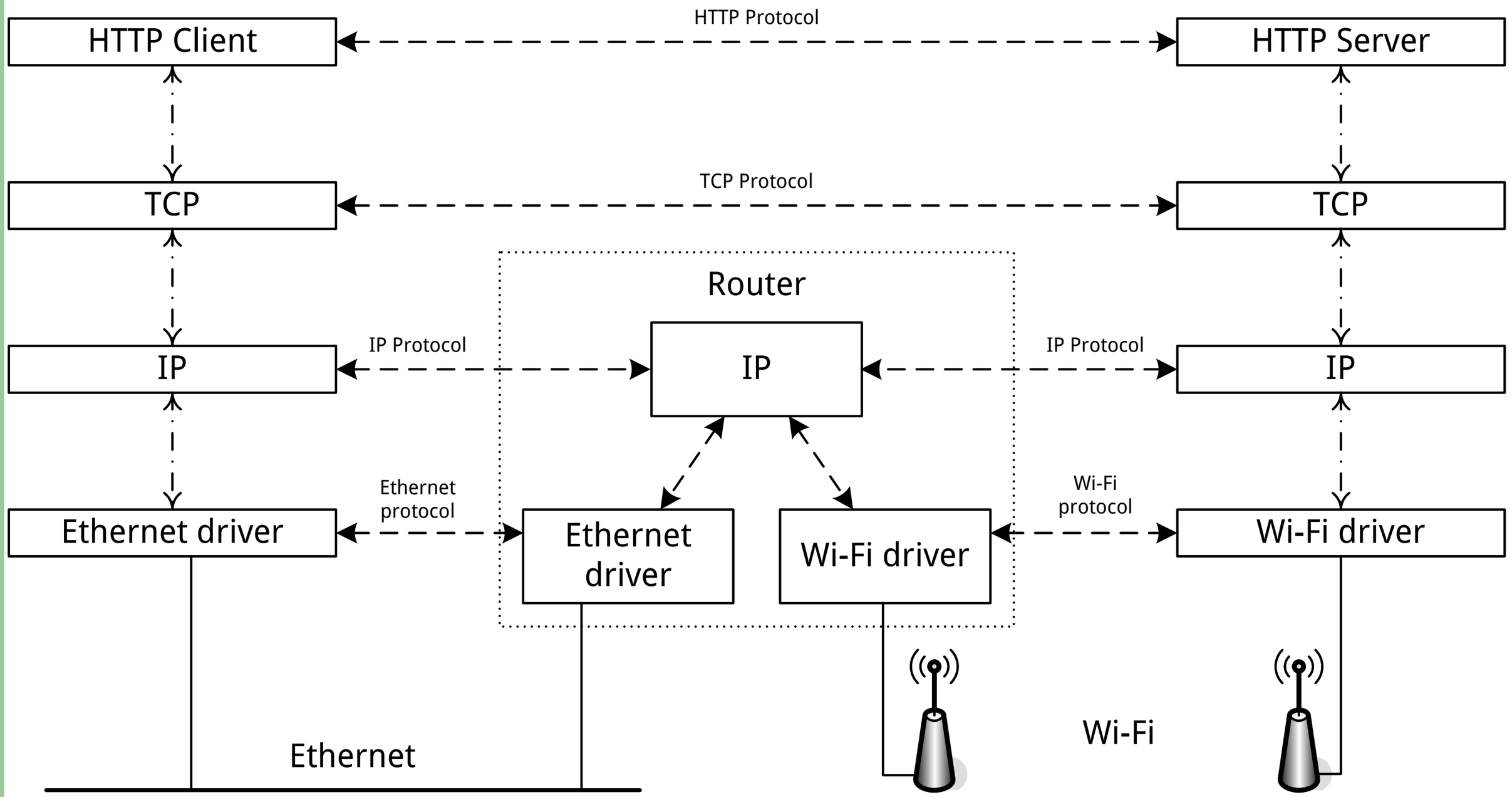

Alice
0 1 1 1 1 0 0 0
One-time Pad
0 1 1 0 0 1 0 0
1 1 1 0 1 0 0 0
0 1 0 0 0 0 0 0
1 1 0 0 1 0 1 0
1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1
0 1 2 3 4 5
0 1 1 1 1 0 0 0
1 1 1 0 1 0 0 0
1 0 0 1 0 0 0 0
One-time Pad
0 1 1 0 0 1 0 0
1 1 1 0 1 0 0 0
0 1 0 0 0 0 0 0
1 1 0 0 1 0 1 0
1 0 1 0 0 0 1 1
0 1 0 1 0 1 0 1
0 1 2 3 4 5
1 0 0 1 0 0 0 0
1 1 1 0 1 0 0 0
0 1 1 1 1 0 0 0
Bob

Crypto

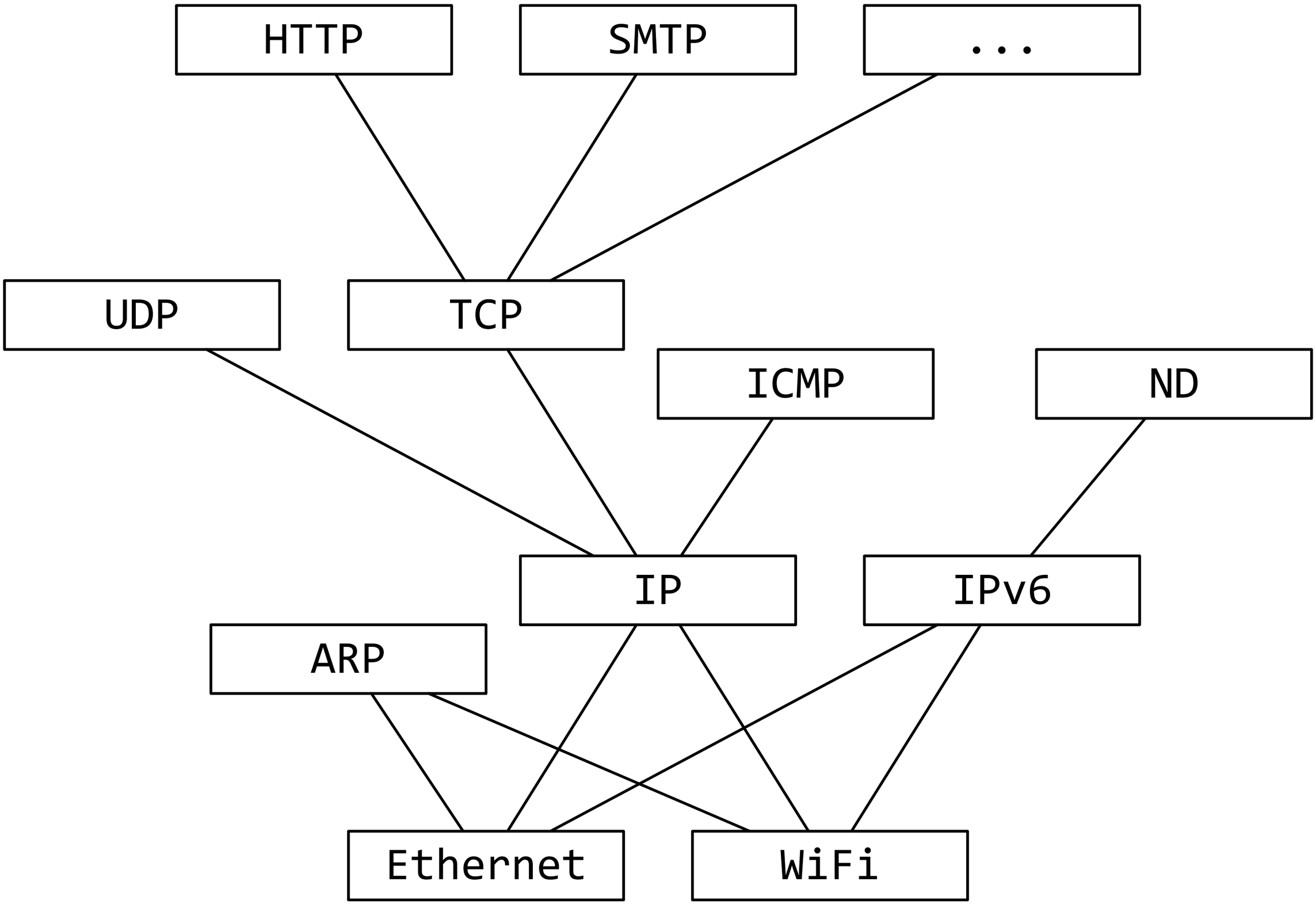
- Криптографски хеш функции
  - e.g. MD5, SHA-1, SHA-2
  - collision resistance
    - трудно да се намерят m1 и m2, за които h(m1)=h(m2)
  - second pre-image resistance
    - при известно m1 е трудно да се намери m2, за което h(m1)=h(m2)
  - preimage resistance
    - при известно h1 е трудно е да се намери m2 за което h1=h(m2)
- HMAC – Hash based message authentication code
- Challenge/response

Въпроси

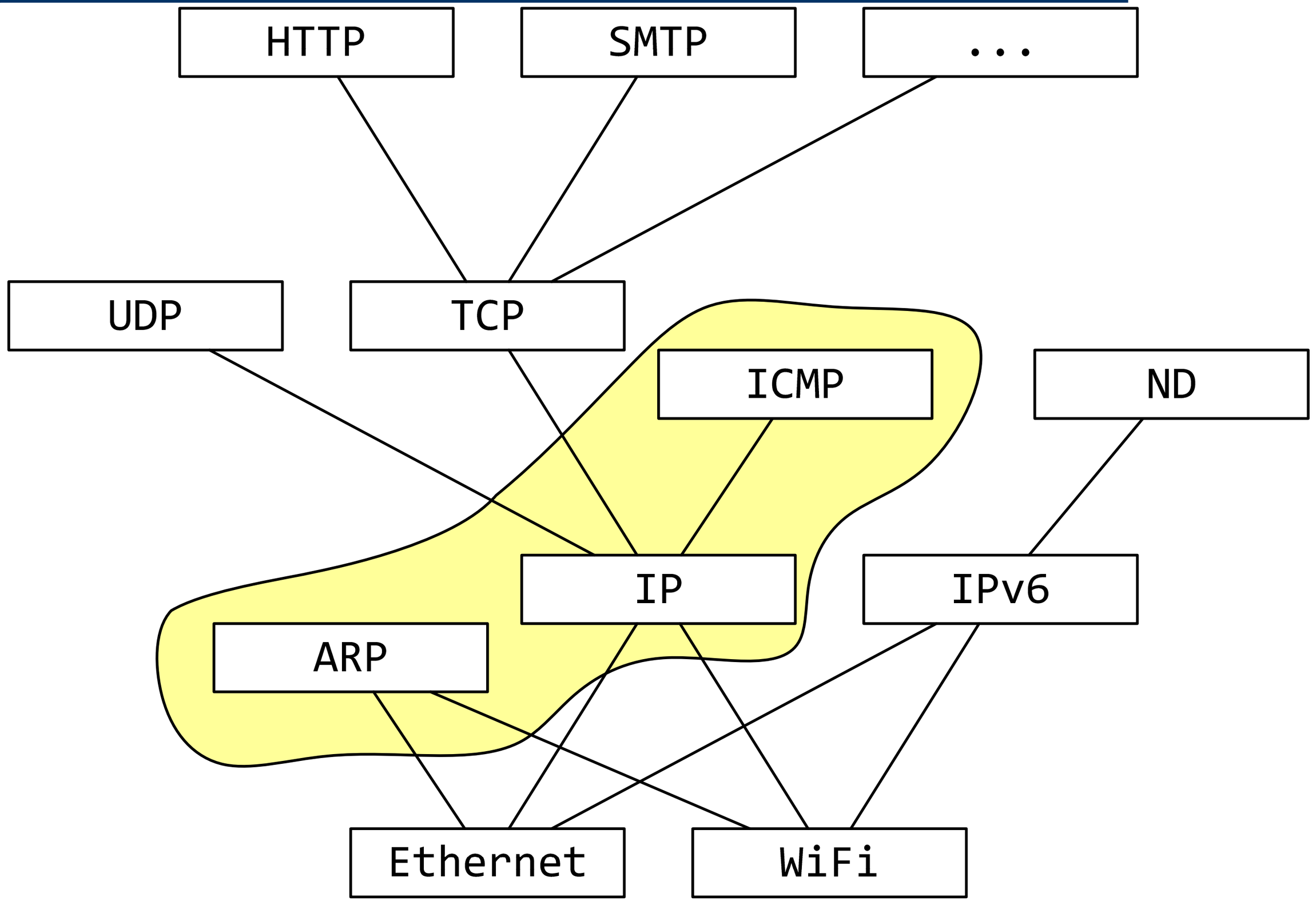
Слоевете


HTTP Client
HTTP Protocol
HTTP Server
TCP
TCP Protocol
TCP
Router
IP
IP Protocol
IP
IP Protocol
IP
Ethernet driver
Ethernet protocol
Ethernet driver
Wi-Fi driver
Wi-Fi protocol
Wi-Fi driver
Ethernet
Wi-Fi

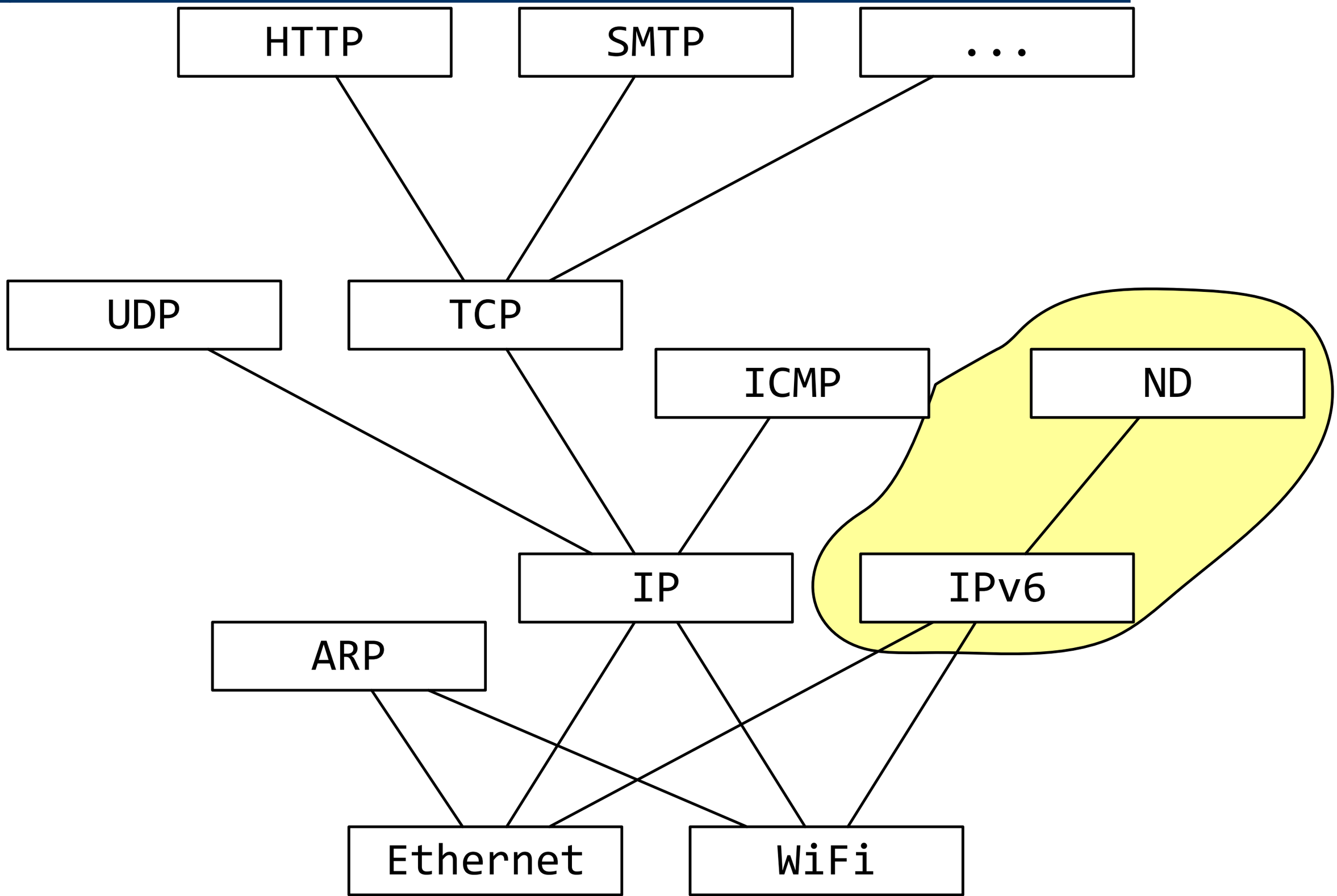
Protocol stack

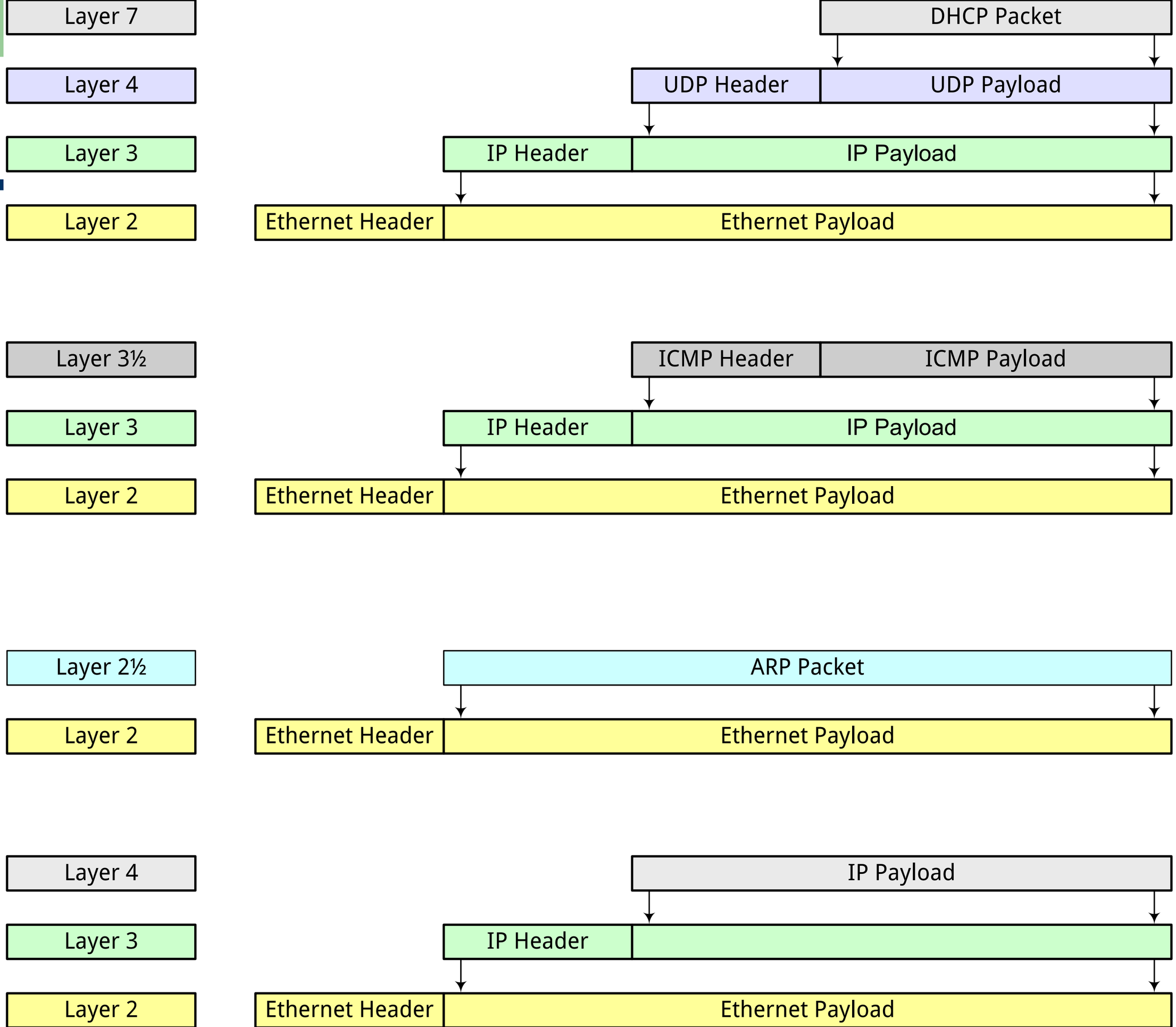


Protocol stack



Protocol stack




Layer 7
DHCP Packet
Layer 4
UDP Header
UDP Payload
Layer 3
IP Header
IP Payload
Layer 2
Ethernet Header
Ethernet Payload
Layer 3½
ICMP Header
ICMP Payload
Layer 3
IP Header
IP Payload
Layer 2
Ethernet Header
Ethernet Payload
Layer 2½
ARP Packet
Layer 2
Ethernet Header
Ethernet Payload
Layer 4
IP Payload
Layer 3
IP Header
Layer 2
Ethernet Header
Ethernet Payload

Терминология

- TCP – сегмент
- IP – пакет
- Ethernet – фрейм

Имената на полетата

- TCP
  - **source port, destination port**
  - sequence number, acknowledge number, window
  - flags – SYN, FIN, ACK, RST, PSH, URG
  - options
  - Urgent pointer
- IP –
  - **source address, destination address (IP)**
  - **protocol**
  - header checksum
  - id, flags, fragmentation offset
  - options
  - etc.
- Ethernet
  - **source address, destination address (MAC)**
  - **ethertype**

Routing

- Longest prefix match
- Recursive lookup

- Static routing
  - таблицата се попълва от администратора

- Dynamic Routing
  - Distance Vector – RIP
  - Link State – OSPF

  - вътрешен, външен, BGP

Въпроси

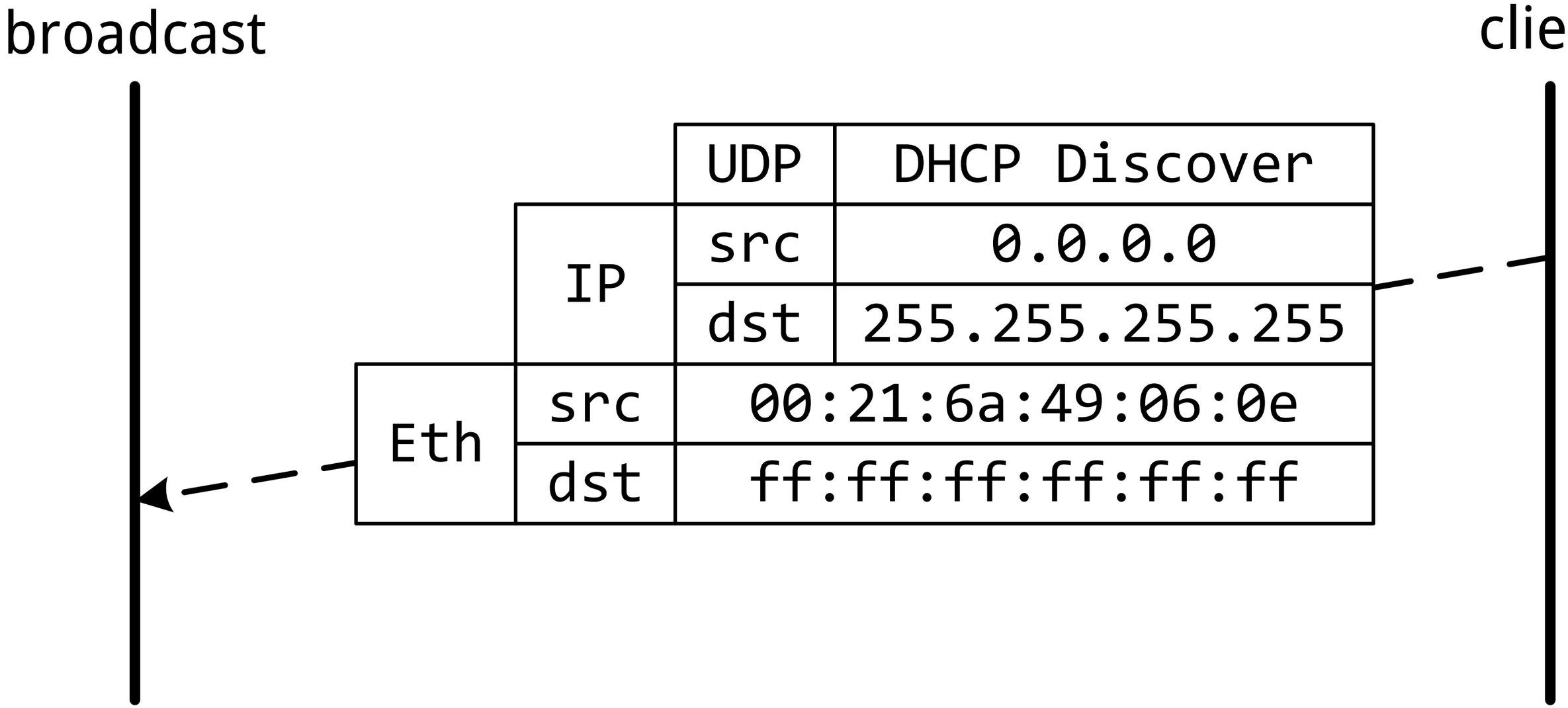
Packet capture example

- DHCP – DISCOVER, OFFER, REQUEST ACK
- ICMP echo from DHCP server
- ARP
  - gratuitous ARP from client
  - unicast ARP request from router

- Ping

- Traceroute

DHCP DISCOVER



Ping from server (address check)

server

client

		ICMP	ICMP Echo
IP		src	192.168.9.1
		dst	192.168.9.198
Eth		src	00:19:d1:a8:15:ed
		dst	00:21:6a:49:06:0e

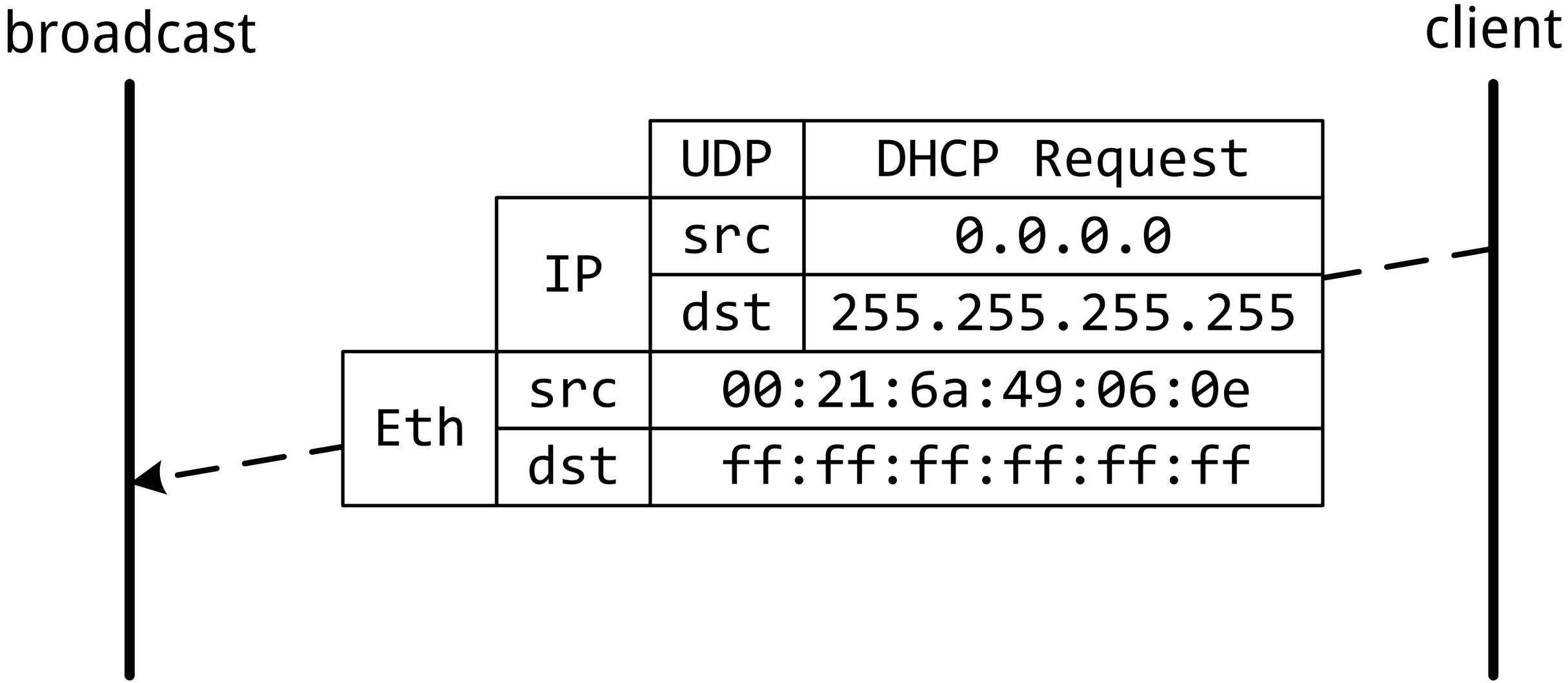
DHCP OFFER

server

client

	UDP	DHCP Offer
IP	src	192.168.9.1
	dst	192.168.9.198
Eth	src	00:19:d1:a8:15:ed
	dst	00:21:6a:49:06:0e

DHCP REQUEST



DHCP ACK

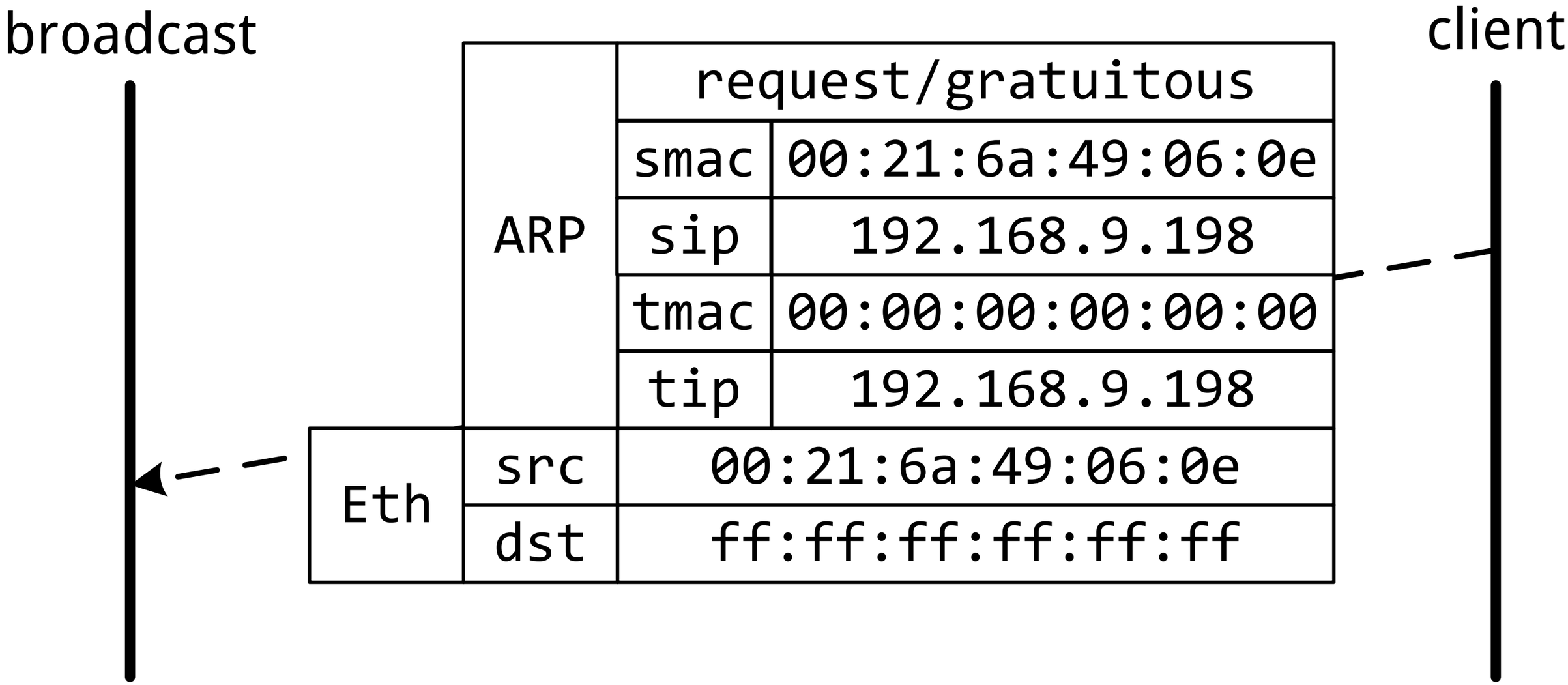
server

client

		UDP	DHCP ACK
	IP	src	192.168.9.1
		dst	192.168.9.198
Eth	src	00:19:d1:a8:15:ed	
	dst	00:21:6a:49:06:0e	

Gratuitous ARP

- duplicate address check



Въпроси

ARP request

server

client

		Request	
ARP	smac	00:19:d1:a8:15:ed	
	sip	192.168.9.1	
	tmac	00:00:00:00:00:00	
	tip	192.168.9.198	
Eth	src	00:19:d1:a8:15:ed	
	dst	00:21:6a:49:06:0e	

ARP reply

client

server

ARP	Reply	
	smac	00:21:6a:49:06:0e
	sip	192.168.9.198
	tmac	00:19:d1:a8:15:ed
	tip	192.168.9.1

Eth		
	src	00:21:6a:49:06:0e
	dst	00:19:d1:a8:15:ed

Въпроси