IMPROVET

Komunikační sítě a internetový protokol verze 6

Lukáš Čepa, Pavel Bezpalec

Autoři: Lukáš Čepa, Pavel Bezpalec
Název díla: Komunikační sítě a internetový protokol verze 6
Vydalo: České vysoké učení technické v Praze
Zpracoval(a): Fakulta elektrotechnická
Kontaktní adresa: Technická 2, Praha 6
Tel.: +420 2 2435 2084
Tisk: (pouze elektronicky)
Počet stran: 74
Vydání: 1.

ISBN 978-80-01-05302-7

Recenzent: Jiří Stibor

Innovative Methodology for Promising VET Areas
http://improvet.cvut.cz

Program celoživotního učení

Tento projekt byl realizován za finanční podpory Evropské unie.
Za obsah publikací odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

Vysvětlivky

	Definice
	Zajímavost
	Poznámka
	Příklad
	Shrnutí
+	Výhody
–	Nevýhody

ANOTACE

Krátící se adresní prostor Internetového protokolu verze 4 (IPv4) byl důvodem pro vznik „IP nové generace“. Do roku 1996 bylo vydáno několik RFC dokumentů definujících Internetový protokol verze 6 (IPv6). I přes tenčící se adresní prostor je IPv4 protokol v roce 2012, díky postupným úpravám, stále hlavním Internetovým protokolem. Avšak s rostoucí popularitou služeb, které vyžadují přímou komunikaci (IP telefonie, videokonference a další) a se zamýšleným rozvojem bezdrátové sítě WiMAX, jako mobilní sítě 4G, která počítá s mobilitou IPv6, by se IPv6 mohla dočkat většího rozšíření. V současné době je IPv6 implementována především na páteřních spojích většiny poskytovatelů Internetu 1. a 2. úrovně.

CÍLE

Hlavním cílem tohoto modulu je seznámit studenta se základy protokolu IPv6. V první řadě modul popisuje datagram, zápis a tvar adres IPv6. Dále se zabývá protokolem ICMPv6, který se používá pro odesílání chybových a informačních zpráv, bez kterých by protokol IPv6 nemohl správně fungovat. A v poslední řadě se modul zabývá mechanismy, které protokol IPv6 používá ke své činnosti. Jsou to mechanismy Objevování sousedů, automatická konfigurace uzlů, DNS a mobilita.

LITERATURA

[1] SATRAPA, Pavel. *IPv6*: *internetový protokol verze 6* [online]. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011, 407 s. [cit. 2012-03-01]. CZ.NIC. ISBN 978-80-904248-4-5 (BROž.). Dostupné z: http://ii.iinfo.cz/r/kd/internetovy-protokol-ipv6-treti-vydani.pdf

[2] Deering, S. – Hinden, R. *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

[3] Conta, A. – Deering, S. – Gupta, M. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, RFC 4443, March 2006.

[4] Johnson, D. – Perkins, C. – Arkko, J. *Mobility Support in IPv6*, RFC 6275, July 2011.

Obsah

1 Vlastnosti IPv6

1.1 Vlastnosti IPv6

Hlavním důvodem vzniku **IPv6** (*Internet Protocol version 6*) jsou následující vlastnosti:

- Rozsáhlý adresní prostor, který byl stanoven na 128 bitů (čtyřnásobek IPv4). K dispozici je tedy $3{,}4 \times 10^{38}$ (2^{128}) adres.
- Více úrovní adresní hierarchie, což umožňuje efektivnější agregaci a sumarizaci cest.
- Jednotné adresní schéma pro Internet i vnitřní sítě.
- Tři typy adres:
  - individuální (*unicast*)
  - skupinové (*multicast*)
  - výběrové (*anycast*)
- Více adres na rozhraní.
- Automatická konfigurace uzlů.
- Optimalizace rychlosti směrování.
- Podpora pro služby se zajištěnou kvalitou **QoS** (*Quality of Service*).
- Zvýšení bezpečnosti (zahrnuto šifrování, autentizace a sledování cesty k odesílateli).
- Rozšířená podpora skupinového směrování (*multicast*).
- Podpora mobility (přenosné počítače, atd.).

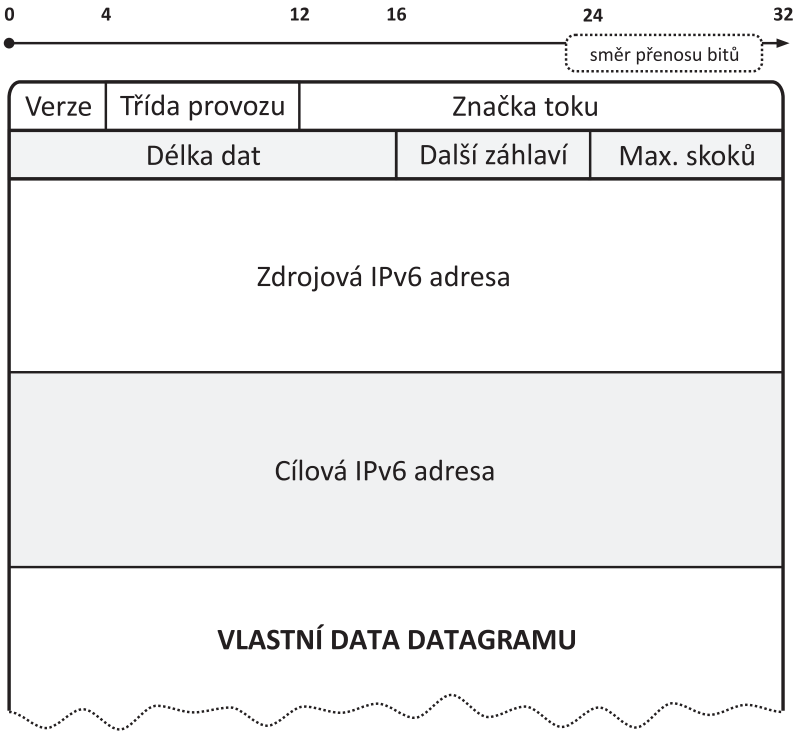
IPv6 je ve velkém rozsahu rozšířením **IPv4** (*Internet Protocol version 4*). Většina přenosových a aplikačních vrstev protokolů nevyžaduje žádné nebo jen malé změny pro funkčnost s IPv6. Výjimkou jsou části aplikací, které pracují se síťovými adresami. Největší změnu prodělal formát datagramu.

2 Formát datagramu

2.1 Datagram

Základním kamenem IPv6 je dokument RFC 2460, který především definuje formát datagramu. Datagram IPv6 se skládá ze základního záhlaví, rozšiřujících záhlaví a dat. Oproti IPv4 má datagram IPv6 konstantní velikost a nepovinné informace jsou přesunuty do samostatných rozšiřujících záhlaví. Tyto záhlaví se mohou, ale nemusí, umísťovat za základní záhlaví. Celková velikost základního záhlaví je dvojnásobně větší oproti záhlaví IPv4. Z 20 bajtů vzrostla na 40 bajtů. Z toho 32 bajtů zabírají adresy.

Z datagramu IPv6 byl odstraněn kontrolní součet. Jeho službu typicky vykonává nižší vrstva síťové architektury.



Základní záhlaví datagramu IPv6

Popis jednotlivých položek základního záhlaví datagramu IPv6:

- Verze (*Version*) – identifikuje verzi protokolu a obsahuje hodnotu 6. Má velikost 4 bity.
- Třída provozu (*Traffic class*) – vyjadřuje prioritu datagramu. Cílem této položky je poskytovat služby se zaručenou kvalitou QoS. Má velikost 8 bitů.

- Značka toku (*Flow label*) – označuje proud datagramů se společnými parametry. Prostřednictvím této značky směrovač pozná, že datagram je součástí určitého toku, což umožňuje zrychlení směrování. Má velikost 20 bitů.

- Délka dat (*Payload length*) – vyjadřuje údaj o délce datagramu v bajtech, do níž se nezapočítává délka základního záhlaví. Položka má velikost 16 bitů, což umožňuje maximální délku datagramu až 64 kB. Pro vytvoření delšího datagramu slouží rozšiřující záhlaví Jumbo obsah.

- Další záhlaví (*Next header*) – identifikuje rozšiřující záhlaví či druh nesených dat následující za základním záhlavím. Má velikost 8 bitů.

- Maximální počet skoků (*Hop limit*) – nahrazuje položku životnost datagramu (TTL) u IPv4. Pokaždé když datagram projde směrovačem, dojde ke snížení hodnoty této položky o jedna. V případě vynulování položky, bude datagram zahozen a k odesilateli se odešle ICMP zpráva o vypršení maximálního počtu skoků. Smyslem této položky je zabránit cyklickému směrování. Položka má velikost 8 bitů.

- Adresy - jsou poslední dvě položky. Jedná se o Zdrojovou adresu (*Source address*) a Cílovou adresu (*Destination address*). Každá položka má velikost 128 bitů.

2.2 Zřetězení záhlaví

Nepovinné a rozšiřující informace jsou přesunuty do samostatných rozšiřujících záhlaví. Tato záhlaví se mohou, ale nemusí, umísťovat za základní záhlaví. Každé rozšiřující záhlaví je samostatným blokem a k propojení jednotlivých záhlaví slouží položka Další záhlaví. Tato položka obsahuje kód, který reprezentuje typy jednotlivých rozšiřujících záhlaví nebo nesená data. Tímto způsobem lze zřetězit libovolný počet záhlaví.

Zřetězení záhlaví datagramu

Cílem je, aby zajímavé informace pro uzly (směrovače) byly umístěny bezprostředně za základním záhlavím a rozšiřující záhlaví, určené pro koncové uživatele, až za nimi. Při zřetězení více rozšiřujících záhlaví je důležité jejich pořadí, které je pevně stanoveno:

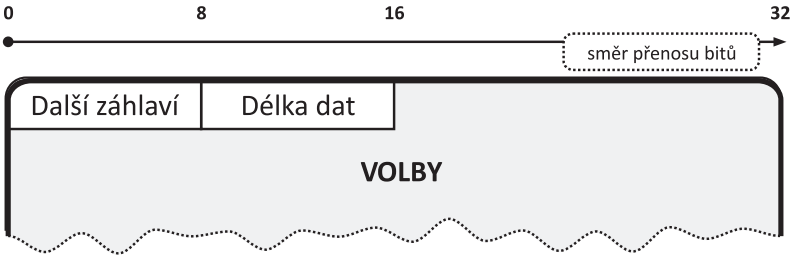
1. základní záhlaví IPv6
2. Volby pro všechny (*Hop-by-hop options*)
3. Volby pro cíl (*Destination options*) – pro první cílovou adresu
4. Směrování (R*outing*)
5. Fragmentace (*Fragment*)
6. Autentizace (*Authentication*)
7. Šifrování obsahu (*Encapsulating security payload*)
8. Volby pro cíl – pro konečného příjemce datagramu
9. Mobilita (*Mobility*)

Každé rozšiřujících záhlaví se v datagramu může objevit pouze jednou, kromě záhlaví Volby pro cíl.

2.3 Volby

Existují dvě záhlaví tohoto typu:

- Volby pro všechny uzly v cestě
- Volby pro cíl – toto záhlaví je zpracováno pouze cílovým uzlem, ostatní jej ignorují



Rozšiřující záhlaví Volby pro všechny a Volby pro cíl

Položka Délka dat udává délku záhlaví v osmicích bajtů, do které se nezapočítává prvních 8 bajtů. Pokud tedy Délka dat obsahuje hodnotu 1, tak délka záhlaví s volbami je 16 bajtů.

Dále následují vlastní volby, z nichž následující jsou společné pro obě záhlaví:

- Pad1 – slouží k vynechání jednoho bajtu, což umožňuje lepší zarovnání ostatních prvků s ohledem na čtyřbajtová slova.
- PadN – plní obdobnou funkci jako předcházející volba, ale slouží k vynechání dvou a více bajtů.

Mezi volby pro všechny uzly v cestě dále patří:

- Upozornění směrovače (*Router alert*) – tato volba upozorňuje všechny směrovače v cestě, že paket nese zajímavá data. Je definovaná v RFC 2711 a nachází uplatnění především v rezervačním protokolu **RSVP** (*Resource Reservation Protocol*), který posílá řídící pakety pro alokaci kapacit po cestě. Právě tyto pakety jsou určeny všem směrovačům.
- Rychlý start (*Quickstart*) – má za cíl zvýšit propustnost transportních protokolů, především protokolu TCP. Stroj, který zahajuje komunikaci, přidá do žádosti o navázání TCP spojení tuto volbu, ve které oznamuje požadovanou přenosovou rychlost. Pokud by se nějakému směrovači tato přenosová rychlost nelíbila, sníží její hodnotu na akceptovatelnou úroveň. V okamžiku, kdy datagram dorazí k cíli, obsahuje volba Rychlý start akceptovatelnou přenosovou rychlost pro všechny směrovače mezi odesilatelem a příjemcem. Tato rychlost se během komunikace může aktualizovat.

- Jumbo obsah (*Jumbo payload*) – umožňuje vytvářet datagramy (jumbogramy) o délce 65 535 až 4 294 967 295 bajtů. Použití jumbogramů má význam pouze v případě, že to umožňuje přenosová technologie dané linky.

K volbám pro cíl dále patří následující volba:

- Domácí adresa (*Home address*) – tato volba byla zavedena v souvislosti s podporou mobility a používá se v okamžiku, kdy se mobilní uzel nachází mimo domácí síť. Informuje cílový uzel o domácí adrese odesilatele.

V současné době se praktického využití dostalo pouze volbám Upozornění směrovače, Jumbo obsah a Domácí adresa.

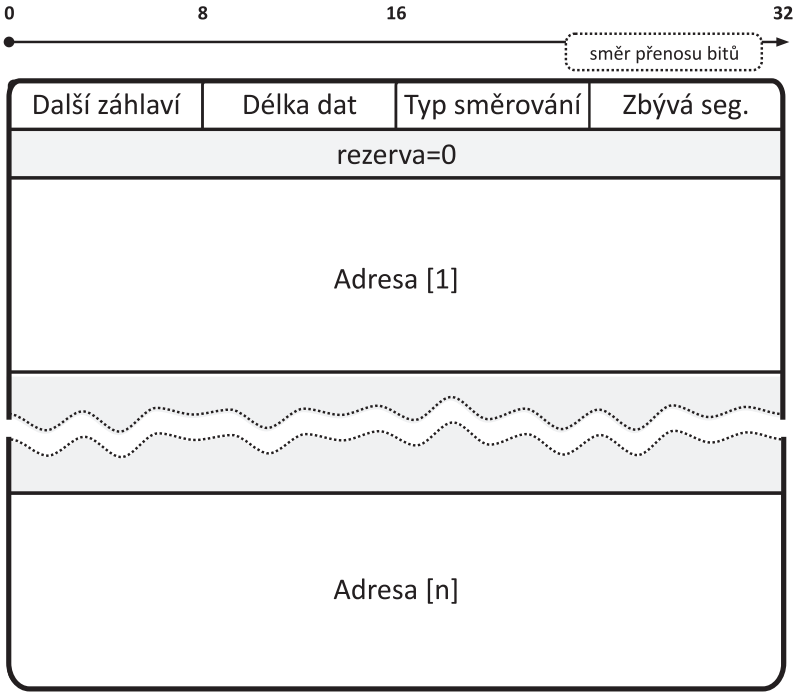
2.4 Směrování

Datagram je stále směrován v závislosti na nejdelší shodě cílové adresy se záznamem ve směrovací tabulce. Rozšiřující záhlaví Směrování umožňuje do tohoto procesu vstoupit a určit přes, které uzly má být daný datagram směrován.

V současné době IPv6 poskytuje dva typy směrování, pro jejichž rozlišení slouží položka Typ směrování.

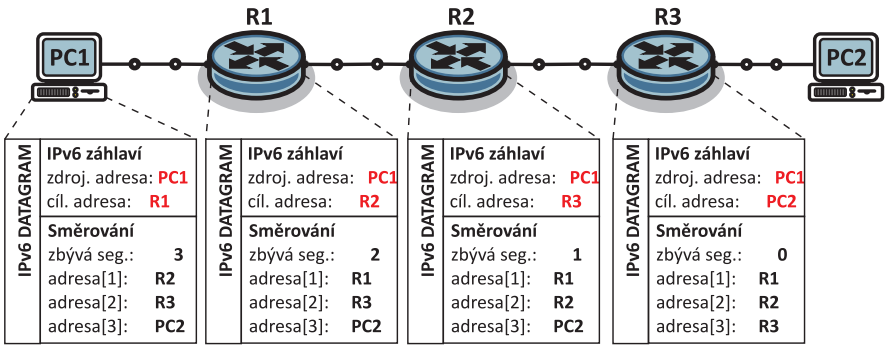
Směrování typu 0

Tento typ směrování umožňuje datagramu předepsat uzly, kterými musí v daném pořadí projít a zároveň slouží jako záznam, kterými z nich již prošel.



Formát rozšiřujícího záhlaví Směrování typu 0

Rozšiřující záhlaví v tomto případě obsahuje seznam všech uzlů, kterými má datagram projít. Odesilatel před odesláním datagramu vezme první adresu ze seznamu a umístí ji do základního záhlaví jako adresu cílovou, a adresu cílového klienta umístí na konec tohoto seznamu. Jakmile datagram dorazí na cílovou adresu, tedy směrovač po cestě, dojde ke snížení položky Zbývá segmentů o hodnotu 1. Tato položka ukazuje od konce seznamu na další adresu uzlu v pořadí. Směrovač tuto adresu umístí do cílové adresy základního záhlaví a datagram odešle. Tento proces se opakuje na každém směrovači, který je uveden v seznamu, dokud datagram nedorazí do svého cíle určení. Tuto skutečnost signalizuje hodnota 0 v položce Zbývá segmentů.



Princip směrování a změny adres v záhlaví datagramu

\+ Jednou z výhod je možnost určit přesnou cestu datagramu a tím ověřit funkčnost tohoto spojení. Tedy směrování typu 0 bylo zavedeno pro testování dosažitelnosti mezi libovolnými adresami.

\− Hlavní nevýhodou tohoto směrování je možnost zahlcení přenosových tras. V datagramu lze zřetězit libovolný počet rozšiřujících záhlaví Směrování a tím zajistit, že se daný datagram bude v síti pohybovat velmi dlouho. Tato skutečnost může vést k vytvoření datových toků s obrovským objemem. Další nevýhodou je možnost průchodu přes **NAT** (*Network Address Translation*), kde se neveřejná adresa uvede jako koncový cíl a veřejná adresa směrovače, provádějící překlad adres, jako mezilehlá. Obdobným způsobem lze proniknout i přes firewall.

Problém se zahlcením tras nakonec vedl k zákazu používání Směrování typu 0 a k definování RFC 5095, které popisuje způsoby, jak zacházet s takto směrovanými datagramy.

Směrování typu 2

Tento typ směrování byl speciálně definován pro mobilitu a používá stejný mechanismus jako typ 0. Typ 2 však omezuje počet zřetězení směrovacích záhlaví pouze na jedinou adresu a tím omezuje její zneužití.

2.5 Fragmentace

Fragmentace je proces, při kterém dochází k rozdělení příliš velkého datagramu na několik menších tak, aby jeho velikost vyhovovala parametru **MTU** (*Maximum Transmission Unit*). MTU udává maximální velikost datagramu, kterou je daná linka[1)] schopna přenést. Minimální hodnota MTU je v případě IPv6 1280 bajtů. Tato velikost je zvolena s ohledem na minimalizaci fragmentace.

Pojem linka zde představuje propojení uzlů v rámci 2. vrstvy referenčního modelu ISO/OSI (např. Ethernet).

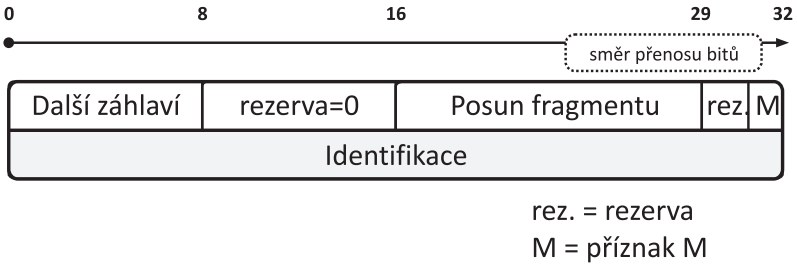
Každá přenosová cesta se skládá z průchozích uzlů a linek, kde každá linka může mít různou velikost MTU. Výsledná hodnota MTU přenosové cesty se nazývá **PMTU** (*Path MTU*) a je potom daná linkou s nejnižší hodnotou MTU.

Fragmentace je náročný proces, který zbytečně zatěžuje průchozí uzly. Tento fakt je v případě protokolu IPv6 zohledněn. Proto IPv6 povoluje fragmentaci pouze a výhradně na straně odesilatele. To znamená, že pokud je kdekoli na cestě linka s menší MTU, dojde k zahození datagramu a uzel, který tento datagram zahodí, informuje odesilatele o této skutečnosti ICMP zprávou Příliš velký paket.

Postup fragmentace

Vzhledem k fragmentaci se datagram dělí na dvě části:

- Nefragmentovatelná část – tuto část tvoří základní a všechny rozšiřující záhlaví IPv6, které se mají zpracovávat po cestě k cílovému uzlu, včetně záhlaví směrování.
- Fragmentovatelná část – tuto část tvoří zbytek datagramu. To jsou všechny ostatní rozšiřující záhlaví, které mají být zpracovány až v cílovém uzlu, včetně dat a záhlaví protokolů vyšších vrstev.

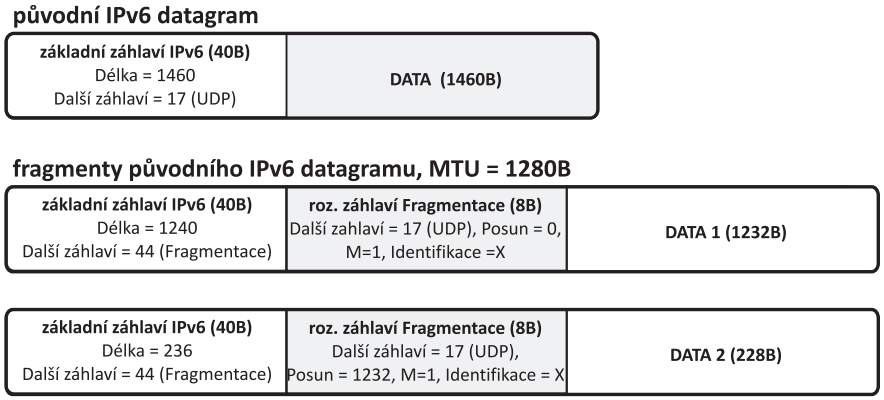


Formát záhlaví Fragmentace

Fragmentace se týká pouze fragmentovatelné části. Ta se rozdělí na části o velikosti násobku osmi bajtů tak, aby byly tyto části zároveň menší, než požadované MTU. Tímto způsobem vzniknou fragmenty, jejichž záhlaví je sestaveno následně:

- Nefragmentovatelná část se převezme a upraví se velikost dat v položce Délka dat v základním záhlaví tak, aby odpovídala velikosti fragmentu. V posledním zřetězeném záhlaví se do položky Další záhlaví zapíše hodnota 44, která odpovídá rozšiřujícímu záhlaví Fragmentace.
- Přidá se rozšiřující záhlaví Fragmentace, které se vyplní následně:
  - Vygeneruje se hodnota identifikátoru a přidělí se všem fragmentům.
  - Převezme se hodnota položky Další záhlaví z nefragmentovatelné části původního datagramu.
  - Posun každého fragmentu se určí jako počet osmic bajtů, kde první fragment má nulový posun. Ostatní fragmenty mají posun roven celistvému násobku délky fragmentu, která je pro všechny stejná, kromě posledního fragmentu.
  - V poslední fragmentu se položka M nastaví na nulu, v ostatních fragmentech bude mít hodnotu jedna. Položka M reprezentuje příznak posledního fragmentu.
- V posledním kroku fragmentace dojde k připojení fragmentu.

Takto vzniklé fragmenty můžeme považovat za samostatné datagramy, které jsou odeslány příjemci. Na straně příjemce se z údajů v záhlaví fragmentace poskládá původní datagram.



Postup fragmentace

2.6 Velikost datagramu

IPv6 je navržena tak, aby minimalizovala proces fragmentace. To úzce souvisí s velikostí odesílaných datagramů. Každý datagram by měl být v ideálním případě co největší, aby nedocházelo k přetížení sítě v důsledku odesílání velkého počtu menších datagramů. Zároveň však velikost datagramu nesmí překročit MTU přenosové cesty. K nalezení ideální velikosti datagramu používá IPv6 algoritmus Objevování MTU cesty. Tento algoritmus je popsán v RFC 1981.

Objevování MTU cesty

Algoritmus při hledání ideální velikosti datagramu postupuje následně:

- Odesilatel pošle datagram o velikosti MTU odchozí linky (celkové MTU cesty nemůže být větší).
- Pokud datagram doputuje do místa určení, byla nalezena MTU cesty.
- Pokud po cestě datagram narazí na linku s menší MTU, uzel na začátku této linky jej zahodí a prostřednictvím ICMP zprávy informuje odesilatele o této skutečnosti. Tato zpráva obsahuje aktuální velikost MTU linky.
- Odesilatel zmenší svoji MTU na základě ICMP zprávy a odešle jej znovu.
- Vše opakuje, dokud nedorazí datagram do místa určení.

V případě, že dojde ke zvýšení MTU cesty, je vhodné tento proces v určitých intervalech opakovat. Doporučená hodnota intervalu je 10 minut.

2.7 Ostatní rozšiřující záhlaví

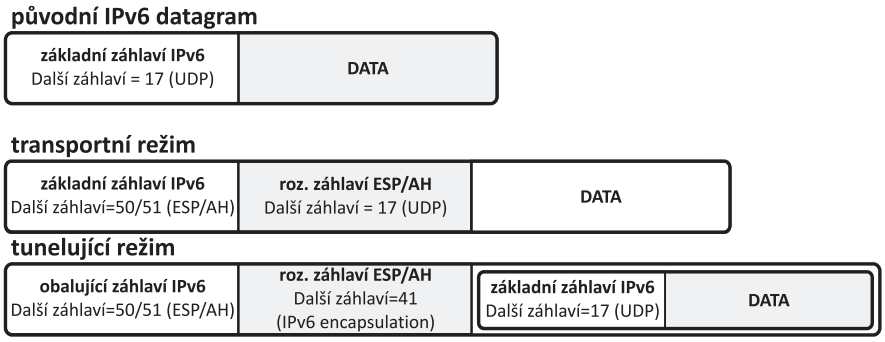
Autentizace a šifrování dat

Pro autentizaci a šifrování dat se vžilo označení **IPsec** (*IP security*). Tato problematika je rozsáhla a zaslouží si vlastní modul, proto se zde pouze zmíním o rozšiřujících záhlavích a jejich režimech vkládání do datagramu.

Jedná se o rozšiřující záhlaví **AH** (*Authentication Header*) a **ESP** (*Encapsulating Security Payload*). První záhlaví se stará o autentizaci (ověření pravosti adres a obsahu) a druhé umožňuje i šifrování obsahu přenášených dat. Datagram může být opatřen jedním či oběma záhlavími zároveň. Implementace IPsec je u IPv6 povinná, na rozdíl od IPv4.

Rozšiřující záhlaví lze vkládat ve dvou režimech:

- Transportní režim – záhlaví jsou vkládána přímo jako součást datagramu.
- Tunelující režim – celý stávající datagram je zapouzdřen jako data do nového datagramu.



Režimy IPsec

Poslední záhlaví

Rozšiřující záhlaví Poslední záhlaví (*No next header*) značí fakt, že datagram nenese žádná data a veškeré informace jsou umístěny v záhlavích. Poslední záhlaví používá hlavně protokol ICMP, který pro svoje účely využívá především rozšiřující záhlaví.

3 Adresy IPv6

3.1 Adresy IPv6

Hlavním důvodem vzniku protokolu IPv6 je jeho enormně velký adresní prostor. Tvůrci se při vývoji řídili heslem „aby nám už nikdy nedošly“ a proto zvolili délku adres 128 bitů. Základní formát adres IPv6 je definován v RFC 4291. Tento dokument definuje délku, tvar a jednotlivé typy adres. Podrobnější specifikace jednotlivých typů adres jsou definovány v samostatných RFC dokumentech. RFC 4291 zavádí následující druhy adres:

- Individuální (*unicast*) – tato adresa identifikuje jedno síťové rozhraní.
- Skupinové (*multicast*) – slouží k adresaci skupiny počítačů či jiných zařízení. Pokud jsou data odeslána na tuto adresu, musí být doručena všem zařízením ve skupině (např. IPTV).
- Výběrové (*anycast*) – jedná se o novinku oproti IPv4. Označují skupinu síťových zařízení, avšak data se doručí pouze jedinému zařízení, a to tomu, které je nejblíže.

Oproti IPv4, se u IPv6 nevyskytují oznamovací (*broadcast*) adresy. Ty jsou nahrazeny skupinovou adresou pro všechny uzly na lince.

Adresa IPv6 je přidělována síťovému rozhraním, nikoli uzlu, a každé rozhraní může mít přiděleno více libovolných adres. IPv6 dokonce přikazuje několik povinných adres pro každý uzel.

Tvar a zápis adres

Adresa IPv6 má délku 128 bitů a skládá se z osmi 16-ti bitových skupin. Každá skupina je vyjádřena čtyřmi číslicemi šestnáctkové soustavy a jednotlivé skupiny jsou vzájemně odděleny dvojtečkou. Příkladem IPv6 adresy je

2001:0718:0000:0000:28F6:19FF:FE00:1984

Důležitou vlastností adres IPv6 je možnost jejich zkrácení:

- Místo 0000 lze psát jednu 0.
- V každé skupině se mohou vynechat počáteční nuly.
- Několik nulových skupin za sebou lze nahradit zápisem „::“ (dvě dvojtečky).
- Koncové nuly ve čtveřicích vynechat nelze.
- Konstrukci „::“ lze v každé adrese použít jen jednou, jinak by nebylo možné jednoznačně určit její původní podobu.

Aplikováním uvedených pravidel lze adresu uvedenou výše zapsat třeba jako

2001:718::28F6:19FF:FE00:1984

Prefixy

Prefixy vyjadřují příslušnost k určité síti nebo podsíti a využívají toho faktu, že všechna rozhraní v rámci jedné sítě mají stejný prefix (začátek adresy). Tento přístup se používá již u protokolu IPv4 a je znám pod názvem **CIDR** (*Classless Inter-Domain Routing*). Z něj je také převzat způsob zápisu prefixu:

IPv6_adresa/délka prefixu

Délka prefixu určuje, kolik bitů od začátku adresy je považováno za prefix. Příkladem 64 bitového prefixu je

2001:718::/64

3.2 Rozdělení adres

Obrovský adresní prostor IPv6 byl rozdělen do několika skupin (typů adres) a každá skupina sdružuje adresy se společnou charakteristikou. Adresy lze k jednotlivým typům přiřadit na základě prefixu. Základní rozdělení adres je v následující tabulce.

Základní rozdělení adres

prefix	význam
::/128	nedefinovaná adresa
::1/128	lokální smyčka (loopback)
FC00::/7	unikátní lokální adresy
FE80::/10	lokální linkové adresy
FF00::/8	skupinové adresy
ostatní	globální individuální adresy

Drtivou většinu z adresního prostoru zabírají globální (celosvětově jednoznačné) individuální adresy, které jsou v současné době přidělovány pouze z prefixu 2000::/3. Ostatní prefixy jsou rezervovány pro budoucí využití.

Z výše uvedené tabulky lze vidět, že výběrové adresy nemají přiřazené žádné speciální rozmezí. Jsou přidělovány ze stejného adresního prostoru, jako adresy individuální.

Několika menším oblastem adresního prostoru byl přidělen speciální význam. Celý prefix ::/8, který je vyhrazen pro tyto oblasti, je deklarován jako nepřiřazený. Některé adresy v jeho rámci však přiřazeny byly. Jedná se především o individuální adresy ::0 a ::1. První se používá v případě, kdy rozhraní nemá přidělenu adresu IPv6. Jedná se o tzv. nedefinovanou adresu. Adresa ::1 se používá jako adresa lokální smyčky (*loopback*). Tato adresa má stejný význam jako IPv4 adresa 127.0.0.1.

Další skupina adres IPv6 identifikuje adresy s omezeným dosahem:

- Lokální linkové adresy (*Link-Local Unicast*) – tyto adresy slouží pro komunikaci v rámci jedné linky a začínají prefixem FE80::/10. Jedná se povinné adresy pro každé rozhraní.
- Místní individuální lokální adresy (*Site-Local Unicast*) – tyto adresy byly původně určeny pro komunikaci v rámci lokální sítě (LAN) a začínaly prefixem FEC0::/10. V současné době se nepoužívají.
- Unikátní individuální lokální adresy (Unique-Local Unicast) – tyto adresy nahradily místní individuální lokální adresy. Začínají prefixem FC00::/7 a mají stejný význam jako privátní adresy IPv4.

3.3 Dosah adres

Další novinkou IPv6 je koncepce dosahu adres. Tato koncepce vymezuje topologii sítě, v níž je adresa jednoznačná a ve své podstatě nahrazuje životnost datagramu (TTL). Dosah adres je definován v RFC 4007.

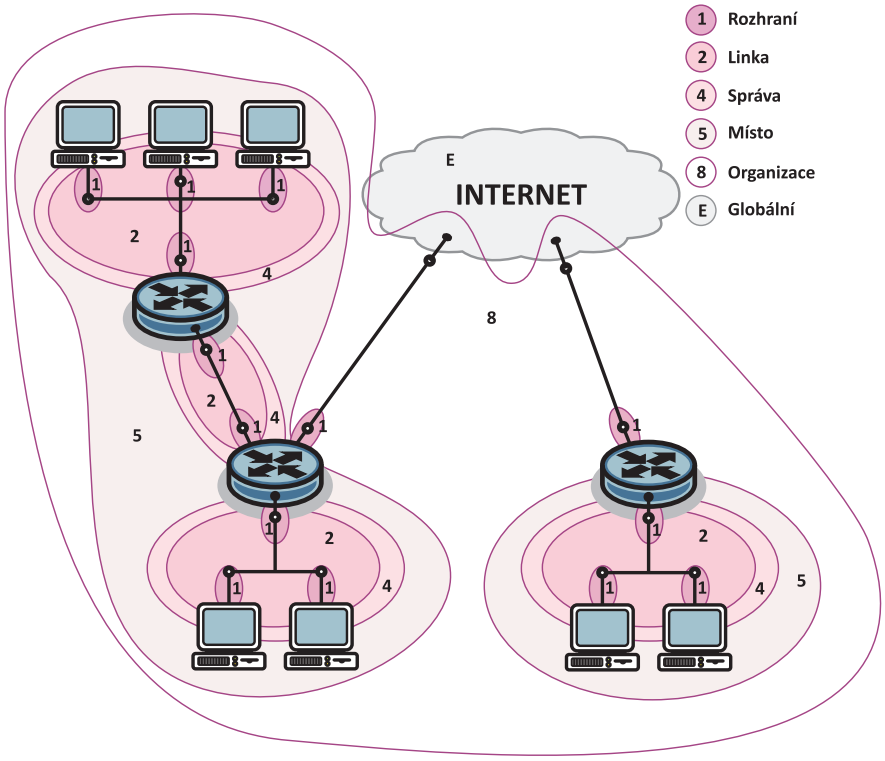
Dostupné dosahy se liší podle druhu adresy. Nejjemnější členění dosahu mají skupinové adresy, pro které jsou definovány následující stupně:

- Rozhraní (1) – používá se pro skupinové vysílání pro lokální smyčku.
- Linka (2) – dosah je omezen na jednu fyzickou síť (např. Ethernet).
- Správa (4) – nejmenší dosah, který musí být konfigurovaný správcem; obvykle se jedná o podsíť.
- Místo (5) – část sítě, která patří jedné organizaci a nachází se v jedné geografické lokalitě (např. zákaznická síť).
- Organizace (8) – pokrývá několik míst jedné organizace.
- Globální (E) – celosvětový dosah.

Pro individuální a výběrové adresy jsou zavedeny pouze dva stupně:

- Lokální pro linku
- Globální

Se zavedením dosahu adres také úzce souvisí pojem Zóna. Jedná se o část sítě, která odpovídá danému rozsahu a v této síti (zóně) je adresa jednoznačná. Hranice zón prochází síťovými zařízeními, nikoliv linkami, a platí, že celá zóna je vždy zahrnuta do nadřízené zóny většího rozsahu. Zóny stejného rozsahu se nesmí překrývat a jsou buď totožné, nebo vzájemně oddělené. Z hlediska směrování musí být zóna souvislá, jinak by datagram mohl během přenosu opustit danou zónu a mohlo by dojít k dezinterpretaci jeho adresy.



Příklad zón (dosahů)

Jednotlivé zóny je nutné rozlišovat i v rámci počítače. K tomu byl zaveden tzv. Identifikátor zón. Ten se skládá z dosahu zóny, která se odvozuje z vlastní adresy, jejíž zápis má tvar *adresa%zóna*, a pořadového čísla. Jednotlivé identifikátory jsou přidělovány každému počítači interně a v rámci jedné zóny nejsou vzájemně synchronizovány se sousedy. Typicky se používají pro identifikaci zón ve směrovacích tabulkách v rámci jednoho počítače.

Příkladem zápisu může být FF02::1%1. Jedná se o skupinovou adresu pro všechny uzly na lince.

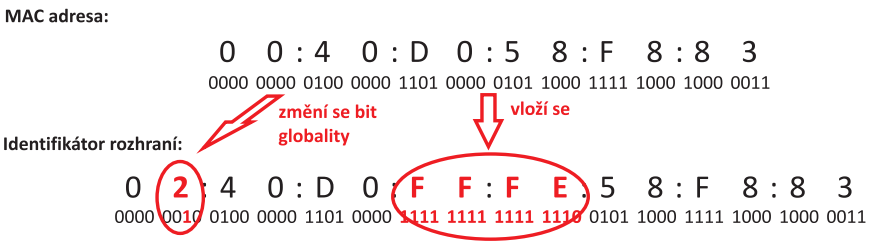
RFC 4007 počítá i s konceptem implicitní zóny (hodnota 0), která se dosadí, pokud adresa neobsahuje identifikátor zóny. Příkladem mohou být globální individuální adresy, pro které existuje pouze jediná zóna. Ta však se explicitně neuvádí.

3.4 Identifikátor rozhraní

Ještě než si probereme jednotlivé adresy, je třeba si vysvětlit způsob generování identifikátoru rozhraní.

Každé síťové rozhraní si generuje vlastní identifikátor podle standardu IEEE EUI-64, který se následně převezme do adresy IPv6 s menší modifikací. Dojde k invertování předposledního bitu v nejvyšším bajtu identifikátoru, který slouží jako příznak globality. Tato změna je z důvodu usnadnění vytváření identifikátoru rozhraní. Jako příklad nám může sloužit sériová linka, která by měla v případě použití původního EUI-64 tvar identifikátoru 200:0:0:1. Modifikací docílíme zjednodušení na 1.

V případě Ethernetu nebo bezdrátových sítí, se identifikátor rozhraní generuje z celosvětově jednoznačné adresy **MAC** (*Media Access Control*). Postup vzniku je jednoduchý. Mezi třetí a čtvrtý bajt MAC adresy se vloží 16 bitů s hodnotou FFFE a dojde k obrácení příznaku globality podle modifikované EUI-64. Takže z MAC adresy 00:40:d0:58:f8:83 vznikne následující identifikátor rozhraní 0240:d0ff:fe58:f883.



Vytvoření identifikátoru rozhraní z MAC adresy

Generováním identifikátoru rozhraní podle modifikované EUI-64 vzniká jednoznačná identifikace rozhraní a tedy i uživatelova počítače. Tato jednoznačná identifikace počítače může být z důvodu bezpečnosti komunikace nežádoucí. Proto byly definovány nové mechanismy, které jsou založeny na náhodném generování identifikátoru rozhraní. Nové mechanismy jsou popsány v RFC 4941.

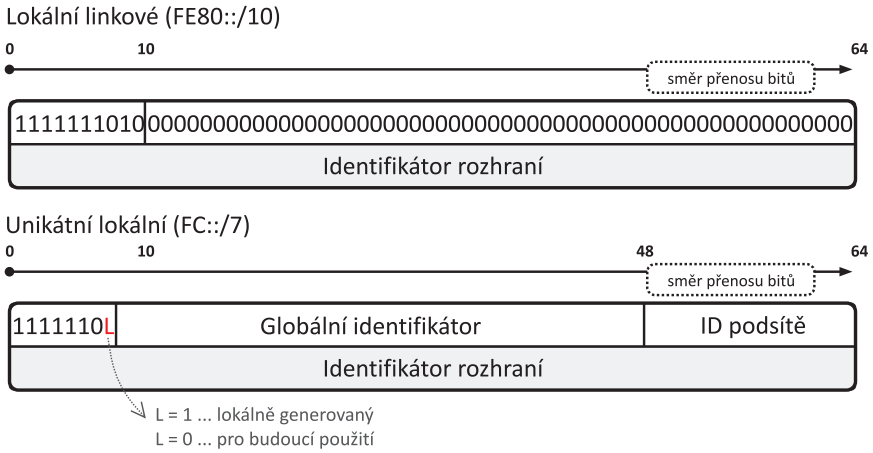
RFC 4941 navrhuje, aby daný počítač měl jeden pevný identifikátor rozhraní, který bude zanesen v **DNS** (*Domain Name Server*) serveru. Tento identifikátor bude sloužit pro komunikaci navazovanou zvenčí. Dále si bude počítač generovat náhodné identifikátory, které bude používat pro komunikaci s ostatními počítači. Tyto identifikátory nebudou zavedeny v DNS. Životnost náhodného identifikátoru může být několik hodin či dnů.

Operační systémy založené na linuxovém jádře primárně používají pro generování identifikátoru rozhraní EUI-64. Avšak generování náhodných adres lze zapnout parametrem jádra. V případě operační systémů firmy Microsoft je to rozdílné. Windows XP generuje identifikátory rozhraní pouze podle EUI-64, kdežto Windows 7 primárně generuje identifikátor rozhraní podle RFC 4941. Náhodné generování identifikátorů rozhraní lze u Windows 7 vypnout pomocí příkazů přes příkazový řádek.

3.5 Lokální adresy

Lokální adresy jsou obdobou privátních neveřejných adres IPv4 a používají se v rámci lokální linky. Tyto adresy nejsou v globálním Internetu směrovány a nejsou žádným způsobem centrálně registrovány či koordinovány. V současné době se používají v kombinaci s NATem. Mezi lokální adresy patří:

- Lokální linkové (FE80::/10)
- Unikátní lokální (FC::/7)



Lokální adresy

Lokální linkové adresy

Největší význam mají lokální linkové adresy, které si každý počítač dokáže vygenerovat sám a pomocí mechanismů automatické konfigurace si ověřit, zda jsou v rámci lokální linky jednoznačné. Díky tomu jsou lokální linkové adresy vždy k dispozici. Tuto skutečnost využívají i některé interní mechanismy. Například automatická konfigurace pomocí DHCP. Lokální linkové adresy jsou definovány v RFC 1918.

Příklad lokální linkové adresy

Unikátní lokální adresy

Unikátní lokální adresy se používají v případech, kdy existuje více koncových sítí (podsítí), které správce považuje za jednu koncovou síť, ve které chce kromě veřejných adres používat i lokální adresy. Tyto podsítě bývají zpravidla propojeny páteřními sítěmi a unikátní lokální adresy tedy nepůsobí problém při přenosu dat

po těchto sítích a zároveň bude mít každá podsíť vlastní prefix, a tedy i odlišné lokální adresy.

Příklad unikátní lokální adresy

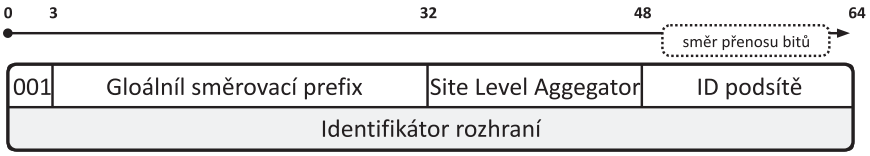
Unikátní lokální adresy jsou definovány v RFC 4193 a začínají prefixem FC::/7. Za ním následuje příznak L, který určuje, zda je adresa generována lokálně či jiným způsobem. V současné době jsou unikátní lokální adresy generovány pouze lokálně. To znamená, že příznak L má hodnotu 1 a proto všechny unikátní lokální adresy začínají prefixem FD::/8.

Dalších 40 bitů obsahuje globální identifikátor, který je generován náhodně. RFC 4193 doporučuje generovat tento identifikátor z aktuálního času, adresy generující stanice a algoritmu SHA-1. Tento prefix spolu s globálním identifikátorem vytváří síťový prefix délky 48 bitů, za kterým následuje 16-ti bitový identifikátor podsítě a 64-ti bitový identifikátor rozhraní podle modifikované EUI-64.

U unikátních lokálních adres je na rozdíl od lokálních linkových adres větší pravděpodobnost, že v takovéto koncové síti nebudou existovat dvě stejné lokální adresy. Pravděpodobnost, že dvojice sítí zvolí stejný globální identifikátor je zhruba 10^{-12}.

3.6 Globální individuální adresy

Globální individuální adresy identifikují svého uživatele v rámci celého Internetu. Jedná se o celosvětově jednoznačné adresy, které lze poznat podle prvních tří bitů v prefixu. Jejich strukturu definuje RFC 3587.



Formát globální individuální adresy

Popis jednotlivých položek:

- Globální směrovací prefix – určuje síť. Bývá zpravidla přidělen **ISP** (*Internet Service Provider*) 1. úrovně a spolu s prefixem 001 je označován jako veřejná topologie.
- Identifikátor podsítě – slouží k identifikaci podsítí v rámci sítě a bývá označován jako místní topologie. 16 bitů toho identifikátoru umožňuje adresovat až 65 535 podsítí.
- Identifikátor rozhraní – slouží k identifikaci rozhraní v rámci podsítě. Pro identifikátor rozhraní je vymezeno 64 bitů, což umožňuje v rámci podsítě adresovat až $18x10^{18}$ různých rozhraní.

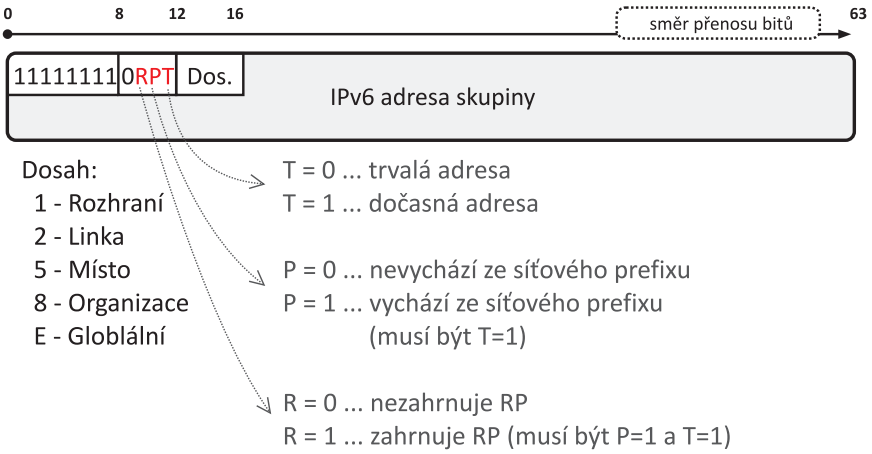
Příklad globální individuální adresy

Globální individuální adresy jsou agregovatelné. To znamená, že se shlukují do skupin podle vzdálenosti, ze které na ně nahlížíme. Agregace adres významným způsobem snižuje počet záznamů ve směrovacích tabulkách, což ovlivňuje výslednou rychlost směrování na páteřních směrovačích. Tato jemnost členění směrovacích informací s rostoucí vzdáleností klesá. To znamená, že se nejprve rozhoduje podle počátečních bitů adresy a blíže k cíli se přesnost zkoumání celé adresy (délky prefixu) zvětšuje. Jedná se o tzv. hierarchické směrování.

3.7 Skupinové adresy

Skupinové adresy slouží k adresaci skupiny počítačů či jiných zařízení a v případě, že jsou na tuto adresu odeslána data, musí být doručena všem zařízením ve skupině. Typickým příkladem použití skupinových adres je distribuce obrazového a zvukového signálu v reálném čase (videokonference, rozhlasové či televizní vysílání).

Skupinové adresy lze jednoduše poznat, protože každá skupinová adresa začíná hodnotou FF (binárně 11111111).

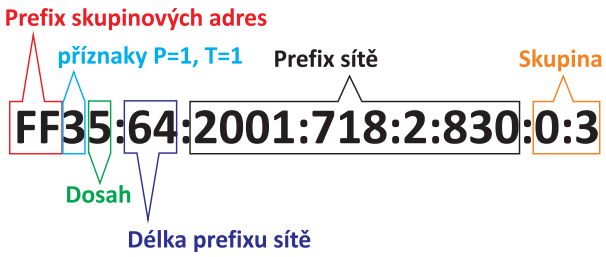


Formát skupinové adresy

Formát skupinové adresy se skládá s následujících položek:

- Volba – skládá se ze čtyř příznaků. První je rezervován pro pozdější využití a za ním následují příznaky R, P a T.
- příznak R – používá se pro skupiny, které souvisejí se směrovacím protokolem **PIM-SM** (*Protocol Independent Multicast – Sparse Mode*). Tento příznak definuje skupinové adresy, které zavádějí tzv. shromaždiště **RP** (*Rendezvous Point*).
- příznak P – byl definován s cílem zavést skupinové adresy, které vychází z adres individuálních. Slouží tedy ke generování jednoznačných skupinových adres, bez nutnosti zjišťování, zda skupinová adresa již v síti existuje. To je dosaženo zařazením prefixu globálních individuálních adres zdejší sítě.
- příznak T – vyjadřuje, zda byla adresa dané skupině přidělena trvale (hodnota 0) nebo pouze dočasně (hodnota 1). Trvalé adresy přiděluje **IANA** (*Internet Assigned Numbers Authority*) a dočasné adresy mohou přidělovat aplikace dle potřeby.
- Dosah – udává, jak daleko mohou být jednotliví členové skupiny od sebe. Jedná se o čtyřbitovou položku, která umožňuje definovat až 16 úrovní dosahu. Koncepce dosahu již byla probrána v kapitole Dosah adres.

- Adresa skupiny – identifikuje skupinu, které mají být data doručena



Příklad skupinové adresy vycházející z globálního rozhraní

Skupinové adresy se nesmí nikdy vyskytnout na místě odesilatele datagramu IPv6 a nesmí být obsaženy ani v rozšiřujícím záhlaví směrování. Mimo to nelze přidělovat skupinové adresy z rozsahu FF0x:0:0:0:0:0:0:0.

Problematika směrování skupinových dat (*multicast*) a tedy i skupinových adres je rozsáhlá. Proto zde uvedu pouze jednotlivé typy skupinových adres, mezi které patří:

- Skupinové adresy vycházející z globálních individuálních adres (RFC 3306)
- Skupinové adresy vycházející z rozhraní (RFC 4489)
- Skupinové adresy pro **SSM** (*Source Specific Multicast*)
- Skupinové adresy obsahující RP (RFC 3956)

Předdefinované skupinové adresy

Existuje celá řada skupinových adres se speciálním významem, které definuje RFC 4291. Jedná se především o skupinové adresy nahrazující adresy oznamovací (*broadcast*). Jsou to adresy pro:

- Všechny uzly v rámci jednoho rozhraní FF01::1 či v rámci jedné linky FF02::1.
- Všechny směrovače v rámci jednoho rozhraní FF01::2, jedné linky FF02::2 či jednoho místa FF05::2.
- Vyzývaný uzel. Tyto adresy mají tvar FF02:0:0:0:0:1:FFxx:xxxx, kde poslední trojice bajtů se převezme z hledané adresy. Adresy vyzývaného uzlu využívá mechanismus Objevování sousedů, což je obdoba ARP protokolu u IPv4.

Výše uvedené speciální skupinové adresy jsou využívány i některými interními mechanismy IPv6.

Další skupinové adresy definuje RFC 2375. Jedná se o adresy, které se používají pro různé síťové protokoly a služby. Například pro servery **NTP** (*Network Time Protocol*) se používají adresy FF0x::101.

3.8 Výběrové adresy

Výběrové adresy se používají především pro servery poskytující různé typy služeb. Ty nejzatíženější servery bývají zpravidla realizovány skupinou spolupracujících zařízení, které patří do jedné výběrové skupiny. Této skupině je potom přiřazena jedna výběrová adresa. Výběrové adresy tedy poskytují prostředky pro vyhledání nejbližšího člena výběrové skupiny realizující daný server a pro rozložení dotazů klienta na tyto členy. Typickým příkladem využití výběrových adres je jejich nasazení u DNS serverů.

\+ Všechny výběrové adresy lze směrovat standardními způsoby. Stačí tedy, aby počítač, který se zapojil do výběrové skupiny, oznámil tuto skutečnost některému směrovači a ten se již postará o distribuci této informace.

\− Nevýhodou výběrových adres je, že nemají vlastní adresní prostor, a proto jsou přidělovány ze stejného adresního prostoru jako adresy individuální. To způsobuje, že výběrové a individuální adresy nelze na první pohled od sebe rozlišit. Proto pokud se rozhraní přiděluje výběrová adresa, je nezbytné tuto skutečnost oznámit během konfigurace.

Společným charakterem výběrové skupiny je skutečnost, že jednotlivá rozhraní všech členů lze zařadit do tzv. Obalové sítě (podsíť) se společným prefix P. Uvnitř této obalové sítě musí mít potom každá výběrová adresa svůj vlastní směrovací záznam, který v jednotlivých směrovačích ukazuje vždy na nejbližšího člena výběrové skupiny. Mimo tuto podsíť není třeba výběrovou adresu rozlišovat. Ta může být klidně zahrnuta do agregovaného bloku adres.

Většímu využití výběrových adres brání skutečnost, která je spojena s rozptýlením členů dané výběrové skupiny. Pokud je rozptýlení členů příliš velké, tak délka společného prefixu P je nulová nebo zanedbatelná. V tomto případě se výběrová adresa přidá do globální směrovací informace, což vede k nárůstu velikostí směrovacích tabulek páteřních směrovačů.

Další omezení nasazení výběrových adres představuje dynamičnost směrování, která způsobuje problémy stavovým protokolům, jako je TCP, a směrovací politika, kdy páteřní směrovače Internetu odmítají příliš dlouhé prefixy, a tedy i záznamy pro výběrové adresy. Navíc jsou různé části páteřní sítě Internetu řízeny různými subjekty, jejichž směrovací politiku lze jen těžko ovlivnit.

Z těchto důvodů je použití globálních výběrových adres silně omezeno.

Výběrové adresy lze využít například pro identifikaci směrovačů jednoho ISP. Tyto adresy lze potom použít jako mezilehlé adresy, které se umísťují do rozšiřujícího záhlaví Směrování, pro efektivní doručení datagramu.

Výběrové adresy lze rovněž použít i k identifikaci směrovačů připojených ke konkrétní podsíti, nebo k identifikaci směrovačů poskytujících přístup k dané doméně.

V současné době se však očekává, že výběrové adresy v globálním měřítku budou nasazeny pouze pro DNS servery. Naproti tomu v menší části sítě, která je pod kontrolou jednoho poskytovatele, mohou výběrové adresy představovat efektivnější adresování.

3.9 Povinné adresy uzlu

V případě IPv4 má rozhraní zpravidla pouze jednu adresu. IPv6 tuto skutečnost mění a přímo nařizuje, aby každé rozhraní mělo více adres. Z tohoto důvodu existuje minimální množina adres, ke kterým se musí každé rozhraní hlásit.

V případě koncového počítače se jedná o následující adresy:

- Lokální smyčka (*loopback*)
- Lokální linková
- Všechny individuální a výběrové adresy, které byly danému rozhraní přiděleny
- Skupinové adresy pro všechny uzly
- Skupinová adresa vyzývaného uzlu pro všechny přidělené individuální a výběrové adresy
- Všechny skupinové adresy, jejichž je rozhraní členem

Každý směrovač se musí hlásit 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

3.10 Výběr adresy

S několika různými adresami přiřazenými jednomu počítači vznikl problém, kterou adresu použít pro danou komunikaci. K tomuto účelu byl definován algoritmus pro volbu adres, který je popsán v RFC 3484.

Kandidátské adresy

Základem algoritmu jsou kandidátské adresy. Pro cílové adresy se seznam kandidátských adres nejčastěji získá prostřednictvím DNS dotazu (převod DNS jména na IPv6 adresu). Tento seznam je následně seřazen podle níže uvedených pravidel od nejvhodnější adresy po nejméně vhodnou, z něhož se vybere nejvhodnější cílová adresa. V případě, že má aplikace k dispozici cílovou IPv6 adresu, výběr cílové adresy odpadá.

K cílové adrese je třeba vybrat nejvhodnější zdrojovou adresu. Pro zdrojové adresy seznam kandidátských adres tvoří všechny individuální adresy přiřazené rozhraní, kterým budou data odeslána k danému cíli. Z toho vyplývá, že každá cílová adresa může mít různé seznamy kandidátských adres pro zdrojovou adresu. V případě směrovače, seznam kandidátských adres pro zdrojovou adresu může obsahovat i individuální adresy ostatních rozhraní, na kterých předává data. Aplikováním níže uvedených pravidel se ze seznamu kandidátských adres vybere nejvhodnější zdrojová adresa.

V případě, že se komunikace nezdaří, může se volba adres opakovat.

Tabulka politik

Tabulka politik slouží k určení místních preferencí. Jednotlivé záznamy obsahují prefix, prioritu a značku, kde priorita určuje výhodnost dané adresy jako cílové a značka určuje, zdali se zvolený pár adres k sobě hodí. V případě shodné značky obou adres, je takovému páru adres dána přednost. Hledaná priorita a značka se určí na základě nejdelšího shodného prefixu.

V případě, že není tabulka politik nakonfigurována administrátorem, použije se výchozí tabulka politik.

Výchozí tabulka politik

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

Výběr zdrojové adresy

Algoritmus má dvě sady pravidel. První se vztahuje na volbu zdrojové adresy a je demonstrována pomocí příkladu, kdy jsou k dispozici dvě zdrojové adresy SA a SB pro daný cíl. Pravidla se aplikují postupně a v případě, že dojde k rozhodnutí, ostatní se neberou v potaz. Jestliže žádné pravidlo nerozhodne, ponechá se volba zdrojové adresy na implementaci. Pořadí pravidel pro volbu zdrojové adresy je:

1. Preferovat totožné adresy – pokud je adresa totožná s cílovou, vyber ji.
2. Preferovat odpovídající dosah – pokud mají adresy rozdílný dosah, seřaď je podle *dosah(SA) < dosah(SB)*. Pokud je *dosah(SA) < dosah(cíl)* vyber adresu SB, jinak vyber adresu SA.
3. Vyhýbat se odmítaným adresám
4. Preferovat domácí adresy
5. Preferovat odchozí rozhraní – pokud je adresa SA přiřazena k rozhraní, kterým budou data odeslána k cíli, a adresa SB nikoli, vyber adresu SA.
6. Preferovat shodné značky – pokud *značka(SA) = značka(cíl)* a *značka(SB) ≠ značka(cíl)*, vyber adresu SA.
7. Preferovat veřejné adresy
8. Použít nejdelší shodný prefix

Algoritmus je symetrický, proto dojde prohození rolí zdrojových adres a k opakované aplikaci pravidel. Aplikováním pravidel se určí nejvhodnější zdrojová adresa pro daný cíl.

Výběr cílové adresy

Při výběru cílové adresy se mimo jiné zvažuje vhodnost zdrojové a cílové adresy. Z tohoto důvodu se pro každou cílovou adresu prvně určí nejvhodnější zdrojová adresa. Následně dojde k uspořádání cílových adres v kandidátském seznamu podle následujících pravidel:

1. Vyhýbat se cílovým adresám, které se nepoužívají – pokud je cílová adresa DB nedosažitelná, nebo pokud *zdroj(DB)* není definován, vyber cílovou adresu DA.
2. Preferovat shodný dosah – pokud je *dosah(DA) = dosah(zdroj(DA))* a *dosah(DB) ≠ dosah(zdroj(DB))*, vyber adresu DA.
3. Vyhýbat se odmítaným adresám
4. Preferovat domácí adresy
5. Preferovat shodné značky – pokud je *značka(zdroj(DA)) = značka(DA)* a *značka(zdroj(DB)) ≠ značka(DB)*, vyber adresu DA.

6. Preferovat nejvyšší prioritu
7. Preferovat přenos nativním protokolem – pokud adresa DA je dosažitelná prostřednictvím přechodového mechanismu (např. zapouzdření IPv6 do IPv4) a adresa DB je dosažitelná prostřednictvím nativního protokolu, vyber adresu DB.
8. Preferovat menší dosah – pokud je *dosah(DA) < dosah(DB)*, vyber adresu DA.
9. Použít nejdelší shodný prefix
10. V opačném případě, nech pořadí beze změny – pokud adresa DA předchází v původním seznam adresu DB, vyber adresu DA. Jinak vyber adresu DB.

Počítač má jediné síťové rozhraní, kterému byly přiděleny následující adresy:

1. FE80::02B5:32FF:FE01:1984 (lokální linková)
2. 2001:718:10:1:02B5:32FF:FE01:1984 (globální individuální)
3. 2001:: 02B5:32FF:FE01:1984 (globální individuální)

Počítač má odeslat data na adresu 2001:718:20:56:E859:A1FF:FE82:AA01 a potřebuje vybrat nejvhodnější zdrojovou adresu. Dále bude použita výchozí tabulka politik, z jejíhož hlediska se všem adresám přiřadí priorita 40 a značka 1.

Lokální linková adresa skončí na pravidle číslo 2, protože její dosah je menší než globální dosah cíle. Mezi globálními adresami rozhodne až pravidlo 8, kdy se jako zdrojová adresa zvolí druhá adresa, protože má shodný nejdelší prefix 2001:718::/32.

Výběr cílové adresy je založen na kandidátském seznamu, který poslal DNS server pro určité doménové jméno. Kandidátský seznam obsahuje následující adresy:

1. 2001:DB8:A29C:5::02 (zdrojová adresa 2001:: 02B5:32FF:FE01:1984)
2. 2001:718::B5:18FF:FE09:1 (zdrojová adresa 2001:718:10:1:02B5:32FF:FE01:1984)

Seznam obsahuje i vhodné zdrojové adresy, které jsou zvoleny na základě algoritmu pro výběr zdrojové adresy. Obě adresy mají shodně přidělenu prioritu 40 i značku 1. Algoritmus rozhodne až na základě pravidla 8, kdy druhá adresa má shodný nejdelší prefix 2001:718::/32. Kandidátský seznam pro cílové adresy bude seřazen následovně:

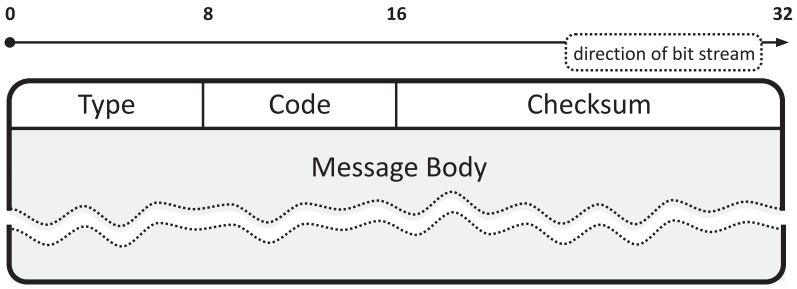
1. 2001:718::B5:18FF:FE09:1
2. 2001:DB8:A29C:5::02

Tedy pro komunikaci bude zvolena adresa 2001:718:10:1:02B5:32FF:FE01:1984 jako zdrojová a adresa 2001:718::B5: 18FF:FE09:1 jako cílová.

4 ICMPv6

4.1 Protokol ICMPv6

Protokol **ICMPv6** (*Internet Control Message Protocol for the Internet Protocol Version 6*) je součástí sady protokolů Internetu a je definován v RFC 4443. Používá se především pro ohlašování chybových stavů, testování dosažitelnosti a pro výměnu některých provozních informací. RFC 4443 definuje pouze základy, jako je formát paketu a základní druhy zpráv, které jsou děleny na chybové a informační. Jednotlivé zprávy jsou přenášeny prostřednictvím datagramu IPv6.



Formát zprávy ICMPv6

Současná verze ICMP definuje čtyři chybové zprávy:

- Nedosažitelnost – oznamuje, že směrovač dostal datagram s nedosažitelnou cílovou IP adresou. Položka Kód podrobněji specifikuje důvod nedoručení datagramu.
- Nadměrný datagram – oznamuje odesilateli, že někde na cestě existuje úsek s MTU nižší, než je velikost datagramu. Ve čtyřbajtové položce, za kontrolním součtem, se přenáší aktuální velikost MTU. Tyto zprávy mají využití při objevování MTU cesty.
- Vypršení životnosti datagramu – tuto zprávu posílá směrovač v případě, že datagramu vypršela doba životnosti (maximum skoků kleslo na nulu). Nebo se posílá v případě, že v daném časovém limitu příjemce neobdržel všechny fragmenty fragmentovaného datagramu.
- Chybný datagram – tato zpráva oznamuje, že příjemce obdržel datagram, s jehož parametry si neví rady. Čtyřbajtová položka za kontrolním součtem specifikuje problém a udává počet bajtů od začátku datagramu, kde začíná položka, které příjemce nerozuměl.

Mezi základní informační zprávy patří:

- Echo a Odpověď na echo – tyto zprávy využívá program ping

- Dotaz a Odpověď na dotaz – umožňují získat základní informace o uzlech (jméno uzlu, adresu IPv4 nebo IPv6, atd.) a slouží spíše pro správu sítě

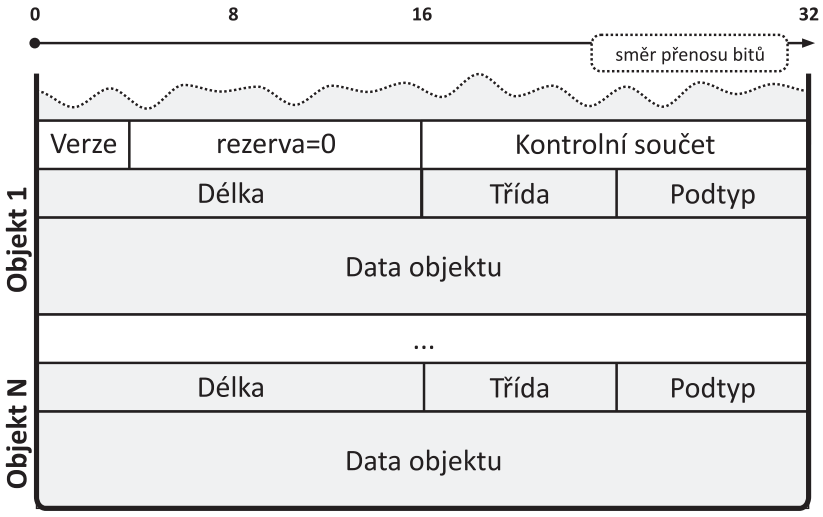
Další typy zpráv a pravidla pro jejich generování doplňují interní mechanismy IPv6. Jedná se například o zprávy Členství ve skupinách, Výzva a Ohlášení směrovače či souseda, Přesměrování a Objevování souseda a zprávy týkající se mobility.

Protokol ICMPv6 má oproti ICMPv4 implementovány bezpečnostní mechanismy. V případě IPv4 mohlo dojít k zneužití zpráv ICMP a tím k omezení funkčnosti sítě. Ve zkratce, cílové zařízení se zahltilo mnoha zprávami ICMP a ostatní provoz neměl šanci projít. Bezpečnostní mechanismy využívají následující opatření:

- Minimální časový odstup mezi zprávami či maximální podíl na celkové šířce pásma, které zařízení generuje. To vede k zaručení dostatečného prostoru pro přenos reálných dat.

- Jednotlivé zprávy lze opatřit šifrovacím záhlavím. Tato záhlaví musí být prověřena, jinak se zprávy ICMPv6 zahodí. Správce by měl mít možnost nastavit zařízení, aby přijímalo pouze zabezpečené zprávy a ostatní ignorovat.

Novinkou protokolu ICMPv6 je jeho rozšířená verze, definovaná v RFC 4884, která umožňuje do těla zprávy vložit další informace a drobně pozměňuje některé existující zprávy, jako jsou Nedosažitelnost či Vypršení životnosti. Záhlaví rozšířené verze se umisťuje za konec těla zprávy ICMPv6. Za ním pak následují vlastní data rozšiřujícího objektu.



Formát rozšířené verze zprávy ICMPv6

Implementace ICMPv6 je povinná v každém zařízení, které podporuje IPv6.

5 Objevování sousedů

5.1 Objevování sousedů

Mechanismus Objevování sousedů **ND** (*Neighbor Discovery*) je obdobou protokolu **ARP** (*Address Resolution Protocol*), který se používá pro zjištění fyzické adresy (MAC adresy) daného rozhraní u IPv4. Objevování sousedů je komplexnější mechanismus, který je definován v RFC 4861 jako jedna ze základních součástí IPv6. Slouží především k následujícím účelům:

- Zjišťování a aktualizace fyzických adres uzlů v rámci stejné lokální sítě
- Hledání směrovačů
- Přesměrování
- Zjišťování prefixů, parametrů sítě a dalších údajů pro automatickou konfiguraci adres
- Ověřování dosažitelnosti sousedů
- Detekce duplicitních adres

Mechanismus objevování sousedů ke své činnosti používá následující typy ICMPv6 zpráv:

- Výzva sousedovi **NS** (*Neighbor Solicitation*)
- Ohlášení souseda **NA** (*Neighbor Advertisment*)

Pro zajištění bezpečnosti počítačových systémů byly definovány i mechanismy zabezpečného objevování sousedů **SEND** (*SEcure Neighbor Discovery*), jehož základy jsou popsány v RFC 3971. Cílem SEND je poskytnout dostatečnou úroveň zabezpečení výměny zpráv.

5.2 Hledání fyzických adres

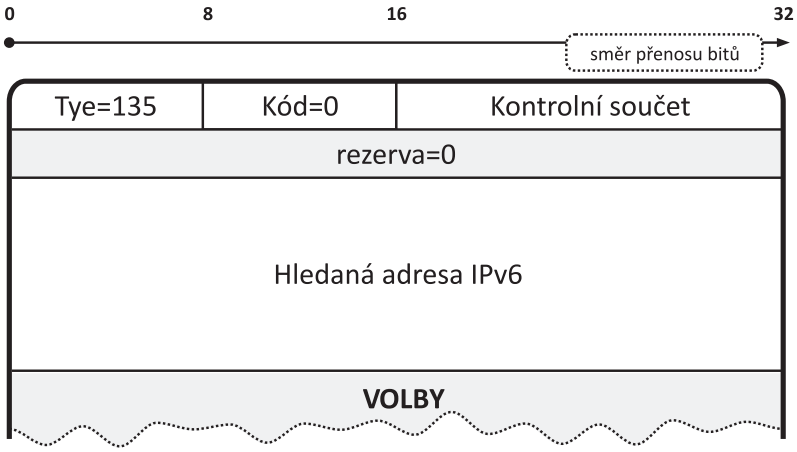
Mechanismus Objevování sousedů ke své činnosti používá skupinovou adresu, která vychází z prefixu FF02:0:0:0:0:1:FF00::/104 a IPv6 adresy souseda, jehož fyzická adresa se hledá. Tato adresa se nazývá Adresa vyzývaného uzlu (*Solicited-Node Multicast address*).

Každé rozhraní může být členem několika sítí s různými prefixy. Z tohoto důvodu se adresa vyzývaného uzlu vytváří převzetím posledních 24 bitů z identifikátoru rozhraní. Tím se docílí, že všechny jeho IPv6 adresy budou mít stejnou adresu vyzývaného uzlu. Aby mechanismus Objevování sousedů správně fungoval, musí uzel posílat dotazy do všech skupin, jejichž je členem.

Pro uchování IPv6 adres s jejich odpovídajícími fyzickými adresami, používá každý uzel interní datovou sktrukturu Cache sousedů (*Neighbor Cache*).

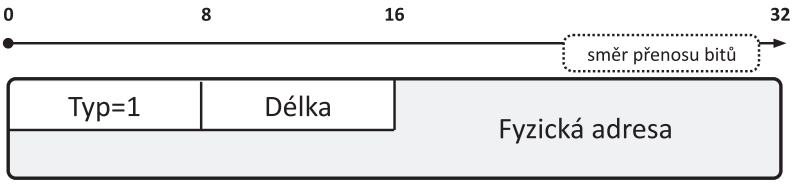
V případě, že uzel zná IPv6 adresu souseda a hledá jeho fyzickou adresu, je postup hledání následující:

- Uzel vytvoří Adresu vyzývaného uzlu z cílové IPv6 adresy a na tuto adresu pošle ICMP zprávu výzva sousedovi, ke které může připojit i svoji fyzickou adresu prostřednictvím volby Fyzická adresa odesilatele a informace o MTU linky prostřednictvím volby MTU.

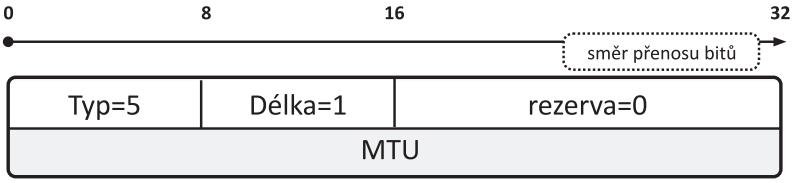


Formát zprávy Výzva sousedovi

- Je-li hledaný soused aktivní, odpoví ICMP zprávou ohlášení souseda, která obsahuje volbu Fyzická adresa odesilatele, v níž je vložena informace o hledané fyzické adrese. Rovněž může připojit i informace o MTU linky.

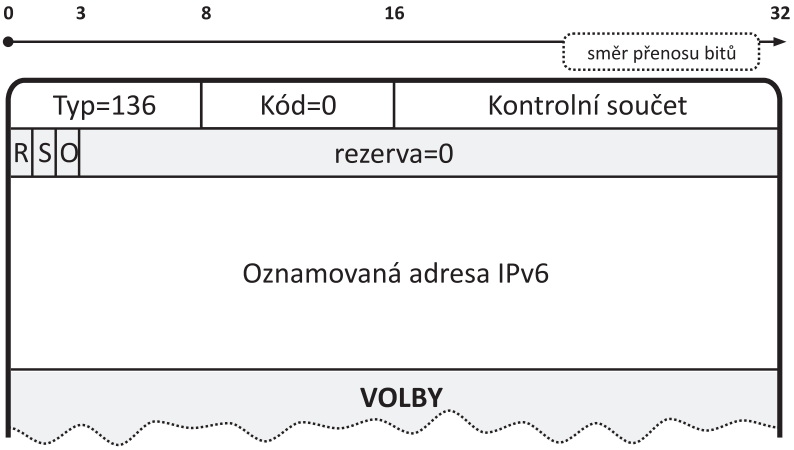


Volba Fyzická adresa odesilatele



Volba MTU

Zprávu Ohlášení souseda může daný uzel poslat i v případě, že došlo ke změně jeho fyzické adresy. Tuto skutečnost uzel oznámí zasláním několika zpráv Ohlášení souseda na skupinovou adresu pro všechny uzly (FF02::1). Ty uzly, které mají ve své Cache sousedů uložen záznam s danou IPv6 adresou, aktualizují tento záznam, ostatní jej ignorují.



Formát zprávy Ohlášení souseda

Zpráva Ohlášení souseda obsahuje i doplňkové informace, které jsou přenášeny prostřednictvím následujících příznaků:

- příznak R (*Router*) – signalizuje, že odesilatelem je směrovač
- příznak S (*Solicited*) – signalizuje, zdali je ohlášení souseda vyžádáno či nikoli
- příznak O (*Override*) – signalizuje, zda informace o fyzické adrese má přepsat dosavadní záznam v cache sousedů

5.3 Detekce dosažitelnosti souseda

Mechanismus aktualizace Cache sousedů není stoprocentně spolehlivý, proto každý uzel aktivně sleduje stav dosažitelných sousedů, se kterými komunikuje. K potvrzení dosažitelnosti slouží dva mechanismy. První mechanismus využívá zpráv vyšších vrstev (např. TCP) a druhý je založen na posílání výzev sousedovi a přijímání ohlášení souseda, jako odpověď.

Základem druhého mechanismu jsou následující stavy, které se přidělují jednotlivým záznamům v Cache sousedů:

- Nekompletní (*incomplete*) – tento stav signalizuje, že fyzická adresa není známá a že byla odeslána výzva sousedovi s cílem zjistit fyzickou adresu, na kterou dosud nedorazila odpověď. V případě, že odpověď nedorazí, bude daný záznam odstraněn z Cache sousedů.

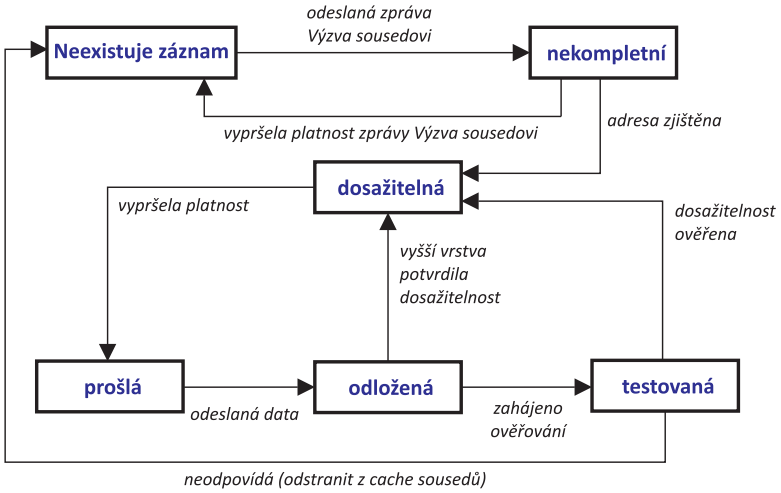
- Dosažitelná (*reachable*) – fyzická adresa je známá a soused je dosažitelný. Tento stav trvá určitý časový interval, který uzlům zpravidla oznamuje výchozí směrovač.

- Prošlá (*stale*) – tento stav signalizuje, že došlo k vypršení časového intervalu dosažitelnosti souseda. V okamžiku, kdy je třeba odeslat data, dojde k jejich odeslání a stav záznamu se změní na Odložená.

- Odložená (*delay*) – tento stav signalizuje prošlou platnost záznamu a skutečnost, že se čeká na potvrzení dosažitelnosti. To buď potvrdí vyšší vrstva, nebo dojde k odeslání zprávy Výzva sousedovi.

- Testovaná (*probe*) – tento stav signalizuje, že se čeká na odpověď na zprávu Výzva sousedovi. V případě, že odpověď dorazí, dojde ke změně stavu na Dosažitelná. V opačném případě dojde k odstranění záznamu z paměti cache sousedů.

Průběh změn jednotlivých stavů během detekce dosažitelnosti souseda je zobrazen na následujícím diagramu.



Změny stavu záznamů v paměti cache sousedů

5.4 Inverzní objevování sousedů

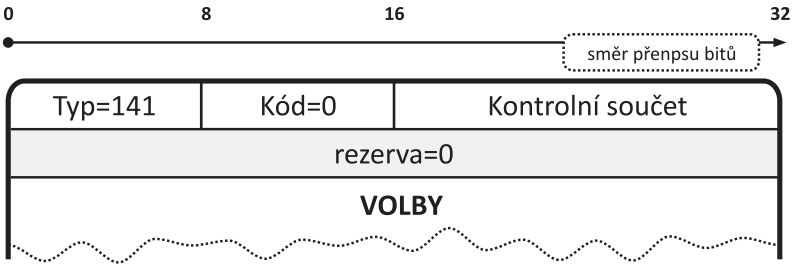
Inverzní objevování sousedů **IND** (*Inverse Neighbor Discovery*) je definováno v RFC 3122 a má za cíl nalézt ke známé fyzické adrese adresu IPv6.

Princip inverzního objevování sousedů je velmi jednoduchý. Uzel, který chce nalézt IPv6 adresu svého souseda (tazatel), pošle přímo na jeho fyzickou adresu ICMP zprávu Výzva, k níž připojí následující povinné volby:

- Zdrojová fyzická adresa (*Source Link-Layer Address*) – obsahuje fyzickou (např. MAC) adresu odesilatele.
- Cílová fyzická adresa (*Target Link-Layer Address*) – obsahuje fyzickou adresu cílového uzlu.

Volitelně může uzel připojit i následující volby:

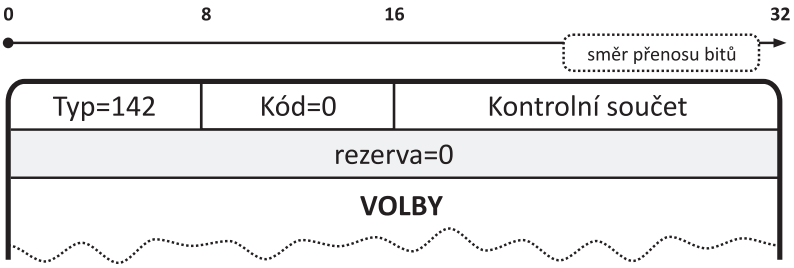
- Seznam zdrojových adres (*Source Address List*) – obsahuje seznam IPv6 adres přiřazených rozhraní, které je identifikovatelné zdrojovou fyzickou adresou. Položka Typ nese hodnotu 9, viz formát volby Seznam adres.
- MTU – obsahuje hodnotu MTU dané linky.



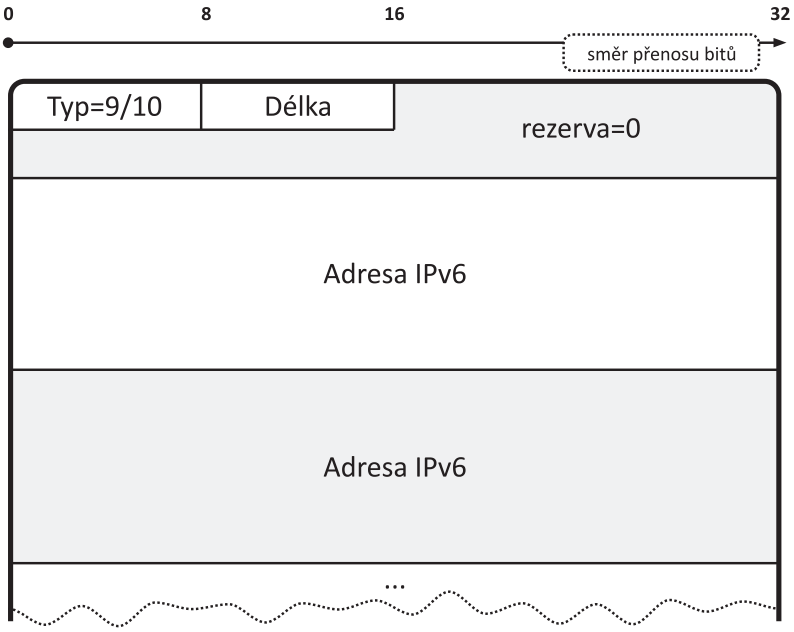
Formát zprávy Výzva inverzního objevování sousedů

Vyzývaný uzel reaguje na výzvu ICMP zprávou Ohlášení, kterou adresuje na fyzickou adresu tazatele, k níž připojí následující povinné volby:

- Cílová fyzická adresa – obsahuje fyzickou adresu tazatele
- Seznam cílových adres (*Target Address List*) – obsahuje seznam IPv6 adres přiřazených rozhraní, které je identifikovatelné cílovou fyzickou adresou. Položka Typ nese hodnotu 10, viz formát volby Seznam adres.



Formát zprávy Ohlášení inverzního objevování sousedů



Formát volby Seznam adres

Tazatel si po přijetí zprávy Ohlášení uloží obdržené informace do Cache sousedů.

Vyzývaný uzel může rovněž připojit i volbu MTU. Volba pro fyzické adresy a MTU linky je stejná jako v případě mechanismu Objevování sousedů.

6 Automatická konfigurace

6.1 Automatická konfigurace

Jedná se o novinku IPv6, která funguje na principu plug and play. To znamená, že si počítač po připojení do sítě automaticky vygeneruje adresu IPv6 a zjistí potřebné parametry pro správnou komunikaci s okolním světem.

Existují dva typy automatické konfigurace:

- bezestavová **SLAAC** (*Stateless Address Autoconfiguration*) – představuje zcela nový způsob automatické konfigurace. Vychází ze skutečnosti, že každá lokální síť má výchozí směrovač, který zná všechny potřebné parametry pro komunikaci s okolním světem. Tyto parametry rozesílá v určitých časových intervalech do všech sítí, ke kterým je připojen. Klientovi tedy stačí pouze naslouchat či o tyto parametry požádat. Bezstavová automatická konfigurace je popsána v RFC 4862.
- stavová **DHCPv6** (*Dynamic Host Configuration Protocol for IPv6*) – jejím základem je server spravující konfigurační parametry, které klientům sděluje na požádání. Pro potřeby stavové automatické konfigurace byl definován protokol DHCPv6, což je modifikace známého protokolu **DHCP** (*Dynamic Host Configuration Protocol*). Protokol DHCPv6 je definován v RFC 3315.

Většina současných implementací IPv6 umožňují kombinaci obou typů automatické konfigurace.

7 Bezestavová automatická konfigurace

7.1 Zprávy ICMPv6

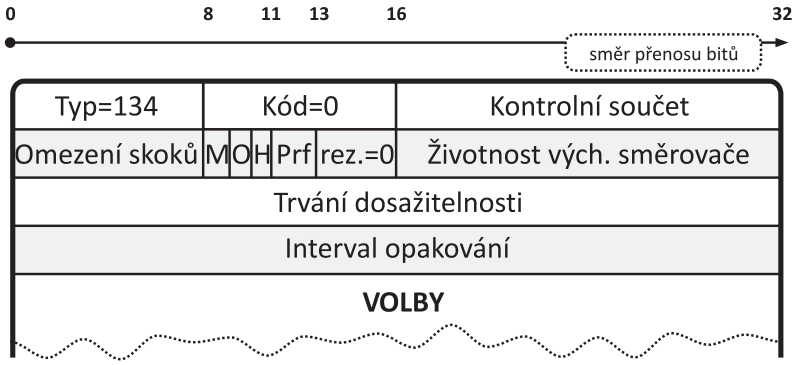
Bezestavová konfigurace používá ke své činnosti následující ICMPv6 zprávy:

- Ohlášení směrovače **RA** (*Router Advertisment*)
- Výzva směrovači **RS** (*Router Solicitation*)
- Přesměrování (*Redirect*)

Předtím než probereme základy bezestavové konfigurace, je nezbytné seznámit se s ICMPv6 zprávou Ohlášení směrovače.

Ohlášení směrovače

Základním kamenem bezstavové konfigurace je ICMP zpráva Ohlášení směrovače, pomocí které se v náhodných časových intervalech rozesílají všechny potřebné parametry pro komunikaci s okolním světem.



Formát zprávy Ohlášení směrovače

Popis důležitých položek zprávy Ohlášení směrovače:

- Omezení skoků (*Cur Hop Limit*) – oznamuje uzlům, jakou hodnotu mají vkládat do položky s maximálním počtem skoků (životnost datagramu).
- příznak **M** (*Managed address configuration*) – příznak Stavové konfigurace adres oznamuje, že adresy a další komunikační parametry jsou přidělovány protokolem DHCPv6.
- příznak **O** (*Other stateful configuration*) – příznak Stavové konfigurace ostatních parametrů oznamuje, že i ostatní parametry jsou přidělovány protokolem DHCPv6, jako je adresa lokálního DNS serveru.

Následující tabulka uvádí význam možných kombinací příznaků M a O.

Možné kombinace příznaků M a O a jejich význam

příznak M	příznak O	význam
1	-	všechny parametry jsou přiděleny protokolem DHCPv6
0	1	kombinace bezstavové konfigurace (adresa, prefix, směrování) a DHCPv6 (pro ostatní parametry)
0	0	Protokol DHCPv6 není k dispozici

- příznak **H** (*Home agent*) – příznak domácího agenta slouží k podpoře mobility a oznamuje, že výchozí směrovač pracuje i jako domácí agent.

- Preference **Prf** (*Default Router Preference*) – umožňuje rozlišit preference výchozích směrovačů a nastavuje se v případě nenulové položky Životnost výchozího směrovače. Existují celkem čtyři úrovně.

Preference výchozího směrovače

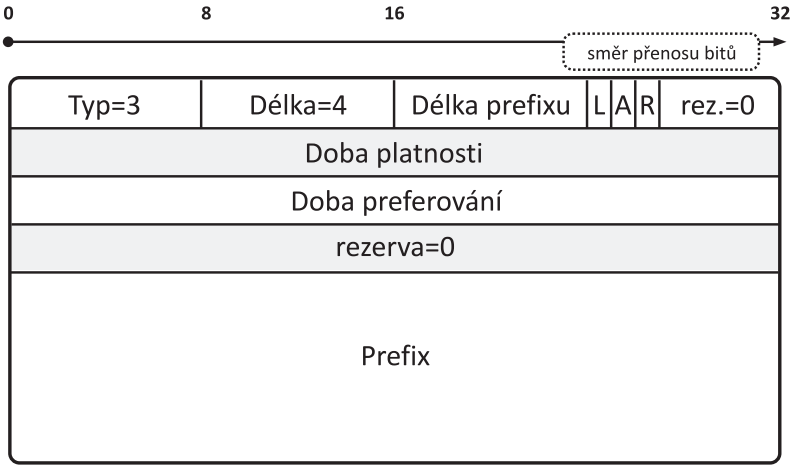
Prf	význam
01	vysoká
00	střední
11	nízká
10	rezervováno (nesmí se používat)

- Životnost výchozího směrovače (*Router Lifetime*) – oznamuje časový interval, po který směrovač bude sloužit jako výchozí. Je-li hodnota nulová, směrovač nebude použit jako výchozí.

- Trvání dosažitelnosti (*Reachable Time*) – oznamuje, jak dlouho má být uzel považován za dosažitelný, poté co byla ověřena jeho momentální dosažitelnost.

- Interval opakování (*Retrans Timer*) – jedná se o interval mezi dvěma výzvami sousedovi

- volby – umožňují připojit informace o fyzické adrese, ohlásit MTU linky a především slouží pro vkládání informací o prefixech. Pro každý prefix se vloží jedna volba Informace o prefixu.



Formát volby Informace o prefixu

Formát volby Informace o prefixu obsahuje tyto důležité položky:

- Délka prefixu (*Prefix Length*) – udává délku prefixu v bitech.
- příznak **L** (*on-Link*) – oznamuje, že daný prefix může být použit k určení, zdali je uzel lokální či nikoli.
- příznak **A** (*Autonomous address-configuration*) – příznak autonomní konfigurace adres oznamuje, že daný prefix lze použít k automatické konfiguraci vlastní adresy. Je-li tento příznak nastaven na hodnotu 0, umožňuje vypnout bezestavovou konfiguraci. Uzel má k dispozici tedy pouze lokální linkovou adresu nebo může k získání adresy použít DHCPv6. V případě, že některé prefixy mají nastaven příznak A i L, může daný uzel použít obě automatické konfigurace pro získání adresy.
- příznak **R** (*Router address*) – příznak adresy směrovače oznamuje, že položka Prefix obsahuje kompletní globální adresu směrovače. Tento příznak byl zaveden pro potřeby mobility. V případě využití pro automatickou konfiguraci se použije pouze prefix a identifikátor rozhraní se bude ignorovat.
- Doba platnosti (*Valid Lifetime*) – udává, jak dlouho bude daný prefix platit.
- Doba preferování (*Preferred Lifetime*) – udává, jak dlouho mají být preferovány adresy, které vznikly prostřednictvím automatické konfigurace. Adresa je po své vzniku označena jako preferována (*preferred*). Uzel ji může bez žádných omezení libovolně používat. Po vypršení doby preferování je adresa označena jako odmítaná (*deprecated*). To znamená, že je sice adresa platná, ale pro zahájení nové komunikace by se již neměla používat. Po vypršení doby platnosti se již adresa nesmí používat, stává se neplatnou.

7.2 Princip bezestavové konfigurace

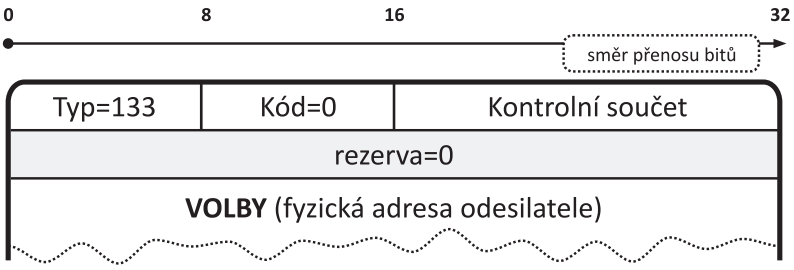
Bezestavová konfigurace umožňuje uzlům si vygenerovat jejich vlastní adresy z lokálně dostupných a směrovačem šířených informací. Typicky směrovače šíří prefixy, které identifikují podsítě přidělené dané lince, zatímco jednotlivé uzly generují identifikátory rozhraní, které jednoznačně identifikují jejich rozhraní. Výsledná adresa pro danou podsíť potom vznikne kombinací jejího prefixu a identifikátoru daného rozhraní. V případě absence směrovače, tedy šířeného prefixu, si uzly vygenerují pouze lokální linkové adresy. Tyto adresy umožní uzlům vzájemnou komunikaci v rámci stejné linky.

Před zahájením vlastní komunikace s okolním světem IPv6, si musí každý uzel vygenerovat svoji vlastní lokální linkovou adresu. To udělá tak, že k prefixu lokálních linkových adres FE80::/10 připojí svůj vlastní identifikátor rozhraní. Takto vygenerovanou adresu musí dále v rámci lokální sítě ověřit, zdali je jednoznačná. K tomu použije mechanismus Detekce duplicitních adres, který je založen na klasickém objevování sousedů. Tento mechanismus používá k detekci duplicitní adresy zprávu Výzva sousedovi, kterou hledá všechny sousedy se stejnou lokální linkovou adresou. Pokud jako reakce na tuto zprávu dorazí zpráva Ohlášení souseda, znamená to, že i jiný uzel v lokální síti má stejný identifikátor rozhraní a automatická konfigurace je následkem toho zastavena. Duplicita adres se testuje i v případě manuální nebo stavové konfigurace adres.

V případě negativní odezvy si uzel vygenerovanou lokální linkovou adresu přidělí. V tomto bodě již uzel může komunikovat prostřednictvím IPv6 protokolu s ostatními sousedy v rámci jedné linky. Další fáze automatické konfigurace zahrnuje čekání na ohlášení směrovače. Z příznaků v ohlášení směrovače uzel pozná, zda má použít pro vygenerování adresy a získání ostatních parametrů sítě bezestavovou konfiguraci či nikoli. Ve volbě Seznam adres je dále uveden u každého prefixu příznak, který říká, zda se má pro daný prefix použít bezestavová konfigurace adres. Pokud ano, připojí k danému prefixu svůj identifikátor rozhraní a adresu si přidělí. Dále je u každého prefixu uvedena jeho životnost, která říká, jak dlouho má být adresa preferována a platná. Jednoznačnost této adresy se již netestuje, protože identifikátor rozhraní je jednoznačný, což bylo ověřeno v počáteční fázi automatické konfigurace.

Směrovače typicky posílají ohlášení směrovače periodicky. Avšak doba mezi úspěšným příjmem těchto zpráv může být delší, než je uzel ochotný čekat. V tomto případě si může uzel o ohlášení směrovače zažádat sám zprávou Výzva směrovači, kterou pošle všem směrovačům v rámci linky.

V opačném případě, kdy se v rámci linky nevyskytuje směrovač, může být pro získání globální individuální adresy použita stavová konfigurace (DHCPv6). Uzel rovněž může oba způsoby kombinovat.



Formát zprávy Výzva směrovači

Protože směrovače posílají ohlášení směrovače periodicky, dochází tak k neustálému aktualizování jednotlivých adres, případně k přidání nových či odstranění neplatných.

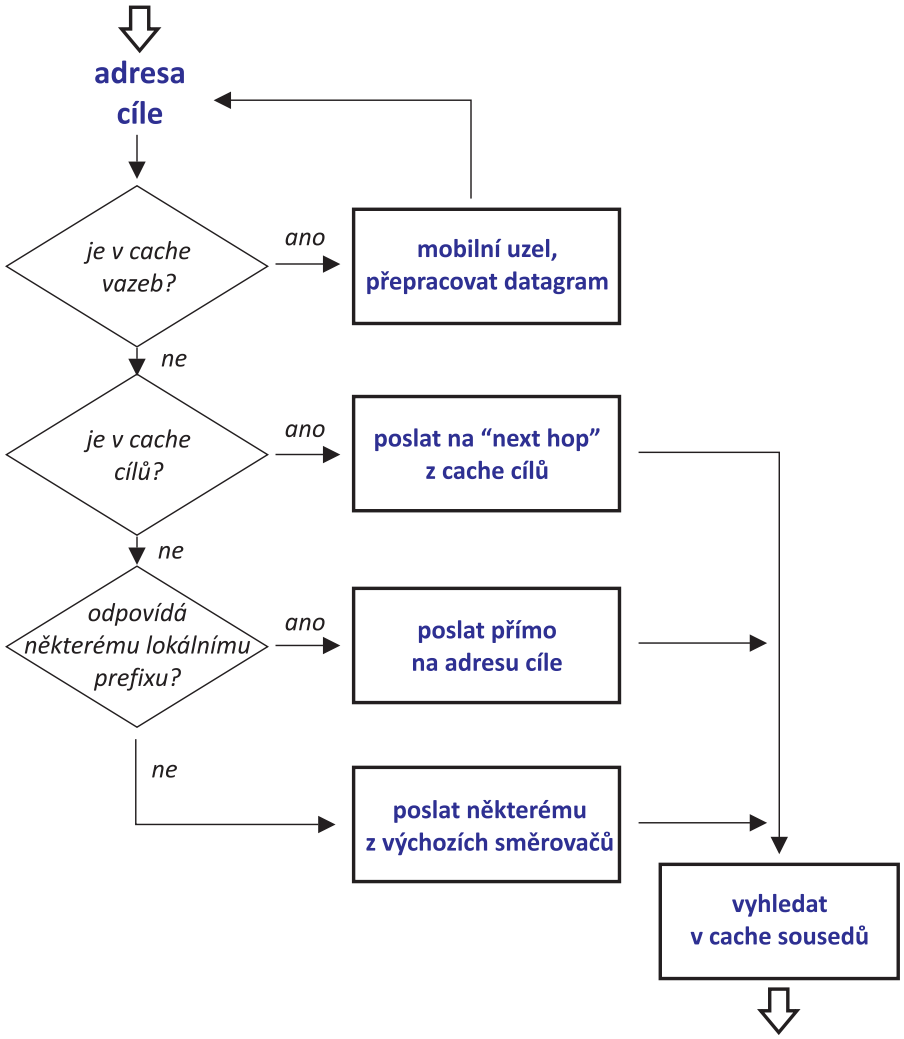
7.3 Konfigurace směrování a DNS

Automatická konfigurace rovněž umožňuje odvození směrovacích informací. K tomu využívá následující základní datové sktruktury, které mohou být realizovány jako jeden celek pomocí směrovací tabulky:

- Cache cílů (*Destination Cache*) – obsahuje směrovací informace pro konkrétní adresy. Každý záznam obsahuje adresu následujícího směrovače (*next hop*).
- Seznam prefixů (*Prefix List*) – slouží k rozhodování, zda je cílový uzel v lokální síti či nikoli
- Seznam výchozích směrovačů (*Default Router List*) – obsahuje seznam všech dostupných výchozích směrovačů

V případě podpory mobility, se ještě přidává Cache vazeb (*Binding Cache*), která oznamuje, že cílový uzel komunikuje na dočasně přidělené adrese. Tato skutečnost znamená, že odchozí datagram bude doplněn o záhlaví Směrování a jeho cílová adresa bude změněna.

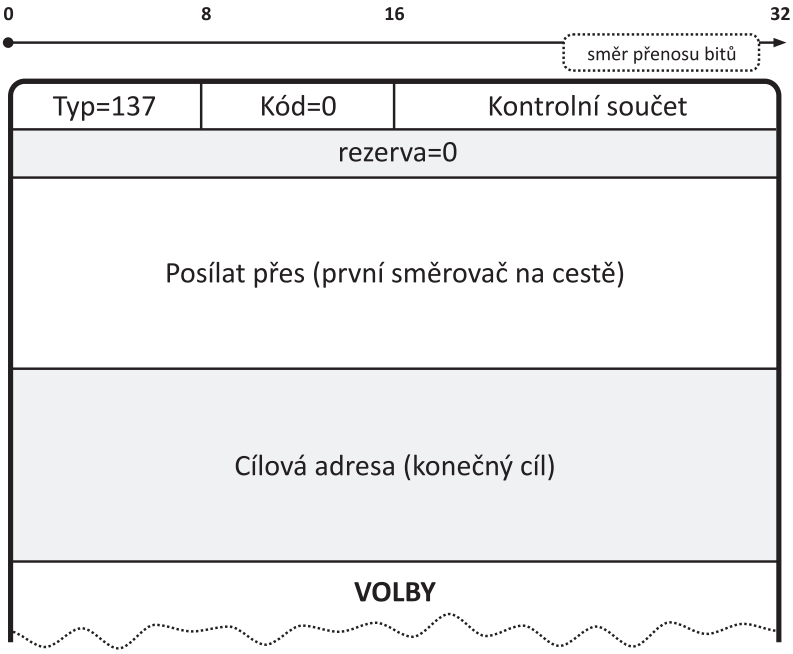
Postup při odesílání datagramu je znázorněn pomocí následujícího diagramu.



Postup při odesílání datagramu

Přesměrování

Dojde-li k nevhodné volbě výchozího směrovače nebo je daný cílový uzel ve skutečnosti v lokální síti, pošle výchozí směrovač odesilateli ICMPv6 zprávu Přesměrování. Ta obsahuje cílovou adresu datagramu a adresu směrovače nebo cíle samotného, na kterou se mají datagramy pro cílový uzel posílat. Tato adresa je uvedena v položce Posílat přes (*Target Address*). Do voleb lze dále zařadit fyzickou adresu směrovače a záhlaví datagramu, který vyvolal přesměrování. Toto záhlaví však musí mít omezenou velikost, aby nedošlo k překročení celkové délky zprávy, která nesmí být větší jak 1280 bajtů.



Formát zprávy Přesměrování

Konfigurace DNS

Základní mechanismy bezestavové konfigurace nepodporují konfiguraci DNS serverů, což je vzhledem tvaru adres IPv6 obrovská nevýhoda. Proto bylo definováno RFC 6106, které doplňuje dvě nové volby pro DNS do ohlášení směrovače bezestavové konfigurace:

- **RDNSS** (*Recursive DNS Server*) – volba Rekurzivní DNS server poskytuje IPv6 adresy místních DNS serverů.
- **DNSSL** (*DNS Search List*) – tato obsahuje doménová jména místo adres IPv6. Princip je založen na vyhledávání a postupném doplňování jmen z prohledávacího seznamu, pokud nebylo jméno zadáno absolutně (končí tečkou).

Pokud například prohledávací seznam obsahuje záznam *cvut.cz*, tak je z daného počítače přístup na stránky *www.cvut.cz* možný pouhým zadáním *www*. Počítač se prvně pokusí najít v DNS serveru adresu IPv6 pro jméno *www* a když neuspěje, bude opakovat pokus s příponou *www.cvut.cz*.

V případě volby RDNSS, kdy volba obsahuje více adres, mají všechny adresy stejnou životnost. Pokud je žádoucí, aby každá adresa rekurzivního DNS serveru měla jinou životnost, je nezbytné pro každou adresu poslat jednu zprávu Ohlášení směrovače, která bude obsahovat volbu RDNSS s danou životností. Doporučená doba životnosti se pohybuje v rozmezí od maximálního intervalu mezi ohlášeními směrovače do jeho dvojnásobku. Životnost s nulovou hodnotou má speciální význam, zakazuje používat příslušný DNS server.

Při každém novém příjmu Ohlášení směrovače s volbou RDNSS dojde na základě jejího obsahu k aktualizaci existujících záznamů, tedy k prodloužení doby životnosti, přidání nových DNS serverů či vyřazení těch, které mají nulovou životnost. Doporučený počet DNS serverů je stanoven na hodnotu 3. Jestliže přidáním nových serverů dojde k překročení tohoto počtu, budou ze seznamu vyřazeny ty, které mají nejkratší životnost.

RFC 6106 počítá i se situací, kdy dochází ke kombinaci ohlášení směrovače od obou automatických konfigurací. V takovém případě, si počítač uchová minimálně jeden záznam od každého aktivního mechanismu.

8 DHCPv6

8.1 Základy protokolu DHCPv6

DHCP (*Domain Host Configuration Protocol*) je služba založená na modelu server-klient, která koncovému systému, klientu, přidělí všechny potřebné parametry pro plnohodnotnou práci v počítačové síti (tj. adresu, síťovou masku, adresu DNS serverů atd.).

DHCPv6 proces pracuje v bezestavovém nebo stavovém režimu.

- Ve **stavovém režimu** (*stateful mode*), jsou klientům přidělovány všechny parametry, tj. nejen adresa a maska sítě, ale i adresy NTP nebo DNS serverů. DHCPv6 server má přehled o všech přidělovaných adresách a je schopen obsluhovat každého klienta samostatně.

- **Bezestavový režim** (*stateless mode*) se používá v situaci, kdy adresy a maska jsou klientem obdrženy bezestavovou službou SLAAC a DHCPv6 mechanismus je použit pro získání dalších parametrů, které nemohou být dodané bezestavovou službou SLAAC. Ve zprávě RA (*Router Advertisement*) je k tomuto účelu vyhrazen příznak s názvem "O" (*other stateful configuration*) ostatní stavové konfigurace. Tento příznak instruuje klienta dotázat se DHCPv6 serveru. Neobsahuje-li zpráva RA žádnou informaci o RDNSS, pak se klient může dotázat DHCPv6 serveru bez ohledu na to, zda příznak "O" je nastaven nebo ne (viz RFC4339).

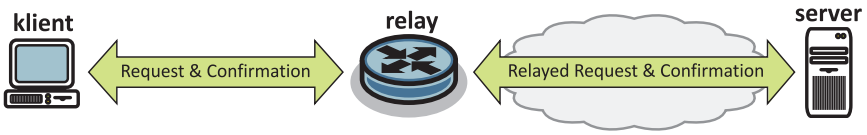
8.2 Komponenty DHCPv6

Procedura DHCPv6 sestává ze třech komponent

- Klient – koncový bod, který se dotazuje na informace
- Server – poskytuje informace
- Relay – zprostředkovatel spojení mezi klientem a serverem, pokud klient a server jsou v různých sítích

Agent je společný termín pro servery nebo relay.

Agent je ten, kdo poskytuje DHCP odpověď (ať už vlastní nebo zprostředkovanou) a nachází se v lokální síti.



Komponenty DHCPv6.

8.3 Identifikace DHCPv6

Identifikace klientů a serverů hraje velmi důležitou roli v DHCPv6 proceduře.

Předchozí verze (DHCP pro IPv4) používá MAC adresu síťového rozhraní jako unikátní klientský identifikátor. V DHCPv6 jsou nově definovány dva nové klientské identifikátory.

- **DUID** (*DHCP Unique identifikátor*)
- **IA** (*Identity Association*)

DUID je automaticky generován při prvním spuštění (boot) operačního systému a je vytvořen na základě parametrů spojové vrstvy nebo parametrů spojové vrstvy a času bootu. Většina implementací jako výchozí obvykle používá druhou možnost. To způsobuje závažný problém, neboť správce sítě není schopen určit DUID nově přidaných klientů před prvním připojením a se mění s každou přeinstalací operačního systému. Každý klient nebo server má jen jeden vlastní DUID.

IA je jedním z parametrů souboru konfiguračních parametrů jednoho rozhraní, vybaven unikátním identifikátorem (IAID).

Klient je jednoznačně identifikován svým **DUID**, klientova rozhraní se pak liší podle **IA**.

8.4 Fáze DHCPv6 dialogu

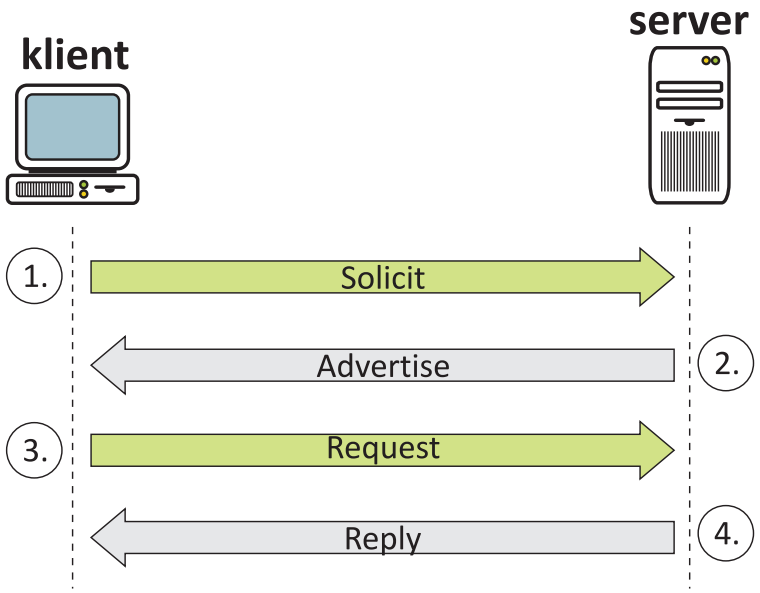
Postup dialogu se ve DHCPv6 výrazně nezměnila v porovnání s jeho předchůdci. DHCPv6 konfigurace je nezbytné ve čtyřech krocích:

1. **Solicit** – klient hledá přátelské servery. Vzhledem k tomu, že klient neví nic o síti odešle svůj požadavek na multicastovou adresu. Žádost obsahuje všechny identifikační údaje (DUID a IA).

2. **Advertise** – odpověď serveru na dotaz "*Solicit*", kterým server dává na vědomí, že je k připraven pro službu DHCP. Zprávu odesílají servery, které jsou ochotny přiřadit klientům parametry (obvykle jen jeden, ale není to podmínkou).

3. **Request** – klient vybere nabídku, která se mu zdá být nejlepší, odpovídající server odešle požadavek na udělení nabízených parametrů.

4. **Confirm** – celý proces končí odesláním potvrzení, kterým server potvrdí, že přiřadil požadované parametry.



Postup DHCPv6 dialogu.

Multicastové adresy přidělené proceduře DHCPv6

- FF02::01:02 – všechny DHCPv6 agenti a servery (je to link-local adresa!)
- FF05::01:03 – všechny DHCPv6 servery

8.5 Životní cyklus DHCPv6, zabezpečení

Použitelnost adres

Přiřazené adresy jsou přidělovány na omezenou dobu.

V polovině doby pronájmu adresy musí klient zažádat o její prodloužení.

Všechny činnost DHCPv6 proceduře zahajuje obvykle klient. Nicméně, jsou situace, ve kterých server sám vyvolá DHCPv6 dialogu. Např. síťové změny, které vyžadují, aby se klienti nové situaci přizpůsobili.

Zabezpečení

Někteří správci sítě mohou chtít zavést ověření zdroje a obsahu DHCPv6 zpráv. Např. klienti mohou být předmětem útoku typu DoS pomocí fiktivních serverů DHCPv6, nebo může neúmyslně dojít ke zmatečné konfiguraci vlivem existence více instancí jednoho DHCP serveru.

Klient, který požaduje ověření DHCPv6 komunikaci, vloží rozšiřující záhlaví "*Authentication option*" do zprávy Solicit. Server odpoví zprávou Advertise, ve které je povinně obsaženo záhlaví "*Authentication option*". Informace nesené v tomto rozšiřujícím záhlaví mohou být použity k spolehlivě identifikaci zdroje DHCPv6 zpráv a potvrzení, že obsah zprávy nebyl narušen.

9 DNS

9.1 DNS

DNS je hierarchický systém doménových jmen, který je realizován DNS servery a DNS protokolem. Součástí DNS Systému jsou jak pravidla pro tvorbu doménových jmen i domén samotných, tak i mechanismy pro vzájemný převod doménových jmen a IP adres uzlů sítě. RFC 1035 definuje základy DNS protokolu. Doménová jména slouží pro pohodlí uživatelů a umožňují používat místo IP adres symbolická jména uzlů sítě, která jsou uspořádaná do hierarchické struktury.

Dále jsou v textu uvedeny pouze změny a rozdíly v DNS, které si vyžádala implementace IPv6. Proto je nezbytné, aby měl čtenář základní znalosti DNS protokolu.

Podpora DNS v prostředí IPv6 byla složitá a urazila dlouhou cestou, než se stabilizovala. Současná implementace DNS v prostředí IPv6 řeší dva problémy:

- ukládání IPv6 adres do DNS – v současné době tento problém řeší RFC 3596.
- komunikace mezi DNS serverem a klientem po IPv6 – komunikace je otázkou implementace DNS serverů a tedy jejich správců.

Tyto problémy jsou do značné míry nezávislé. Klient může klidně s DNS serverem komunikovat prostřednictvím protokolu IPv4 a vyměňovat si informace o IPv6 a naopak.

Existuje několik informativních RFC dokumentů, které se zabývají otázkami soužití IPv6 s DNS. RFC 3901 se zabývá rekurzivními servery umístěných v koncových sítích, které řeší dotazy místních klientů. RFC 4074 popisuje možné chybové stavy DNS serverů v případě, že obdrží dotaz na záznam typu AAAA. A RFC 4472 komplexně popisuje problematiku soužití IPv6 s DNS. Zabývá se především otázkami typu: "Jaké IPv6 adresy by se měli či neměli zapisovat do DNS?" a "Jaký protokol by se měl použít v případě, že počítač má k dispozici oba protokoly?". Odpovědi na obě otázky jsou stručně popsány dále v textu.

9.2 IPv6 Adresy v DNS

IPv6 adresy se ukládají do DNS stejným způsobem jako v případě IPv4. Klient pro komunikaci s DNS serverem používá následující typy dotazů:

- Dopředné dotazy
- Reverzní dotazy

Dopředné dotazy

Pro dopředný dotaz byl zaveden nový typ záznamu AAAA. Název je odvozen z délky IPv6 adresy, která je čtyřnásobná v porovnání s IPv4 adresou. V případě IPv4, se pro podředný dotaz používá záznam A.

Má-li počítač *host.cvut.cz* adresu 2001:718:8DE:128:3201:A1FF:FE67:12, bude v zónovém souboru pro doménu *cvut.cz* obsažen záznam:

```
host   IN   AAAA   2001:718:8DE:128:3201:A1FF:FE67:12
```

Příklad záznamu AAAA v zónovém souboru

Potom definice domény *cvut.cz*, ve které se nachází jeden autoritativní server a jeden počítač, může vypadat následovně:

```
$ORIGIN cvut.cz
@  IN  SOA server.cvut.cz. root.server.cvut.cz. (
       2012040400  ; serial
       28800       ; refresh
       14400       ; retry
       3600000     ; expire
       86400       ; default_ttl
       )

; DNS servery
         IN    NS        server

; adresy počítačů
server   IN    AAAA      2001:718:8DE:128:12:67FF:FE1A:3201
host     IN    AAAA      2001:718:8DE:128:3201:A1FF:FE67:12
```

Příklad zónového souboru

V okamžiku, kdy síť používá více prefixů, mají počítače typicky více adres. Potom každá adresa musí mít i odpovídající záznam AAAA v DNS serveru.

Reverzní dotazy

Reverzní dotaz slouží k získání doménového jména ke známé IPv6 adrese. Stejně jako v případě IPv4 se používají záznamy PTR. Reverzní dotaz je tvořen obráceným pořadím šestnáctkových číslic z IPv6 adresy k jejímuž konci se připojí doména ip6.arpa. IPv6 adresa musí být kompletní. Tedy, musí obsahovat všechny nuly. Reverzní dotaz pro výše uvedenou adresu 2001:718:8de:128:3201:A1FF:FE67:12 má tvar:

```
2.1.0.0.7.6.E.F.F.F.1.A.1.0.2.3.8.2.1.0.E.D.8.0.8.1.7.0.1.0.0
.2.ip6.arpa
```

Příklad reverzního dotazu

Díky obrácenému pořadí číslic se prefix dostává na konec, což umožňuje realizovat distribuovanou správu reverzních domén.

Má-li síť CVUT prefix 2001:718:8DE::/48, dostane do správy reverzní doménu E.D.8.0.8.1.7.0.1.0.0.2.ip6.arpa. Pro počítač *host.cvut.cz*, bude v zónovém souboru pro reverzní doménu záznam:

```
2.1.0.0.7.6.E.F.F.F.1.A.1.0.2.3.8.2.1.0 PTR host.cvut.cz.
```

Záznam pro reverzní doménu

Potom definice reverzní domény, která odpovídá výše uvedené doméně *cvut.cz*, může vypadat následovně:

```
$ORIGIN E.D.8.0.8.1.7.0.1.0.0.2.ip6.arpa.
@       IN      SOA server.cvut.cz. root.server.cvut.cz. (
                2012040400  ; serial
                28800       ; refresh
                14400       ; retry
                3600000     ; expire
                86400       ; default_ttl
                )

; DNS servery
        IN      NS      server

; reverzní záznamy
1.0.2.3.A.1.E.F.F.F.7.6.2.1.0.0.8.2.1.0  PTR  server.cvut.cz.
2.1.0.0.7.6.E.F.F.F.1.A.1.0.2.3.8.2.1.0  PTR  host.cvut.cz.
```

Zónový soubor reverzní domény

9.3 Obsah Domén

Každé rozhraní počítače má více IPv6 adres s různým dosahem i životností. Z tohoto důvodu vyvstala otázka: "Jaké IPv6 adresy ukládat do DNS? Rozhodně by to měli být všechny globální individuální adresy s dlouhodobější platností a dlouhodobě platné adresy přechodových mechanismů. Naopak do DNS nepatří lokální linkové adresy a náhodně generované krátkodobé adresy, které se používají pro zachování soukromí.

Pro ostatní IPv6 adresy, zejména ty, které jsou přiděleny bezstavovou či stavovou konfigurací, neexistuje univerzální doporučení. Tyto adresy mají většinou krátkodobou platnost, proto jejich zapsání by vyžadovalo nasazení dynamické aktualizace DNS.

Další otázka vyvstává v okamžiku, kdy počítač komunikuje prostřednictvím obou protokolů: "Jaký typ adresy má počítač použít?" Nabízejí se dva základní přístupy:

- Stejné doménové jméno pro oba typy adres
- Odlišná doménová jména pro jednotlivé typy adres

Stejné doménové jméno

Má-li počítač *host.cvut.cz* IPv4 adresu 192.168.121.57 a IPv6 adresu 2001:718:8DE:128:3201:A1FF:FE67:12, bude v zónovém souboru pro doménu *cvut.cz* obsažen záznam:

```
host    IN      A       192.168.121.57
        IN      AAAA    2001:718:8DE:128:3201:A1FF:FE67:12
```

Příklad záznamů pro stejné doménové jméno

Pokud bude chtít počítač *pc* komunikovat s počítačem *host.cvut.cz*, pošle mu DNS server obě dvě adresy a počítač *pc* si na základě typu připojení vybere vhodnou adresu. V okamžiku, kdy počítač *pc* má k dispozici oba typy protokolů, bude mít IPv6 adresa přednost, protože současné operační systémy upřednostňují IPv6.

Tento přístup však z důvodu současně nedostatečné implementace IPv6 není zcela spolehlivý. Pokud se nepodaří navázat spojení prostřednictvím IPv6, dojde v případě TCP komunikace k navázání spojení prostřednictvím IPv4. TCP protokol disponuje mechanismy pro bezpečné doručování dat, díky kterým zjistí, že je IPv6 síť nefunkční. Interval potřebný pro detekci nefunkčnosti IPv6 sítě může být až několik minut. V případě UDP komunikace, k navázání spojení nedojde vůbec.

Odlišná doménová jména

V případě odlišných doménových jmen bývá zvykem uvést pod-doménu (často nazvanou ip6 nebo ipv6), ve které jsou zařazeny IPv6 adresy daného počítače. Použití komunikačního protokolu tedy přímo vyplývá z doménového jména.

Potom pro počítač *host.cvut.cz* by měl zónový soubor obsahovat následující záznam:

```
host          IN      A       192.168.121.57
host.ip6      IN      AAAA    2001:718:8DE:128:3201:A1FF:FE67:12
```

Příklad záznamů pro odlišná doménová jména

S velkou pravděpodobností se však jedná o dočasnou variantu, než bude implementace IPv6 stoprocentně dostupná.

10 Mobilita

10.1 Podpora mobility v IPv6

IPv6 umožňuje zařízením zůstat dosažitelné i při pohybu v IPv6 prostoru Internetu. Každé mobilní zařízení je jednoznačně identifikováno svou domácí adresou, bez ohledu na jeho aktuální umístění v Internetu. V době, kdy se nachází mimo svůj domov, je mobilní zařízení přiřazena dočasná adresa, která zprostředkuje informace aktuálním umístění mobilního zařízení. IPv6 pakety adresované na domovskou adresu mobilního zařízení jsou transparentně směrovány na tuto dočasnou adresu. Protokol umožňuje mobilnímu zařízení ukládat si do mezipaměti vazbu mezi domovskou a dočasnou adresou, přesměrovat zasílání paketů určených pro mobilní zařízení přímo na jeho dočasnou adresu.

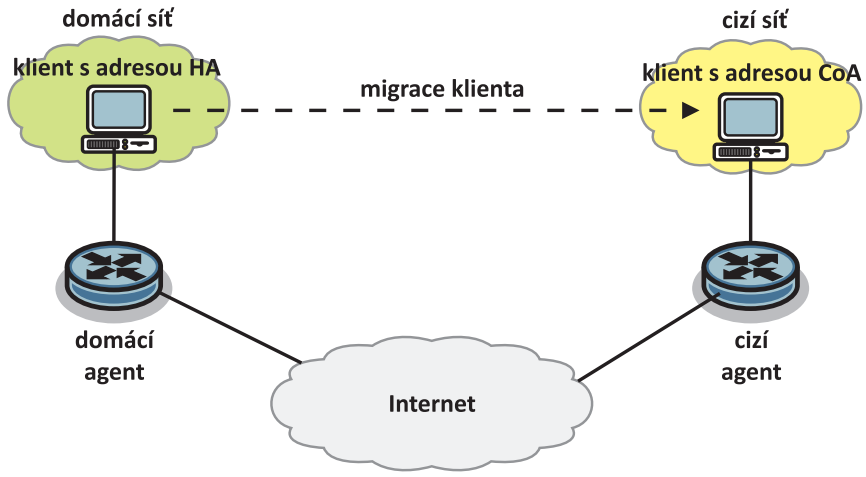
Mobilní zařízení mohou komunikovat se všemi IPv6 zařízeními, ať už mobilními nebo stacionárními.

10.2 Základní princip mobility v IPv6

Každé zařízení, dokonce i mobilní, je někde doma.

V domovské síti si mobilní zařízení registruje svoji domácí adresu **HA** (*Home address*), která je fixní a pevně svázána s DNS záznamem. Toto mobilní zařízení ustanoví také tzv. domácího agenta, který shromažďuje informace o mobilních zařízeních, jejichž trvalé adresa je v domovské síti agenta.

V době, kdy se nachází mimo svou domácí síť, registruje si mobilní zařízení dočasnou adresu, **CoA** (*Care-of Address*), která je svázána se sítí, ve které se mobilní zařízení zdržuje, a ustanoví si cizího agenta. Pokud cizí agent není v hostující síti k dispozici, mobilní zařízení se musí vlastními prostředky postarat o získání adresy a její propagaci do domácí sítě.

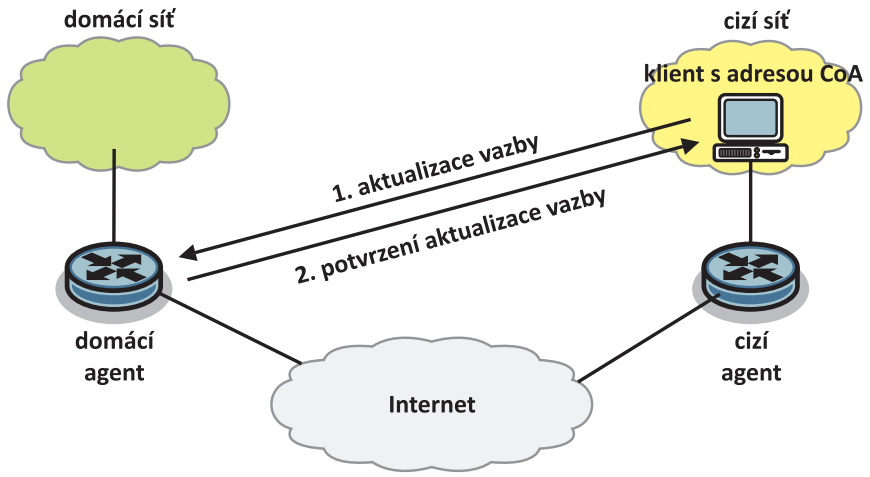


Základní IPv6 mobility scénář

Mobilita v IPv6 specifikuje, jakým způsobem se mobilní zařízení registruje svému domácímu agentu a jak se směrují data do mobilního zařízení přes tunel mezi domácím a cizím agentem.

10.3 Mobilní vazba v IPv6

Vztah mezi domácí adresou mobilního zařízení HA a dočasnou adresou CoA se nazývá vazba (*binding*) pro mobilní zařízení. V době, kdy se mobilní zařízení nachází mimo svou domácí síť, registruje si primární dočasnou adresu, CoA, a prostřednictvím cizího agenta si vytvoří vazbu se svým domácím agentem. Toto nastavení vazby provádí mobilní zařízení odesláním zprávy "*Binding Update*" svému domácímu agentu. Domácí agent potvrdí akci zasláním zprávy "*Binding Acknowledge*".

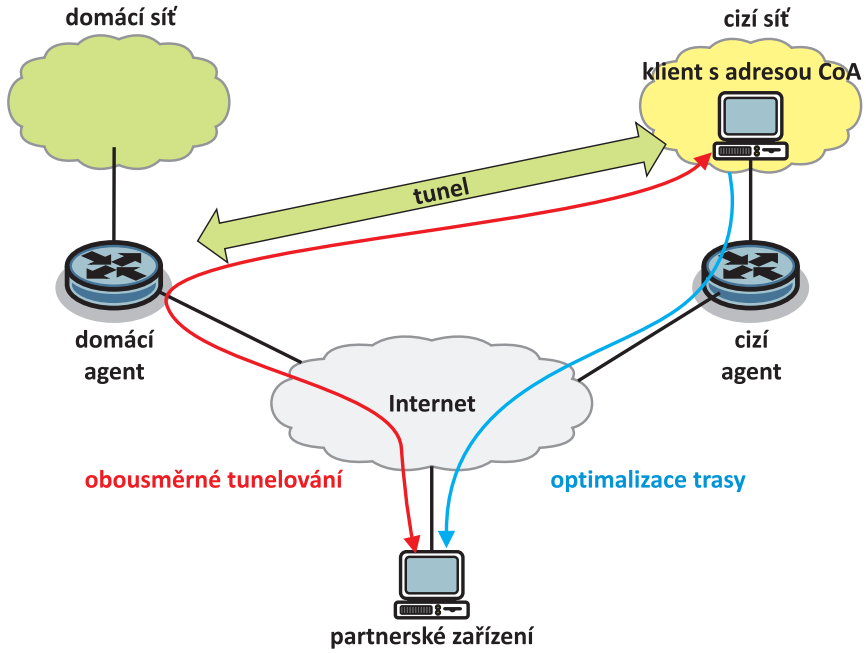


Mobilní vazba v IPv6

10.4 Scénáře směrování

Pro komunikaci mezi mobilním zařízením s okolím existují dva možné scénáře

- **Obousměrné tunelování** (*Bidirectional Tunneling*) – to je k dispozici i v případě, že mobilní zařízení nemá registrovánu svou současnou vazbu s partnerským zařízení.
    - Pakety **od** partnerského zařízení jsou směrovány domácímu agentu a pak tunelovány do mobilního zařízení.
    - Pakety **do** partnerského zařízení jsou tunelovány z mobilního zařízení k domácímu agentu (reverzní tunelování) a pak směrovány normálním způsobem z domácí sítě partnerskému zařízení.
- **Optimalizace trasy** (*Route Optimization*) – vyžaduje, aby existovala vazba nejen mezi mobilním zařízením a domácím agentem, nýbrž i vazba mezi mobilním zařízením a partnerským zařízením.
    - Pakety **od** partnerského zařízení jsou směrovány přímo na CoA adresu mobilního zařízení.
    - Při odesílání paketu na jakoukoli IPv6 destinaci, mobilní zařízení prohledává svou vyrovnávací paměti vazeb. Pokud je tato destinace nalezena, mobilní zařízení směruje data přímo s využitím záhlaví "*IPv6 routing header*".



Scénáře směrování pro IPv6 mobilitu

11 Mechanismy přechodu z IPv4 na IPv6

11.1 Přehled přechodových mechanismů

Není možné skokově přejít ze stávajícího protokolu IPv4 na nový protokol IPv6. Proto jsou třeba mechanismy, které umožní současný provoz obou protokolů. Pro existenci a vzájemnou spolupráci obou protokolů existuje celá řada návrhů. Tyto návrhy lze rozdělit do tří skupin:

- Dvojí zásobník (*Dual Stack*) – příslušné zařízení obsahuje oba protokoly, což umožňuje komunikaci mezi IPv4 a IPv6 světem. Kooperace mezi oběma protokoly se odehrává až na aplikační vrstvě, pokud je tedy zapotřebí. Odpovídající aplikace si vyzvedne data, která dorazila jedním protokolem, a v závislosti na svých vlastnostech a případné konfiguraci je upraví a odešle druhým protokolem danému příjemci. Tento princip není ideální, protože se počítá s existencí IPv4 i do budoucna. Nicméně je východiskem pro zbývající dvě skupiny, protože všechny další způsoby totiž vyžadují, aby alespoň některá zařízení podporovala oba protokoly.

- Tunelování – tunely se používají ke spojení dvou IPv6 sítí prostřednictvím sítě IPv4, kde se IPv6 datagram přenáší zabalený jako data v IPv4 datagramu.

- Translátory (překladače) – zprostředkovávají styk obou protokolů. Překladače překládají IPv6 datagramy na IPv4 datagramy a naopak.

Stručný seznam přechodových mechanismů je uveden v následující tabulce. Tabulka obsahuje i RFC dokumenty, kde jsou podrobněji popsány jednotlivé mechanismy.

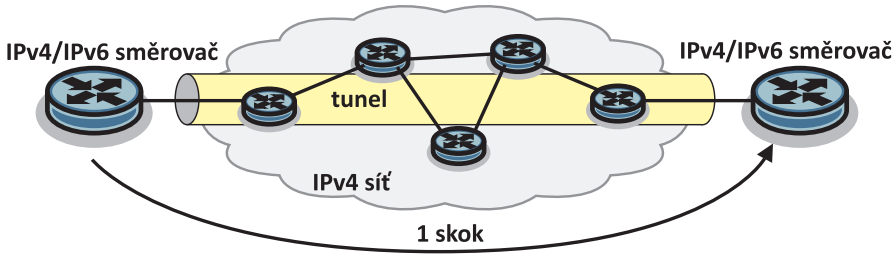
Seznam přechodových mechanismů

tunelování		translátory	
tunel server/broker	RFC 3053	SIIT	RFC 6145
6to4	RFC 3056	NAT64	RFC 6146
6rd	RFC 5569	TRT	RFC 3142
6over4	RFC 2529	BIH	draft
ISATAP	RFC 5214	SOCKS64	RFC 3089
Teredo	RFC 4380		
Dual-Stack Lite	RFC 6333		

V následujících kapitolách jsou uvedeny pouze obecné principy tunelování a překládání.

11.2 Tunelování

Obecný princip tunelování je zobrazen na následujícím obrázku.



Mechanismus tunelování

Každý tunel má obecně dva konce a každý konec má svoji vlastní IP adresu. Pokud se zařízení rozhodne na jednom konci, na základě směrovací tabulky nebo speciální adresy příjemce v příchozím IPv6 datagramu, že daný IPv6 datagram má odeslat tunelem, vezme jej a vloží jako data do nově vytvořeného IPv4 datagramu. Cílová adresa nového IPv4 datagramu bude IPv4 adresa druhého konce tunelu a jako adresa odesilatele se vezme IPv4 adresa zdejšího konce tunelu. Do položky Protokol v IPv4 datagramu se uloží hodnota 41, čímž dá najevo, že se jedná o tunelovaný IPv6 datagram.

Datagram se odešle běžným způsobem sítí IPv4 na druhý konec tunelu. Podle hodnoty 41 v položce Protokol pozná příjemce na druhé straně tunelu, že obdržel tunelovaný IPv6 datagram. Příjemce IPv6 datagram vybalí a dále zpracuje na základě jeho cílové IPv6 adresy a IPv6 směrovací tabulky příjemce. Z hlediska IPv6 je celý průchod tunelem počítán za jeden skok a zařízení na druhé straně tunelu (směrovač) zmenší položku Maximální počet skoků v IPv6 záhlaví o jedna.

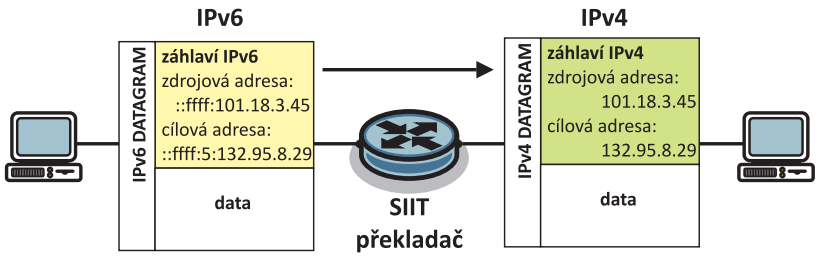
V případě spolupráce IPv4 a IPv6 se používají dva režimy tunelování:

- Manuální – tunely jsou ručně nastaveny správcem. Detailnější popis lze nalézt v RFC 4213.
- Automatické – vznikají samy na základě obsažených informacích v adresách. Detailnější popis lze nalézt v RFC 2893.

11.3 Translátory

Obecná sada pravidel překládání jednotlivých položek záhlaví datagramu, kterou používají v základě všechny překladače, je definována v RFC 2765: *Stateless IP/ICMP Translation Algorithm (SIIT)* a RFC 6145: *IP/ICMP Translation Algorithm*. Tato sada pravidel je značně omezena a nepodporuje žádná rozšíření, jako jsou volby ze strany IPv4 nebo rozšiřující záhlaví IPv6. To znamená, že překladače tyto rozšíření zahazují.

Translátory překládají každý datagram samostatně, bez vazeb na předchozí datagramy a bez uchování datových struktur s informacemi o historii či aktuálním stavu probíhající komunikace. Průchodu datagramu SIIT překladačem je znázorněn na následujícím obrázku.



Průchod datagramu SIIT překladačem

Součástí překladu je i mapování adres. To je převod IPv6 adres na IPv4 adresy a naopak. K tomu se aktuálně používají adresy obsahující IPv4 adresy (*IPv4-embedded*). Tyto adresy mají vyhrazen obvykle 96 bitový prefix, za který přidávají IPv4 adresu. Může se jednat buď o univerzální prefix 64:FF9B::/96, nebo lokální prefix přidělený místním správcem. Formát adres obsahující IPv4 adresy je popsán v RFC 6052.

Převod IPv4 adresy na IPv6 adresu lze provádět bezestavově. To znamená, že za daný IPv6 prefix se připojí IPv4 adresa. V opačném případě už to tak jednoduché není. Nejčastěji se používá dynamické mapování podobné převodu adres, které využívá **NAT** (*Network Address Translation*).