



VYSOKÉ UČENÍ FAKULTA
TECHNICKÉ INFORMAČNÍCH
V BRNĚ TECHNOLOGIÍ



4

Síťová vrstva

IPK 2021/2022 L

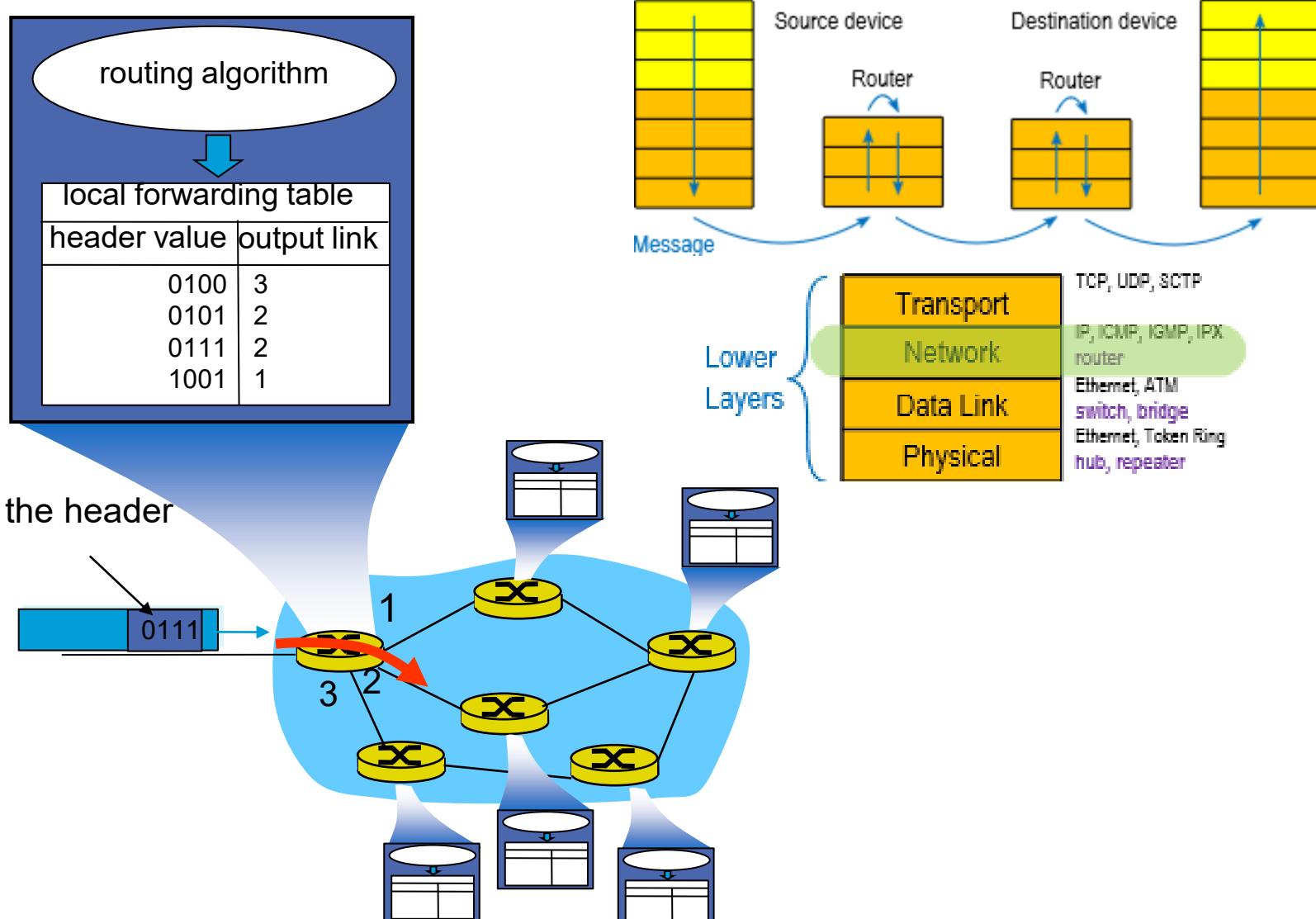
Obsah

- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

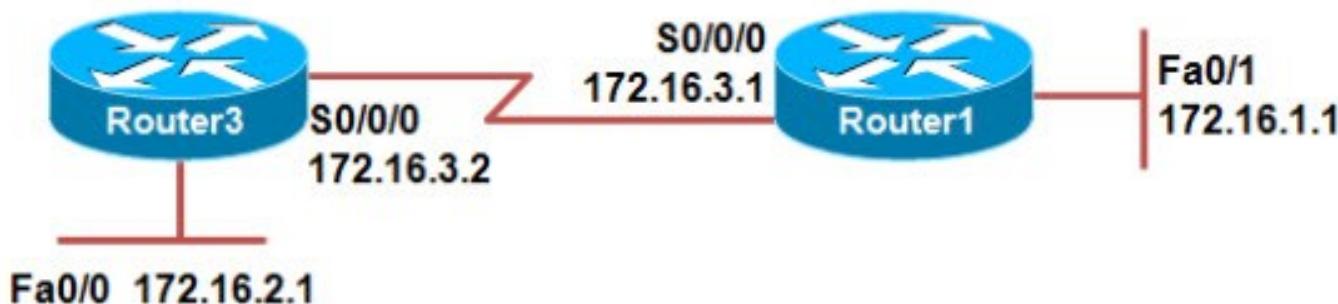
Klíčové funkce síťové vrstvy

- Přeposílání paketů (**packet forwarding**)
 - Přesunutí (přepsání) paketu ze vstupního rozhraní směrovače na výstupní rozhraní
- Směrování (**routing**)
 - Zjištění cesty (**route**) pro každý paket, který je přeposílán směrovačem
- Klíčovým prvkem je směrovač (**router**)
 - Pracuje na síťové vrtstvě (je adresovatelný IP adresou)
 - Využívá směrovací tabulku (ta určuje kam bude paket přeposlán)

Směrování



Reálná směrovací tabulka



```
R3# show ip route
<output omitted>
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

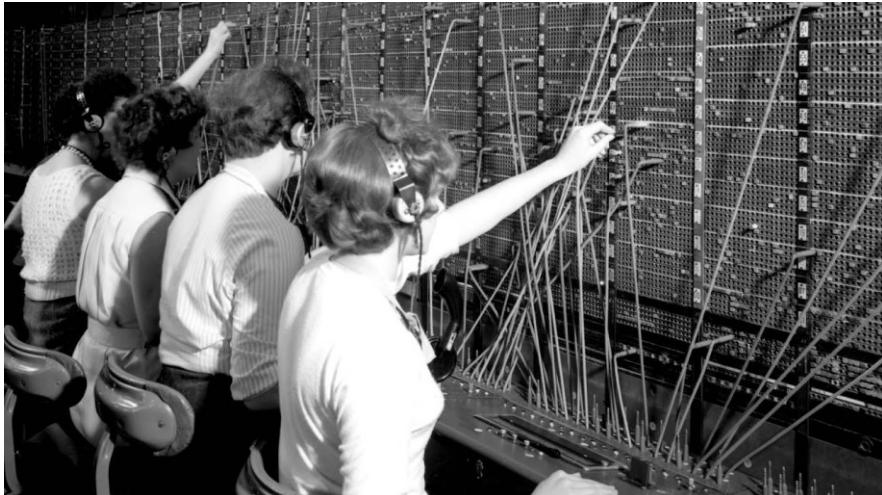
    172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D      172.16.0.0/16 is a summary, 00:20:29, Null0
D      172.16.1.0/24 [90/2297856] via 172.16.3.1, 00:13:56, Serial0/0/0
C      172.16.2.0/24 is directly connected, FastEthernet0/0
C      172.16.3.0/30 is directly connected, Serial0/0/0
S*     0.0.0.0/0 is directly connected, Serial0/0/0
```

(Ne)Spojované L3 služby

- Datagramové sítě poskytují nespojovanou službu
 - Best effort delivery
 - Bezstavové směrovače
- Sítě s virtuálními okruhy poskytují spojově orientovanou službu
 - Stavové směrovače
 - Služba: host-host
 - Různé služby
 - Garantované přenosové pásmo
 - Ztráta paketů
 - Pořadí paketů
 - Zpoždění paketů

CO vs. CL (1)

- Connection-Oriented



- Connection-Less

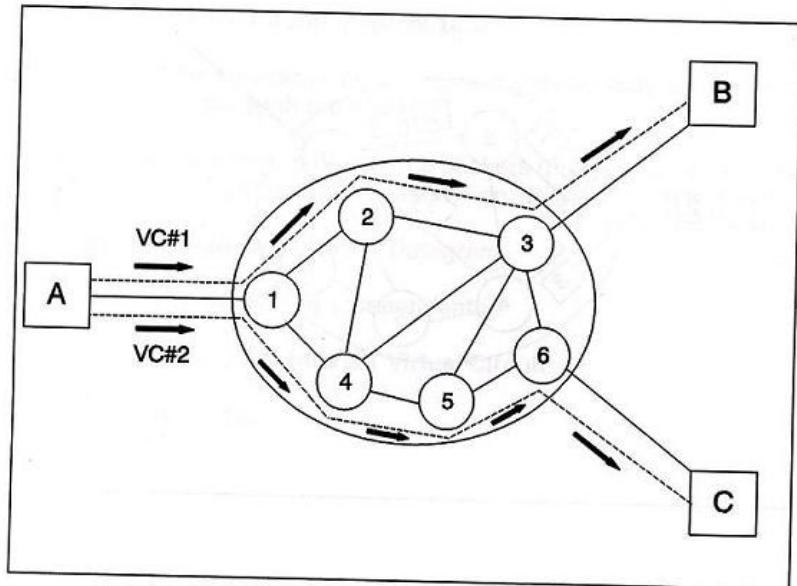


In a few years, men will be able to communicate more effectively through a machine than face to face. That is a rather startling thing to say, but it is our conclusion.

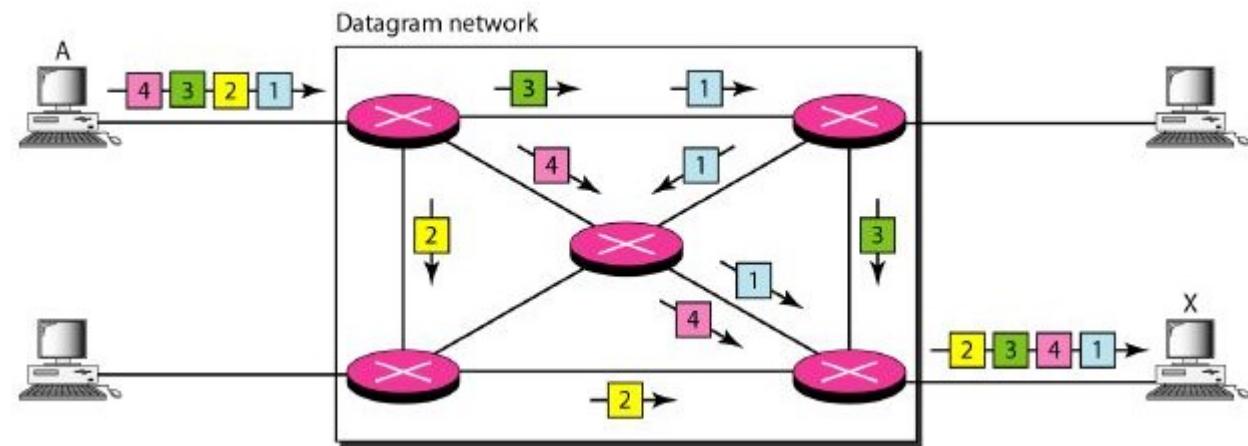
— J. C. R. Licklider —

AZ QUOTES

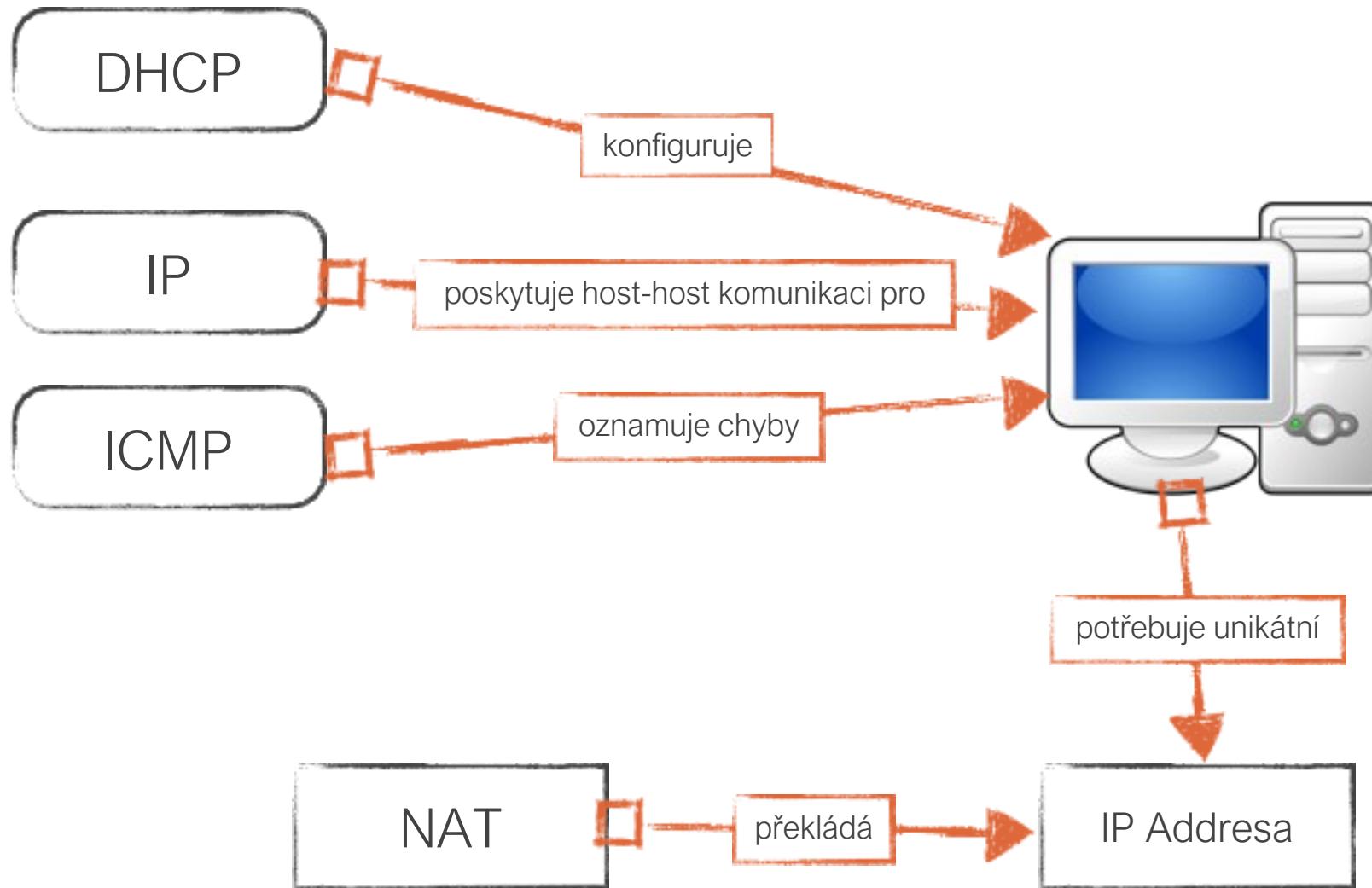
CO vs. CL (2)



- ISO/OSI iniciativa



Technologie

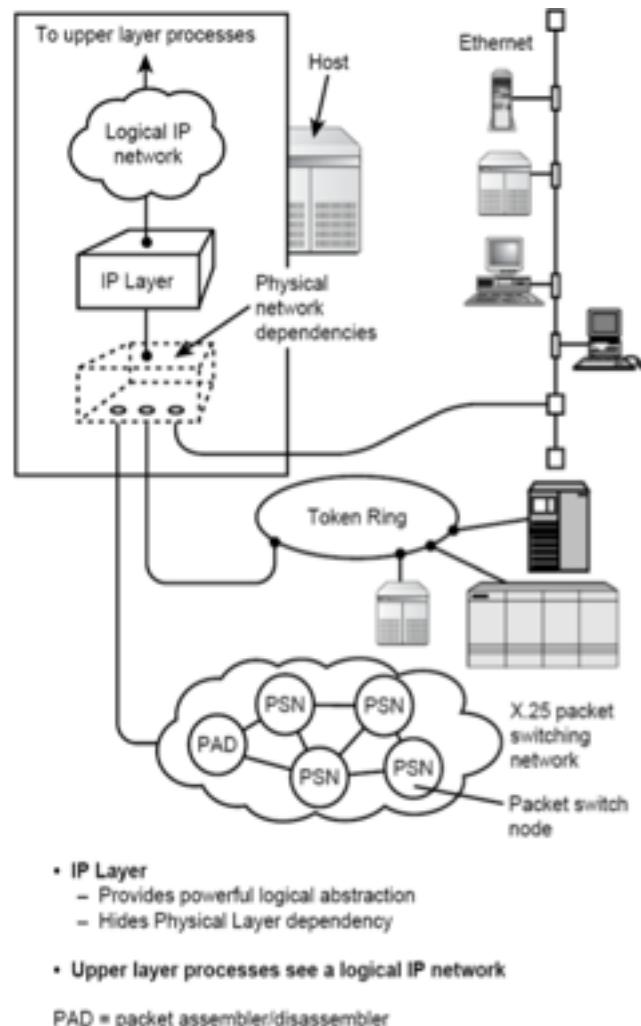


Obsah

- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

IPv4

- Internet Protocol verze 4
- RFC 791, STD [5], rok 1981
- IP pakety přenášeny rámci linkové vrstvy
 - Různé technologie linkové vrstvy (Ethernet, Token Bus, FDDI, ...)
- Quality of Service (QoS)
 - poskytuje možnost mapování požadavků na kvalitu služby pro aplikace
 - parametry pro QoS jsou předávány spolu s daty z transportní vrstvy



RFC 791

[Docs] [txt|pdf] [Tracker] [Errata]

Updated by: [1349](#), [2474](#), [6864](#)

RFC: 791

INTERNET STANDARD
Errata Exist

INTERNET PROTOCOL

DARPA INTERNET PROGRAM

PROTOCOL SPECIFICATION

September 1981

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

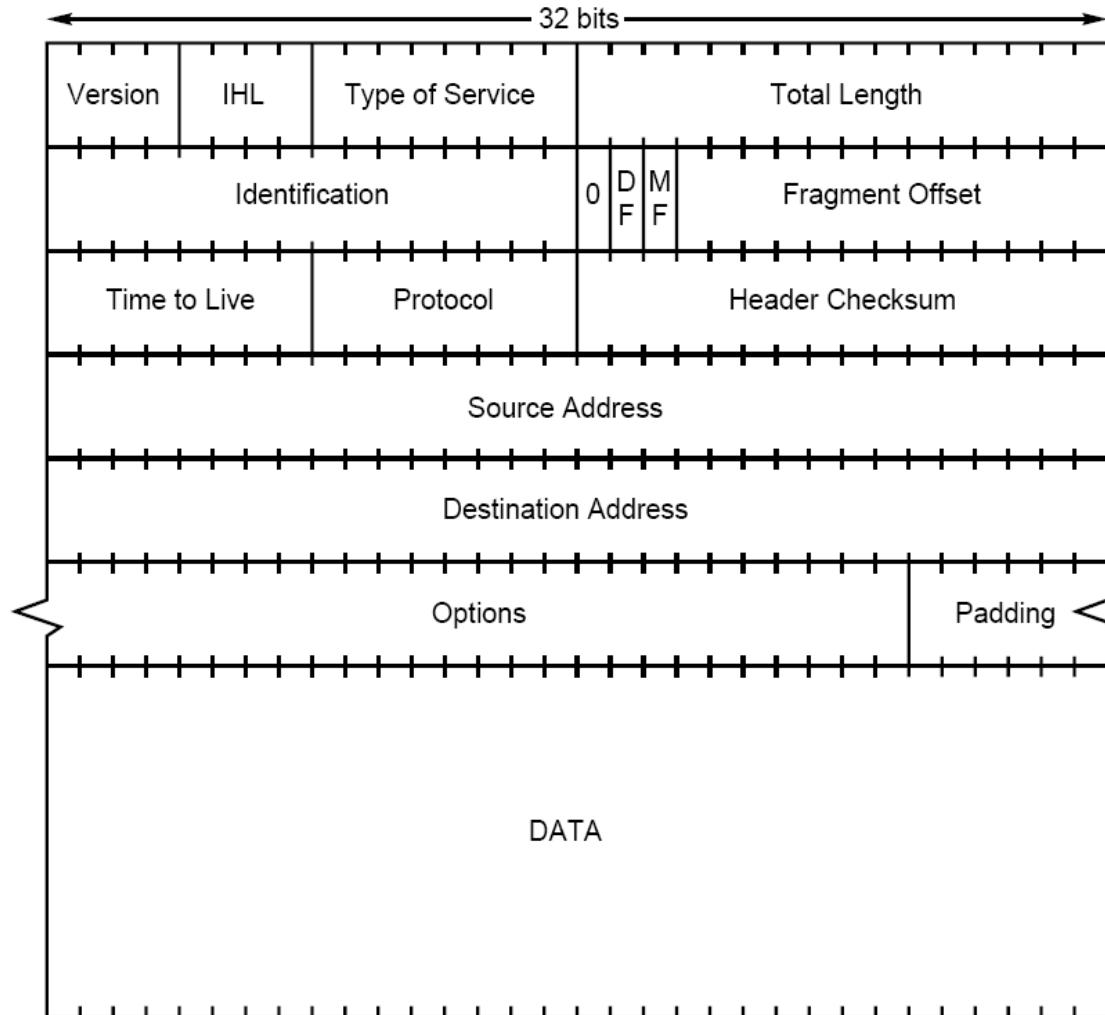
September 1981

Internet Protocol

TABLE OF CONTENTS

PREFACE	iii
1. INTRODUCTION	1
1.1 Motivation	1
1.2 Scope	1
1.3 Interfaces	1
1.4 Operation	2
2. OVERVIEW	5
2.1 Relation to Other Protocols	9
2.2 Model of Operation	5
2.3 Function Description	7
2.4 Gateways	9
3. SPECIFICATION	11
3.1 Internet Header Format	11
3.2 Discussion	23
3.3 Interfaces	31
APPENDIX A: Examples & Scenarios	34
APPENDIX B: Data Transmission Order	39
GLOSSARY	41
REFERENCES	45

IPv4 Hlavíčka



IPv4 Políčka (1)

- **Verze (*Version*)**
 - verze protokolu IP, pro IPv4 hodnota 4, pro IPv6 (IPng) hodnota 6 (jiný formát rámce), hodnoty 0-3 nepoužité, 7-9 experimentální protokoly (proměnná délka adresy)
- **Délka hlavičky (*Internet Header Length, IHL*)**
 - v počtu 32 bitových slov, proměnná délka hlavičky, minimum 20 byte, maximum 60 byte
- **Typ služby (*Type of Service, ToS*)**
 - možnost definice požadavku kvality služby, nespecifikováno v RFC
- **Celková délka (*Total Length*)**
 - délka IP paketu (hlavička+data), maximum 65535, minimálně 576 [512 B data + 64 B hlavička]

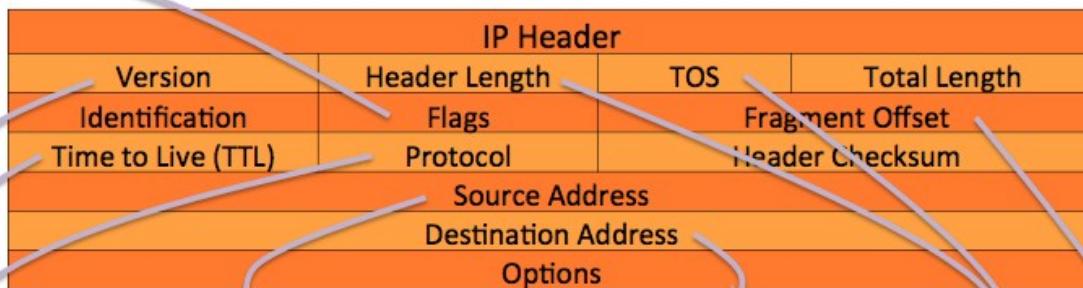
IPv4 Políčka (2)

- **Identifikace datagramu (*Identification*)**
 - unikátní (náhodné) číslo identifikující každý datagram (většinou inkrementováno, globální čítač v OS), používá se k identifikaci fragmentace IP datagramů
- **Příznaky fragmentace a pozice fragmentu**
 - DF (Don't Fragment), MF (More Fragments)
 - Offset=počítány po 8 bytových blocích (13 bitů)
- **Životnost datagramu (*Time To Live, TTL*)**
 - původně doba v sekundách, později jako počet skoků (hop count), sníženo každým směrovačem o 1, hodnota 0 znamená vypršení doby života, datagram je zahozen, řeší zacyklení mezi směrovači
- **Protokol vyšší vrstvy (*Protocol*)**
 - identifikuje PDU protokolu, přenášeného v datech
 - 1=ICMP, 2=IGMP, 4=IP, 6=TCP, 17=UDP, 46=RSVP, 88=IGRP, 89=OSPF

IPv4 Políčka (3)

- Kontrolní součet hlavičky (*Header Checksum*)
 - jedničkový doplněk součtu 16-bitových slov, bez Checksum, nutný přepočítat na každém směrovači! Proč?
- Zdrojová adresa (*Source Address*)
 - 32-bitová adresa hosta posílajícího datagram (host=NIC)
- Cílová adresa (*Destination Address*)
 - 32-bitová adresa hosta přijímacího datagram
- Volby
 - volitelné, bezpečnost, timestamp, record route, strict source routing

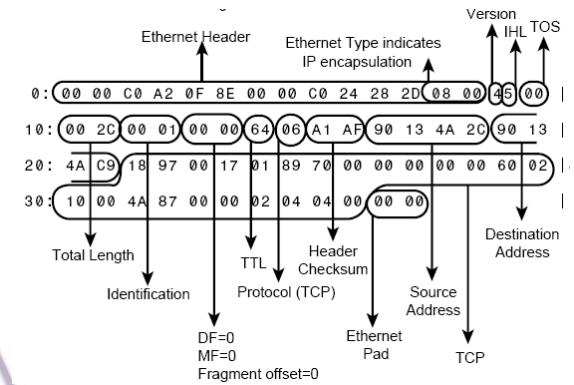
Příklad IP Paketu



```

Internet Protocol Version 4, Src: 10.100.16.200 (10.100.16.200), Dst: 10.100.185.66 (10.100.185.66)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
 0000 00.. = Differentiated Services Codepoint: Default (0x00)
.... 00.. = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length: 1420
Identification: 0x126d (4717)
Flags: 0x02 (Don't Fragment)
 0... .... = Reserved bit: Not set
 1... .... = Don't fragment: Set
 ..0.... = More fragments: Not set
Fragment offset: 0
Time to live: 255
Protocol: TCP (6)
Header checksum: 0x98ad [correct]
  [Good: True]
  [Bad: False]
Source: 10.100.16.200 (10.100.16.200)
Destination: 10.100.185.66 (10.100.185.66)

```



Minimum Transmission Unit

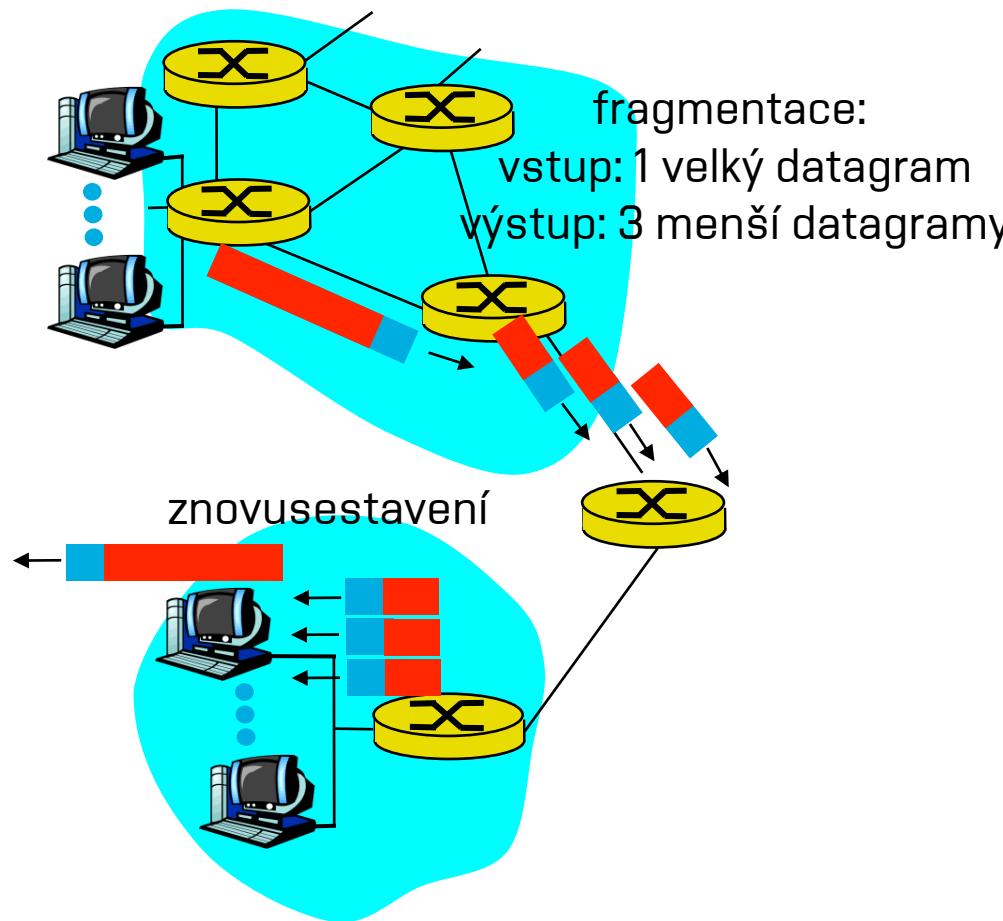
- Každá IPv4 implementace musí být schopna povinně přenést 576 bytů (celý IP datagram)
- MTU závisí na linkové vrstvě (přenosová technologie)

Media Type	Speed	Frame MTU	Maximum Frame Length
Ethernet	10 Mbps	1500	1518
802.3	10 Mbps	1518	1536
802.3u	100 Mbps	1518	1536
802.3z/ab	1 Gbps	1518	1536
802.3ae/an	10 Gbps	1518	1536
802.3ba	100 Gbps	1518?	1536?
802.5	4 Mbps	4528	4550
802.5	16 Mbps	18173	18200
802.5	100 Mbps	18173	18200
802.11g	54 Mbps	2312	2346
FDDI	100 Mbps	4352	4470
Fiber Channel	2 Gbps	65280	65280
POS/OC48	2.5 Gbps	9180	9180
ATM/AAL5		9180	9180

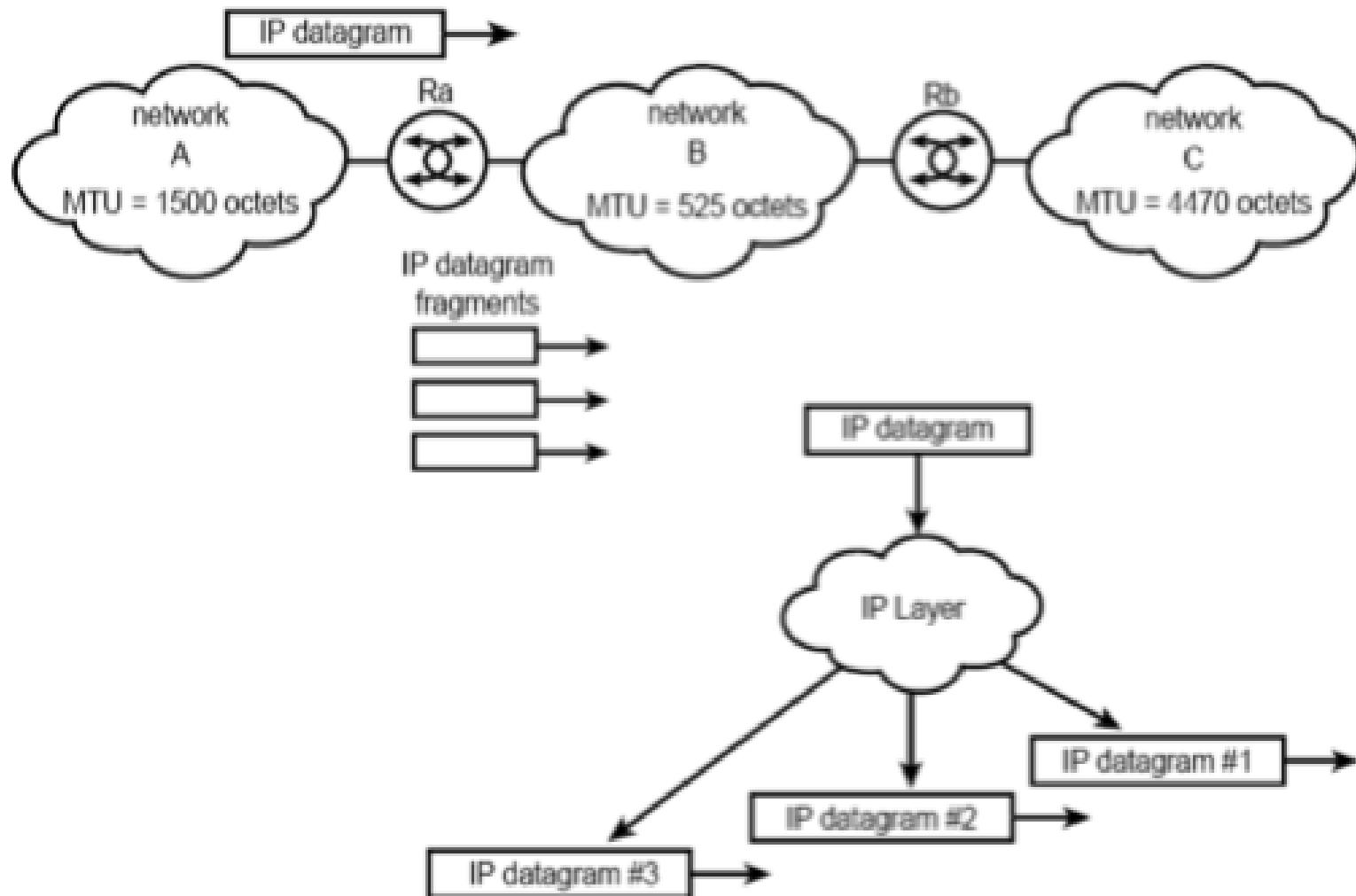
- Příklad:
 - Token Ring@4Mbps
 - THT=8.58 ms * 4 Mbps=36000 bits=4500 B
 - 4500 – 15 (MAC header) – 30 (Routing inf.) – 4 (LLC header) – 5 (SNAP header) – 6 (MAC trailer) = 4440 B

Fagmentace

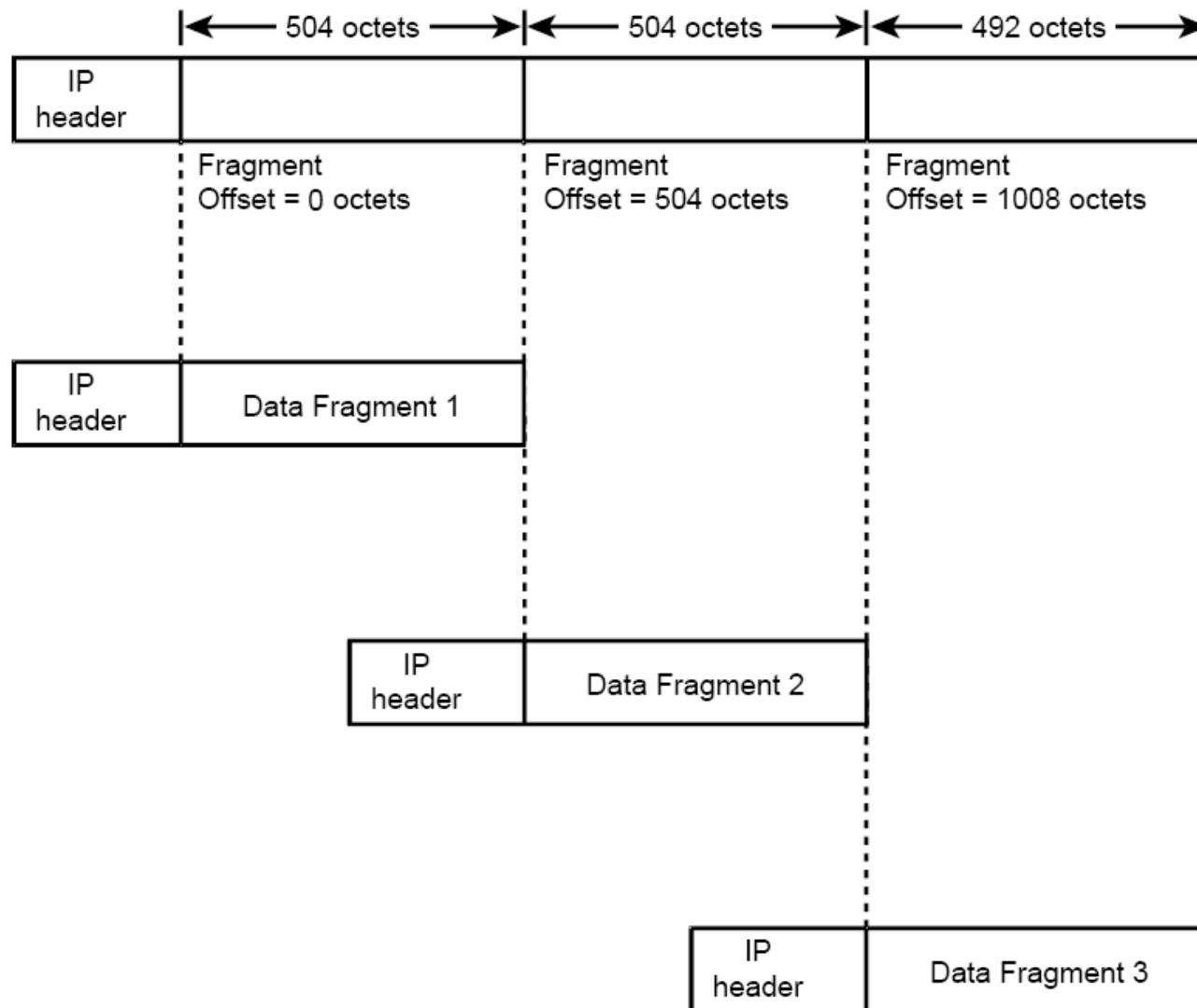
- Fyzická linka omezuje velikost přenášených dat (MTU)
 - Různé linky => různé MTU
- Pokud je v cestě linka s $MTU < \text{velikost IP datagramu}$ a $DF=0$, potom směrovač fragmentuje původní IP datagram
- Datagram sestavuje až koncový host (nikoliv další směrovač v cestě)
- Při sestavení se čeká určitou dobu; pokud vyprší časovač, ICMP zpráva indikuje expiraci časovače
- Nadměrná fragmentace vede k nadměrnému přenosu a nižší efektivitě
- Path MTU Discovery RFC 1191, RFC 2923



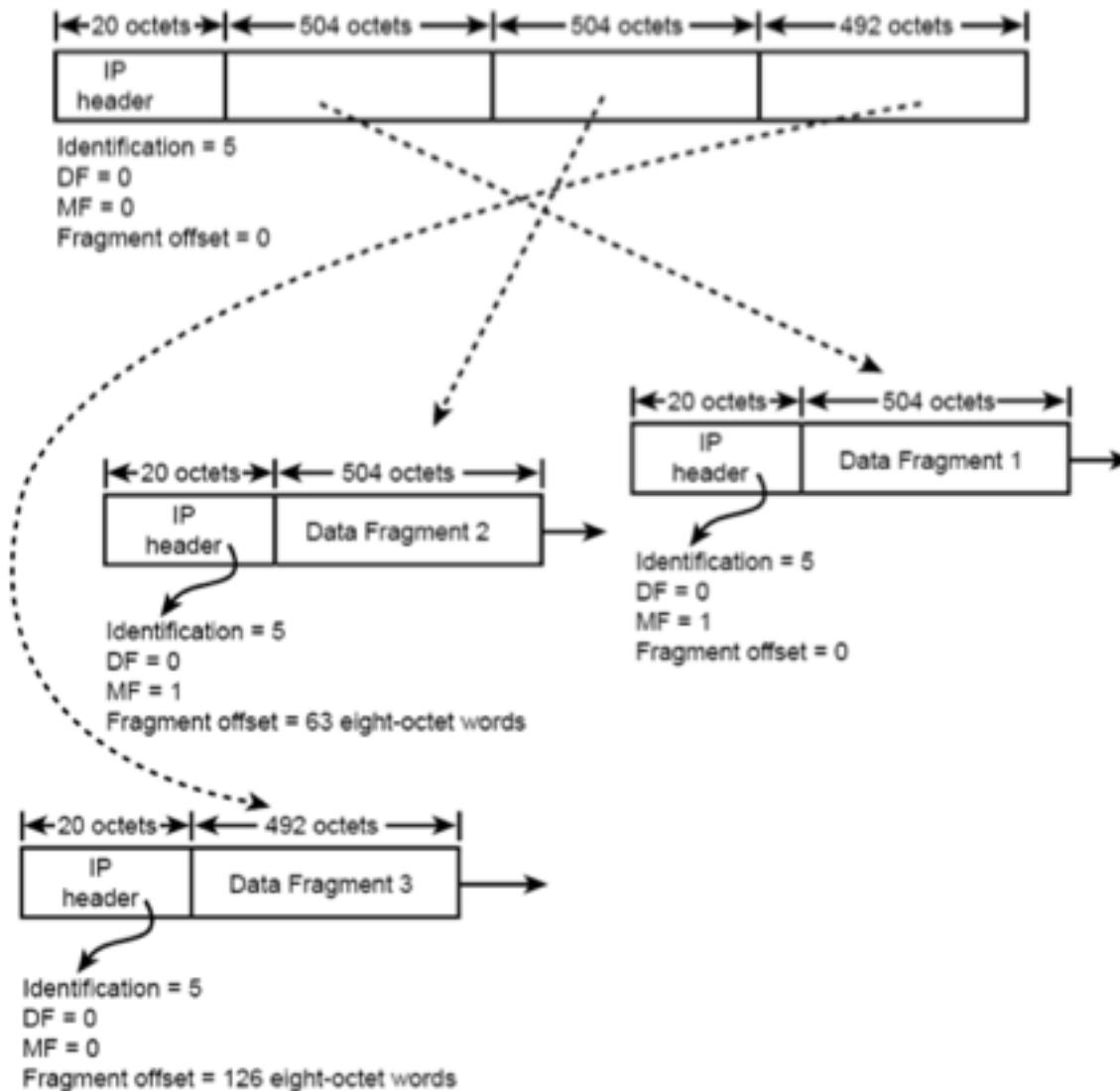
Příklad fragmentace (1)



Příklad fragmentace (2)

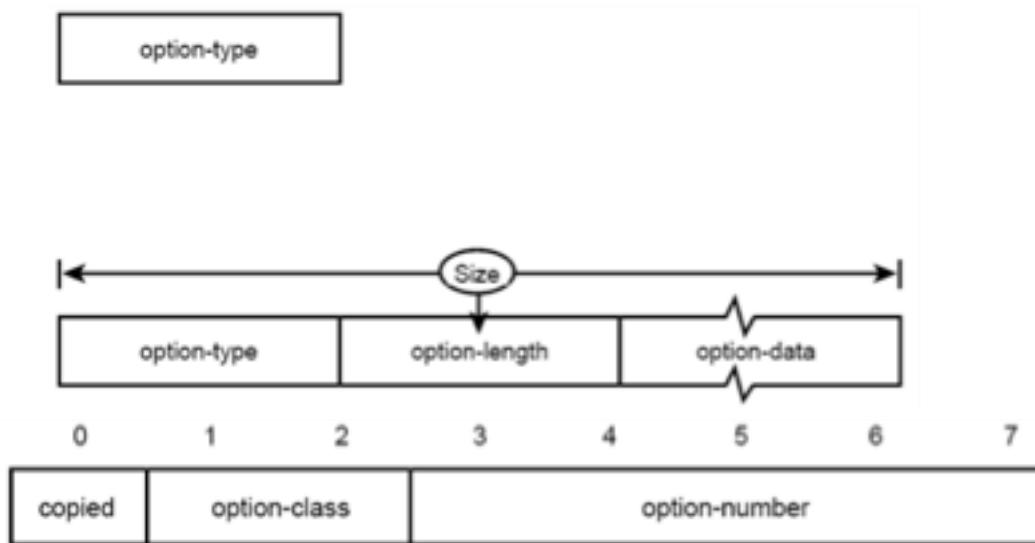


Příklad fragmentace (3)



Volby v IP hlavičce

- 2 formáty: single octet, variable length
- Copied: má se volba dostat do fragmentů?
- Option class: 0 Network control, 2 Debug & Measurement, zbytek reserved
- Option number: 0 End of Option List, 1 No Operation, 7 Record Route, 4 Timestamp



Obsah

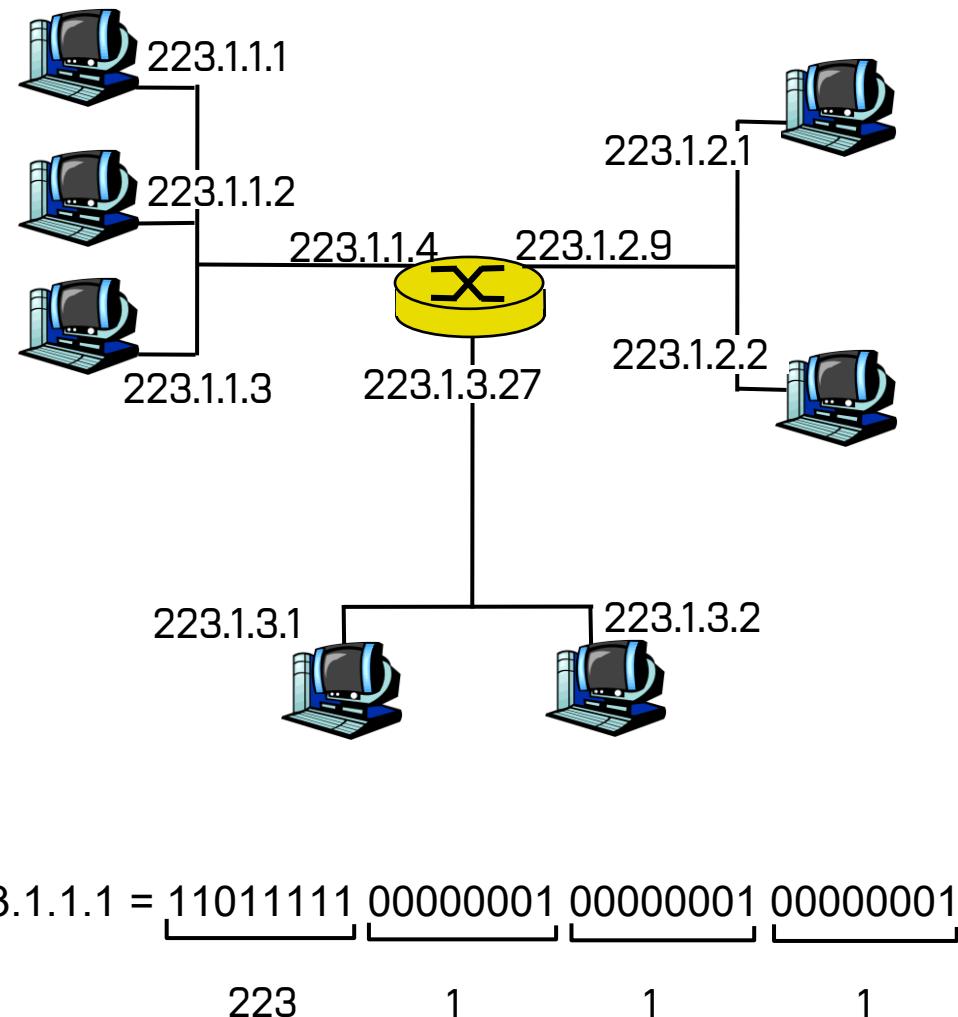
- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

IPv4 adresování

- IPv4 používá adresu pevné délky 32 bitů
- Zápis jednotlivých oktetů 147.229.176.14
- Kolik je různých adres?
 - 0.0.0.0 a 255.255.255.255 jsou rezervované
- Adresa se skládá ze 2 částí:
 - Identifikace sítě (NetId) + Identifikace hosta (HostId)
 - Identifikace sítě, identifikace hosta: 147.229.0.0 adresa sítě; 0.0.176.14 adresa hosta
- Třídní adresování (Classfull addressing)
 - Původní koncept, máme třídy adres A-E, jasné co je adresa sítě a adresa hosta
- Beztřídní adresování (Classless addressing)
 - Adresa je tvořena adresou sítě, adresou podsítě a adresou hosta, hranici mezi podsítí a je určena maskou

Proč potřebuje znát NetID?

- Síťové rozhraní (interface): spojení mezi hostem/směrovačem a fyzickým přenosovým médiem
 - Směrovač jich má obvykle více
 - Každé je identifikováno adresou
- V rámci lokální sítě/podsítě se pakety doručují bez intervence směrovače (brána, first hop router)
 - Používá se adresa linkové vrstvy



Třídy adres

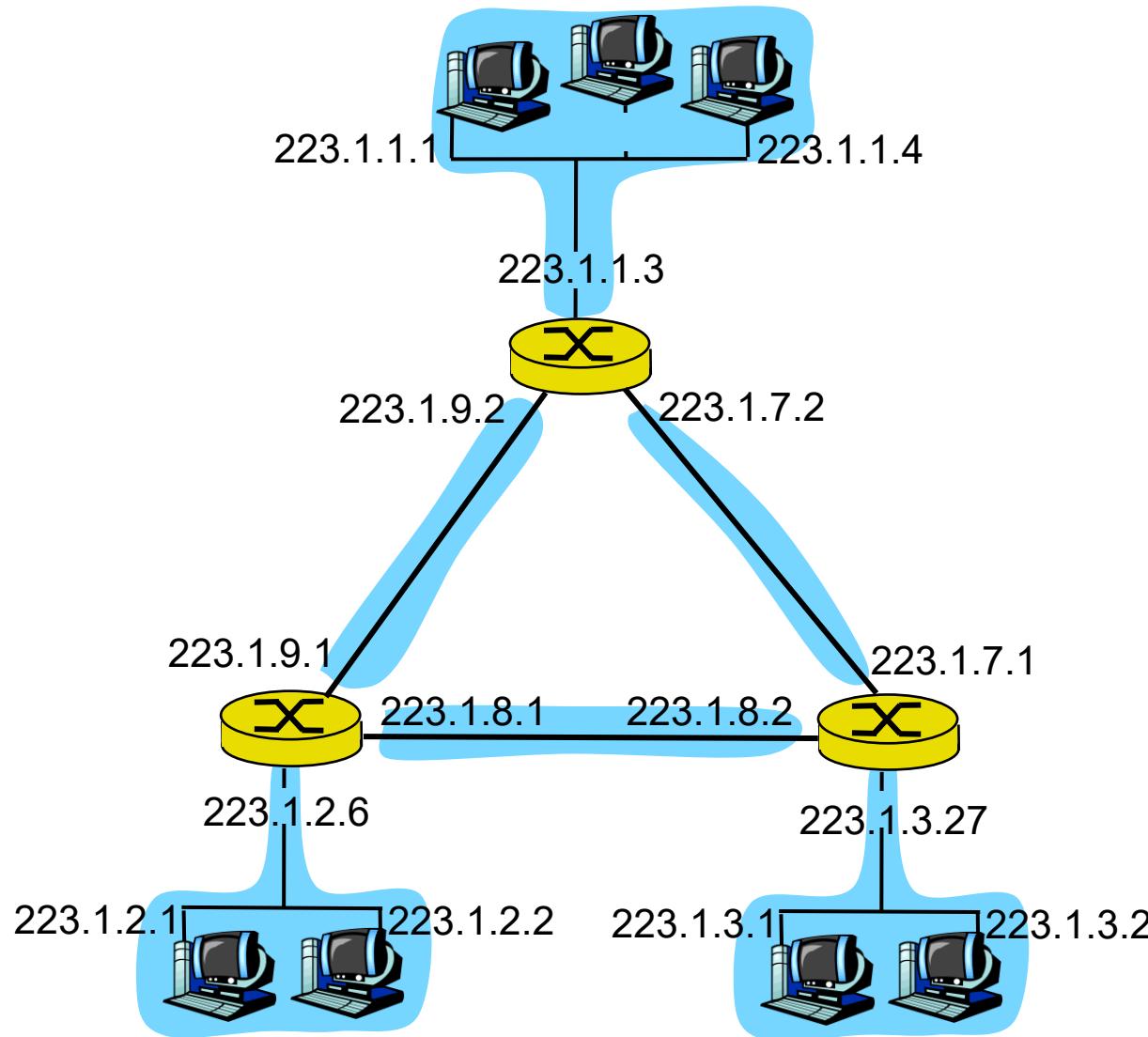
Třídy IP adres

Třída	Začátek (bin)	1. bajt	Standardní maska	Bitů sítě	Bitů stanice	Sítí	Stanic v každé síti
A	0	0–127	255.0.0.0	7	24	126	16 777 214
B	10	128–191	255.255.0.0	14	16	16384	65534
C	110	192–223	255.255.255.0	21	8	2 097 152	254
D	1110	224–239		multicast			
E	1111	240–255		vyhrazeno jako rezerva			

Rozsahy IP adres a masky sítě

Třída	1. bajt	Minimum	Maximum	Maska podsítě
A	0–127	0.0.0.0	127.255.255.255	255.0.0.0
B	128–191	128.0.0.0	191.255.255.255	255.255.0.0
C	192–223	192.0.0.0	223.255.255.255	255.255.255.0
D	224–239	224.0.0.0	239.255.255.255	255.255.255.255
E	240–255	240.0.0.0	255.255.255.255	-----

Počet podsítí?



Speciální adresy a typy

- Adresa obecně:
 - **Unicast** – konkrétní počítač (individuální adresa)
 - **Broadcast** - všechny počítače na síti (všešměrová adresa)
 - **Multicast** – skupina počítačů, člen skupiny může být v libovolné síti (skupinová adresa)
- **IP address ::= { network , host }**
 - { network , 0 } – “This” Network
 - { network , -1 } – Directed Broadcast
 - { -1 , -1 } – Limited Broadcast, pouze jako cílová adresa
 - { 0 , 0 } – All Zeros IP Address, pouze jako zdrojová adresa
 - { 0 , host } – IP address on This Network
 - { 127 , <any> } – Software Loopback

Subnetting

- V průběhu 80 let RFC 917, RFC 950
- Zavedlo mechanismus podsítě
- **Maska podsítě (subnet mask)**
 - 32 bitové číslo (255.255.255.192)
 - Kde je hranice mezi adresou podsítě a adresou hosta
- Původně $a \ll 0$ nebo $a \ll 1$ v adrese podsítě nebyly povolené, později ano viz. RFC 1812

Subnetting sítě B třídy

<i>Number of Bits in Network Addresses Prefix</i>	<i>Subnet Mask</i>	<i>Number of Usable Subnet</i>	<i>Number of Usable Host Addresses, Per Subnet</i>
2	255.255.192.0	4	16,382
3	255.255.224.0	8	8,190
4	255.255.240.0	16	4,094
5	255.255.248.0	32	2,046
6	255.255.252.0	64	1,022
7	255.255.254.0	128	510
8	255.255.255.0	256	254
9	255.255.255.128	512	126
10	255.255.255.192	1,024	62
11	255.255.255.224	2,048	30
12	255.255.255.240	4,096	14
13	255.255.255.248	8,192	6
14	255.255.255.252	16,384	2

Příklad subnetting

- Síť $193.168.125.0/24$ rozdělte na 8 podsítí /27!

<i>Network #</i>	<i>Binary Address</i>	<i>Decimal Address</i>
Base	11000001.10101000.01111101.00000000	193.168.125.0
Subnet 0	11000001.10101000.01111101.000-00000	193.168.125.0
Subnet 1	11000001.10101000.01111101.001-00000	193.168.125.32
Subnet 2	11000001.10101000.01111101.010-00000	193.168.125.64
Subnet 3	11000001.10101000.01111101.011-00000	193.168.125.96
Subnet 4	11000001.10101000.01111101.100-00000	193.168.125.128
Subnet 5	11000001.10101000.01111101.101-00000	193.168.125.160
Subnet 6	11000001.10101000.01111101.110-00000	193.168.125.192
Subnet 7	11000001.10101000.01111101.111-00000	193.168.125.224

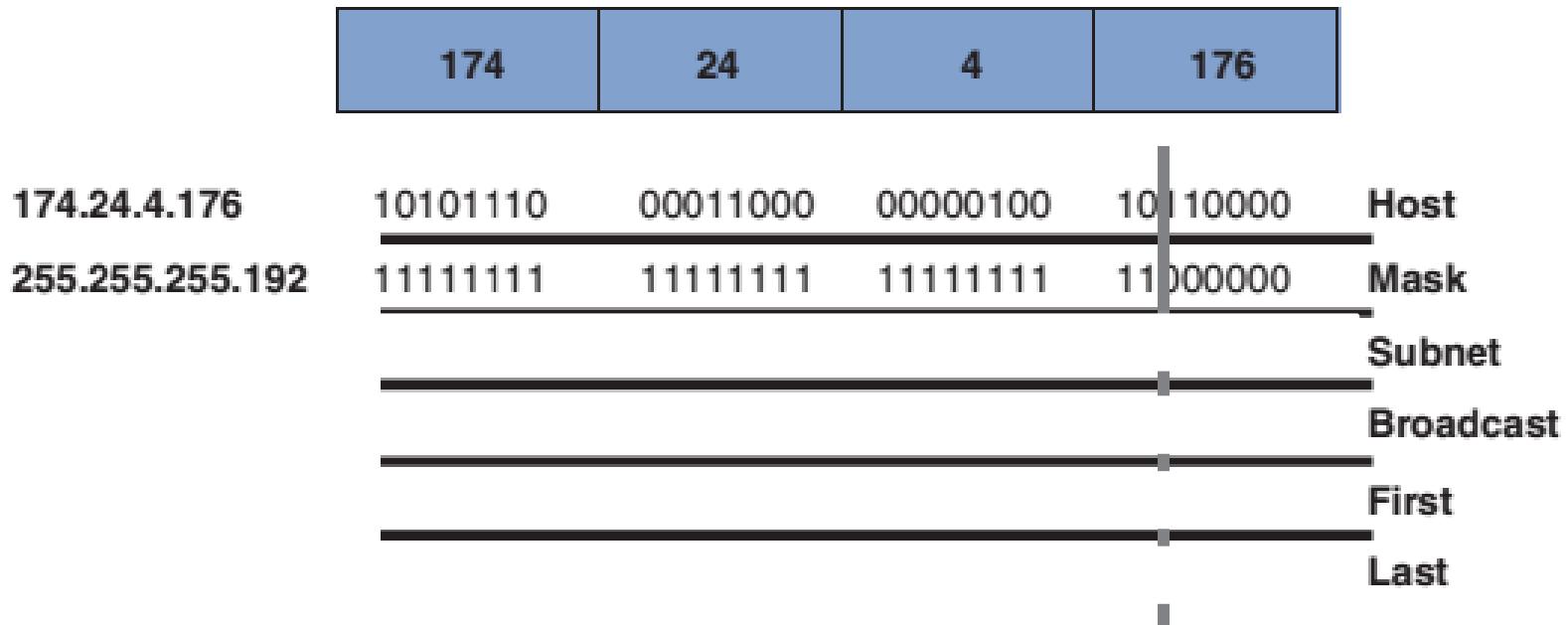
Příklady ①

- Jaká je adresa sítě, do které patří host s adresou 172.16.2.160/26?*

Network	Subnet	Host
172.16.2.160	10101100	00000010
255.255.255.192	11111111	11111111

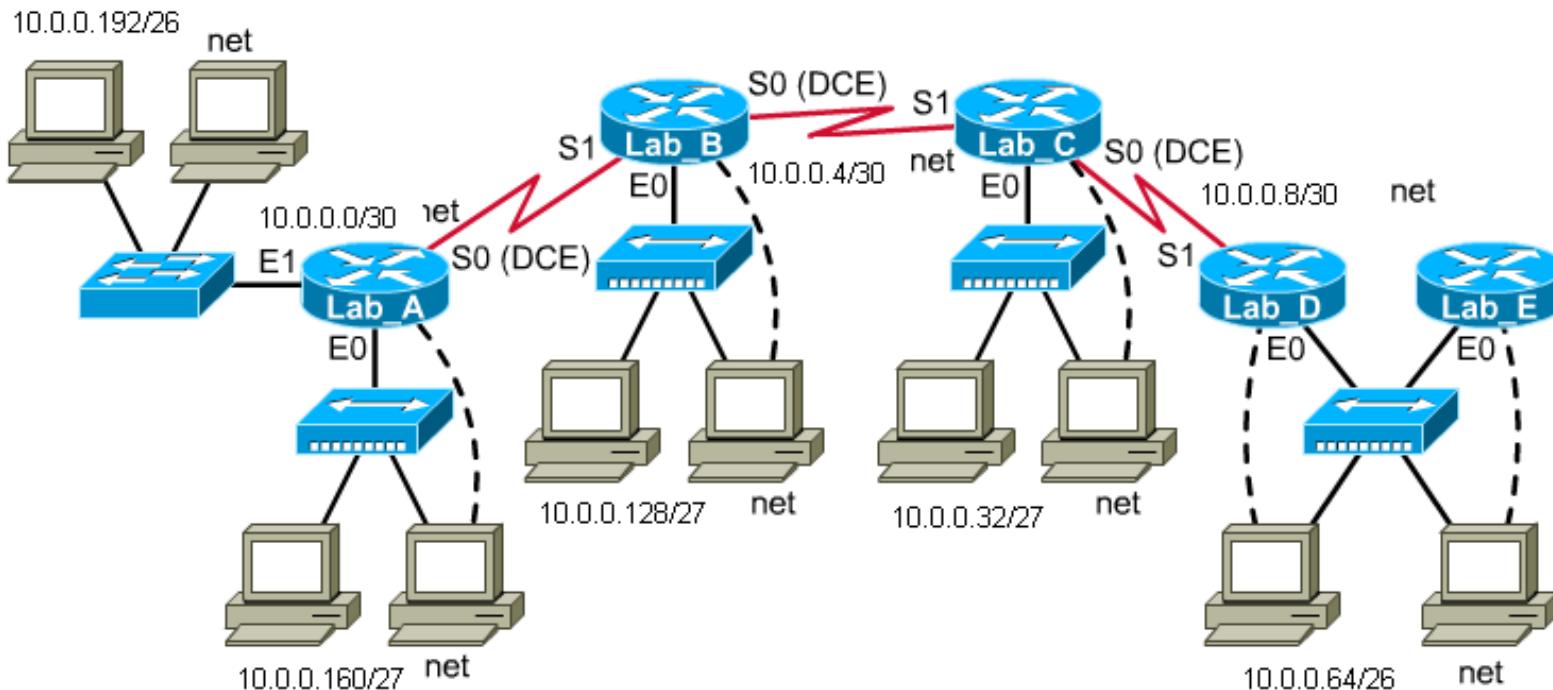
Příklady ②

- Spočítejte adresu sítě, broadcastovou adresu a první + poslední použitelnou hostovskou adresu, pokud vám je zadána IP 174.24.4.176/26!*



Příklady ③

- Rozdělte síť $10.0.0.0/24$ na podsítě tak, aby platilo:
 - A, B, C spojnice pro 2 hosty / D, E, F pro 30 hostů / G, H pro 62 hostů



Router Name - Lab_A
Router Type - 2514
E0 = 10.0.0.161
E1 = 10.0.0.193
S0 = 10.0.0.1

Router Name - Lab_B
Router Type - 2503
E0 = 10.0.0.129
S0 = 10.0.0.5
S1 = 10.0.0.2

Router Name - Lab_C
Router Type - 2503
E0 = 10.0.0.33
S0 = 10.0.0.9
S1 = 10.0.0.6

Router Name - Lab_D
Router Type - 2501
E0 = 10.0.0.65
S1 = 10.0.0.10

Router Name - Lab_E
Router Type - 2501
E0 = 10.0.0.66

Pomůcky (1)

/slash	# Hosts	Netmask	Wildcard
/30	4	255.255.255.252	0.0.0.3
/29	8	255.255.255.248	0.0.0.7
/28	16	255.255.255.240	0.0.0.15
/27	32	255.255.255.224	0.0.0.31
/26	64	255.255.255.192	0.0.0.63
/25	128	255.255.255.128	0.0.0.127
/24	256	255.255.255.0	0.0.0.255
/23	512	255.255.254.0	0.0.1.255
/22	1,024	255.255.252.0	0.0.3.255
/21	2,048	255.255.248.0	0.0.7.255
/20	4,096	255.255.240.0	0.0.15.255
/19	8,192	255.255.224.0	0.0.32.255
/18	16,384	255.255.192.0	0.0.63.255
/17	32,768	255.255.128.0	0.0.127.255
/16	65,536	255.255.0.0	0.0.255.255
/15	131,072	255.254.0.0	0.1.255.255
/14	262,144	255.252.0.0	0.3.255.255
/13	524,288	255.248.0.0	0.7.255.255
/12	1,048,576	255.240.0.0	0.15.255.255
/11	2,097,152	255.224.0.0	0.31.255.255
/10	4,194,304	255.192.0.0	0.63.255.255
/9	8,388,608	255.128.0.0	0.127.255.255
/8	16,777,216	255.0.0.0	0.255.255.255

Subnet mask quick reference							
Host Bit length	math	Max hosts	Subnet mask	Mask octet	Binary mask	Mask length	Subnet length
0	$2^0 =$	1	255.255.255. 255	4	11111111	32	0
1	$2^1 =$	2	255.255.255. 254	4	11111110	31	1
2	$2^2 =$	4	255.255.255. 252	4	11111100	30	2
3	$2^3 =$	8	255.255.255. 248	4	11111000	29	3
4	$2^4 =$	16	255.255.255. 240	4	11110000	28	4
5	$2^5 =$	32	255.255.255. 224	4	11100000	27	5
6	$2^6 =$	64	255.255.255. 192	4	11000000	26	6
7	$2^7 =$	128	255.255.255. 128	4	10000000	25	7
8	$2^8 =$	256	255.255. 255.0	3	11111111	24	8
9	$2^9 =$	512	255.255. 254.0	3	11111110	23	9
10	$2^{10} =$	1024	255.255. 252.0	3	11111100	22	10
11	$2^{11} =$	2048	255.255. 248.0	3	11111000	21	11
12	$2^{12} =$	4096	255.255. 240.0	3	11110000	20	12
13	$2^{13} =$	8192	255.255. 224.0	3	11100000	19	13
14	$2^{14} =$	16384	255.255. 192.0	3	11000000	18	14
15	$2^{15} =$	32768	255.255. 128.0	3	10000000	17	15
16	$2^{16} =$	65536	255. 255.0.0	2	11111111	16	16
17	$2^{17} =$	131072	255. 254.0.0	2	11111110	15	17
18	$2^{18} =$	262144	255. 252.0.0	2	11111100	14	18
19	$2^{19} =$	524288	255. 248.0.0	2	11111000	13	19
20	$2^{20} =$	1048576	255. 240.0.0	2	11110000	12	20
21	$2^{21} =$	2097152	255. 224.0.0	2	11100000	11	21
22	$2^{22} =$	4194304	255. 192.0.0	2	11000000	10	22
23	$2^{23} =$	8388608	255. 128.0.0	2	10000000	9	23
24	$2^{24} =$	16777216	255.0.0.0	1	11111111	8	24

<http://c128.com/sites/default/files/field/image/netmask.JPG>

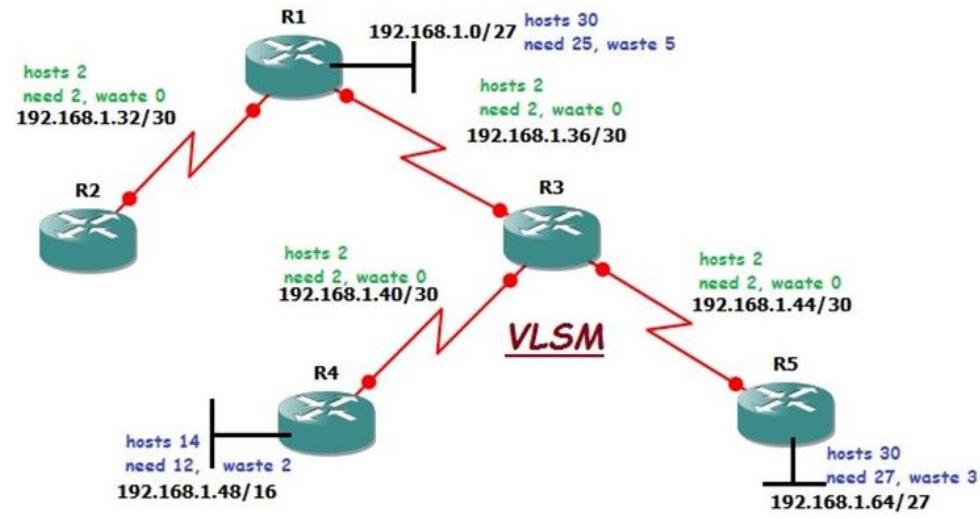
<https://s-media-cache-ak0.pinimg.com/564x/9b/df/d9/bdfd9263fbebe0be625266acf9be292.jpg>

Pomůcky (2)

	/25 255.255.255.128	/26 255.255.255.192	/27 255.255.255.224	/28 255.255.255.240	/29 255.255.255.248	/30 255.255.255.252
.0						
.4						
.8						
.12						
.16						
.20						
.24						
.28						
.32						
.36						
.40						
.44						
.48						
.52						
.56						
.60						
.64						
.68						
.72						
.76						
.80						
.84						
.88						
.92						
.96						
.100						
.104						
.108						
.112						
.116						
.120						
.124						
.128						
.132						
.136						
.140						
.144						
.148						
.152						
.156						
.160						
.164						
.168						
.172						
.176						
.180						
.184						
.188						
.192						
.196						
.200						
.204						
.208						
.212						
.216						
.220						
.224						
.228						
.232						
.236						
.240						
.244						
.248						
.252						
	/25 (1 subnet bit)	/26 (2 subnet bits)	/27 (3 subnet bits)	/28 (4 subnet bits)	/29 (5 subnet bits)	/30 (6 subnet bits)
	1 subnet	3 subnets	7 subnet	15 subnet	31 subnet	62 hosts
	126 hosts		30 hosts	14 hosts	6 hosts	2 hosts

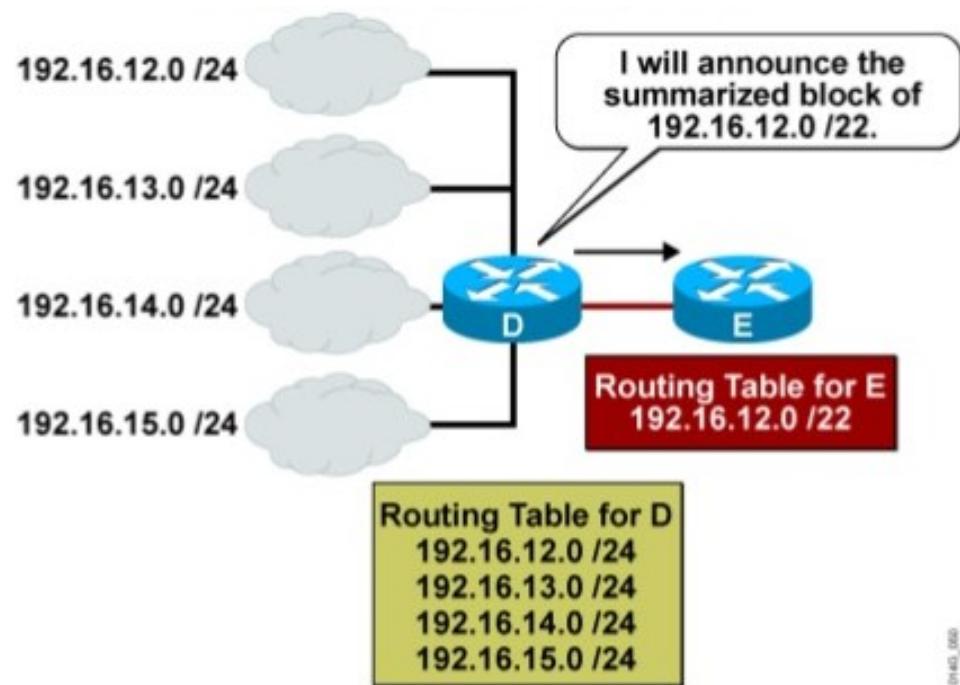
VLSM

- Variable Length Subnet Mask (v roce 1987, RFC 1009)
- Efektivnější využití adresového prostoru
- Extended network prefix
 - 147.229.176.14/23
 - 23 počet bitů masky 255.255.254.0
- Adresa bez masky nedává smysl
- „Přidávání bitů zprava“



CIDR

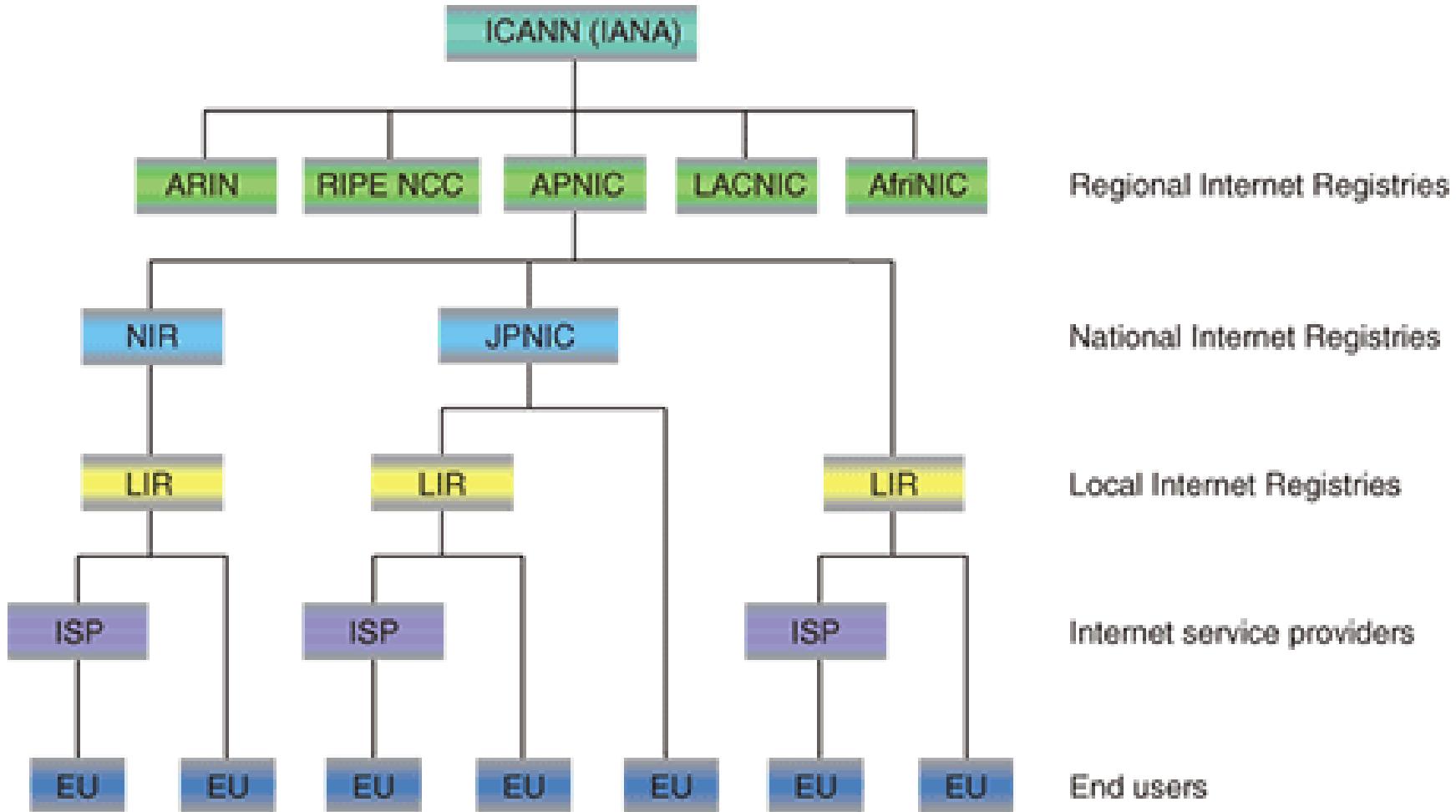
- Classless Interdomain Routing
- V roce 1992
 - Téměř vyčerpání B třídy adres
 - Směrovací tabulky příliš velké
- V roce 1993
 - Agregace adres pro směrování
 - Supernetting
 - Eliminace classfull adresování
 - RFC 1517 až 1520
 - „Přidávání bitů zleva“
- RFC 1918
 - Malá úprava: třída A je teď identifikována jako x/8, B jako x.y/16 ...



Obsah

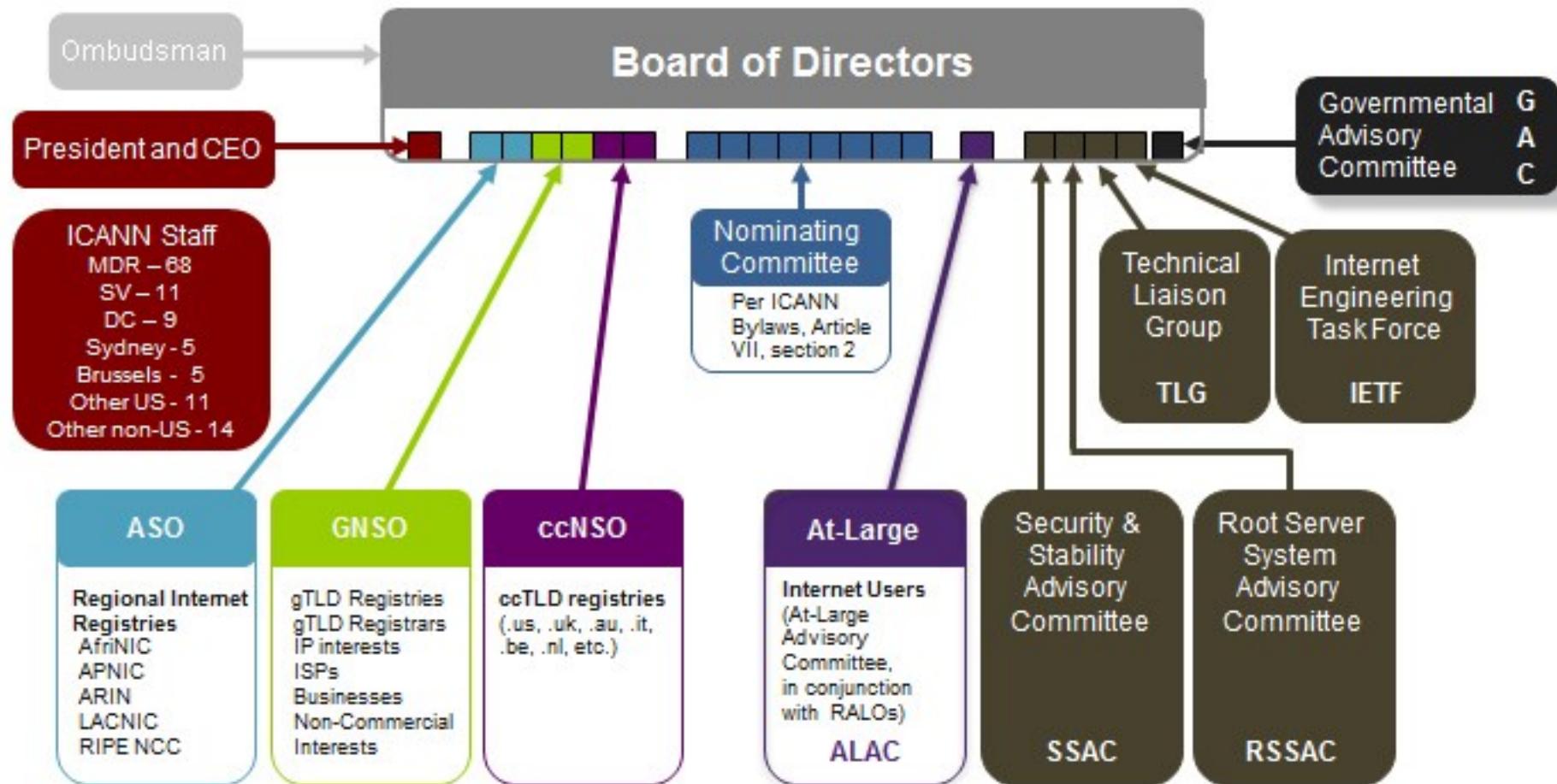
- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

Hráči



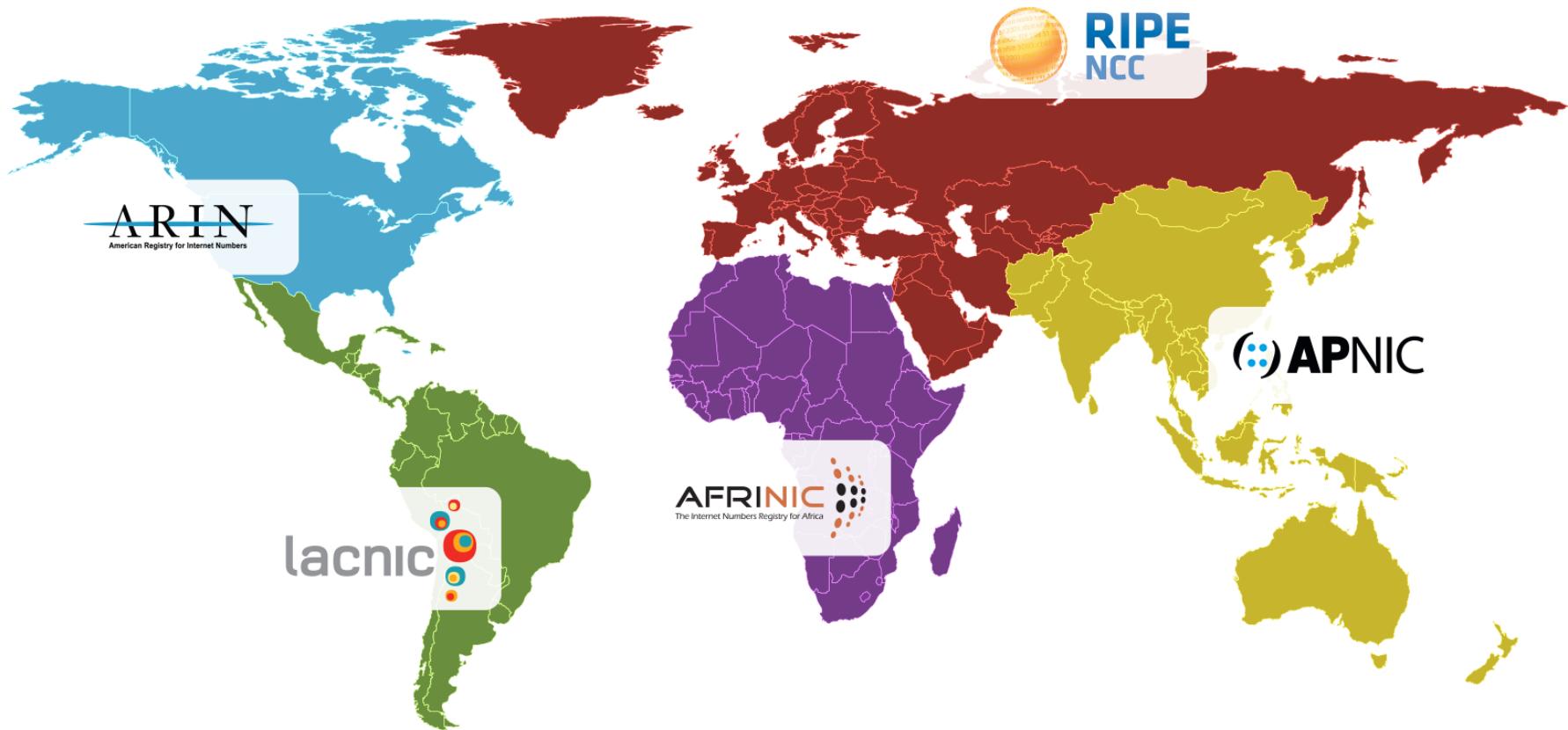
- https://www.internetsociety.org/wp-content/uploads/2016/05/IANA_Timeline_20170117.pdf

ICANN

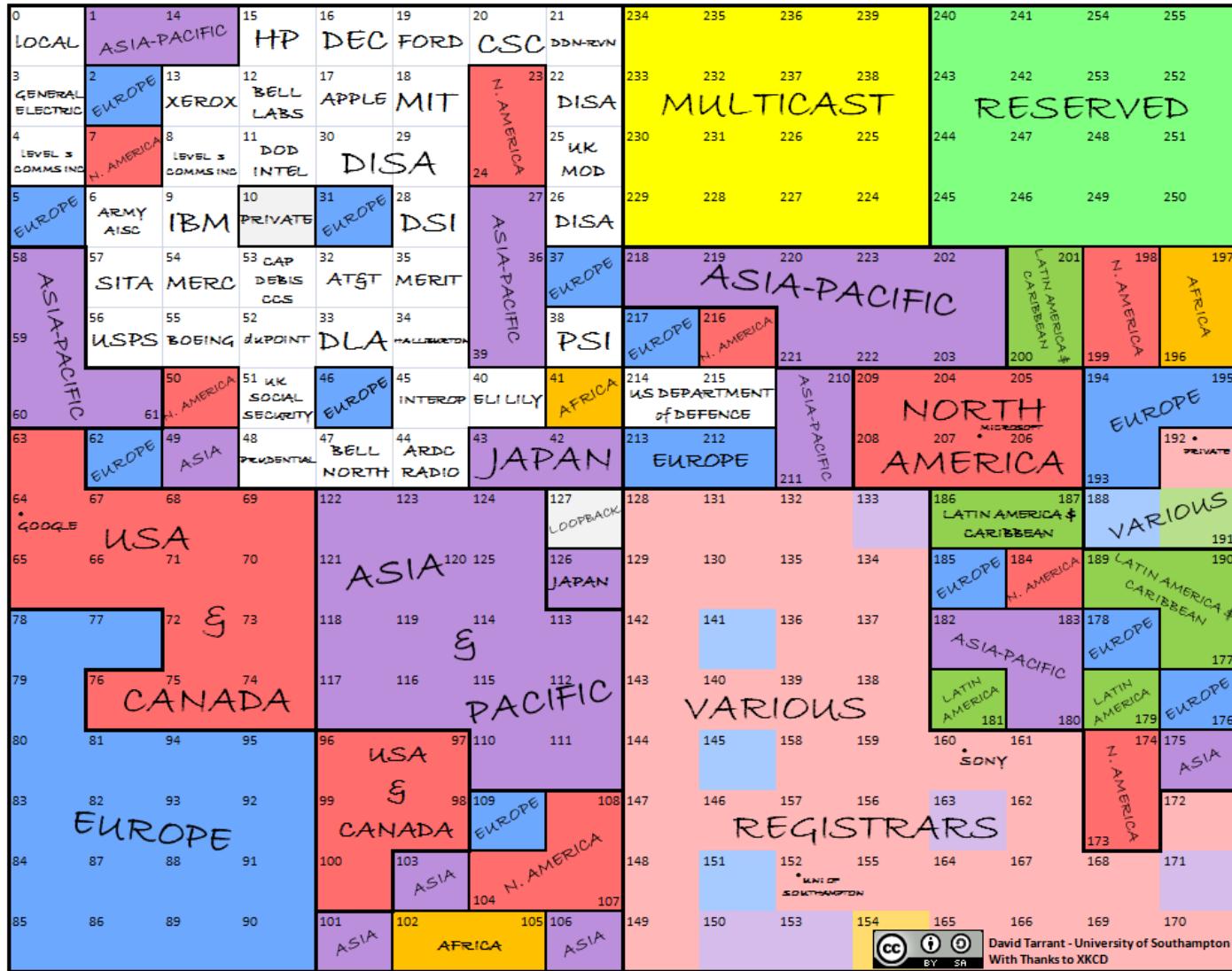


IPv4 adresní prostor

- O rozdělování adres se starají nadnárodní registrátoři

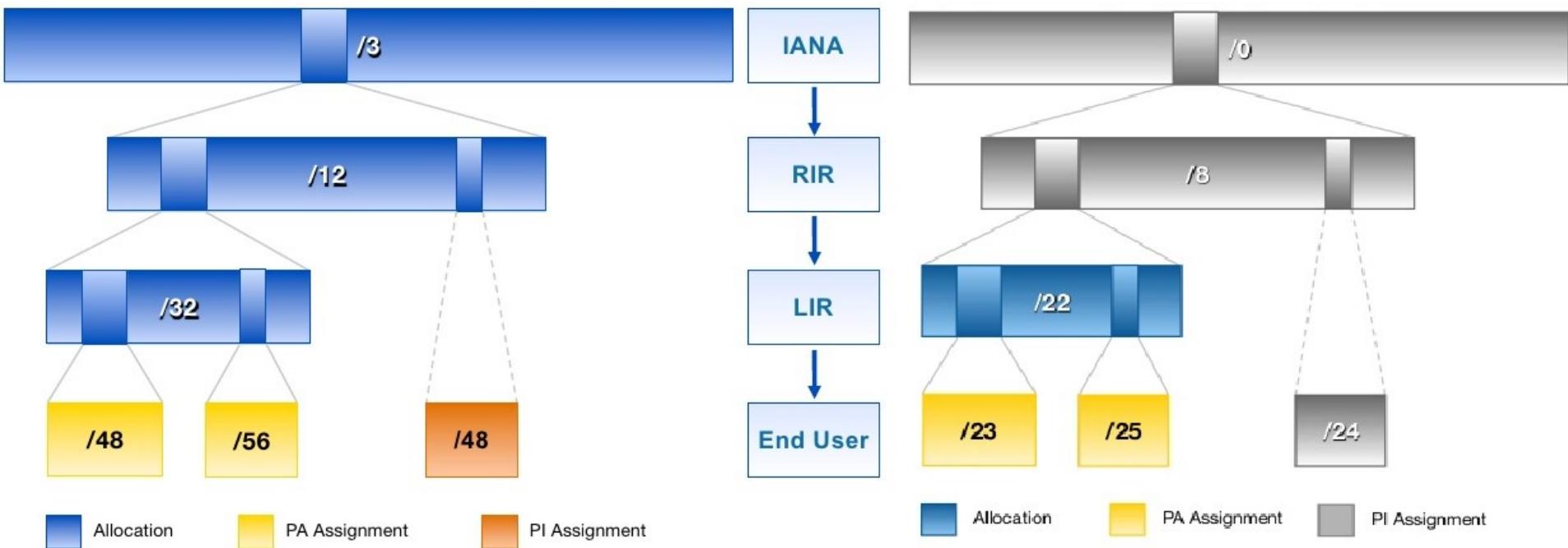


IPv4 adresní prostor



David Tarrant - University of Southampton
With Thanks to XKCD

Delegace IP prostoru



IPv4 sítě na páteři

- <https://ipv4.potaroo.net/> a <http://bgp.potaroo.net/as6447/>
- <http://routeserver.org/>

```
route-views.routeviews.org - PuTTY
BGP router identifier 128.223.51.103, local AS number 6447
BGP table version is 68135525, main routing table version 68135525
787893 network entries using 195397464 bytes of memory
23934128 path entries using 2872095360 bytes of memory
3616548/130500 BGP path/bestpath attribute entries using 896903904 bytes of memory
3346798 BGP AS-PATH entries using 169530898 bytes of memory
3 BGP ATTR_SET entries using 120 bytes of memory
101436 BGP community entries using 12157590 bytes of memory
859 BGP extended community entries using 55066 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4146140282 total bytes of memory
BGP activity 3073719/2217489 prefixes, 218184206/192401772 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent     TblVer  InQ OutQ Up/Down State/PfxRcd
4.69.184.193  4      3356      0      0      1      0      0  6w4d   Active
5.101.110.2   4      14061     0      0      1      0      0  never   Active
12.0.1.63     4      7018  33391166  129913  68135543  0      0  11w5d  724660
37.139.139.0  4      57866    1806957  4506  68135543  0      0  1d10h  729532
64.71.137.241 4      6939  18016190  129896  68135543  0      0  11w5d  754266
66.59.190.221 4      6539      0      0      1      0      0  never   Active
66.110.0.86   4      6453      0      0      1      0      0  never   Active
66.185.128.48 4      1668      0      0      1      0      0  never   Active
69.31.111.244 4      4436      0      0      1      0      0  never   Active
80.241.176.31 4      20771     0      0      1      0      0  never   Idle
89.149.178.10 4      3257      0      0      1      0      0  4d13h  Active
91.218.184.60 4      49788    27264246  97713  68135543  0      0  11w5d  731188
94.142.247.3  4      8283  172221593  10241  68135543  0      0  1w1d   732708
95.85.0.2     4      14061     0      0      1      0      0  never   Active
--More--
```

Date

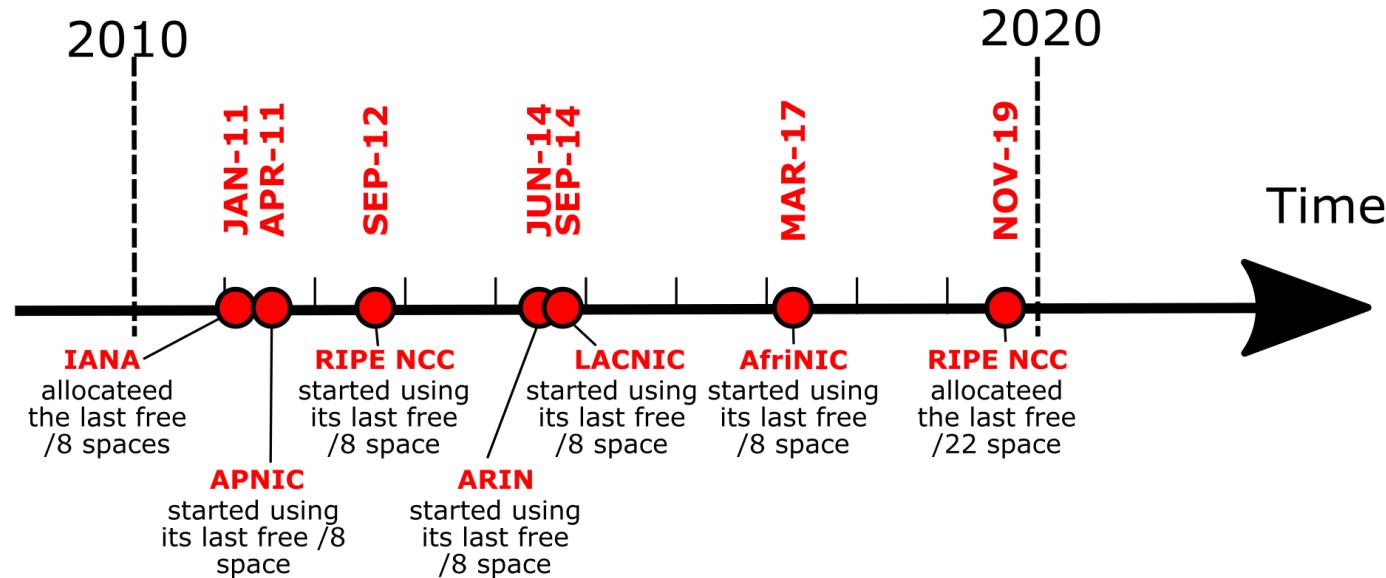
Veřejné a privátní adresy

- Pokud síť není připojená k Internetu, můžeme použít libovolné adresy
- RFC 1597
 - definuje privátní adresy (neroutovatelné v Internetu)
 - pro privátní použití
 - může použít každý v Internetu, adresy se nepoužívají mimo Vaši síť
 - Třída A: 10.0.0.0–10.255.255.255
 - Třída B: 172.16.0.0–172.31.255.255
 - Třída C: 192.168.0.0–192.168.255.255
- Special-Use addresses
 - RFC 3330
 - Několik další adres sítí rezervovaných
 - 169.254.0.0/16 „link-local address block“ aka Zeroconf viz. RFC 3927

Rezervované adresy

Address block	Range	Number of addresses	Scope	Purpose
0.0.0.0/8	0.0.0.0 – 255.255.255.255	16,777,216	Software	Used for broadcast messages to the current ("this") ^[1]
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16,777,216	Private network	Used for local communications within a private network ^[2]
100.64.0.0/10	100.64.0.0 – 100.127.255.255	4,194,304	Private network	Used for communications between a service provider and its subscribers when using a carrier-grade NAT ^[3]
127.0.0.0/8	127.0.0.0 – 127.255.255.255	16,777,216	Host	Used for loopback addresses to the local host ^[4]
169.254.0.0/16	169.254.0.0 – 169.254.255.255	65,536	Subnet	Used for link-local addresses between two hosts on a single link when no IP address is otherwise specified, such as would have normally been retrieved from a DHCP server ^[5]
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1,048,576	Private network	Used for local communications within a private network ^[2]
192.0.0.0/24	192.0.0.0 – 192.0.0.255	256	Private network	Used for the IANA IPv4 Special Purpose Address Registry ^[6]
192.0.2.0/24	192.0.2.0 – 192.0.2.255	256	Documentation	Assigned as "TEST-NET" for use in documentation and examples. It should not be used publicly. ^[7]
192.88.99.0/24	192.88.99.0 – 192.88.99.255	256	Internet	Used by 6to4 anycast relays ^[8]
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65,536	Private network	Used for local communications within a private network ^[2]
198.18.0.0/15	198.18.0.0 – 198.19.255.255	131,072	Private network	Used for testing of inter-network communications between two separate subnets ^[9]
198.51.100.0/24	198.51.100.0 – 198.51.100.255	256	Documentation	Assigned as "TEST-NET-2" for use in documentation and examples. It should not be used publicly. ^[7]
203.0.113.0/24	203.0.113.0 – 203.0.113.255	256	Documentation	Assigned as "TEST-NET-3" for use in documentation and examples. It should not be used publicly. ^[7]
224.0.0.0/4	224.0.0.0 – 239.255.255.255	268,435,456	Internet	Reserved for multicast ^[10]
240.0.0.0/4	240.0.0.0 – 255.255.255.254	268,435,456	Internet	Reserved for future use ^[11]
255.255.255.255/32	255.255.255.255	1	Subnet	Reserved for the "limited broadcast" destination address ^[11]

Nedostatek IPv4 adres



- Spekulování s IP adresami na prodej či pronájem je legitimní business
 - <https://www.google.com/search?q=ipv4+addresses+for+lease>

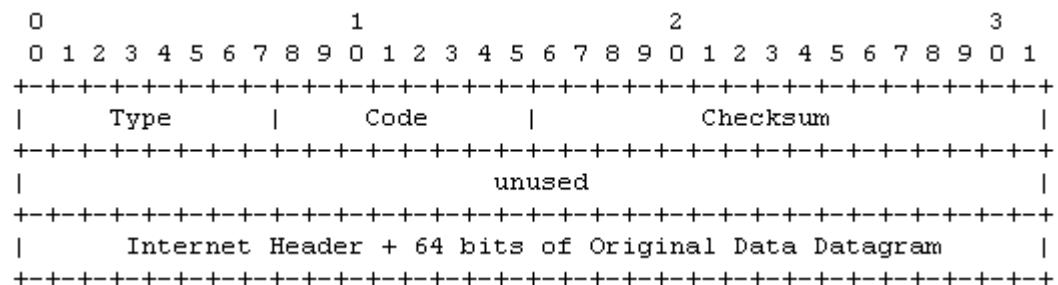


Obsah

- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

ICMP protokol

- Internet Control Message Protocol
- Používán hosty, směrovači pro oznámení chyb, diagnostiku sítě
 - Požadovaná služba není dosažitelná
 - Cílová síť/host je nedosažitelná
- RFC 792, STD [5]
- Obecně 2 typy zpráv
 - Oznámení chyby
 - Dotaz na službu
- ICMP data přenášena v IP datagramu



ICMP protokol

Type	Code	Description
0	0	echo reply (ping)
3	0	dest. network unreachable
3	1	dest host unreachable
3	2	dest protocol unreachable
3	3	dest port unreachable
3	6	dest network unknown
3	7	dest host unknown
4	0	source quench (congestion control - not used)
8	0	echo request (ping)
9	0	route advertisement
10	0	router discovery
11	0	TTL expired
12	0	bad IP header

Ping Aplikace

- ping

```
C:\ Příkazový řádek
C:\Users\Me>ping www.seznam.cz      ping www.seznam.cz <= požadavek na odezvu z cíle
Pinging www.seznam.cz [77.75.77.39] with 32 bytes of data:
Reply from 77.75.77.39: bytes=32 time=9ms TTL=248
Reply from 77.75.77.39: bytes=32 time=9ms TTL=248
Reply from 77.75.77.39: bytes=32 time=11ms TTL=248
Reply from 77.75.77.39: bytes=32 time=8ms TTL=248
Ping statistics for 77.75.77.39:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
   Approximate round trip times in milli-seconds.
         Minimum = 8ms, Maximum = 11ms, Average = 9ms

C:\Users\Me>ping 10.133.23.7
Pinging 10.133.23.7 with 32 bytes of data:
Reply from 10.133.23.34: Destination host unreachable.
```

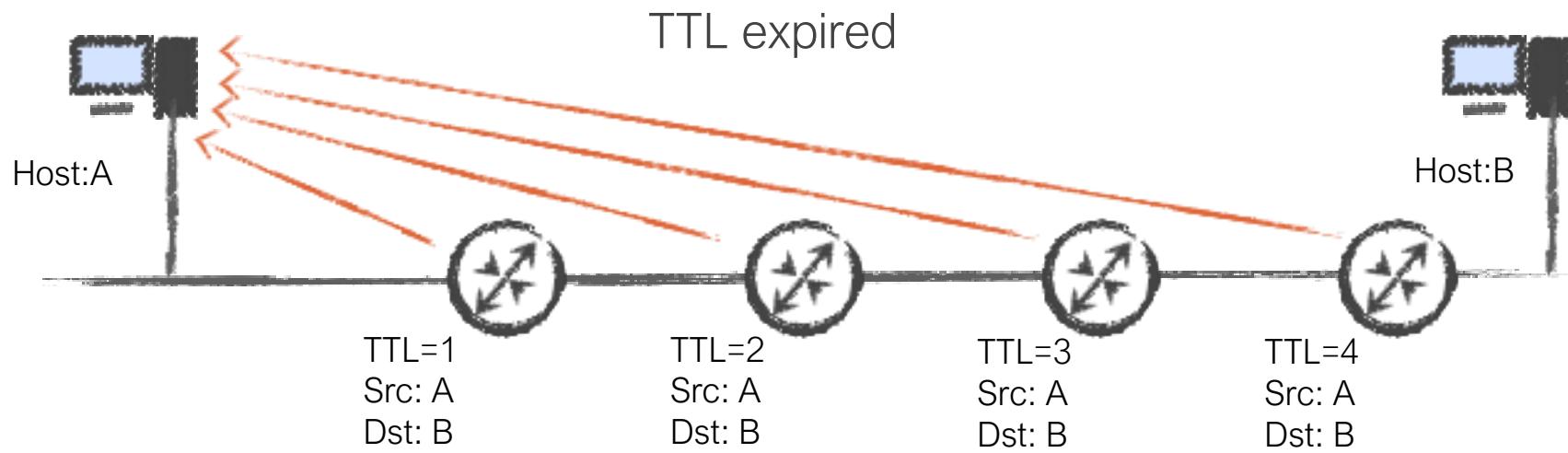
Jméno přeloženo na IP
adresu => funguje DNS

Statistika

Cíl je nedostupný
nebo neodpovídá

<http://www.pvfree.net/obrazky/diag-ping.png>

Traceroute



TraceRoute Aplikace

- Windows: tracert
- Unix: traceroute, mtr

C:\Users\Mordeth>tracert www.seznam.cz

Tracing route to www.seznam.cz [77.75.79.53]
over a maximum of 30 hops:

Hop	RTT (ms)	RTT (ms)	RTT (ms)	RTT (ms)	RTT (ms)
1	<1 ms	<1 ms	<1 ms	10.20.40.1	
2	1 ms	<1 ms	<1 ms	gw.vcit.vutbr.net [185.62.108.65]	
3	1 ms	1 ms	<1 ms	pe-ant.net.vutbr.cz [147.229.254.154]	
4	<1 ms	<1 ms	<1 ms	rt-ant.net.vutbr.cz [147.229.253.233]	
5	3 ms	3 ms	3 ms	213.195.192.247	
6	4 ms	3 ms	4 ms	nix4.seznam.cz [91.210.16.195]	
7	4 ms	4 ms	4 ms	n7k-ko-a-vdc-1-po1.seznam.cz [185.66.188.7]	
8	4 ms	4 ms	4 ms	n7k-ko-a-vdc-2-po3.seznam.cz [185.66.188.25]	
9	4 ms	3 ms	4 ms	www.seznam.cz [77.75.79.53]	

Trace complete.

		Pings				
		Min	Avg	Best	Wrst	StDev
9.	38.104.103.254	0.0%	38	17.6	17.8	10.1
	38.104.103.130					82.0
10.	209.85.254.128	5.3%	38	10.2	12.2	10.1
11.	209.85.250.30	0.0%	38	10.9	10.9	10.4
12.	ord08s07-in-f1.1e100.net	0.0%	38	10.2	10.5	10.2
						13.8
						0.6

ICMP ve Wiresharku

The screenshot shows the Wireshark interface with a list of captured ICMP frames. A terminal window is open next to it, displaying the results of a ping command.

Wireshark Filter: icmp

Terminal Output:

```
C:\Users\Zack> ping -n 10 www.ust.hk

Pinging www.ust.hk [143.89.14.34] with 32 bytes of data:
Reply from 143.89.14.34: bytes=32 time=238ms TTL=234
Reply from 143.89.14.34: bytes=32 time=235ms TTL=234
Reply from 143.89.14.34: bytes=32 time=240ms TTL=234
Reply from 143.89.14.34: bytes=32 time=236ms TTL=234
Reply from 143.89.14.34: bytes=32 time=235ms TTL=234
Reply from 143.89.14.34: bytes=32 time=242ms TTL=234
Reply from 143.89.14.34: bytes=32 time=235ms TTL=234
Reply from 143.89.14.34: bytes=32 time=235ms TTL=234
Reply from 143.89.14.34: bytes=32 time=238ms TTL=234
Reply from 143.89.14.34: bytes=32 time=235ms TTL=234

Ping statistics for 143.89.14.34:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 235ms, Maximum = 242ms, Average = 236ms
```

<https://zaccouplet.files.wordpress.com/2012/05/wsicmp.png>

Obsah

- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- Překlad adres, NAT

DHCP

- Dynamic Host Configuration Protocol
- Rozšíření původního BOOTP protokolu (pro bezdiskové stanice)
- DHCP klient / DHCP server
- Poskytuje:
 - Mechanismus přidělení IP adresy a TCP/IP parametrů
 - Dohodu a přenos specifických informací pro hosta
- Aplikační protokol !
- UDP, porty 67 a 68

DHCP Discover

DHCP Discover

ETH:

```
src mac: AA:AA:AA:AA:AA:AA  
dst mac: FF:FF:FF:FF:FF:FF  
(broadcast)
```

IP

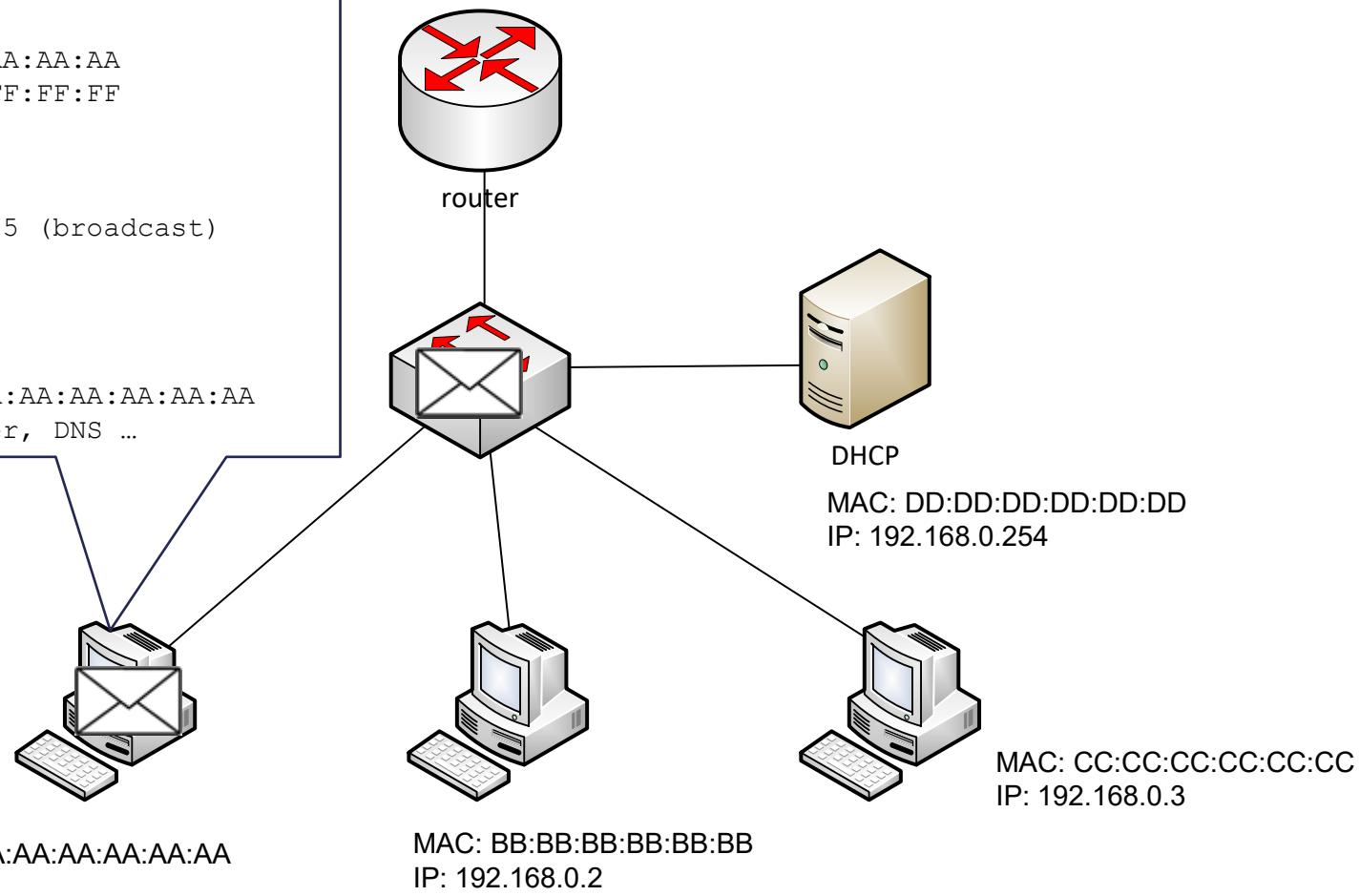
```
src: 0.0.0.0  
dst: 255.255.255.255 (broadcast)
```

UDP

```
src port 68  
dst port 67
```

DHCP

```
Client MAC addr: AA:AA:AA:AA:AA:AA  
Requests: IP, Router, DNS ...
```

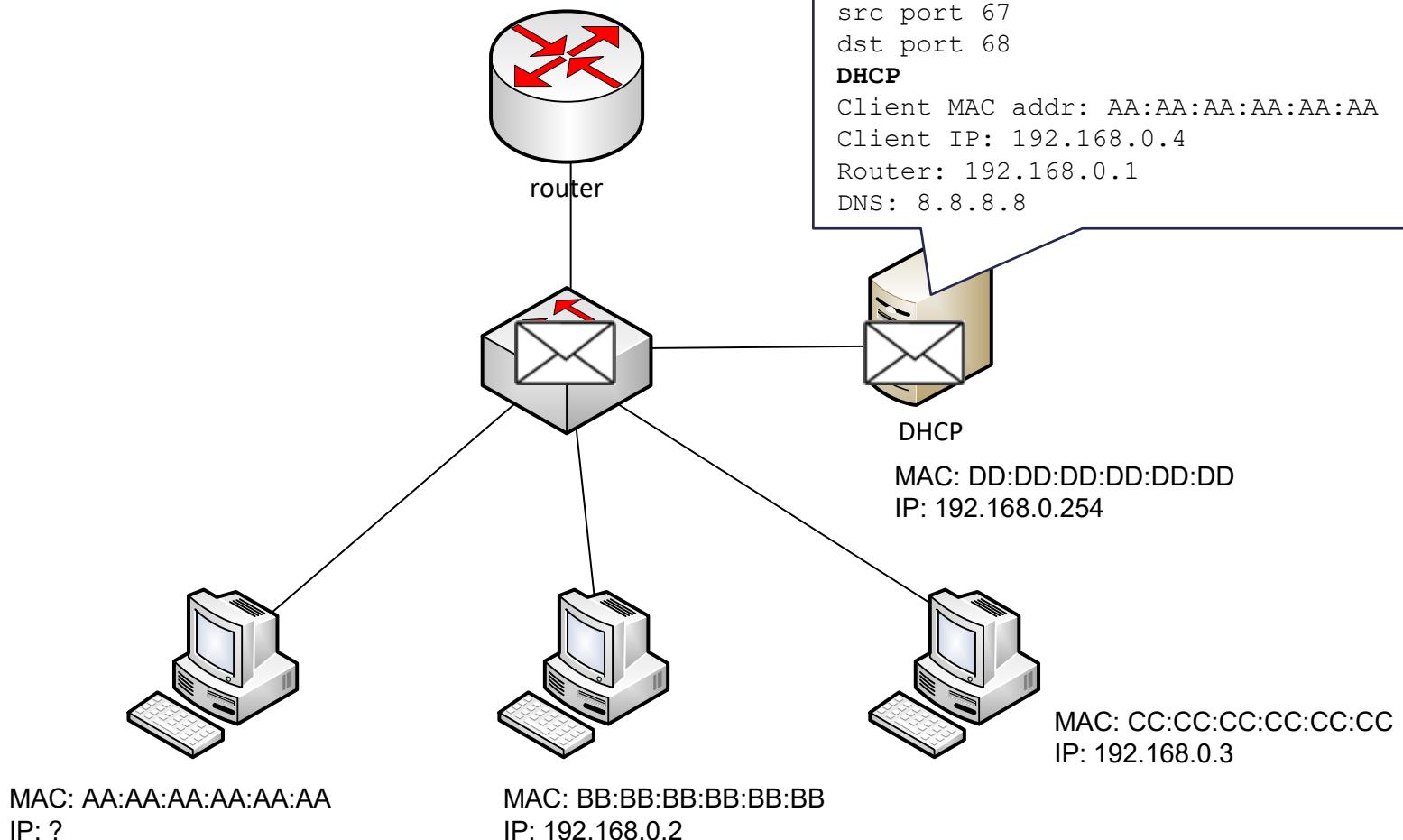


MAC: AA:AA:AA:AA:AA:AA
IP: ?

MAC: BB:BB:BB:BB:BB:BB
IP: 192.168.0.2

MAC: CC:CC:CC:CC:CC:CC
IP: 192.168.0.3

DHCP Offer



DHCP Request

DHCP Request

ETH:

```
src mac: AA:AA:AA:AA:AA:AA  
dst mac: FF:FF:FF:FF:FF:FF  
(broadcast)
```

IP

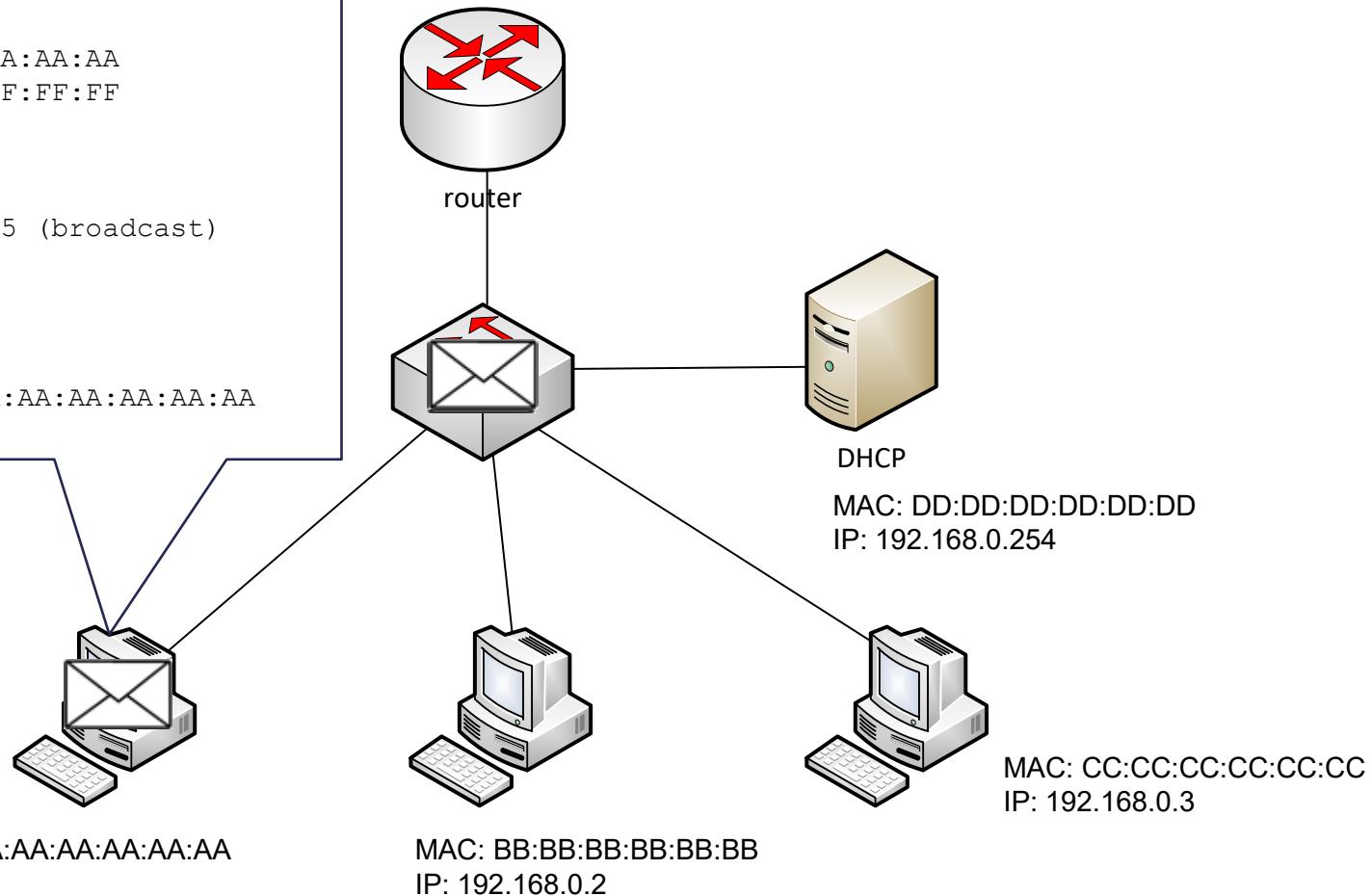
```
src: 0.0.0.0  
dst: 255.255.255.255 (broadcast)
```

UDP

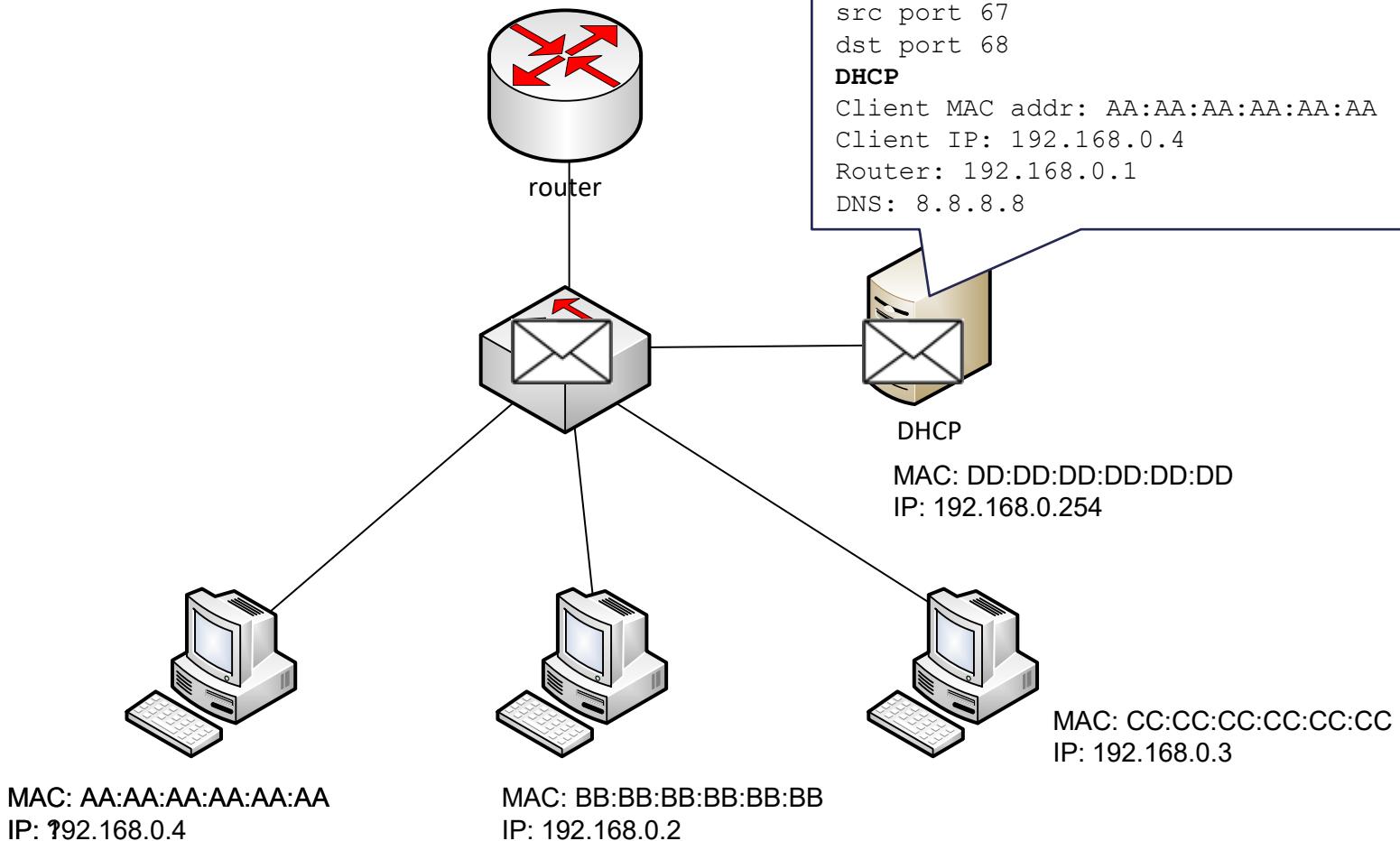
```
src port 68  
dst port 67
```

DHCP

```
Client MAC addr: AA:AA:AA:AA:AA:AA  
IP, Router, DNS ...
```

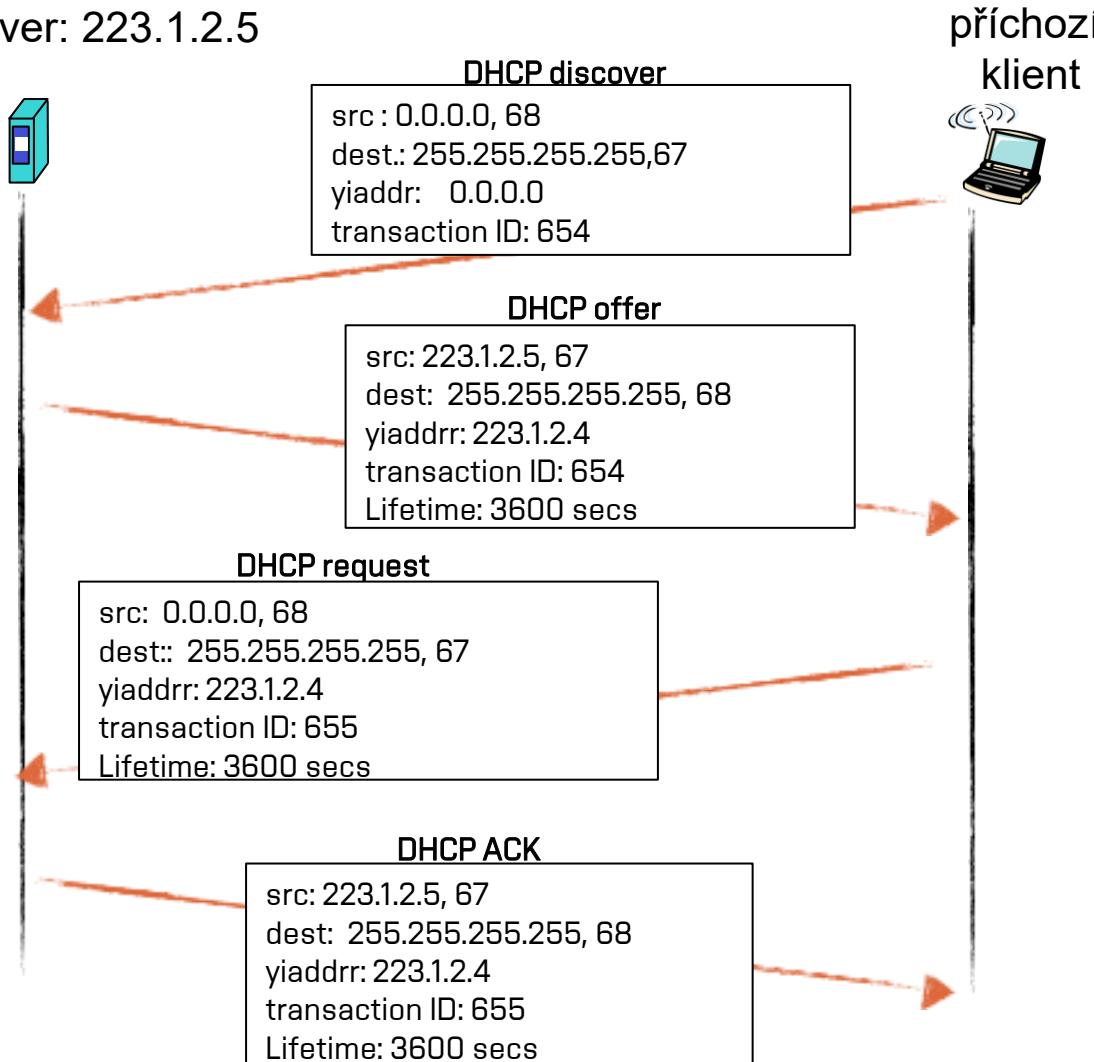


DHCP Ack

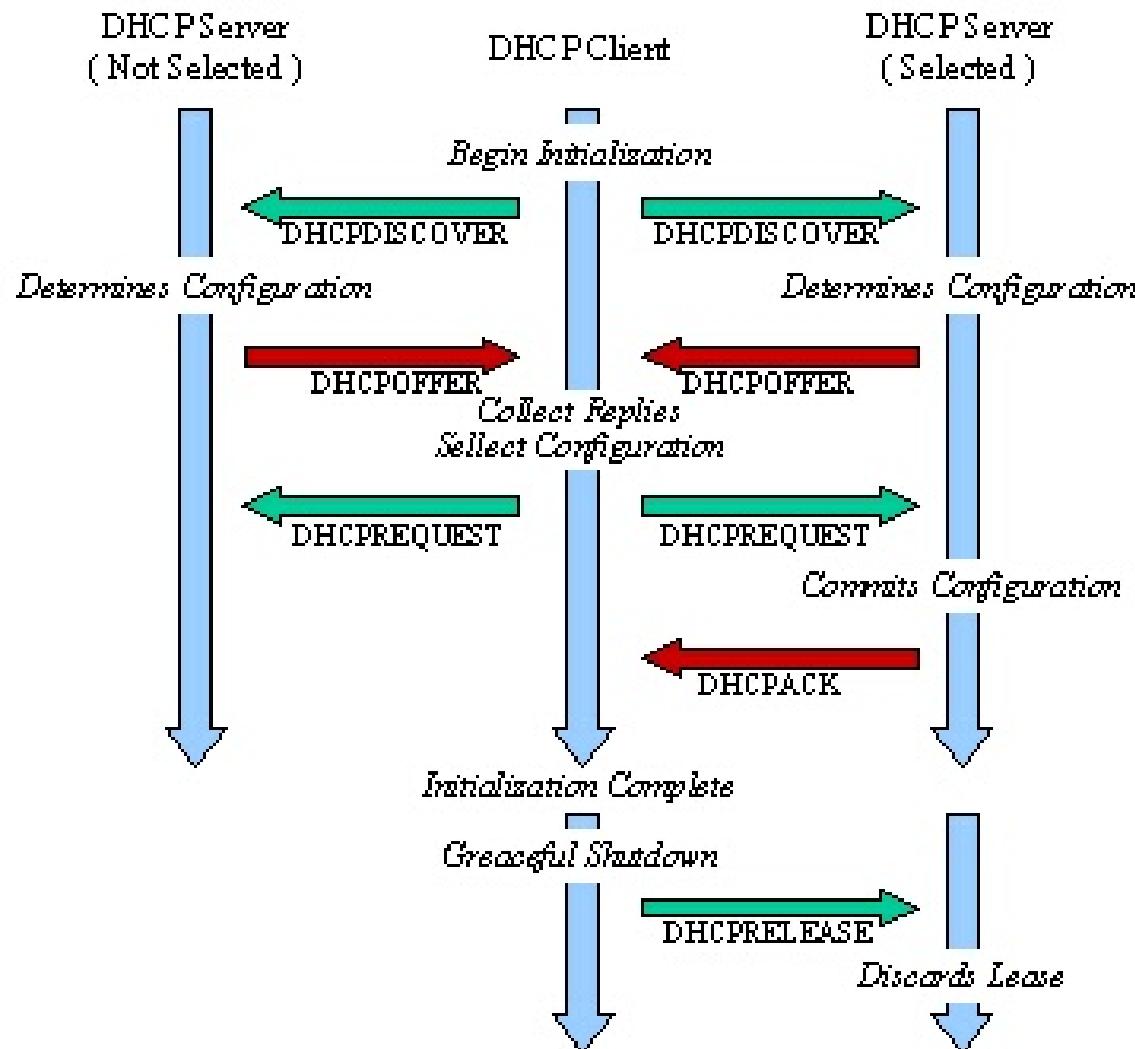


DHCP Server Bcast příklad

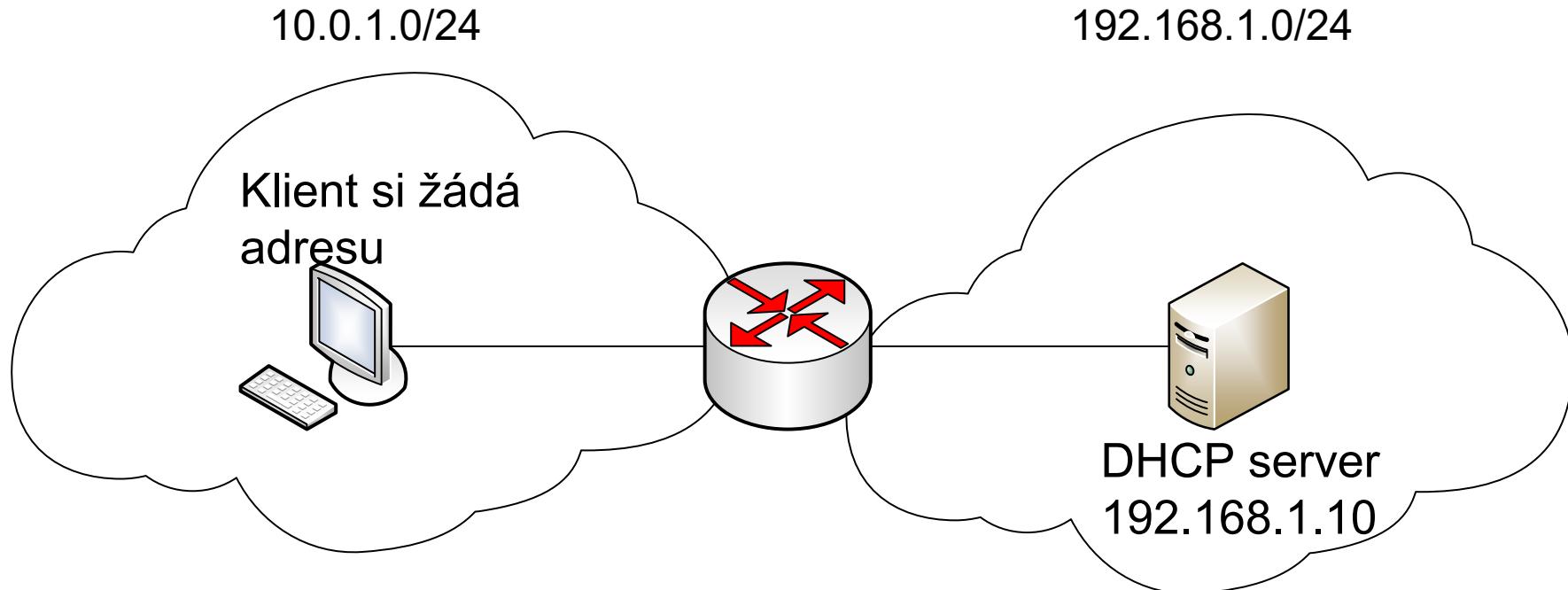
DHCP server: 223.1.2.5



Proč DHCP broadcastuje?

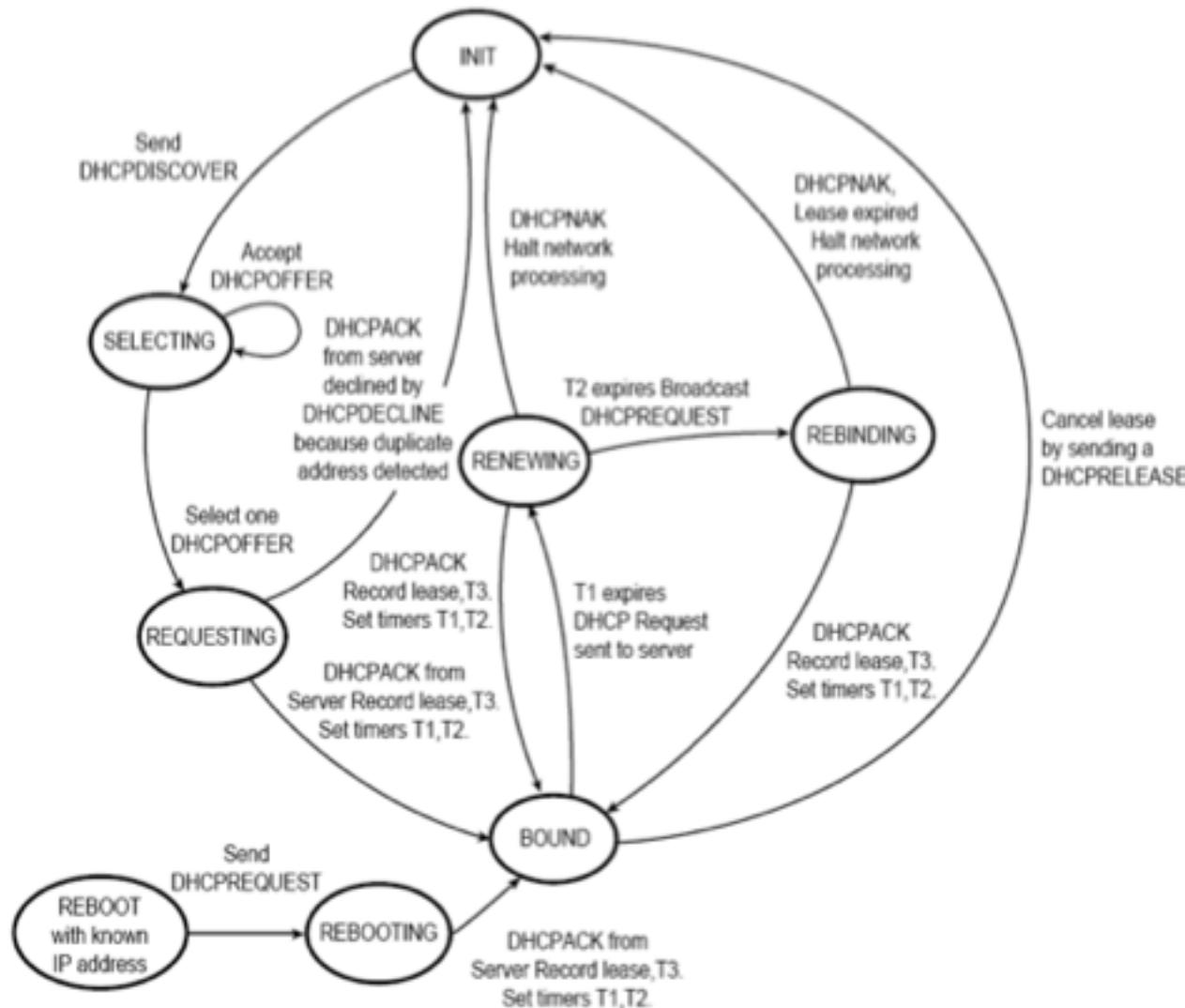


DHCP mimo subnet



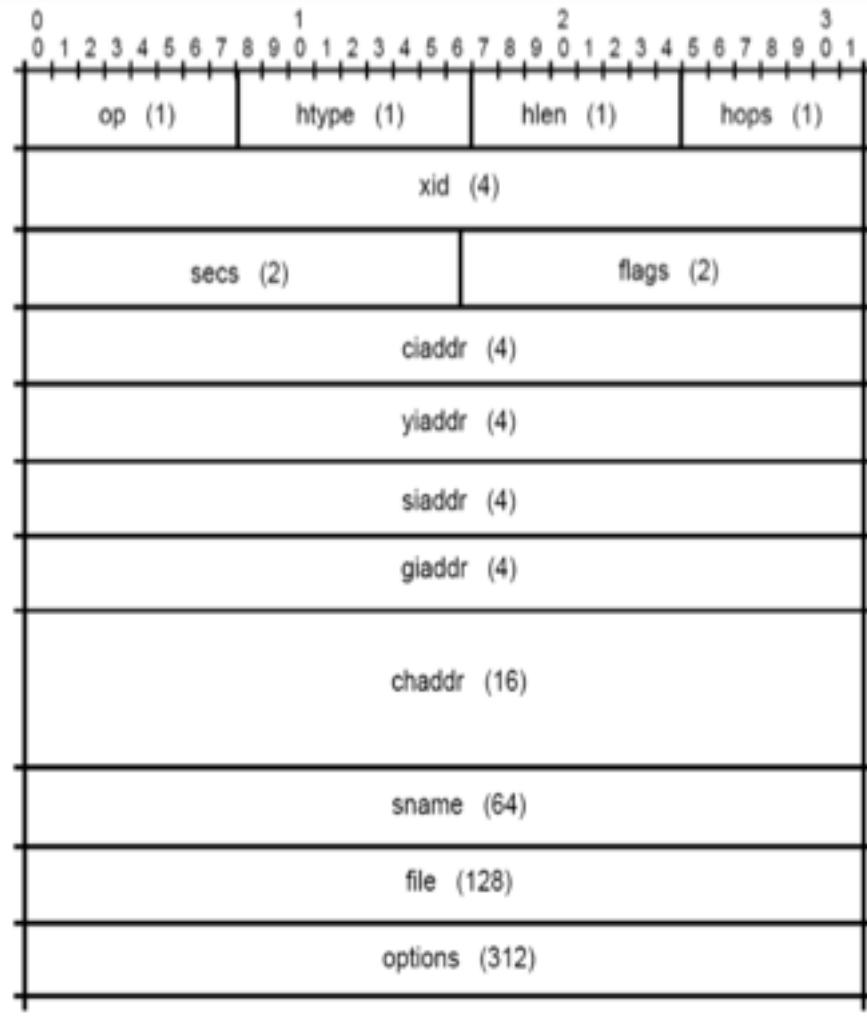
- Option-82

DHCP stavy a interakce

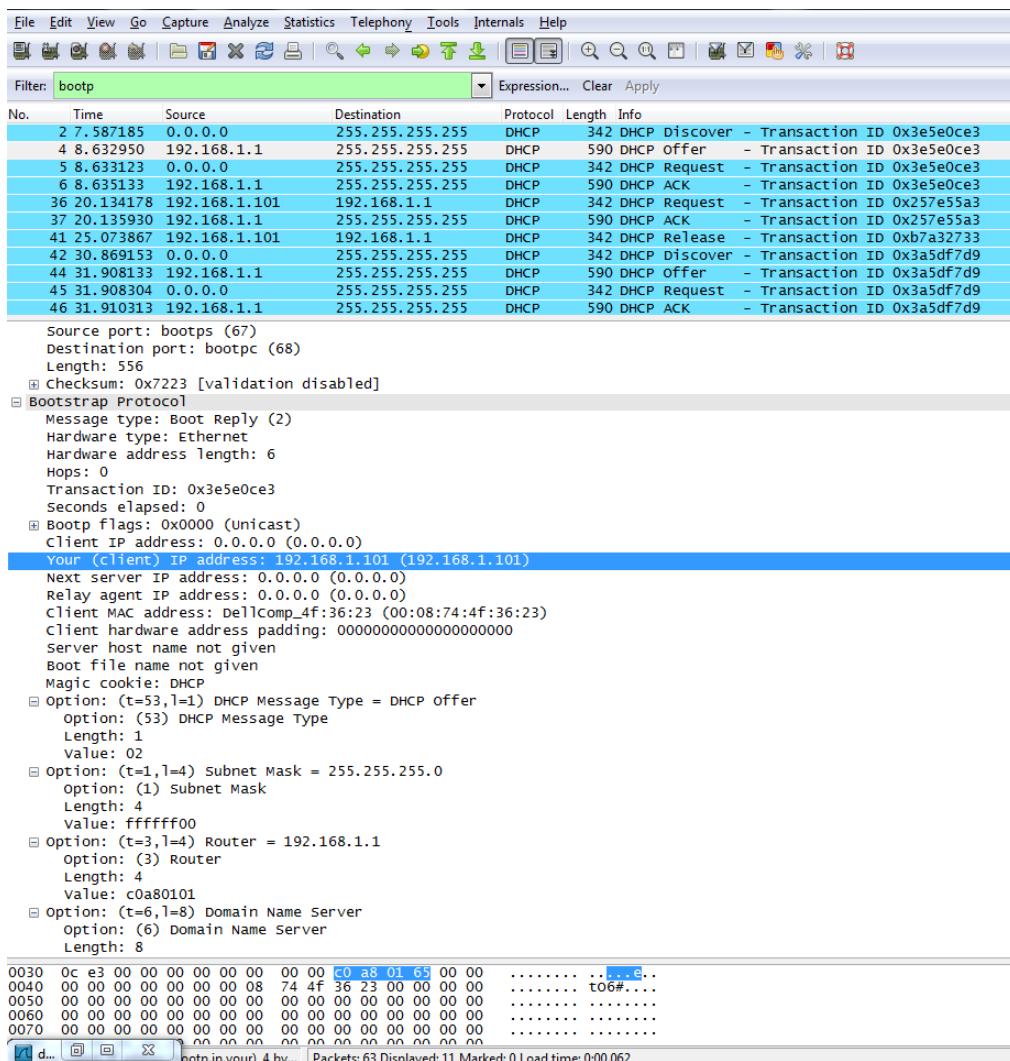


Formát DHCP zprávy

- op: dotaz nebo odpověď
- htype: typ hw adresy
- hlen: délka hw adresy v oktetech
- hops: počet skoku, pro DHCP relay
- xid: Transaction ID, náhodné číslo transakce
- secs: počet sekund od počátku bootování
- flags: broadcast nebo unicast
- ciaaddr: IP adresa klienta (v odpovědi)
- yiaddr: Your IP address, přiděluje server klientovi
- siaddr: IP adresa serveru
- giaddr: IP adresa relay agenta
- chaddr: HW adresa klienta
- sname:volitelně jméno serveru
- file: image filename
- options: další volby



DHCP ve Wiresharku

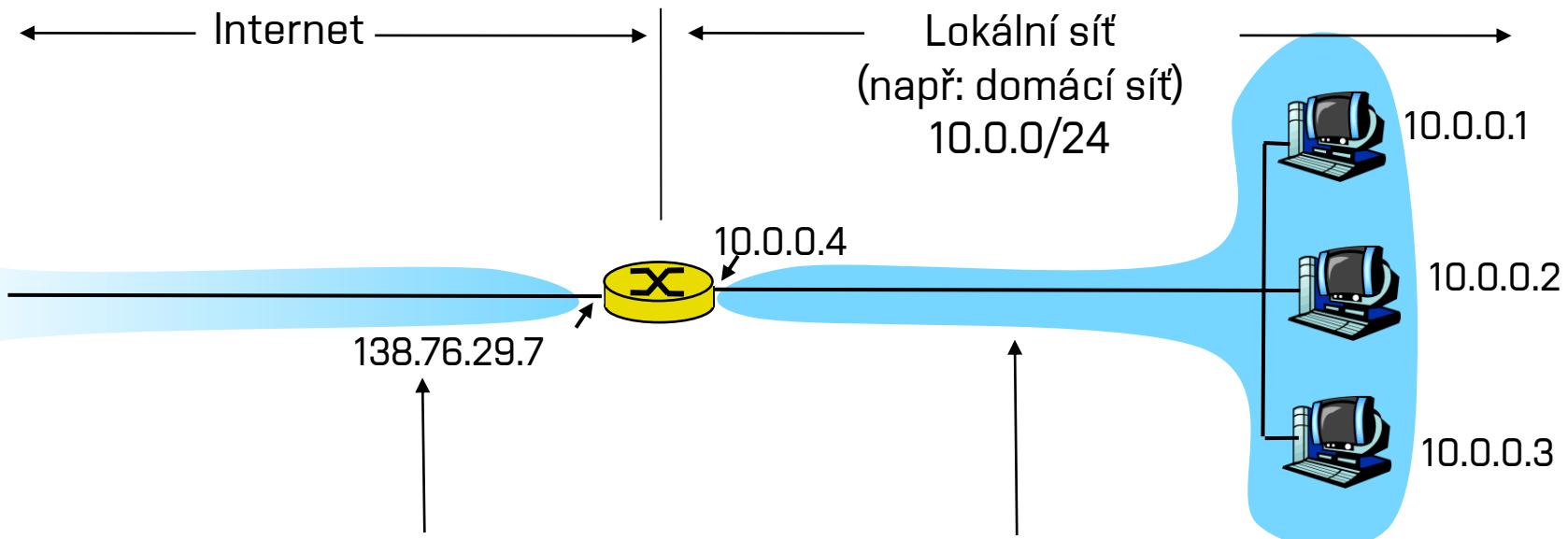


Obsah

- Služby a funkce síťové vrstvy
- Protokol IPv4
 - Funkce, formát
 - Fragmentace a znovusestavení
 - Adresování v IPv4
- Správa adresního prostoru
- Protokol ICMP
 - Funkce, formát
 - Příklady služeb využívající ICMP
- Protokol DHCP
 - Funkce, formát
- **Překlad adres, NAT**

Překlad adres

- Network address translation, RFC 1918



Všechny datagramy opouští lokální síť se stejnou jednou zdrojovou NAT IP adresou: 138.76.29.7, různé zdrojové porty pro TCP/UDP

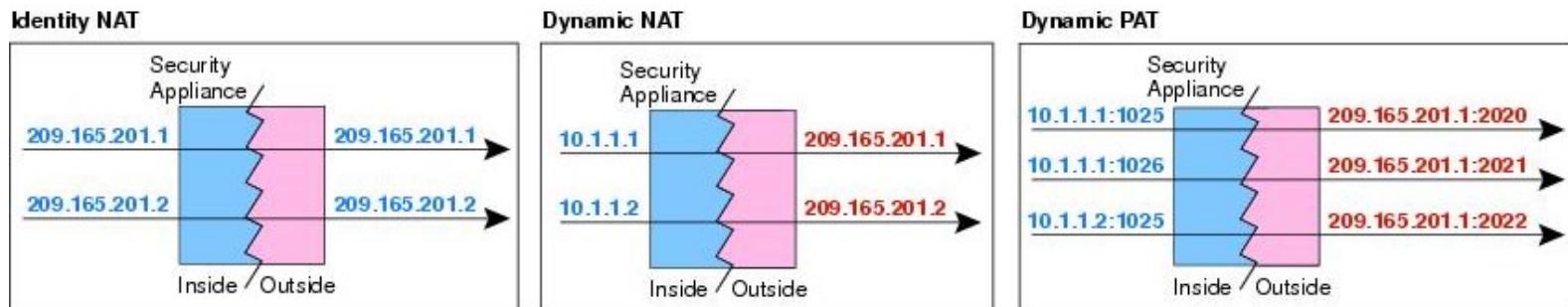
Datagramy mají zdrojovou nebo cílovou adresu v síti v rozsahu 10.0.0/24

Zhodnocení

- **Výhody**
 - Není třeba rozsah adres od poskytovatele připojení: stačí jedna adresa pro všechna zařízení
 - Můžeme měnit adresy v lokální síti aniž bychom to museli někomu sdělit/žádat
 - Můžeme změnit poskytovatele (veřejnou adresu) bez nutnosti něco měnit v lokální síti
- **Nevýhody**
 - Zařízení v lokální síti nejsou explicitně adresovatelné, nejsou viditelné z Internetu
 - ~ bezpečnostní mechanismus (!)

Typy NATu

- Static NAT
 - 1:1 address mapping
- Dynamic NAT
 - N:M address mapping
 - Private address are mapped onto pool of public addresses
 - IF there is no address in public pool THEN NAT cannot work
- Overloading NAT a.k.a. Port Address Translation (PAT)
- Dynamic NAT using one public address
- Rewriting port numbers of TCP and UDP

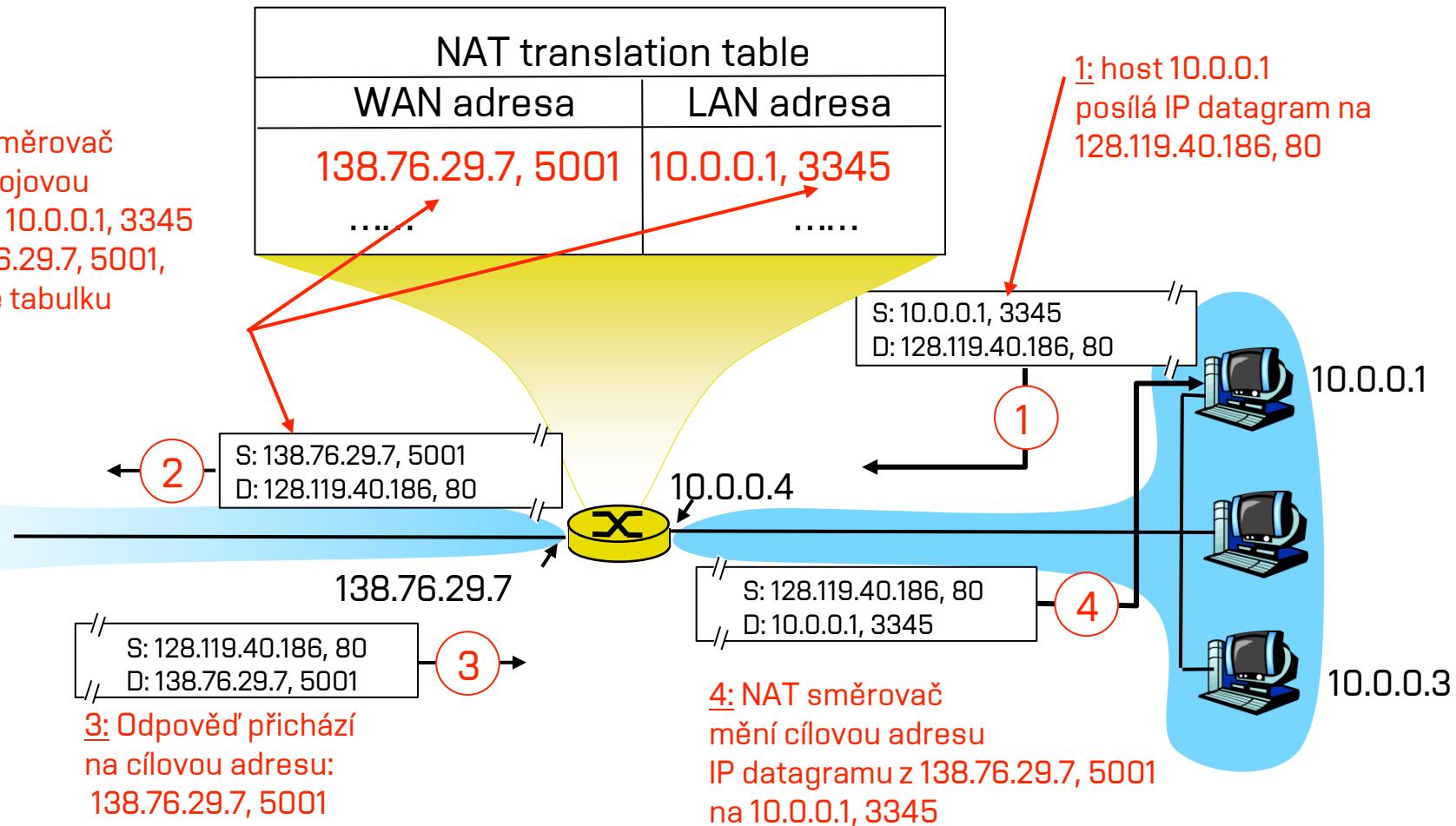


Překlad portů

- 16-bitové číslo portu TCP nebo UDP
 - > 65 535 současných spojení
- NAT modifikuje hlavičku
 - Pokud v aplikačním protokolu klient identifikuje svoji adresu, nastává problém (adresy se liší)
 - Aplikační protokol by měl být navržen tak, aby jej NAT neomezil
 - Router by měl pracovat na 3 vrstvě (překlady dělá obecně brána ...)

Překladová tabulka

2: NAT směrovač mění zdrojovou adresu z 10.0.0.1, 3345 na 138.76.29.7, 5001, updatuje tabulku



NAT ve Wiresharku

The image shows two Wireshark windows side-by-side, illustrating the process of Network Address Translation (NAT). Both windows display a single TCP SYN packet.

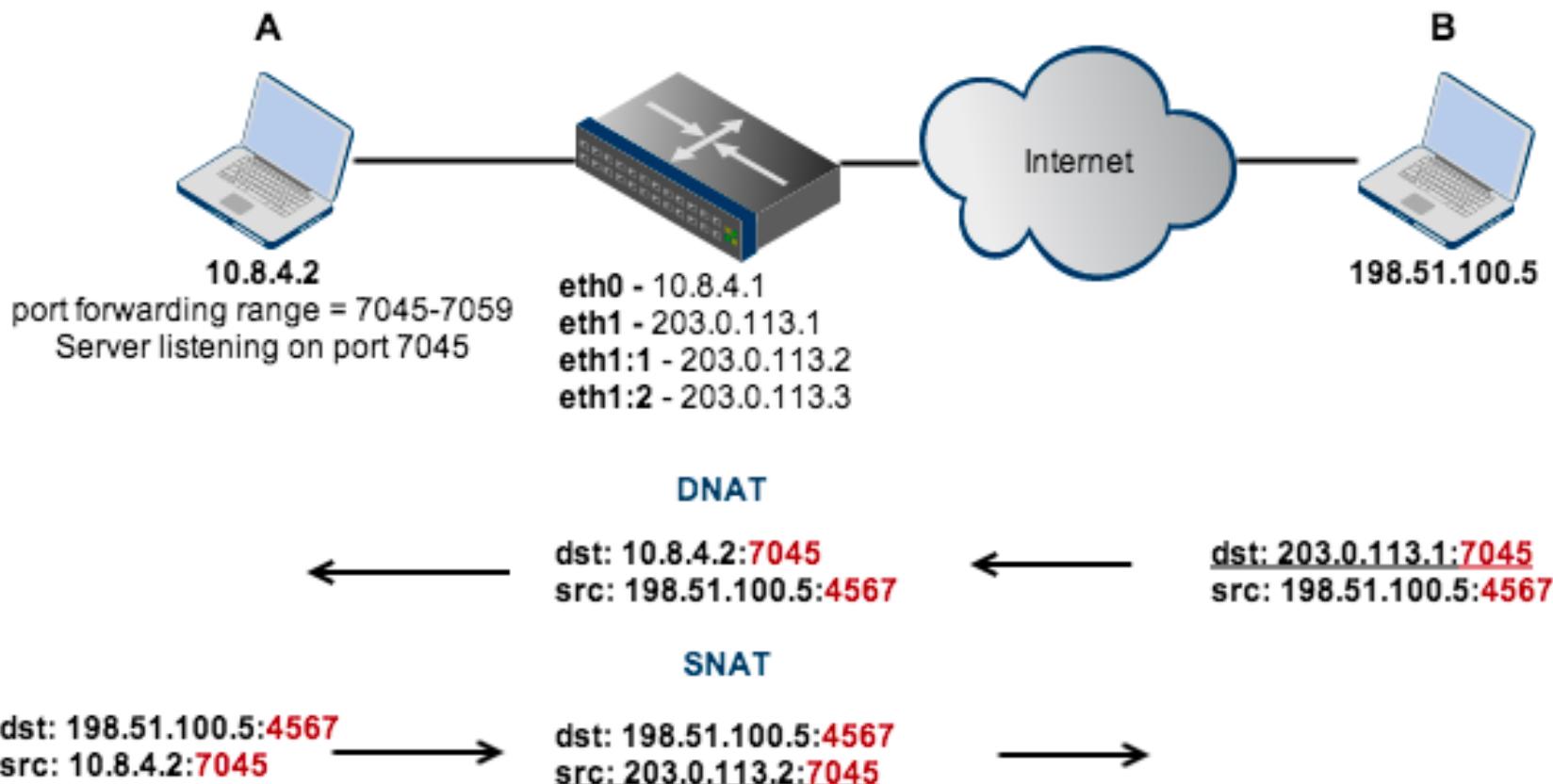
Left Window (Original Source):

- Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface **Ethernet II**, Src: LogicMod_51:66:00 (00:00:ab:51:66:00), Dst: ca:01:19:34:00:1e
- Internet Protocol Version 4, Src: 192.168.0.12 (192.168.0.12), Dst: 1.23.28.43
 - Version: 4
 - Header Length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT)
 - Total Length: 60
 - Identification: 0x875b (34651)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 64
 - Protocol: TCP (6)
 - Header checksum: 0xd56a [validation disabled]
 - Source: 192.168.0.12 (192.168.0.12)
 - Destination: 1.23.28.43 (1.23.28.43)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 53044
 - Source Port: 53044 (53044)
 - Destination Port: 22 (22)
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence number: 1734683627
 - Acknowledgment number: 0
 - Header Length: 40 bytes
 - 0000 0000 0010 = Flags: 0x002 (SYN)
 - window size value: 3840
 - [calculated window size: 5840]
 - Checksum: 0x43c6 [validation disabled]
 - Urgent pointer: 0
 - Options: (20 bytes), Maximum segment size, SA

Right Window (Translated Destination):

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface **Ethernet II**, Src: ca:01:19:34:00:08 (ca:01:19:34:00:08), Dst: ca:02:11:b4:00:08
- Internet Protocol Version 4, Src: 137.186.57.12 (137.186.57.12), Dst: 1.23.28.43
 - Version: 4
 - Header Length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (No ECN Capable))
 - Total Length: 60
 - Identification: 0x875b (34651)
 - Flags: 0x02 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 63
 - Protocol: TCP (6)
 - Header checksum: 0xd458 [validation disabled]
 - Source: 137.186.57.12 (137.186.57.12)
 - Destination: 1.23.28.43 (1.23.28.43)
 - [Source GeoIP: Unknown]
 - [Destination GeoIP: Unknown]
- Transmission Control Protocol, Src Port: 53044 (53044), Dst Port: 22 (22), seq: 1734683627
 - Source Port: 53044 (53044)
 - Destination Port: 22 (22)
 - [Stream index: 0]
 - [TCP Segment Len: 0]
 - Sequence number: 1734683627
 - Acknowledgment number: 0
 - Header Length: 40 bytes
 - 0000 0000 0010 = Flags: 0x002 (SYN)
 - window size value: 3840
 - [calculated window size: 5840]
 - Checksum: 0x41b4 [validation disabled]
 - Urgent pointer: 0

SNAT vs DNAT



DNAT: DMZ

The screenshot shows the configuration interface for an Asus RT-AX88U router running Asuswrt-Merlin firmware version 384.19. The main menu on the left includes options like Quick Internet Setup, General, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, Game, Open NAT, USB Application, AiCloud 2.0, Tools, Advanced Settings, Wireless, LAN, and WAN. The WAN tab is currently selected. The top bar displays the operation mode as "Wireless router", the firmware version, and the SSID "Slysim_jak mat...". The navigation bar at the top right includes Logout, Reboot, and English language selection. Below the navigation bar, there are tabs for Internet Connection, Dual WAN, Port Trigger, Virtual Server / Port Forwarding, DMZ (which is selected), DDNS, and NAT Passthrough. The main content area is titled "WAN - DMZ" and contains a descriptive paragraph about Virtual DMZ. It also lists "Special Applications" with two bullet points: "Some applications require special handler against NAT. These special handlers are disabled in default." and "Please add a rule to port forwarding list for USB Disk access properly on FTP service." A "DMZ FAQ" section follows. At the bottom, there are input fields for "Enable DMZ" (radio buttons for Yes and No, with No selected) and "IP Address of Exposed Station" (set to 192.168.1.2), along with an "Apply" button.

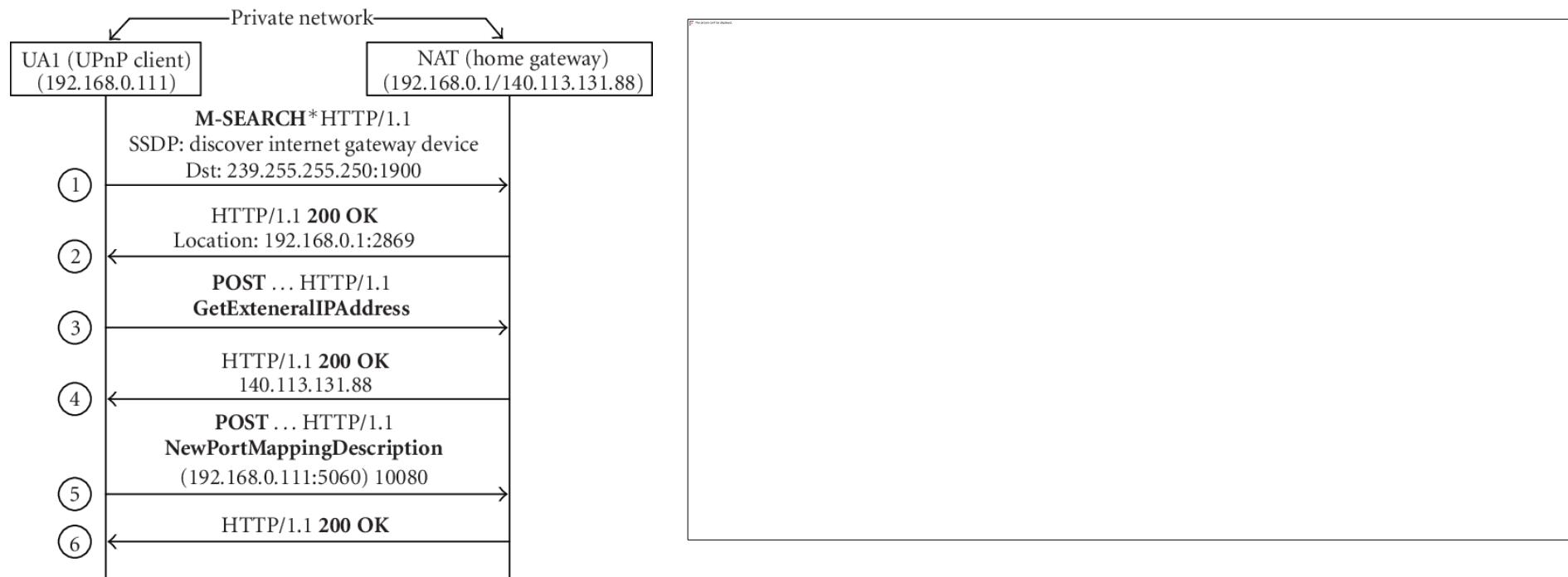
DNAT: Port Forwarding

The screenshot shows the configuration interface for an Asus RT-AX88U router running Asuswrt-Merlin. The top navigation bar includes the router model, powered by Asuswrt-Merlin, Logout, Reboot, and language selection (English). The main menu on the left lists various settings like Quick Internet Setup, General, Network Map, Guest Network, AiProtection, Adaptive QoS, Traffic Analyzer, Game, Open NAT, USB Application, AiCloud 2.0, Tools, Advanced Settings, Wireless, LAN, and WAN. The WAN tab is selected in the top navigation bar. The main content area is titled "WAN - Virtual Server / Port Forwarding". It explains what port forwarding does and provides instructions for specifying port ranges. A list of port forwarding rules is shown, with one entry for "mstsc" configured with an external port of 111, internal port of 3389, internal IP address of 10.102.1.2, and protocol TCP. An "Add profile" button is at the bottom of the list.

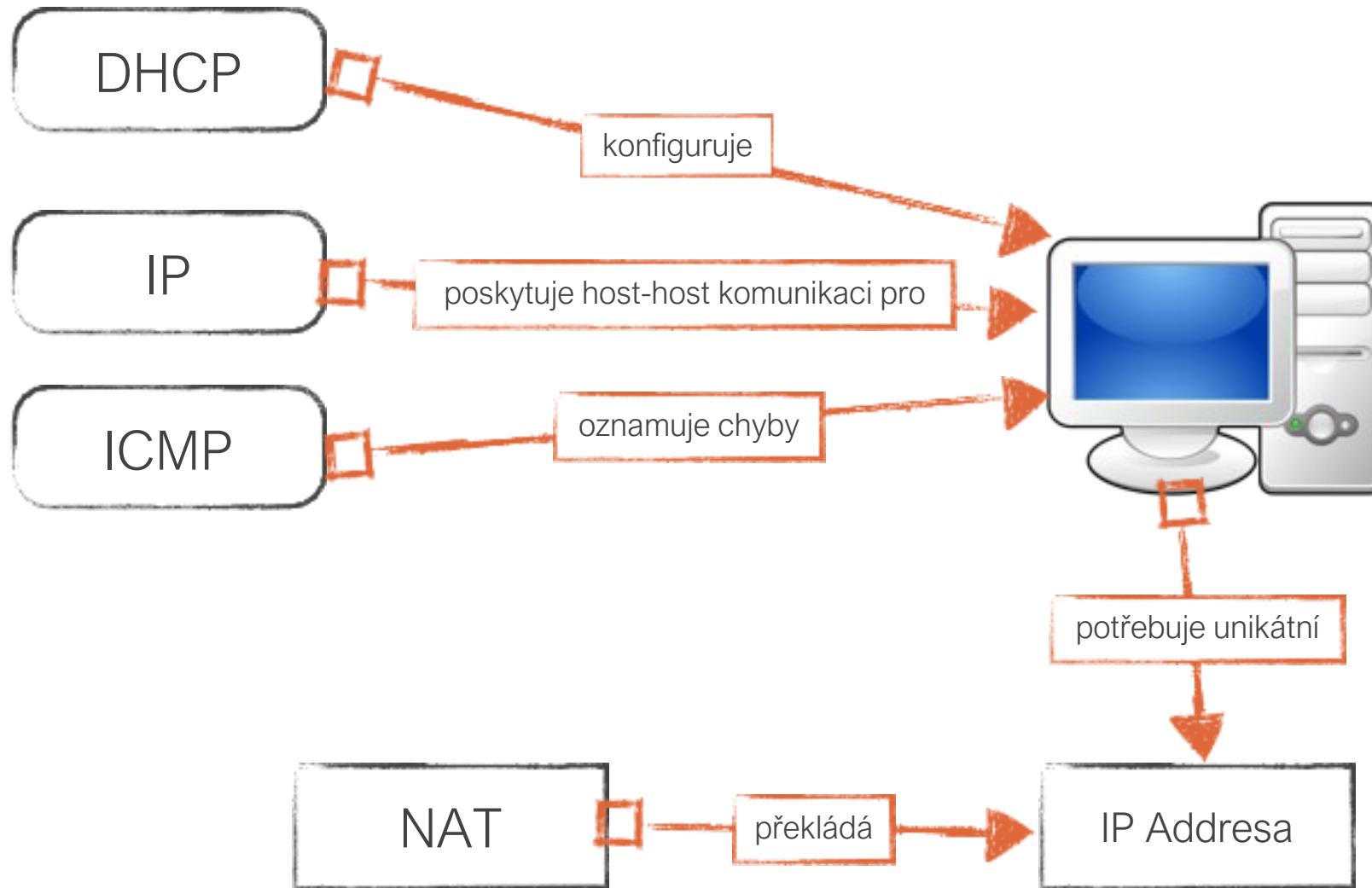
Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
mstsc	111	3389	10.102.1.2	TCP			

Překonávání NATu

- Dynamicky Universal Plug and Play (UPnP)
- Internet Gateway Device (IGD) Protocol – TCP; STUN – UDP
- TURN



Technologie



Studijní materiály

- Kurose J.F., Ross K.W.: [Computer Networking, A Top-Down Approach Featuring the Internet](#). Addison-Wesley, 2003.
- Stevens, W.R.: [TCP/IP Illustrated, Volume 1](#). Addison-Wesley, 1994.
- RFC 791, 792, 950, 1918,