Zdroj: Pavel Satrapa Internet protokol 6 http://knihy.nic.cz/ipv6/

Adresy v IPv6

Rychle se tenčící adresní prostor byl jedním z hlavních hnacích motorů vzniku IPv6.Základním dokumentem pro definici adres je RFC 4291: *IP Version 6 AddressingArchitecture* určující jejich délku a podobu, typy adres a další koncepční prvky.

Jak se adresuje

Existují tři druhy adres s odlišným chováním:

Individuální (unicast) každá z nich identifikuje jedno síťové rozhraní a data mají být dopravena právě jemu.
Skupinové (multicast) slouží pro adresování skupin počítačů či jiných zařízení. Pokud někdo odešle data na tuto adresu, musí být doručena všem členům skupiny.
Výběrové (anycast) představují novinku a nejzajímavější přírůstek v IPv6. Také výběrové adresy označují skupinu, data se však doručí jen jedinému jejímu členovi – tomu, který je nejblíže.

Zmizely oznamovací (broadcast) adresy, protože jejich funkce přebírají adresy skupinové. Jsou definovány speciální skupiny, např. pro všechny uzly na dané lince, které nahrazují původní oznamování.

IPv6 umožňuje, aby rozhraní mělo libovolný počet adres různých druhů. Přikazuje několik povinných adres, které musí být přiděleny (viz dále).

Podoba a zápis adresy

Při rozhodování o velikosti adresy pro IPv6 se autoři řídili heslem „aby nám už nikdy nedošly“. Frustrace způsobená nedostatkem IPv4 adres byla velmi silná. Proto se rozhodli délku prodloužit na čtyřnásobek.

Standardním způsobem je zápis adres do skupin po čtyřech číslicích šestnáctkové soustavy, které vyjadřují hodnoty 16 bitů dlouhých částí adresy. Navzájem se oddělují dvojtečkami.
Příkladem IPv6 adresy je
fedc:ba98:7654:3210:fedc:ba98:7654:3210
Očekává se, že uživatelé budou striktně používat DNS a ručního psaní uvedených hrůz budou ušetřeni. Černý Petr zbude v rukou správců sítí, kteří se jim při sebevětším úsilí nevyhnou ...

Častou hodnotou je nula, nabízí se dvě možnosti pro zkrácení zápisu. Jednak v každé čtveřici můžete vynechat počáteční nuly.
Místo „0000“ tedy lze psát jen „0“.

Například adresu

0123:0000:0000:0000:fedc:ba98:7654:3210

můžete zkrátit na
123:0:0:0:fedc:ba98:7654:3210
nebo dokonce jen na
123::fedc:ba98:7654:3210

Úplný extrém představuje nedefinovaná adresa

0000:0000:0000:0000:0000:0000:0000:0000

kterou lze zkrátit až na samotné
::

Konstrukci „::“ můžete v každé adrese použít jen jednou. Jinak by nebylo jednoznačné, jak se má adresa rozvinout do původní podoby. Například

0123:0000:0000:0000:4567:0000:0000:0000

můžete psát jako

123::4567:0:0:0 nebo 123:0:0:0:4567::

nikoli však

123::4567::

Některé přechodové mechanismy potřebují vyjádřit **IPv4-mapované adresy**, které pocházejí ze světa IPv4. Slouží k tomu tak zvané IPv4-mapované adresy, jejichž počátečních 80 bitů obsahuje samé nuly, následuje 16 bitů jedničkových a v posledních 32 bitech je zapsána IPv4 adresa.

Například adresu 147.230.49.73

bychom tímto způsobem vyjádřili jako

::ffff:93e6:3149

Abyste nemuseli pracně převádět hodnoty mezi desítkovou soustavou používanou v IPv4 a šestnáctkovou pro IPv6, lze poslední čtveřici bajtů **IPv4- mapované adresy** zapsat jako běžnou IPv4 adresu. Komfortní zápis by proto vypadal následovně:

::ffff:147.230.49.73

Starší specifikace definovaly také **IPv4-kompatibilní adresy,** které měly adresy počátečních 96 bitů nulových a za nimi následovalo 32 bitů s IPv4 adresou.Opět byl umožněn pohodlný zápis, takže adresa 147.230.49.73 zapsaná jakoIPv4-kompatibilní IPv6 adresa má podobu:

::147.230.49.73

Aktuální mechanismy pro přechod od starší verze protokolu k novější však **IPv4-kompatibilní adresy nepoužívají, proto jsou v RFC 4291 prohlášeny za odmítnuté**. Nadále zůstávají v platnosti pouze **IPv4-mapované adresy.**

Příslušnost k určité síti nebo podsíti se vyjadřuje prefixem – všechna rozhraní v jedné síti mají stejný prefix (začátek adresy – něco jako dříve síťová část IP adresy). **Jeho délka může být různá.** Záleží na tom, s jakou podrobností se na adresy díváte. Může vás zajímat jen prefix poskytovatele Internetu (který bude poměrně krátký) nebo o poznání delší prefix určité konkrétní podsítě.

Tento přístup se používá již v současném Internetu pod názvem *Classless Inter-Domain Routing (CIDR)*. Odtud je také převzat způsob zápisu:

IPv6 adresa/délka prefixu

Délka prefixu určuje, kolik bitů od začátku adresy je považováno za prefix.

Například 60 bitů dlouhý prefix 12ab 0000 0000 cd3 lze zapsat libovolným z těchto způsobů:

12ab:0:0:cd30:0:0:0:0/60

12ab::cd30:0:0:0:0/60

12ab:0:0:cd30::/60

Za nejvhodnější by se dal označit poslední, protože konstrukcí „::“ logicky nahrazuje závěrečnou část adresy, která je z pohledu prefixu nezajímavá.

Prefix nemusí končit na hranici šestnáctkových číslic. Například

prefix 2000::/3 požaduje, aby první tři bity adresy obsahovaly hodnotu 001 (binárně). Tomu vyhoví všechny IPv6 adresy, jejichž první číslicí je 2nebo 3.

Ve zkratce lze použít i zápis, který současně oznamuje jak konkrétní adresu rozhraní, tak délku prefixu (a tudíž adresu podsítě):

12ab:0:0:cd30:123:4567:89ab:cdef/60

Typy adres

Obrovský adresní prostor, který má IPv6 k dispozici, byl rozdělen do několika skupin – typů adres. Každý typ sdružuje adresy se společnou charakteristikou.

Příslušnost k jednotlivým typům určuje prefix adresy. Dříve se pro tyto určující počáteční bity používal termín *prefix formátu* (format prefix, FP), novější dokumenty však od tohoto pojmu upouští.

::/128	**nedefinovaná adresa**
::1/128	**smyčka (loopback)**
fc00::/7	**unikátní individuální lokální**
fe80::/10	**individuální lokální linkové**
ff00::/8	**skupinové adresy**
ostatní	**individuální globální**

Drtivou většinu zabírají **globální (celosvětově jednoznačné) individuální adresy**. Z jejich prostoru je navíc **většina prefixů dosud nepřiřazena**, zatím se využívá pouze výše zmiňovaný prefix 2000::/3.

Ostatní se ponechávají **jako rezerva** a očekává se, že budoucí RFC jim přiřknou určitý význam a vnitřní strukturu. Aktuální stav jejich přidělení najdete na adrese

www *http://www.iana.org/assignments/ipv6-address-space*

Skupinové adresy jsou snadno identifikovatelné, protože jejich **první bajt má v šestnáctkovém zápisu hodnotu ff.**

Výběrové adresy nemají přiřazeno žádné speciální rozmezí a přidělují se ze stejného prostoru, jako adresy individuální.

Několika menším oblastem adresního prostoru byl přidělen specifický význam.

Celý prefix ::/8 byl původně rezervován pro speciální účely. **Nyní je deklarován jako nepřiřazený,** některé adresy v jeho rámci však přiřazeny byly.
Jedná se o **individuální adresy ::0 a ::1.** První se používá pro nedefinovanou adresu. Říká, že dotyčnému rozhraní dosud nebyla přidělena

IPv6 adresa. ::1 je pak adresou lokální smyčky (loopback), kterou počítač může komunikovat sám se sebou. Spadá sem také prefix přidělený pro IPv4-mapované adresy (::ffff:0:0/96).

Skupinka prefixů identifikuje **adresy s omezeným dosahem**. Nejčastěji se setkáte s **lokálními linkovými adresami (link- local)**, které jsou jednoznačné vždy jen v rámci jedné linky (jednoho Ethernetu, jednéWi-Fi buňky,. . .).Poznáte je podle prefixu **fe80::/10** a najdete je u každého rozhraní se zapnutým IPv6.

Vedle nich dříve existovaly **místní individuální lokální adresy (site-local) s prefixem fec0::/10 jednoznačné v místní síti. Později však byly zrušeny,** proto se jejich prefix v tabulce nevyskytuje. Nahradily je **unikátní individuální lokální adresy s prefixem fc00::/7.**

Globální individuální adresy

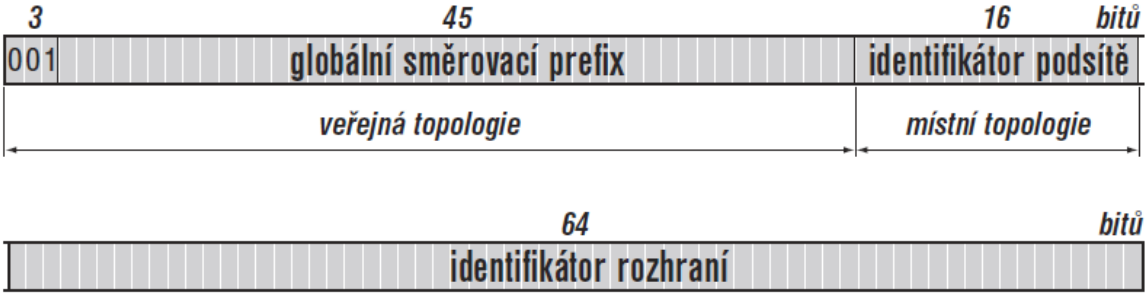
Tento typ adres je nejdůležitější, protože se jedná o protipól adres současného IPv4. Globální naznačuje, že identifikují svého nositele v rámci celého Internetu a musí být celosvětově jednoznačné.

Zatím byla **definována jen část z nich (prefix 001 binárně)**, jejíž strukturu definuje RFC 3587: *IPv6 Global Unicast Address Format*.

Globální adresy **jsou přidělovány hierarchicky podle pravidel podobných CIDR ze světa IPv4**. To znamená, že poskytovatel Internetu (neboli lokální registr, LIR) obdrží určitý prefix, jehož části v podobě delších prefixů se shodným začátkem pak přiděluje svým zákazníkům. **Cílem tohoto přístupu je agregace směrovacích údajů** – aby bylo možné při pohledu zvenčí celou poskytovatelovu síť i se všemi zákazníky popsat jediným záznamem ve směrovacích tabulkách, obsahujícím onen společný prefix..

Toto shlukování je velmi důležité, protože významným způsobem zmenšuje velikost směrovacích tabulek. Jemnost členění směrovacích informací klesá se vzdáleností od místa určení.

Původně se **koncept agregace promítal i do struktury adresy, která byla složena z identifikátorů několika úrovní.** K praktickému **naplnění této vize však nedošlo** a reálně používané adresy původní koncept nedodržovaly. Proto byl opuštěn a RFC 3587 zavedlo **maximálně zjednodušený model, v podstatě odpovídající struktuře adresy pro IPv4. Ta má tři části: adresu sítě, podsítě a rozhraní v podsíti.** Analogické části má i IPv6 adresa, jen adresa sítě byla přejmenována na globální směrovací prefix. Jejich délky jsou definovány zcela obecně, podle současných pravidel přidělování však globální směrovací prefix měří 48 bitů, adresa podsítě 16 bitů a adresa rozhraní v podsíti 64 bitů.



Globální směrovací prefix identifikuje globální směrovací koncovou síť. Je síti přidělen „zvenčí“ prefix lokálním internetovým registrem, zpravidla poskytovatelem Internetu.Proto bývá tato část adresy označována jako „veřejná topologie“.

Identifikátor podsítě slouží k rozlišení jednotlivých podsítí v rámci dané sítě. Tato část adresy je, společně s identifikátorem rozhraní, záležitostí správy koncové sítě a používá se pro ni označení „místní topologie“. Dva bajty umožňují adresovat báječných 65 536 podsítí, což by mělo dostačovat i pro opravdu velké sítě.

Pouze v ojedinělých případech, jako jsou například propojovací podsítě na linkách spojujících pouhá dvě zařízení, má smysl uvažovat o dlouhých adresách podsítě a ponechání jen minimálního prostoru pro identifikátor rozhraní.

Alternativou k postupnému číslování podsítí je vytvořit si vlastní hierarchii (vetší množství - stovky podsítí). Například prvním bajtem adresy podsítě identifikovat areál či budovu a druhým pak rozlišit podsítě v ní. Dá to více práce a vyplýtváte některé adresy, ovšem směrovací tabulky budou menší, protože pro celé skupiny identifikátorů postačí vždy jen jedna položka.

Závěrečný *identifikátor rozhraní* zabírá identifikátor rozhraní celou polovinu adresy, což umožňuje v jedné podsíti rozlišit miliardy adres.
Motivací k takto velkorysému dimenzování podsítě byla snaha o maximální zjednodušení automatické konfigurace počítačů. Nicméně nelze přehlížet, že AppleTalk zvládal automatickou konfiguraci s jediným bajtem[1] a IPv4 stačí čtyři bajty pro celosvětově jednoznačné adresy. **Investovat osm bajtů na dosažení jednoznačnosti v jediné podsíti je plýtvání.**
Přesto RFC 4291 jednoznačně stanoví, že pro všechny individuální adresy (s výjimkou adres s prefixem 0::/3) **je vyžadována délka identifikátoru rozhraní 64 bitů** a používání identifikátorů ve tvaru modifikovaného EUI-64.

Používání EUI-64 je velmi přímočaré, ale ozývají se proti němu ochránci soukromí uživatelů. Jelikož je EUI-64 odvozeno z MAC adresy, která je celosvětově jednoznačná a mění se jedině s výměnou síťové karty, vzniká tak jednoznačná identifikace uživatelova počítače.
Navíc **tato část adresy zůstává stejná, i když se počítač pohybuje**. Jak se dočtete v kapitolách o automatické konfiguraci a mobilitě, počítač si svou adresu generuje stále stejně: zjistí prefix zdejší podsítě a připojí k němu svůj identifikátor rozhraní. **Pokud se někomu podaří odposlouchávat síťový provoz na strategických místech, může krásně sledovat, s kým vším váš počítač komunikuje a jak se pohybuje po světě.** Nepomůže ani šifrování, protože se šifruje jen obsah datagramu. Adresy musí zůstat otevřené.

Reakcí na tyto problémy je RFC 4941: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*. V podstatě **navrhuje náhodné generování identifikátorů rozhraní**, které budou mít **životnost několik hodin až dnů** a počítač je bude neustále měnit. Ovšem je potřeba i nějaký **pevný bod, aby se s takovýmto počítačem dalo vůbec navázat spojení**. Proto RFC 4941 navrhuje, aby počítač měl **jeden pevný identifikátor rozhraní** (podle EUI-64), pod nímž **bude zaveden v DNS**. Hlavním smyslem této adresy je sloužit jako **cílový bod pro komunikaci navazovanou zvenčí**. Navíc si bude počítač generovat náhodné dočasné identifikátory. Adresám z nich odvozeným bude dávat přednost, když sám navazuje spojení s někým jiným. Tyto identifikátory nebudou zavedeny v DNS (jinak by se celý efekt znehodnotil – počítač by sice střídal adresy, ale dal by se identifikovat podle shodného jména v DNS). Díky tomu klienti na daném počítači používají náhodné krátkodobé adresy a nelze dlouhodobě sledovat jejich aktivity.

RFC 3972 zavedlo **další odrůdu identifikátorů rozhraní**, jež **umožňují generované identifikátory kryptograficky zabezpečit proti objevování sousedů**. Vycházejí z veřejného klíče svého vlastníka a znemožňují nepřátelské stanici vydávat se za někoho jiného.

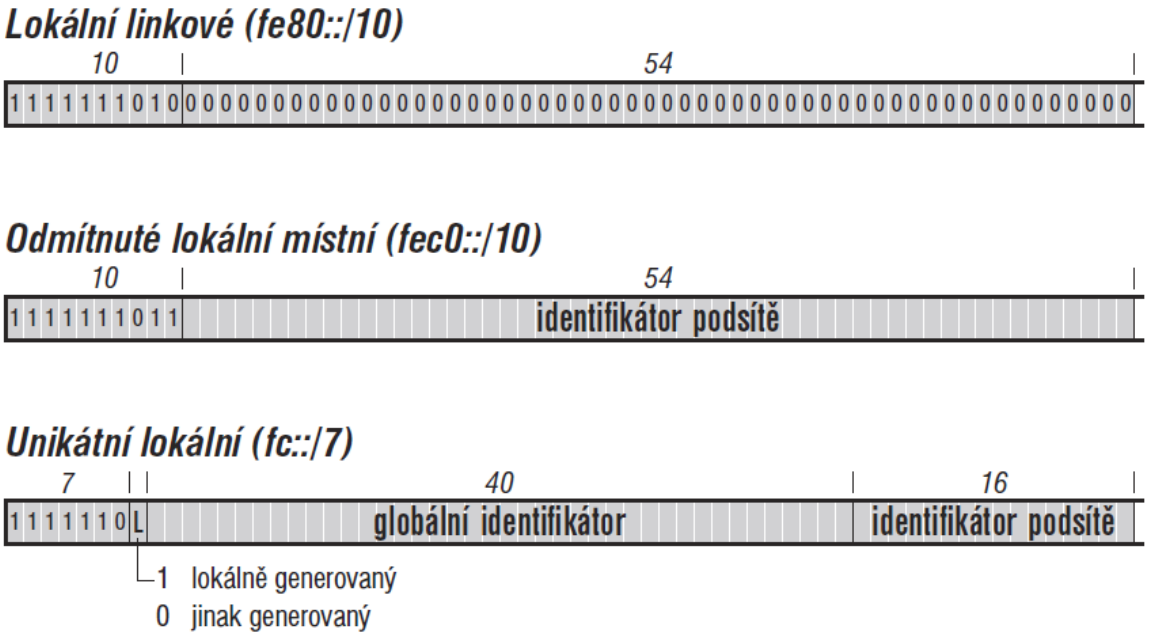
Lokální adresy

Koncept adres, které neplatí v celém Internetu, ale pouze v jeho malé části, zavedlo RFC 1918: *Address Allocation for Private Internets*.

Malou část adresního prostoru IPv4 vyhradilo pro neveřejné adresy, které lze používat v koncových sítích, ale nejsou podporovány za jejich hranicemi. Tyto adresy nejsou celosvětově jednoznačné.

IPv6 posouvá myšlenku privátních adres o krok dál. Zavádí **koncept dosahu adres.** Ten je ale přínosný především pro skupinové adresy, jejichž součástí je přímo informace o dosahu.

Pro individuální adresy jsou možnosti dosahu omezené. Existuje několik typů adres s omezeným dosahem. Níže jsou první poloviny adres, protože druhá polovina ve všech třech případech obsahuje standardní identifikátor rozhraní. Typy lokálních adres:



Linkové lokální – link local

Největší význam mají *lokální linkové adresy (link* lokální linkové *local)*. V adresní architektuře mají svou vyhrazenou část – **začínají prefixem fe80::/10**. Následujících 54 bitů je nulových, za nimi najdete 64bitový identifikátor rozhraní podle modifikovaného EUI-64.
Např.: počítač s ethernetovou adresou 00:8c:a0:c2:71:35 by tomuto rozhraní přidělil lokální linkovou adresu:

fe80::28c:a0ff:fec2:7135

Vzhledem k její standardní podobě si tuto adresu vytvoří sám a pomocí nástrojů automatické konfigurace ověří, že je pro danou linku skutečně jednoznačná.

První část neslouží ke směrování, protože hodnota těchto bitů je pevně dána a je u všech stejná. Nijak to nevadí, protože dosah lokálních linkových adres je omezen na jedinou linku. Tedy na skupinu počítačů propojených Ethernetem či bezdrátovou sítí Wi-Fi.

Datagramy nesoucí lokální linkovou adresu jako cíl neprojdou žádným směrovačem, protože za ním již leží jiné linky.

Jejich hlavní výhodou je, že počítač si takovou adresu dokáže vygenerovat sám a nepotřebuje k tomu žádnou infrastrukturu. Díky tomu je lokální linková adresa k dispozici vždy. Stačí propojit počítače ethernetovým přepínačem a mohou rovnou komunikovat prostřednictvím lokálních linkových adres.

Všudypřítomnost lokálních linkových adres využívají i některé interní mechanismy související s IPv6. **Například automatická konfigurace pomocí DHCP používá pro výměnu zpráv mezi klientem a serverem tyto adresy**.

Lokální místní –site local - odmítnuté

Pozn.:
Roli velmi podobnou adresám z RFC 1918 hrály ve starších definicích adresního prostoru pro IPv6 ***lokální místní adresy (site* lokální místní *local).*** Byl jim přidělen prefix fec0::/10 a jejich platnost byla omezena na jedno „místo“. Typickým místem je koncová síť organizace připojené k Internetu.

Jenže existují také organizace připojené k Internetu v několika lokalitách téhož města či dokonce v různých městech a státech. Mají být areály MFF UK v na Karlově, v Karlíně, v Tróji a na Malé Straně považovány za čtyři různá místa nebo za jedno místo? **Praxe ukázala, že definice místa je vágní** a její výklad se velmi liší. Navíc se připojily problémy s konfiguracemi směrovačů a další obtíže při pokusech o reálné použití místních adres.

Výsledkem bylo RFC 3879: *Deprecating Site Local Addresses*, které místní **lokální adresy zamítlo a dokonce zakazuje novým implementacím podporovat speciální zpracování adres s prefixem fec0::/10.**

Unikátní lokální - ULA

Nástupcem lokálních místních adres se staly ***unikátní lokální adresy (unique local, ULA)*** definované v RFC 4193: *Unique Local IPv6 Unicast Addresses*.

Poznají se podle prefixu fc::/7. Za ním následuje **jednobitový příznak *L*, zda byl prefix adresy přiřazen lokálně (L=1) nebo jinak.** Vzhledem k tomu, že všechny v současnosti používané adresy tohoto typu jsou generovány lokálně, mají nastaven příznak L na jedničku a začínají proto prefixem fd::/8.

Dalších 40 bitů obsahuje globální identifikátor, kterým je **náhodně vygenerované číslo**. RFC 4193 výslovně zakazuje jeho sekvenční či jinak předvídatelné určení a v části 3.2.2 **doporučuje postup vycházející z aktuálního času, adresy generující stanice a algoritmu SHA-1.**

Čtyřicetibitová položka může nabývat více než bilionu různých hodnot. Pravděpodobnost, že dvojice sítí zvolí stejný globální identifikátor je tedy zhruba 10^{-12}. Při milionu koncových sítí je pořád ještě pravděpodobnost, že si alespoň dvě vygenerují stejný globální identifikátor, méně než poloviční.

Prefix společně s globálním identifikátorem dohromady vytvoří obvyklý síťový prefix délky 48 bitů. Za ním následuje běžný 16bitový identifikátor podsítě a 64bitový identifikátor rozhraní podle modifikovaného EUI-64.

Proč se globální jednoznačnost těchto adres považuje za tak podstatnou, když se beztak předpokládá jejich lokální využití a stejně jako v případě místních adres nejsou směrovány v internetové páteři?

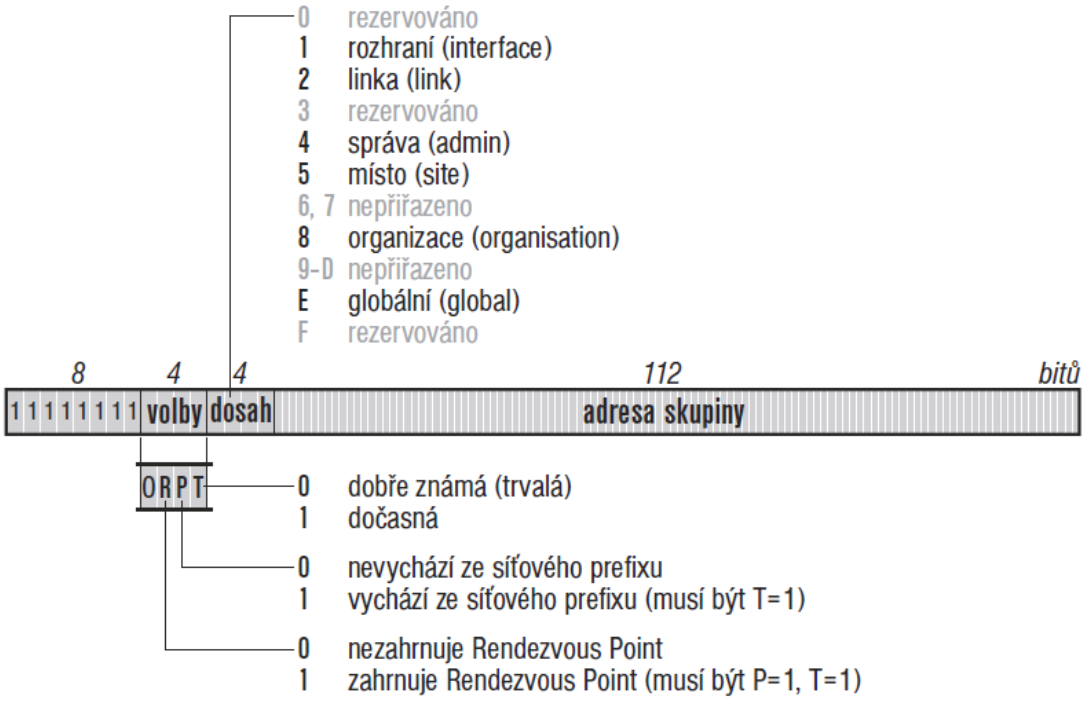
Vyjděme z výše uvedeného příkladu se čtyřmi pražskými lokalitami MFF UK. Řekněme,že správci sítě je považují za jedno místo a kromě veřejných adres chtějí používat také lokální adresy. Vygenerují si tedy prefix, řekněme fdd6:c246:22a9::/48, který ponesou všechny lokální adresy ve spravované síti. Adresami podsítí pak rozliší jednotlivé podsítě. To vše by se snadno dalo zajistit i místními lokálními adresami.

Jednotlivé lokality jsou ale poměrně vzdáleny a k jejich propojení bude využita některá páteřní síť, v daném případě nepochybně PASNET. Po ní budou zároveň směrovány analogické lokální adresy ostatních fakult a univerzit. **Unikátní lokální adresy nezpůsobí problém – různé sítě si vygenerovaly odlišné prefixy a budou mít proto jiné adresy**. V případě **místních lokálních adres, které obsahují jen konstantní prefix**, identifikátor podsítě a rozhraní je naproti tomu **značná pravděpodobnost kolize**. Například lze očekávat, že **podsíť 1 si vytvoří více institucí.** Jejich **propojení sdílenou páteřní sítí by vyžadovalo tunely, virtuální privátní síť či podobnou nadstandardní konfiguraci.** Navíc by případné „prosáknutí“ směrovacích informací mohlo způsobit zmatek v jiných částech sítě, zatímco unikátní lokální adresy tímto problémem netrpí.

Skupinové adresy - multicast

Princip skupin a skupinových adres není žádnou výjimkou již v současném Internetu. Slouží především k **distribuci zvukového a obrazového signálu v reálném čase** (videokonference, rozhlasové či televizní vysílání a podobně).

Ve skupinách podle IPv6 by nemělo dojít k žádné zásadní revoluci. Struktura adresy je níže:



Největší část slouží k identifikaci skupiny, které mají být data dopravena (48bitů).

Dále jsou zde **dvě krátké podpůrné položky: příznaky a dosah skupiny (4+4bity)**.

Volby - příznaky
První je rezervován pro pozdější použití a zatím musí být nulový.

R (rendezvous point),
P (prefix)
T (transient)

Příznak „P“ byl definován v RFC 3306: *Unicast-* P*refix-based IPv6Multicast Adresses* .**Pro skupinové adresy vycházející z individuálních adres.**

Vlastní adresní architektura definuje příznak T. „příznak T“ (transient) a signalizuje, zda je daný **identifikátor skupiny přidělen trvale a jedná se o dobře známou adresu („0“)** nebo zda je přidělen **pouze dočasně (T má hodnotu 1**).

Dobře známé adresy přiděluje IANA, zatímco **dočasné si mohou generovat aplikace** podle potřeby. Právě jimi se zabývá většina dalších specifikací a návrhů.

Dosah skupiny
Dosah skupiny sděluje, jak daleko od sebe mohou jednotliví členové být. Jedná se opět o čtyřbitovou položku se šestnácti možnými hodnotami. **Význam byl zatím přidělen deseti z nich.**

dosah	*význam*
0	rezervováno
1	lokální pro rozhraní
2	lokální pro linku (fyzickou síť)
3	rezervováno
4	lokální pro správu
5	lokální pro místo
6	–
7	–
8	lokální pro organizaci
9	–
A	–
B	–
C	–
D	–
E	globální
F	rezervováno

Nepřiřazené dosahy jsou volně k použití. Určitý **význam jim může přidělit například poskytovatel Internetu či správce části sítě**. Mělo by přitom zůstat **zachováno, že větší hodnota dosahu v adrese bude znamenat doručování paketů do větší části Internetu**, než dosahy menší.

Například v síti CESNET2, stejně jako v dalších evropských národních akademických sítích, je definován dosah A pokrývající danou národní síť. Skupinové pakety s dosahem A budou proto u nás doručovány všem zájemcům v rámci sítě CESNET2. Lze očekávat, že podobný přístup zavedou i komerční poskytovatelé Internetu a dosah A bude všeobecně znamenat „poskytovatel a jeho zákazníci“.

Permanentní skupina – dobře známá skupina má příznak identifikátory T má hodnotu 0, je **její identifikátor stále platný a nezávisí na dosahu.**

Například skupina adres **ff0*x*::101**
(**kde *x* představuje různé dosahy)** byla **přidělena NTP (network time protokol) serverům**.

Důsledkem jsou následující významy adres:

ff01::101 NTP servery na tomtéž rozhraní (čili on sám)
ff02::101 NTP servery na stejné lince (např. Ethernetu)
ff05::101 NTP servery v daném místě (lokalitě)
ff0e::101 NTP servery v celém Internetu

Dočasná skupina má význam jen v rámci svého dosahu.
například skupina s adresou ff15::101
nemá žádný vztah ke skupině, která má stejnou adresu, ale je vytvořena na jiném místě. Nemá ani žádný vztah ani k dočasné skupině se stejným identifikátorem, ale jiným dosahem (např. ff1e::101) ani k trvalým skupinám se stejným identifikátorem. Nemá tedy nic společného s žádnou z výše uvedených skupin NTP serverů.

Pravidla pro přidělování identifikátorů skupinových adres definuje RFC 3307: *Allocation Guidelines for IPv6 Multicast Addresses*.

Teoreticky je pro identifikátor skupiny k dispozici 112 bitů. **Některé formáty definují strukturu i v této části adresy a pro skutečný identifikátor skupiny ponechávají jen posledních 32 bitů.**

RFC 3307 toto omezení kodifikuje a navíc rozděluje skupinové identifikátory do tří oblastí:

0–3fff:ffff skupiny přidělené IANA

4000:0000–7fff:ffff identifikátory přidělené IANA

8000:0000–ffff:ffff dynamické, volně k použití

Do první skupiny patří případy, kdy IANA definuje celé skupinové adresy, jako například výše zmíněnou adresu ff0*x*::101 pro NTP servery

Ve druhé skupině jsou identifikátory, kde IANA definuje pouze samotný skupinový identifikátor, zatímco prefix před ním může být libovolný. Předpokládá se jejich použití především pro adresy odvozené z individuálních

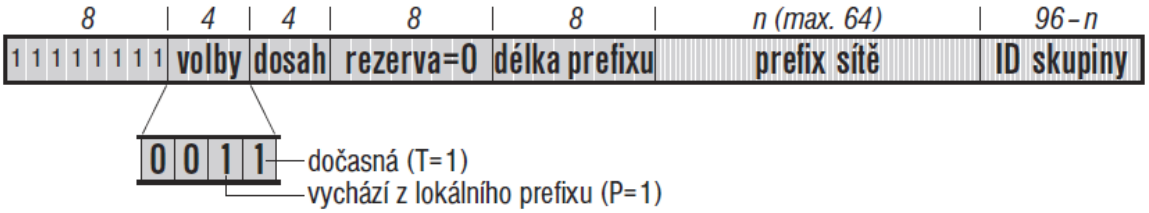
Zatím byl definován jediný, 4000:0000 pro proxy sítě, většina definic IANA spadá do první skupiny.

Do třetí skupiny spadají identifikátory, které si mohou přidělovat podle potřeby jednotlivé aplikace a služby. Existují **dva základní přístupy ke správě tohoto typu identifikátorů**. Jedním je alokační server, u nějž si aplikace požádají o přidělení skupinového identifikátoru[6]. Podle druhého si berou identifikátory samostatně prostřednictvím vhodného autokonfiguračního protokolu.

V každém případě se však jedná o adresy dočasné, jejich příznak T proto musí mít hodnotu 1.

Skupinové adresy vycházející z individuálních adres(příznak P). Vznikly s **cílem usnadnit generování jednoznačných skupinových adres, aniž by generující stroj musel komplikovaně zjišťovat, zda adresa již někde neexistuje**.. Proto je jako součást adresy zařazen prefix individuálních adres zdejší sítě. Ten je celosvětově jednoznačný, takže stačí zajistit jednoznačnost identifikátoruv rámci sítě a máme vystaráno.

Jedná se vlastně o jeden možný konkrétní formát pro identifikátor skupiny. Jeho uspořádání najdete na obrázku níže. Začíná osmibitovou rezervovanou položkou, jejíž hodnotou jsou povinně samé nuly. Následuje délka použitého prefixu, tedy počet významných bitů v něm. Nejčastěji bude obsahovat hodnoty 48 či 64. V dalších bitech je uložen prefix odpovídající části sítě, z níž tato skupinové adresa pochází. jejich počet odpovídá délce z předchozí



položky, nanejvýš jich však může být 64. A konečně závěrečných minimálně 32 bitů obsahuje vlastní identifikátor skupiny.

Příznak P s hodnotou 1 oznamuje, že identifikátor skupiny ve skupinové adrese byl vytvořen tímto způsobem.

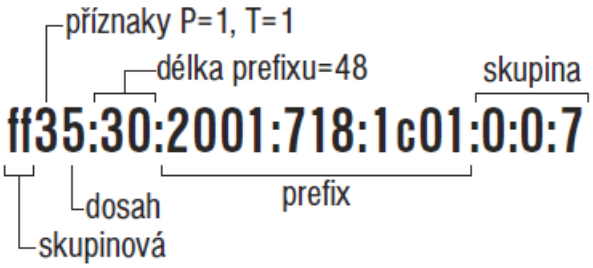
Je-li P=1, musí se jednat o dočasnou adresu a proto musí mít i příznak T hodnotu 1. Zároveň RFC 3306 požaduje, aby dosah takové adresy nepřesahoval dosah prefixu použitého při jejich vytvoření.

Například Technická univerzita v Liberci má pro své individuální IPv6 adresy přidělen prefix

2001:718:1c01::/48.

Řekněme, že z tohoto prefixu chceme odvodit skupinovou adresu s dosahem pro místo (dosah 5) se skupinovým identifikátorem 7.

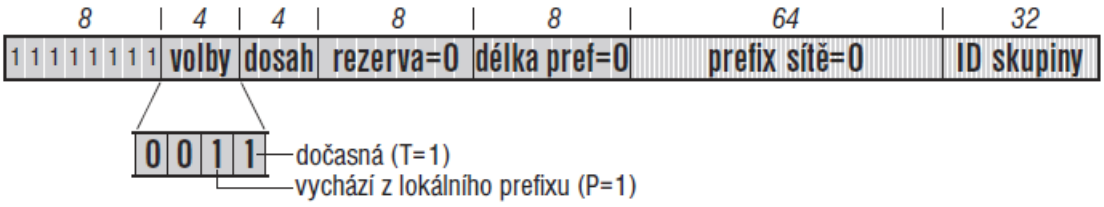
Výsledkem bude skupinová adresa ff35:30:2001:718:1c01:0:0:7 s níže popsanou strukturou:



Adresy pro SSM – Source Specific Multicast

Speciálním případem skupinově adresovaného vysílání je tak zvaný *Source Specific Multicast (SSM)*. Slouží pro přenosy dat z jednoho zdroje skupině příjemců, například pro internetové rádio či televizi.

Pro něj byla vyčleněna samostatná **část skupinových adres založených na individuálních.** Pozná se podle toho, že délka prefixu i prefix sítě jsou nulové. Skupinové adresy pro SSM tedy mají prefix ff3*x*::/96, za nímž následuje 32b identifikátor skupiny.

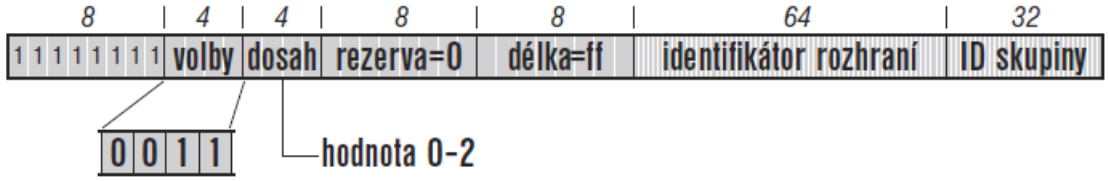


Jednoznačnosti zde není těžké dosáhnout, protože skupiny mají vždy jen jediného odesilatele. Stačí, aby on sám si udržel pořádek v jejich identifikátorech.

Skupina je jednoznačně určena dvojicí zdrojové adresy svého jediného odesilatele a skupinové adresy.

***Skupinové adresy* vycházející z rozhraní** definované v RFC 4489: *A Method for Generating Link-Scoped IPv6 Multicast Addresses*.

Jejich dosah **nesmí být větší než jediná linka,** za to si je ale **každý stroj může generovat sám bez rizika konfliktu s adresami generovanými jeho sousedy**. Adresa tohoto typu totiž obsahuje jeho identifikátor rozhraní, který je na lince vždy jednoznačný. Stačí tedy, aby si udržoval přehled o přidělených identifikátorech skupin, a může si být jist, že všechny používané adresy tohoto typu jsou jednoznačné.



Volby má nastaveny stejně jako v předchozím případě (P=1, T=1),od adresy vycházející z prefixu sítě se pozná podle hodnoty pole *Délka prefixu*, jejíž všechny bity obsahují jedničky. Následujících 64 bitů je tvořeno identifikátorem rozhraní, tedy spodní polovinou jeho lokální linkové adresy. Závěrečných 32 bitů nese identifikátor skupiny.

Počítač s ethernetovou adresou **00:8c:a0:c2:71:35**

si vygeneruje lokální linkovou adresu

fe80::28c:a0ff:fec2:7135

a po ověření její jednoznačnosti **ji může začít používat pro vytváření skupinových adres.**

Jejich prefix bude **ff32:ff:28c:a0ff:fec2:7135::/96.**

Další popis skupinových adres s příznaky R přesahuje rámec stručného seznámení s touto oblastí. Více ve výše uvedeném zdroji.

Výběrové adresy - anycast

Výběrové adresy představují nejzajímavější novinku v oboru adresování. Poskytují velmi zajímavé možnosti. Jejich prostřednictvím **lze řešit třeba zdvojování počítačů, směřující ke zvýšení výkonu či spolehlivosti. Mohou se také využít k vyhledání nejbližšího stroje poskytujícího určitou službu.**

Například **současné nejzatíženější servery bývají ve skutečnosti realizovány skupinou spolupracujících počítačů.**

Prostřednictvím triků **s DNS se dosahuje rozkládání dotazů na jednotlivé členy skupiny**. Zbývá však celá řada obtíží (jak rovnoměrně rozkládat zátěž, připojení k Internetu musí mít odpovídající kapacitu apod.).

S výběrovými adresami lze daný problém řešit daleko elegantně: servery ze skupiny rozmístíte ve **vhodných místech Internetu a přidělíte jim výběrovou adresu.** Klient bude posílat pakety na tuto adresu a standardní směrovací mechanismy zajistí, že dorazí vždy k nejbližšímu ze skupiny serverů. Navíc lze **složení skupiny průběžně měnit podle potřeby.**

Výkladní skříní výběrových adres se staly kořenové DNS servery. Těch by na jedné straně mělo být mnoho, aby docházelo k rozkládání zátěže, služba byla rychle dostupná z libovolné části Internetu a lépe odolávala útokům usilujícím o její zahlcení (DoS, DDoS). Na druhé straně by jich ale mělo být málo, protože jejich adresy musí znát skoro všechny ostatní DNS servery.

Seznam adres by proto měl být krátký a velmi konzervativní. Výběrové adresy právě pro tento případ nabízejí **ideální řešení: adres kořenových serverů je třináct**, ovšem postupně přecházejí na výběrové. **V polovině roku 2008 bylo pět z nich výběrových a za třinácti adresami se díky tomu skrývalo kolem 150 serverů.**

Jejich složení lze navíc průběžně měnit, aniž by se to projevilo na seznamu adres kořenových serverů. Vzhledem ke své zjevné užitečnosti byl **koncept výběrových adres později převzat i pro v IPv4.**

Nejčastěji se nasazením výběrové adresy sleduje některý z následujících cílů:

Přibližné rozkládání zátěže – dotazy z určité části sítě se sejdou vždy na jednom z uzlů poskytujících výběrově adresovanou službu. **Dochází k rozdělení sítě na spádové oblasti.**

Zrychlení doby odezvy díky kratší cestě mezi klientem a serverem.

Lepší odolnost proti útokům typu DoS a DDoS – útočníci jsou schopni „dosáhnout“ jen na servery, v jejichž spádových obastech se sami nacházejí.

Zmenšení počtu adres, na nichž je služba poskytována. Představte si, že seznam adres kořenových DNS serverů by měl 150 položek a měnil se několikrát za měsíc. . .

Výběrovým adresám nebyla rezervována samostatná část adresního prostoru.

Pocházejí ze stejných oblastí jako adresy individuální a mohou se s nimi libovolně míchat. Syntakticky je od sebe nelze rozlišit a ze samotné adresy se nedozvíte, zda je individuální či výběrová.

Pokud přidělujete některému rozhraní výběrovou adresu, musí se to příslušným způsobem odrazit v konfiguraci. Vezmete-li všechna rozhraní, která nesou určitou výběrovou adresu, jistě dokážete najít jistou (co nejmenší) obalovou síť či skupinu sítí, v níž jsou obsažena. Tuto síť lze charakterizovat prefixem *P*. Například pokud se budou všichni členové výběrové skupiny nacházet ve stejné podsíti, bude *P* prefix (adresa) této podsítě.

Uvnitř sítě dané prefixem *P* musí mít výběrová adresa svůj vlastní směrovací záznam, který v jednotlivých směrovačích ukazuje vždy na nejbližšího člena skupiny. Podle těchto záznamů jsou doručovány pakety adresované výběrové skupině. Mimo oblast danou prefixem *P* pak již není třeba s výběrovou adresou zacházet nijak speciálně a může být zahrnuta do agregovaného bloku adres.

Skutečnost, že výběrové adresy lze směrovat obvyklými metodami (de facto se jedná o cesty k individuálním počítačům, které dnešní směrovací algoritmy a protokoly podporují), je rozhodně dobré

Existence globálních výběrových adres je velmi silně omezena a ani do budoucna se neočekává, že by si je snadno mohl zřizovat kdokoli.

Pošlete-li sérii datagramů na stejnou výběrovou adresu, **mohou být dopraveny různým počítačům. To způsobuje problémy stavovým protokolům, jako je TCP**, ale i službám uchovávajícím stav na straně serveru. Možným řešením je **rozdělit komunikaci na dvě fáze**. V úvodní, která používá výběrové adresy, klient zjistí od serveru jeho individuální adresu a tu pak použije pro vlastní, stavovou fázi přenosu dat.

Ideálem výběrového adresování je služba bez potřeby stavových informací.Typickým příkladem je právě DNS, kdy dotaz a odpověď představují po jednom datagramu přenášeném protokolem UDP.

Směrovací politiky, kdy páteřní internetové směrovače odmítají příliš dlouhé prefixy, a tedy záznamy pro výběrové adresy. Agregace prefixů, která může napáchat na směrování výběrových adres nepěkné škody.

Změny ve skupině mohou být vyhodnoceny jako kolísání (flapping) a následně blokovány. Mohou mít také problémy s bezpečnostními RPF testy(penetrační testy), které mohou v jejich případě neprávem vyhodnotit zdrojovou adresu jako falšovanou.

Výše uvedené vede k závěru, že **výběrové adresování je v globálním měřítku použitelné jen velmi omezeně pro úzký sortiment vybraných služeb** (kořenové DNS servery).

Uvnitř menší části sítě (v jednom autonomním systému či v koncové zákaznické síti), kde směrování má zcela pod kontrolou jeden provozovatel, **může výběrové adresování představovat rozumně a celkem široce použitelný mechanismus**. Výše popsané problémy jsou zde řešitelné bez většího úsilí a lze očekávat i řídké změny topologie, takže datagramy budou zpravidla doručovány témuž stroji.

Výběrové lokální adresy adresy v rámci jediné podsítě

Určitý **extrém představují výběrové lokální adresy adresy v rámci jediné podsítě**. U nich pochopitelně nemá smysl mluvit o nejbližším členovi, z pohledu směrování jsou všichni členové stejně daleko.

Slouží jako obecné adresy, kdy počítač chce komunikovat se strojem poskytujícím určitý typ služby a nezáleží mu na tom, s kým konkrétně.

Tyto výběrové adresy **mají podobu pevně definovaných identifikátorů rozhraní, před nějž se přidá prefix příslušné podsítě.**

Zatím byly definovány dvě takové adresy:

samé nuly v identifikátoru rozhraní znamenají výběrovou adresu pro směrovače v podsíti

adresa *prefix*:fdff:ffff:ffff:fffe identifikuje domácí agenty v podsíti (mobilita).

Kromě toho RFC 2526: *Reserved IPv6 Subnet Anycast Addresses* rezervuje horních **128 identifikátorů rozhraní pro různé speciální účely.**

Význam těchto adres je jednotný **a postupně je přiděluje IANA.** Zatím jedinou přidělenou adresou z tohoto balíku je výše zmíněná adresa pro domácí agenty. Tabulka poskytuje **přehled pevně definovaných výběrových adres pro podsíť:**

adresa	*význam*
prefix:0:0:0:0	směrovače v podsíti
prefix:fdff:ffff:ffff:ff80 až *prefix*:fdff:ffff:ffff:fffd	rezervováno
prefix::fdff:ffff:ffff:fffe	domácí agenti

Dřívější definice adresní architektury IPv6 zavedla – vzhledem k nedostatku zkušeností – pro výběrové adresy značná omezení. Směly být přiřazeny jen směrovačům a bylo zakázáno uvádět je do zdrojové adresy IPv6 datagramu. V současnosti již tato omezení neplatí.

Povinné adresy uzlu

V IPv4 mívalo rozhraní zpravidla právě jednu adresu. Existovaly sice výjimky (např. virtuální WWW servery bývaly svého času realizovány tak, že počítač slyšel na několik IP adres pro totéž rozhraní), ale valná většina uzlů toto pravidlo dodržovala.

IPv6 naproti tomu umožňuje, že rozhraní bude mít více adres, ale dokonce mu to nařizuje. Existuje totiž jasně definovaná minimální množina adres, ke kterým se každý uzel IPv6 sítě *musí* hlásit.

Pro koncový pro počítač počítač se jedná o následující adresy:

lokální linková adresa pro každé rozhraní

všechny individuální a výběrové adresy, které mu byly přiděleny

lokální smyčka (loopback)

skupinové adresy pro všechny uzly

skupinová adresa pro vyzývaný uzel pro všechny přidělené individuální a výběrové adresy

všechny skupinové adresy, jejichž je členem

Například pro KZ platí :

lokální linková	fe80::22a:fff:fe32:5ed1
přidělená individuální	2001:db8:a319:15:22a:fff:fe32:5ed1
přidělená individuální	2001:db8:a319:3:22a:fff:fe32:5ed1
lokální smyčka	::1
všechny uzly v rámci rozhraní	ff01::1
všechny uzly v rámci linky	ff02::1
vyzývaný uzel	ff02::1:ff32:5ed1
přidělená skupinová	ff15::ac07

Směrovač se povinně musí hlásit pro směrovač ke všem adresám jako počítač a navíc k následujícím:

výběrová adresa pro směrovače v podsíti (pro každé rozhraní, kde funguje jako směrovač)

skupinové adresy pro všechny směrovače

Například:

směrovače v podsíti	2001:db8:a319:15::
směrovače v podsíti	2001:db8:a319:3::
vyzývaný uzel	ff02::1:ff00:0
přidělená výběrová	2001:db8:a319:15:fdff:ffff:ffff:fffe
přidělená výběrová	2001:db8:a319:3:fdff:ffff:ffff:fffe
vyzývaný uzel	ff02::1:ffff:fffe
všechny směrovače na rozhraní	ff01::2
všechny směrovače na lince	ff02::2
všechny směrovače v místě	ff05::2

Dosahy adres

IPv4 původně počítalo výlučně s celosvětově jednoznačnými adresami. Později bylo doplněno několik lokálních adres (10.0.0.0, 192.168.0.0 a spol.), které mají platnost omezenu na místní síť a nesmí být předávány do Internetu.

IPv6 bere koncept dosahu adres jako jeden ze standardních prvků adresace. Věnuje se mu RFC 4007: *IPv6 Scoped Address Architecture*.

Formálně je dosah definován jako vymezení topologické oblasti sítě, v níž je daná adresa jednoznačná. Dostupné dosahy se liší podle druhu adresy.

Nejjemnější členění mají skupinové, pro které je v současnosti definováno šest stupňů lokality.

Individuální adresy rozlišují jen dva stupně: lokální pro linku a globální.

Výběrové adresy spadají mezi individuální, takže mají i stejné dosahy.

Dosah význam

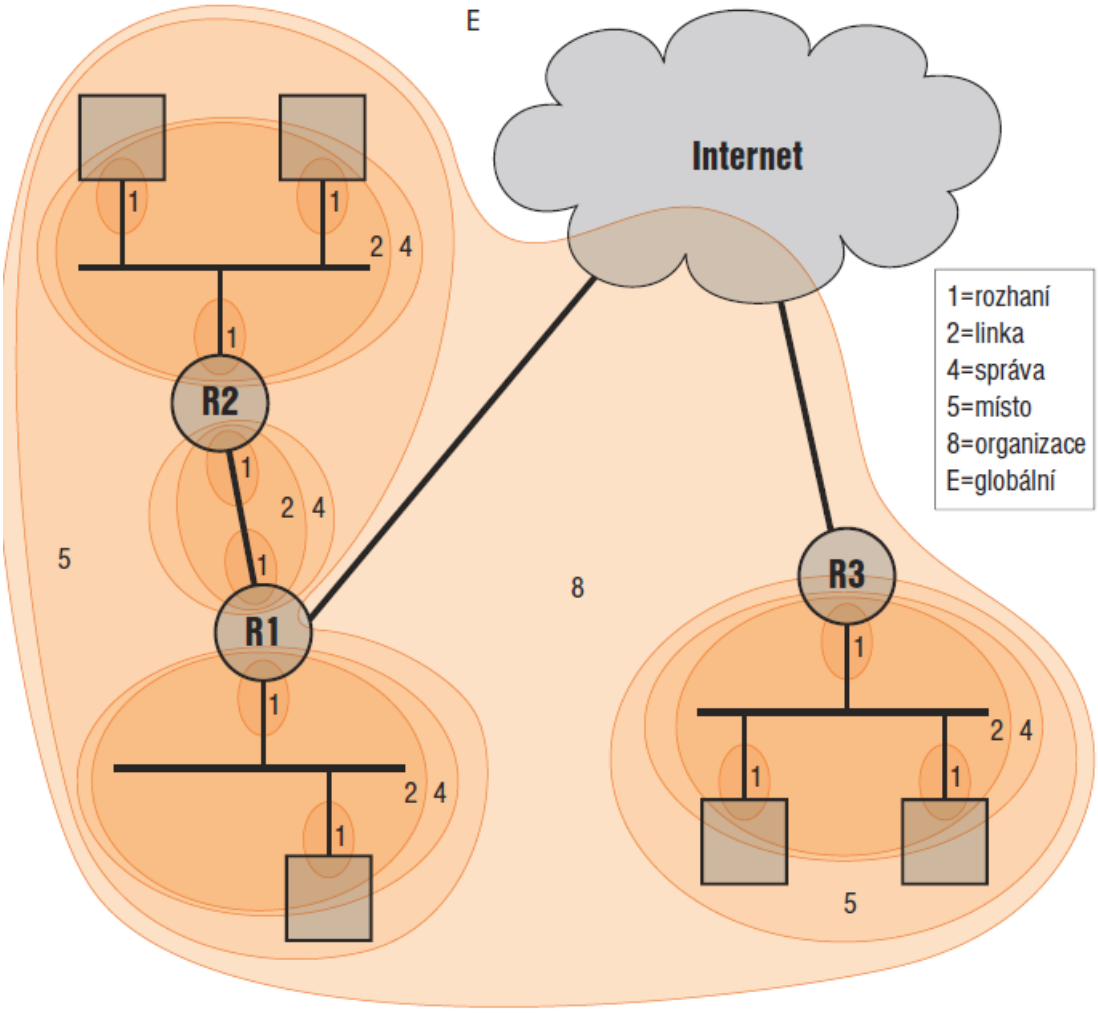
dosah	*význam*
1=rozhraní	nepřekročí jediné rozhraní; používá se pro skupinové vysílání do rozhraní pro lokální smyčku (loopback, adresa ::1)
2=linka	dosah je omezen na jednu fyzickou síť (např. Ethernet či pouhou sériovou linku se dvěma účastníky)
4=správa	nejmenší dosah, který musí být konfigurován správcem (čili nelze jej automaticky odvodit z fyzické topologie či dalších informací); obvykle se jedná o podsíť
5=místo	část síťové topologie, která patří jedné organizaci a nachází se v jedné geografické lokalitě, prostě koncová zákaznická síť
8=organizace	pokrývá několik míst náležejících téže organizaci, například pobočky téže firmy v různých městech
E=globální	celosvětový dosah

V souvislosti s dosahy se též objevuje **zóna. Jedná se právě o tu část síťové topologie, která odpovídá danému dosahu (adresa je v zóně jednoznačná).**

Hranice zón procházejí počítači, nikoli linkami. Pochopitelně platí, že celá zóna je vždy zahrnuta do „nadřízené“ zóny většího dosahu. Naopak zóny stejného dosahu se nemohou překrývat (jsou buď totožné nebo zcela oddělené).

Z hlediska směrování musí být zóna souvislá – pokud by datagram během přepravy opustil zónu, mohlo by dojít k dezinterpretaci jeho adresy.

Dosah zóny se odvodí z vlastní adresy. Kompletní zápis adresy pak má tvar *adresa*%*zóna*. Například pokud bude spodní Ethernet připojený ke směrovači R1 reprezentován identifikátorem linkové zóny 1, bude mít skupinová adresa pro všechny uzly na této lince
plný tvar ff02::1%1.



Komentář si zaslouží změny, jimiž postupně prochází sortiment definovaných dosahů. **Zatím směřují jednoznačně ke zjednodušení, během několika let zmizely dva dříve definované dosahy.**

Individuální adresy původně obsahovaly ještě dosah lokální pro místo, který odpovídal dosahu 5 u skupinových adres.

Výběr adresy

Přiřazení několika různých adres témuž rozhraní vyvolává nový problém, kterou z nich si vybrat.

Odpověď poskytuje RFC 3484: *Default Address Selection for Internet Protocol version 6 (IPv6)*, jež stanoví přesný postup pro výběr adres v odesílaném datagramu. **Jeho cílem je, aby se všechny implementace IPv6 chovaly konzistentně a předvídatelně.** Na druhé straně ovšem ponechává správci stroje možnost ovlivňovat výběr adres nastavením určitých priorit.

Základem algoritmu je výběr adresy z několika kandidátek, případně jejich seřazení podle vhodnosti.

Aplikace, která chce komunikovat, má někdy k dispozici cílovou IP adresu. Pak je kandidátka jen jedna a výběr cílové adresy odpadá.

Většinou je ale cíl zadán doménovým jménem. Aplikace v tom případě nejprve zavolá systémovou službu *getaddrinfo( )*,kterou požádá o převod DNS jména na IP adresu. **Z DNS dotazu vzejde *seznam kandidátek na cílovou adresu* a ten je následně podle určitých pravidel uspořádán od nejvhodnější adresy po nejméně vhodnou.**

Příkladem je implicitní tabulka priorit – místních preferencí

prefix	*priorita*	*značka*
::1/128	50	0
::/0	40	1
2002::/16	30	2
::/96	20	3
::ffff:0:0/96	10	4

Vhodným nastavením tabulky politik může správce systému přizpůsobit chování výběru adres svým potřebám.

Algoritmus pro volbu adresy definuje dvě sady pravidel. Jedna se vztahuje na zdrojovou adresu a druhá na cílovou.

Vícedomovci čili multihoming

Vícedomovci jsou opakem bezdomovců.

Příklady známých vícedomovců[7] jasně naznačují, že **být vícedomovcem je výhodné**. V síťové praxi se tímto pojmem označují zákaznické sítě, které jsou připojeny k několika poskytovatelům připojení.

Hlavním **cílem je zajistit zákaznické síti spojení s Internetem i v případě, že u některého z poskytovatelů dojde k výpadku** a cesta vedoucí přes něj se přeruší.

Vícedomovci se stávají především poskytovatelé služeb, jejichž výpadek by byl kritický a znamenal ztrátu, ať už přímou finanční či poškození jména.

Například Seznam by jistě nepotěšilo, kdyby byly jeho servery několik hodin nedostupné. Podobně by kterákoli banka špatně nesla ztrátu spojení svého platebního systému.

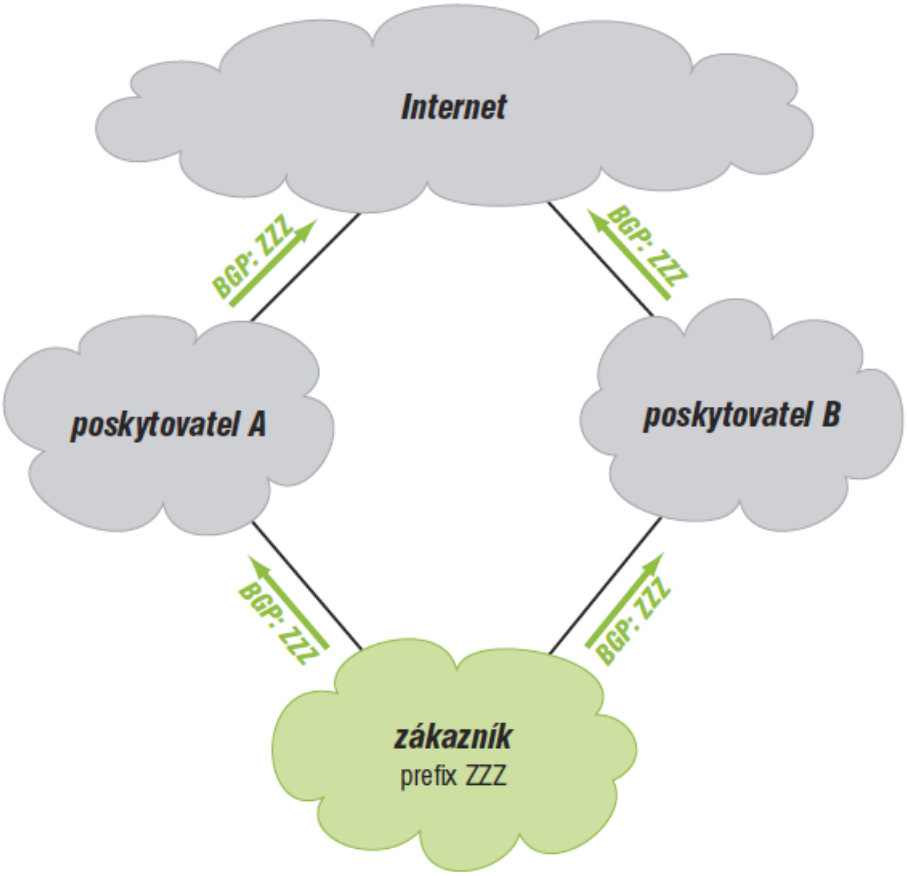
Podrobněji cíle vícedomovectví pitvá RFC 3582: *Goals for IPv6 Site-Multihoming Architectures*.

Vedle redundance a odolávání výpadkům se docílí **i rozkládání zátěže a zvyšování výkonu díky paralelním přenosům různými sítěmi.**

Důležitým požadavkem je transparentnost vůči vyšším vrstvám. Jestliže dojde k výpadku a provoz je převeden na jiného poskytovatele, měla by navázaná spojení normálně pokračovat a nemělo by to ani omezit možnost navazovat nová v obou směrech.

Směrování při vícedomovectví je problém.

Současná **běžná praxe** je taková, že **síť, která chce být připojena k několika poskytovatelům Internetu, si založí svůj vlastní autonomní systém (AS)** a vstoupí do globálních směrovacích tabulek. To znamená, že má svůj záznam na nejvyšší úrovni směrování v páteřních směrovačích Internetu. Ten šíří všichni poskytovatelé, k nimž je připojena. Standardní směrovací mechanismy se postarají o nalezení optimální cesty k ní i o její aktualizace při změnách v síti. Stejné řešení se používá i ve světě IPv4.



V IPv6 tento přístup nejde celý přijmout, protože jedním ze základních východisek při návrhu **adresní struktury IPv6 bylo, aby umožňovala masivní slučování (agregaci) prefixů a snižovala tak počet záznamů ve směrovacích tabulkách páteřních směrovačů.** Dosavadní praxe je v jasném rozporu s tímto cílem.

Na druhé straně je třeba přiznat, že tento přístup zatím jako jediný skutečně funguje a až na škálovatelnost splňuje všechny ostatní požadavky. Navíc nevyžaduje žádné změny v používaných protokolech a systémech, jen opatření administrativního charakteru.

Některé **další teoretické cesty naznačuje mobilita** RFC 4177: *Architectural Approaches to Multi-homing for IPv6*. Řešení pro mobilní systémy.

Mobilní zařízení je někde doma a pokud je na cestě, poskytuje ostatním informaci „momentálně jsem k zastižení na adrese X“. Doma jej mezitím zastupuje domácí agent, kterému přeposílá datagramy přicházející na jeho domácí adresu.

Vícedomovecká síť by v tomto případě dostala dva prefixy – *PA* od prvního poskytovatele a *PB* od druhého. Jestliže stroj v ní komunikuje na adrese *PA:X* a cesta přes prvního poskytovatele padne, může využít mobilní mechanismy a sdělit svým partnerům„ momentálně jsem k zastižení na adrese *PB:X*“.

Toto řešení naráží na několik problémů:

Mobilita není dosud v implementacích příliš dobře podporována.

Koncový počítač se musí dozvědět, že používané spojení bylo přerušeno a že by měl partnerům oznámit změnu adresy.

Problém představuje zabezpečení. Aby se kdokoli nemohl prohlásit za jiný uzel na cestách, následuje po přijetí zprávy „mám adresu *X* a momentálně jsem k zastižení na adrese *Y*“ test, zda její odesilatel skutečně přijímá data na obou uvedených adresách. Teď jsme ovšem v situaci, kdy jedna z adres nefunguje a test proto nemůže proběhnout úspěšně.

Značné **úsilí je v současnosti věnováno vývoji mechanismů, které by vedly k rozdělení výše uvedených dvou úloh adresace.** Aby každý stroj **měl svůj jeden neměnný identifikátor**, **který by používaly protokoly vyšších vrstev a který by nezávisel na aktuální síťové situaci.** Kromě toho by ovšem měl **přiřazen jeden či několik dočasných lokátorů** využívaných při směrování, které by pružně měnil v závislosti na stavu sítě – při svém pohybu Internetem, při výpadcích a startech linek. Lokátory by sloužily nižším vrstvám komunikační architektury k zajištění vlastních přenosových služeb.

O určitý kompromis se snaží pracovní skupina IETF nazvaná *Site Multihoming by IPv6 Intermediation*, která se v současné době jako jediná zabývá problematikou vícedomovců. Vyvíjí protokol nazvaný ***Shim6*** *(Level 3 Multihoming Shim Protocol for IPv6)*.

Slovo „shim“ znamená podložku a mezi programátory se používá pro jednoduchou knihovnu, která převádí jedno aplikační rozhraní na jiné. Docela pěkně to vystihuje jeho funkci. Protokol se zatím nachází ve fázi pracovního návrhu,

Přidělování adres

IPv6 se do praxe prosazuje sice pomalu, ale z hlediska administrativního je dnes se svým předchůdcem srovnatelný. **Procedura přidělování jeho adres je dnes totožná pro oba protokoly:** centrální autoritou je *IANA (Internet Assigned Numbers Authority)*, která přiděluje velké bloky adres *regionálním registrům (Regional Internet Registry, RIR)*.

AFRINIC Afrika
APNIC Asie a Pacifik
ARIN Severní Amerika
LACNIC Latinská Amerika
RIPE NCC Evropa a Blízký východ

Jednotlivé regionální registry přidělují menší bloky *registrům lokálním (Local Internet Registry, LIR)*. Roli lokálních registrů zpravidla zastávají poskytovatelé Internetu. Od nich získávají adresy koncové instituce – zákazníci.

Konkrétně v Evropě je aktuálně stanoví pravidla přidělování dokument ripe-421: *IPv6 Address Allocation and Assignment Policy* z listopadu roku 2007. Podle něj **RIPE NCC přiděluje lokálním registrům prefixy délky 32 bitů.**

Aby jej LIR mohl získat, musí splnit níže uvedené podmínky. Stručně řečeno: pokud jste

LIR a plánujete do dvou let poskytovat IPv6 služby, máte nárok na 32bitový prefix:

1. Žadatel musí být lokálním registrem.
2. Pokud má být přidělený adresní prostor použit v Internetu, musí jej ve směrování ohlašovat jako jediný prefix.
3. Žadatel musí mít plán jak alokovat části přiděleného IPv6 prostoru dalším organizacím a sítím do dvou let.

Standardní délka prefixu přidělovaná koncových sítím je 48 bitů. Lokální registr má tedy k dispozici 16 bitů pro rozlišení svých zákazníků.

TJ. prostor pro 65 536 zákaznických prefixů. Pokud by to bylo málo, politika RIR připouští v odůvodněných případech přidělit lokálnímu registru prefix kratší nebo skupinu 32bitových prefixů.

Pokud se týče délky zákaznických prefixů, základním dokumentem je RFC 3177: *IAB/IESG Recommendations on IPv6 Address Allocations to Sites*.

Podle něj by LIR měl postupovat následovně:

48 bitů je standardní délka prefixu, který by měl být **přidělován drtivé většině připojených sítí** (malé i velké instituce, domácí sítě a podobně).

Použití prefixů délky 48 bitů má řadu výhod. Je nezávislé na poskytovateli, takže usnadňuje změnu poskytovatele či multihoming. Odpovídá prefixům již zavedených služeb a protokolů (např. 6to4).

Pouze u mimořádně velkých institucí lze uvažovat o přidělení kratšího prefixu nebo skupiny několika prefixů /48.

Prefix délky 64 bitů přidělovat v případech, kdy je zcela jisté, že dotyčná instalace nebude vyžadovat podsítě. Jako příklad jsou uváděny mobilní sítě (v autě či osobní síť za mobilním telefonem).

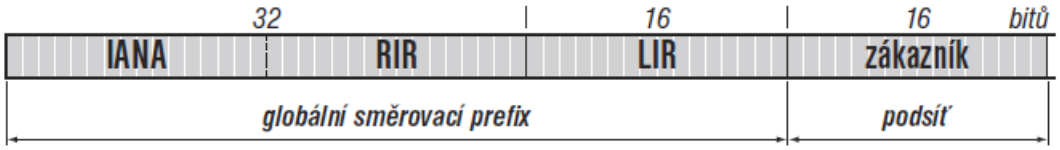
Pokud bude zcela jisté, že se připojuje jen jediné zařízení, lze přidělit prefix délky 128 bitů, tedy jedinou adresu.

Operuje zde s takzvaným **poměrem H, v podstatě se vyjadřuje poměr mezi počtem reálně přidělených adres a celkovou velikostí dostupného adresního prostoru.**

Praxe ukázala, že **problémy s nedostatkem adres** se začnou objevovat, když **poměr H vzroste nad 0,25.** Při 45 bitech pro adresu sítě (z prefixu /48 je třeba odečíst první tři bity, jejichž hodnota 001 identifikuje tuto část adresního prostoru) **dojde k této situaci po přidělení přibližně 180 miliard prefixů.**

Americký úřad pro sčítání lidu odhaduje celosvětovou populaci v roce 2050 na 10 miliard lidí. To znamená, že na každého obyvatele zeměkoule lze bez problémů přidělit téměř 20 sítí s prefixem délky 48 bitů.

Přesto se již řadu let opakovaně **objevují úvahy**, **že 48bitový prefix je pro některé účely zbytečně velký, že by se mělo šetřit hned od začátku** a že by bylo účelné přidělovat malým sítím prefix délky 56 bitů.



První část adresy přiděluje IANA regionálním registrům. Její délka kolísá**, zpočátku IANA šetřila a přidělovala prefixy délky 23 bitů**. **V říjnu 2006, ale každý RIR dostal po jednom dvanáctibitovém prefixu.**

Následuje **část přidělovaná regionálním registrem.** Zde je **hranice pevná** a dohromady s počátkem od IANA **tvoří 32bitový prefix přidělovaný lokálním registrům.**

Lokální registry mají pod kontrolou následujících 16 bitů, jimiž definují 48bitový prefix zákaznické sítě.

Za ním pak následuje **16bitový identifikátor podsítě.**

S trochou zjednodušení dostáváme čtyři šestnáctibitové identifikátory, které po řadě přidělují IANA, RIR, LIR a zákazník.

Podle těchto pravidel bylo do konce června 2008 přiděleno 2350 prefixů pro lokální registry, z toho zhruba polovina v oblasti spravované RIPE NCC.

Celkem v nich byl prostor na bezmála pět miliard zákaznických 48bitových prefixů. Aktuální čísla si můžete prohlédnout na adrese
www *http://www.ripe.net/rs/ipv6/stats/index.html*
Přehled prefixů přidělených IANA najdete na stránce
www *http://www.iana.org/assignments/ipv6-unicast-address-assignments*

O IPv6 adresy je zájem. Reálně bylo v polovně roku 2008 ve směrovacích tabulkách ohlašováno zhruba tisíc z 2350 přidělených prefixů.
Jejich statistiky připravuje pro pravidelné RIPE Meetingy Gert Döring a najdete je na adrese
www *http://www.space.net/~gert/RIPE/*