Identifikace L2 – linková vrstva

Identifikace KZ na linkové vrstvě

Opakování
Typ adresace – unicast, broadcast, multicast

V datových sítích obecně rozlišujeme několik typů adresací podle toho, koho chceme oslovit. Jedná se o **obecně platné rozdělení nezávislé na linkové technologii nebo na vrstvě**, na které adresujeme KZ.

Adresace jednoho zařízení se nazývá unicast. Adresa je proto **unikátní (jedinečná) v rámci nějaké části počítačové sítě např. LAN**. Každé KZ má svoji unicast adresu, při jejím použití je osloveno a musí data zpracovat. **Takto se „adresuje" datový blok nejčastější.**

Adresace skupiny zařízení se nazývá multicast. Adresa se nazývá také **skupinová.** Nejčastěji se používá na úrovni **LAN – lokální, proto se jedná o lokální multicast**. Tento typ adresace je součástí mnoha infrastrukturních protokolů (provozních). V současnosti se rozšiřuje i využíváním tzv. streamových vysílání např. šíření videa pro skupinu uživatelů pomocí multicast vysílání apod. Ty KZ, která jsou členy určité skupiny, musí zpracovat data multicast rámce. **Adresní prostor pro multicast adresaci je vyhrazen** (viz.dále).

Adresaci všech zařízení zajišťuje broadcast. Broadcast se **může volně šířit jen v určité části počítačové sítě** (jinak by vzniknul pěkný zmatek..). Jedná se převážně o lokální síť- LAN. Všechna KZ na LAN jsou jej povinna zpracovat a eventuálně reagovat. Broadcast adresace **je důležitým prvkem mnoha provozních protokolů (ARP, DHCP apod.).** Pro broadcast je vyhrazena **vždy nejvyšší adresa v rozsahu adres.** Broadcast lze chápat i jako krajní typ multicast adresace (IPv6).

Pozn.:

Dalším typem adresace je anycast. Na linkové vrstvě se nepoužívá. Bude vysvětleno v rámci IP protokolů (síťová vrstva).

Fyzická adresa

Na linkové vrstvě komunikují síťová rozhraní (HW- síťové karty). Každá síťová technologie (nebo také linková) používá jiný formát rámců a fyzických adres (komunikace mezi dvěma sítěmi různé technologie se tedy nemůže opírat o fyzické adresy!).

Síťové rozhraní (karta) má svou unikátní **fyzickou adresu (unicast adresa)** nebo **HW adresu** nebo **MAC adresu** (Media Access Control) nebo **linkovou adresu (**jak je libo…**).** HW adresa je tedy **principiálně neměnná a pevně umístěna výrobcem např. do EEPROM**.

Fyzická adresa musí být v rámci LAN unikátní. Při duplicitě dochází k vážné chybě sítě a k zhroucení jejího chodu. V některých případech **jde její unikátní část měnit pomocí driverů rozhraní (**v LNX např. ethtools nebo přímo v nabídce oken OS nastavení sítě, vždy záleží na výrobci HW).

Fyzickou adresu má přiřazenou síťové rozhraní (karta), nikoliv počítač (jeden počítač může mít několik síťových karet i virtuálních).

Síťové rozhraní **přijímá jen jemu adresované rámce** a v nich přenášená data předává počítači k dalšímu zpracování. **Rámce určené jiným stanicím síťové rozhraní ignoruje** a data v nich přenášená počítači nepředává. **Chybné rámce obvykle ignoruje.**

Síťová karta může pracovat v promiskuitním režimu. Ten umožňuje zachytávat i síťovou komunikaci, která není přímo určena pro dané zařízení nebo počítač (tzv. *packet sniffing*).

Režim používají analyzátory paketů pro zachytávání dat na routerech, na počítačích připojených k přepínači (switch), pro bezdrátové sítě nebo softwarových přepínačích (switchích) hardwarové virtualizace.

Mnoho operačních systémů vyžaduje pro povolení promiskuitního režimu oprávnění správce. Síťový uzel v promiskuitním režimu může sledovat síťovou komunikaci, která mu není adresována pouze pokud přichází ze (nebo odchází do) stejné broadcastové domény. Počítače připojené do stejného rozbočovače (huby) splňují tuto podmínku i proto jsou použity síťové přepínače (switche) pro boj proti zneužívání promiskuitního režimu.

Promiskuitní režim je často používán k diagnostice problémů s připojením k síti. Analýzou paketů se ukáží uživateli všechna data přenášená přes síť. Proto pozor na otevřené komunikace (FTP, Telnet, http, smtp..)

Promiskuitní režim může být použit ke škodlivým účelům (odposlech v síti), Takto mohou některé programy posílat odpovědi na rámce, které byly adresované jinému zařízení. O*dposlouchávači* (sniffer) tomu mohou zabránit (např. pomocí pečlivého nastavení firewallu). Příkladem je odesílání pingu (ICMP echo request) se špatnou MAC adresou, ale správnou IP adresou. Pokud adaptér pracuje v normálním režimu, zahodí tento rámec a zařízení tak na tento ping neodpoví. Pokud je adaptér v promiskuitním režimu, rámec bude předán dál a IP stack zařízení (u kterého MAC adresa nemá žádný význam) na tento ping odpoví stejně jako na jakýkoliv jiný. Zabránit tomuto lze tím, že firewall bude blokovat ICMP provoz.

Zdroj: Wikipedie

Ethernet fyzická adresa (MAC adresa) a její struktura

Sortiment formátu fyzických adres se v současnosti ustálil na ethernetovém formátu. **MAC adresa je 48 bitová (6B),** např. 00-00-64-65-73-74. Zapisuje se hexadecimálně po bytech. Oddělovačem je většinou dvojtečka a pomlčka (nebo i jiný běžný oddělovač).

Jiné formáty jako ARCNET fyzická adresa o rozsahu 1B se nepoužívají.

Je rozdělena na dvě části. První tři oktety (byte) identifikují výrobce nebo skupinovou (multicast) adresu, další 3B zajišťují lokální jedinečnost.

00-00-64 65-73-74

Pozn.: funkce „MAC lookup“ nám umožní na Internetu zjistit o jakého výrobce se jedná – vyzkoušejte pro výše uvedenou adresu.

Kromě těchto jedinečných adres (unicast) existují i **další typy:**

Broadcast fyzická adresa - oběžník pro všechny stanice v LAN (na lince – L2)

FF-FF-FF-FF-FF-FF

Adresný oběžník (multicast) – 0. bit 1. B nastaven na 1 - určen stanicím v LAN nastaveným na akceptování adresného oběžníku (prakticky se nepoužívá)

Nultý a první bit prvého bytu mají specifický význam:

Pozn.:

EUI 64 - Extended Unique Identifier (64bitový identifikátor rozhraní)

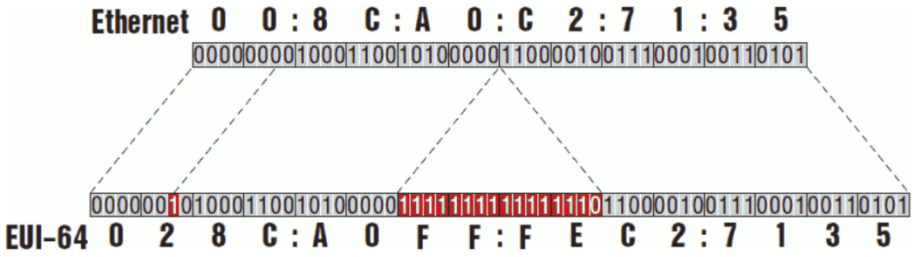
Identifikátor rozhraní, který by měly používat **individuální adresy IPv6**, je odvozen z identifikátoru IEEE EUI-64 (je to druhá půlka IPv6 adresy dlouhá 8B).

Vznikne z linkové ethernetové adresy **vložením konstanty „FFFE“ mezi třetí a čtvrtý byte**.

V IPv6 se navíc obrací **význam druhého bitu v adrese, který rozlišuje globální identifikátory od lokálních**. Původně nulová hodnota znamená, že identifikátor je globálně jednoznačný, v modifikovaném EUI-64 používaném pro IPv6 nulová hodnota označuje lokálně jednoznačný identifikátor. Cílem této úpravy je, aby identifikátory odvozené z EUI-64 byly konzistentní s ručně přidělovanými (například **identifikátor 1, který je zjevně jednoznačný jen lokálně** v rámci podsítě).

Z ethernetové adresy	00:8c:a0:c2:71:35
tak vznikne IPv6 identifikátor rozhraní	28c:a0ff:fec2:7135

Způsob jeho vytvoření ilustruje následující obrázek:



Pozn.
Jako identifikátor rozhraní v IPv6 je možné použít i jiné řešení dle RFC 7136 (kvůli bezpečnosti). Jestliže je však odvozován z MAC add musí se použít EUI-64.

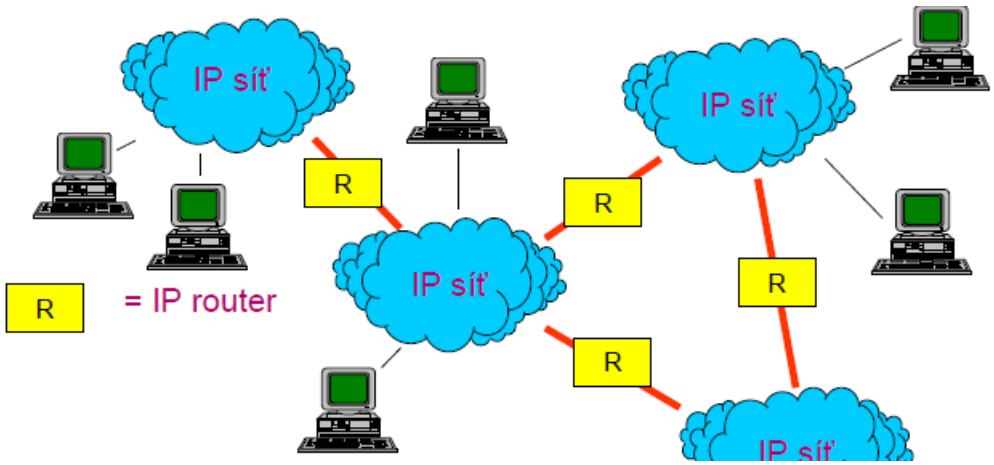
Jednotná adresace na L3 – síťové vrstvě

Internet protokol musí vytvořit jednotné

- Prostředí
- Služby
- Adresaci

Adresace na síťové vrstvě je zajištěna pomocí logických adres – IP adres v rámci protokolu verze 4. Tyto adresy jsou nezávislé na různých identifikacích KZ nižších vrstev (např. fyzické adresy). IP adresa není nutně přiřazena počítači pevně (může být klidně každý den jiná).

Jednotlivé dílčí sítě (IP sítě – **adresa sítě - AS)** jsou vzájemně propojeny na úrovni síťové vrstvy pomocí směrovačů (routerů). **Adresa gateway - GW** je označení brány sítě do internetu (do vyšší úrovně propojení sítí).



Logické adresy

Logické adresy musí být

- Transparentní vzhledem k soustavě propojených sítí (internetu) – síť by měla být z adresy zřejmá – **síťová část adresy**
- Umožňující jednoznačný převod na fyzické adresy přenosových technologií – **uzlová (místní, host) část adresy**
- Vyhovující potřebám směrování
    - **celosvětově jednoznačné**
    - **dostatečně malé – analýza pomocí HW**

Z výše uvedeného vyplývá, že adresy jsou dvousložkové. V levé části je síťová část oddělená pohyblivou hranicí od pravé uzlové části.

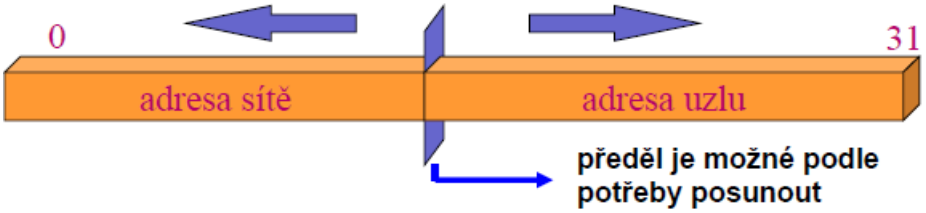
V praxi mohou existovat různé IP sítě:

- **velké sítě s hodně velkým počtem uzlů** (např. větším než 65 536 uzly), může jich být málo
- **střední sítě** (např. 250 až 60 000 uzlů)
- **malé sítě s hodně malým počtem uzlů** (např. menším než 255), kterých může být velmi mnoho

Autoři TCP/IP proto navrhli proměnný formát IP adres – s pohyblivou hranicí.

IPv4 adresa

- je **32-bitová** neboli 4B dlouhá
- zapisuje se dekadicky po bytech
- oddělovačem mezi byty je „ . “



Posun hranice mezi částmi IP adresy lze provádět po

- bytech – pomocí rozsahu 1B adresy – potom se jedná o rozdělení adres do tříd
- bitech –pomocí
    - maskování síťové části – síťová maska (zkratka NM – network mask)
    - uvedení počtu bitů síťové části – prefixové vyjádření – prefix adresy

Třídy IP adres

Jedná se o původní členění do tříd a to se při přidělování veřejných adres opustilo. Přesto se používá nadále v rámci adresních plánů (privátní adresy). Znalost příslušnosti IP adresy do třídy je potřeba.

Třídy IP adres

Třída	začátek (bin)	1. bajt	bitů sítě	bitů stanice	sítí	stanic v každé síti
A	0	0–127	7	24	$2^7 = 128$	$2^{24}-2 = 16\,777\,214$
B	10	128–191	14	16	$2^{14} = 16384$	$2^{16}-2 = 65\,534$
C	110	192–223	21	8	$2^{21} = 2\,097\,152$	$2^8-2 = 254$
D	1110	224–239	lokální multicast			
E	1111	240–255	vyhrazeno jako rezerva			

Pozn.:
Adresy tříd A, B a C jsou unicast. Třída D obsahuje lokální multicast.

Vyhrazené adresy

Rozsah adres použitelný v určité síti je snížen o 2 (červeně). Jedná se o vyhrazené adresy, které nemůže mít přiděleny žádná stanice v síti.

Adresa sítě (AS, NA) – nejnižší adresa v rozsahu adres sítě (např. 10.0.0.0)
Broadcast adresa (BA) - nejvyšší adresa v rozsahu adres sítě (např. 10.255.255.255)

Pozn.: V současnosti by se měly odebírat 3 adresy z adresovatelného prostoru. Třetí adresou je port směrovače – output gateway. Izolované sítě bez připojení k internetu (WAN) takřka neexistují.

Local loopback – localhost – vyhrazená adresa sítě pro vytvoření lokální smyčky (nutné pro testování apod.) – síť 127.0.0.0 a localhost 127.0.0.1 .

Nespecifikovaná adresa – obecná – 0.0.0.0 – je to nejnižší adresa „všech sítí“. Jestliže se cílová síť nenajde mezi záznamy ve „směrovací tabulce“, pak se použije směr této adresy, kde reprezentuje záznam pro všechny ostatní sítě. Žádnému zařízení se nepřidělují adresy v rozsahu sítě 0.0.0.0. Naopak adresa 255.255.255.255 má podobný význam, ale naopak reprezentuje pouze jedno rozhraní (nejvyšší adresa v rozsahu sítí je takto vymezena úplně).

Další vyhrazené adresy - privátní jsou uvedeny dále.

Maskování a prefixové vyjádření

Posun hranice mezi síťovou a uzlovou částí IP adresy po bitu je řešen pomocí

- **maskování síťovou maskou (NM – Network Mask).** Logická „1“ vyjadřuje část sítě a „0“ část uzlu. Jedná se proto v binární formě o spojitý sled jedniček zleva. Vyjadřuje se stejně jako IP adresa dekadicky s oddělením po bytech tečkou.

  Síťové masky dopovídající třídám se nazývají **přirozené nebo defaultní masky**
  A 255.0.0.0
  B 255.255.0.0
  C 255.255.255.0

- **prefixové vyjádření prefixovým údajem** (celkovým počtem jedniček sítě) za IP adresou oddělený lomítkem. Např.: 10.0.0.0/8.

Pozn.: Maska nebo prefix je dalším povinným údajem nastavení síťové části OS.

Způsoby efektivního využití adresního prostoru IPv4

Prostor IPv4 adres s rozvojem internetu byl rychle čerpán. Jeho efektivní využití bylo a je proto nutnosti. Způsoby lze rozdělit na dvě části, ty které lze použít okamžitě bez dalších úprav a ty které bylo možno použít až po zavedení opatření.

Přehled způsobů efektivního využití adresního prostoru IPv4:

- Okamžité použití

  Přidělování adres po menších kvantech
  Vytváření podsítí

- Použití po úpravách

  Vytváření supersítí (supernetting) či směrů a z toho vyplývající přidělování IP adres po blocích (CIDR)

  Privátní sítě

Detailní popis

- Okamžité použití

  - **Přidělování adres po menších kvantech -** opatření spočívá pouze v tom, že se raději přidělí více menších rozsahů adres než jeden větší. Nevyužité adresy jsou blokovány. Proto je vždy vhodné při tvorbě adresním plánu (plánů přidělení adres všem potřebným síťovým rozhraním - portům) provést na počátku bilanci spotřeby adres. Např. spotřeba vyjde 258 – zvolí se 2 x C než 1x B (rozdíl v blokaci adres je veliký – 2x256=512, 1x 65536). Nevýhodou je množení záznamů ve směrovacích tabulkách směrovačů. Toto může mít za následek jejich přetečení.

  - **Vytváření podsítí –** podsítě (subnetting) se provádí přemaskováním původní masky posunem hranice doprava. Počet bitů, o který se maska posouvá, je prostorem pro adresaci podsítí (posun o tři bity - 2^3= 8 podsítí). Nevýhodou je „neviditelnost“ podsítí z původní sítě – zvnějšku (před přemaskováním není žádná informace o podsítích).
    Podsítě se obecně používají.

- Použití po úpravách
    - **Vytváření supersítí (supernetting) či směrů a z toho vyplývající přidělování IP adres po blocích (CIDR).** Jedná se slučování jednotlivých sítí do směru a to přemaskováním posunutím hranice do leva. Počet bitů, o který se maska posouvá, určuje, kolik sítí může být v daném směru.

      Podmiňující úprava - zařízení musí umět slučovat sítě do směrů tj. agregovat do směrů vzhledem k portu. Výsledkem je agregace směrovacích tabulek směrovačů a podstatně efektivnější směrování.

      Díky vyváření směrů lze adresy přidělovat po blocích bez ohledu na třídy (třídy představují pouze „část bloků“ adres). Jedná se o podstatně šetrnější způsob přidělování adres hierarchicky uspořádaný. Tento způsob se nazývá **CIDR – Classless InterDomain Routing**.

Autority internetu a CIDR

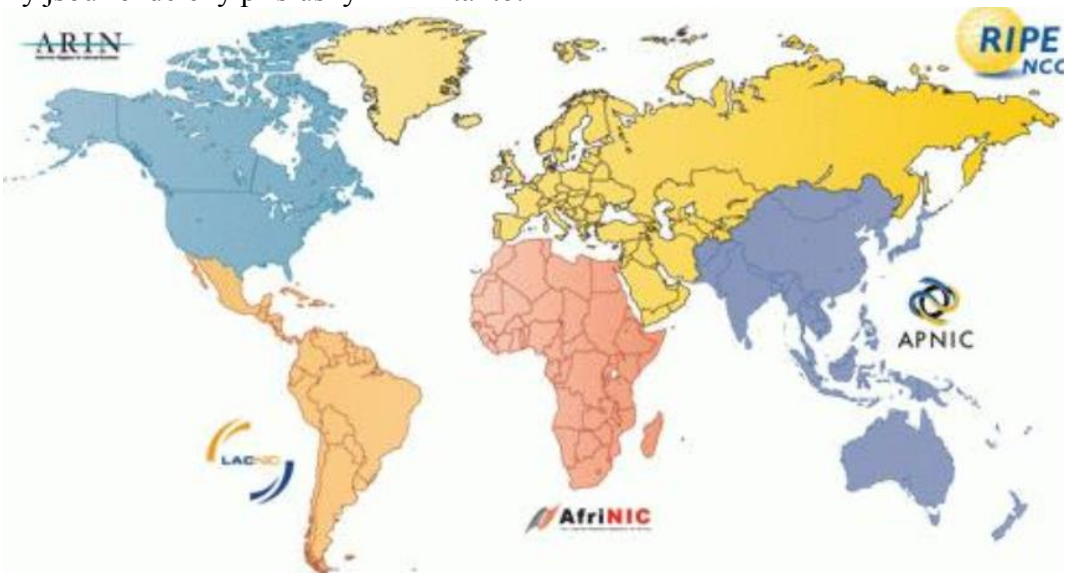
Přidělování IP adres (**veřejných – internetových**) je potřeba koordinovat. Ta je potřeba i při dalších činnostech. Proto je nutná struktura autorit internetu. Na jejich oficiálních webových stránkách najdete vždy validní informace.

ICANN (Internet Corporation for Assigned Names and Numbers)– je nejvyšší autorita odpovídající za provoz a rozvoj. Na konferencích se rozhoduje o směrech vývoje internetu. Jedná se o mezinárodní globální organizaci se snahou o co největší nezávislost. Oficiální stránky jsou http://www.icann.org/.

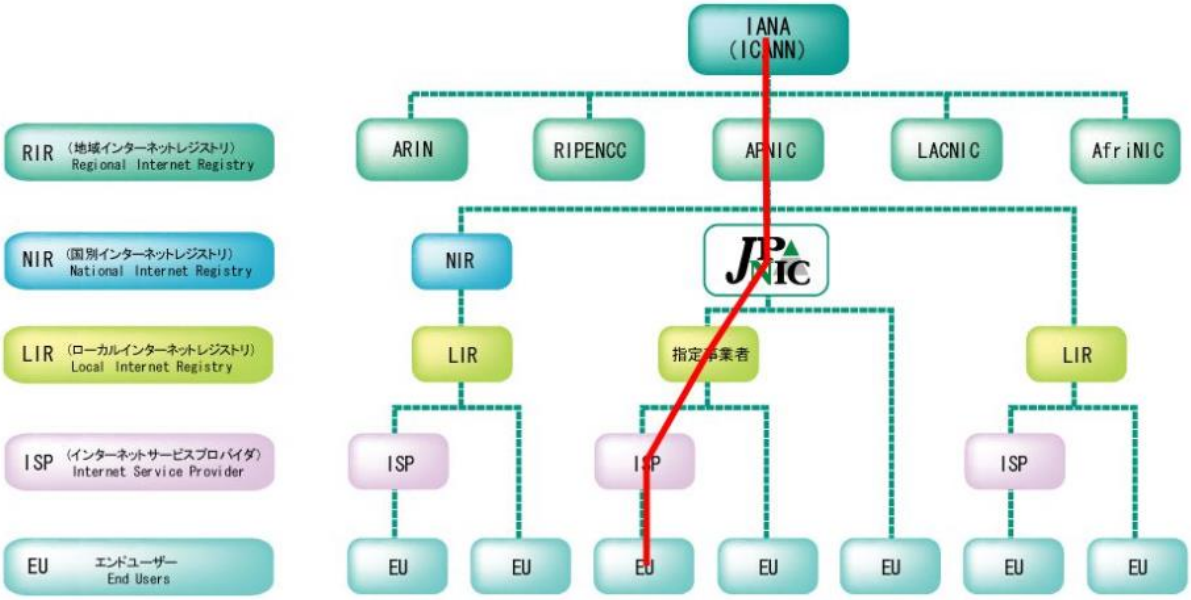
IANA (Internet Assigned Numbers Authority) – autorita zajišťující „provoz“ internetu. Podléhá ICANN. Činnost je rozdělena do tří oblastí – Adresace, jména (DNS) a „zařazení“ protokolů (Protocol Assignments). Oficiální stránky jsou http://www.iana.org/.

Přidělování adres po blocích probíhá pomocí **RIR (regionálních registrátorů**) až po ISP (internet service provider).

Regiony jsou rozděleny příslušným RIR takto:



Příklad struktury „přidělovatelů“ adres až po koncového uživatele (pro APNIC):



Pozn.: Bloky adres se kupují, cena je dle velikosti bloku. Ty jsou large (extra large, podobně dále), medium a small.

Pro Evropu je **RIR RIPE NCC** **(Réseaux IP Européens Network Coordination Centre).**

Oficiální stránky jsou http://www.ripe.net/

IETF(The Internet Engineering Task Force) – autorita odpovídající za dokumentaci „vývoje“, tj. podklady a standardizace. Výstupem jsou dokumenty RFC (Request for Comment) a STD (Standards). Na „RFC pages“ jsou k dispozici znění dokumentů. Oficiální stránky jsou http://www.ietf.org/.

Detailní popis – pokračování

- **Privátní sítě –** myšlenka možnosti opakování stejných adres v původně izolovaných sítích je realizována v prostředí internetu po nutných opatřeních. Prvním je určení prostoru privátních adres (vyhrazené privátní adresy), které nesmí být šířený mimo tento prostor. Vyhrazené privátní adresy jsou:

Třída	Adresa sítě	Počet sítí
A	**10.0.0.0**	**1**
B	**172.16.0.0-172.31.0.0**	**16**
C	**192.168.0.0-192.168.255.0**	**256**

Druhým opatřením je zajištění oddělení privátní a veřejné sítě (veřejná síť je prezentována internetem). Především je potřeba zajistit překlad adres privátní na veřejné. Vývojem dochází k oddělení různých prostorů adres (např. různých ISP nebo různých technologií) mezi kterými je potřeba zajistit překlady adres. **IPv4 síť je postupem času různými překlady adres přetížena.**

Překlady jsou realizovány na:

- **aplikační vrstvě – proxy** – pomocí proxy serveru. Nevýhodou je, že každá aplikace musí být nastavena pro použití proxy . Např. ve škole je proxy server na IP 10.0.0.44 :3128, potom jsou požadavky mimo intranet školy směrovány na proxy server (10.0.0.44) a ten komunikuje s veřejnou sítí a vyřizuje.

- **síťové vrstvě**

  - NAT (network adress translation) – kontinuální překlad adres, kdy více privátním adresám přiřazujeme více veřejných adres.

  - PAT (port adress translation) – překlad více privátních adres na jednu veřejnou. Je to případ NATu. Je to nejběžnější případ. Požadavku je přiřazen port pro jeho identifikaci vzhledem k jedné veřejné adrese.

Překlady zajišťuje aktivní prvek na rozhraní, tj. většinou směrovač. Privátní sítě se používají obecně. Oddělní sítí umožňuje realizovat v místě hranice bezpečnostní mechanismy. Funkci NAT mají firewally (FW).

Lokální multicast v IPv4 – třída D

V tabulce jsou uvedeny přidělené skupinové adresy:

IP multicast address range	Description	Routable
224.0.0.0 to 224.0.0.255	Local subnetwork[1]	No
224.0.1.0 to 224.0.1.255	Internetwork control	Yes
224.0.2.0 to 224.0.255.255	AD-HOC block 1[2]	Yes
224.3.0.0 to 224.4.255.255	AD-HOC block 2[3]	Yes
232.0.0.0 to 232.255.255.255	Source-specific multicast[1]	Yes
233.0.0.0 to 233.255.255.255	GLOP addressing[1]	Yes
233.252.0.0 to 233.255.255.255	AD-HOC block 3[4]	Yes
234.0.0.0 to 234.255.255.255	Unicast-prefix-based	Yes
239.0.0.0 to 239.255.255.255	Administratively scoped[1]	Yes

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 Addressing Architecture* určující jejich délku a podobu, typy adres a další koncepční prvky.

Typ adresace – unicast (unikátní), multicast (skupinové) a anycast (výběrové)

Zmizely broadcast adresy, protože jejich funkce přebírají adresy skupinové(multicast).

Výběrové (anycast) - výběrové adresy označují skupinu (například. službu – DNS apod.) , data se doručí od volného člena, který je nejblíže .

Adresa IPv6 je

- 16B (128bitů) dlouhá
- tvoří 8 skupin po 2B
- oddělovač je „:“
- zapisuje se hexadecimálně

Příkladem IPv6 adresy je
fedc:ba98:7654:3210:fedc:ba98:7654:3210

Způsoby zápisu

Zkrácený zápis
Častou hodnotou je nula, proto jsou dvě možnosti pro zkrácení zápisu.

- V každé čtveřici vynechat počáteční nuly. Místo „0000“ tedy lze psát jen „0“. Např.:

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

  můžete zkrátit na

  123**:0:0:0:**fedc:ba98:7654:3210

  nebo jen na

  123**::**fedc:ba98:7654:3210

Nespecifikovaná adresa je potom

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

Zkrácena na

::

Pozor: 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::

Kompatibilita s IPv4 adresami

Některé přechodové mechanismy potřebují vyjádřit IPv4-mapované adresy, které pocházejí ze světa IPv4.

IPv4-mapované adresy

První část je vyplněna „0“, na konci adresy je 16 bitů jedničkových a v posledních 32 bitech je zapsána IPv4 adresa.

Například adresu
147.230.49.73 mapujeme na ::ffff:93e6:3149 nebo ::ffff:147.230.49.73

Pozn.: poslední čtveřici bajtů **IPv4- mapované adresy** zapsat jako běžnou IPv4 adresu.

Síťová/uzlová část

Příslušnost k určité síti nebo podsíti se vyjadřuje prefixem. Délka prefixu 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 v 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 – část síťovou (stejně jako v IPv4). Nepoužívá se vyjádření pomocí síťové masky. Proto to není počet jedniček („1“ = síťová část), ale univerzálně počet bitů.

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

Prefix nemusí končit na hranici šestnáctkových číslic. Například prefix

2000::/3 tj . binárně první byte 001/x 0000

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

Používá se zápis, který současně oznamuje jak konkrétní adresu rozhraní, tak délku prefixu:

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

Vyhrazené adresy - 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 (obecná)**

::1/128 **smyčka (loopback) – lokální smyčka**

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**. Jsou to adresy, které navazují na veřejné IPv4 adresy. Z jejich prostoru je navíc **většina prefixů dosud nepřiřazena**, zatím se využívá pouze prefix

2000::/3

Ostatním i budoucí RFC 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.**

ff00::/8

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

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 existují **místní unikátní individuální lokální adresy s prefixem fc00::/7** jednoznačné v místní síti (**dříve site-local**).

Individuální adresy IPv6

Globální individuální adresy

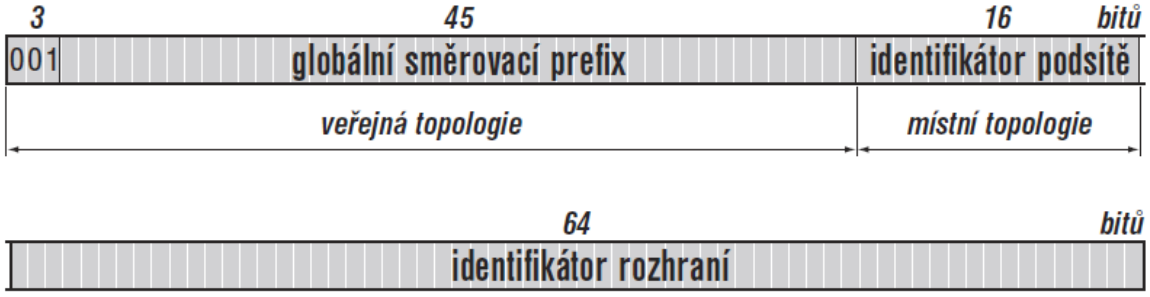
Tento typ adres je nejdůležitější. Globální znamená, že identifikují svého nositele v rámci celého Internetu a musí být celosvětově jednoznačné.

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. Jeho části v podobě delších prefixů se shodným začátkem pak přiděluje svým zákazníkům. **Cílem tohoto přístupu je agregace směrovacích údajů** (viz. IPv4).

Zjednodušený model odpovídá struktuře adresy pro IPv4. **Ta má tři části:**

- **adresu sítě** - globální směrovací prefix - 48 bitů (32 iana + 16 RIR/LIR)
- **podsítě** – 16 bitů
- **rozhraní v podsíti** – 64 bitů



Globální směrovací prefix identifikuje globální směrovací koncovou síť a je síti přidělen. Autoritou - lokálním internetovým registrem, zpravidla poskytovatelem Internetu - 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.

Identifikátor rozhraní umožňuje v jedné podsíti rozlišit miliardy adres. Motivací k takto velkorysému dimenzování podsítě byla snaha o maximální zjednodušení automatické konfigurace počítačů.
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.

Pozn.: 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. T**ato část adresy zůstává stejná, i když se počítač pohybuje**. 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 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.

Problémy s ochranou soukromí řeší RFC 4941: *Privacy Extensions for Stateless Address Autoconfiguration in IPv6 .*

Identifikátor rozhraní je náhodně generován a má životnost až několik dnů. Pevným bodem, aby se s takovýmto počítačem dalo vůbec navázat spojení je jeden pevný identifikátor rozhraní (podle EUI-64) a pod ním bude zaveden v DNS.

Identifikátory rozhraní je možné kryptograficky zabezpečit proti objevování sousedů. Vycházejí z veřejného klíče svého vlastníka a znemožňují nepřátelské stanici vydávat se za někoho jiného.

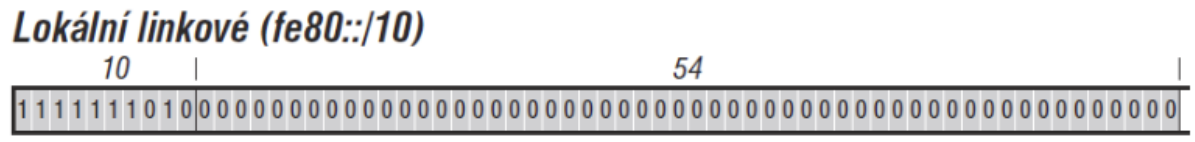
Lokální adresy

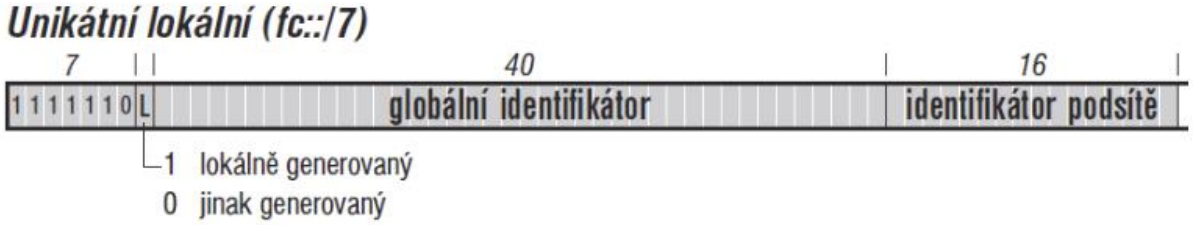
Tyto adresy zapadají do konceptu adres, které neplatí v celém Internetu, ale pouze v jeho malé části (privátní adresy).

IPv6 zavádí koncept dosahu adres. Ten je přínosný především pro skupinové adresy.Pro individuální adresy jsou možnosti dosahu omezené. Existuje několik typů adres s omezeným dosahem.

Dále řešíme první polovinu adres, protože druhá polovina ve všech případech obsahuje standardní identifikátor rozhraní.

Typy lokálních adres:





Linkové lokální – link local

Mají největší význam a v adresní architektuře mají svou vyhrazenou část – začínají prefixem

fe80::/10.

Následujících 54 bitů je nulových a za nimi je 64bitový identifikátor rozhraní

Např.: Počítač s ethernetovou adresou 00:8c:a0:c2:71:35 by tomuto rozhraní přidělil lokální linkovou adresu:

fe80::28c:a0ff:fec2:7135

Tuto adresu si vytvoří sám a pomocí nástrojů automatické konfigurace. Následovně ověří, že je pro danou linku skutečně jednoznačná.

První část lokální linkové adresy neslouží ke směrování, hodnota těchto bitů je pevně dána a je u všech stejná**.** 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.

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 (switchem) 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.

Pozn.: Dříve ještě existovala skupina adres - lokální místní –site local – fec0::/10. Tyto jsou **odmítnuté.** Jejich platnost byla omezena na jedno „místo“. Typickým místem je koncová síť organizace připojené k Internetu. Protože existují organizace připojené k Internetu v několika lokalitách, je definice místa nedostatečná a byly problémy s konfiguracemi směrovačů.

Unikátní lokální - ULA

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

fc::/7

Za prefix. částí následuje jednobitový příznak L, zda byl prefix adresy přiřazen lokálně (L=1) nebo jinak**.** 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. Identifikátor je generován z aktuálního času, adresy generující stanice a algoritmu SHA-1.

Čtyřicetibitová položka může nabývat více než bilionu různých hodnot. Je minimální pravděpodobnost, že dvojice sítí zvolí stejný globální identifikátor (zhruba 10^{-12}).

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.

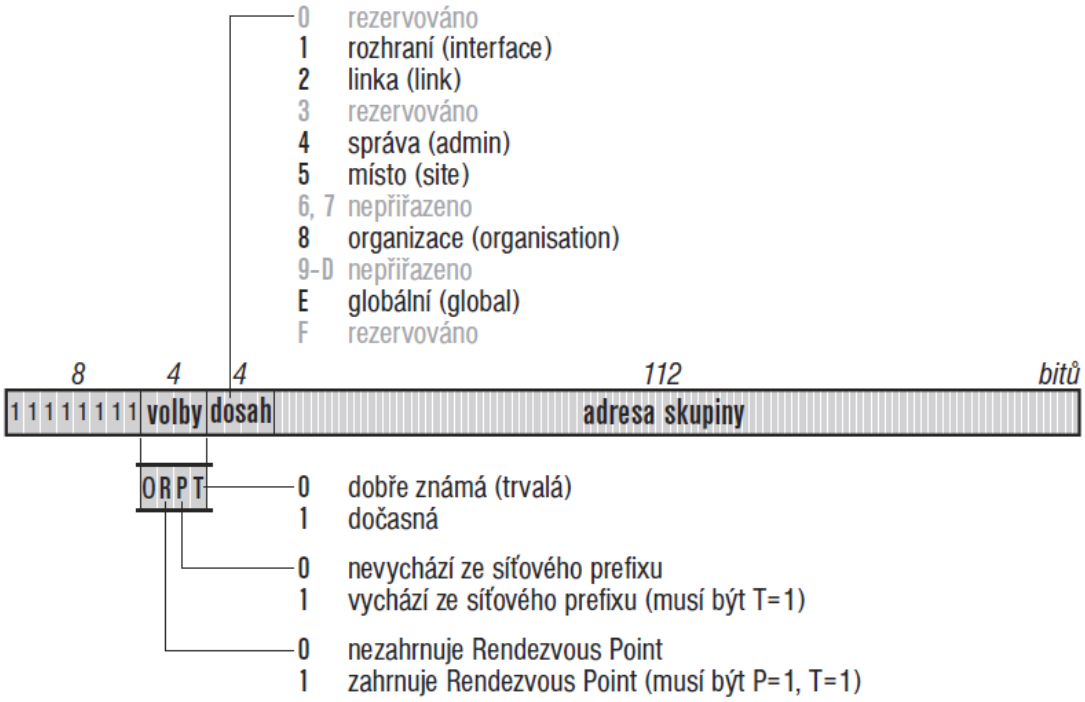
Globální jednoznačnost těchto adres je podstatná pro směrování.

Skupinové adresy – multicast IPv6

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). Skupinové adresy začínají prefixem

ff00::/8

Struktura adresy



Největší část adresy slouží k identifikaci skupiny, které mají být data dopravena. Dále jsou zde dvě krátké podpůrné položky volby- příznaky a dosah skupiny (4+4bity).

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

R (rendezvous point) – bod pro distribuční strom – směrování ano/ne
P (prefix) – vychází ze síťového prefixu ano/ne
T (transient) – indentifikátor skupiny trvale 0/dočasně 1

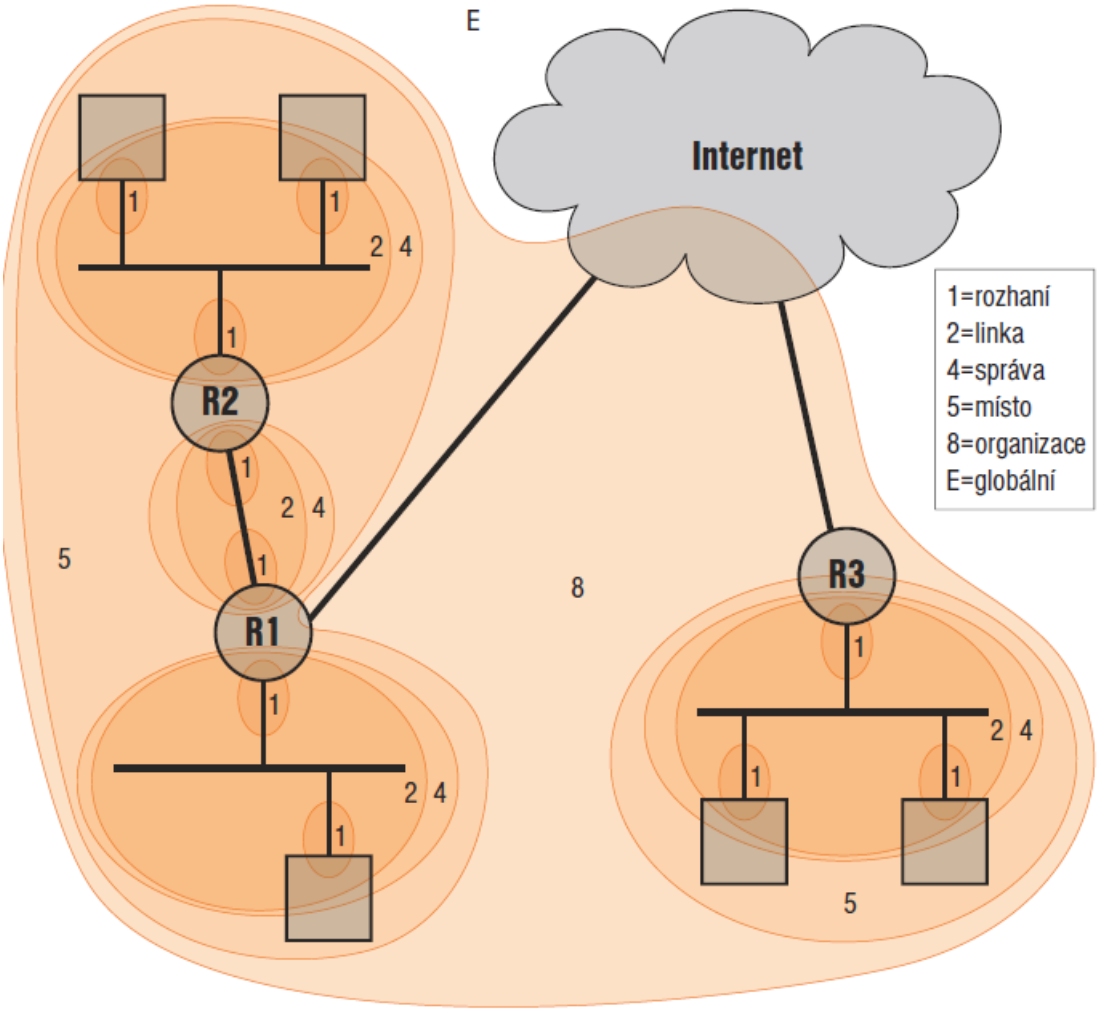
Trvalé tj. dobře známé adresy přiděluje IANA, zatímco dočasné si mohou generovat aplikace podle potřeby.

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

Dosah skupiny
Dosah skupiny sděluje, jak daleko od sebe mohou jednotliví členové být. Význam byl zatím přidělen deseti z nich (z 16 – 4 bity). ¨

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“.

Adresa skupiny - identifikátor

Pro identifikátor skupiny je k dispozici 112 bitů. Skupinové identifikátory jsou rozděleny do tří oblastí:

0–3fff:ffff skupiny přidělené IANA - např. ff0x::101 pro NTP servery

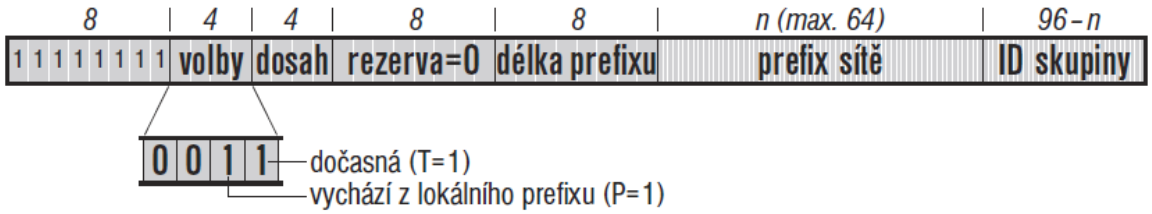
4000:0000–7fff:ffff identifikátory přidělené IANA- byl definován jediný, 4000:0000 proxy sítě

8000:0000–ffff:ffff dynamické, volně k použití – dle potřeby aplikace a služby

Skupinové adresy vycházející z individuálních adres (příznak P-1, T-1)

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 celosvětově jednoznačný prefix individuálních adres zdejší sítě.**

Jedná se o jeden možný formát pro identifikátor skupiny, který je uveden na obrázku). Délka prefixu je většinou 48 či 64 bitů.

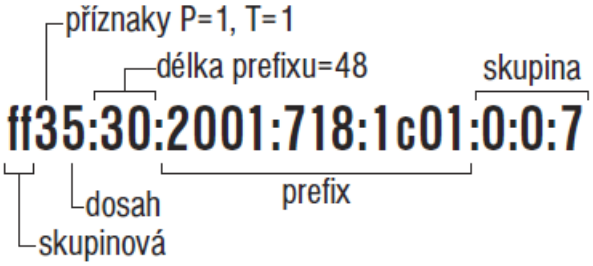


Je-li P=1, musí se jednat o dočasnou adresu a proto musí mít i příznak T hodnotu 1.

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

2001:718:1c01::/48.

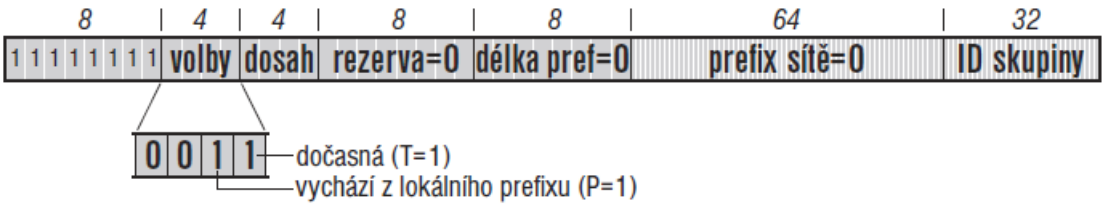
Z tohoto prefixu odvodíme skupinovou adresu s dosahem pro místo (dosah 5) se skupinovým identifikátorem 7.



Skupinové 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.

Délka prefixu i prefix sítě jsou nulové. Skupinové adresy pro SSM tedy mají prefix ff3*x*::/96, za nímž následuje 32b identifikátor skupiny.

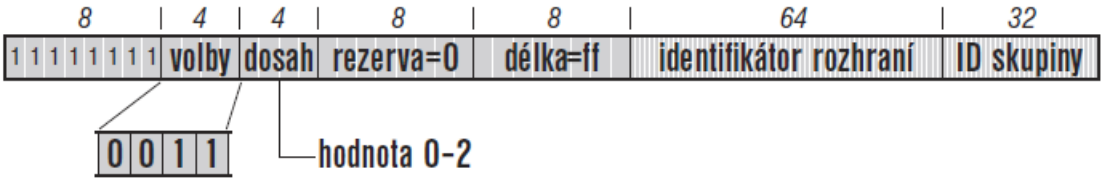


Jednoznačnosti zde není těžké dosáhnout, protože skupiny mají vždy jen jediného odesilatele. Stačí, aby on sám si udržel pořádek v jejich identifikátorech.

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

Skupinové adresy vycházející z rozhraní

Jejich dosah nesmí být větší než jediná linka. Každý stroj může generovat sám.



Výběrové adresy - anycast

Jejich prostřednictvím lze řešit zdvojování počítačů, směřující ke zvýšení výkonu či spolehlivosti. Mohou se využít k vyhledání nejbližšího stroje poskytujícího určitou službu. Současné nejzatíženější servery bývají ve skutečnosti realizovány skupinou spolupracujících počítačů.
Například nastavením DNS se dosáhne rozkládání dotazů na jednotlivé členy skupiny.

Příklad:
Kořenových DNS serverů by 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.

Výběrové adresy nabízejí řešení. Adres kořenových serverů je třináct a postupně přecházejí na výběrové. Za třinácti adresami se skrývá více než 150 serverů.

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

Výběrové lokální adresy v rámci jediné podsítě

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).

Povinné adresy uzlu

IPv6 rozhraní má více adres. Minimální množina adres, ke kterým se každý uzel IPv6 sítě musí hlásit, je níže:

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

Pro směrovač platí navíc následující:

- 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

Výběr adresy

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

Aplikace, která chce komunikovat, má někdy k dispozici jedinou cílovou IP adresu.

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 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. Obecně platí pravidlo „ od konkrétního k obecnému“.

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