KOMUNIKAČNÉ A INFORMAČNÉ SIETE

SIEŤOVÁ VRSTVA

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas

OBSAH

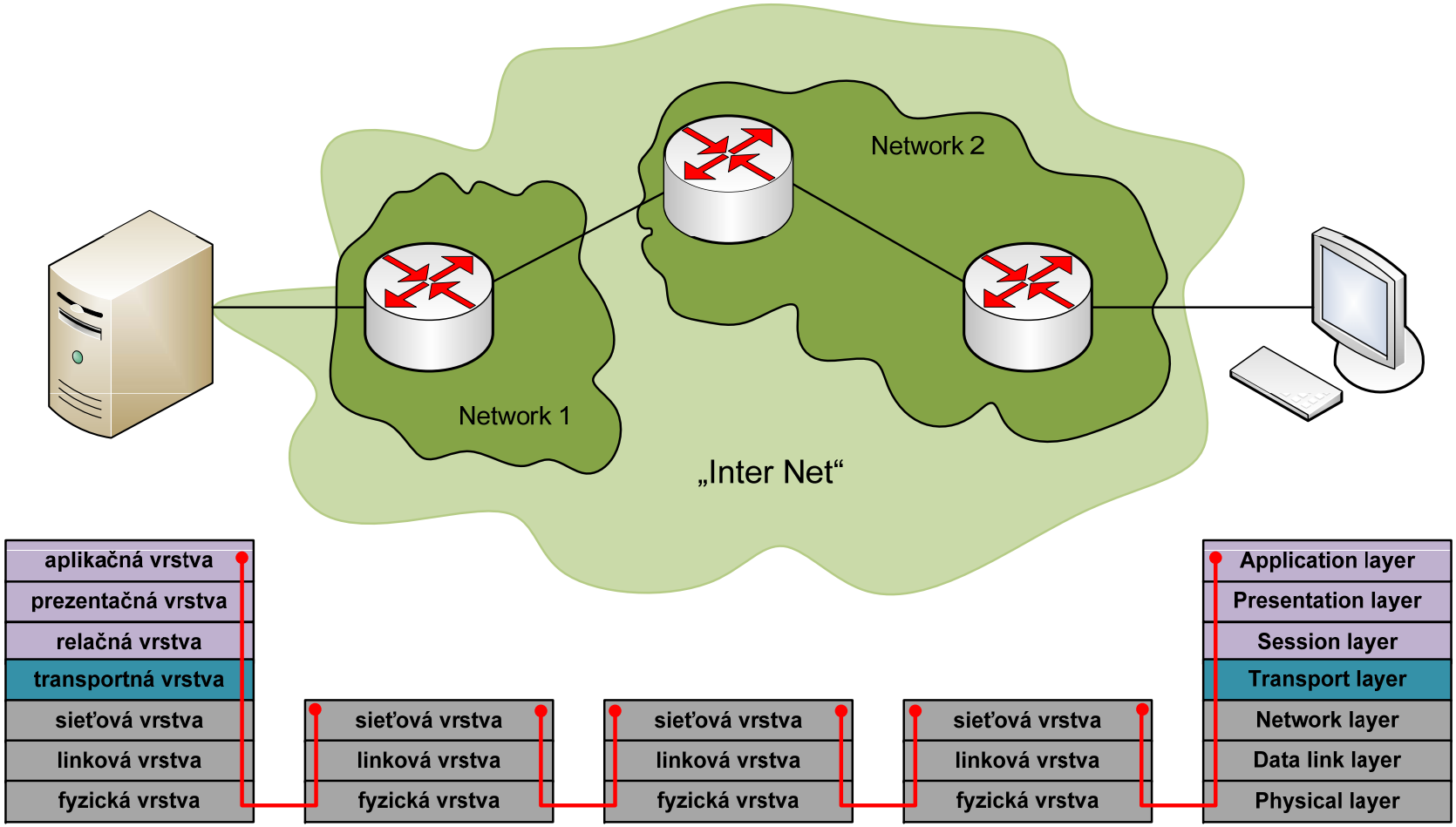
- základné funkcie
- protokoly IP, ARP, RARP, ICMP, IGMP
- IPv4, IPv6, fragmentácia
- adresácia
- Classful addressing, triedy sietí
- Classless addressing

Sieťová vrstva

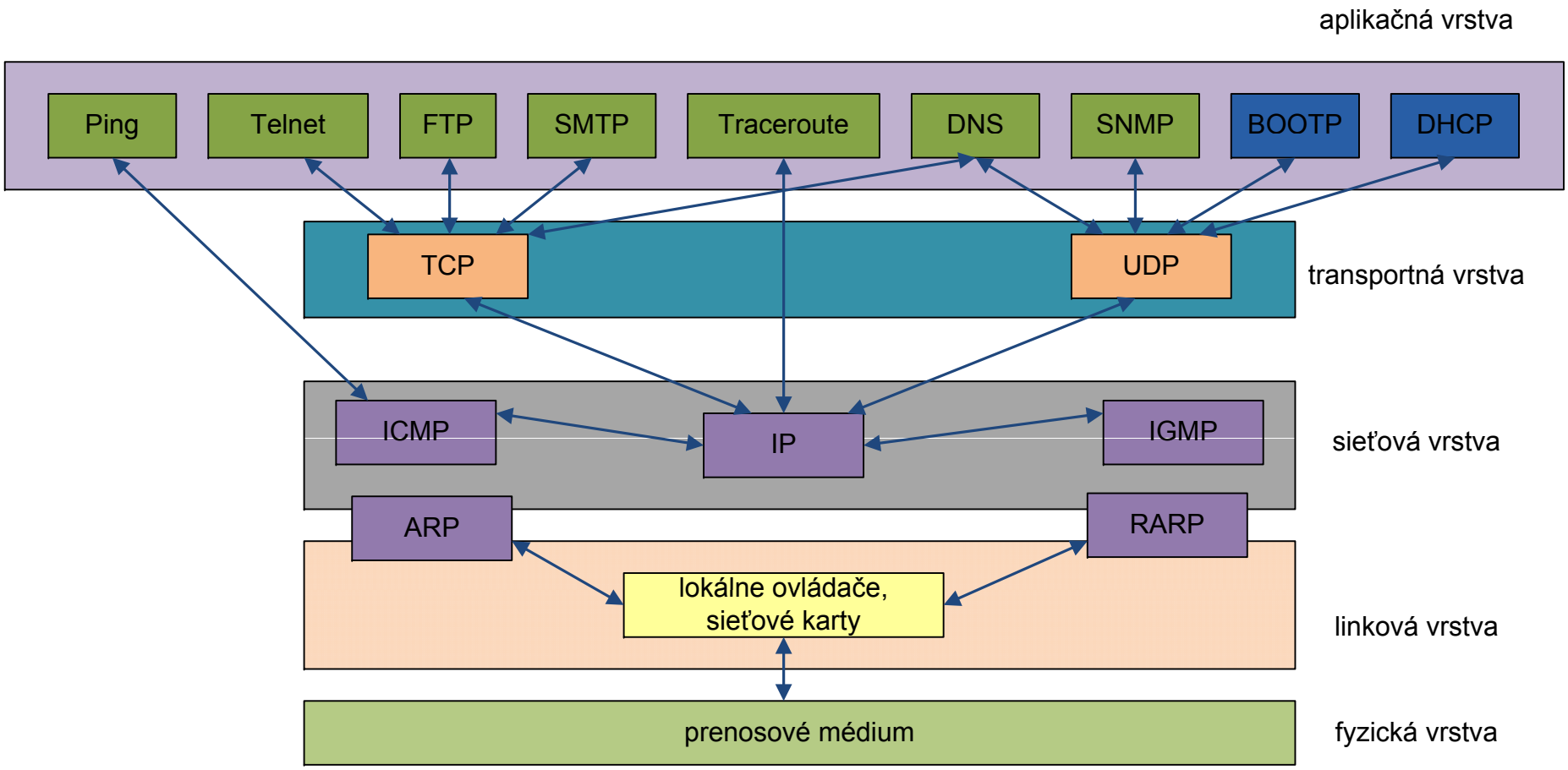
- **3. vrstva RM OSI** zodpovedá **2. vrstve TCP/IP** Internetová vrstva “Internet layer”,
- používa logickú adresu, prenáša pakety,
- úlohy ,
  - prenos paketov konečnému adresátovi,
  - v prostredí, kde nie je priame spojenie hľadá najvhodnejšiu cestu až k cieľu,
  - musí zohľadňovať skutočnú topológiu celej siete,
  - zabezpečuje smerovanie informácií v sieti (routing),
- prenos údajov zabezpečujú smerovače (router).

Sieťová vrstva

- Internet – súbor podsietí (autonómnych systémov)



Protokoly sieťovej vrstvy



Protokoly sieťovej vrstvy

- IP protokol (Internet Protocol)
  - prenos dát sieťou od zdroja k cieľu,
  - prenáša IP pakety (IP PDU),
  - nespoľahlivé nespojovo orientované služby,
    - (bez spojenia, bez potvrdenia)
  - adresovanie,
    - IP adresy (logické adresy)
  - fragmentácia.

Protokoly sieťovej vrstvy

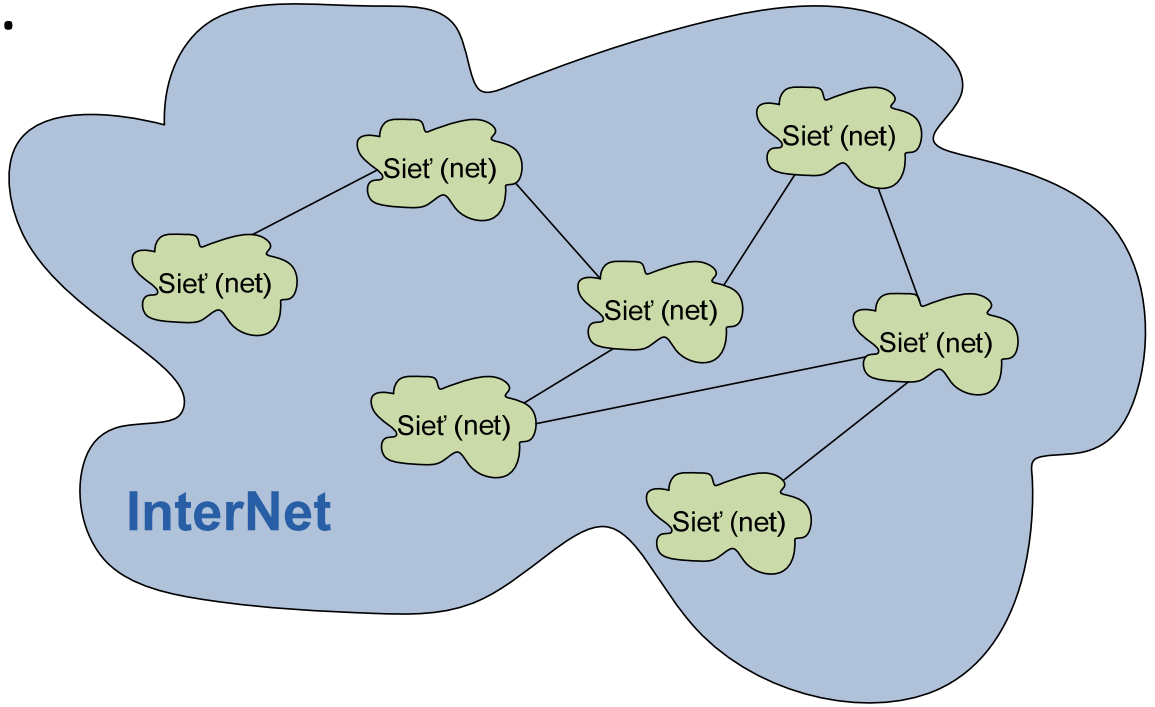
- podporné protokoly,
  - vnorené do IP paketu
- ICMP (Internet Control Message Protocol),
  - prenos chybových a iných riadiacich správ medzi smerovačmi a koncovými uzlami siete,
- IGMP (Internet Group Management Protocol),
  - používaný pre šírenie “multicast” správ smerovačmi a koncovými uzlami.

Protokoly sieťovej vrstvy

- protokoly pre mapovanie adries,
  - (logická adresa ↔ fyzická adresa),
  - IP adresa ↔ MAC adresa,
- ARP (Address Resolution Protocol),
  - IP adresa → MAC adresa,
- RARP (Reverse Address Resolution Protocol),
  - MAC adresa → IP adresa.

IP protokol

- IP – Internet protocol,
- pôvodne InterNet Protocol,
- umožňuje spojiť jednotlivé lokálne siete medzi sebou.



IP protokol

- protokol 3. vrstvy OSI modelu,
- základný protokol TCP/IP modelu,
- prenos dát sieťou od zdroja k cieľu (end-to-end),
- prenáša bloky dát, tzv. IP pakety (IP PDU) niekedy označované aj ako datagramy,
- poskytuje nespoľahlivú datagramovú službu,
  - best effort,
  - neposkytuje ohľadne doručenia paketu takmer žiadne záruky,
  - paket môže prísť poškodený, mimo poradia, duplikovane alebo ho sieť môže úplne zahodiť.

IP protokol

- Adresovanie
  - je najkomplexnejším aspektom IP protokolu,
  - IP adresy (logické adresy),
  - spôsob, akým sú koncovým strojom priraďované IP adresy a ako sú rozdelené a zoskupené podsiete IP adries,
- Smerovanie
  - spôsob, akým je prenášaný paket od zdroja k cieľu,
  - smerovanie vykonávajú smerovače (router),
  - využívajú sa smerovacie tabuľky a smerovacie protokoly,
- Fragmentácia

IP protokol

- Verzie
  - 1, 2, 3 - v dobe vývoja internetových protokolov
  - **IPv4 (RFC 791)**
    - **najrozšírenejší,**
    - **momentálne štandard.**
  - 5 - experimentálny Stream Transport protokol, prenos dát v reálnom čase, neujal sa
  - **IPv6 (RFC 2460)**
    - **nová vylepšená verzia, nástupca IPv4**
  - 7 - pokus o vytvorenie novej generácie protokolov IP, TCP, UDP
  - 8 - nie veľmi prijateľný návrh nástupcu IPv4
  - 9 - pokus Číny o vytvorenie protokolu konkurujúcemu IPv6, hlavný dôvod kontrola údajov

IP protokol

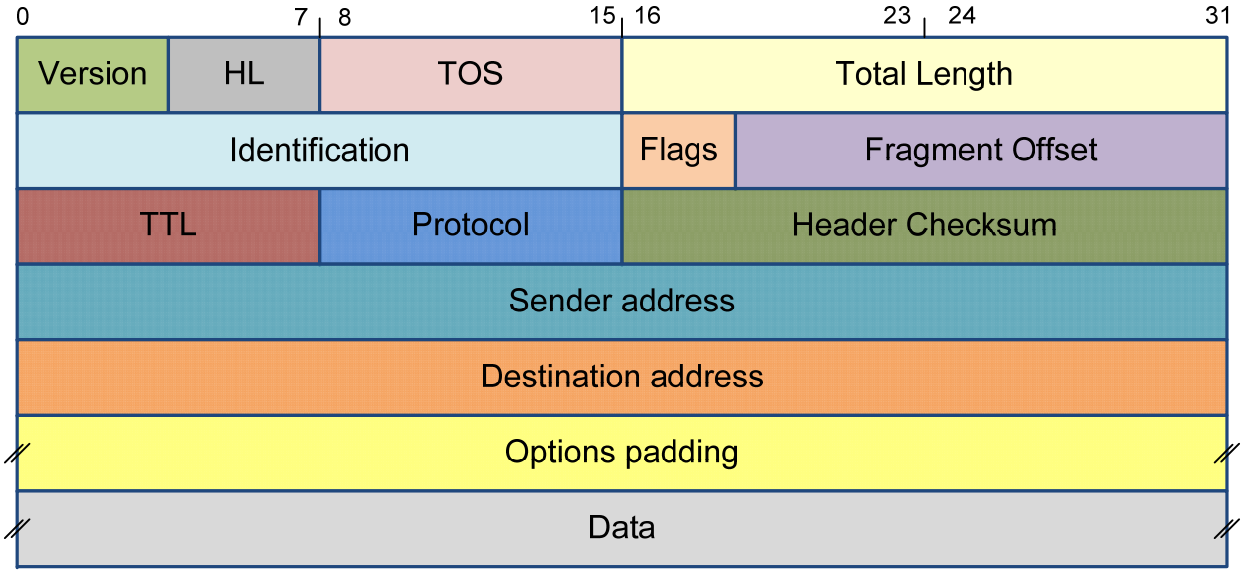
- Verzie
  - IPv4
    - na adresáciu používa 32 bitov
    - dnes najpoužívanejší typ
    - jednotlivé osmice bitov oddeľujeme bodkou
    - príklad: 147.175.103.10/29
  - IPv6
    - na adresáciu používa 128 bitov
    - relatívne nový typ adries
    - zatiaľ málo používané
    - v budúcnosti preferované
    - príklad: 2001:0db8:85a3:0000: 1319:8a2e:0370:7334 /10

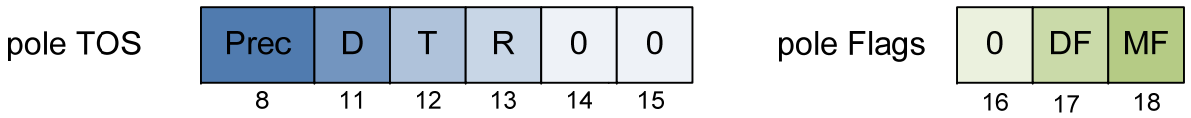
IPv4

- IETF RFC 791, september 1981
- 32-bitové adresy
  - adresný priestor je 4 294 967 296 jedinečných adries,
  - viacero z nich je vyhradených pre zvláštne účely ako lokálne siete alebo multicastové adresy,
  - v dnešnej dobe nedostatočný počet adries použiteľných ako verejné internetové adresy.

IPv4

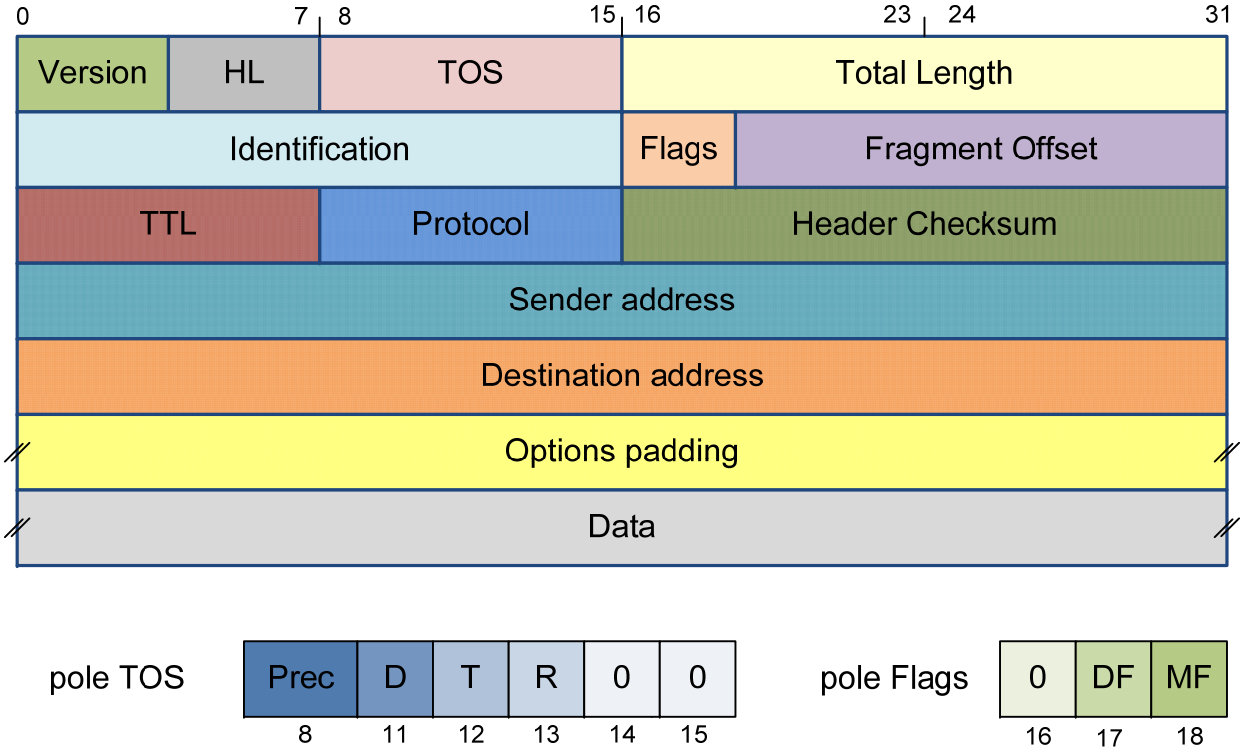
- **Version** (4b) – verzia protokolu = 4
- **HL** (4b) Header Length – dĺžka hlavičky
  - uvádza počet 4B blokov, hodnota 5 → 5x4B → hlavička 20B





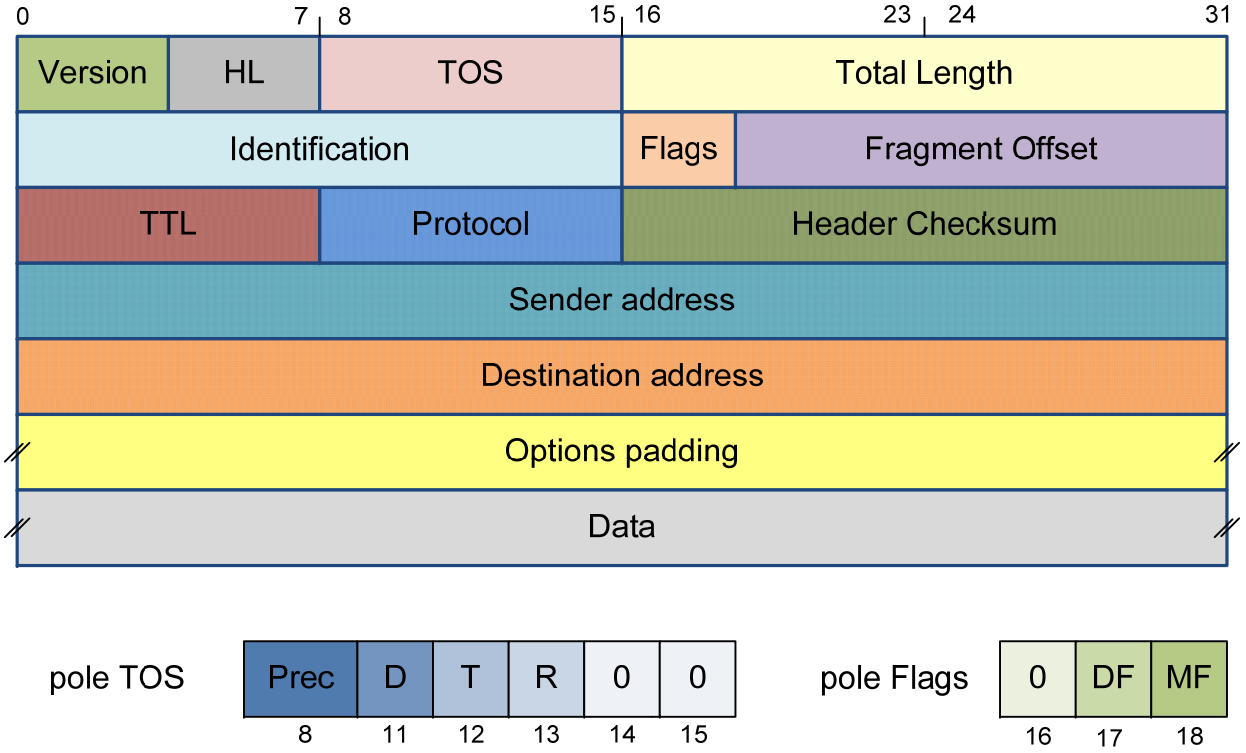
IPv4

- **TOS** (8b) Type of Service – typ služby
  - špecifikácia preferencie prenášaných údajov, napr: nízke zdržanie alebo vysoká spoľahlivosť,
  - dnes využívané pre DiffServ služby.



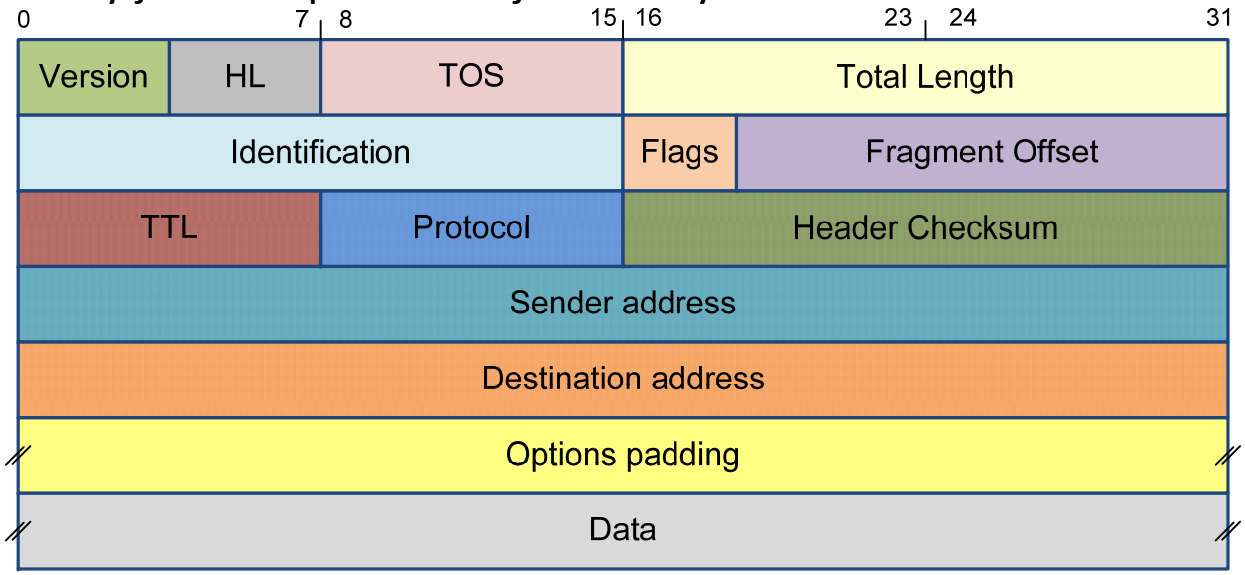
IPv4

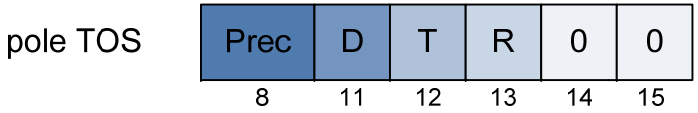
- **Total Length** (16b) – celková dĺžka paketu
  - uvádzaná v B,
  - max. dĺžka IP paketu 65535 B.

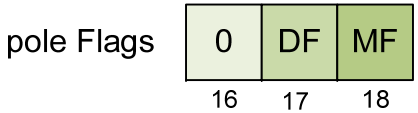


IPv4

- **Identification** (16b) – identifikácia
  - jednoznačná identifikácia paketu, operačný systém vkladá pre každý paket iné číslo,
  - využíva sa pri fragmentácii ,na určenie, ktoré fragmenty patria spolu, všetky fragmenty jedného paketu majú rovnaký identifikátor.

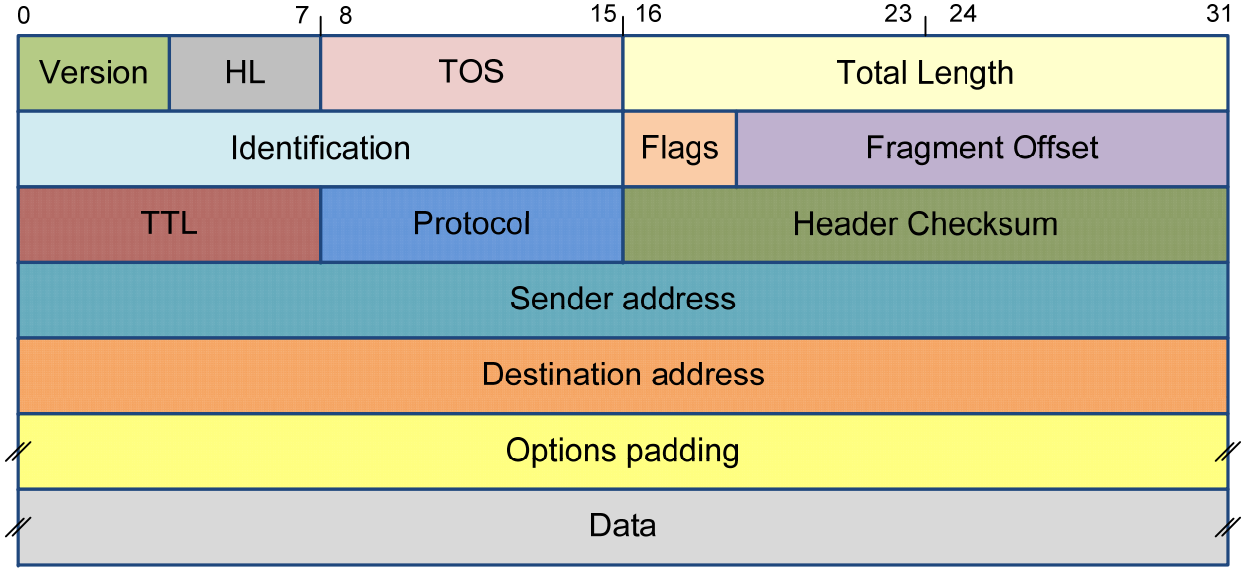


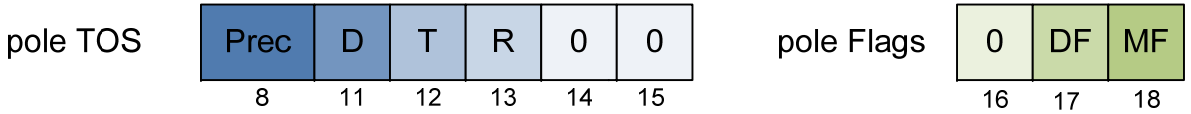




IPv4

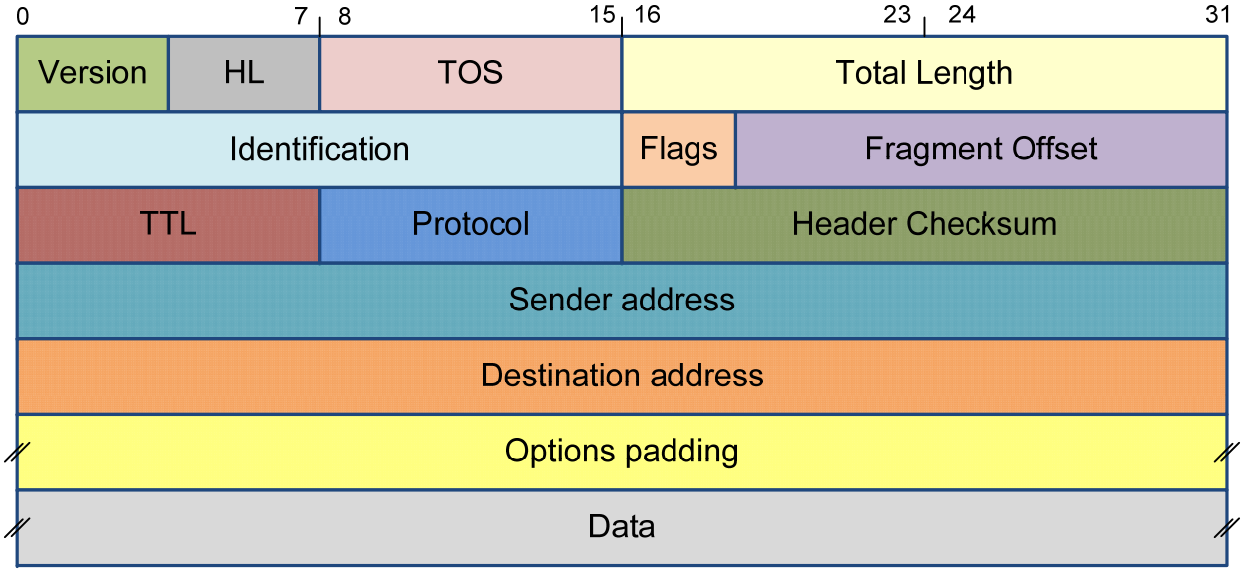
- **Flags** (3b) – príznaky
  - Reserved bit – musí byť 0, určený pre budúce využitie,
  - **DF** Don't Fragment – ak 1, tak je zakázaná fragmentácia paketu,
  - **MF** More fragments – ak 1, tak existuje minimálne jeden ďalší fragment paketu, posledný fragment daného paketu MF = 0.

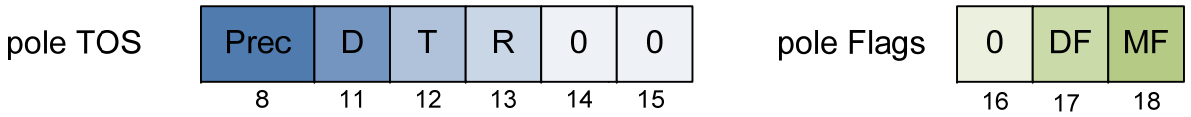




IPv4

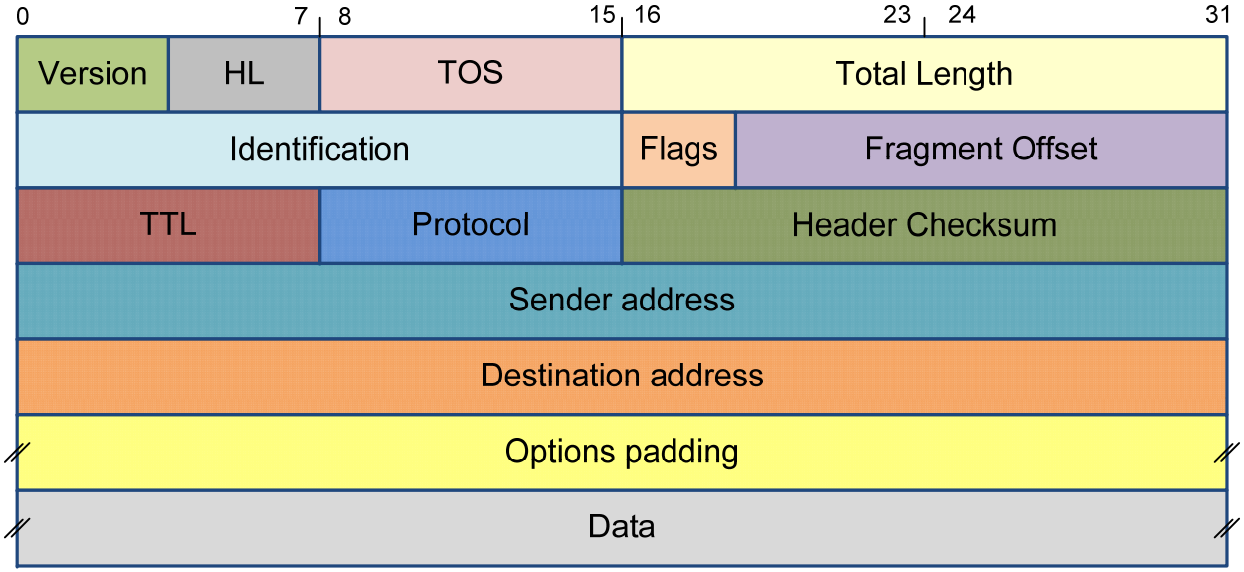
- **Fragment Offset** (13b) – posun fragmentu
  - pozícia fragmentu v pôvodnom pakete,
  - udáva koľko bajtov dátovej časti pôvodného paketu bolo vložených do predchádzajúcich fragmentov.

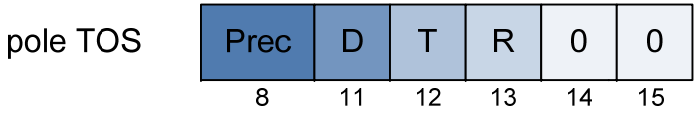


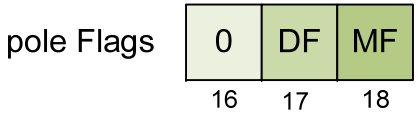


IPv4

- **TTL** (8b) Time to live – doba života paketu
  - slúži na zamedzenie nekonečného túlania sa paketu v sieti,
  - každý smerovač jej hodnotu zmenší min. o 1, východisková hodnota nastavená operačným systémom.

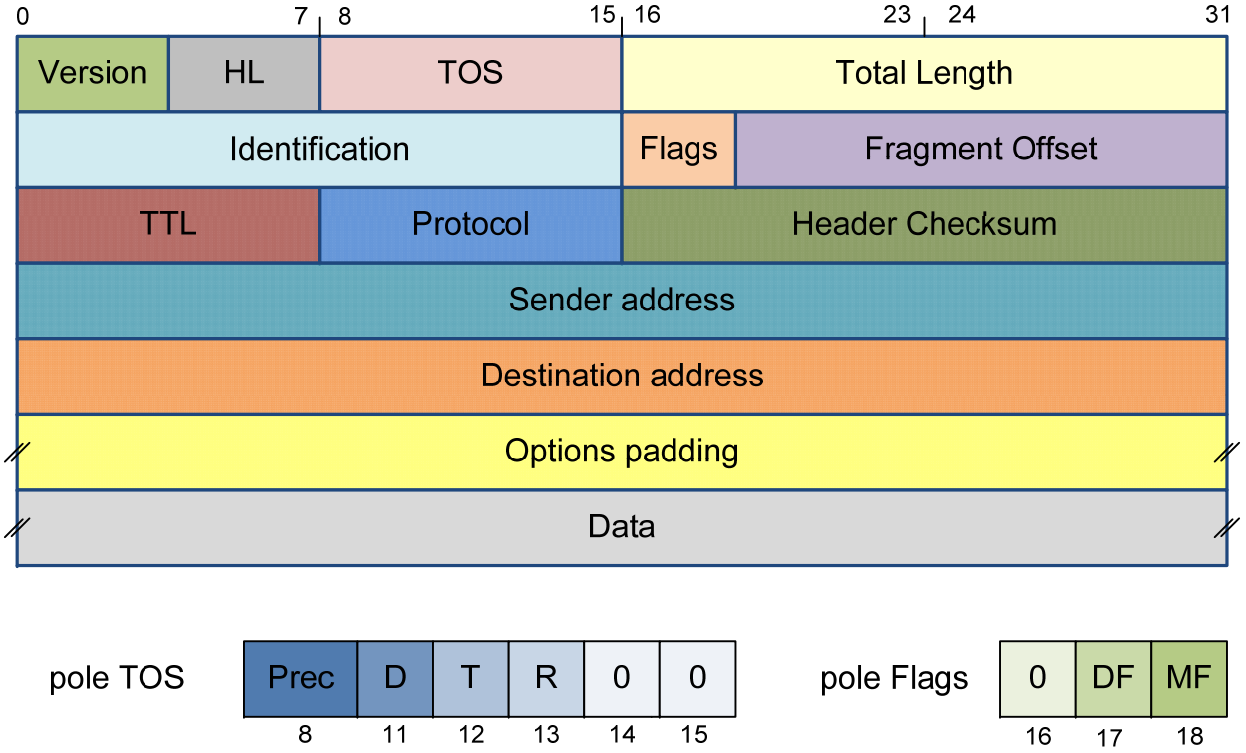






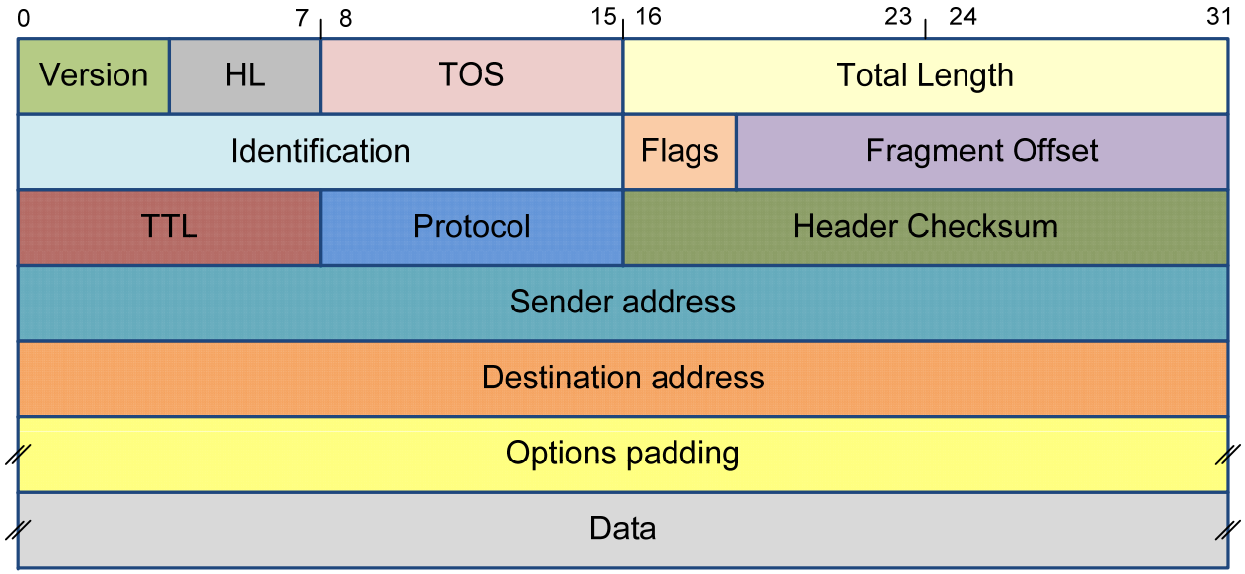
IPv4

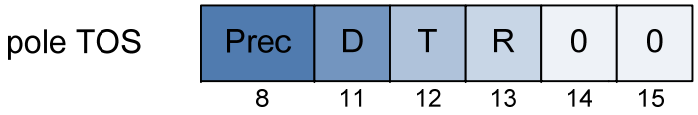
- **Protocol** (8b) – protokol vyššej vrstvy
  - aký protokol vyššej vrstvy je prenášaný, väčšinou TCP (6_{10}) alebo UDP (17_{10})

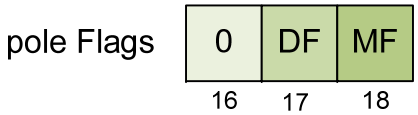


IPv4

- **Header Checksum** (16b) – kontrolný súčet hlavičky
  - podľa RFC-1071 a RFC-1141,
  - nie CRC, každý smerovač mení hlavičku a tým aj kontrolný súčet

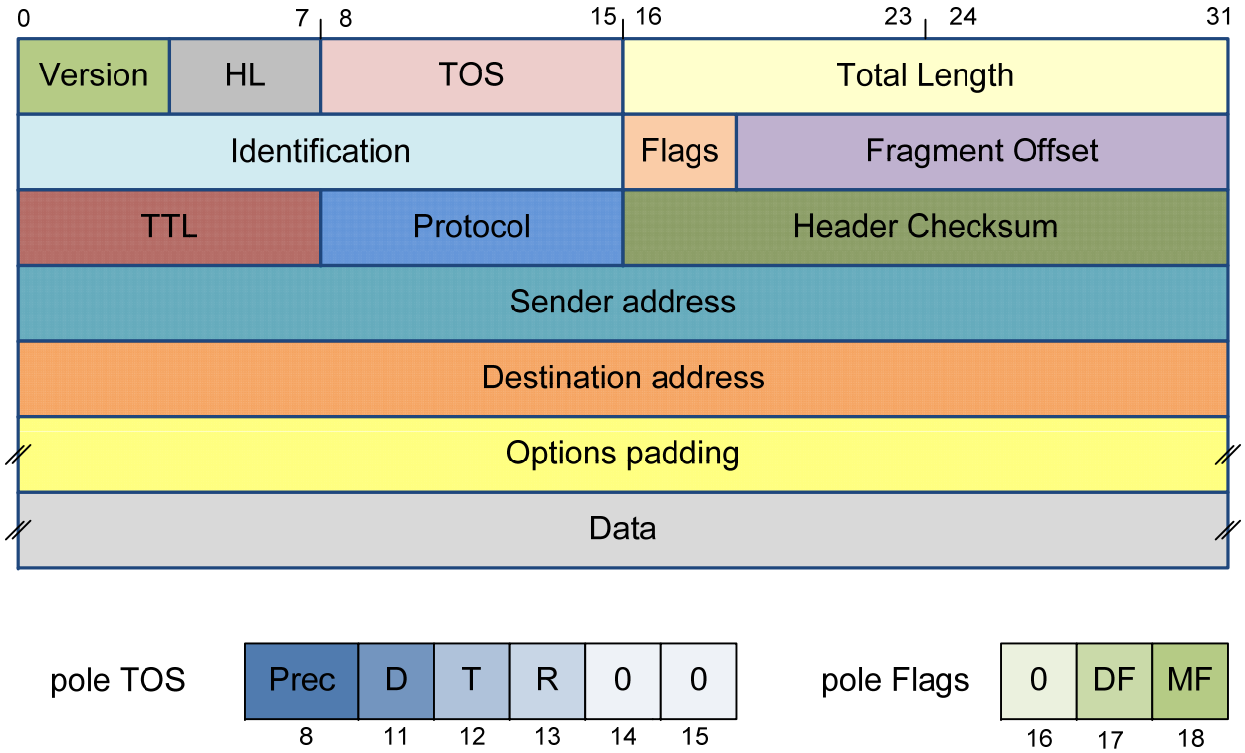






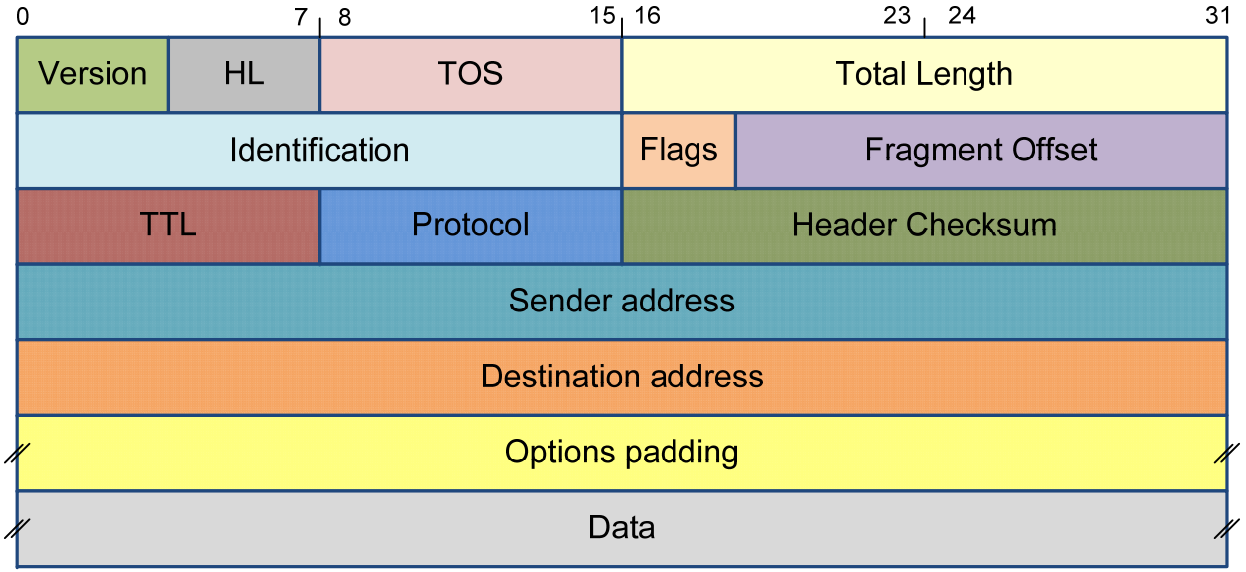
IPv4

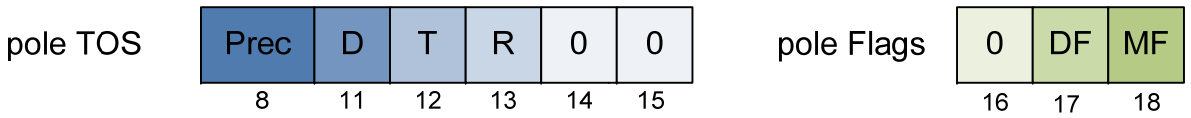
- **Sender address** (32b) – IP adresa odosielateľa
- **Destination address** (32b) – IP adresa prijímateľa



IPv4

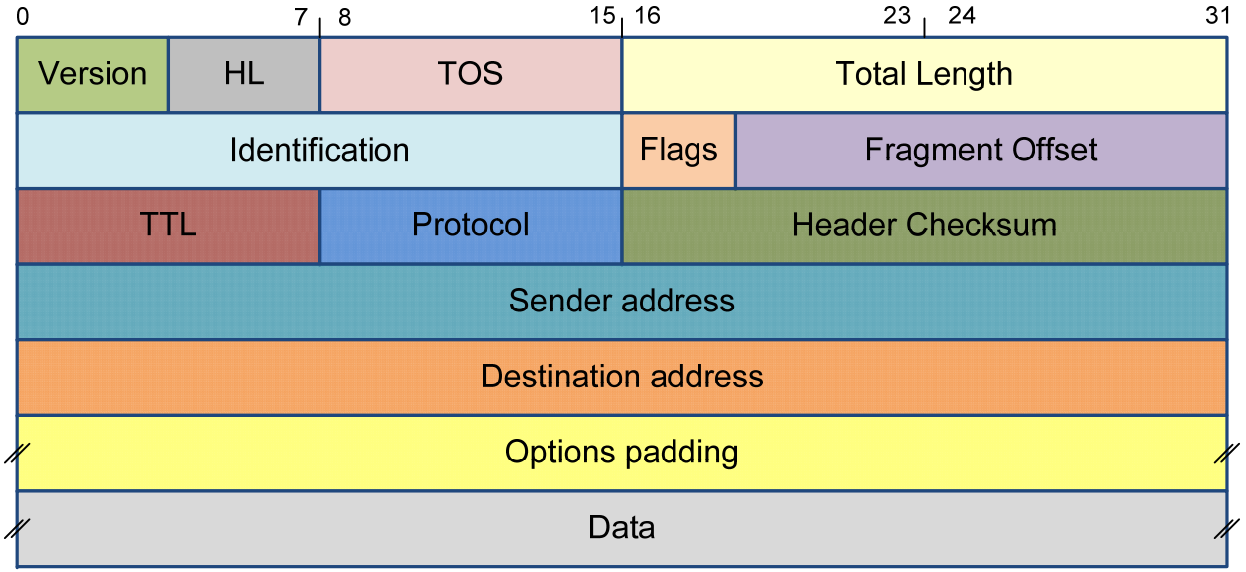
- **Options + padding** (max 320b) – voliteľné položky
  - veľkosť v násobkoch 32b,
  - record route, timestamp, loose source routing, strict source routing, IP Router Alert Option.

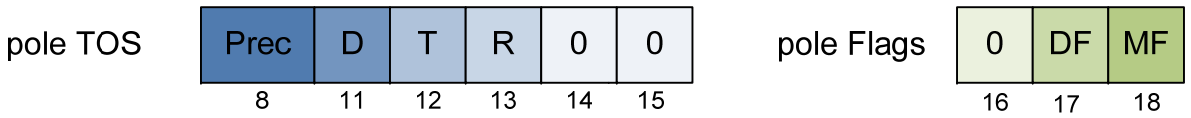




IPv4

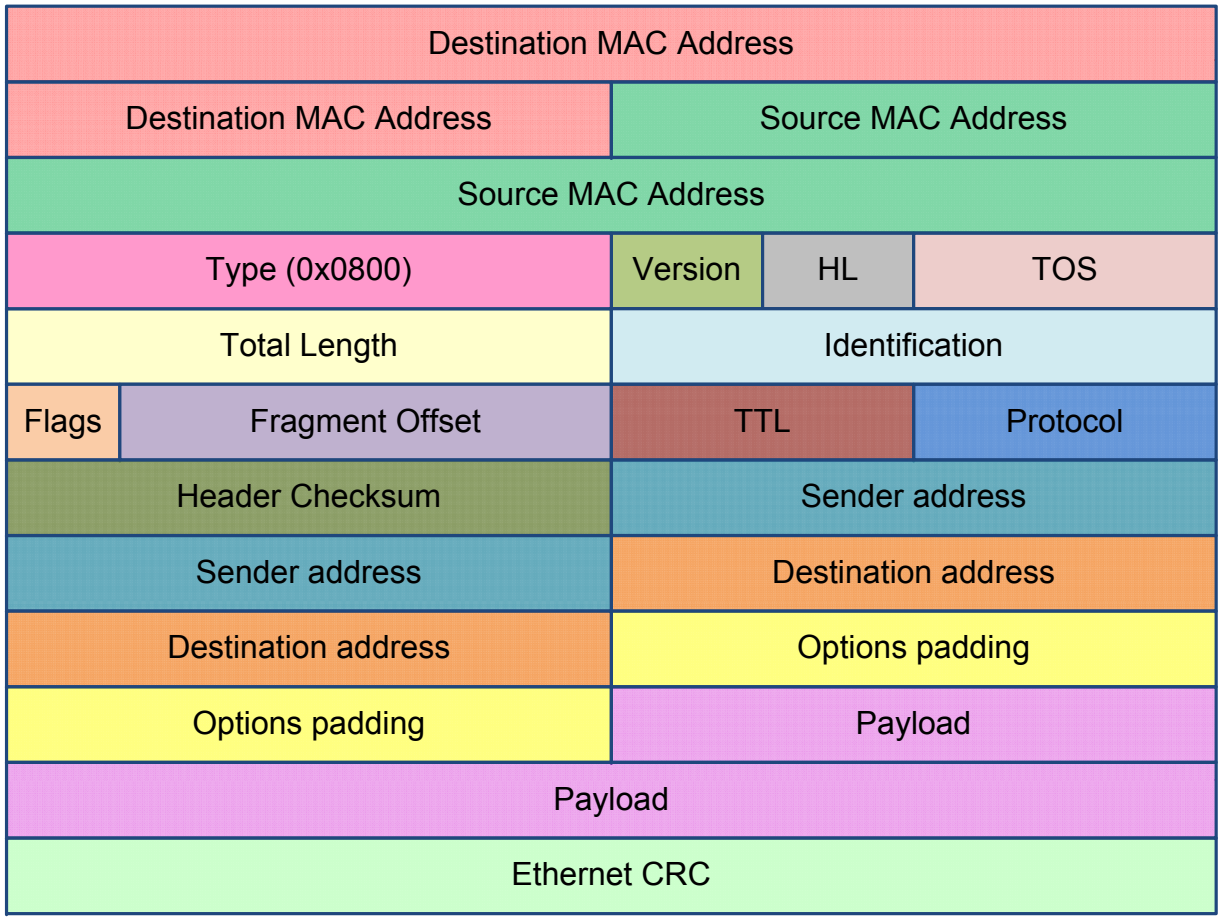
- **Data** – dáta protokolov vyšších vrstiev
  - v násobkoch 8b, maximálne tak, aby hlavička + dáta = 65535B





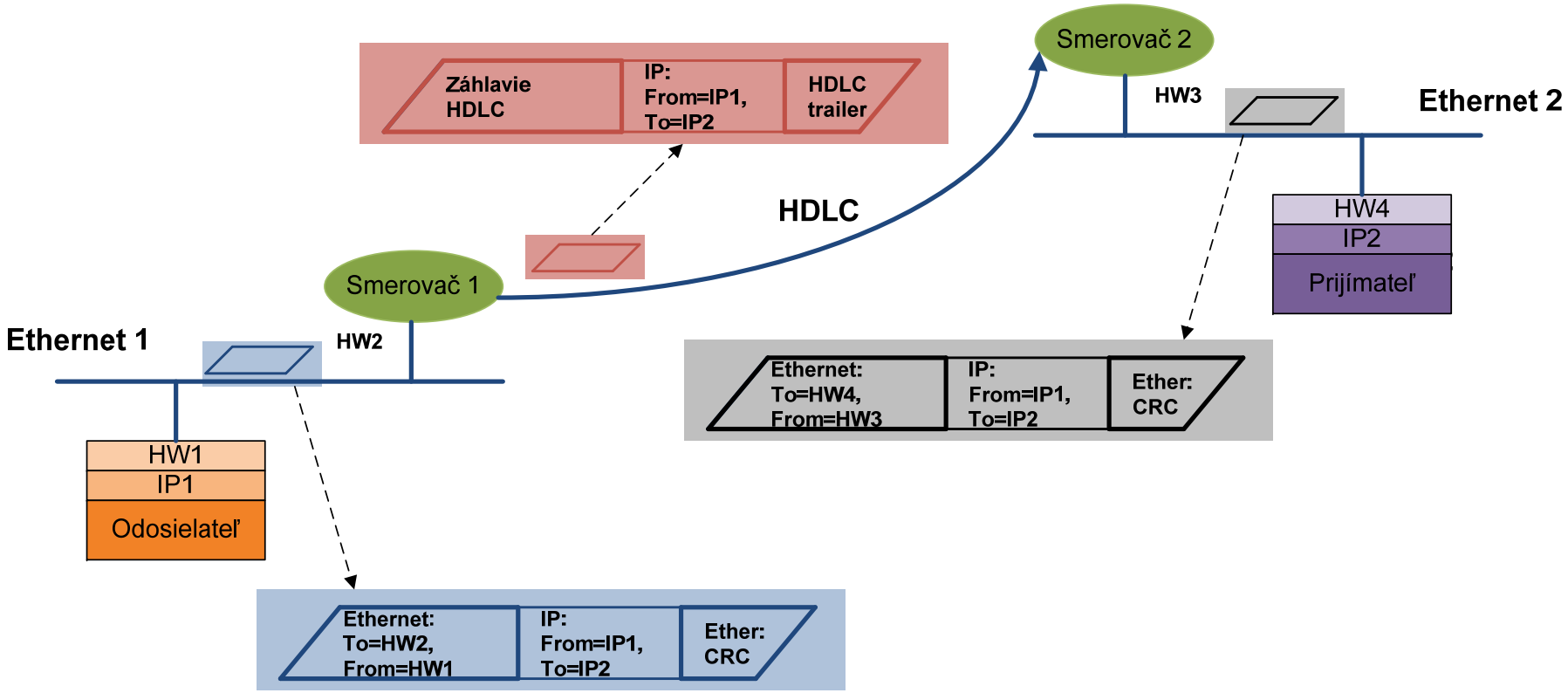
IPv4

- Zapúzdrenie IP paketu do Ethernet rámca



IPv4

- Zapúzdrenie IP protokolu do rámcov linkovej vrstvy pre prenos sieťou



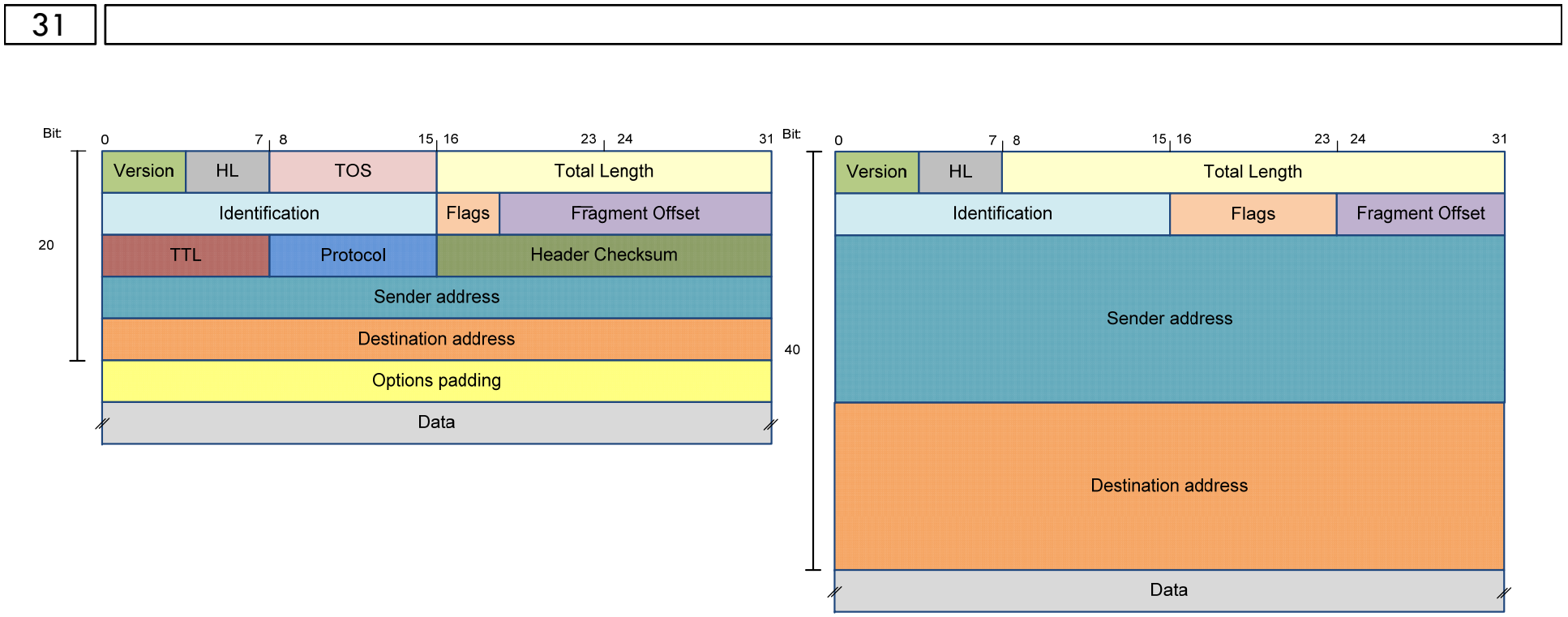
IPv6

- možnosť spolupráce s IPv4,
- rozšírenie adresného priestoru,
- podpora QoS mechanizmov,
- zmenšenie smerovacích tabuliek,
- zjednodušenie štruktúry protokolu,
- zrýchlenie spracovania paketov smerovačmi,
- zlepšenie bezpečnosti,
- podpora multicastingu.

IPv6

- nekompatibilný s IPv4
  - možná spolupráca využitím tunelovacích mechanizmov,
  - kompatibilný s protokolmi vyšších vrstiev TCP, UDP, BGP, DNS, ICMP, IGMP ...,
- adresa 16B (IPv4 4B)
  - 3.4×10^{38} adries,
  - jednotlivé šestnástice bitov oddeľujeme „:“,
  - 2001:0db8:85a3:0000:1319:8a2e:0370:7334,
  - 2001:0db8:85a3::1319:8a2e:0370:7344,
- jednoduchšia hlavička 7 polí (IPv4 13 polí),
- fixná veľkosť hlavičky 40B (IPv4 20B-60B).

IPv6


31
Bit:
0
7
8
15
16
23
24
31
20
Version
HL
TOS
Total Length
Identification
Flags
Fragment Offset
TTL
Protocol
Header Checksum
Sender address
Destination address
Options padding
Data
Bit:
0
7
8
15
16
23
24
31
40
Version
HL
Total Length
Identification
Flags
Fragment Offset
Sender address
Destination address
Data

Fragmentácia

- Paket pri prechode sieťou je fragmentovaný na linkovej vrstve v závislosti od MTU použitej prenosovej technológie, vždy je však na konci každej prenosovej linky zostavený do pôvodného stavu.
- Fragmentácia môže nastať aj na 3. vrstve, kedy paket fragmentuje odosielateľ a znovu je zostavený do pôvodného stavu až v prijímači.
- Pre každý fragment 3. vrstvy je potrebné vytvoriť osobitnú IP hlavičku a je smerovaný sieťou nezávisle od ostatných fragmentov.

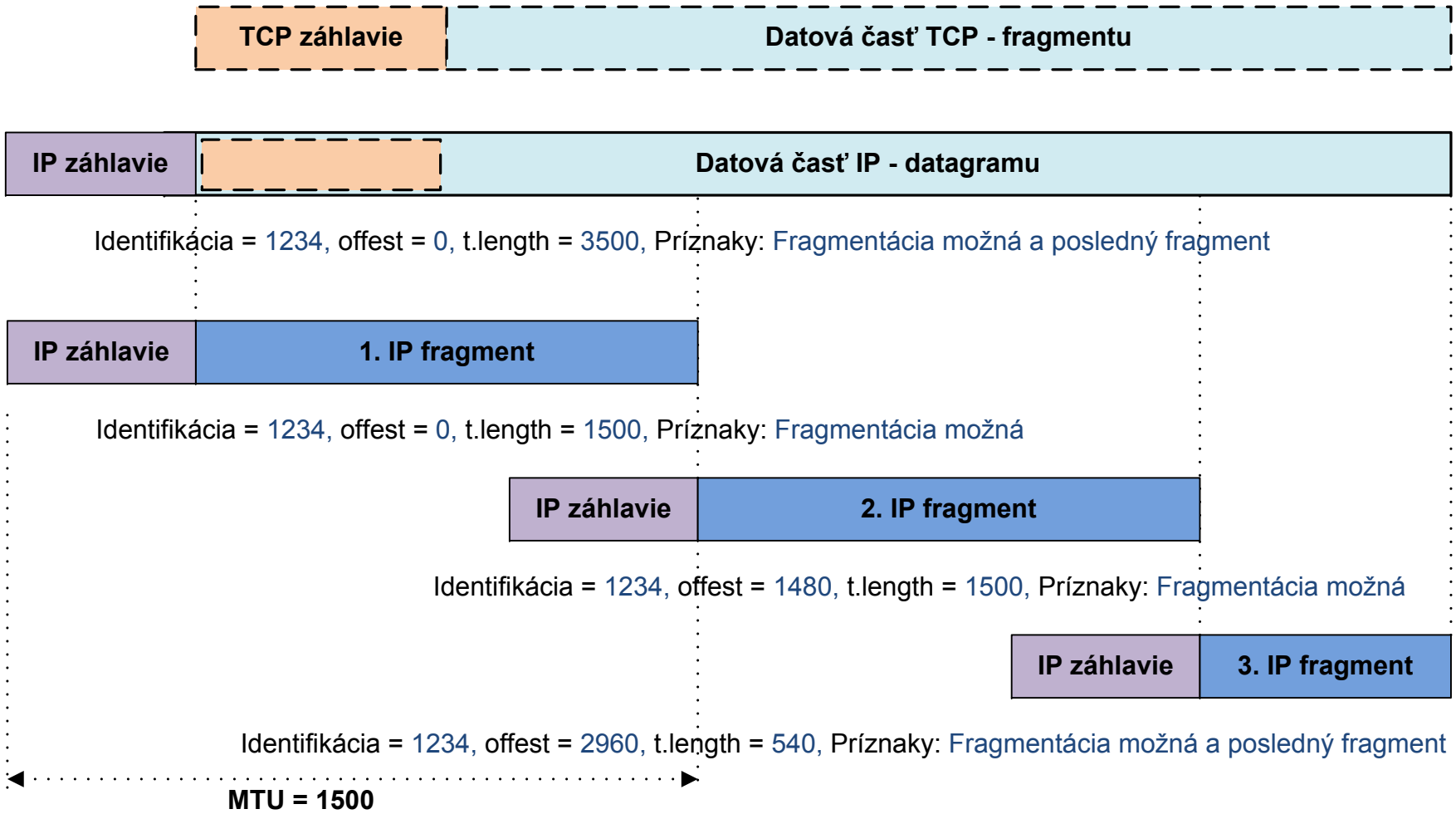
Fragmentácia

- Obmedzenie fragmentácie je možné nastaviť pomocou flagu DF v hlavičke IP paketu.
- V prípade, že je paket fragmentovaný, všetky jeho fragmenty okrem posledného, majú flag MF=1, posledný fragment má MF=0.
- Každý IP paket má v hlavičke svoju identifikáciu v poli „identification“, každý jeho fragment ju bude mať rovnakú.

Fragmentácia

- Jednoznačnú pozíciu fragmentu v pôvodnom pakete určuje pole „fragment offset“, ktorý udáva, koľko bajtov dátovej časti pôvodného paketu bolo vložených do predchádzajúcich fragmentov.
- Pole „total length“ vždy udáva dĺžku fragmentu, nie pôvodného fragmentovaného paketu.

Fragmentácia



ICMP

- Internet Control Message Protocol,
- služobný protokol IP sietí určený na signalizáciu rôznorodých stavov siete,
- dátové pakety ICMP protokolu sú zapuzdrené v IP paketoch,
- často nie je implementovaná celá množina podporovaných správ,
- mnoho krát sú ICMP správy z dôvodu bezpečnosti zahadzované smerovačmi.

ICMP

Bity	0 - 7	8 - 15	16 - 23	24 - 31
0	Type	Code	Checksum	
32	ID		Sequence	

- **Type** (8b) – typ
  - základný typ správy
- **Code** (8b) – kód
  - presnejšie označenie typu správy
- **Checksum** (16b) – kontrolný súčet
  - kontrolný súčet hlavička + dáta
- **Data** (32b) – dáta
  - doplňujúce dáta, ich štruktúra a význam závisí od typu správ

ICMP

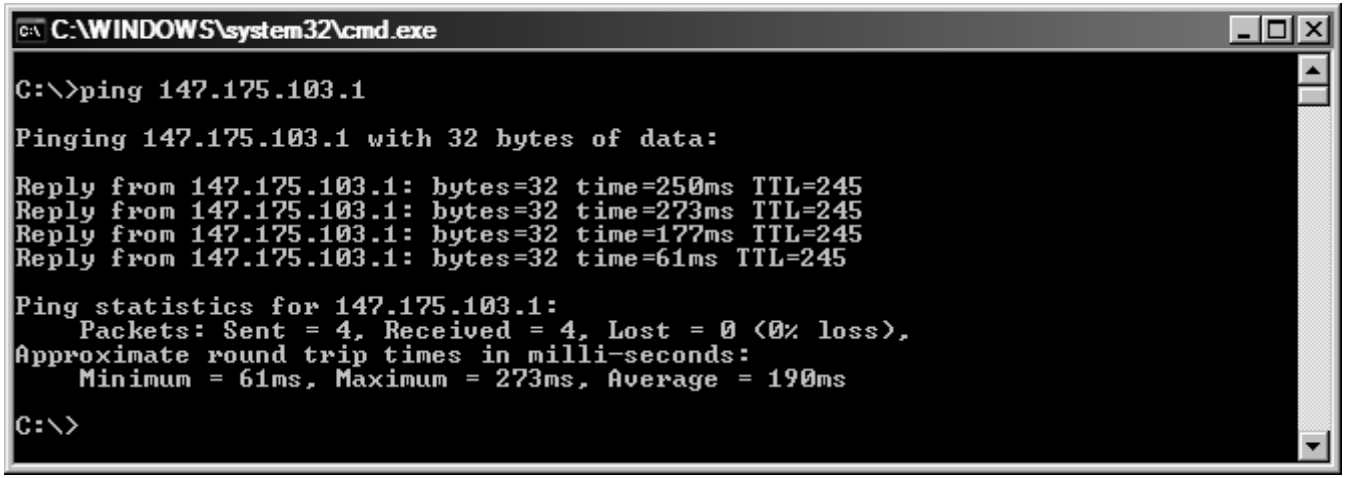
- Základné typy správ:
  - 0 – Echo
  - 3 – Nedoručený IP paket
    - Nedosiahnuteľná sieť/uzol/protokol/UDP port, zakázaná fragmentácia, explicitné smerovanie zlyhalo, cieľová sieť neznáma, ...
  - 4 – Zníž rýchlosť vysielania
  - 5 – Zmeň smerovanie
    - Zmeň smerovanie pre sieť/uzol/sieť a daný typ služby/uzol a daný typ služby
  - 8 – Žiadosť o echo
  - 9 – Odpoveď na žiadosť o smerovaní

ICMP

- základné typy správ
  - 10 – Žiadosť o smerovanie
  - 11 – Vypršal čas
    - vypršal čas počas transportu TTL, vypršal čas na zostavenie paketu z jeho fragmentov
  - 12 – Chybný parameter
    - chybná IP hlavička, chýba voliteľný parameter
  - 13 – Požiadavka na časovú synchronizáciu
  - 14 – Odpoveď na časovú synchronizáciu
  - 15 – Žiadosť o masku podsiete
  - 16 – Odpoveď na žiadosť o masku

ICMP

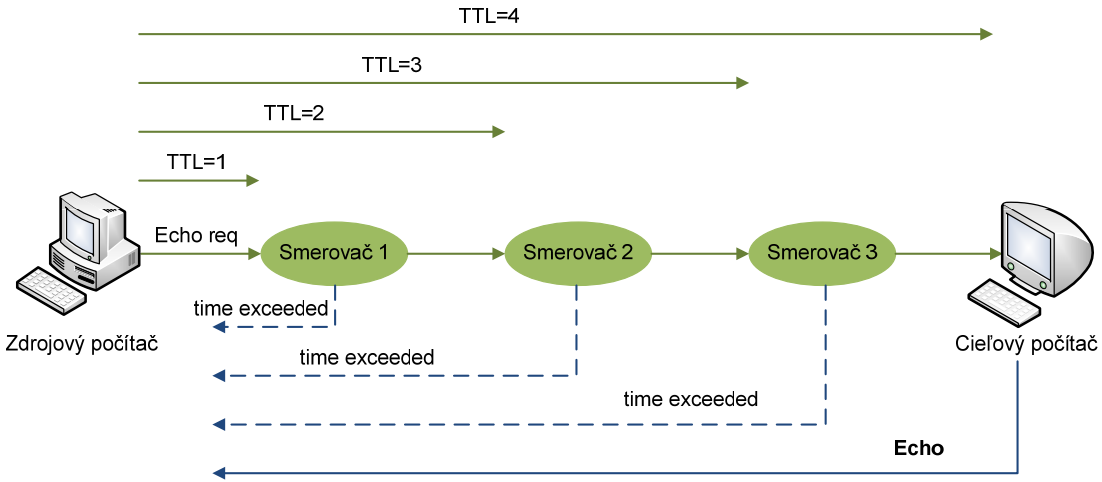
- Echo
  - slúži sa na zistenie dostupnosti uzla v sieti
  - Žiadateľ vysiela ICMP správu „Žiadosť o echo – Echo request“
  - pri prijatí ICMP paketu cieľový uzol musí odpovedať správou „Echo“ s rovnakým identifikátorom aký bol použitý v žiadosti
  - využíva sa pri príkaze **ping**



ICMP

- Čas vypršal – Time exceeded
  - využíva sa príkazom **tracert** na zistenie IP adries jednotlivých smerovačov na ceste k cieľovému uzlu,
  - vysiela ICMP pakety “Echo request” postupne s TTL=1,2,3,4…..,
  - čas života paketu s TTL=1 vyprší na prvom smerovači, ten automaticky odpovedá ICMP správou „čas vypršal“, podobne na paket s TTL=2 odpovie druhý smerovač, atď.

ICMP




```
C:\WINDOWS\system32\cmd.exe
C:\>tracert 147.175.103.1

Tracing route to owl.ktl.elf.stuba.sk [147.175.103.1]
over a maximum of 30 hops:

  1    48 ms    <1 ms    <1 ms  my.router [192.168.1.1]
  2     1 ms     1 ms     1 ms  172.30.30.128
  3    72 ms    42 ms    52 ms  192.168.64.130
  4     *        *        *     Request timed out.
  5    86 ms    41 ms    39 ms  rev-195-91-54-142.t-mobile.sk [195.91.54.142]
  6    56 ms    57 ms   106 ms  rev-195-91-54-142.t-mobile.sk [195.91.54.142]
  7    56 ms    58 ms    63 ms  rev-195-91-54-141.t-mobile.sk [195.91.54.141]
  8   118 ms    40 ms    38 ms  194.154.236.35
  9    35 ms    39 ms    38 ms  194.154.236.42
 10    51 ms    62 ms    55 ms  Sanet-gw.six.sk [192.108.148.10]
 11    51 ms    59 ms   106 ms  FEI-Bratislava.sanet2.sk [194.160.8.130]
 12    59 ms    38 ms    53 ms  193.87.2.20
 13    44 ms    53 ms    95 ms  owl.ktl.elf.stuba.sk [147.175.103.1]

Trace complete.

C:\>
```

IGMP

- Internet Group Management Protocol:
- služobný protokol, slúži na šírenie adresných obežníkov – multicast v LAN sieťach,
- viacero verzií:
  - IGMP v1 RFC 1112,
  - IGMP v2 RFC 2236,
  - IGMP v3 RFC 3376,
- najčastejšie je používaná verzia 2,
- IGMP paket má vždy nastavený TTL=1.

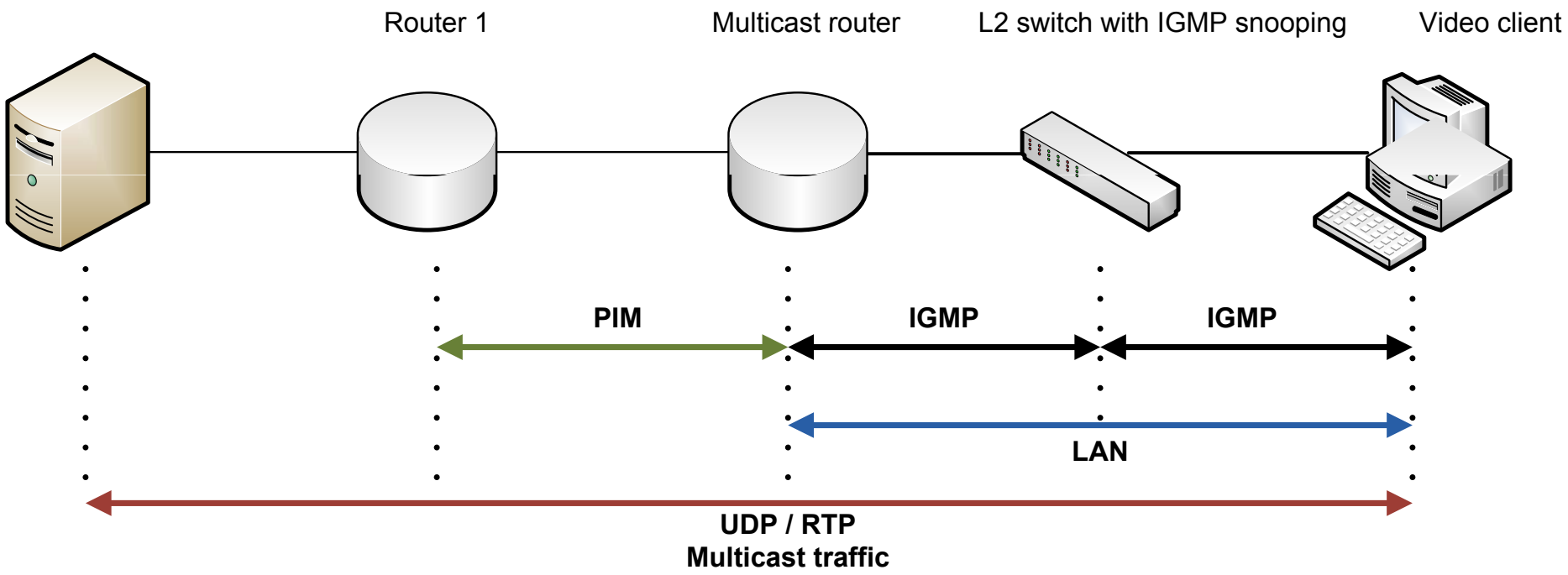
IGMP

Bity	0 - 7	8 - 15	16 - 23	24 - 31
0	Type	MRT	Checksum	
32	Group Address			

- **Type** (8b) – typ
  - typ správy
- **MRT** Maximum response time (8b) – Maximálny čas odpovede,
  - časový interval, v ktorom musia členovia multicast skupiny opakovať svoju požiadavku na členstvo v skupine.
- **Checksum** (16b) – kontrolný súčet
- **Group address** (32b) – IP adresa multicast skupiny

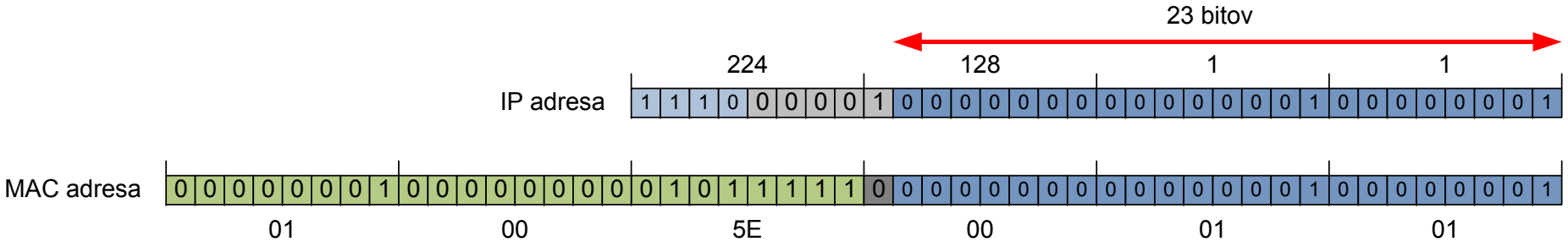
IGMP

- IGMP použiteľné len v broadcast LAN sieťach



IGMP

- transformácia IP multicast adresy (trieda D) na MAC adresu,
- IANA – fiktívny výrobca kariet 00:00:5E,
- nie jednoznačný proces mapovania multicast IP adresy na multicast MAC adresu,
- IP adresy 224.0.1.1, 224.128.1.1 a 225.0.1.1 sa budú mapovať na 01:00:5E:00:01:01,
- nadbytočné multicast obežníky musí odfiltrovať sieťová vrstva.



Identifikácia zariadení

- Komunikačné zariadenie pracujúce na sieťovej vrstve má dvojitú identifikáciu.
- Dva typy adries:
  - Fyzická adresa linkovej vrstvy = MAC adresa
  - Logická adresa sieťovej vrstvy = IP adresa
- Fyzická adresa
  - jednoznačný identifikátor každého sieťového zariadenia,
  - jedinečná a unikátna, daná pri výrobe a napálená do sieťovej karty,
  - jedno sieťové rozhranie môže mať len jednu MAC adresu,
  - MAC adreasa 6B napr: 00:90:96:1F:D3:FC.

Identifikácia zariadení

- Logická adresa
  - môže sa meniť v závislosti na tom, ako sa mení sieť v ktorej sa zariadenia nachádza,
  - každé zariadenia pracujúce na 3. vrstve, je identifikované svojou IP adresou,
  - jedno sieťové rozhranie môže mať viacero IP adries,
  - adresa je prideľovaná administratívne,
  - IP adresa IPv4 4B napr: 147.175.103.1.

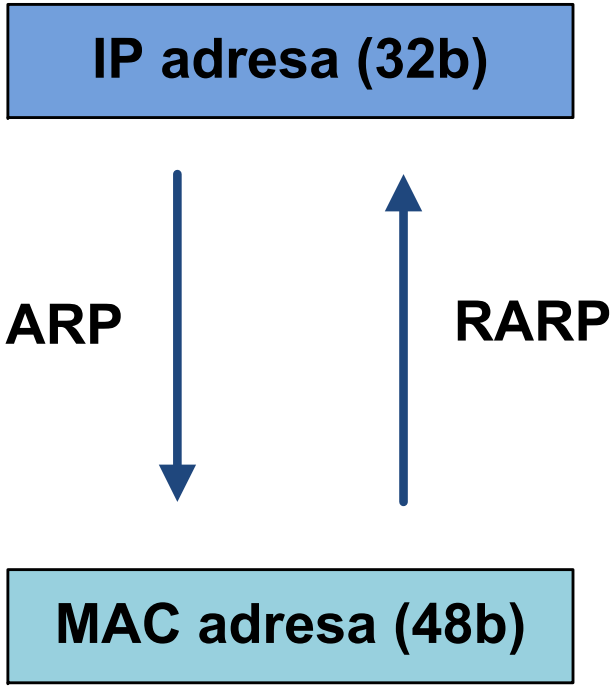
Identifikácia zariadení

- Prideľovanie IP adries celosvetovo zabezpečujú sieťové autority a správcovia sietí:
  - Európa: RIPE (Résean IP Européenee),
  - Amerika: ARIN (American Registry for Internet Numbers),
  - Ázia: APNIC (Asia Pacific Network Information Center).

  - **Slovensko: SK-NIC**

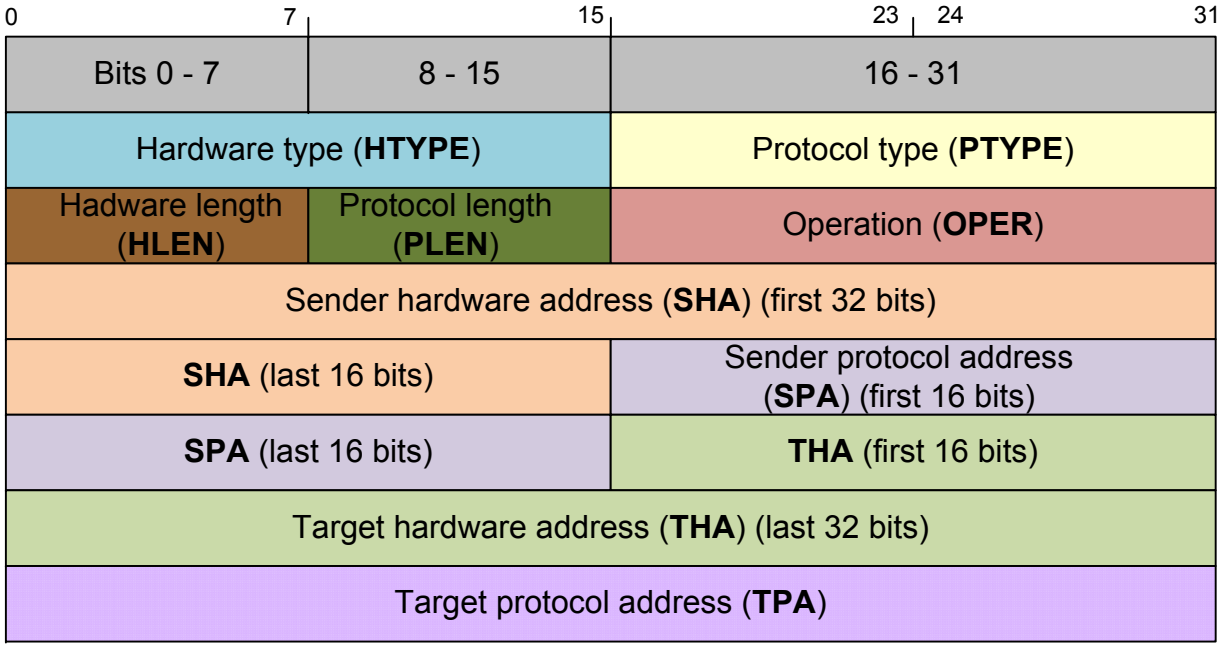
ARP

- Address Resolution Protocol:
- RFC 826,
- slúži na zistenie MAC adresy na základe známej IP adresy,
- vnorenie: ARP → Ethernet,
- využíva broadcast,
- zdrojový a cieľový uzol v tej istej boadcast doméne alebo je potrebné využiť ARP proxy.



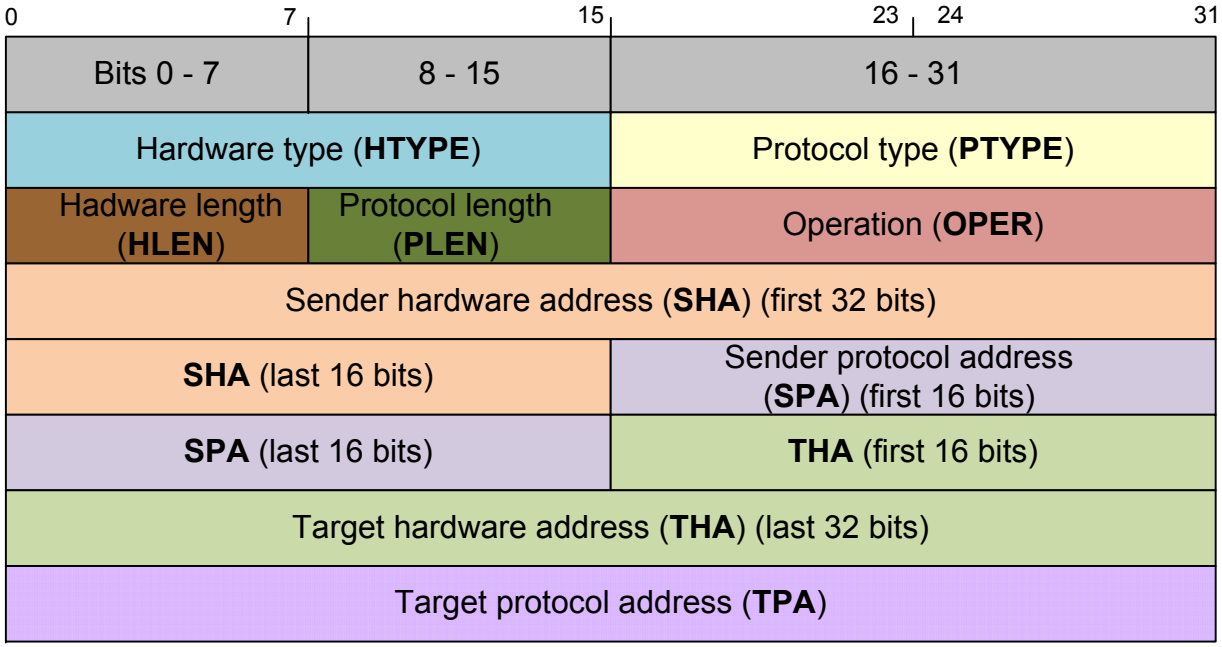
ARP

- **HTYPE** (16b) Hardware type – typ linkového protokolu
  - pre Ethernet II je 1
- **PTYPE** (16b) Protocol type – typ sieťového protokolu
  - pre IP je 800_{16}



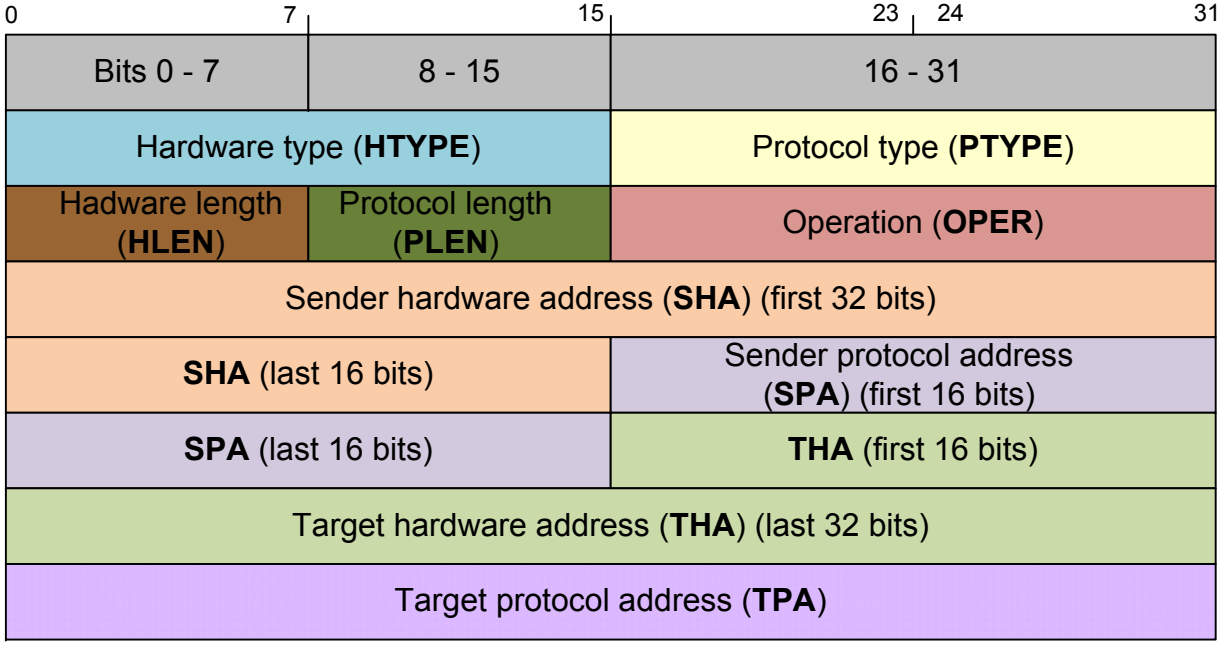
ARP

- **HLEN** (8b) Hardware length – dĺžka linkovej adresy
- **PLEN** (8b) Protocol length – dĺžka sieťovej adresy



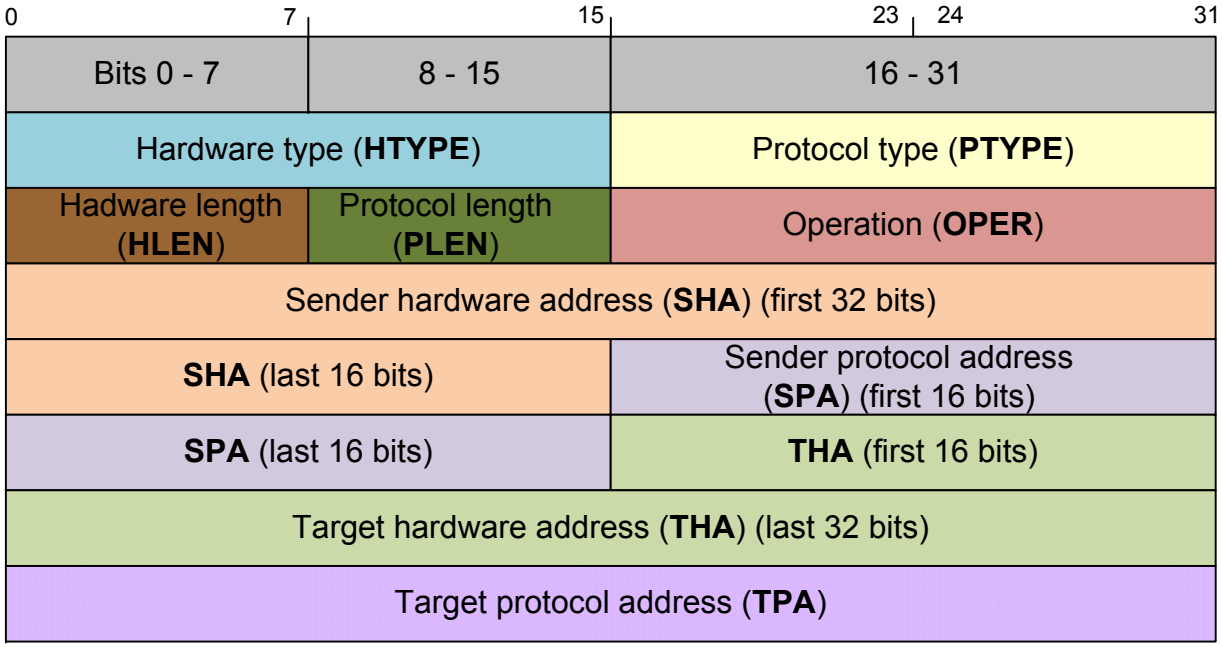
ARP

- **OPER** Operation (16b) – Operácia
  - ARP žiadosť- 1
  - ARP odpoveď – 2
  - RARP žiadosť – 3
  - RARP odpoveď – 4



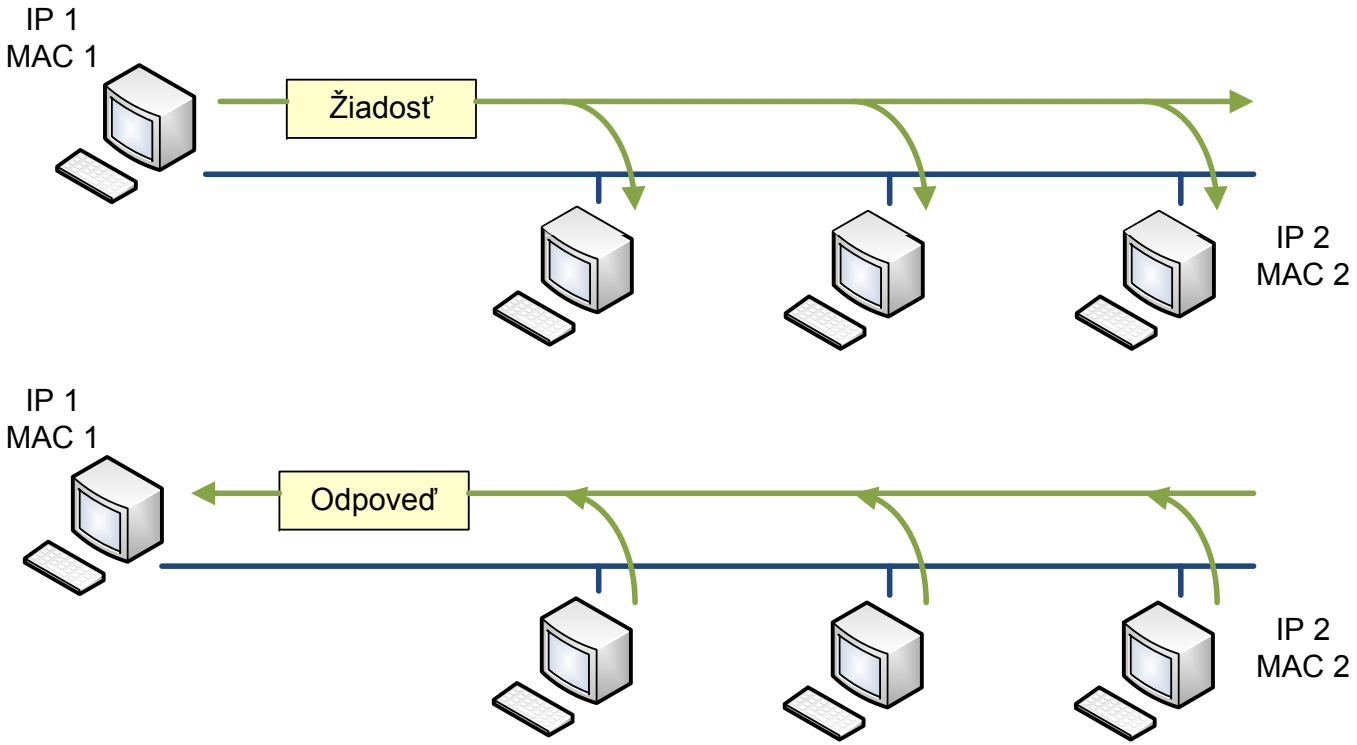
ARP

- **SHA, SPA, THA, TPA** (48b, 32b) Sender/Target Hardware/Protocol Address – linková/sieťová adresa príjemcu/odosielateľa
  - pokiaľ nie je niektorá položka známa, nastaví sa na 0



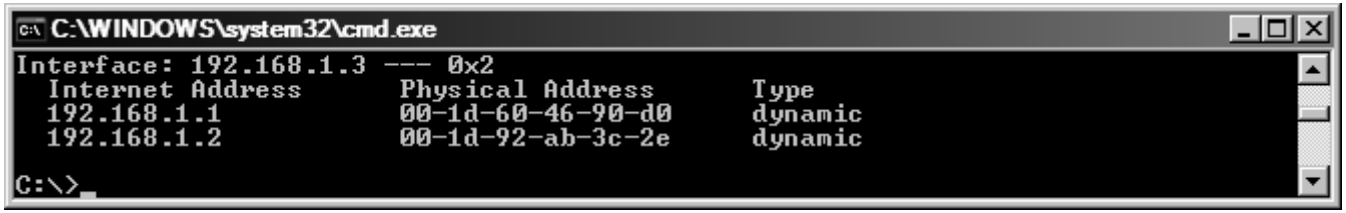
ARP

- Zdrojová stanica vysiela žiadosť s prosbou o nájdenie fyzickej adresy.
- Cieľová stanica, ktorej sa žiadosť týka, dostane túto žiadosť a vyšle odpoveď so svojou fyzickou adresou.



ARP

- Získané informácie o dvojiciach MAC adresa ↔ IP adresa si komunikačné uzly uchovávajú vo vyrovnávacích tabuľkách tzv. ARP Cache.
- Položky sú v ARP Cache zapísané:
  - staticky –explicitne príkazom **arp**. Ostávajú v pamäti stále. Periodicky sa musia aktualizovať.
  - dynamicky – zapisujú sa automaticky pomocou ARP mechanizmu. Ich doba života je nastavená jadrom OS (približne 20 min.).



Gratuitous ARP

- Špeciálny typ ARP paketu:
  - zdrojová IP adresa a cieľová adresa sú rovnaké – udávajú IP adresu odosielateľa,
  - MAC adresa cieľa je FF:FF:FF:FF:FF:FF (broadcast),
  - na takýto paket nie je odoslaná odpoveď,
  - slúži na nevyžiadané oznámenie zariadeniam v sieti, že odosielateľ má danú MAC a IP adresu,
  - vhodné pre detekciu konfliktov, v prípade rovnakých IP adries v sieti,
  - aktualizácia ARP Cache komunikačných zariadení,
  - väčšinou sa vygeneruje pri spustení komunikačnej linky.

RARP

- Reverse ARP:
- slúži na zistenie IP adresy na základe známej MAC adresy,
- formát paketu rovnaký ako ARP,
- využíval sa bezdiskovými stanicami na zistenie pridelenej IP adresy,
- v dnešnej dobe sa skoro vôbec nepoužíva, nahradil ho aplikačný protokol DHCP.

Adresácia v IP

- v dnešnej dobe najviac používaná IPv4,
- adresa môže byť uvádzaná vo viacerých typoch zápisu:
- Desiatková notácia
  - 147.175.103.1
- Dvojková notácia
  - 10010011.10101111.01100111.00000001
- Šestnástková notácia
  - 93.AF.67.1

Adresácia v IP

- IP adresa môže byť pridelená:
  - staticky – trvalo nakonfigurovaná v komunikačnom zariadení,
  - dynamicky – pri štarte zariadenia alebo nadviazaní spojenia,
    - pomocou protokolov DHCP, RARP, BOOTP, PPP,
    - pridelená adresa sa môže dynamicky meniť alebo môže byť konfiguračne nastavená staticky pre dané zariadenie,
  - jedno sieťové rozhranie môže mať viacero IP adries.

Adresácia v IP

- IP adresa sa vždy skladá z dvoch častí:
  - adresa siete,
  - adresa zariadenia v sieti.
- Ako zistiť, ktorá časť 32b adresného poľa je adresa siete, a ktorá adresa zariadenia v sieti?
- Dva spôsoby:
  - Classfull addressing,
  - Classless addressing.

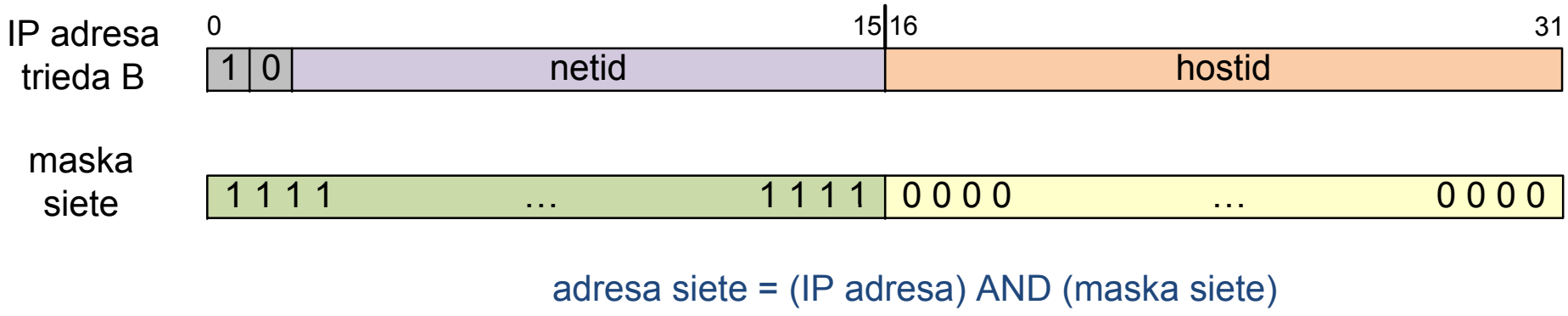
Adresácia v IP

- Maska siete:
  - určuje, ktoré bity v IP adrese tvoria adresu siete, a ktoré tvoria adresu zariadenia,
  - CIDR prefix udáva počet bitov označujúcich adresu siete.
- Zariadenie je jednoznačne adresované svojou IP adresou a maskou siete.
- Na základe IP adresy zariadenia a masky siete je možné určiť:
  - adresu siete,
  - broadcast adresu v danej sieti.

Adresácia v IP

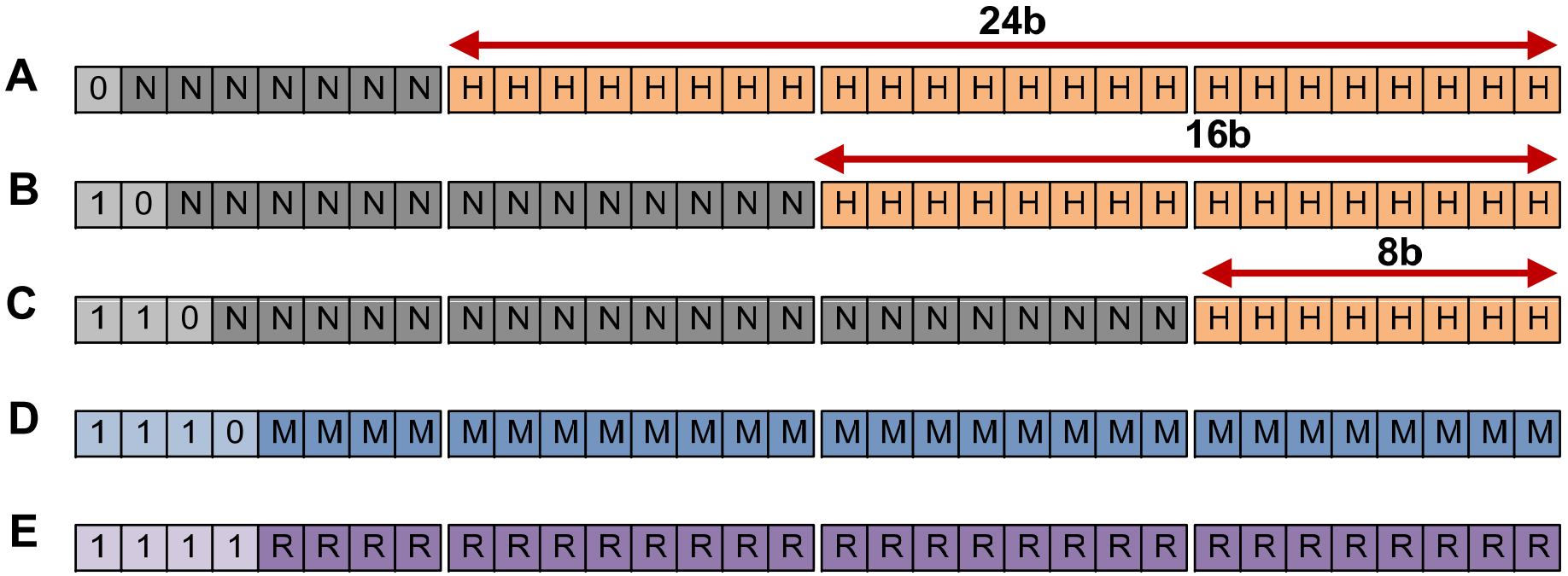
63

- Adresa siete = IP adresa AND maska siete
- Broadcast adresa je posledná adresa v danej sieti
  - všetky bity adresy zariadenia = 1



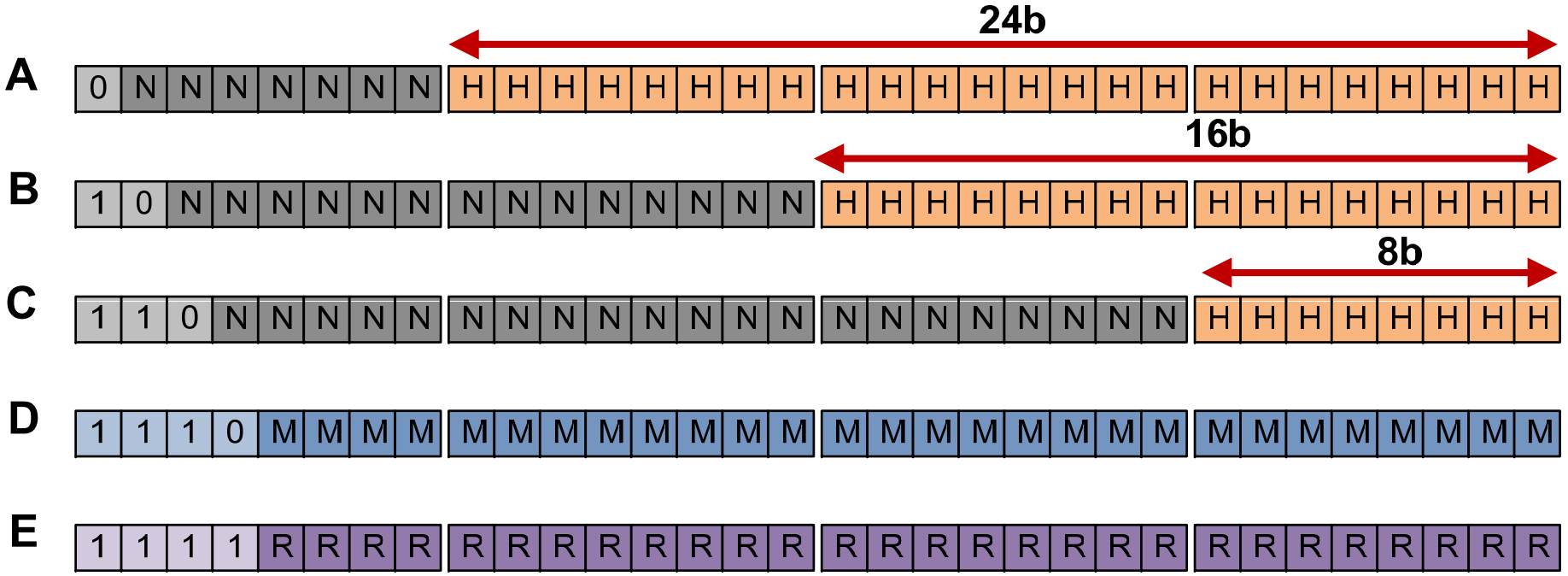
Classful addressing

- Pôvodný prístup k adresácii do roku 1993 RFC 796.
- IP adresy sa delia na 5 tried, v ktorých je definované, akú veľkú časť adresy tvorí adresa siete a akú adresa zariadenia.



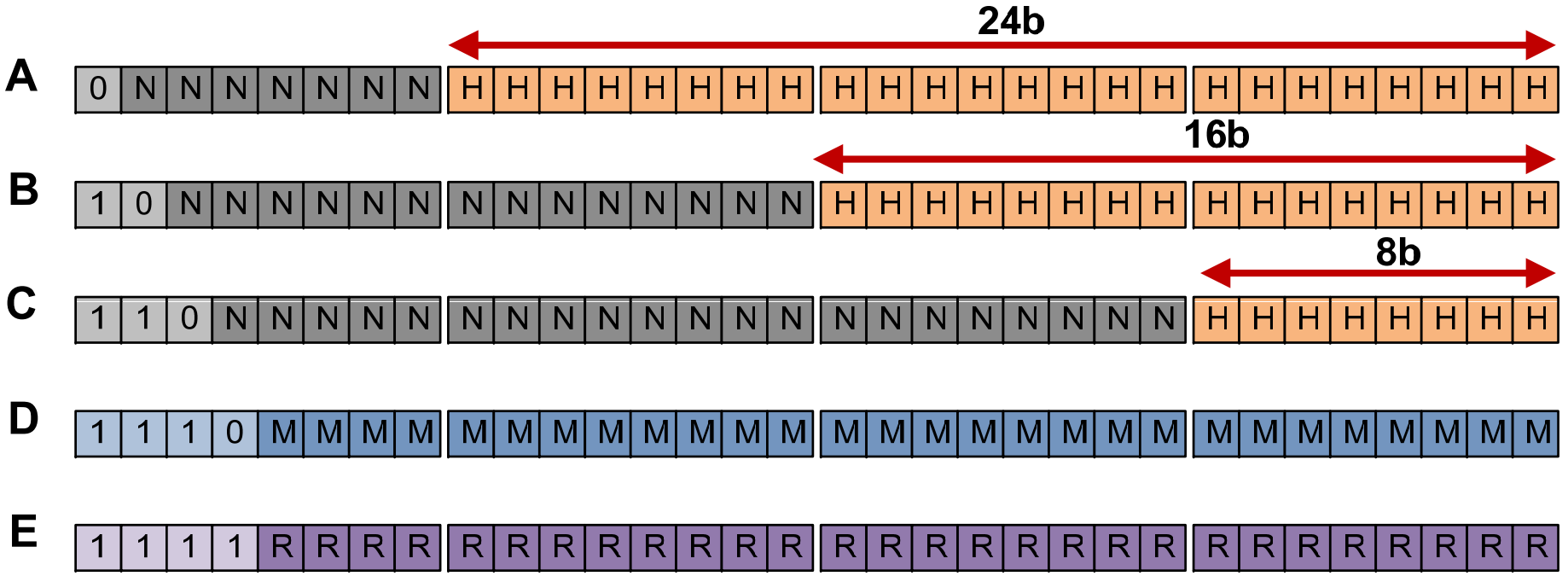
Classful addressing

- Trieda A
  - len pre veľké spoločnosti a obrovské siete,
  - rozsah adries 0.0.0.0 – 127.255.255.255,
  - maska 255.0.0.0 , CIDR prefix /8 – prvých 8 bitov adresy je adresa siete,
  - 126 sietí a v každej 16 777 214 zariadení.



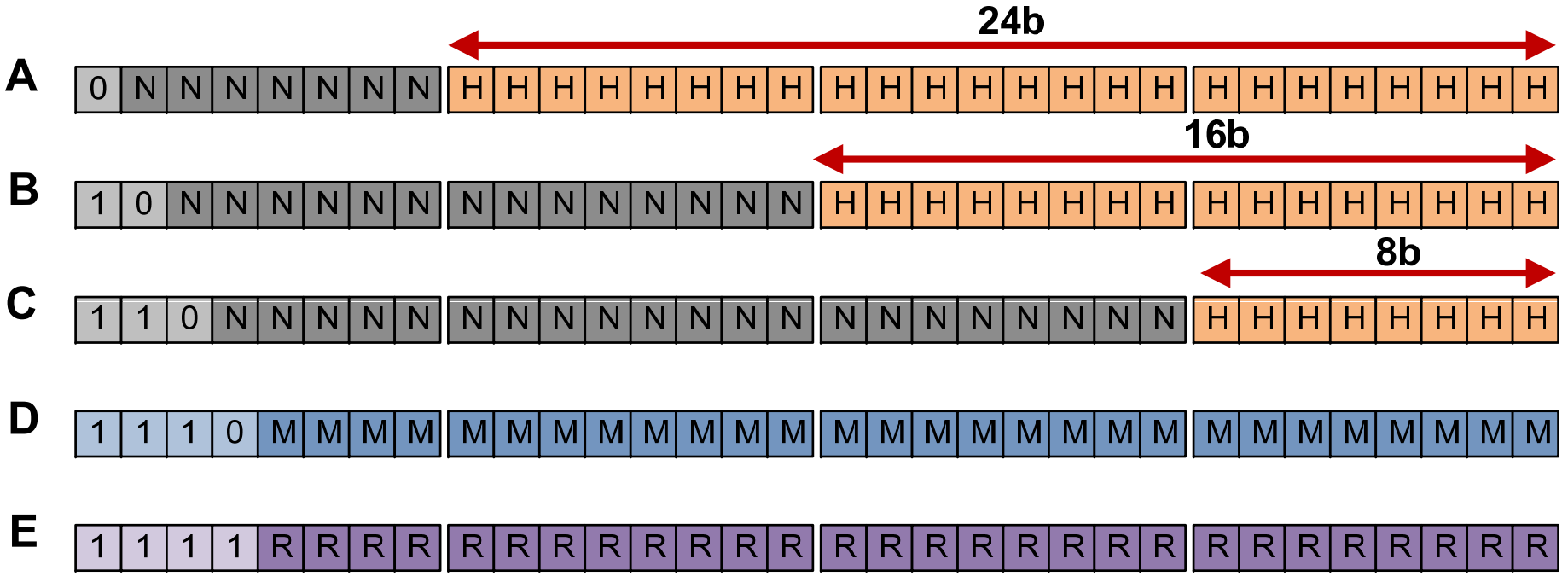
Classful addressing

- Trieda B
  - stredne veľké až veľké siete,
  - rozsah adries 128.0.0.0 – 191.255.255.255,
  - maska 255.255.0.0, CIDR /16,
  - 16 384 sietí a v každej 65 534 zariadení.



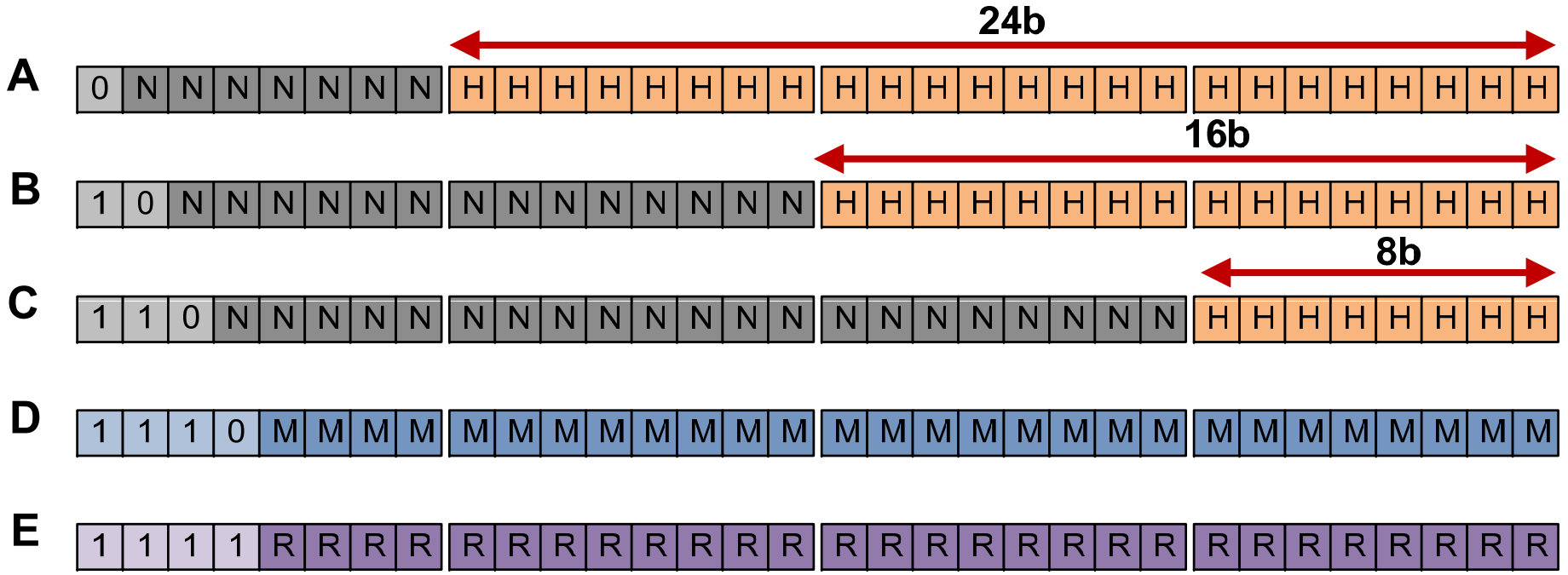
Classful addressing

- Trieda C
  - malé siete,
  - rozsah adries 192.0.0.0 – 223.255.255.255,
  - maska 255.255.255.0, CIDR /24,
  - 2 097 152 sieti a v každej 254 zariadení.



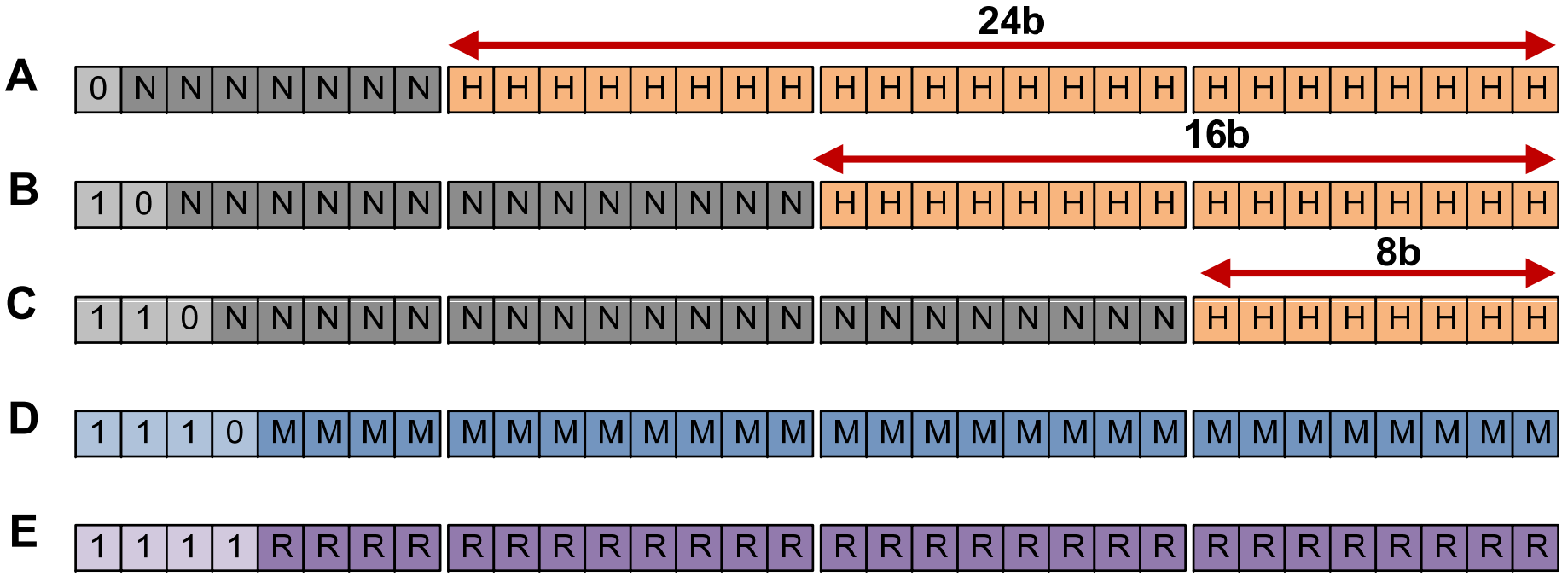
Classful addressing

- Trieda D
  - multicastové (skupinové) adresovanie,
  - rozsah adries 224.0.0.0 – 239.255.255.255,
  - CIDR /4.



Classful addressing

- Trieda E
  - rezervované pre experimentálne použitie ,
  - rozsah adries 240.0.0.0 – 255.255.255.255,
  - CIDR /4.



Classful addressing – Trieda A

- Príklad IP adresa triedy A
- IP adresa : 61.165.57.103
- sieťová maska: 255.0.0.0
- adresa siete: 61.0.0.0
- broadcast adresa: 61.255.255.255

IP adresa	00111101	10100101	00111001	01100111
maska	11111111	00000000	00000000	00000000
adresa siete	00111101	00000000	00000000	00000000
broadcast adresa	00111101	11111111	11111111	11111111
	NET	HOST		

Classful addressing – Trieda B

- Príklad IP adresa triedy B
- IP adresa : 147.103.43.139
- sieťová maska: 255.255.0.0
- adresa siete: 147.103.0.0
- broadcast adresa: 147.103.255.255

IP adresa	10010011	01100111	00101011	10001011
maska	11111111	11111111	00000000	00000000
adresa siete	10010011	01100111	00000000	00000000
broadcast adresa	10010011	01100111	11111111	11111111
	NET		HOST	

Classful addressing – Trieda C

- Príklad IP adresa triedy C
- IP adresa : 211.176.186.134
- sieťová maska: 255.255.255.0
- adresa siete: 211.176.186.0
- broadcast adresa: 211.176.186.255

IP adresa	11010011	10110000	10111010	10000110
maska	11111111	11111111	11111111	00000000
adresa siete	11010011	10110000	10111010	00000000
broadcast adresa	11010011	10110000	10111010	11111111
	NET			HOST

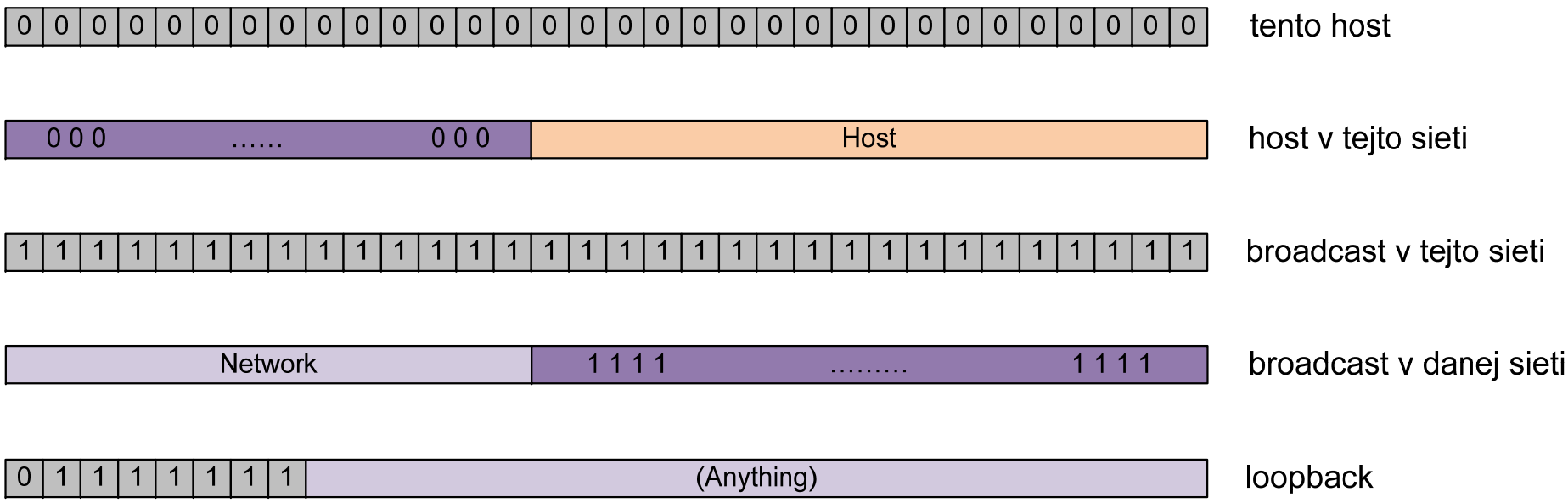
Classful addressing

- Špeciálne rozsahy IP adries určené pre špecifické účely

Adresy	CIDR	Účel	RFC	Trieda	Celkový počet adries
0.0.0.0 - 0.255.255.255	0.0.0.0/8	Zero Addresses	RFC 1700	A	16.777.216
10.0.0.0 - 10.255.255.255	**10.0.0.0/8**	**Private IP addresses**	**RFC 1918**	**A**	**16.777.216**
127.0.0.0 - 127.255.255.255	**127.0.0.0/8**	**Localhost Loopback Address**	**RFC 1700**	**A**	**16.777.216**
169.254.0.0 - 169.254.255.255	169.254.0.0/16	Zeroconf / APIPA	RFC 3330	B	65.536
172.16.0.0 - 172.31.255.255	**172.16.0.0/12** *	**Private IP addresses**	**RFC 1918**	**B**	**1.048.576**
192.0.2.0 - 192.0.2.255	192.0.2.0/24	Documentation and Examples	RFC 3330	C	256
192.88.99.0 - 192.88.99.255	192.88.99.0/24	IPv6 to IPv4 relay Anycast	RFC 3068	C	256
192.168.0.0 - 192.168.255.255	**192.168.0.0/16** *	**Private IP addresses**	**RFC 1918**	**C**	**65.536**
198.18.0.0 - 198.19.255.255	198.18.0.0/15 *	Network Device Benchmark	RFC 2544	C	131.072
224.0.0.0 - 239.255.255.255	224.0.0.0/4	Multicast	RFC 3171	D	268.435.456
240.0.0.0 - 255.255.255.255	240.0.0.0/4	Reserved	RFC 1166	E	268.435.456

Classful addressing

- Špeciálne IP adresy

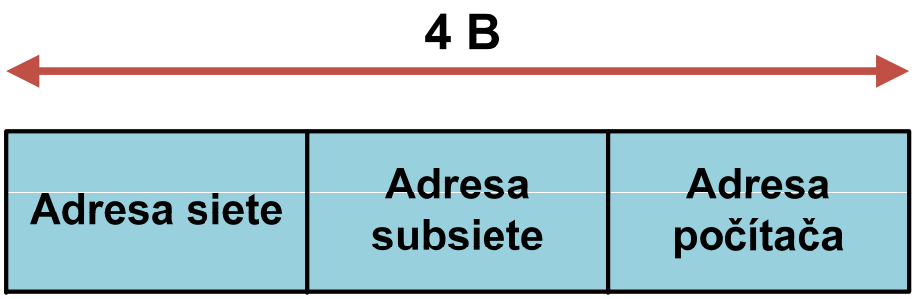


Classless addressing

- Problém s nedostatkom IP adries a ich neefektívnym delením na siete tried A,B,C.
- RFC 1517 a RFC 1520 v roku 1993
  - CIDR Classless Inter-Domain Routing.
- Siete sa prestávajú deliť na triedy.
- Rozlišujú sa výhradne na základe sieťových masiek.
- Bajty v maske môžu nadobúdať aj iné hodnoty ako 0 a 255.
- Sieťová maska musí byť vždy jeden súvislý rad jednotiek.

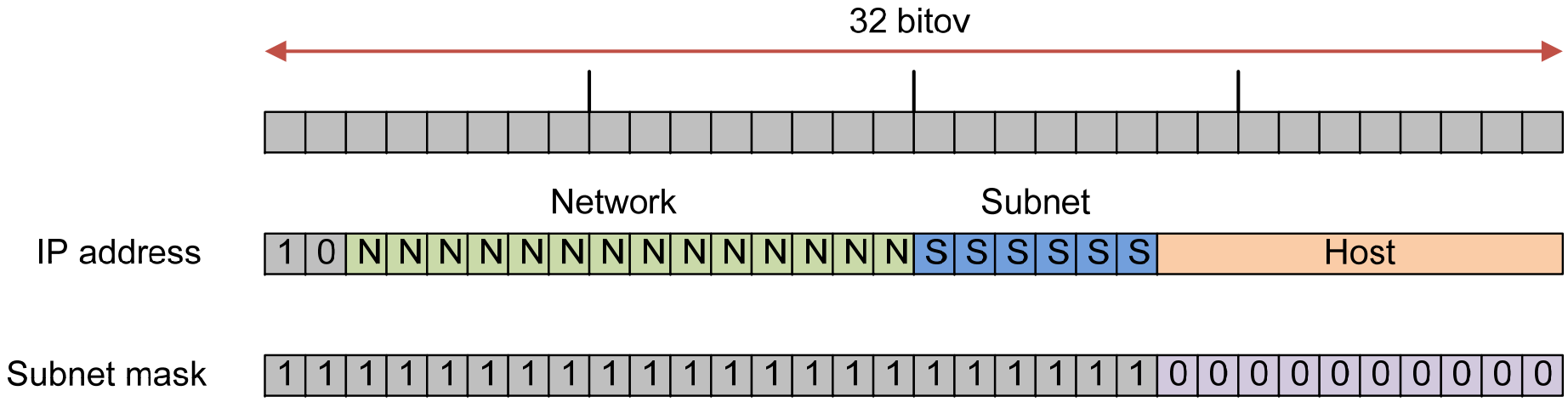
Classless addressing

- pôvodný priestor adresy koncového zariadenia sa rozdelil na adresu subsiete a adresu zariadenia,
- z hľadiska masky je adresa siete a adresa podsiete jeden celok,
- pre jednoznačné označenie je potrebné uvádzať IP adresu a masku súčasne,
- pre každú IP adresu existuje štandardná maska daná príslušnosťou k pôvodnej triede.



Classless addressing

- Sieť B rozdelená na 62 podsietí ($2^6 - 2$)
- maska: 255.255.252.0
  - 252 = (11111100)
  - zápis /22 – 22 bitov určených pre sieť a podsieť



Classless addressing

- Vznikajú subsiete a supersiete:
- Subsieť:
  - maska má viacej „jedničiek“ ako štandardná maska,
  - pôvodná trieda sa delí na viacero menších subsietí.
- Supersiete:
  - maska má menej „jedničiek“ ako štandardná maska,
  - zlučuje viacero sietí v danej triede do jednej väčšej siete.

Classless addressing - subsiete

Maska	Počet jedničiek v maske (zľava)	Interval IP adries	Skrátený zápis siete
255.248.0.0	13	192.168.0.0 až 192.175.255.255	192.168.0.0/13
255.252.0.0	14	192.168.0.0 až 192.171.255.255	192.168.0.0/14
255.254.0.0	15	192.168.0.0 až 192.169.255.255	192.168.0.0/15
255.255.0.0	16	192.168.0.0 až 192.168.255.255	192.168.0.0/16
255.255.248.0	21	192.168.0.0 až 192.168.7.255	192.168.0.0/21
255.255.252.0	22	192.168.0.0 až 192.168.3.255	192.168.0.0/22
255.255.254.0	23	192.168.0.0 až 192.168.1.255	192.168.0.0/23
255.255.255.0	24	192.168.0.0 až 192.168.0.255	192.168.0.0/24
255.255.255.128	25	192.168.0.0 až 192.168.0.127	192.168.0.0/25
255.255.255.192	26	192.168.0.0 až 192.168.0.63	192.168.0.0/26
255.255.255.224	27	192.168.0.0 až 192.168.0.31	192.168.0.0/27
255.255.255.240	28	192.168.0.0 až 192.168.0.15	192.168.0.0/28
255.255.255.248	29	192.168.0.0 až 192.168.0.7	192.168.0.0/29
255.255.255.252	30	192.168.0.0 až 192.168.0.3	192.168.0.0/30
255.255.255.254	31	192.168.0.0 až 192.168.0.1 Takáto sieť nemá zmysel lebo má len 2 IP adresy.	192.168.0.0/31
255.255.255.255	32	Adresa samostatného počítače (host address) 192.168.0.0	192.168.0.0/32

Classless addressing

- Sieťová maska 255.255.255.192
  - **(11111111 11111111 11111111 11000000)** – CIDR /26
- Rozdelí LAN (147.175.103.X) na 4. podsiete (pôvodne trieda B)
- 1. podsieť 147.175.103.0 **(10010011 10101111 01100111 00000000)**
  - uzly siete 147.175.103.1 – 147.175.103.62
    - **(10010011 10101111 01100111 00000001)**
    - **(10010011 10101111 01100111 00111110)**
  - boadcast v sieti 147.175.103.63 **(10010011 10101111 01100111 00111111)**
- 2. podsieť 147.175.103.64 **(10010011 10101111 01100111 01000000)**
  - uzly siete 147.175.103.65 – 147.175.103.126
    - **(10010011 10101111 01100111 01000001)**
    - **(10010011 10101111 01100111 01111110)**
  - boadcast v sieti 147.175.103.127 **(10010011 10101111 01100111 01111111)**

Classless addressing

- Sieťová maska 255.255.255.192
  - **(11111111 11111111 11111111 11000000)** – CIDR /26
- Rozdelí LAN (147.175.103.X) na 4. podsiete
- 3. podsieť 147.175.103.128 **(10010011 10101111 01100111 10000000)**
  - uzly siete 147.175.103.129 – 147.175.103.190
    - **(10010011 10101111 01100111 10000001)**
    - **(10010011 10101111 01100111 10111110)**
  - boadcast v sieti 147.175.103.191 **(10010011 10101111 01100111 10111111)**
- 4. podsieť 147.175.103.192 **(10010011 10101111 01100111 11000000)**
  - uzly siete 147.175.103.193 – 147.175.103.254
    - **(10010011 10101111 01100111 11000001)**
    - **(10010011 10101111 01100111 11111110)**
  - boadcast v sieti 147.175.103.255 **(10010011 10101111 01100111 11111111)**

Classless addressing

- účel sieťovej masky, je určiť ktoré bity tvoria adresu siete,
- adresa siete = IP adresa AND maska,
- do akej siete patrí uzol 147.175.103.187 ak je maska 255.255.255.192.

IP adresa	147.175.103.187	→	**10010011**	**10101111**	**01100111**	**10111011**
maska	255.255.255.192	→	**11111111**	**11111111**	**11111111**	**11000000**
				AND		
adresa siete	147.175.103.128	←	**10010011**	**10101111**	**01100111**	**10000000**
broadcast	147.175.103.191	←	**10010011**	**10101111**	**01100111**	**10111111**

Classless addressing

- Konštantné sieťové masky
  - Rozdelenie na subsiete rovnakej veľkosti:
    - sieťová adresa: 192.135.120.0,
    - štandardná maska: 255.255.255.0,
    - 32 subsietí, každá má 8 adries,
    - maska subsiete: 255.255.255.248.
- Subsieť:
  - 192.135.120.00001000 -00001111 192.135.120.10/29
  - 192.135.120.00010000 -00010111 192.135.120.22/29
- atď.

Classless addressing

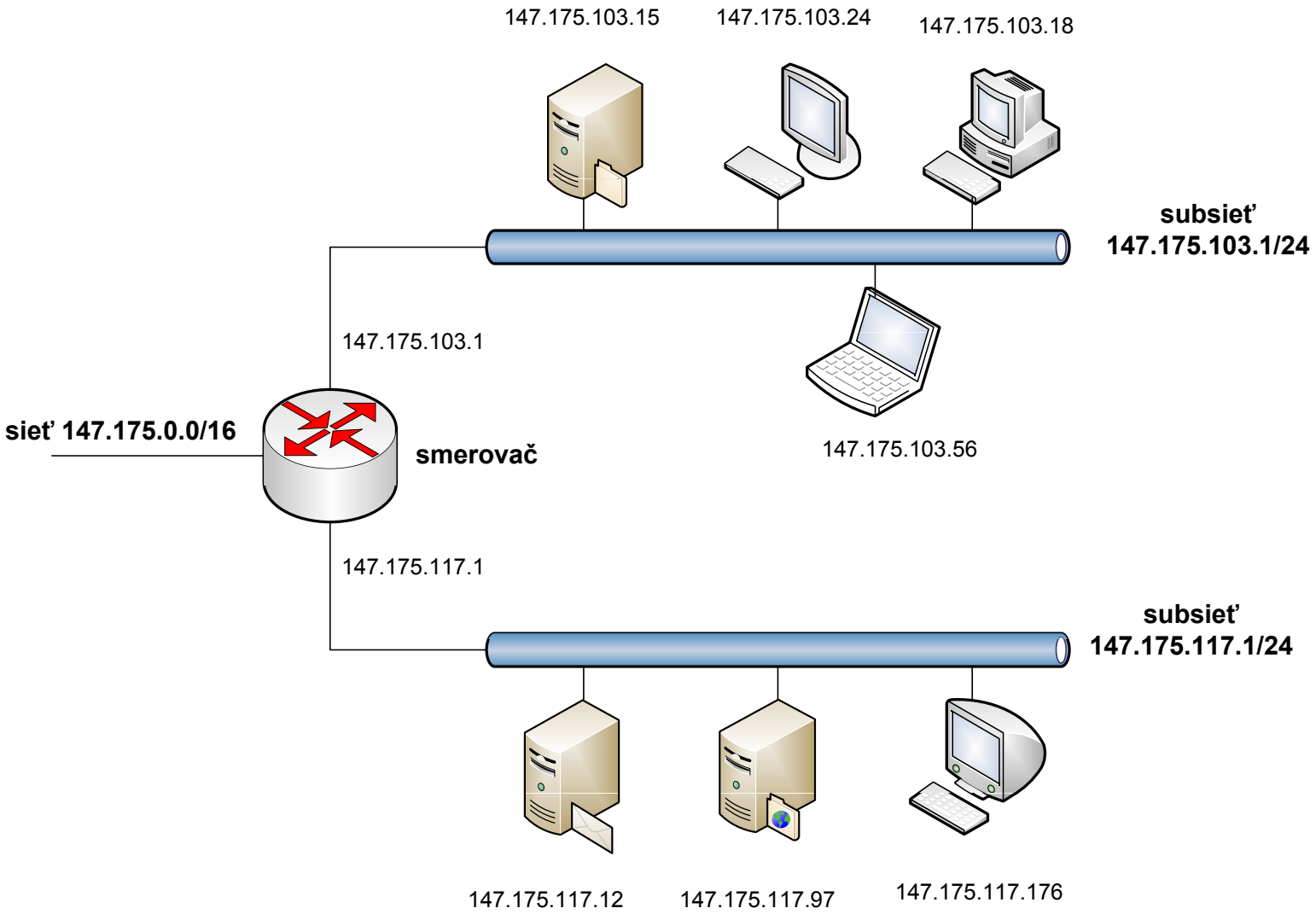
- Variabilné sieťové masky
  - rozdelenie na subsiete rôznej veľkosti
    - sieťová adresa: 192.135.120.0
    - štandardná maska: 255.255.255.0
- subsieť:
  - 192.135.120.00000100 -00000111
    255.255.255.252 192.135.120.6/30
  - 192.135.120.00010000 -00011111
    255.255.255.240 192.135.120.19/28
- atď.

Classless addressing

- Supersiete
  - spojenie súvislých intervalov IP adries na jednu adresu supersiete.
- Príklad:
  - adresy triedy C, štandardná maska: 255.255.255.0,
  - supersieť: 192.142.8.0 s maskou255.255.248.0 (192.142.8.0/21),
  - intervaly: 192.142.8.0 až 192.142.15.0.

	192	142	8		0
adresa siete	11000000	10001110	00001	000	00000000
	192	142	15		0
adresa siete	11000000	10001110	00001	111	00000000
	NET			HOST	

Classless addressing



Privátne IP adresy

- Trieda A – 10.0.0.0/8
  - 10.0.0.0 -10.255.255.255
  - 2_{24} = 16 777 216 adries
- Trieda B – 172.16.0.0/12
  - 172.16.0.0 -172.31.255.255
  - 2_{20} = 1 048 576 adries
- Trieda C – 192.168.0.0/16
  - 192.168.0.0 -192.168.255.255
  - 2_{16} = 65 536 adries
- interné využitie je ľubovoľné,
- nesmú sa objaviť na internete.

KOMUNIKAČNÉ A INFORMAČNÉ SIETE

SIEŤOVÁ VRSTVA

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas