



Katedra softwarového inženýrství,
Matematicko-fyzikální fakulta,
Univerzita Karlova, Praha



Rodina protokolů TCP/IP, verze 2.6

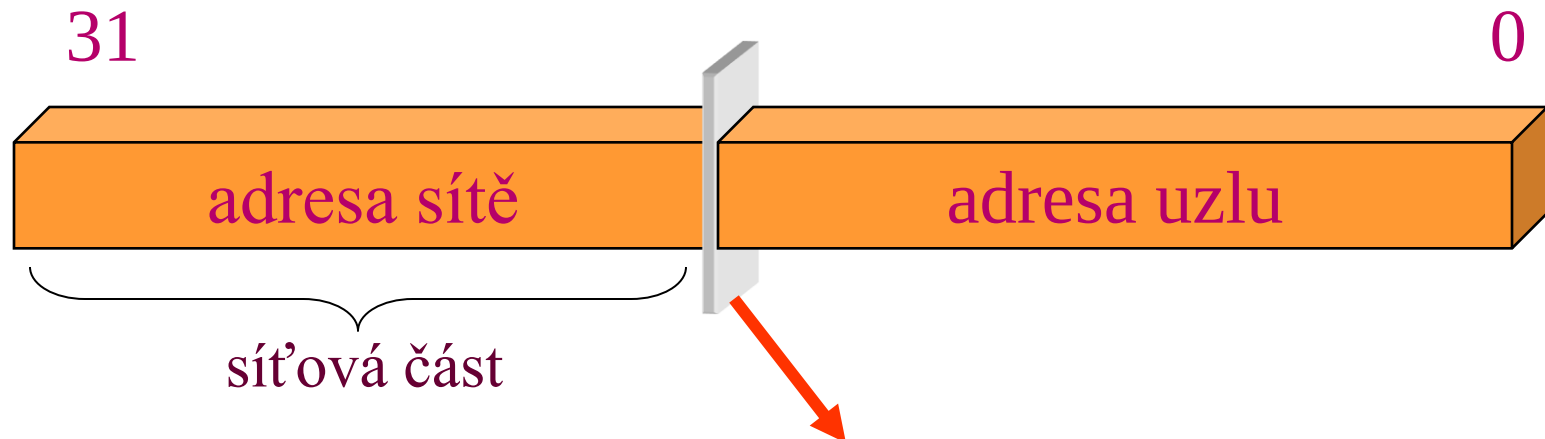
Část 3: IP adresy

Jiří Peterka, 2010

výchozí předpoklady

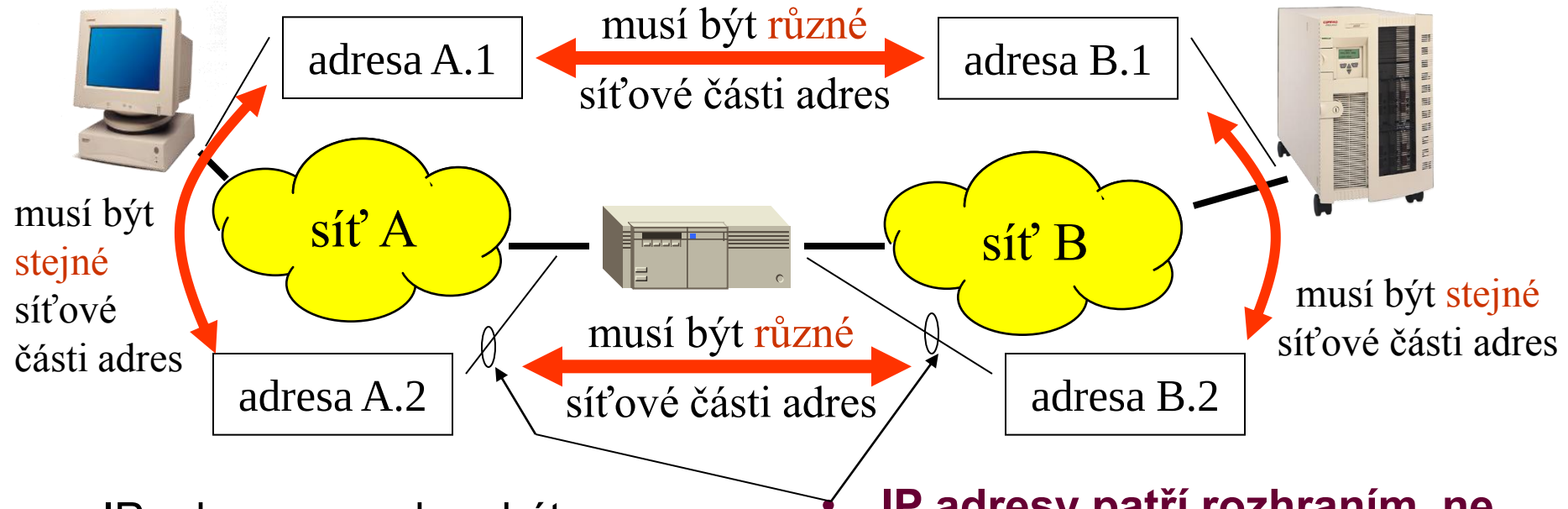
- každý uzel musí mít unikátní IP adresu
 - aby jej bylo možné rozlišit
 - dnes existují výjimky
 - jde o obecné pravidlo, týká se jen "přímo dostupných uzlů", ne uzlů schovaných za firewally
- rozhodnutí autorů TCP/IP:
 - IP adresy budou abstraktní
 - nebudou mít žádný bezprostřední ekvivalent v linkových adresách
 - IP adresy budou všude stejné
 - i "nad" různými typy linkových adres budou IP adresy stejného typu
 - náročné na převodní mechanismy
 - IP adresy budou mít 32 bitů
- IP adresy musí vycházet vstříc potřebám TCP/IP protokolů
- představě katenetového modelu
 - "svět" je složen z:
 - dílčích sítí
 - uzlů (hostitelských počítačů a směrovačů)
- potřebám směrování:
 - směrovací algoritmy se rozhodují na základě příslušnosti přijímajícího uzlu k síti
 - ne na základě "celé" adresy
 - výjimka: host-based route
 - důvod: snaha minimalizovat objem směrovacích tabulek i složitost rozhodování
 - proto musí být možné "extrahovat" z IP adresy identifikaci cílové sítě

důsledek:



- IP adresy jsou
 - **fyzicky** "jednotlivé" (každá má 32 bitů)
 - **logicky** dvousložkové, mají
 - **sít'ovou část** (s adresou sítě, identifikující síť jako celek)
 - (relativní) **adresu uzlu** v rámci sítě
- hranici mezi oběma logickými složkami tvoří bitová pozice
 - sít'ovou část tvoří vyšší bity IP adresy, relativní adresu uzlu zbývající nižší bity
 - **původně**: hranice je pevně dána (ve 3 možných pozicích)
 - **dnes**: hranice je volitelná

způsob přidělování IP adres



- IP adresy nemohou být přidělovány libovolně
 - **musí být respektováno rozdělení na sítě**
 - uzly ve stejné síti musí mít IP adresy se stejnou síťovou částí
 - uzly v různých sítích musí mít IP adresy s různými síťovými částmi

IP adresy patří rozhraním, ne uzlům !!!!

- IP adresy se musí přidělovat po celých blocích
 - se stejnou síťovou částí
- **IP adresy přidělené jedné síti nelze použít v jiné síti !!!!!!!!!!!!!!!**
 - nemá proto smysl je vracet

velikost adresové části IP adres

- důsledek dvousložkového charakteru IP adres:
 - každé síti je vždy třeba přidělit celý blok IP adres
 - všechny IP adresy se stejnou síťovou částí, která přísluší dané síti
 - bez ohledu na to, kolik se jich skutečně využije
 - takto přidělené ale nevyužité adresy není možné "přenechat" jiné síti
- příklad:
 - pokud by síťová část měla "napevno" 16 bitů (a adresa uzlů zbývajících 16 bitů), pak by:
 - každá síť by musela dostat přiděleno celkem 2^{16} (tj. 65536) individuálních IP adres (všechny se stejnou síťovou částí)
 - bez ohledu na skutečný počet uzlů v síti !!!!
- autoři TCP/IP museli pečlivě zvažovat, jak volit velikost síťové části IP adresy
- kdyby zvolili pevnou velikost síťové části (např. 16 bitů), hrozilo by:
 - že bude existovat více sítí než kolik připouští síťová část
 - IP adresy se budou přidělovat po příliš velkých blocích

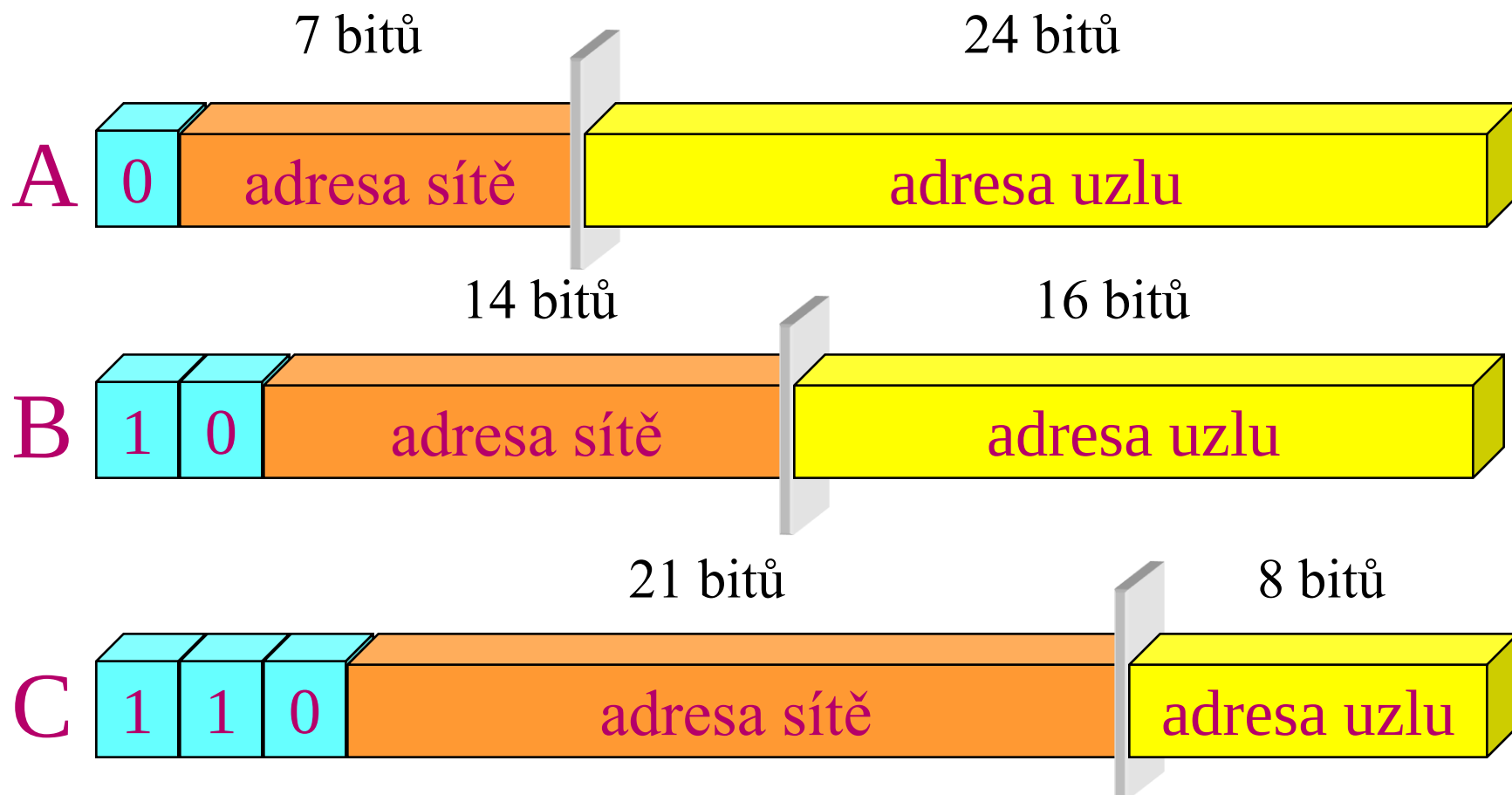


příklad: síť o 2000 uzlech by dostala přiděleno 65536 IP adres, z nich by **97% zůstalo nevyužito** (a bez možnosti využití)

velikost adresové části IP adres

- autoři TCP/IP vyšli z předpokladu že bude existovat:
 - malý počet opravdu velkých sítí
 - vyžadují malou síťovou část, a naopak velkou část pro relativní adresu uzlu
 - střední počet středně velkých sítí
 - měly by mít srovnatelně velkou síťovou i relativní část
 - velký počet malých sítí
 - vyžadují velkou síťovou část, stačí jim malá část pro relativní adresy
 - tomu uzpůsobili i velikost síťové části IP adresy
 - má 3 možné polohy, které odpovídají 3 třídám adres
 - **třída A**
 - pro velmi velké sítě, poloha hranice 8:24 (rozděluje 32bitů na 8 a 24)
 - **třída B**
 - pro středně velké sítě, 16:16
 - **třída C**
 - pro malé sítě, 24:8
- 
- tímto se autoři snažili zmenšit plýtvání s IP adresami

představa IP adres – třídy A, B a C



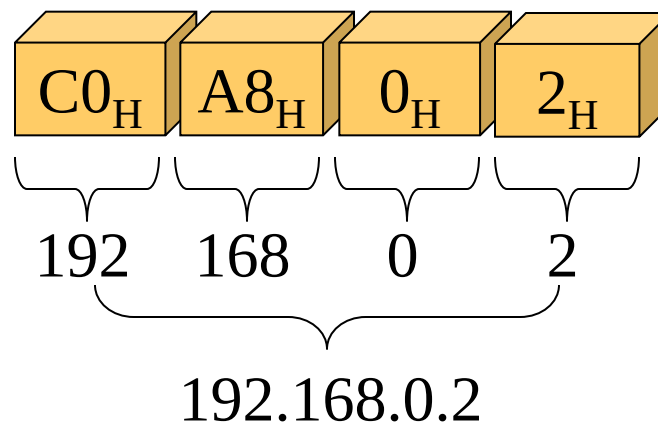
symbolický zápis IP adres

- IP adresu lze chápat jako jedno velké (32-bitové) binární číslo

- ale to se špatně zapisuje i čte

- používá se jednotný způsob zápisu:

- obsah každého bytu je vyjádřen jako desítkové číslo
 - jednotlivé části jsou spojeny tečkou
 - příklad: 193.84.57.34
 - příklad: 147.3.1.3



- třída A:
 - od 1.x.x.x do 126.x.x.x
- třída B:
 - od 128.0.x.x do 191.255.x.x
- třída C:
 - od 192.0.0.x do 223.255.255.x

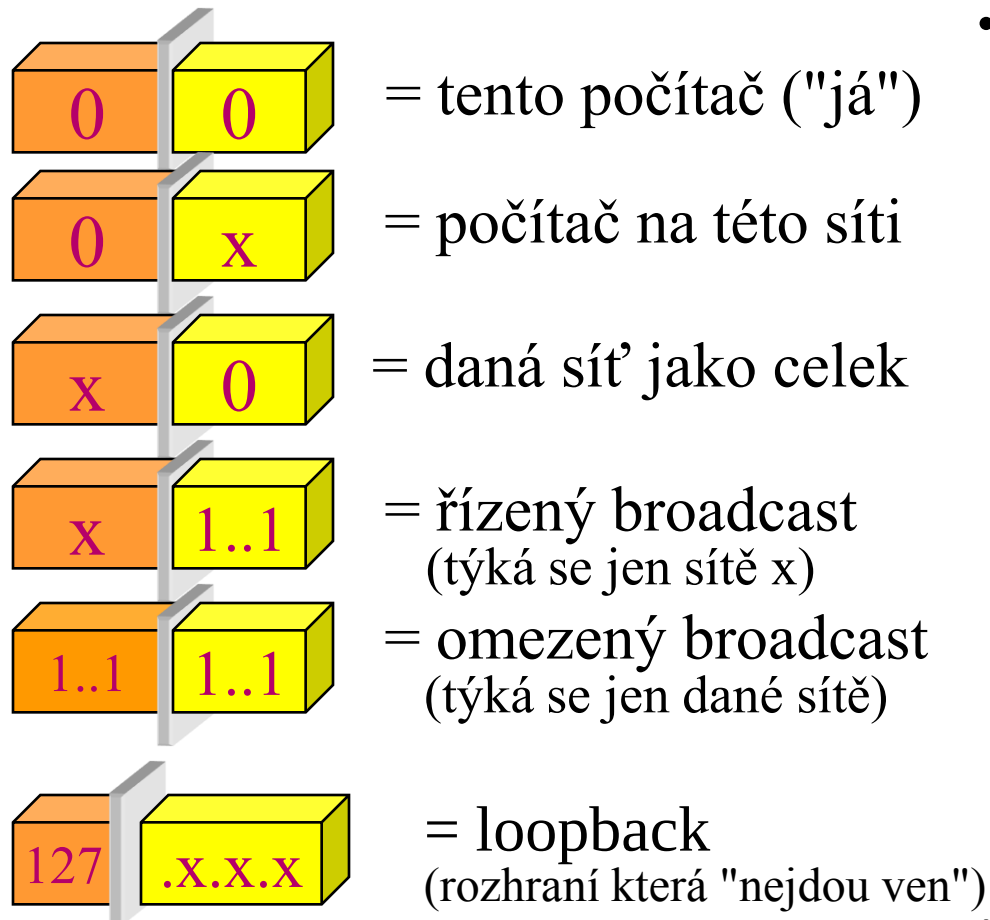
terminologické odbočení

- IP adresy se přidělují po celých blocích
 - odpovídajících adresám se stejnou síťovou částí (stejnou adresou sítě)
 - v případě adres třídy C jde o 256 individuálních IP adres
 - v případě adres třídy B jde o 65536 IP adres
 -
- když se řekne "získat jednu adresu třídy C"
 - míní se tím získání 256 individuálních IP adres
 - 256 čísel z množiny všech 32-bitových čísel
 - analogicky pro třídy B a A



fakticky použitelných je jen
254 adres
(kromě obou "krajních")

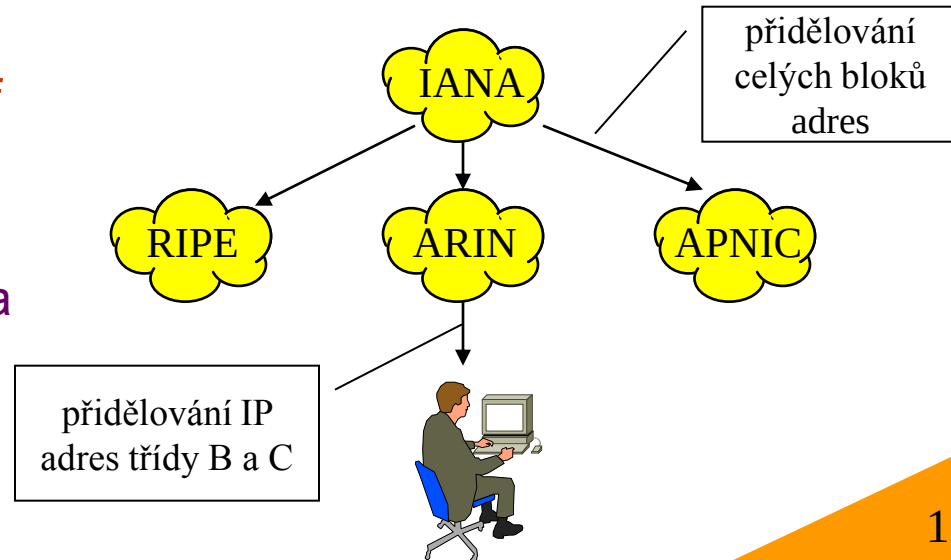
speciální adresy



- existují ještě dvě speciální třídy IP adres:
 - **třída D** je určena pro tzv. **multicasting** (skupinový přenos)
 - třídu D tvoří adresy 224.0.0.0 až 239.255.255.255
 - **třída E** je vyhrazena pro **budoucí využití**
 - třídu E tvoří adresy 240.0.0.0 až 255.255.255.255
 - třída E nebyla fakticky využita pro rozšíření (IP adresy v IPv6)
- adresy třídy D a E nejsou logicky dvousložkové
 - lze je přidělovat jednotlivě

způsob distribuce IP adres

- **zásada:**
 - žádná IP adresa nesmí být přidělena dvakrát
 - dnes již existují výjimky
- **řešení:**
 - bude existovat centrální autorita, která je bude přidělovat
 - původně bylo touto autoritou středisko SRI NIC (při Univ. of Stanford v USA, později přejmenované na IANA)
 - každý zájemce z celého světa žádal přímo SRI NIC, ta přidělovala adresy přímo
 - časem se to stalo organizačně neúnosné
- **další vývojové stádium:**
 - centrální autoritou se stala organizace IANA
 - IANA přidělovala celé bloky IP adres regionálním "přidělovatelům," (tzv. **RIR, Regional Internet Registry**)
 - RIPE (Evropa)
 - APNIC (Asie a Pacific)
 - Internic (ARIN, v USA)



problém s (původními) IP adresami

- úbytek IP adres byl velký
 - původně se nepočítalo s tak velkým zájmem
 - přidělování po celých třídách (A, B a C) bylo ve většině případů plýtváním
 - přidělovalo se "nejbližší vyšší" kvantum
 - např. pro síť o 1000 uzlech se přidělila 1 adresa třídy B
 - fakticky 65536 IP adres
 - využilo se jen 1000

začalo hrozit vyčerpání 32-bitového prostoru všech IP adres !!!!

problémem byla malá "granularita" tříd IP adres (nebylo možné se jemněji přizpůsobit skutečné velikosti sítě)

- IAB začala zvonit na poplach
 - založila v IETF celou oblast (Area) věnovanou řešení tohoto problému
 - vypsala se výzva k předkládání řešení
 - začalo se měřit, jak dlouho adresy ještě vydrží ...

čerpání IPv4 adres v čase

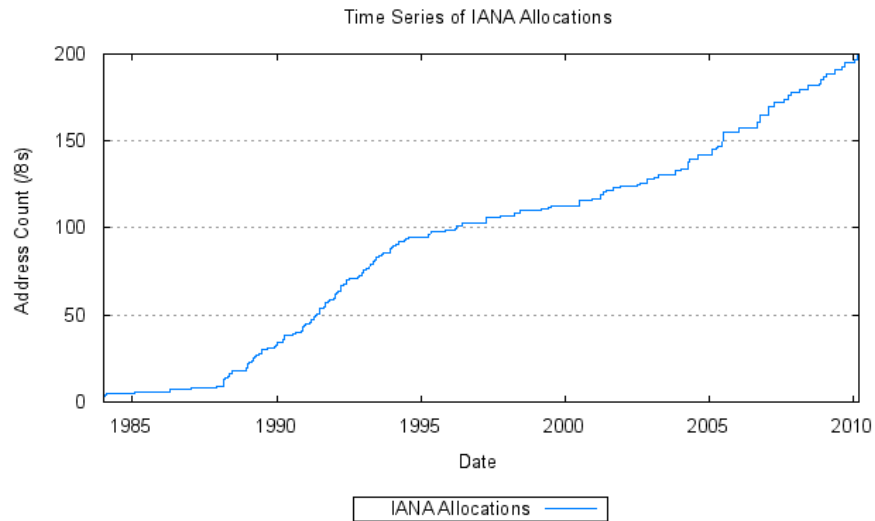


Figure 6 - Cumulative IANA Address allocations

- jednotkou na grafu jsou CIDR bloky prefixem 8 bitů
 - tj. obdoba 1 adresy třídy A, resp. 2^{24} IP adres
- zdroj: Jeff Houston, www.potaroo.net
- aktuální odhady vyčerpání IPv4 prostoru:
 - na úrovni IANA: 27. září 2011
 - na úrovni RIR: 15. září 2012

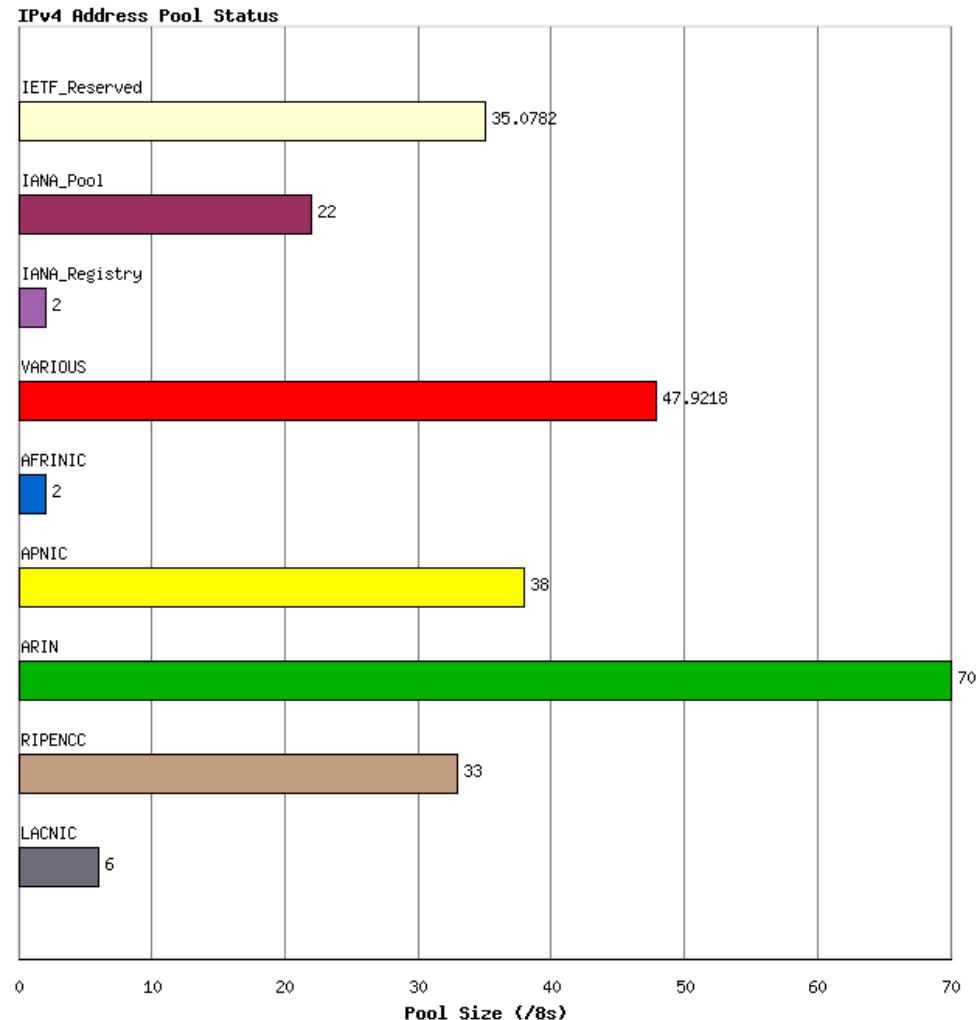


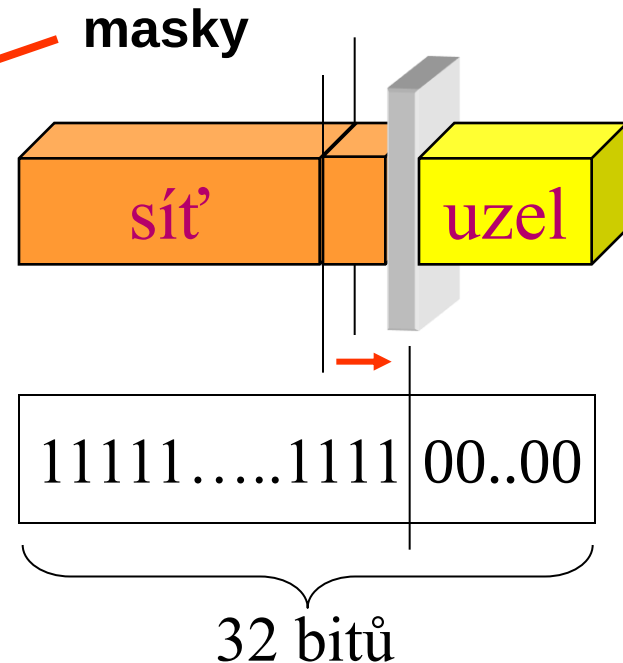
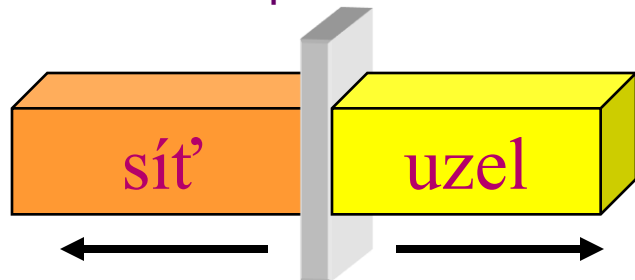
Figure 2 - Address allocations to RIRs

přehled řešení problému

- "okamžité" řešení:
 - přidělovat IP adresy v násobcích "největších nižších" kvant
 - příklad: síť, 1000 uzlů
 - dříve: dostala by 1 x B
 - nyní: dostane 4-8 x C
 - problém: bobtnají směrovací tabulky
 - **subnetting**
 - další (lokální) dělení skupin IP adres v podsítích
 - s jediným vstupním bodem
 - viditelnost je pouze lokální
- dočasná řešení
 - **privátní IP adresy**
 - možnost použít stejné adresy vícekrát, v privátních sítích
 - "prostupnost" mezi veřejnou a privátní sítí může být řešena:
 - na aplikační vrstvě, pomocí firewallů
 - na síťové vrstvě, pomocí **překladu IP adres (NAT/PAT)**
 - **CIDR** (Classless Interdomain Routing)
 - možnost přidělovat IP adresy po libovolných kvantech
 - které jsou mocninou 2
- "definitivní" řešení
 - **IPv6**
 - 128-bitové adresy

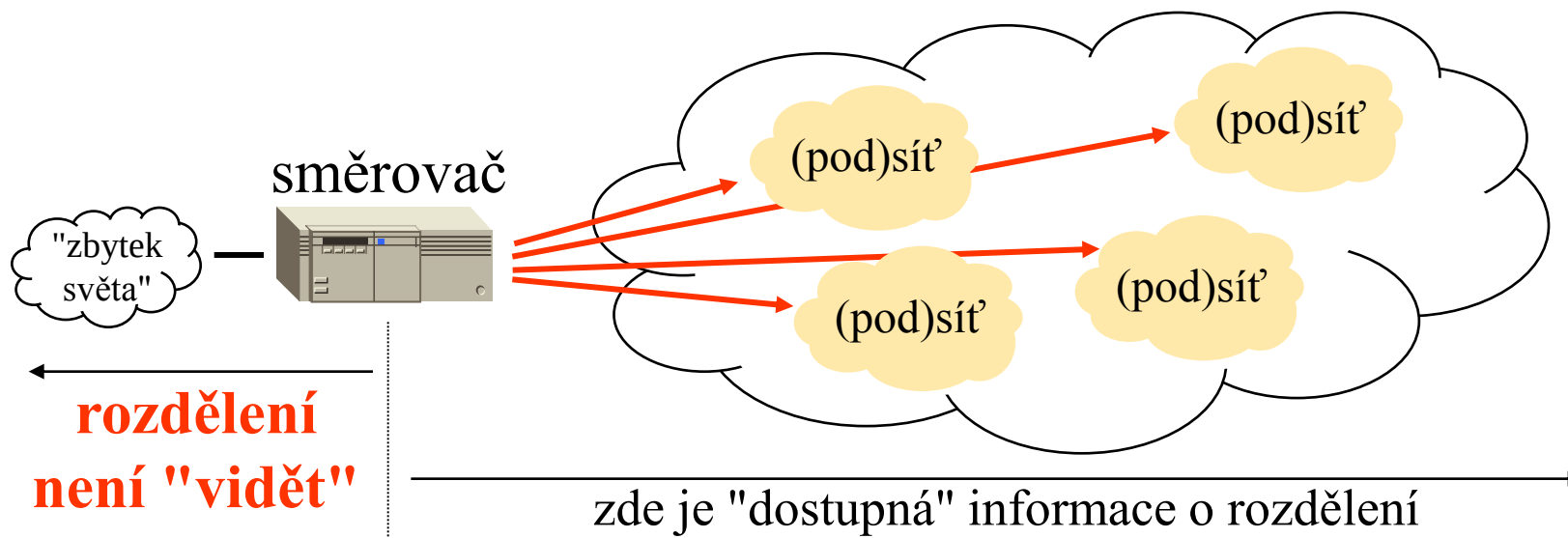
možnost zjemnění granularity

- princip řešení:
 - jemnější "granularitu" tříd IP adres by bylo možné dosáhnout posunem hranice (bitové pozice) mezi síťovou částí a relativní adresou uzlu
- problém:
 - původní mechanismy práce s IP adresami na to obecně nebyly připraveny
 - některé ano, ale nešlo se na to spoléhat
- nutnost použití masky:
 - u tříd je hranice (bitová pozice) určena nejvyššími bity
 - jemnější nastavení hranice musí být určeno jiným způsobem – pomocí tzv. masky



princip subnetting-u

- idea:
 - hranice (bitová pozice) se posune směrem k nižším bitům
 - tj. adresy uzlů se rozdělí na několik skupin
 - velikosti mocniny 2, aby to byl posun o celé bitové pozice
 - použijí se masky
 - **vše se udělá někde "izolovaně"** (v rámci jedné soustavy dílčích sítí)
 - a informace o tomto rozdělení není šířena "do světa"

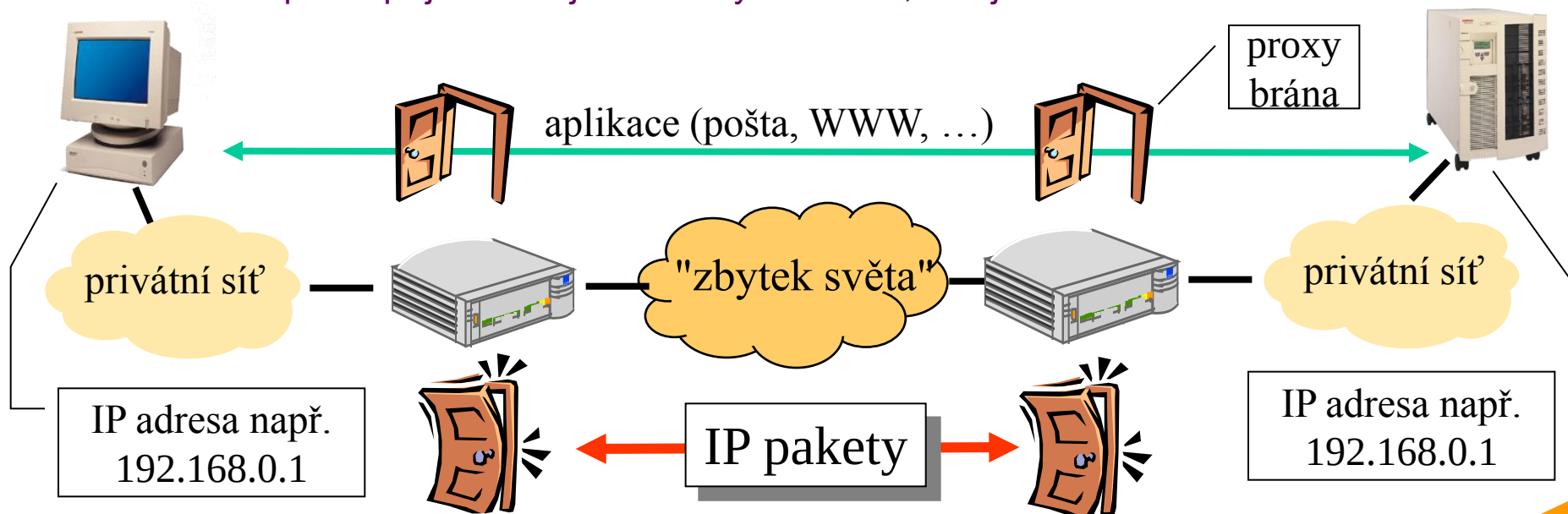


smysl subnettingu

- jde o možnost využít 1 síťovou adresu (třídy A, B či C) pro více sítí
 - jinak by to musely být samostatné síťové adresy
 - příklad:
 - díky subnettingu 4 malé sítě vystačí dohromady s 1xC (256 individuálních adres)
 - bez subnettingu by spotřebovaly 4xC (4x256, tj. 1024 individuálních IP adres)
- lze ale využít jen tam, kde soustava sítí má jeden vstupní bod
 - neboť informace o rozdělení (pomocí masky) není šířena "do světa"
 - a kdyby bylo více vstupních bodů, nevědělo by se který z nich vybrat
- není to problémem tam, kde má soustava sítí stromovitou strukturu
 - subnetting lze použít v podstromu

privátní IP adresy

- co brání vícenásobnému použití IP adres?
 - to, že by směrovací algoritmy nevěděly, kam doručovat IP pakety
- idea: tam, kde nebude existovat přímá komunikace (nutnost směrovat) by se adresy mohly opakovat
 - tato situace nastává v sítích bez přímé IP konektivity ("**privátních sítích**"), které jsou odděleny od "ostatního světa" vhodnou bránou (firewallem)
 - "prostup" je zde zajištěn na vyšší vrstvě, než je vrstva síťová!!

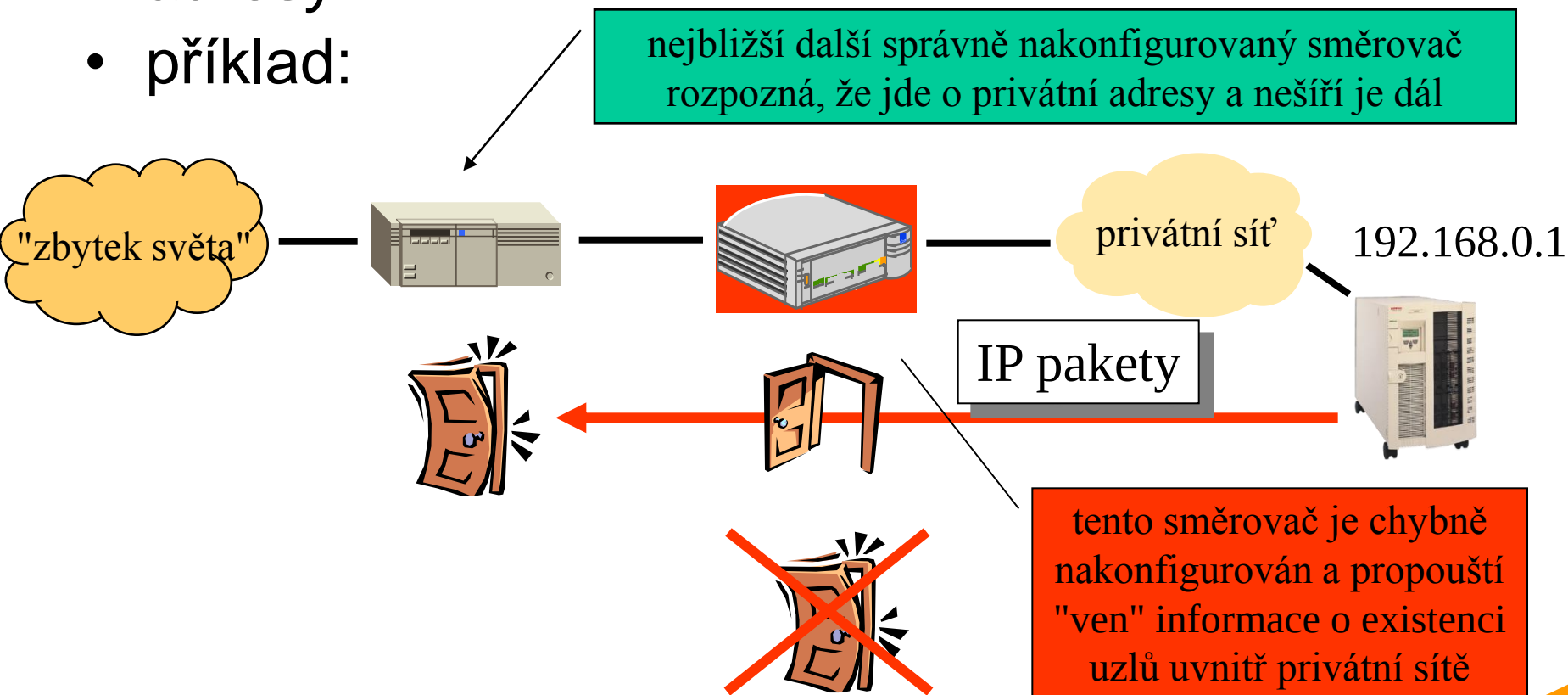


privátní IP adresy

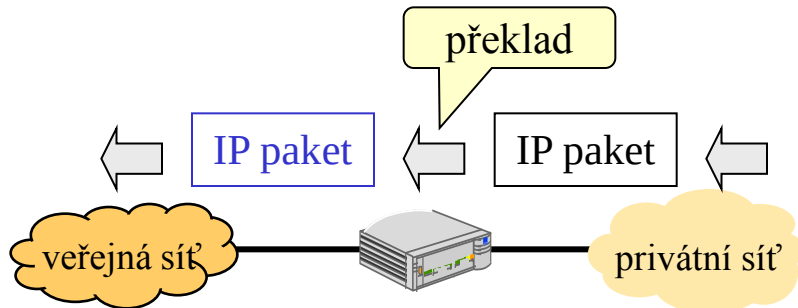
- podmínka fungování:
 - na hranicích privátních sítí je třeba zastavit šíření směrovacích informací
 - "ohlašujících" existenci uzlů uvnitř privátních sítí
 - důsledek:
 - v privátních sítích lze použít v zásadě libovolné IP adresy
 - uvnitř jedné privátní sítě musí být jednoznačné
 - v různých privátních sítích mohou být použity stejné IP adresy
 - doporučení:
 - nepoužívat úplně libovolné IP adresy, ale takové, které byly k tomuto účelu vyhrazeny (RFC 1597)
 - jsou to adresy:
 - 1x síťová adresa třídy A:
10.0.0.0 – 10.255.255.255
 - 16x adresa třídy B:
– 172.16.0.0 – 172.31.255.255
 - 256x adresa třídy C
– 192.168.0.0 –
192.168.255.255
- je vhodné používat i tam, kde
sít' není (nechce, nebude)
připojena k Internetu

privátní IP adresy

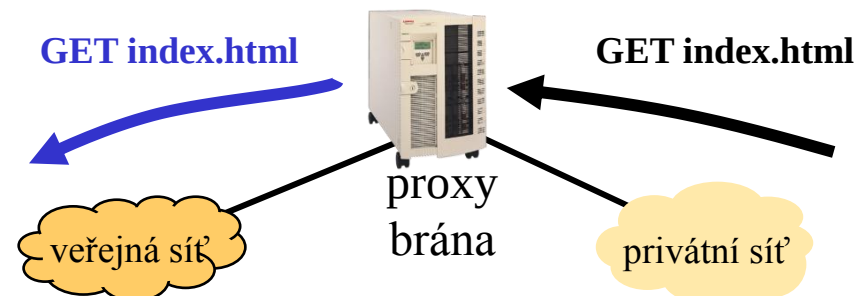
- proč je vhodné používat v privátních sítích vyhrazené ("privátní") IP adresy, a ne libovolné IP adresy?
- příklad:



jak zajistit "průchod" z/do privátních sítí?



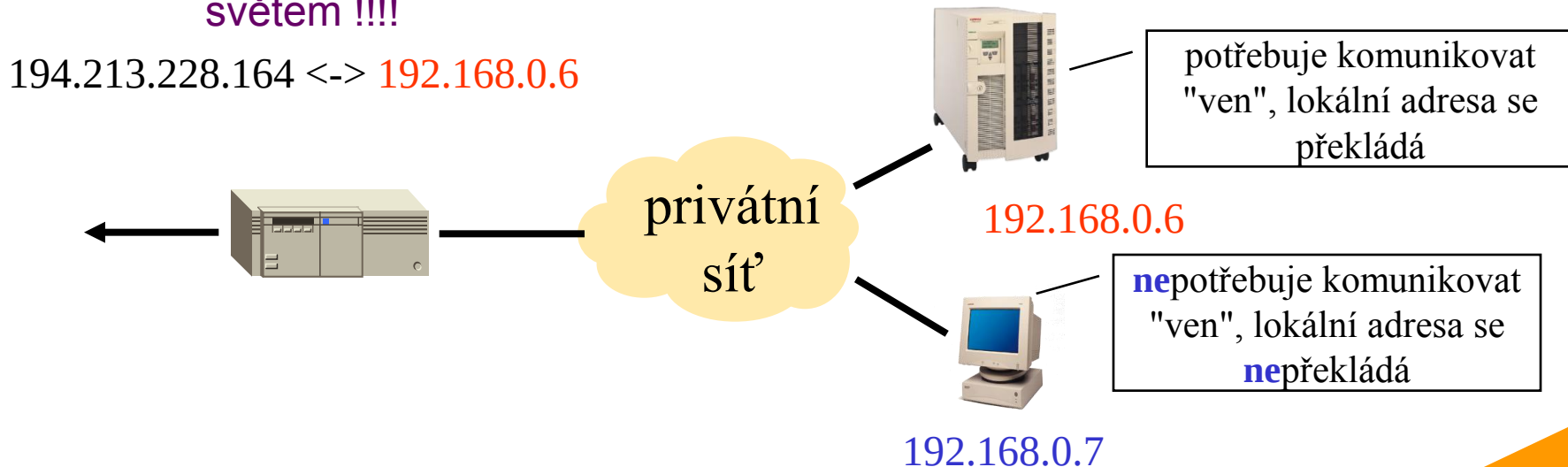
- na síťové vrstvě
 - dochází k průběžnému překladu mezi "veřejnými" a "privátními" IP adresami
 - NAT – Network Address Translation
 - pro aplikace není překlad viditelný
 - aplikace není nutné speciálně nastavovat
 - řešení je "aplikačně nezávislé"
 - funguje (obecně) pro všechny aplikace
 - ale pro některé speciálnější aplikace fungovat nemusí
 - » pokud vkládají zdrojové adresy do nákladové části IP paketů, kde nejsou překládány



- na aplikační vrstvě
 - na rozhraní mezi veřejnou a privátní sítí je proxy brána
 - má dvě síťová rozhraní, do veřejné i privátní sítě
 - není přístupná na síťové vrstvě
 - často je proxy brána součástí firewallu
 - pro aplikace uvnitř privátní sítě je toto řešení viditelné
 - aplikace musí být nastaveny tak, aby používaly proxy bránu
 - řešení je "aplikačně závislé"
 - pro každou aplikaci musí být (samostatná) proxy brána

NAT – Network Address Translation

- překládá (mění "za chodu") IP adresy (RFC 1631)
 - používá se na rozhraní mezi privátní sítí a veřejným Internetem
 - překládá lokální (privátní, vícenásobně použitelné) adresy na veřejné (unikátní) adresy
 - poskytuje zabezpečení
 - lokální adresy "nejsou vidět" z veřejné sítě
 - šetří IP adresy
 - pokud jen část lokálních uzlů potřebuje komunikovat s vnějším světem !!!!



varianty NAT-u

pokud: vztah mezi "vnitřními" a "vnějšími" IP adresami je 1:1

statický NAT

- vztah mezi "vnitřními" a "vnějšími" IP adresami je pevně dán
 - má statický charakter
- vnitřní uzly mohou být přístupné z vnější sítě
 - lze využít například při "stěhování" mezi ISP
 - bez nutnosti měnit IP adresy dle CIDR

• dynamický NAT

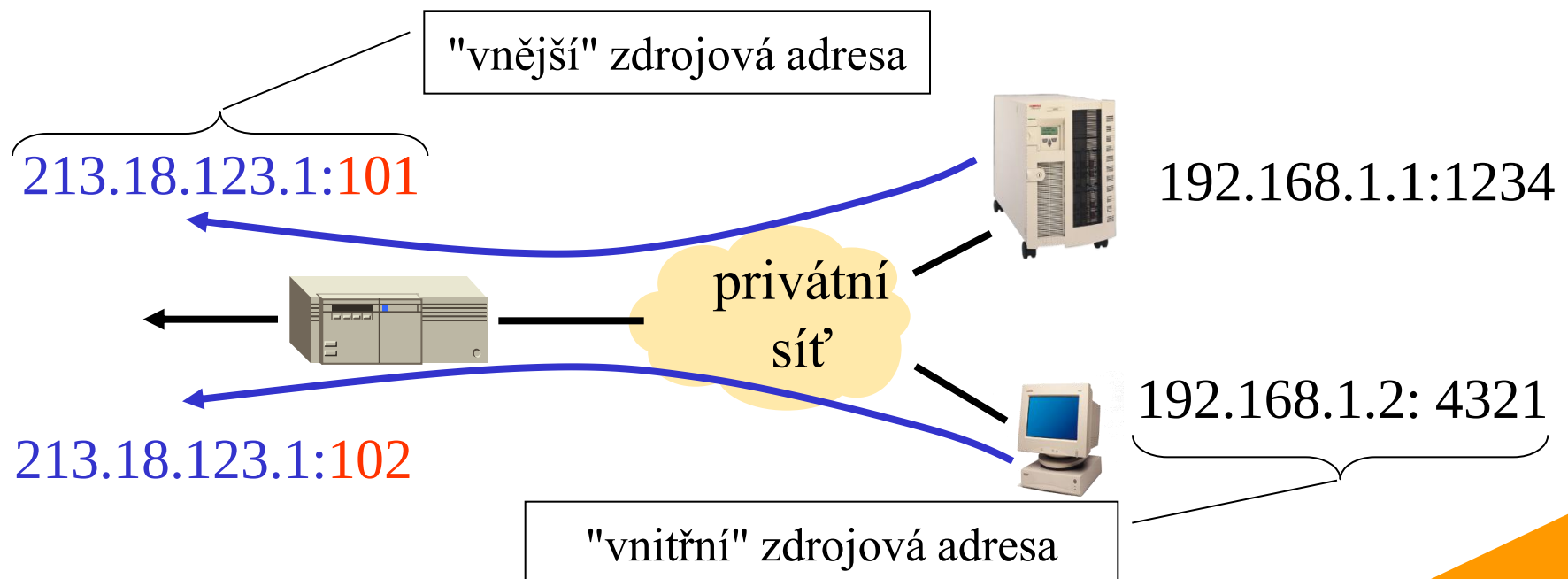
- "vnitřním" IP adresám jsou přiřazovány "vnější" IP adresy dynamicky, podle potřeby
 - vnitřní uzly nejsou obecně dostupné z vnějšku
 - lze ušetřit "vnější" IP adresy
 - pokud některé vnitřní uzly nepotřebují

varianty NAT-u, PAT

pokud: vztah mezi "vnitřními" a "vnějšími" IP adresami je 1:N

"overloading", alias: PAT (Port Address Translation)

- všechny "vnitřní" IP adresy se mapují do 1 vnější IP adresy
 - "rozlišující" informace se uchovávají v číslech portů



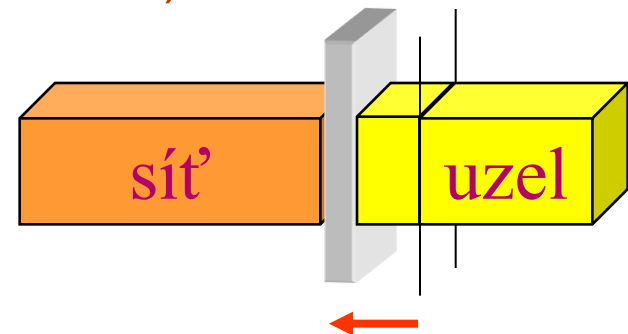
výhody NAT/PAT

- overloading, PAT, též: NAT 1:N
 - dokáže využít 1 veřejnou adresu pro "hodně" uzlů v privátní síti
 - používají to ISP (Internet Service Provider) u některých služeb
 - např. Eurotel Data Nonstop přes APN internet
 - dříve ADSL
- nebezpečí (pro NAT obecně):
 - nelze navazovat spojení směrem dovnitř
 - pro některé aplikace/služby nemusí NAT fungovat vůbec
 - pro takové, které přenáší IP adresy i jinde než v hlavičce (kde o tom NAT neví a nemůže adresy měnit – např. IPSEC)
 - "inteligentní NAT"
 - snaží se rozpoznat konkrétní protokoly, které skrz něj prochází, a mění IP adresy i v těle IP paketů

mechanismus CIDR

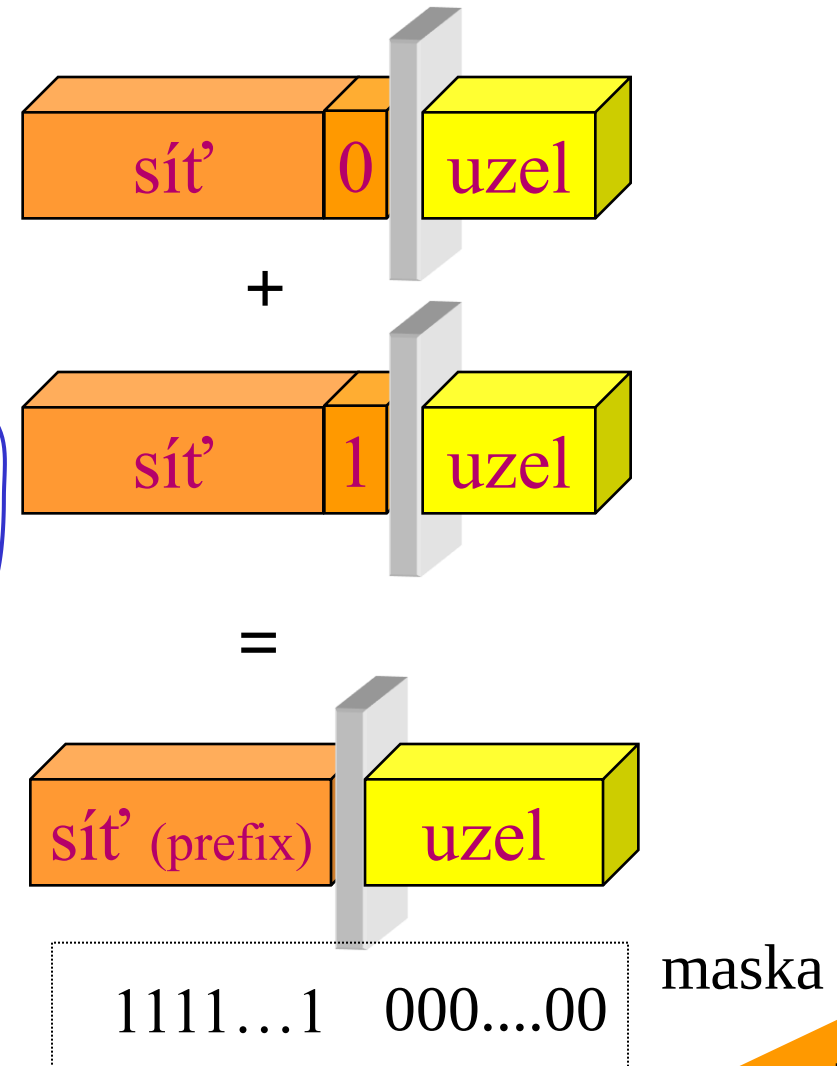
Classless InterDomain Routing

- řeší problém úbytku IP adres
 - umožňuje přidělovat koncovým sítím "přesně velké" skupiny IP adres
 - v zásadě to nahrazuje původní systém tříd A, B a C
- řeší problém nárůstu směrovacích tabulek
 - dosud platilo: co 1 síťová adresa třídy A, B nebo C, to jedna položka ve směrovací tabulce
 - směrovací tabulka se prohledává při každém rozhodnutí o volbě směru
- princip mechanismu CIDR
 - je v zásadě inverzní k subnettingu
 - také se tomu říká **supernetting**
 - předpokládá posun hranice (bitové pozice) mezi síťovou částí a adresou uzlu směrem "doleva" (k vyšším bitům)



princip CIDR-u

- dochází k tzv. agregaci
 - slučování "sousedních" síťových IP adres
 - vzniká 1 výsledná "agregovaná" adresa (adresa supernet-u)
- síťová část je nyní označována jako "prefix"
 - a jeho velikost je vyjadřována v počtu bitů (síťové části)
- **adresy jsou dnes přidělovány zásadně jako tzv. CIDR bloky**
 - např. **194.213.228/24** je CIDR blok odpovídající 1 dřívější síťové adrese C (má 24 bitů prefixu, zbývá 8 na adresu uzlu)

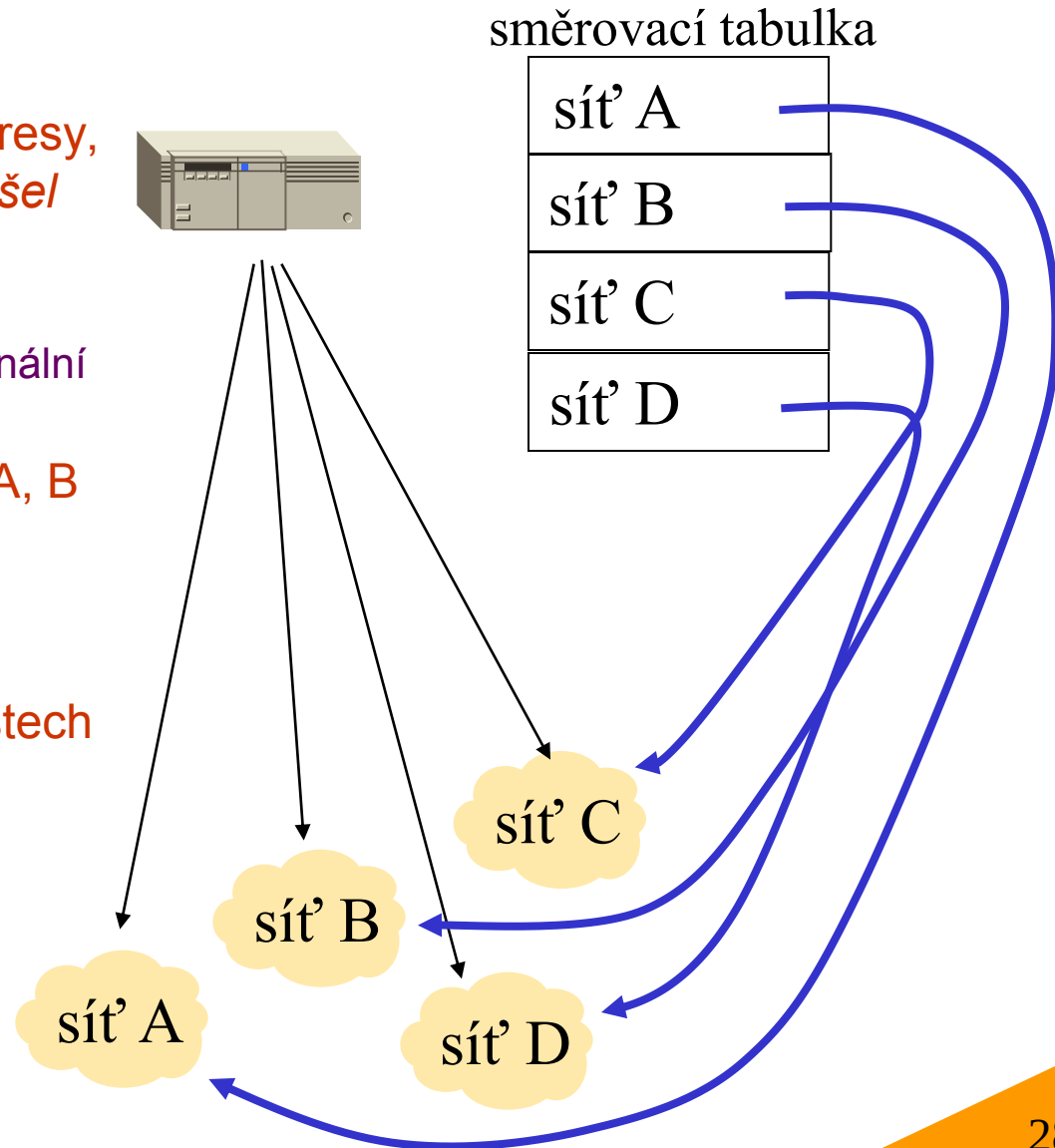


problém směrovacích tabulek

- dříve platilo:

- přidělovaly se celé síťové adresy, a to systémem "*kdo první přišel ...*"
 - nebyl v tom žádný systém, kromě distribuce mezi regionální přidělovatele
- pro každou síťovou adresu (A, B nebo C) musela být ve směrovacích tabulkách samostatná položka
- směrovačům v páteřních částech Internetu začaly přetékat směrovací tabulky

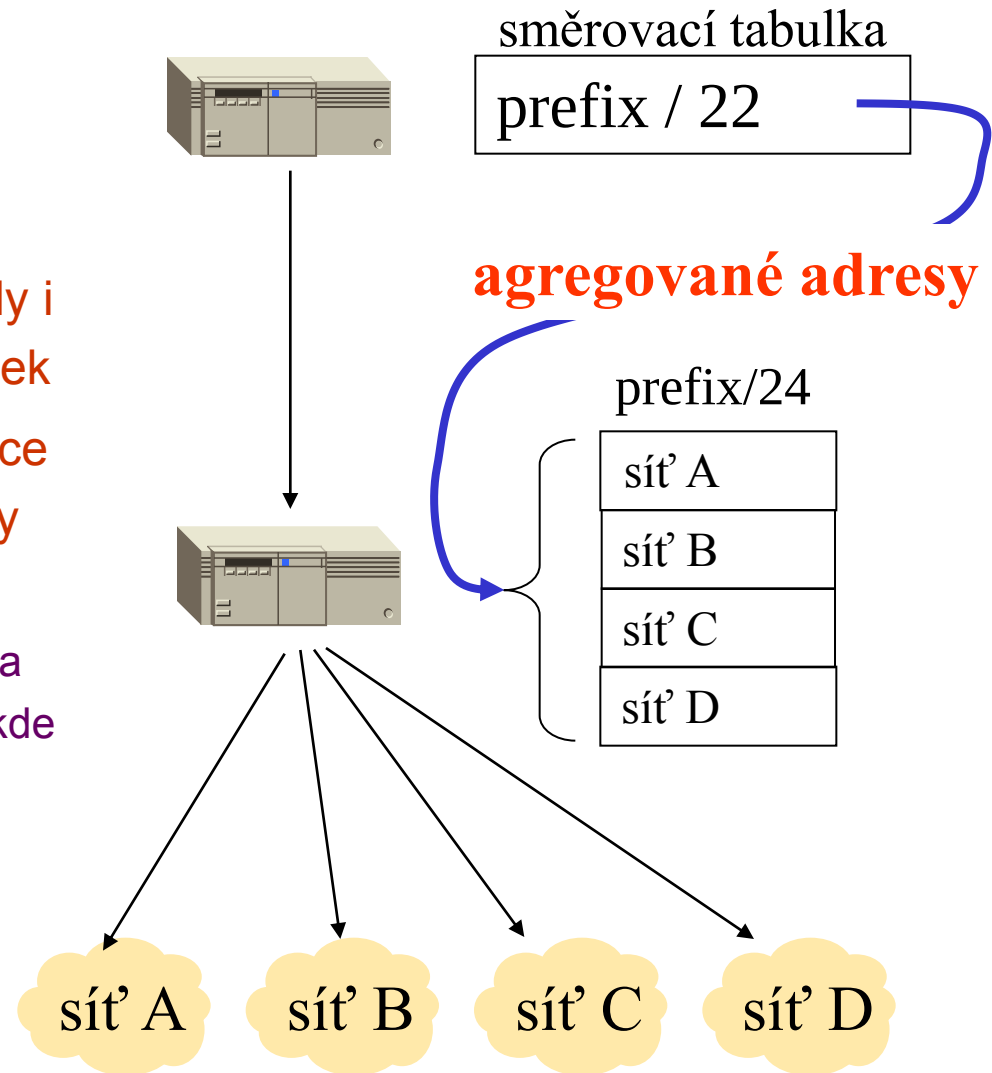
IP adresy byly nezávislé
na způsobu připojení !!



agregace směrovacích informací

- CIDR bloky umožňují agregovat (slučovat) i směrovací informace
 - jakoby: slučovat dohromady i položky směrovacích tabulek
 - detailní směrovací informace nemusí být zbytečně šířeny "do světa"
 - mohou zůstat lokalizována tam, kde jsou zapotřebí, kde vznikají a kde se mění

pozor:
IP adresy se stávají závislými na způsobu připojení !!!!

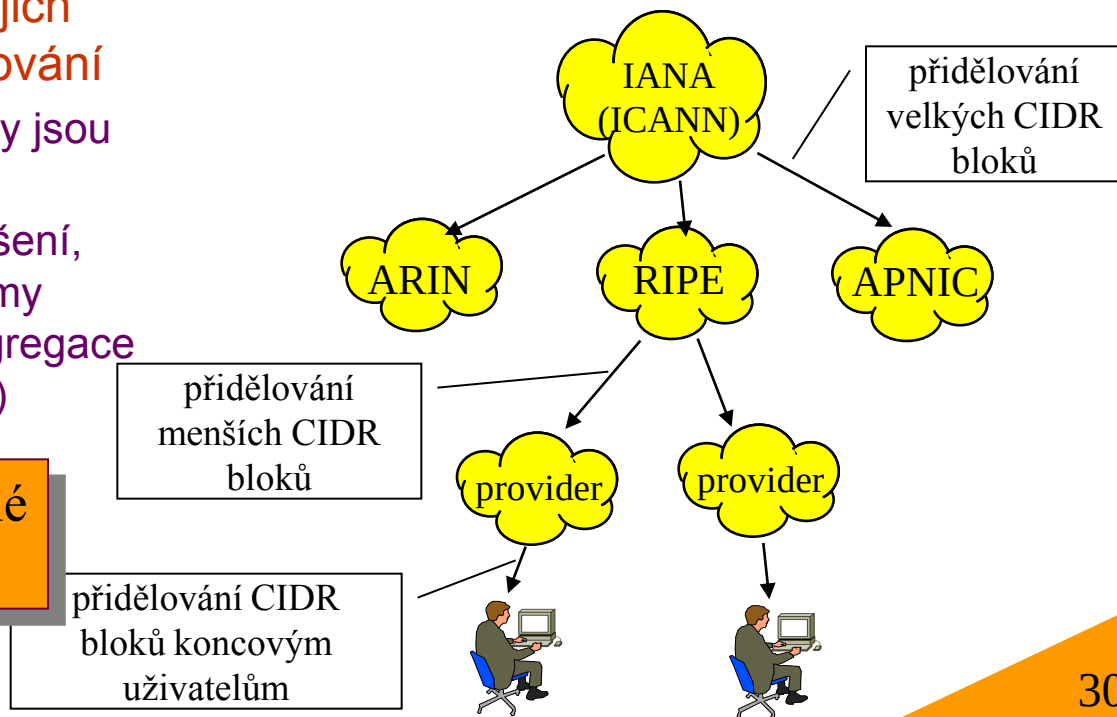


důsledky mechanismu CIDR

- šetří se IP adresami
 - byl dále zpomalen úbytek adres
 - ale příčina problému nebyla odstraněna
- šetří se směrovací tabulky
 - umožnilo to redukovat jejich objem, tím zrychlit směrování
 - ale nepostačuje, tabulky jsou již tak neúnosně velké
 - jsou nutná ještě jiná řešení, např. autonomní systémy (zavádí další stupeň agregace směrovacích informací)

při změně providera musí uživatelé změnit IP adresy svých uzlů !!!

- musel se změnit způsob distribuce IP adres
 - **"přidělovatelem" nyní musí být jednotliví poskytovatelé (ISP)**
 - musí se registrovat u regionálních přidělovatelů



ISP vs. RIPE



- RIPE (Réseaux IP Européens) <http://www.ripe.net/>
 - je regionální přidělovatel IP adres (RIR) pro Evropu
 - jednotliví ISP se u něj registrují, aby mohli dostávat přidělení CIDR bloky IP adres
 - a platí mu příspěvky na provoz
 - v kategoriích: extra large, large, medium, small, very small
 - podle toho mohou dostat různě velké CIDR bloky
 - extra large platí 6750 EUR ročně, extra small 2000 EUR ročně
 - registrace je podle zemí, kde jsou IP adresy využívány
 - za ČR jsou registrováni i zahraniční ISP
 - např. Tiscali (Extra Large), Český Telecom (small), Eurotel (extra small), Holy See - Vatican City State (extra small)

IPv6 – základní principy

- IPv6 rozšiřuje původní 32-bitový adresový prostor IPv4 na 128-bitový
 - ale není to zdaleka jediná změna
 - IPv6 mění řadu dalších aspektů a vlastností IPv4
 - napravuje různé nedostatky, nedomyšlenosti, věci které se neosvědčily, ...
 - např. multicast místo broadcastu,
 - IPv6 přidává řadu nových vlastností
 - např. podporu QoS, podporu bezpečnosti, mobilitu, ...
 - anycast, ...
 - IPv6 není radikálním (zásadním) odklonem od dosavadních principů fungování IP a TCP/IP
- změny týkající se adresování:
 - větší adresový prostor
 - hierarchické členění adresového prostoru
 - a hierarchické přidělování IP adres
 - eliminace "obezliček"
 - jako např. NAT/PAT, ...
 - lepší podpora multicastu
 - v IPv6 je povinný
 - zavedení anycast-u
 - možnost autokonfigurace a přečíslování
 - lepší řešení fragmentace a defragmentace
 - lepší podpora mobility
 - ...

přechod z IPv4 na IPv6

- původní předpoklad:
 - bude to (muset být) velmi brzy
- dnešní situace:
 - "dočasná" řešení uspěla natolik, že potřeba přechodu na IPv6 byla oddálena
 - časový horizont je neurčitý
 - nejdále s přechodem jsou akademické sítě
- kompatibilita:
 - zpětná ano
 - zařízení IPv6 je schopné komunikovat se sítí IPv4
 - dopředná ne
 - zařízení IPv4 není schopné komunikovat se sítí IPv6
- jak je realizována zpětná kompatibilita?
 - strategie koexistence sítí IPv4 a IPv6
 - "dual-stack"
 - zařízení podporuje současně IPv4 i IPv6
 - překlad
 - směrovače s "dual-stack": překládají požadavky mezi IPv4 a IPv6
 - tunelování
 - pakety IPv6 jsou tunelovány (zapouzdřovány, vkládány do) paketů IPv4 a prochází skrz síť IPv4

unicast, multicast a broadcast

- IPv4:

- unicast

- označují právě jeden uzel
 - přesněji: právě jedno síťové rozhraní
 - původně třídy A,B a C
 - dnes adresy dle CIDR

- multicast

- označují skupiny uzlů
 - původně třída D
 - implementace je volitelná a skutečná podpora mizivá

- broadcast

- označuje všechny uzly (v síti)
 - relativní adresu uzlu tvoří samé 1
 - s šířením IP broadcastů byly/jsou problémy

- IPv6:

- unicast

- přidělují se způsobem který připomíná spíše CIDR než třídy A, B a C

- multicast

- nahrazuje broadcast v IPv4
 - jeho podpora v IPv6 je povinná !!!

- anycast

- jedna IP adresa může být přiřazena více uzlům současně
 - reagovat (ozvat se) by měl vždy ten uzel, který je "nejblíže"

symbolický zápis IPv6 adres

- *straight-hex*
 - každé slovo se zapíše jako (4-místné) hexadecimální číslo
 - např.: **805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF**
- *leading zero suppressed*
 - nulová slova se zkrátí na jedinou číslici
 - např.: **805B:2D9D:DC28:0:0:FC57:D4C8:1FFF**
- *zero-compressed*
 - nulová slova se zcela vynechají
 - např.: **805B:2D9D:DC28::FC57:D4C8:1FFF**
- *mixed notation*
 - posledních 32 bitů se zapíše jako u IPv4
 - pro tzv. "embedded IPv4 adresy"
 - např. **::212.200.31.255**

IPv4 adresy - např.: 192.168.1.1

rozdělení adresových prostorů

IPv4 původně (třídy A až E)

třída A: od 1.x.x.x do 126.x.x.x
třída B: od 128.0.x.x do 191.255.x.x
C: od 192.0.0.x do 223.255.255.x
D: od 224.0.0.0 až 239.255.255.255
E: od 240.0.0.0 až 255.255.255.255

měřítko "velmi"
nesouhlasí !!

IPv6 (zjednodušeně)

000.....
001.....
010.....
011.....
100.....
101.....
110.....
111.....

přiděleno
(různé účely)

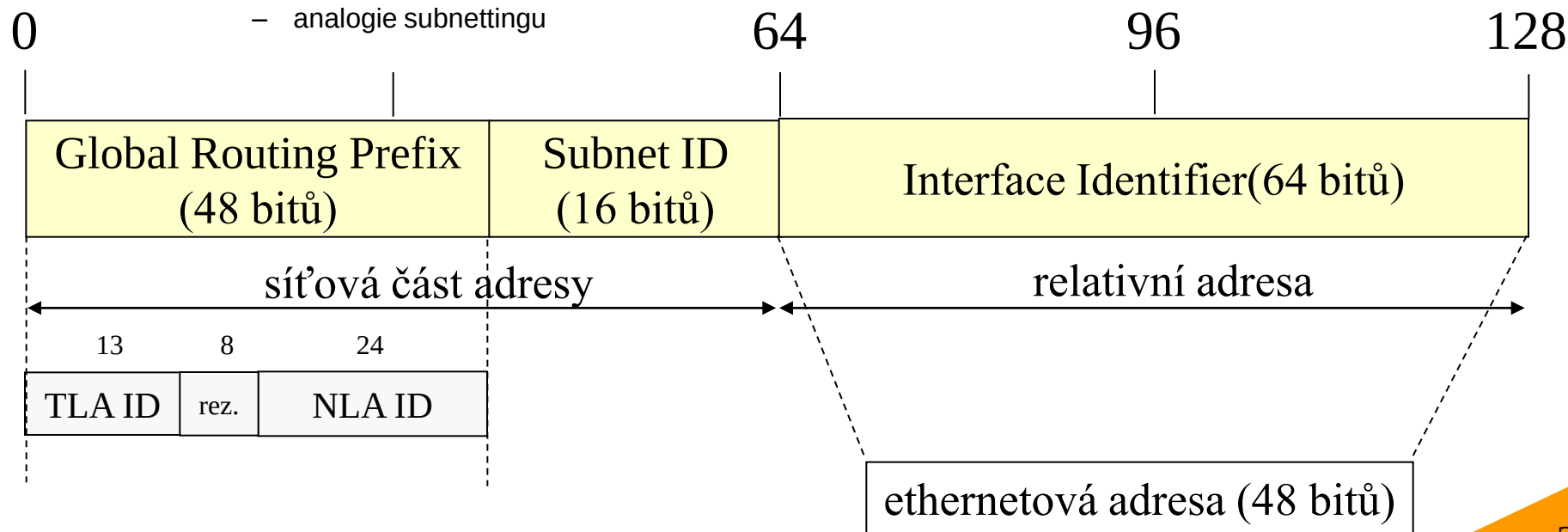
přiděleno
(unicast adresy)

(/dosud) nepřiděleno

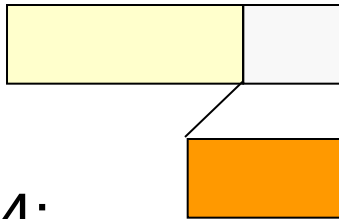
přiděleno
(místní a multicast
adresy)

IPv6 unicast adresy

- jsou logicky dvousložkové
 - relativní část adresy má 64 bitů
 - "Interface Identifier"
 - síťová část adresy má dvě části
 - Global Routing Prefix
 - identifikuje koncového zákazníka (site)
 - Subnet ID:
 - rozlišuje (pod)sítě u zákazníka
 - analogie subnettingu
- Global Routing Prefix
 - je definováno jeho dělení, pro
 - TLA (Top-Level Aggregators)
 - velké regionální přidělovatele IP adres, jako je RIPE, ARIN, APNIC, ...
 - NLA (Next-Level Aggregators)
 - typicky ISP, přidělují adresy zákazníkům
 - v praxi se nerespektuje
 - RFC 3587 fakticky **zrušilo** toto dělení

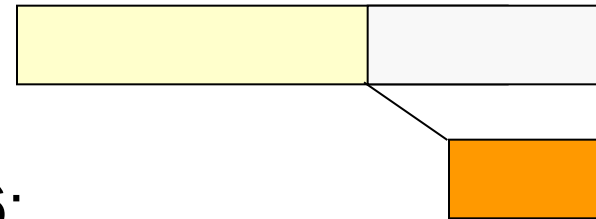


IPv6 Interface Identifier



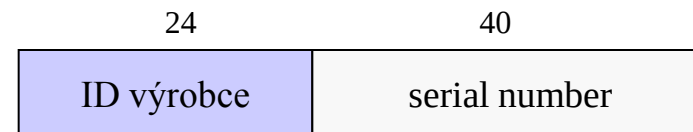
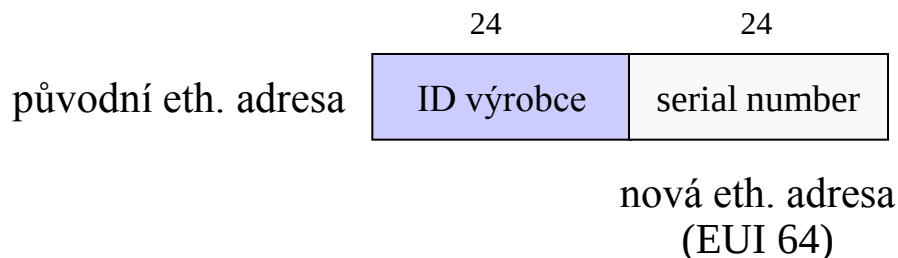
- IPv4:

- relativní část adresy měla typicky méně jak 48 bitů
 - nejčastější linkovou adresou byla 48-bitová ethernetová adresa
- bylo nutné složité převádění mezi relativní částí síťové adresy a linkovou adresou
 - např. protokolem ARP (Address Resolution Protocol)



- IPv6:

- relativní část adresy má 64 bitů
 - umožňuje to snadno "namapovat" na 48-bitové ethernetové adresy
- předpokládá se ale použití "větších" ethernetových adres, *modified EUI-64*
 - vychází z rozšířených ethernetových adres
 - "64-bit extended unique identifier", od IEEE
 - mají 24 bitů na výrobce, 40 na serial number

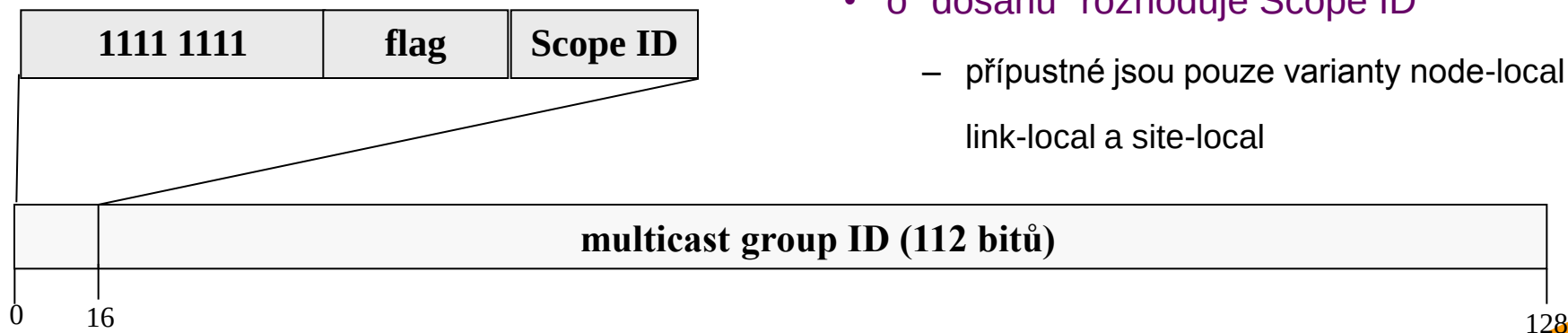


vyhrazené adresy v IPv6

- adresy začínající na FE (1111 1110) jsou vyhrazeny jako privátní
 - FE::cokoli
- dělí se na:
 - "site-local"
 - jsou přenášeny jen v rámci soustavy sítí zákazníka (site)
 - nejsou šířeny k jeho ISP a dále
 - začínají na FEC, FED, FEE, FEF
 - "link-local"
 - směrovače je vůbec nepropouští, používají se jen v rámci daného segmentu/spoje
 - začínají na FE8, FE9, FEA, FEB
- loopback
 - ::1
 - resp. 0:0:0:0:0:0:0:1
- nespecifikovaná IP adresa
 - ::
 - resp. 0:0:0:0:0:0:0:0
 - používá ji např. uzel, který se teprve dotazuje na svou IP adresu
- vnoření (embedded) IPv4 adresy
 - adresy IPv4, chápané jako adresy IPv6
 - doplní se zleva samými nulami
 - např. ::192.168.1.1

skupinové (multicast) adresy IPv6

- začínají na FF
 - jsou logicky jednosložkové
 - obsahují 4-bitový příznak
 - flag - říká např. zda je adresa přidělena trvale nebo dočasně
 - obsahují 4-bitový příznak "dosahu"
 - scope ID
 - node-local, link-local, site-local, organization-local, global, ...
- některé multicast adresy jsou dopředu vyhrazeny:
 - **FF0x:0:0:0:0:0:1** zahrnuje všechny uzly
 - o "dosahu" rozhoduje Scope ID
 - přípustné jsou pouze varianty node-local a link-local
 - fakticky nahrazuje broadcast
 - **FF0x:0:0:0:0:0:2** zahrnuje všechny směrovače
 - o "dosahu" rozhoduje Scope ID
 - přípustné jsou pouze varianty node-local, link-local a site-local



autokonfigurace v IPv6

- v IPv4 je nutné explicitně přidělovat IP adresy
 - "pevně"
 - nastavením v konfiguraci uzlu
 - "na žádost"
 - uzel si řekne jinému uzlu (serveru) o svou IP adresu
 - pomocí protokolů jako je DHCP, BOOT, RARP
- v IPv6 je možné, aby si uzel určil svou IP adresu sám
 - skrze tzv. **autokonfiguraci**
 - výrazně to usnadňuje správu sítě
- lze i hromadně přečíslovávat
 - **device renumbering**
 - princip:
 - se síťovým prefixem, který uzel dostane přidělen, je spojen časový limit (lease). Po jeho vypršení si uzel musí vyžádat nový
- postup autoconfigurace
 - uzel si zvolí dočasnou "link-local" IP adresu
 - pro relativní část adresy (Interface Identifier) vezme např. svou linkovou adresu
 - nebo něco jiného
 - uzel otestuje, zda je zvolená "link-local" adresa unikátní
 - snaží se kontaktovat případné sousedy se stejnou IP adresou
 - pokud jeho adresa není unikátní, zkusí zvolit jinou
 - uzel kontaktuje místní směrovače
 - pomocí mechanismů pro "router solicitation"
 - od směrovačů si vyžádá další informace
 - např. komu si má říci o svou "definitivní" IP adresu
 - nebo jak rozšířit "link-local" adresu na "site-local" a používat ji nadále
 - ...