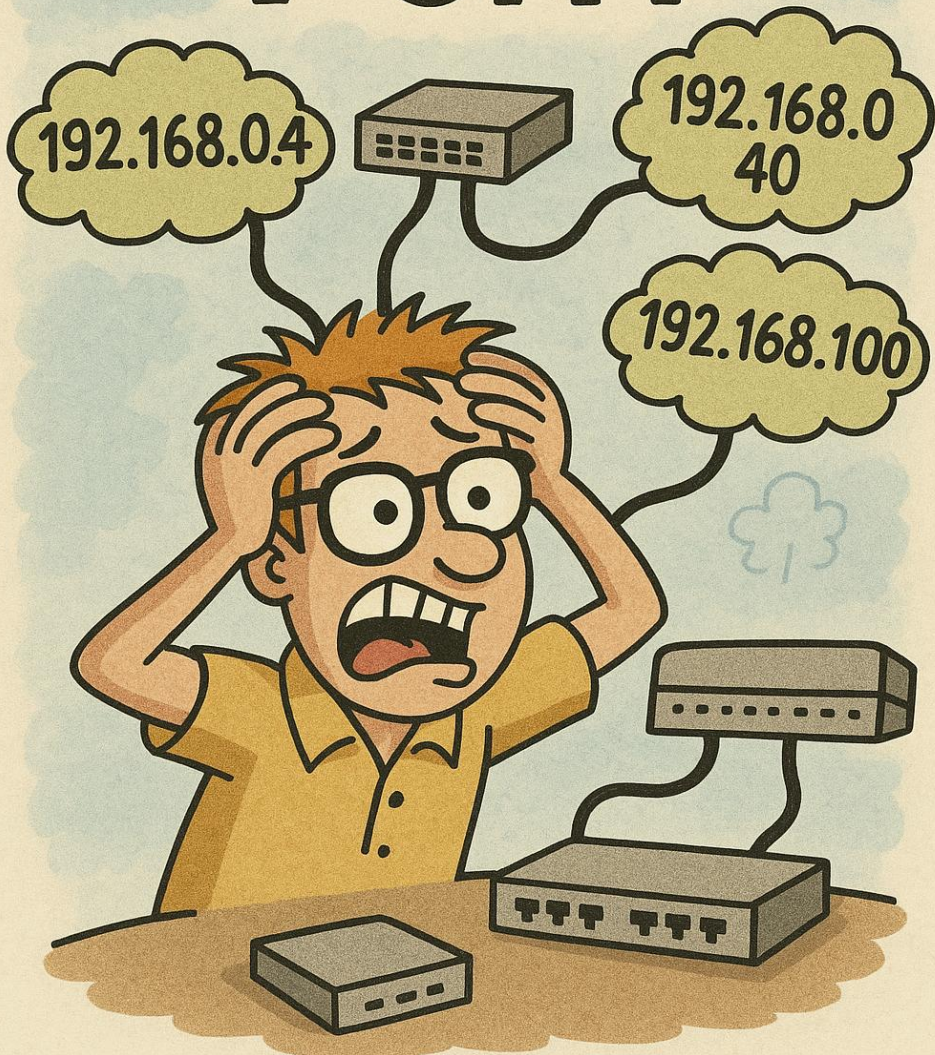


# ADRESACE V SÍTI



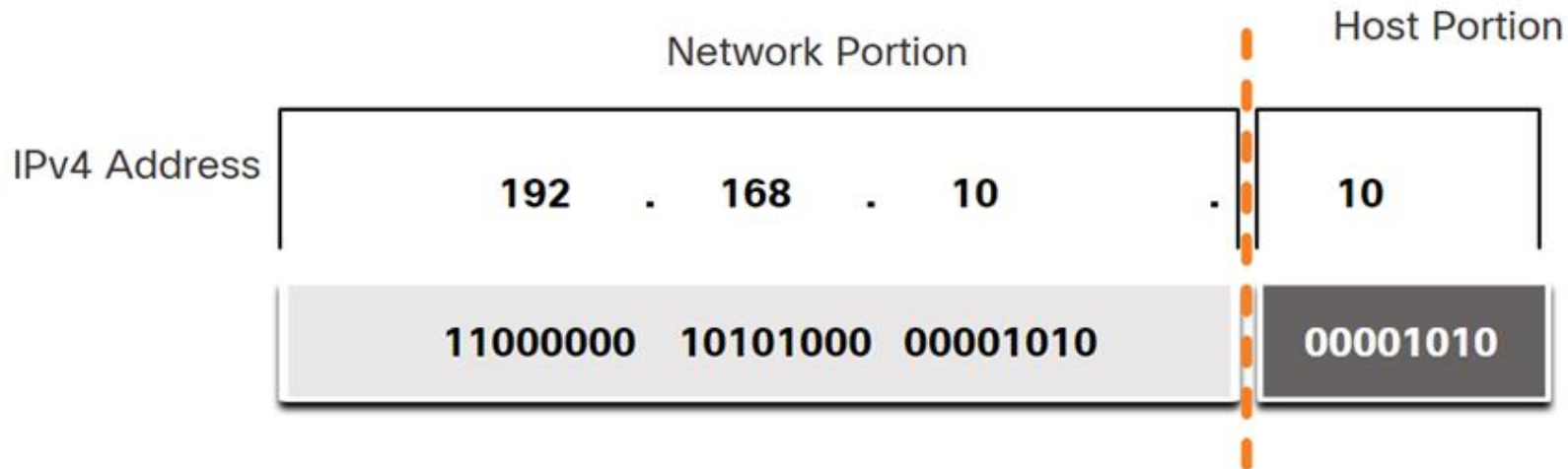
IPv4 adresace,  
výpočty rozsahu  
a adres sítě

Ing. Petr Orvoš

SOŠ a SOU NERATOVICE

# IPv4 adresa

Adresa IPv4 je 32bitová hierarchická adresa, která se skládá ze síťové části a hostitelské části. Při určování síťové části a hostitelské části se musíte podívat na 32bitový datový proud, jak je znázorněno na obrázku.



Bity v síťové části adresy musí být stejné pro všechna zařízení, která jsou umístěna ve stejné síti.

VIDEO vše vysvětlí  
(klikni na ikonu, IPv4 sleduj pouze **do 04:30 min**,  
pak následují IPv6)



# IPv4 adresa

**IP adresa** je logická adresa zařízení v síti IP.

- IPv4 se skládá se ze 4 částí zvaných **octety**, každá část je veliká 8 bitů, a zapisuje se oddělená tečkou.
- adresa se většinou zapisuje v dekadické formě.
- pojem octet nebo oktet – 8 bitů. Termín je často používán u počítačových sítí, když termín byte může být dvojznačný. U běžných počítačových systému jde o synonyma.
- Minimální teoreticky použitelná adresa je **0.0.0.0**
- Maximální teoreticky použitelná adresa je **255.255.255.255**

***Zapište následující IP adresy v binární podobě:***

192.168.1.56, 252.168.25.123, 127.135.222.169, 212.151.32.2

# Podsít - subnet

Sít dělíme na síťové vrstvě na podsítě - subnets - subnetworks.

- **subnety** slouží k logickému dělení sítě do menších hierarchických částí
- příklad: velký ISP má určitý síťový rozsah (subnet), ten dělí na části, které přiděluje firmám a ve firmě se ještě dělí na menší části.

**Ke spojování jednotlivých subnetů slouží routery.**

Dělení sítě na subnety je důležité nejen proto, že naši sít oddělíme od jiných sítí, ale také z výkonových důvodů.

Řada informací se v rámci subnetu šíří pomocí broadcastů, tedy vysílání všem zařízením, což je značná zátěž pro sít i zařízení.



# Maska podsítě (subnet mask)

255 . 255 . 255

0

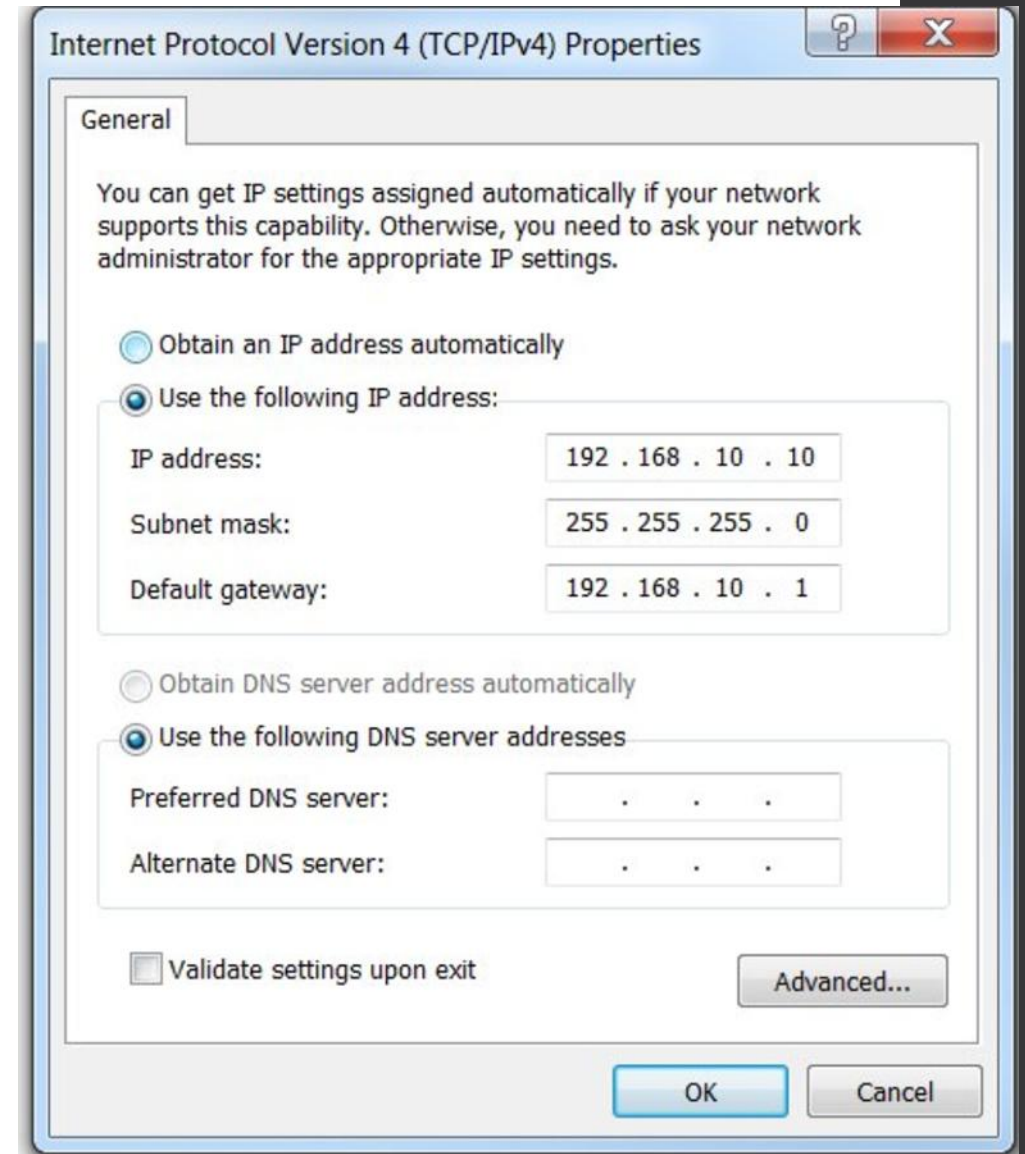
11111111 11111111 11111111

00000000

*Všimněte si, že maska podsítě je postupná sekvence 1 (bitů) následovaná postupnou sekvencí 0 bitů.*

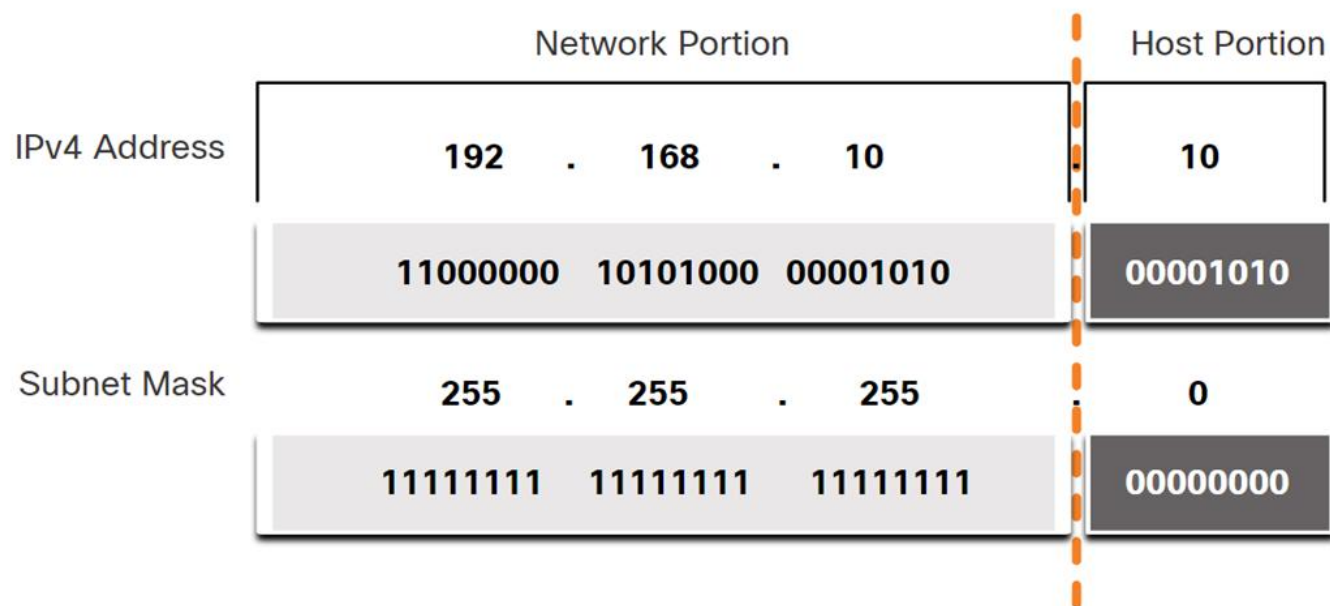
Maska podsítě (subnet mask) je číslo, které určuje, jaká část IP adresy označuje síť a jaká část označuje zařízení (hosta) v této síti.

- používá se k rozdělení IP adresního prostoru na menší podsítě
- pomáhá směrovačům rozhodnout, zda je zařízení ve stejné síti, nebo je třeba poslat data jinam



# Maska podsítě

- zápis je stejný jako u IP adresy, ale platné hodnoty jsou pouze ty, které mají v binárním tvaru zleva jedničky a zprava nuly (pokud se zleva na některé pozici objeví nula, dále již musí následovat pouze nuly)
- **jedničky v masce jsou tzv. network ID** a je to část, která je pro daný subnet stále stejná
- **nuly jsou tzv. host ID** a tedy část, která je proměnná a určuje adresu hosta v daném subnetu.



## ***Možné kombinace v octetu:***

binárně	dekadicky
00000000	0
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

VIDEO vše vysvětlí  
(klikni na ikonu)



# Zkrácený zápis masky podsítě - CIDR

**Subnet maska** se může zapisovat také ve zkrácené formě, které se říká **CIDR notace** (*Classless Inter-Domain Routing*).

Ta se zapisuje jako IP adresa následovaná lomítkem (/) a číslem, které reprezentuje počet jedničkových bitů v masce podsítě v binární formě. Protože celkový počet bitů v masce je 32, tak počet nul je 32 - počet jedniček.

Příklad CIDR notace je 10.0.5.2/20 a tedy maska je 255.255.240.0.

dekadicky	255 .	255 .	240 .	0	
binárně	11111111	11111111	11110000	00000000	
počet jedniček	8	8	4	0	= 20

**Délka předpony (CIDR) je počet bitů nastavených v masce podsítě na hodnotu 1.**

# Zkrácený zápis masky podsítě - CIDR

Maska podsítě	32bitová adresa	Délka předpony
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30



# Inverzní maska (Wildcard mask)

**Wildcard mask** nebo také **inverzní maska** je speciální zápis síťové masky, který používá například Cisco u Access listů.

**Jedná se o opak ke klasické masce, počítají se zde nuly místo jedniček.**

*Takže například ke klasické masce **255.255.255.240** je inverzní maska **0.0.0.15**.*

*Inverzní masku dostaneme tak, že normální masku zobrazíme binárně, provedeme inverzi a převedeme na dekadickou hodnotu. Nebo jednodušeji stačí, u každého octetu spočítat  $255 - \text{hodnota}$ . Tedy v našem příkladě  $255 - 255 = 0$ ,  $255 - 240 = 15$ .*

## ✓ Maska podsítě

255.255.255.240

V binárním zápisu:

1111111.1111111.1111111.11110000

## ↻ Inverzní maska (wildcard mask)

0.0.0.15

V binárním zápisu:

00000000.00000000.00000000.00001111

# Variable Length Subnet Mask

VLSM (Variable Length Subnet Mask) je technika, která umožňuje **přidělovat podsítě s různě dlouhou maskou** podle potřeby – tedy **efektivněji využívat IP adresy**.

## Jak VLSM funguje – jednoduše:

1. **zvolíš základní síť** (např. 192.168.1.0/24)
2. **zanalyzuješ, kolik zařízení potřebuješ v jednotlivých podsítích**
3. **začneš největší potřebnou síť** a přidělíš jí nejmenší možnou masku, která ji pokryje
4. **zbytek sítě** rozdělíš na další menší podsítě s vhodnými maskami
5. **opakuješ**, dokud nepokryješ všechny potřeby.



## **Příklad:**

Máš síť **192.168.1.0/24** a potřebuješ:

- 1 síť pro 50 zařízení
- 1 síť pro 20 zařízení
- 1 síť pro 10 zařízení
- 1 síť pro 2 zařízení

Postupně je maskou rozdělíš:

- **/26** → 64 adres (pro 50 zařízení)
- **/27** → 32 adres (pro 20 zařízení)
- **/28** → 16 adres (pro 10 zařízení)
- **/30** → 4 adresy (pro 2 zařízení)

# Variable Length Subnet Mask

Název sítě	Požadovaných hostů	Přidělená podsít'	Maska	Inverzní maska	Rozsah IP (host)	Broadcast	Počet použitelných IP
Sít' A	50	192.168.1.0/26	255.255.255.192	0.0.0.63	192.168.1.1 - 192.168.1.62	192.168.1.63	62
Sít' B	20	192.168.1.128/27	255.255.255.224	0.0.0.31	192.168.1.129 - 192.168.1.158	192.168.1.159	30
Sít' C	10	192.168.1.192/28	255.255.255.240	0.0.0.15	192.168.1.193 - 192.168.1.206	192.168.1.207	14
Sít' D	2	192.168.1.224/30	255.255.255.252	0.0.0.3	192.168.1.225 - 192.168.1.226	192.168.1.227	2

# Třídy IP adres – Classfull addressing

V roce 1981 byly IPv4 adresy přidělovány pomocí classful addressing.

Zákazníkům byla přidělena síťová adresa na základě jedné ze tří tříd, A, B nebo C. RFC rozdělilo rozsahy **unicast vysílání** do konkrétních tříd následovně:

Třída	začátek (bin)	1. bajt	standardní maska	CIDR	bitů stanice	stanic v každé síti
<b>A</b>	0	0–127	<b>255.0.0.0</b>	/8	24	$2^{24}-2 = 16\,777\,214$
<b>B</b>	10	128–191	<b>255.255.0.0</b>	/16	16	$2^{16}-2 = 65\,534$
<b>C</b>	110	192–223	<b>255.255.255.0</b>	/24	8	$2^8-2 = 254$
<b>D</b>	1110	224–239	multicast			
<b>E</b>	1111	240–255	vyhrazeno jako rezerva			

**Dnes se prakticky nepoužívá.**

# Třídy IP adres – Classless network

Od classfull network se již před dlouhou dobou ustoupilo a začalo se používat adresování CIDR, které je více flexibilní při dělení sítě na podsítě.

**V komunikaci používáme vždy IP adresu spolu s maskou.**

I když se opustily classful network, tak se v praxi běžně setkáme s označováním subnetů jako třída C apod., myslí se tím však **typ masky** (červeně v předchozí tabulce).

*U Cisco switchů a routerů se používá příkaz pro použití classless network, který je defaultně zapnutý.*

VIDEO vše vysvětlí  
(klikni na ikonu)





# Neveřejné síťové rozsahy a speciální

Některé síťové rozsahy mají speciální vlastnosti, tou hlavní je, že se neroutují, tzn. neprochází do dalšího subnetu. To se využívá u privátních subnetů, které neprochází do internetu. V praxi je využívá většina firem v lokální síti a do internetu přistupují přes veřejnou adresu za pomoci **NAT** (*budeme brát později podrobněji*).

třída	síť	adresa sítě	broadcast adresa	adresy hostů
<b>A</b>	10.0.0.0/8	10.0.0.0	10.255.255.255	10.0.0.1 - 10.255.255.254
<b>B</b>	172.16.0.0/12	172.16.0.0	172.31.255.255	172.16.0.1 - 172.31.255.254
<b>C</b>	192.168.0.0/16	192.168.0.0	192.168.255.255	192.168.0.1 - 192.168.255.254

A ještě speciální adresy:

síť	adresa sítě	broadcast adresa	označení
127.0.0.0/8	127.0.0.0	127.255.255.255	Localhost Loopback Addresses
169.254.0.0 /16	169.254.0.0	169.254.255.255	Zeroconf Address

# Localhost Loopback Address

Dalšími speciálními subnety jsou:

**Localhost** je speciální název, který v operačních systémech (Windows, Linux, macOS) odkazuje na lokální počítač – tedy zařízení, na kterém uživatel pracuje.

**Loopback adresa** je IP adresa, která také odkazuje zpět na lokální zařízení.

IP adresy loopback rozhraní:

- nejznámější: 127.0.0.1 (v IPv4), celý rozsah: 127.0.0.0/8, tedy od 127.0.0.1 do 127.255.255.254
- V IPv6: ::1 je ekvivalent 127.0.0.1

## Využití:

1. **testování síťových aplikací** (např. webový server běžící na http://127.0.0.1:8000 ti umožní přístup k lokální aplikaci v prohlížeči)
2. **diagnostika sítě** (příkaz ping 127.0.0.1 testuje, zda funguje TCP/IP stack na zařízení)
3. **bezpečnost a sandboxing** (omezení přístupu pouze na lokální zařízení – například databáze PostgreSQL může přijímat připojení pouze z 127.0.0.1, aby k ní nemohl nikdo z internetu).
4. **vývoj webových stránek** (frameworky např. Node.js, Flask, Django standardně běží na localhost, dokud není aplikace připravena k nasazení do produkce).

# Zeroconf Address

**Zeroconf (Zero Configuration Networking)** je technologie, která umožňuje zařízení v počítačové síti komunikovat bez potřeby ruční konfigurace (*např. bez DHCP serveru nebo ručního nastavení IP adres*).

**Je to užitečné např. v domácnostech nebo malých sítích, kde:**

- není žádný DHCP server
- chceme, aby zařízení „samo fungovalo“

**Rozsah IP:** 169.254.0.0/16 (nejčastější adresa, kterou zařízení získá: 169.254.x.x)

Tento blok je rezervován pro **Automatic Private IP Addressing (APIPA)**

## Využití:

1. **automatické přiřazení IP adresy** (zkontroluje, zda adresa není v konfliktu (pomocí ARP), pokud není, použije ji)
2. **komunikace bez routeru** (např. pro přímé spojení dvou počítačů kabelem, tiskáren, kamer nebo IoT zařízení)
3. **podpora v operačních systémech**

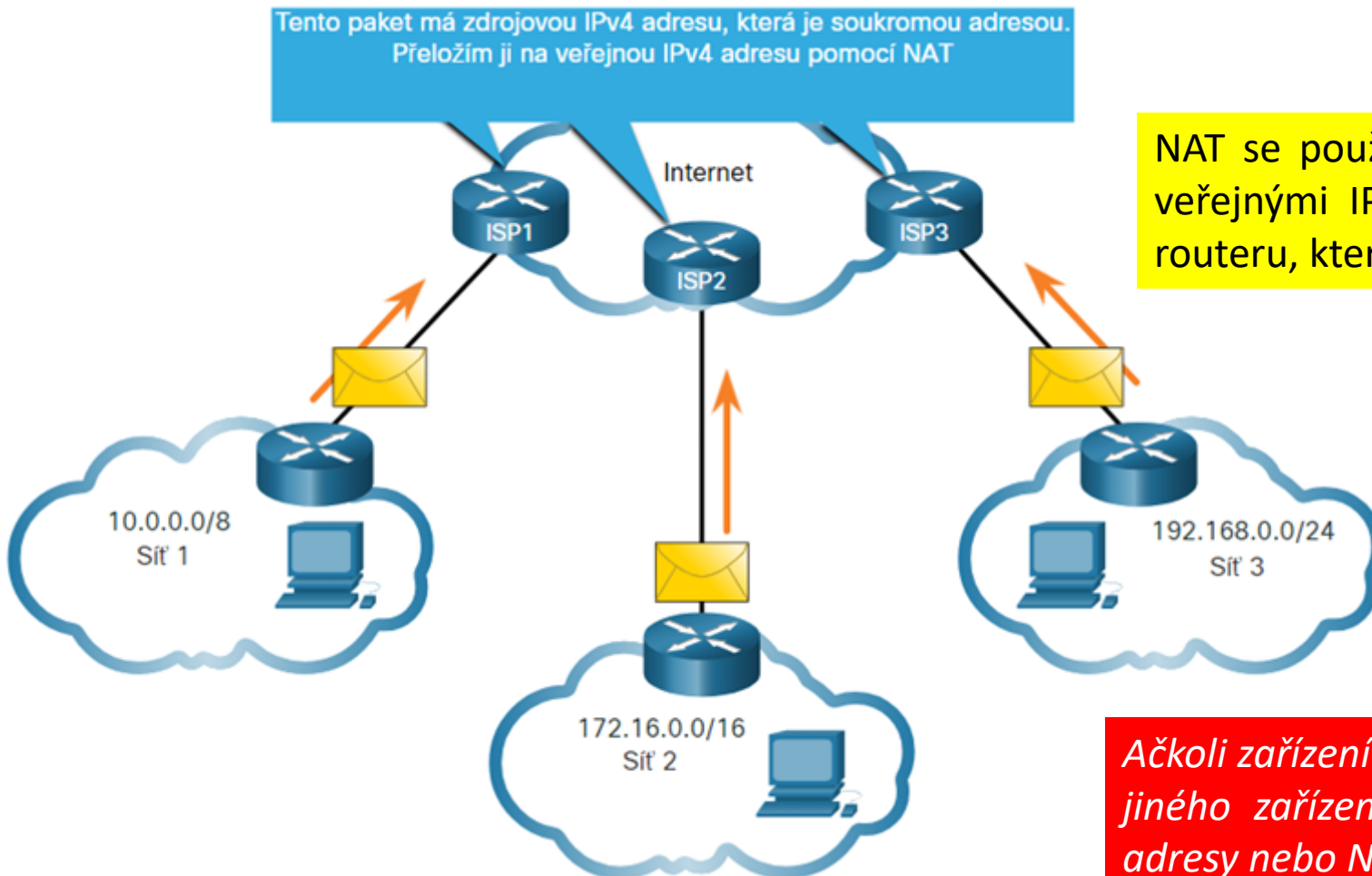
## Omezení:

- funguje pouze v rámci jedné broadcast domény
- nepracuje přes routery – tedy žádný přístup na internet

# Směrování neveřejných adres do internetu

Většina interních sítí, od velkých podniků až po domácí sítě, používá privátní IPv4 adresy pro adresování všech interních zařízení (intranet) včetně hostitelů a routerů.

**Soukromé adresy nejsou globálně směrovatelné!**

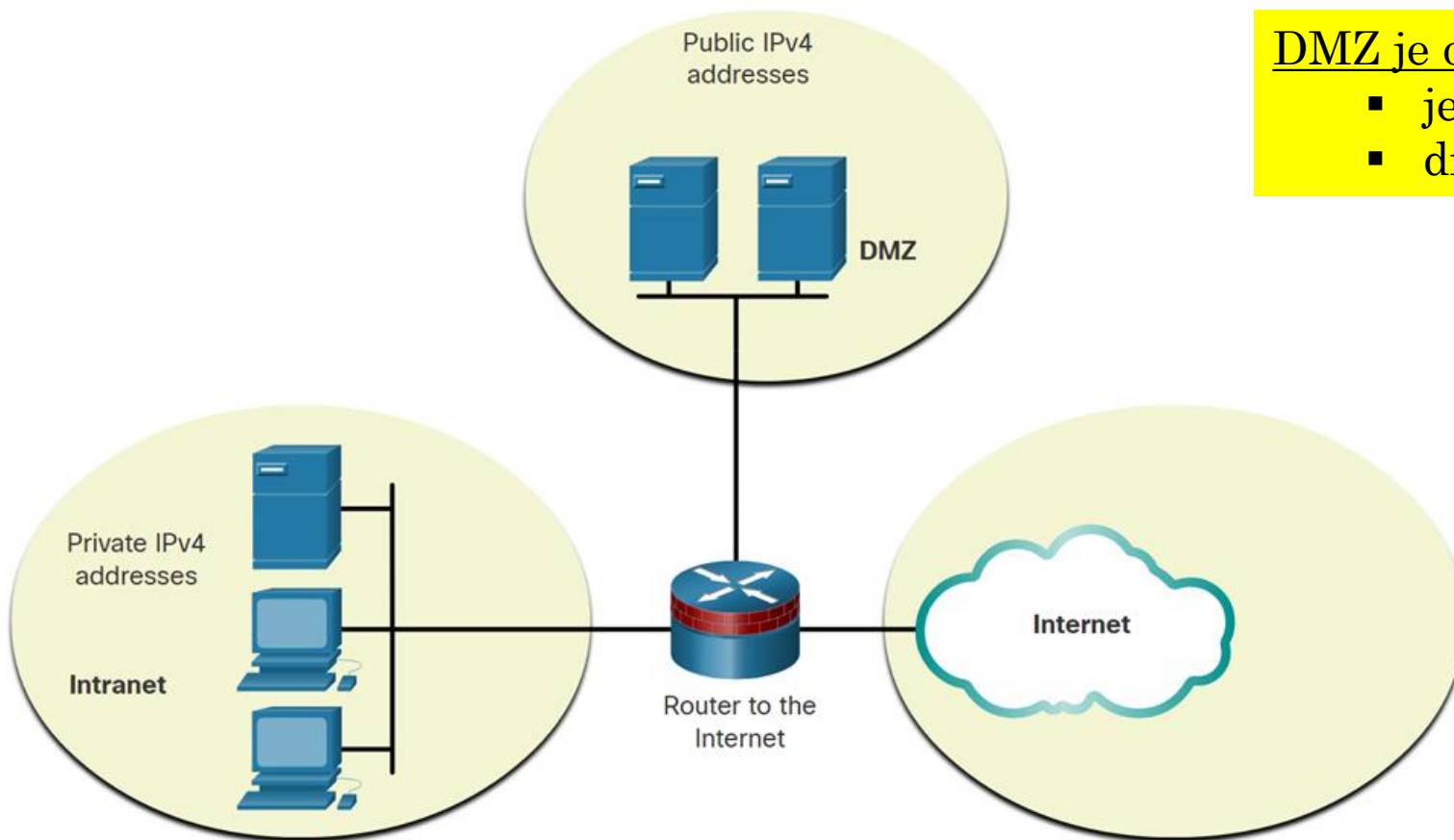


NAT se používá k překladu mezi soukromými IPv4 a veřejnými IPv4 adresami. To se obvykle provádí na routeru, který připojuje interní síť k síti ISP.

*Ačkoli zařízení se soukromou IPv4 adresou není přímo přístupné z jiného zařízení přes internet, IETF nepovažuje soukromé IPv4 adresy nebo NAT za účinná bezpečnostní opatření.*

# DMZ (demilitarizovaná zóna)

DMZ je část sítě, která je oddělená od vnitřní (důvěryhodné) sítě, ale zároveň přístupná z internetu. Používá se hlavně pro zvýšení bezpečnosti.



DMZ je obvykle chráněná dvěma firewally:

- jeden mezi internetem a DMZ
- druhý mezi DMZ a interní sítí

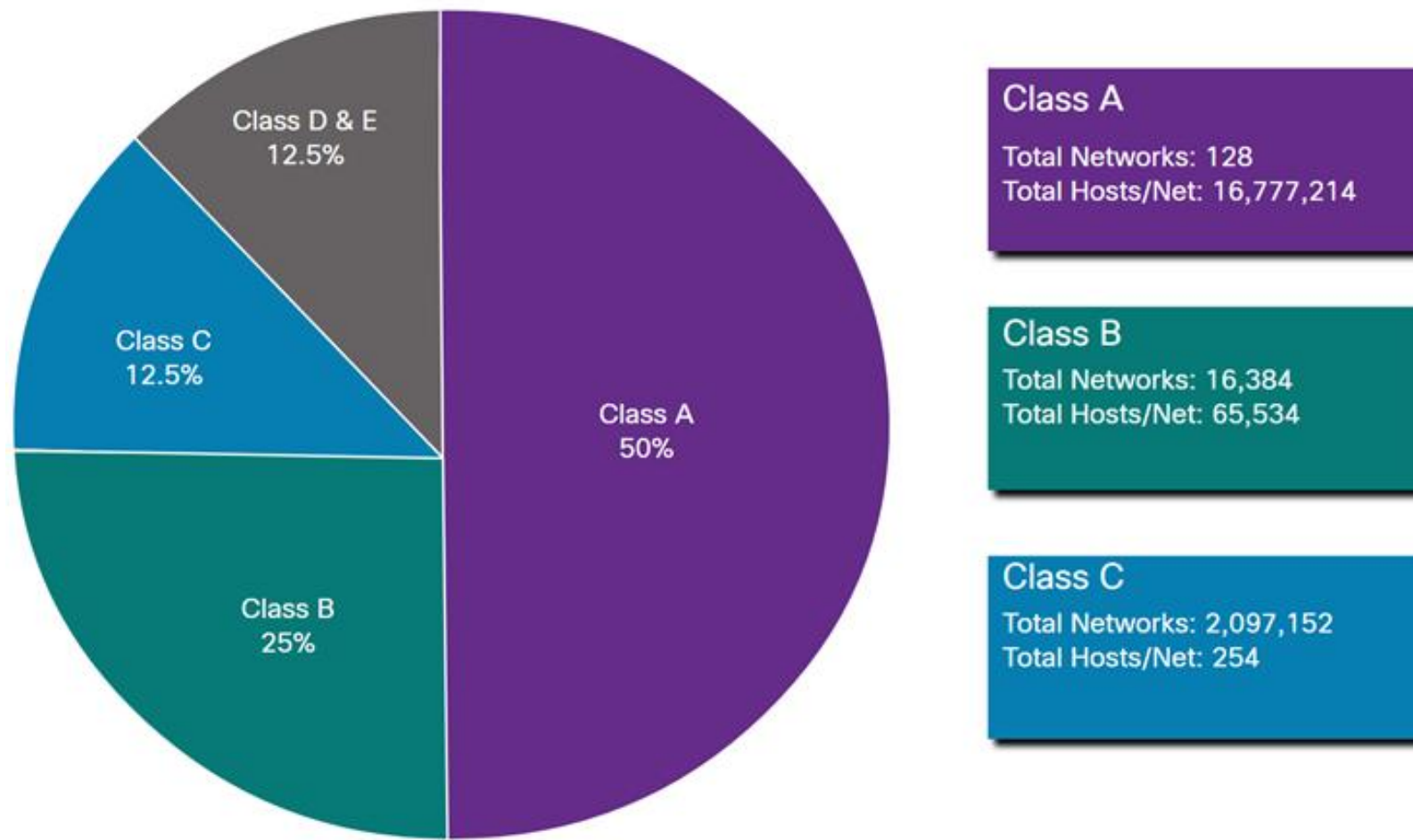


- pokud útočník napadne server v DMZ, nemá přímý přístup k interní síti
- firewall mezi DMZ a interní sítí blokuje neautorizovaný přístup

Router na obrázku provádí nejen směrování, ale také provádí NAT a funguje jako firewall pro zabezpečení.



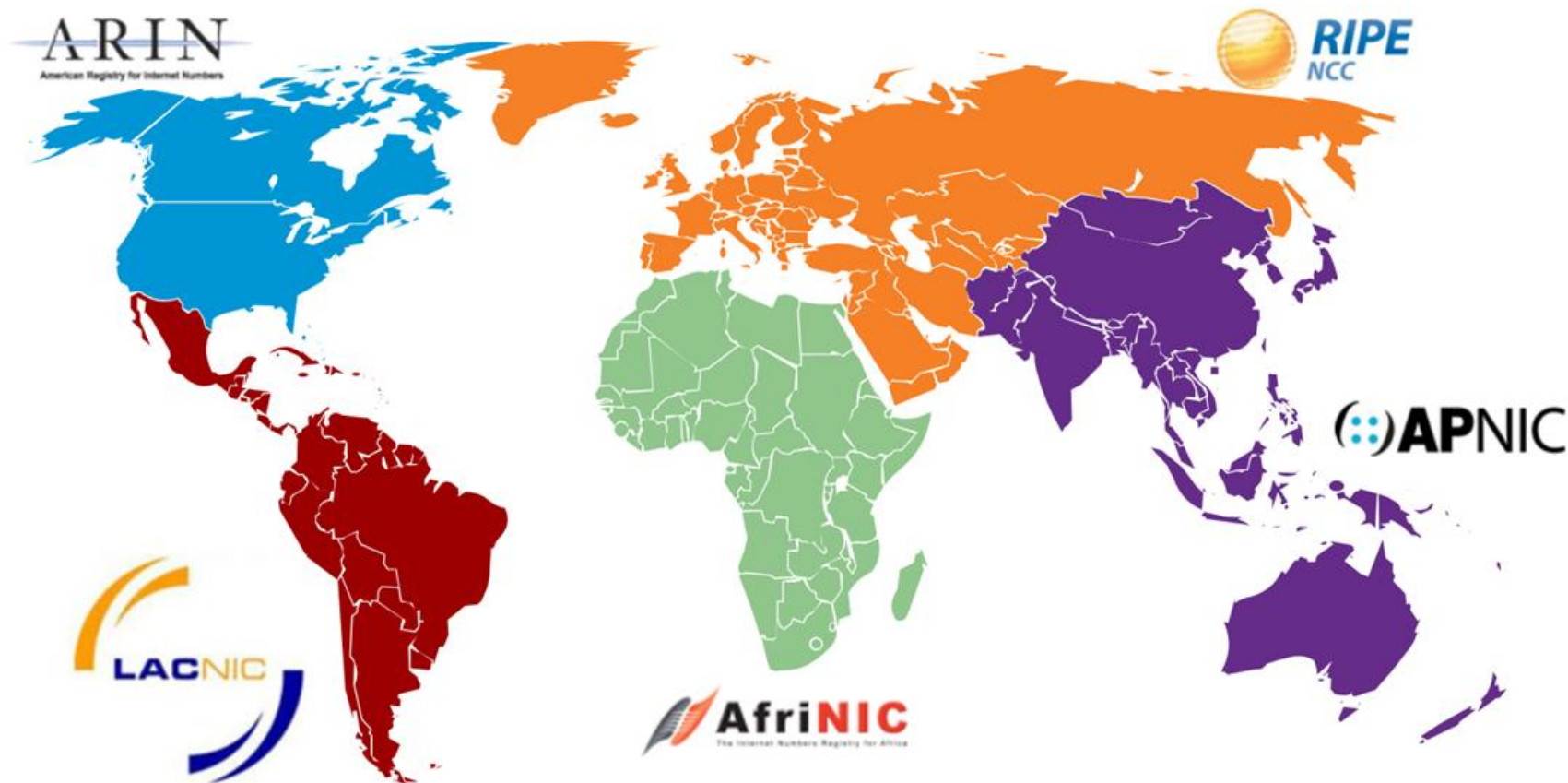
# Přiřazení IPv4 adres?



**Veřejné IPv4 adresy musí být jedinečné.**

# Přiřazení IPv4 adres

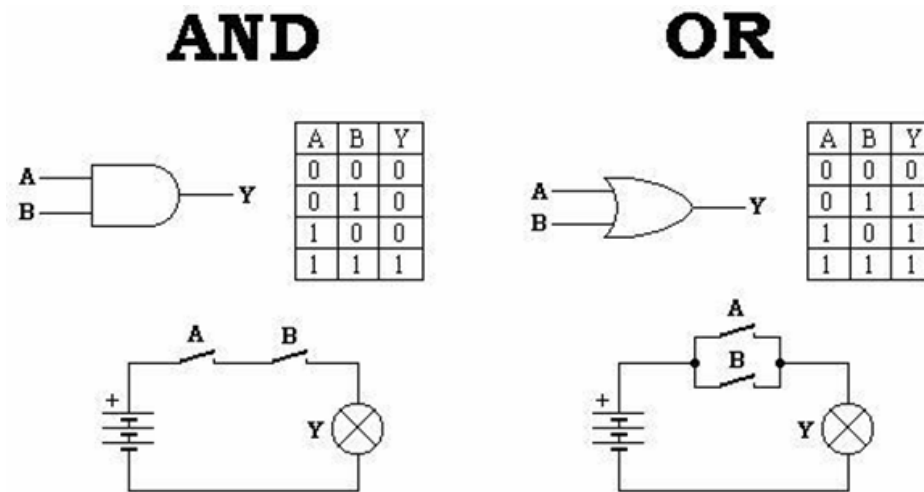
Adresy IPv4 i IPv6 jsou spravovány úřadem IANA (Internet Assigned Numbers Authority). IANA spravuje a přiděluje bloky IP adres regionálním internetovým registrům (RIR).



# Určení sítě – logické AND

Logický operátor AND je jednou ze tří booleovských operací používaných v booleovské nebo digitální logice. Další dvě jsou OR a NOT.

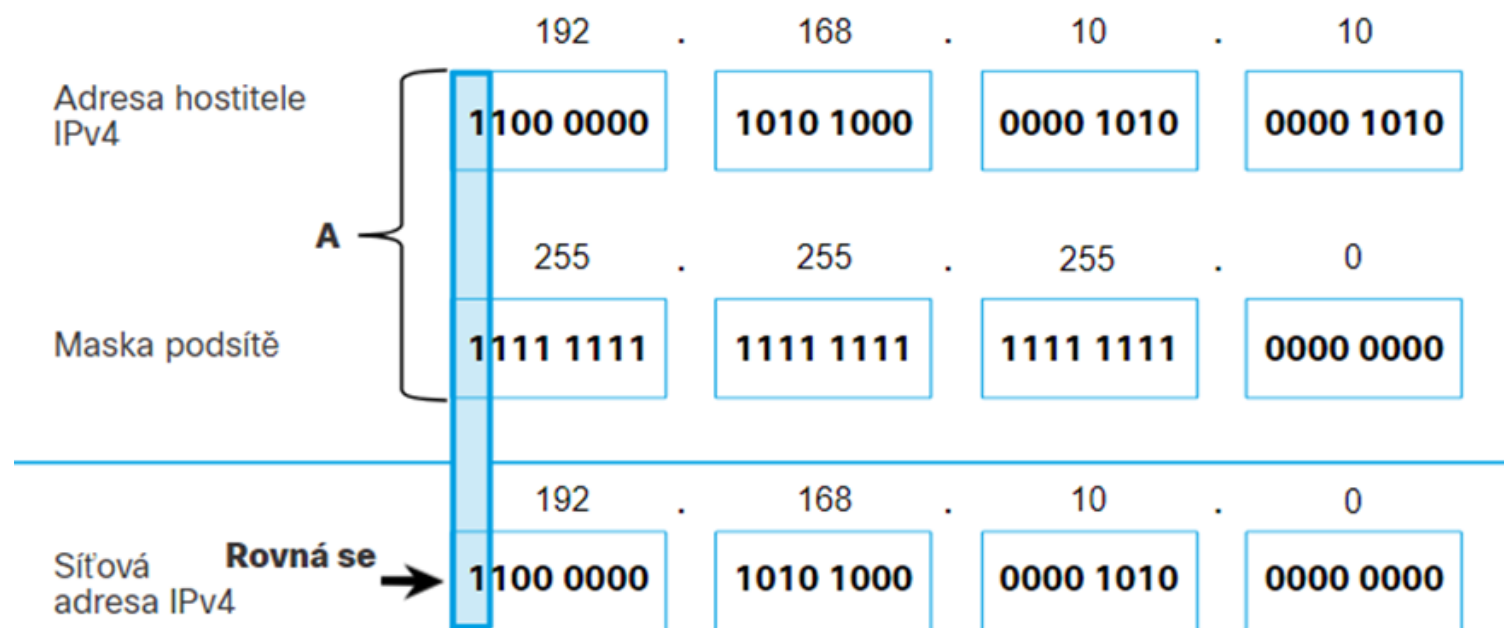
**Operace AND se používá k určení síťové adresy, OR k určení broadcast.**



Aby bylo možné identifikovat síťovou adresu hostitele IPv4, je adresa IPv4 logicky ANDována, bit po bitu, pomocí masky podsítě. **ANDing mezi adresou a maskou podsítě poskytuje síťovou adresu.**

# Určení adresy sítě (network ID)

*Pro ilustraci toho, jak se operátor AND používá ke zjištění síťové adresy, zvažte hostitele s adresou IPv4 192.168.10.10 a maskou podsítě 255.255.255.0:*



Výsledkem operace AND mezi adresou hostitele IPv4 (192.168.10.10) a maskou podsítě (255.255.255.0) je síťová adresa IPv4 (192.168.10.0) pro tohoto hostitele.

Jedná se o důležitou operaci IPv4, protože hostiteli říká, do jaké sítě patří.

# Ostatní důležité adresy

Na základě předchozího výpočtu můžeme dále určit:

- adresu prvního a posledního hosta v síti
- a ve finále i adresu broadcastového vysílání (*bude ukázáno dále*)

Network Address	First Usable Host	Last Usable Host	Broadcast Address
192.168.10.0	192.168.10.1	192.168.10.254	192.168.10.255

192.168.10.10

(falls within the range of usable host addresses)



# Nalezení Network ID – jiný příklad

Nalezení první adresy podsítě se může zdát jednoduché, ale někdy to na první pohled vidět není. Pak musíme použít logiku nebo matematiku.

Network ID se dá vypočítat z binárního zápisu adresy a masky, kdy se provede bitový logický součin AND.

Příklad pro adresu 10.217.123.7/20:

IP binárně	00001010.11011001.01111011.00000111
maska binárně	11111111.11111111.11110000.00000000
operace AND	00001010.11011001.01110000.00000000
dekadicky	<b>10.217.112.0</b>

# Určení Broadcast sítě

Broadcastovou adresu subnetu nalezneme podobně jako network ID.

Matematicky můžeme použít bitový logický součet **OR** mezi IP adresou a negovanou maskou.

Příklad pro adresu 10.217.123.7/20:

IP binárně	00001010.11011001.01111011.00000111
maska binárně	11111111.11111111.11110000.00000000
negace masky	00000000.00000000.00001111.11111111
operace OR	00001010.11011001.01111111.11111111
dekadicky	<b>10.217.127.255</b>

# Výpočet počtu subnetů a hostů

Při výpočtu postupujeme tak, že vezmeme octet masky, v kterém je přechod mezi jedničkami a nulami.

Podle počtu jedniček v tomto octetu a celkového počtu nul spočítáme počet podsítí (z jedniček) a počet hostů (z nul).

**$2^{\text{počet jedniček}} = \text{počet subnetů}$**

**$2^{\text{počet nul}} - 2 = \text{počet hostů}$**

# Postup výpočtů parametrů sítě

1. Zapiš si IP adresu a CIDR - např. **192.168.1.18 /17**
2. Urči síťovou masku z CIDR - /17 znamená 17 bitů pro masku → **255.255.128.0**
3. Spočítej binární zápis IP adresy a masky, vypočítej adresu sítě (AND IP & maska) - provádíme „AND-ing“)  
IP: 192.168.1.18 → 11000000.10101000.00000001.00010010  
Maska: /17 → 11111111.11111111.10000000.00000000  
→ 11111111.11111111.00000000.00000000 → **192.168.0.0 /17**
4. Vypočítej broadcast adresu (OR IP & inverzní maska - provádíme „OR-ing“)  
IP: 192.168.1.18 → 11000000.10101000.00000001.00010010  
Inverzní maska: /17 → 00000000.00000000.01111111.11111111  
→ 11000000.10101000.01111111.11111111 → **192.168.127.255**
6. Urči první host adresu: **adresa sítě + 1** → **192.168.0.1**
7. Urči poslední host adresu: **broadcast - 1** → **192.168.127.254**
8. Spočítej počet hostů: vzorec:  $2^{(32 - \text{CIDR})} - 2$  → pro /17:  $2^{15} - 2 = 32\,766$  hostů

# Příklad 1

Máme adresu 192.168.1.25/24

Spočítejte adresu sítě a její broadcast adresu

192.168.1.25	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	0	0	1
255.255.255.0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
192.168.1.0	1	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
192.168.1.255	1	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1

**Závěr:**

Adresa sítě – 192.168.1.0

Netmask – 255.255.255.0

Broadcast adresa – 192.168.1.255



# Příklad 2

Máme adresu 192.168.1.2

Netmask: 255.255.255.224

Napište adresu sítě včetně CIDR a její broadcast adresu

192.168.1.2	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
255.255.255.224	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
192.168.1.0	1	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
192.168.1.31	1	1	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	1	1	1	1	1

**Závěr:**

Adresa sítě – 192.168.1.0/27

Broadcast adresa – 192.168.1.31

**Dodatečný závěr:** V této síti je použitelných 30 IP adres pro hosty ( $2^5 - 2$ )

# Příklad 3

Máme adresu 10.1.5.20

Netmask: 255.255.255.240

Napište adresu sítě včetně CIDR, její broadcast adresu, počet host adres, rozsah host adres.

10.1.5.20	0	0	0	0	1	0	1	0		0	0	0	0	0	0	0	1		0	0	0	0	0	1	0	1		0	0	0	1	0	1	0	0
255.255.255.240	1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		1	1	1	1	1	1	1	1		1	1	1	1	0	0	0	0
10.1.5.16	0	0	0	0	1	0	1	0		0	0	0	0	0	0	0	1		0	0	0	0	0	1	0	1		0	0	0	1	0	0	0	0
10.1.5.31	0	0	0	0	1	0	1	0		0	0	0	0	0	0	0	1		0	0	0	0	0	1	0	1		0	0	0	1	1	1	1	1

## Závěr:

Adresa sítě – 10.1.5.16/28 Broadcast adresa – 10.1.5.31

Rozsah host adres: 10.1.5.17 - 10.1.5.30 - celkem 14 adres

# Příklad – určení adres v síti 1

Ze zadané IP adresy vypočtete IP adresu sítě včetně CIDR označení masky a ostatní požadované adresy uvedené v tabulce (broadcast adresa, nejnižší host adresa, nejvyšší host adresa, počet host adres.

Zadaná IP adresa:	<b>170.61.212.110</b>
Prefix:	<b>/24</b>
Vypočtená adresa sítě včetně prefixu:	
Prefix převeden o oktetového zápisu:	
Nejnižší host adresa:	
Nejvyšší host adresa:	
Vypočtená broadcast adresa:	
Počet host adres:	

**Řešíme postupně na tabuli a studenti si píší poznámky:**

# Příklad – určení adres v síti 2

Ze zadané IP adresy vypočtete IP adresu sítě včetně CIDR označení masky a ostatní požadované adresy uvedené v tabulce (broadcast adresa, nejnižší host adresa, nejvyšší host adresa, počet host adres.

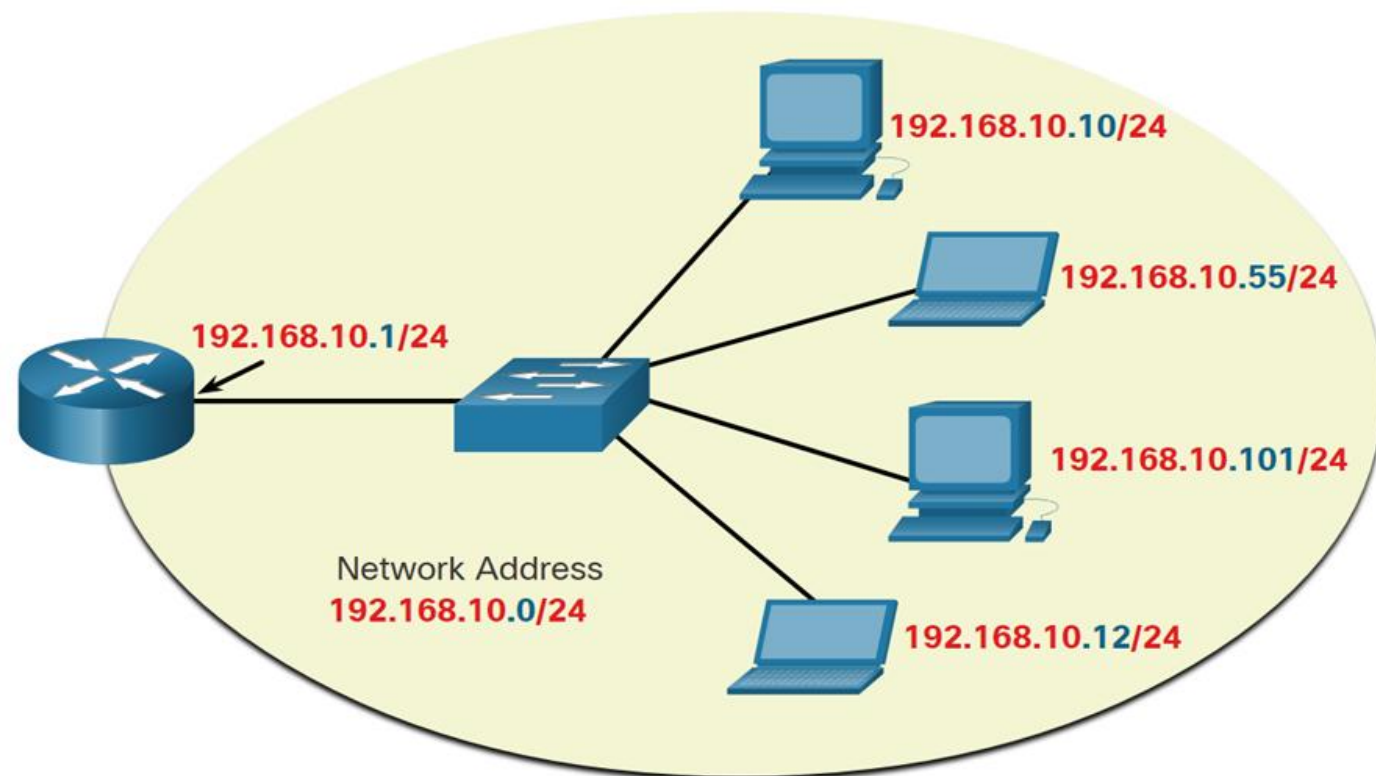
Zadaná IP adresa:	<b>170.61.212.110</b>
Prefix:	<b>/22</b>
Vypočtená adresa sítě včetně prefixu:	
Prefix převeden o oktetového zápisu:	
Nejnižší host adresa:	
Nejvyšší host adresa:	
Vypočtená broadcast adresa:	
Počet host adres:	

**Řešíme postupně na tabuli a studenti si píší poznámky:**

# Síťové, hostitelské a vysílací adresy

Zařízení patří do stejné sítě, pokud splňuje tři kritéria:

- má stejnou masku podsítě jako síťová adresa;
- má stejné síťové bity jako síťová adresa, jak je uvedeno v masce podsítě;
- je umístěna ve stejné vysílací doméně jako ostatní hostitelé se stejnou síťovou adresou.



**Síťová adresa nemůže být přiřazena zařízení!**

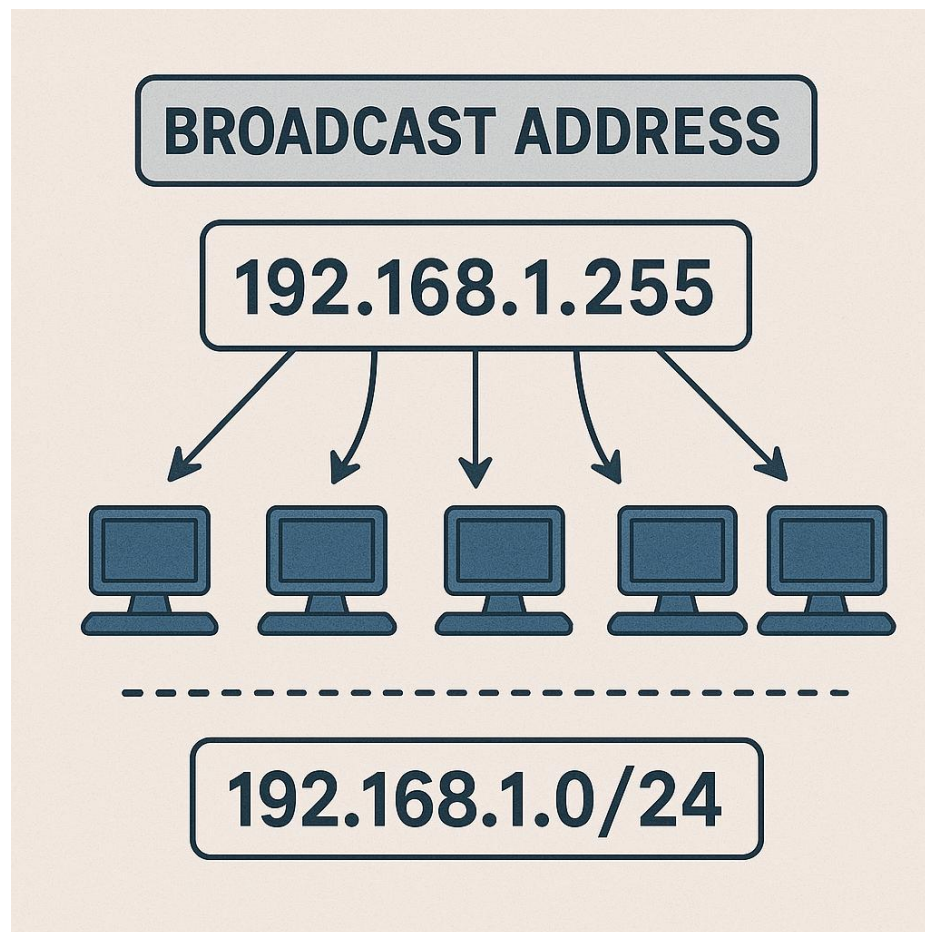
# Adresa všesměrového vysílání - broadcast

**Broadcast adresa v síti IPv4** slouží k odeslání dat *všem zařízením* (hostům) v dané podsíti najednou.

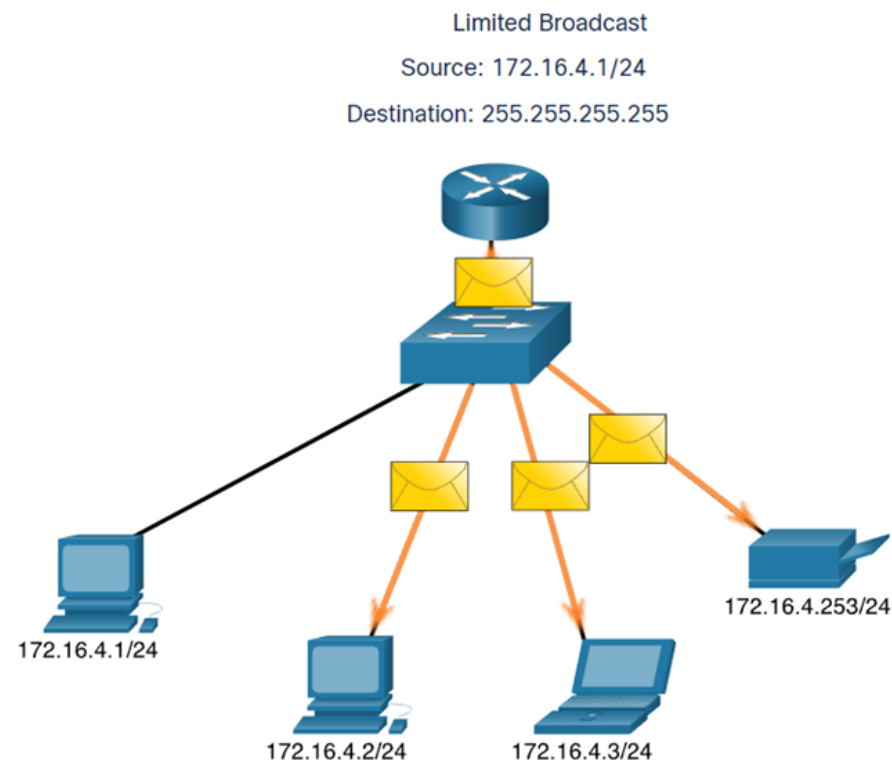
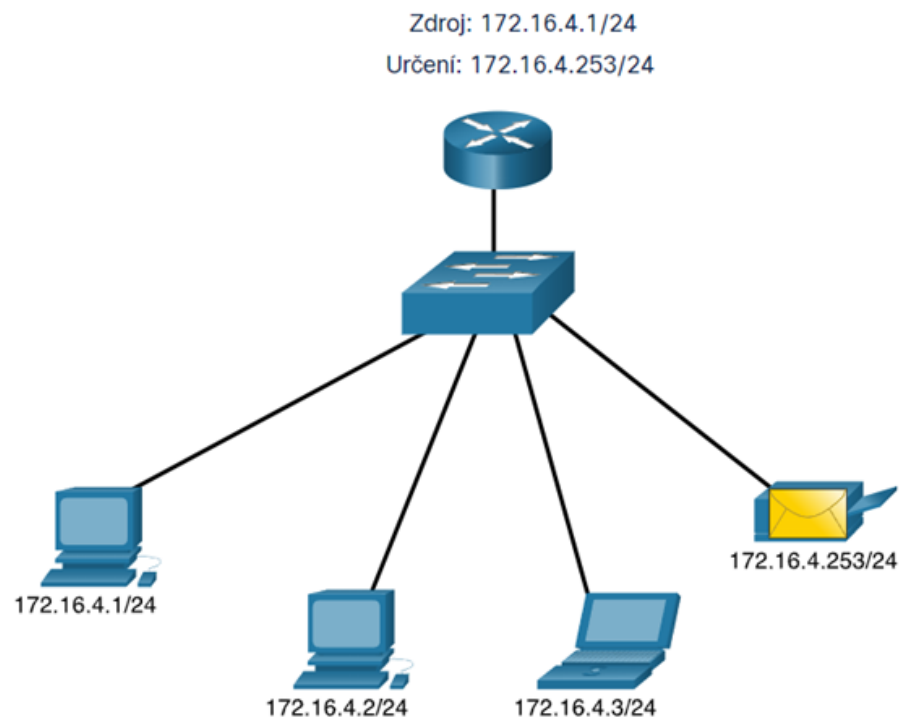
- broadcast adresa je poslední adresa v rozsahu dané podsítě
- když zařízení odešle paket na tuto adresu, dorazí ke všem aktivním zařízením v síti (např. všem počítačům)

Používá se například při:

- vyhledávání jiných zařízení (např. ARP dotazy)
- zasílání informací bez znalosti konkrétní IP adresy cíle



# Vysílání v IPv4 – unicast a broadcast



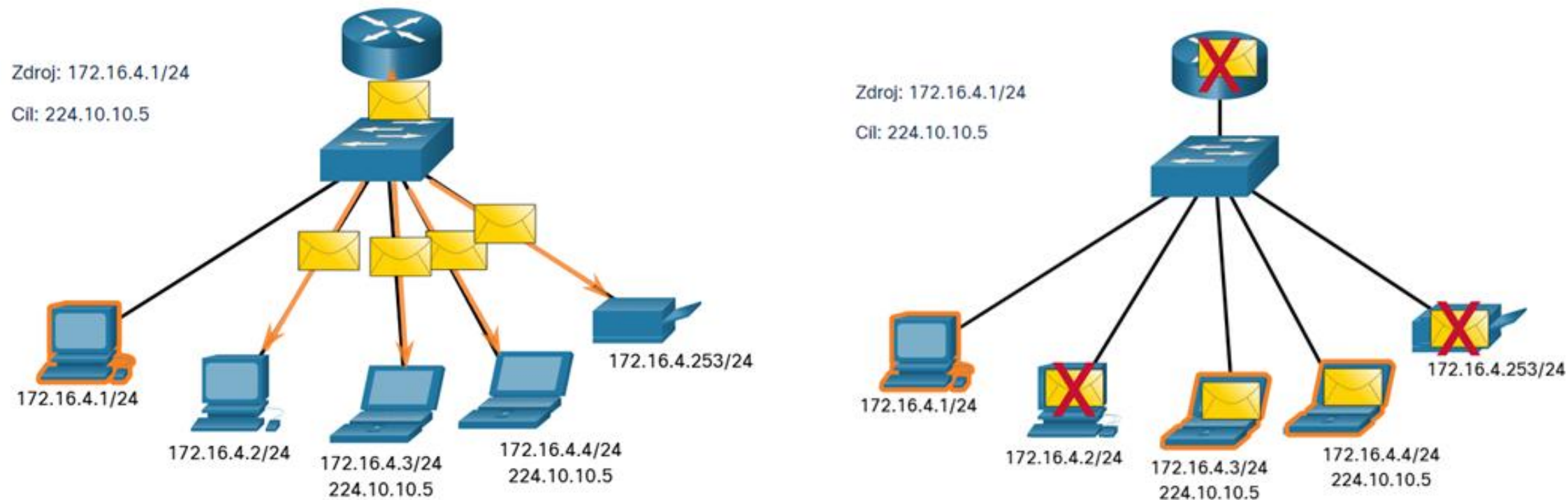
Broadcast paket má cílovou IP adresu se všemi jedničkami (např. 172.16.4.255), nebo 32 jednorázovými (1) bity (na obrázku).

**ALE, POZOR**

**Ve výchozím nastavení routery všesměrové vysílání nepřeposílají!**



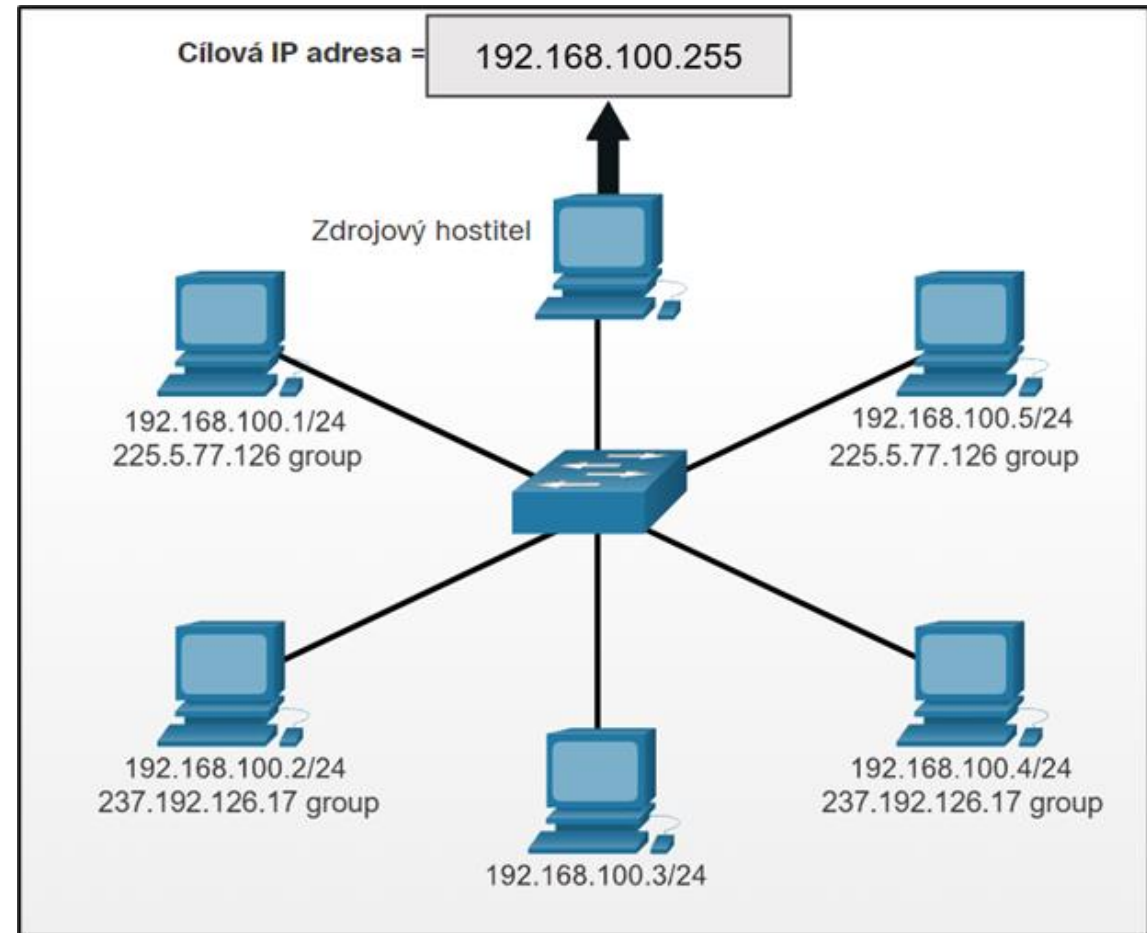
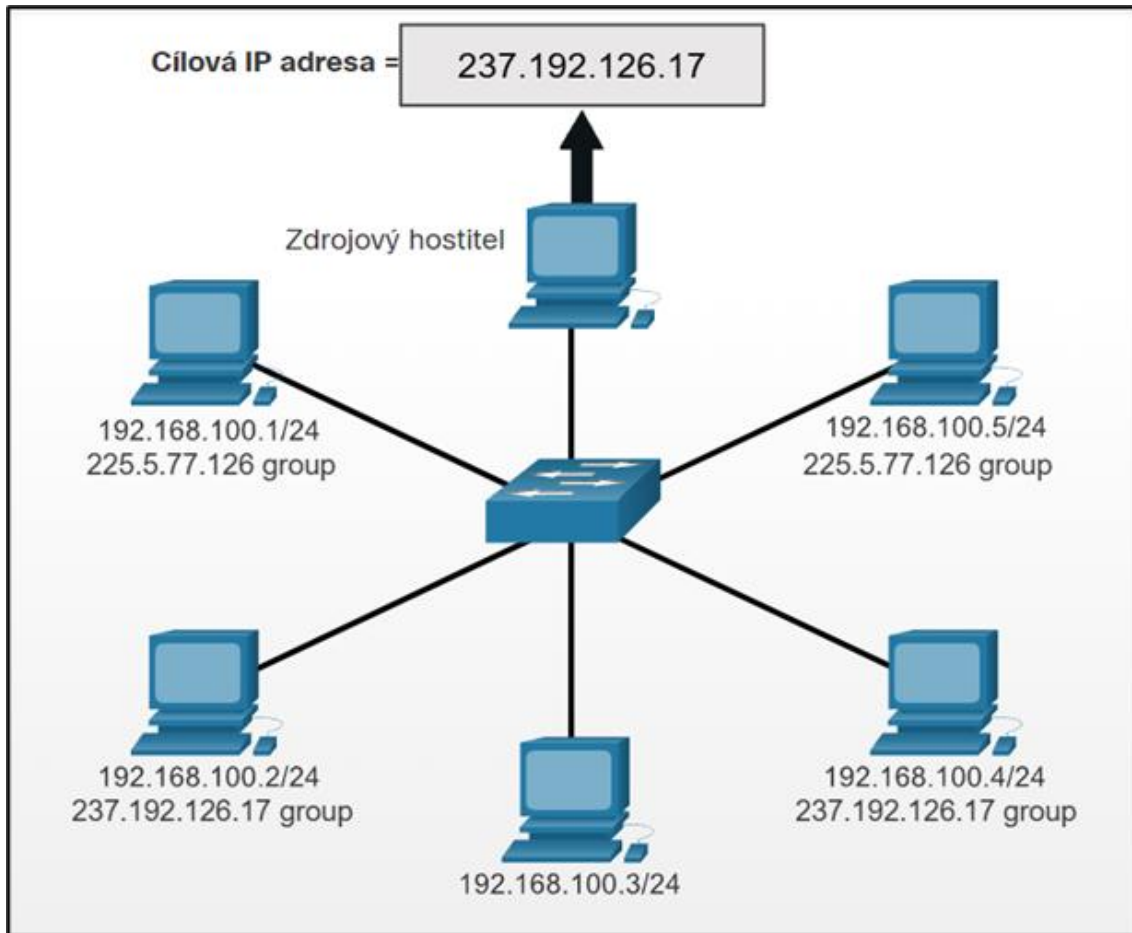
# Vysílání v IPv4 – multicast



Přenos multicastového vysílání snižuje provoz tím, že umožňuje hostiteli odeslat jeden paket vybrané sadě hostitelů, kteří se přihlásí k odběru skupiny multicastového vysílání.

Paket multicastového vysílání je paket s cílovou adresou IP, která je adresou multicastového vysílání. Protokol IPv4 vyhradil adresy 224.0.0.0 až 239.255.255.255 jako rozsah multicastového vysílání.

# Komu to půjde?



# Zdroje

- Cisco: výukový portál Netacad.com
- Jiří Peterka – [www.e-archiv.cz](http://www.e-archiv.cz) (sborník přednášek Počítačové sítě II)
- Adresování v IP sítích | SAMURAJ-cz.com dostupné na: <https://www.samuraj-cz.com/clanek/adresovani-v-ip-sitich/>
- přednáška Ing. V. Bohaty (SPŠMB)

*"Části této prezentace byly vytvořeny s využitím generativní umělé inteligence (OpenAI - ChatGPT 4.0, verze z roku 2025) jako podpůrného nástroje pro získávání informací a formulaci textu. Výsledky byly následně editovány a ověřeny autorem."*