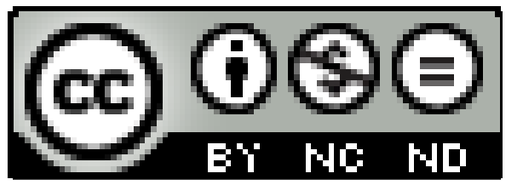
Мрежова сигурност I

http://training.iseca.org/

IP – лекции 1/7 и 2/7



Boyan Krosnov

Преговор и план на курса

- Увод в мрежовата сигурност
- Криптография
- Увод в мрежите
- Ethernet
- Wi-Fi

→ IP

- UDP, DHCP, ARP, IP routing protocols
- IPv6
- TCP
- Тест – средата-края на Ноември
- Демо
- …

План

- История
- Стандартите
- IP service model
- Адресиране
  - основи
  - специални адреси
  - CIDR
  - алокиране на IP адреси
- The IPv4 protocol
  - header format
  - basic routing
  - fragmentation
  - options

История

- 1969 – ARPANET transmits first packets
- 1974 – first TCP spec – RFC 675
- 1981 – current TCP/IP base specification – RFC 791, 792, 793, 768
- Плавни ъпгрейди и промени през годините
  - вкл. 1993 - CIDR

Слоевете

7. HTTP, FTP, SMTP, POP3, IMAP4, SIP, XMPP, IRC, SNMP, SSH, DNS, NTP, DHCP
4/5. TCP, UDP, RTP, SCTP
3. IP / IPv6
2. Ethernet, Wi-Fi, etc.
1. physical media, modulation and coding

Стандартите

- IETF
  - http://www.rfc-editor.org/rfcsearch.html
- IETF Draft, RFC, STD, BCP, etc.
  - Request for Comment
    - Status
      - Informational - някои стават FYI
      - Best Current Practice - някои стават BCP
      - Experimental
      - Standards Track - някои стават STD
        - Draft Standard -> Proposed Standard -> Internet Standard
    - Version
      - Updates, Updated by, Obsoletes, Obsoleted by

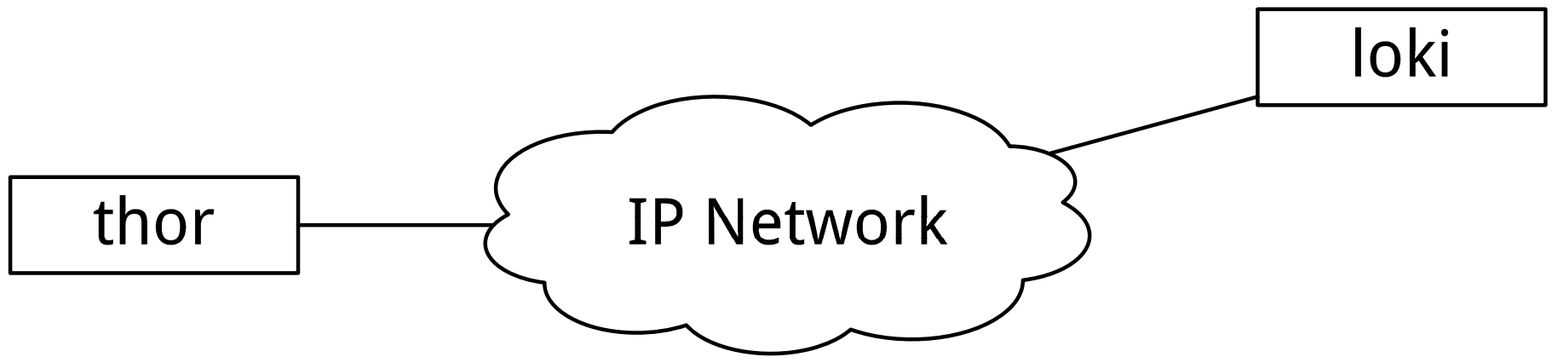
Стандартите

- STD5 съдържа
  - **RFC791** – IP
    - Updated by **RFC1349** - TOS
  - **RFC792** – ICMP
    - Updated by **RFC950**
    - Updated by **RFC4884** - Support Multi-Part ICMP Messages
  - **RFC919** – Broadcasting Internet Datagrams
  - **RFC950** – Internet Standard Subnetting Procedure
  - **RFC1112** – Host extensions for IP multicasting
    - Updated by **RFC2236** - IGMPv2

IP service model

- End-to-end principle
  - dumb network
  - smart hosts

- IP services
  - Addressing
  - Routing
  - и други



- Няма гаранции за
  - Доставка изобщо
  - Доставка в последователен ред
  - Доставка само веднъж (повторение)
  - Грешки в съдържанието

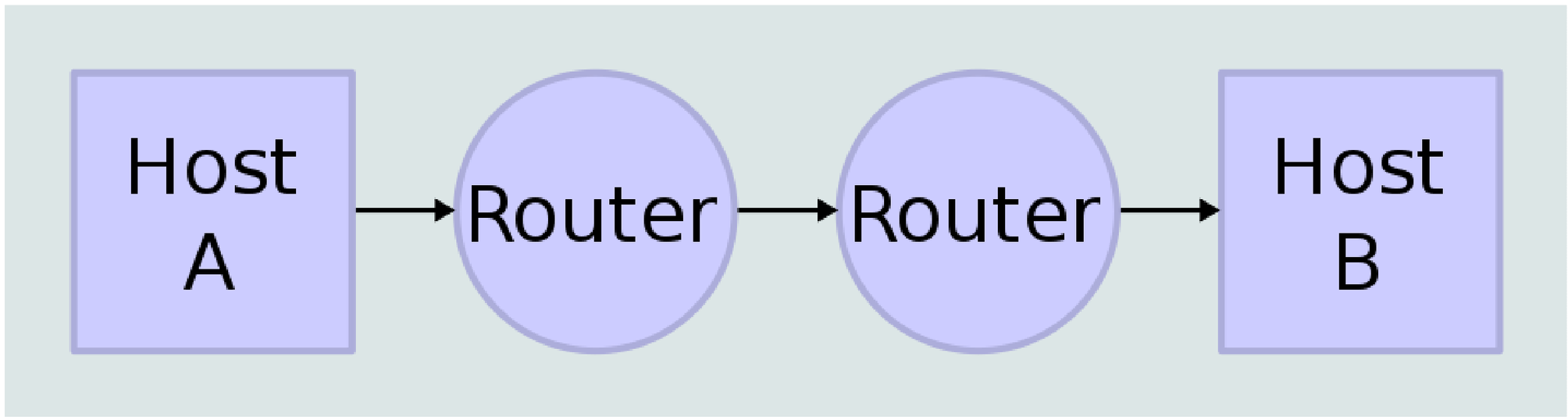
Адресиране

- IP адрес
  - 32 битово число без знак – 0 до 4 294 967 295
  - Записва се `0.0.0.0` до `255.255.255.255`
    - старши байт първо

- Unicast адреси
  - `0.0.0.0` до 223.255.255.255
- Multicast адреси (бивш class D)
  - `224.0.0.0` до `239.255.255.255`
- Експериментални адреси (бивш class E)
  - `240.0.0.0` до `255.255.255.255`

Unicast адреси

- Всеки IP интерфейс има IP адрес
  - адреса не е на хоста
  - адреса не е на кабела или мрежовата карта
- Всеки IP пакет съдържа адреса на изпращача (source address) и адреса на получателя (destination address)
- Мрежата доставя IP пакета на един IP интерфейс на базата на destination address



Адресиране

- Част от адреса е глобален мрежов локатор
  - обозначава мястото в мрежата
- Част от адреса е локален хост идентификатор
  - обозначава кой хост от локалната мрежа

IP Address, decimal	62	44	96	11
Netmask, decimal	255	255	255	0
Netmask, binary	1111 1111	1111 1111	1111 1111	0000 0000

- Йерархично адресиране

Смятане на маски

- Prefix notation
  - a.b.c.d/n
  - n е броя битове които са 1-ца в мрежовата маска
  - примерно 255.255.255.0 = /24, 255.255.240.0 = /20, 255.255.255.248 = /27
- host адрес – 62.44.96.11
- маска – /24 = 255.255.255.0
- host AND mask = network address –> 62.44.96.0
- host OR NOT mask = broadcast –> 62.44.96.255
- рутерът типично е на network+1, понякога на broadcast-1

Смятане на маски

62.44.96.11/24

IP Address, decimal	62	44	96	11
IP Address, binary	0011 1110	0010 1100	0110 0000	0000 1011
Netmask, binary	1111 1111	1111 1111	1111 1111	0000 0000
Netmask, decimal	255	255	255	0
Network, decimal	62	44	96	0
Network, binary	0011 1110	0010 1100	0110 0000	0000 0000
Broadcast, binary	0011 1110	0010 1100	0110 0000	1111 1111
Broadcast, decimal	62	44	96	255

Смятане на маски

62.44.96.11/24

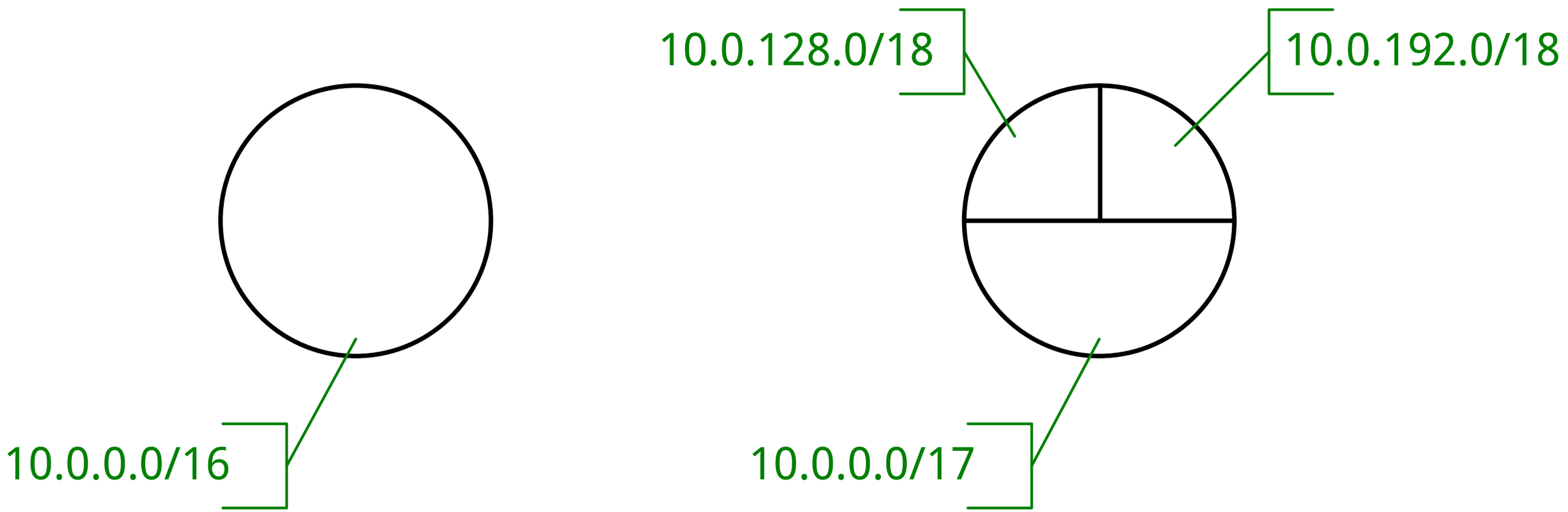
IP Address, decimal	62	44	96	11
IP Address, binary	0011 1110	0010 1100	0110 0000	0000 1011
Netmask, binary	1111 1111	1111 1111	1111 1111	0000 0000
Netmask, decimal	255	255	255	0

Network, decimal	62	44	96	0
Network, binary	0011 1110	0010 1100	0110 0000	0000 0000

Broadcast, binary	0011 1110	0010 1100	0110 0000	1111 1111
Broadcast, decimal	62	44	96	255

Въпроси

Йерархия на адресите



Йерархия на адресите (пример)

- IANA – управлява `0.0.0.0/0`
- IANA алокира на RIPE – `42.0.0.0/8`
- RIPE алокира на български LIR – `42.12.224.0/19`
- Български LIR заделя за цел бизнес клиенти в София `42.12.240.0/20`
- Български LIR алокира на клиента си Банка А – `42.12.241.0/24`
- Банката алокира за локалната мрежа за сървъри – `42.12.241.0/25`
- И на конкретен сървър – `42.12.241.100/32`

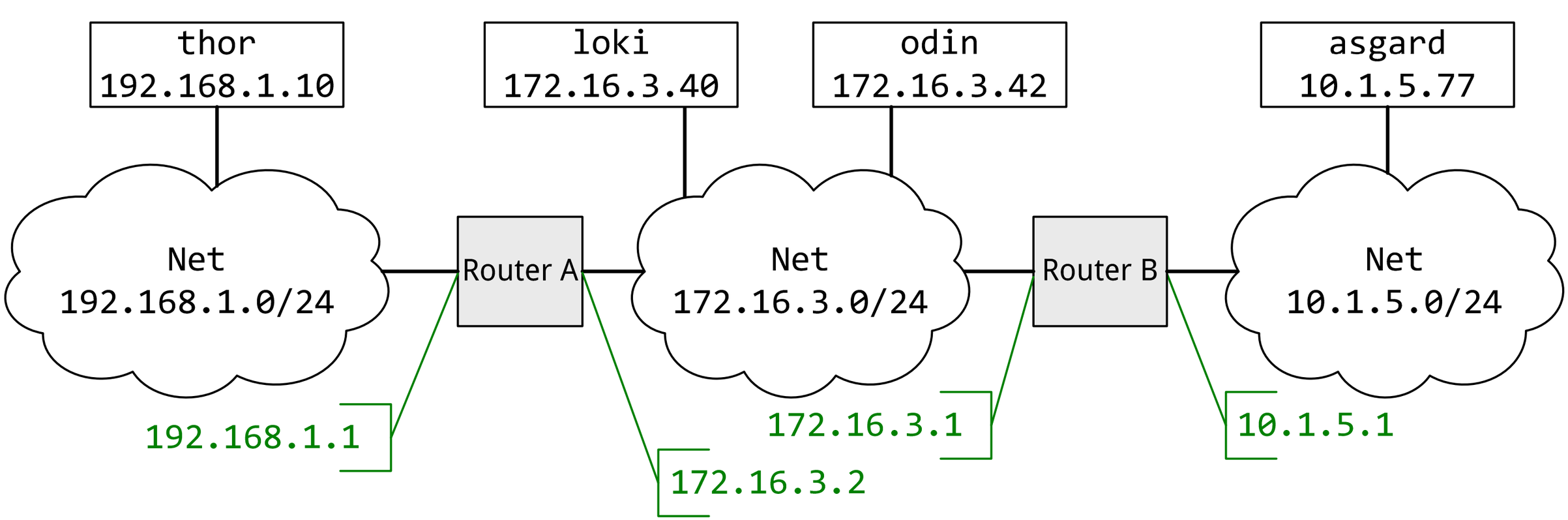
Йерархия на адресите (пример)

the Internet	0.0.0.0/0	2^32	4 294 967 296
RIPE block 42	42.0.0.0/8	2^24	16 777 216
BG LIR block	42.12.224.0/19	2^13	8 192
LIR sub-block	42.12.240.0/20	2^12	4 096
Bank A block	42.12.241.0/24	2^8	256
servers LAN	42.12.241.0/26	2^6	64
DB server	42.12.241.42/32	2^0	1

- 42.12.241.42/32 се съдържа в 42.12.241.0/26, което се съдържа в 42.12.241.0/24 <- 42.12.240.0/20 <- 42.12.224.0/19 <- 42.0.0.0/8 <- 0.0.0.0/0

Адресиране

- Комуникацията между хостове в същия subnet е директна – не преминава през рутери
  - multi-access мрежи (E.g. Ethernet, Wi-Fi)
  - рутиране в хоста

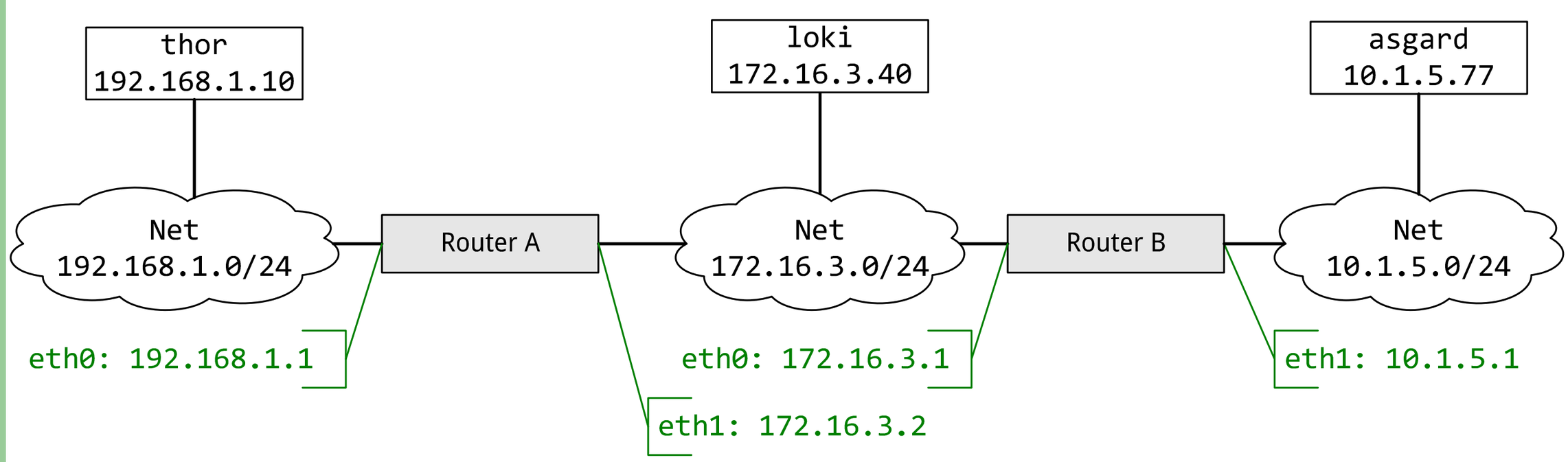


Routing tables

directly connected
indirect

Router A routing table	
Network	Through
192.168.1.0/24	eth0
172.16.3.0/24	eth1
10.1.5.0/24	172.16.3.1

Router B routing table	
Network	Through
10.1.5.0/24	eth1
172.16.3.0/24	eth0
192.168.1.0/24	172.16.3.2



thor routing table	
Network	Through
192.168.1.0/24	-
172.16.3.0/24	192.168.1.1
10.1.5.0/24	192.168.1.1

loki routing table	
Network	Through
172.16.3.0/24	-
192.168.1.0/24	172.16.3.2
10.1.5.0/24	172.16.3.1

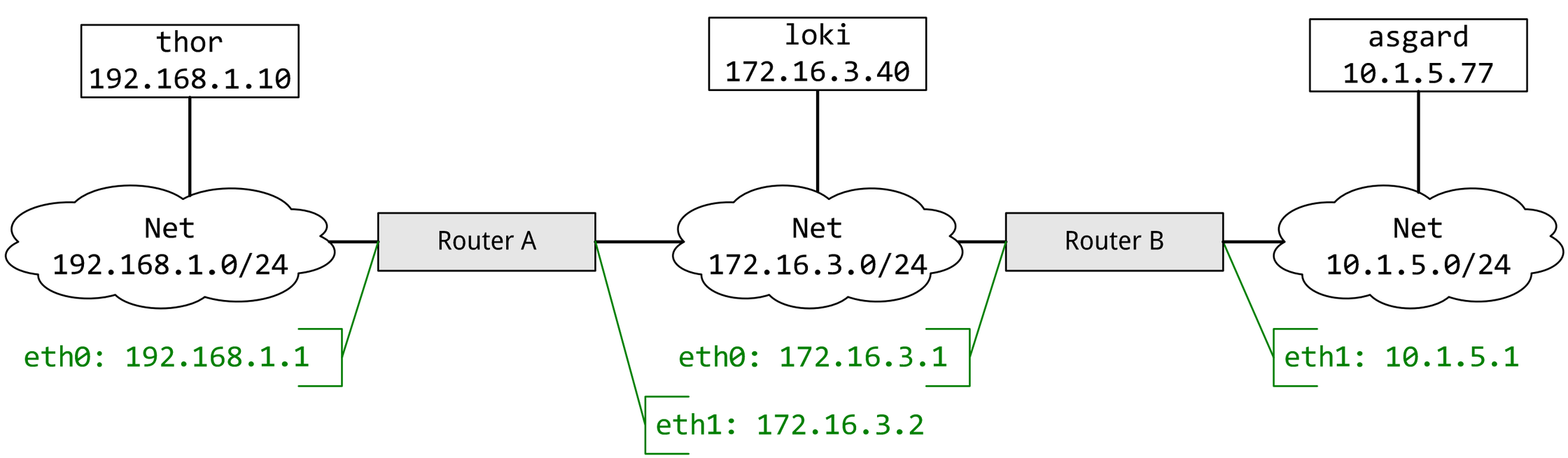
asgard routing table	
Network	Through
10.1.5.0/24	-
172.16.3.0/24	10.1.5.1
192.168.1.0/24	10.1.5.1

Routing tables (recursive lookup)

directly connected
indirect

Router A routing table	
Network	Through
192.168.1.0/24	eth0
172.16.3.0/24	eth1
10.1.5.0/24	172.16.3.1

Router B routing table	
Network	Through
10.1.5.0/24	eth1
172.16.3.0/24	eth0
192.168.1.0/24	172.16.3.2



thor routing table	
Network	Through
192.168.1.0/24	-
172.16.3.0/24	192.168.1.1
10.1.5.0/24	172.16.3.1

loki routing table	
Network	Through
172.16.3.0/24	-
192.168.1.0/24	172.16.3.2
10.1.5.0/24	172.16.3.1

asgard routing table	
Network	Through
10.1.5.0/24	-
172.16.3.0/24	10.1.5.1
192.168.1.0/24	172.16.3.2

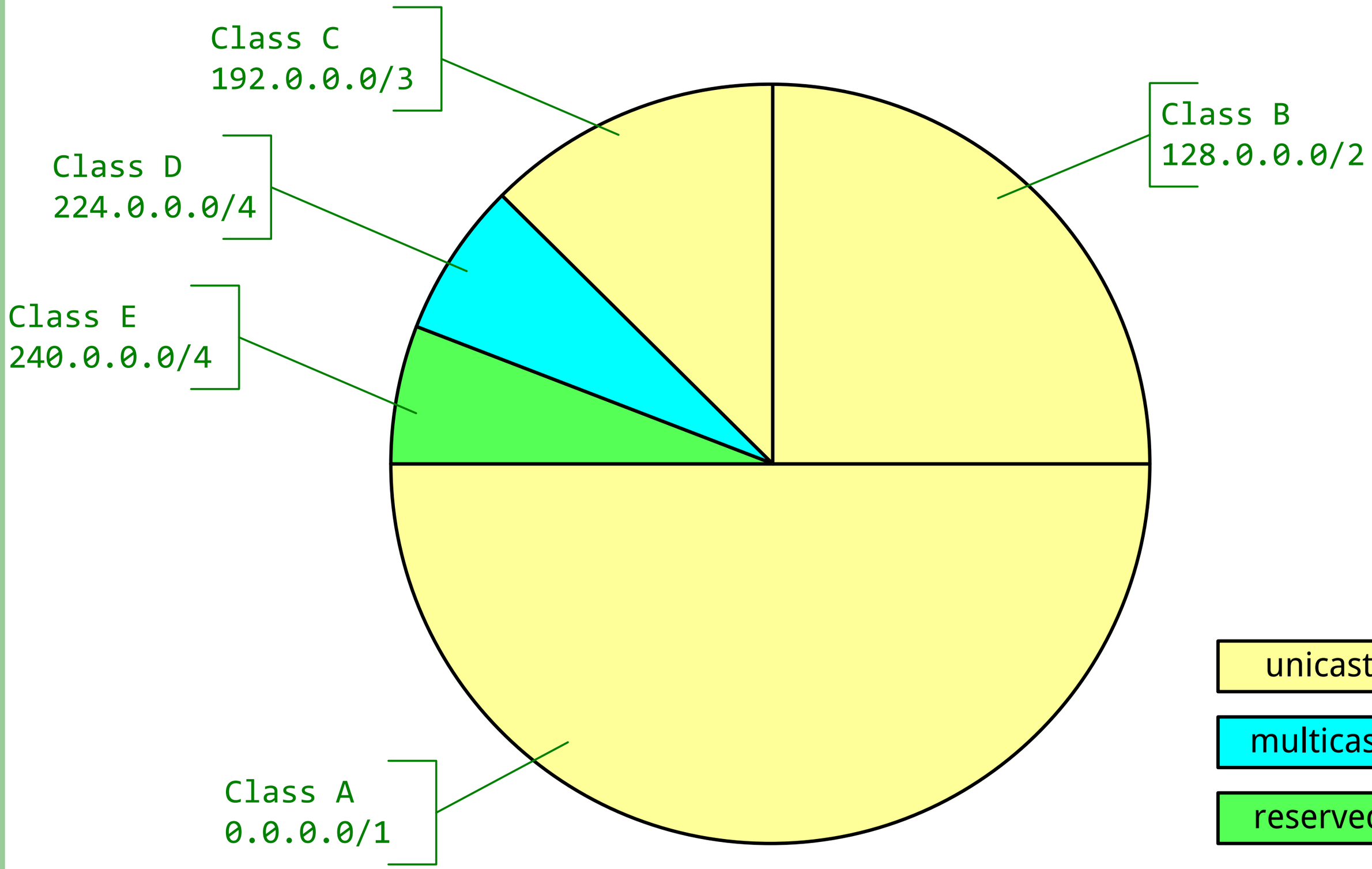
Специални адреси

- Unknown/Unassigned – `0.0.0.0`
- Broadcast – `255.255.255.255`
- Loopback – `127.0.0.0/8`
- Link Local – `169.254.0.0/16` (RFC3927)
- Organization Scope Addresses (RFC1918)
  - `10.0.0.0/8`
  - `172.16.0.0/12`
  - `192.168.0.0/16`
- Фалшиви, Истински, Реални и Имагинерни адреси
  - Публични, Public
  - Частни, Private (RFC1918)

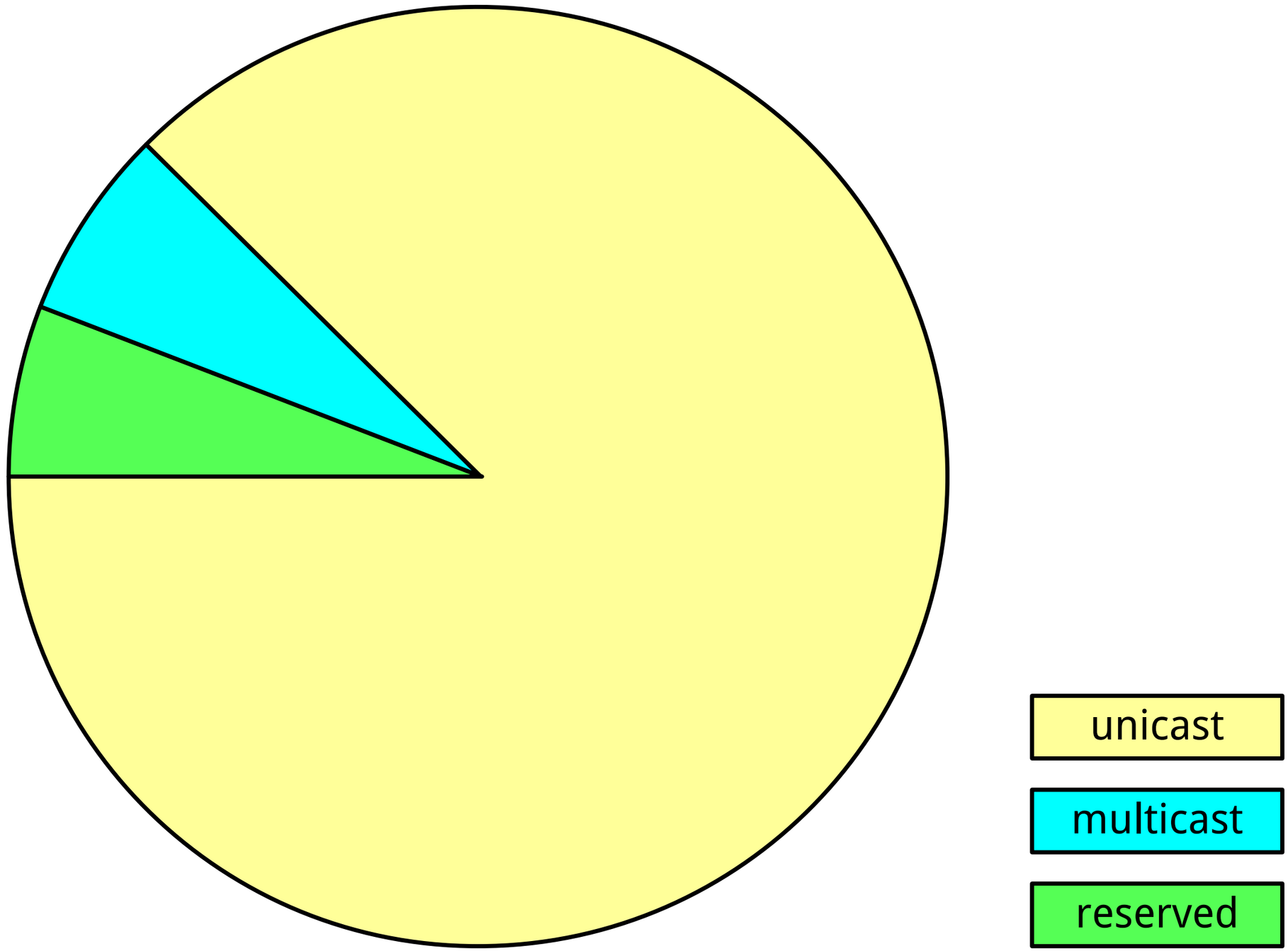
Classless inter-domain routing

- RFC1518 (Sept 1993)
- Класовете
  - A – 0.0.0.0/1, leading bits (0), маска /8
  - B – 128.0.0.0/2, leading bits (10), маска /16
  - C – 192.0.0.0/3, leading bits (110), маска /24
  - D – 224.0.0.0/4, leading bits (1110)
  - E – 240.0.0.0/4, leading bits (1111)
- Защо без класове
- “- Дай ми едно клас Це.”
  - казвайте /24, “слаш-двайсчетири”

Class-full


Class C
192.0.0.0/3
Class B
128.0.0.0/2
Class D
224.0.0.0/4
Class E
240.0.0.0/4
Class A
0.0.0.0/1
unicast
multicast
reserved

Class-less



Алокиране на IP адреси

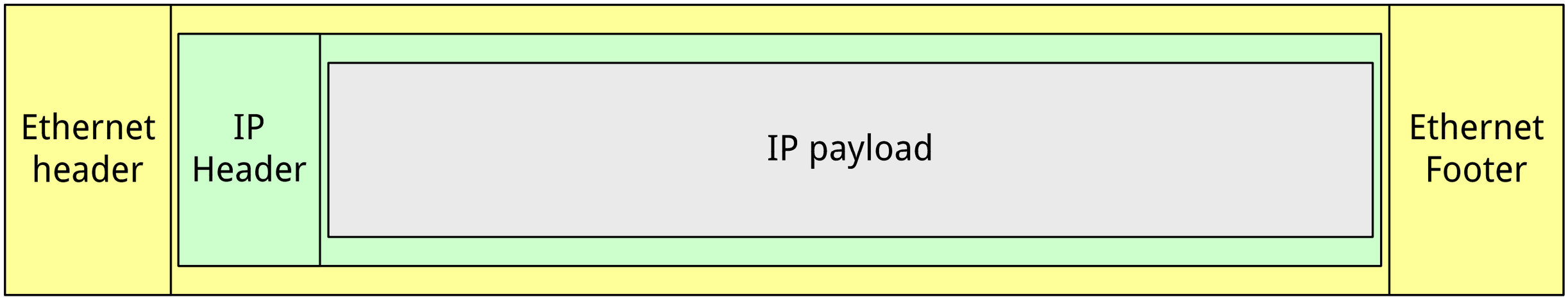
- ICANN (Internet Corporation for Assigned Names and Numbers)
- IANA (Internet Assigned Numbers Authority)
  - `0.0.0.0/0`
- RIR (Regional Internet Registry)
  - ARIN, RIPE, APNIC, LACNIC, AFRINIC
  - /8s
- NIR (National Internet Registry)
- LIR (Local Internet Registry)

Въпроси

IP encapsulation

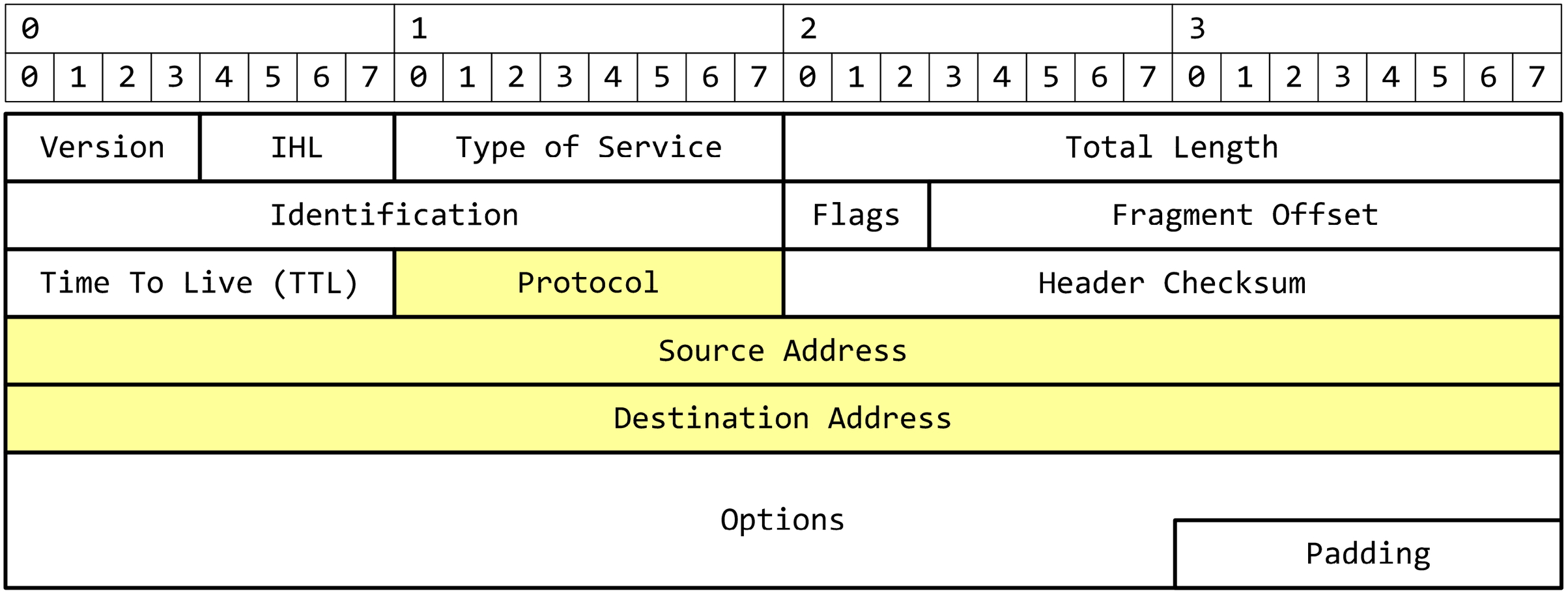
Ethernet frame

IP packet



- IP върху Ethernet, Wi-Fi, etc
- TCP върху IP, UDP върху IP, etc.

IP header



- Обичайните полета – source, destination, protocol
- Други полета
- Big-endian (MSB first)

Как работи рутера

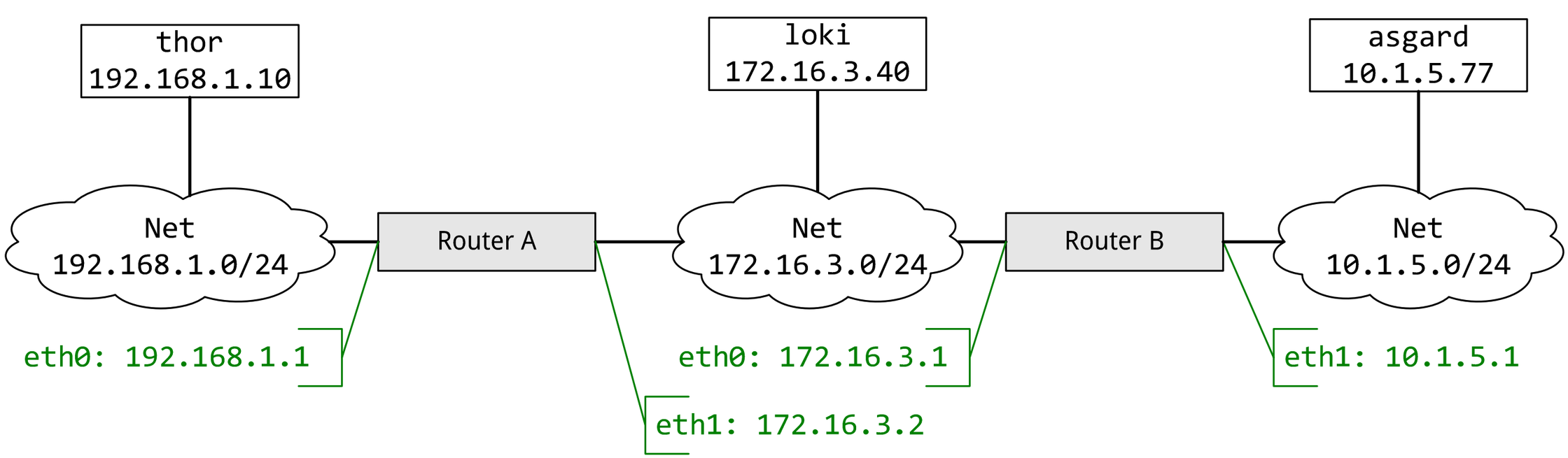
- Рутинг таблица
  - Попълва се статично от администратора
  - ... или динамично (routing protocol)
  - Всеки ред съдържа
    - Prefix – e.g. `10.22.33.0/24`
    - Next hop – e.g. `via 192.168.1.1 on eth0`
- Longest prefix match
  - Имаме пътища за `10.0.0.0/8`, `10.22.33.0/24` и `10.22.33.44/32` в таблицата
  - Пристига пакет за `10.22.33.42`
  - Кой път да изберем ?
- Default route, default gateway – `0.0.0.0/0`

Routing tables

directly connected
indirect

Router A routing table	
Network	Through
192.168.1.0/24	eth0
172.16.3.0/24	eth1
10.1.5.0/24	172.16.3.1

Router B routing table	
Network	Through
10.1.5.0/24	eth1
172.16.3.0/24	eth0
192.168.1.0/24	172.16.3.2



thor routing table	
Network	Through
192.168.1.0/24	-
172.16.3.0/24	192.168.1.1
10.1.5.0/24	172.16.3.1

loki routing table	
Network	Through
172.16.3.0/24	-
192.168.1.0/24	172.16.3.2
10.1.5.0/24	172.16.3.1

asgard routing table	
Network	Through
10.1.5.0/24	-
172.16.3.0/24	10.1.5.1
192.168.1.0/24	172.16.3.2

Как работи рутера

- Hop-by-hop
  - Обработката на IP пакет във всеки рутер зависи само от информация (routing таблица) която се намира в рутера
  - Всеки рутер предава пакета на следващия рутер в посоката на destination address
  - Стъпка по стъпка, пакета се приближава и евентуално достига destination
- Stateless Routers
  - Обработката на IP пакет не оставя никаква следа в рутера. Всеки пакет се обработва сам за себе си
  - От пакети спомен няма

Switch vs. Router

- Bridge и Switch – Layer 2 – Ethernet
  - MAC address learning
  - lookup destination MAC in table
  - forward

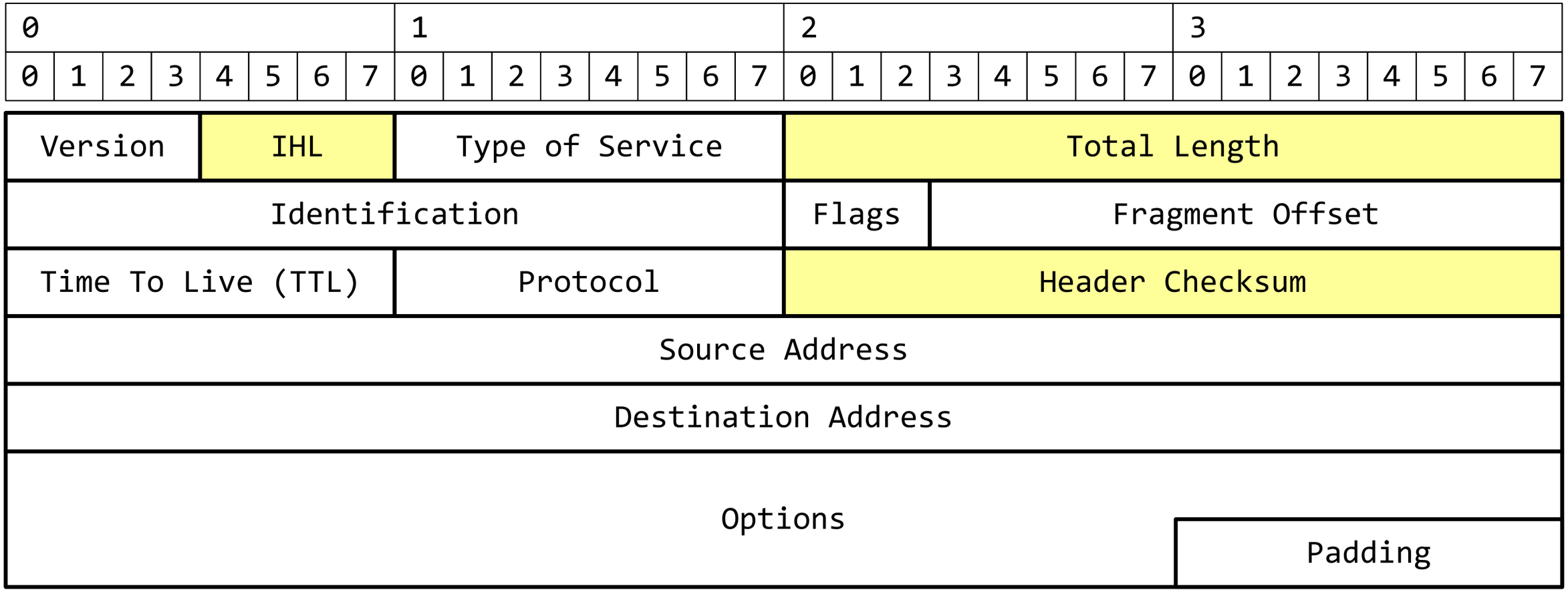
- Router – Layer 3 – IP
  - lookup destination IP in table
  - forward
  - няма научаване на IP адреси
    - таблицата се попълва статично от администратора или динамично от routing protocol

Какво е NAT

- Ще говорим за NAT в лекцията за Firewalls & Tunnels

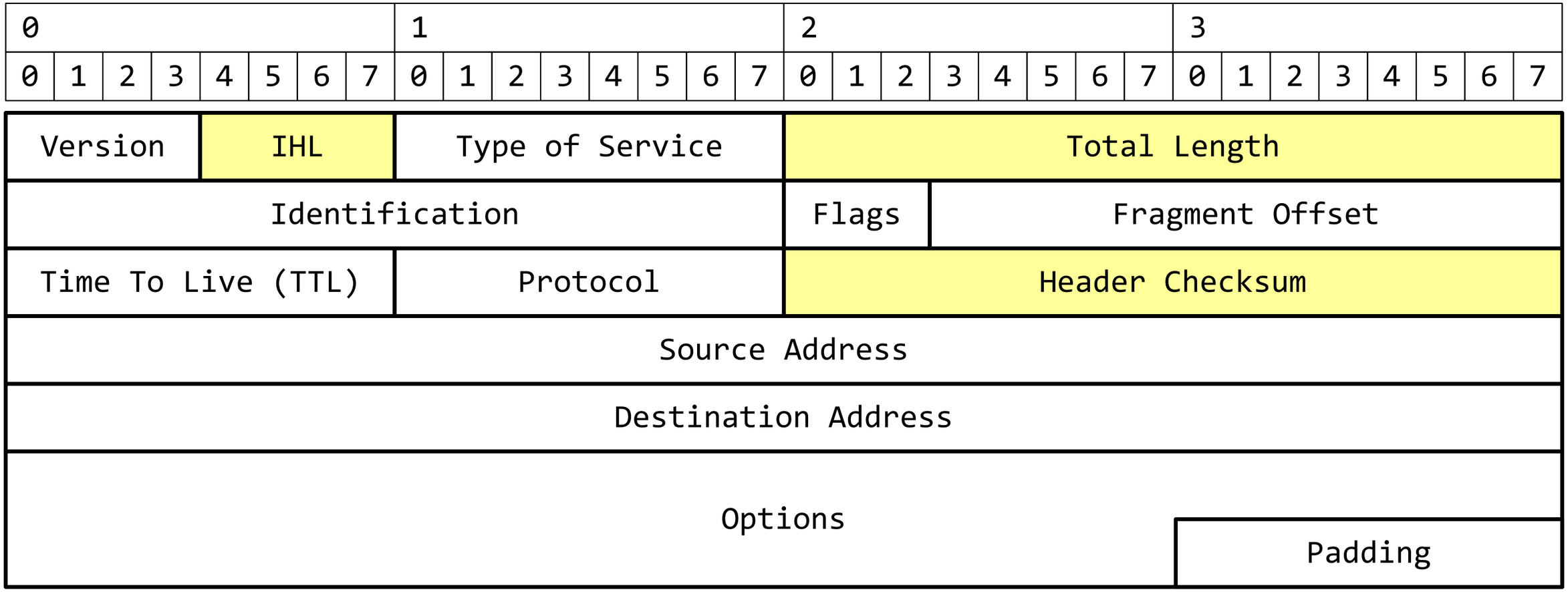
Въпроси

Length, Checksum



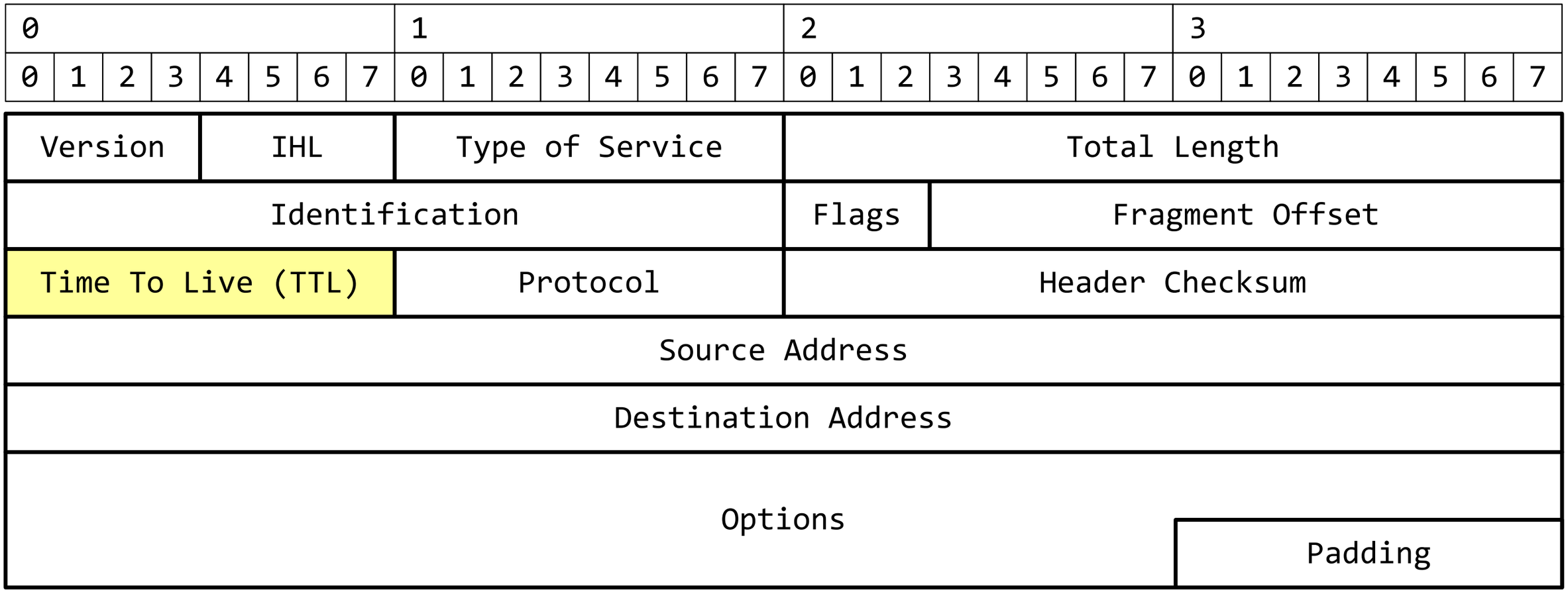
- IHL – Internet Header Length
  - *4 или <<2
  - 5 -> 20, ако няма опции

Length, Checksum



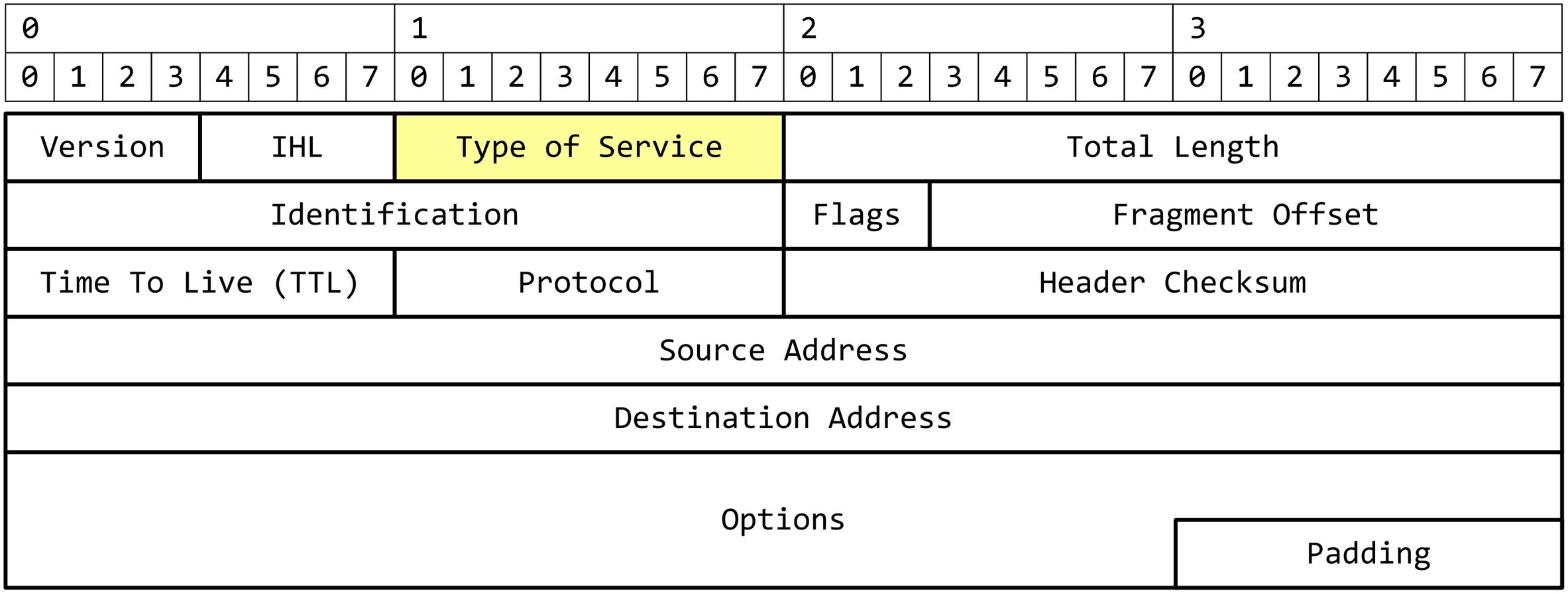
- Total Length – дължина на целия пакет
- Header Checksum – 16-битова чек сума на хедъра

TTL



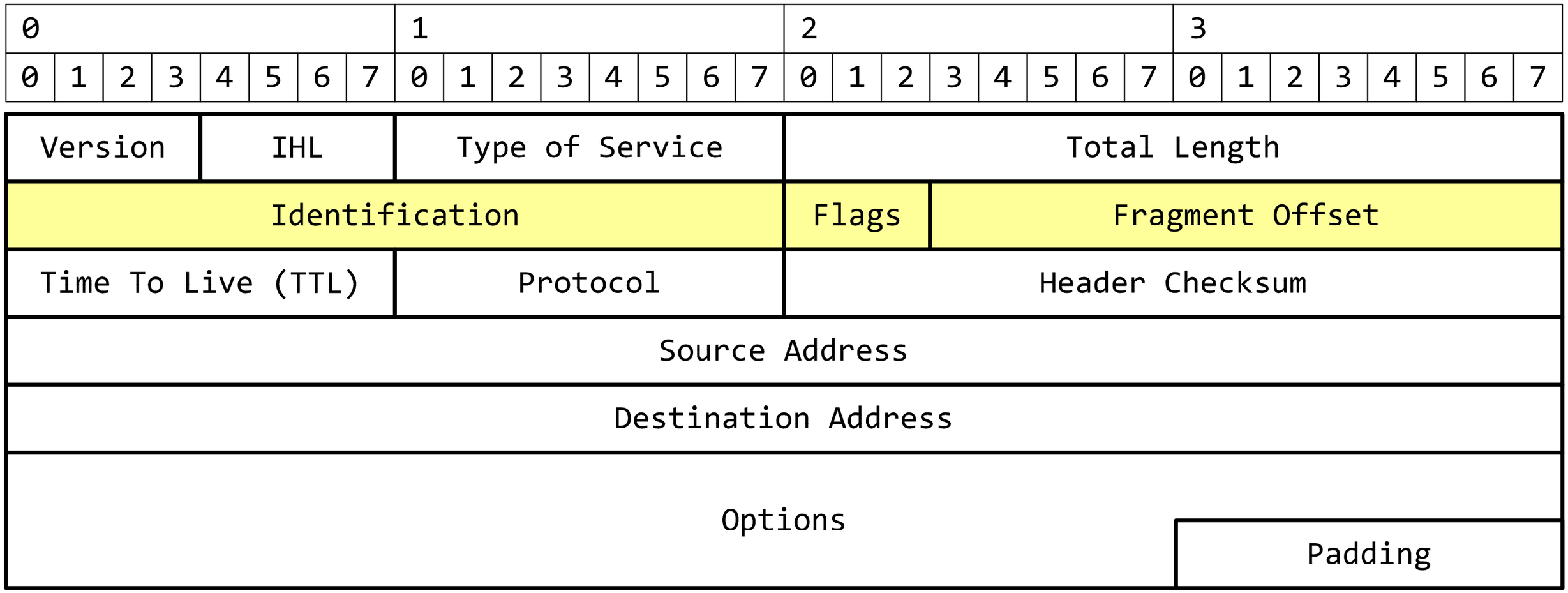
- Намалява се с 1 от всеки рутер
- Ако е станал 0 – drop и генерираме ICMP грешка

DSCP/TOS field



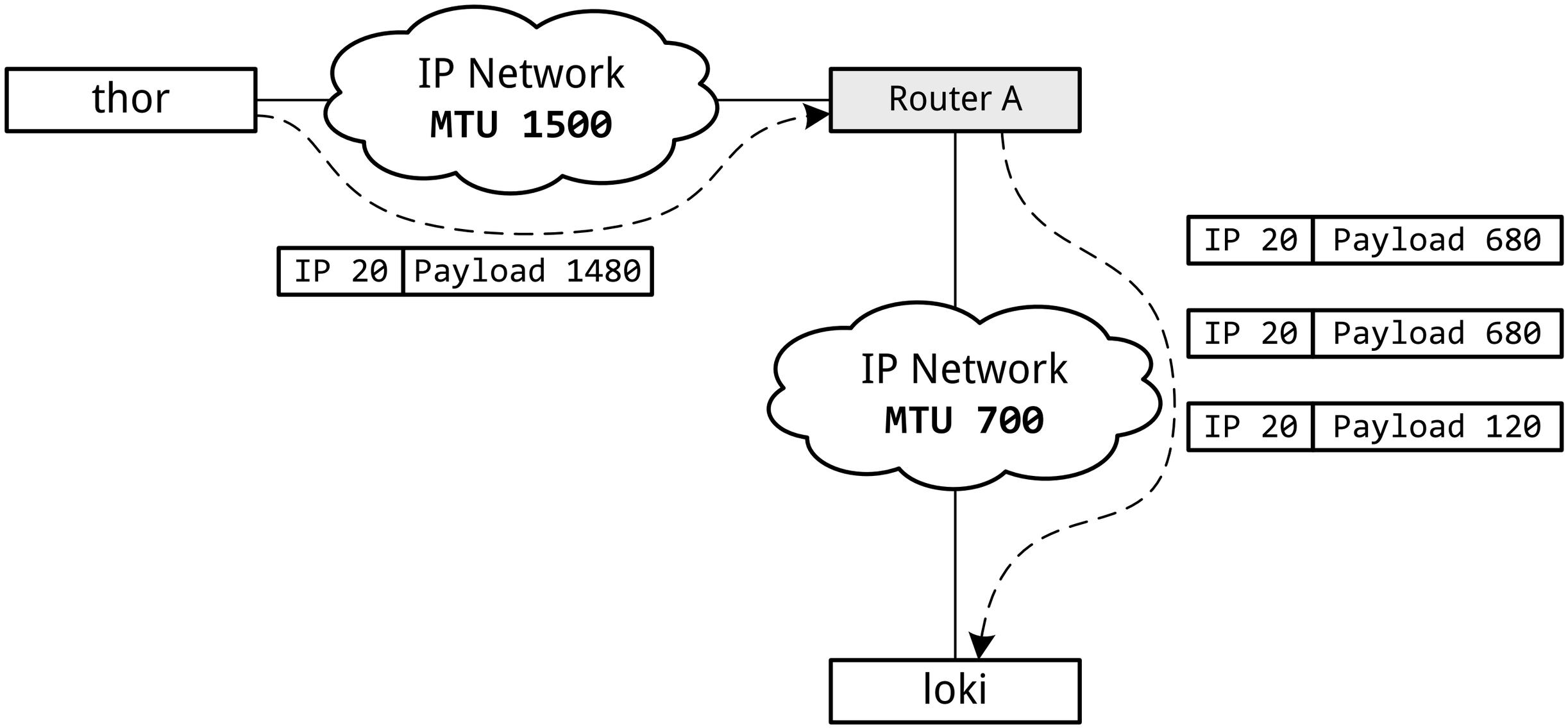
- Пре-дефиниран 3 пъти – виж допълнителния материал
- 6 бита DSCP – приоритет, клас на трафика
- 2 бита ECN flags

Фрагментация

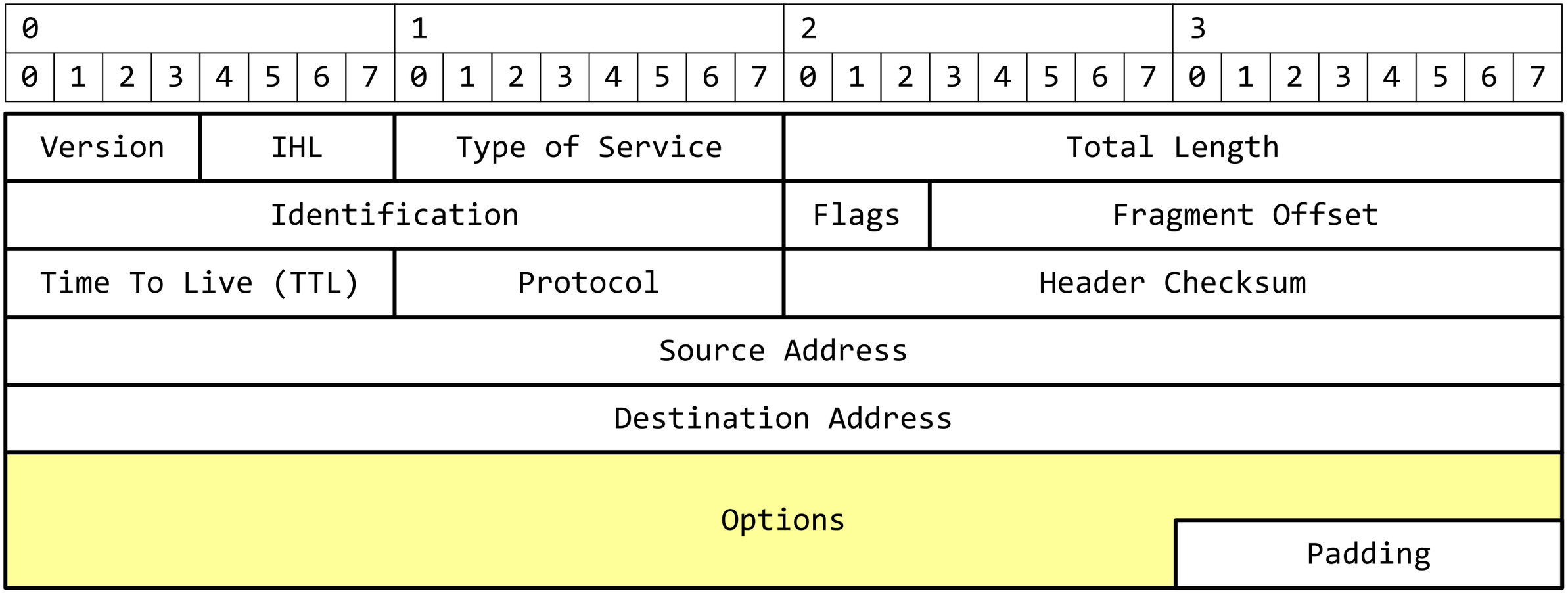


- Identification
- Fragment Offset *8 или <<3
- Don’t Fragment (DF) flag
- More Fragments (MF) flag

Фрагментация



IP Опции


0 1 2 3
0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time To Live (TTL)
Protocol
Header Checksum
Source Address
Destination Address
Options
Padding

IP опции

- Source Routing
  - Strict
  - Loose
- Record route

- Други глупости
  - http://www.iana.org/assignments/ip-parameters

IP features и производителност

- Fast path
  - TTL > 1
  - и no options
  - и no fragmentation needed
- Slow path
  - TTL = 1
  - или Fragmentation needed
    - DF set
    - DF not set
  - или IP options

Въпроси