1. 2 Protokol IP verze 6

1.2.1 Nedostatky protokolu IPv4

Donedávna byl provoz v Internetu na úrovni síťové vrstvy zajišťován výhradně protokolem IP verze 4 (IPv4) definovaným v RFC791. Tento protokol je již po mnoho let provozován pouze s minimálními změnami[1]. Díky masovému nárůstu počtu připojených zařízení (včetně zařízení jako PDA, mobilní telefony či výrobky spotřební elektroniky) se však koncem devadesátých let ukázalo, že přestává dostačovat původně navržený prostor IP adres. Zejména se ukázal omezující způsob dělení tohoto prostoru na třídy A,B a C, který neodpovídá současné realitě velmi variabilního počtu stanic v jednotlivých nově připojovaných sítích. Ačkoli byl před časem velmi ožehavý problém nedostatku IP adres dočasně vyřešen zrušením tříd a přidělováním délek prefixů sítí podle reálné potřeby a hlavně obecným rozšířením využívání privátních adres překládaných na malý počet veřejných pomocí mechanismu NAT (Network Address Translator), není toto řešení výhodné proto, že neumožňuje univerzální komunikaci a jednoznačnou adresovatelnost všech do Internetu připojitelných zařízení. Právě s cílem vyřešit problém nedostatku adres byl v roce 1995 navržen protokol IP verze 6[2]).

Jelikož je návrh a zejména široká implementace nového protokolu síťové vrstvy pro prostředí Internetu záležitostí, která se děje jen velmi zřídka, bylo rozhodnuto změny využít a do protokolu zapracovat také další rozšíření, umožňující řešit aktuální požadavky na protokol, se kterými návrháři IPv4 původně nepočítali. Jedná se zejména o následující vylepšení:

- možnost automatické konfigurace adres na základě adres spojové vrstvy (MAC adres) a prefixu získaného od směrovače na dané LAN
- podpora šifrování a autentizace
- podpora pro mobilitu komunikujících stanic
- rozšířená podpora skupinového vysílání (multicast)
- podpora QoS

Přechod na nový protokol není uskutečnitelný ze dne na den a to nejen z organizačních důvodů. V Internetu pracuje velké množství hardware, který IPv6 nepodporuje a nikdy podporovat nebude. Proto se předpokládá několikaletá koexistence obou protokolů a byly navrženy mechanismy, jak současné používání obou těchto protokolů realizovat.

1.2.2 Adresování v IPv6

Při návrhu adresního schematu protokolu IPv6 se autoři poučili z problémů, které přinesly v posledních letech adresy IPv4 a z řešení, jimiž internetová komunita alespoň některé nedostatky obešla. Nedostatek adres byl v IPv6 pravděpodobně jednou pro vždy vyřešen čtyřnásobným prodloužením IP adresy (ta má nyní 16 bajtů) a zavedením víceúrovňové hierarchické struktury adres, která umožní při jejich rozumném přidělování dobrou agregovatelnost směrovacích záznamů

[1] např. upřesnění významu pole Type of Service v hlavičce IP paketu
[2] protokol IP verze 5 existoval pouze ve verzi experimentální

v páteřních směrovačích. Mimo běžných individuálních (unicast) adres IPv6 rovněž rozšiřuje užití adres skupinových (multicast) a zavádí nový speciální typ adresy, tzv. anycast (česky někdy nazývané jako "výběrové adresy"). Jednotlivé třídy adres se odlišují prefixem - nejvýznamnějšími bity adresy.

1.2.2.1 Typy adres v IPv6

Individuální adresy jsou v terminologii IPv6 plným jménem nazývány agregovatelné globální unicast adresy. Standardem RFC2374 původně navrhovaná struktura globální individuální adresy IPv6 se skládala z těchto částí:

- prefix 001 - – příznak, že jde o globální individuální adresu
- Top-Level Aggregation (TLA) - identifikátor autority přidělující adresu
- Next-Level Aggregation (NLA) – identifikátor ISP
- Site-Level Aggregation (SLA) – „podsíť“ v rámci instituce.
- Identifikátor rozhraní (64 bitů) - obvykle bývá zkonstruován dále popisovaným způsobem na základě MAC adresy příslušného rozhraní. To umožňuje automatickou konfiguraci adresy rozhraní bez explicitního zásahu správce.

Délky polí TLA a NLA nebyly pevně určeny, ale byla mezi nimi ponechána rezerva dovolující rozšířit kterékoli z nich podle potřeb praxe. Dvouúrovňový hierarchický systém se však příliš neujal, protože nekopíruje realitu v rozdělování adres mezi poskytovatele, která je velmi různorodá. Proto bylo později od formálního rozdělení na TLA a NLA upuštěno a v současné době se v rámci „veřejné infrastruktury“ přidělují prefixy síťové adresy odpovídající délky podle potřeby. Podstatné je, že pro směrovače není vnitřní struktura adresy tak jako tak zajímavá - orientují se pouze podle prefixu a jeho délky s tím, že paket je přeposílán na základě řádku směrovací tabulky, u kterého se prefix shoduje s prefixem cílové adresy paketu na co největší počet míst.

V obecné struktuře IPv6 adresy bylo pro identifikátor rozhraní vyhrazeno 64 bitů. Ačkoli adresu rozhraní lze obecně nastavit jakkoli, je výhodné ji převzít z MAC adresy, která sama o sobě je již unikátní a na spojové vrstvě využívána většinou současných síťových technologií. Pro identifikátor rozhraní se používá mírně modifikovanému standardu IEEE EUI-64, definujícího celosvětově jednoznačné 64-bitové identifikátory pro síťová rozhraní. Převod MAC adresy na EUI-64 spočívá ve vložené hodnoty FFFEh mezi třetí a čtvrtý bajt (tedy doprostřed) MAC adresy. Mimo to je třeba invertovat příznak globality - ten je u MAC adres umístěn stejně jako v EUI-64 jako druhý nejméně významný bit nejvyššího bajtu, avšak s opačnou logikou). Například z MAC adresy 00:CC:01:A1:D5:80 tak vznikne identifikátor rozhraní s hodnotou 02CC:01FF:FEA1:D580[3].

[3] Všimněme si, že narozdíl od IPv4 můžeme při takovémto způsobu konstrukce identifikátoru rozhraní z IP adresy u IPv6 vyčíst celosvětově jednoznačnou identifikaci fyzického zařízení, se kterým komunikujeme. Jelikož toto může být vnímáno jako zásah do soukromí uživatelů, byly navrženy způsoby, jak s použitím dynamického generování střídavě používaných alternativních adres možnosti identifikace konkrétního zařízení zamezit.

Mimo globálních individuálních adres definuje IPv6 také tzv. lokální individuální linkové adresy (prefix FE80::/10 doplněný zprava o MAC adresu), které mají platnost pouze v rámci lokálního segmentu a používají se pro vysílání paketů některých podpůrných protokolů. Také existuje obdoba privátních adres známých z IPv4, tzv. lokální individuální místní (angl. „site“) adresy začínající prefixem FEC0::/10.

Dalším zajímavým rozšířením u protokolu IPv6 je skutečnost, že rozhraní může mít více globálních individuálních adres (tzv. multihoming). To je užitečné např během přeadresování sítě při přechodu k jinému poskytovateli.

Adresy typu multicast (skupinové) slouží pro aplikace, které chtějí zajistit doručení paketu celé skupině příjemců (např. rozhlasové či televizní vysílání po Internetu). Obecná struktura adresy typu multicast vypadá u IPv6 následovně:

- FF00:/8 – prefix skupinové adresy
- příznaky (4b)
- identifikátor dosahu (4b)
- identifikátor skupiny (112b)

Dosah skupiny určuje oblast, v rámci níž mohou být příjemci dané skupiny rozprostřeni (lokální linka, místo, organizace, globální dosah). Skupiny v IPv6 se dále dělí na obecně známé permanentní (well-known) a dočasné (transient). Lze to rozeznat podle jednoho z příznakových bitů. Identifikátory permanentní skupiny jsou plošně (tj. nehierarchicky) přidělovány organizací IANA a jsou nezávislé na dosahu - bez ohledu na dosah vždy identifikují tutéž skupinu. Naopak identifikátory u adres transientních skupin jsou vždy unikátní pouze v rámci svého dosahu. Stejný identifikátor v rámci dvou různých tranzientních skupinových adres lišících se pouze dosahem tak vždy označuje různé skupiny. Problém přidělování jednoznačných multicastových adres navrhuje IPv6 řešit také na základě adres odvozených z přidělených prefixů adres individuálních (tzv. unicast-prefix-based adresy).

Ačkoli má pole identifikátoru skupiny délku 112 bitů, v současné době se předpokládá použití pouze nejnižších 32 z nich (zbývajících bity jsou nulové). Ty pak lze snadno mapovat na šestibajtové MAC adresy - první dva bajty multicastových MAC adres nesoucích pakety IPv6 pro skupinovou adresu mají hodnotu 3333h, zatímco zbývající čtyři jsou přímo zkopírovány z 32-bitového identifikátoru skupiny. Tím bylo dosaženo jednoznačnosti mapování skupinových adres IPv6 na MAC adresy, které bylo u protokolu IPv4 víceznačné.

Nově zavedeny byly tzv. výběrové adresy, nebo-li adresy adresy typu anycast. Výběrová adresa může být přiřazena několika různým fyzickým rozhraním a to i rozprostřeným v rámci WAN. Pakety zaslané na adresu anycast jsou doručeny některému (nejbližšímu) rozhraní s touto adresou. Smyslem je zajistit vyhledání nejbližšího člena nějaké skupiny (např. proxy DNS serverů). Takovéto mechanismy mohou být užitečné pro automatické vyhledávání různých služeb nebo pro rozkládání zátěže mezi redundandní servery. Směrování na adresy typu anycast může být zajištěno propagováním této adresy ("host route") z několika zdrojů. V současné době jsou mechanismy související s využitím adres typu anycast spíše ve stádiu experimentálním a to zejména kvůli

nevyjasněnosti některých aspektů bezpečnosti a návaznosti na vyšší vrstvy a protokoly stavového charakteru, zejména použití spolu s protokolem TCP.
Adresy typu anycast nemají speciální prefix, jsou totiž zařazeny pod stejný prefix, jako adresy individuální. Z pohledu na adresy tak není možné rozhodnout, zda se jedná o adresu individuální nebo anycast.
Všimněme si rozdílu skupinových adres oproti adresám výběrovým. Zatímco paket zaslaný na výběrovou adresu má být doručen některému členu skupiny, paket zaslaný na adresy skupinovou je určen pro všechny členy skupiny. Také si všimněme, že IPv6 zcela vypustila adresu typu broadcast. Její dosah byl u IPv4 totiž reálně omezen na jeden segment sítě, takže se ukázalo vhodnější nahradit ji pro každý jednotlivý způsob použití samostatnou adresou typu multicast s příslušným dosahem.

1.2.2.2 Zápis adres

Adresy IPv6 mají 128 bitů, tedy 16 bajtů. Zapisujeme je na rozdíl od IPv6 v hexadecimálním tvaru, vždy po dvojicích bajtů oddělených dvojtečkami, například
FEDC:02A5:0000:002A:00C0:7600:0C12:1C47

Nevýznamné (úvodní) nuly každé čtveřice můžeme z výše uvedeného zápisu vypustit a adresu zapsat jako FEDC:2A5:0:2A:C0:7600:C12:1C47. Jelikož často bývá delší část adresy nulová, můžeme více následných nulových bitů vyjádřit symbolem "::". Například adresu FEDC:02A5:0000:0000:00C0:7600:0C12:1C47 můžeme zkrátit na FEDC:2A5::C0:7600:C12:1C47. Použili jsme zde navíc možnost vypustit nevýznamné úvodní nuly. Zápis "::" se může vyskytovat i na začátku nebo konci adresy, např. ::FE12:CCD0 nebo DC80:FD87:A800:: Dvě dvojtečky na začátku adresy využijeme zejména u tzv. IPv4-kompatibilních adres (viz dále); dvě dvojtečky na konci zase při zápisu prefixu, kde nevýznamné pozice v pravé části adresy jsou všechny nulové. Všimněme si, že z důvodu jednoznačnosti se zápis "::" může v adrese objevit pouze jednou. Např. adresu FD08:0000:0000:DAC8:0000:0000:0000:DACD můžeme zapsat jako FD08::DAC8:0000:0000:0000:DACD nebo FD08:0000:0000:DAC8::DACD. Kdybychom použili (nesprávného) zápisu FD08::DAC8::DACD, nebyla by adresa jednoznačná, jelikož by ze zápisu nebylo zřejmé, kolik nulových pozic reprezentuje první a kolik druhý výskyt symbolu "::".

Poslední variantou, jak vyjádřit adresu IPv6, je zápis tzv. IPv4-kompatibilních adres. Ty byly zavedeny z důvodu koexistence s adresami IPv4. IPv4-kompatibilní adresy mají prefix 0:0:0:0:0:0, poslední dvě čtveřice hexadecimálních číslic se však zapisují jako čtyři dekadické hodnoty bajtů adresy IPv4 oddělených tečkami. Například 0:0:0:0:0:0:158.196.1.10.

Často potřebujeme vyjádřit také prefix adresy. Počet bitů tvořících prefix zapisujeme za lomítko za hodnotu prefixu, zapsanou podle konvencí zápisu adres IPv6. Jedná se o stejný zápis, na jaký jsme již zvyklí z beztřídního adresování u IPv4 (CIDR). Například 60-bitový prefix s hodnotou AAAABBBBCCCCDDDh zapíšeme AAAA:BBBB:CCCC:DDD0::/60 Zápisem "::" na konci prefixu dáváme najevo, že zbývající bity adresy jsou z pohledu prefixu nevýznamné, a mohou být stejně jako při označování sítí jako takových u adres protokolu IPv4 chápány jako nulové. Adresa ::0/128 je používána jako tzv. nedefinovaná adresa. Používá se pro vyjádření faktu, že adresa

nějakého rozhraní doposud nebyla přiřazena. Adresa ::1/128 je představuje zpětnovazební smyčku (loopback) a odpovídá adrese 127.0.0.1 používané pro tento účel u IPv4.

1.2.2.3 Automatická konfigurace

Při návrhu IPv6 byl kladen důraz na to, aby uživatelé při připojení do sítě nemuseli pokud možno nic nastavovat a aby jim všechny potřebné parametry pro síťovou komunikaci byly přiděleny automaticky službami v sítí. K tomu účelu IPv6 nabízí dvě možnosti – tzv. stavovou a bezestavovou automatickou konfiguraci.

Stavová konfigurace předpokládá zprovoznění speciálního serveru, který parametry připojení na žádost přiděluje. Jde o stejný princip jako u známého protokolu DHCP (Dynamic Host Configuration Protocol, RFC2131), hojně používaného v IPv4. Protokol DHCPv6, určený pro přidělování parametrů v IPv6 má oproti klasickému DHCP některá rozšíření, avšak princip zůstává stejný – stanice nejprve s použitím skupinové adresy vyhledá DHCP server, který ji nabídne na určitou dobu pronájem jisté síťové adresy a spolu s ní další parametry, jako výchozí bránu a adresu DNS serveru. Stanice si jednu z nabídek vybere a s DHCP serverem, který tuto adresu nabídnul, si požadavek na přidělení vzájemně potvrdí.
Je pamatováno i na případ, kdy chceme jednomu fyzickému zařízení přidělovat pokaždé tutéž adresu – na rozdíl od standardního DHCP však nejsou stanice jednoznačně identifikovány pouze MAC adresou (síťová karta může být vyměněna), ale jsou navrženy i jiné identifikátory odvozené z různých forem jednoznačné identifikace hardware konkrétních stanic.

DHCP server musí být s klienty na témže segmentu, avšak specifikace DHCPv6 pamatuje i na přeposílání požadavků přes prostředníka (proxy). Oproti DHCP pro IPv4 si může v DHCPv6 server aktivně vynutit, aby klient změnil parametry, které mu server předtím přidělil.

Druhou alternativou dynamického přidělování adres v IPv6 je bezestavová konfigurace. Ta nevyžaduje DHCP servery, ale vychází z toho, že stanice si svou adresu zkonstruuje ze své MAC adresy a prefixu lokální sítě, kterou periodicky ohlašuje směrovač na všech rozhraních svých LAN. K tomu se používá zpráva protokolu ICMPv6 Router Advertisement. Směrovač pak rovněž stanici poslouží jako výchozí brána. Pokud stanice nechce čekat celou periodu na zprávu ICMPv6 Router Advertisement, může si její okamžité zaslání všemi směrovači na segmentu vyžádat zprávou ICMPv6 Router Solicitation na skupinovou adresu pro všechny směrovače.

1.2.3 Paket IPv6

1.2.3.1 Hlavička paketu

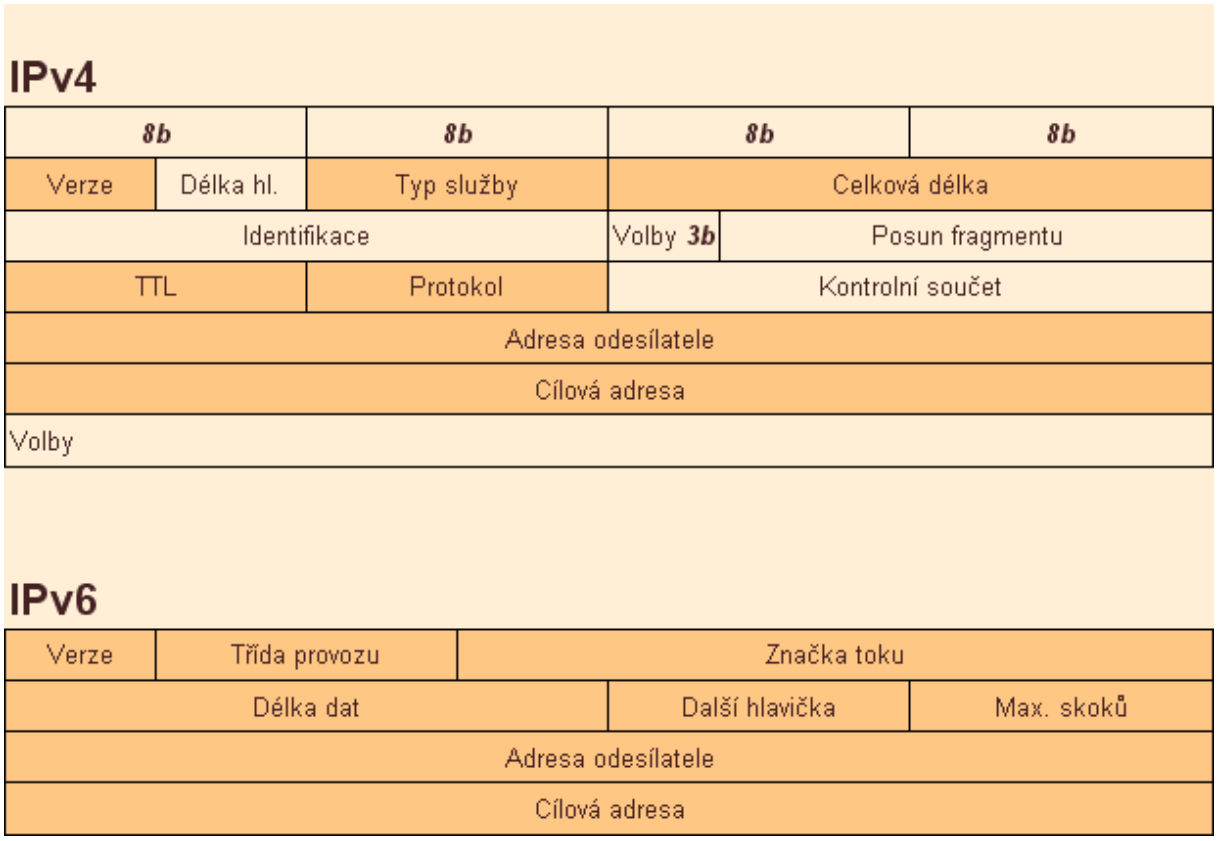
Podíváme-li se na základní formát paketu protokolu IPv6, vidíme, že je oproti paketu IPv4 značně zjednodušen (obr. 1.15). Stejně jako u IPv4 je tvořen hlavičkou a datovou částí, která však může mít délku až 4GB (tzv. Jumbo Packet). Připomeňme, že pakety IPv4 mohou mít délku maximálně 64kB. Hlavička paketu IPv6 byla oproti IPv4 zjednodušena. Mnohá pole byla vypuštěna, některá však také pozměněna nebo i přidána. Zjednodušení hlavičky má za cíl urychlit zpracování paketů, které nevyžadují žádné speciální zacházení. Takovýchto paketů se v síti pohybuje nejvíce. Pakety,

které speciální zacházení vyžadují, si k tomu účelu nesou přídavnou informaci ve volitelných rozšiřujících hlavičkách, které se mohou jedna za druhou řetězit. K rozšiřujícím hlavičkám i mechanismu řetězení se vrátíme později.

Nejdůležitější části základní hlavičky IPv6 je zdrojová a cílová IP adresa. Ty byly v protokolu IPv6 rozšířeny na 16 bajtů. Dále je přítomné pole odpovídající poli Time to Live u protokolu IPv4, kterému však byl upraven název s ohledem na způsob, jakým je pole skutečně využíváno (dekrementace hodnoty při každém průchodu směrovačem a likvidace pravděpodobně cyklujícího paketu v případě dosažení nulové hodnoty).

Novým polem hlavičky je pole Next Header. To umožňuje za popisovanou základní hlavičku volitelně připojit hlavičky další a základní hlavičku minimalizovat (viz kap. 1.2.3.2). Vypuštěním polí, která nejsou u konkrétního paketu využita, se sníží režie a zrychlí zpracování paketů ve směrovačích. Další zrychlení přináší vypuštění kontrolního součtu hlavičky, který se tak nemusí při předávání paketu neustále přepočítávat. Předpokládá se, že zabezpečení zajistí spojová vrstva, nebo vrstvy vyšší.

Dále byla zavedena položka Flow Label. Její použití není doposud přesně specifikováno, ale předpokládá se, že pomůže omezit opakované pomalé a někdy i rekurzivní vyhledávání ve směrovacích tabulkách pro pakety jednoho datového toku. Datovým tokem zde rozumíme posloupnost paketů na některém transportním protokolu (TCP/UDP), vycházející z jisté zdrojové aplikace dané zdrojovou adresou a portem a směřující do cílové aplikace, opět identifikované IP adresou a portem. Podrobněji je předpokládané použití položky Flow Label vysvětleno v kapitole 1.2.5.3.



Obr. 1.15 - Srovnání hlaviček IPv6 a IPv4

1.2.3.2 Řetězení hlaviček

Aby v hlavičkách paketu nebylo nutné rezervovat pole na pomocné mechanismy jako např. fragmentaci, nebo volby, které nemusí být zdaleka vždy použity, byl zaveden princip řetězení hlaviček. Za základní hlavičkou může následovat jedna nebo více tzv. rozšiřujících hlaviček, z nichž každá je chápána jako samostatný blok nesoucí informace týkající se jednoho z rozšiřujících mechanismů. Řetěz obsahuje pouze hlavičky, které jsou v daném paketu nutné. V současné době jsou definovány tyto hlavičky:

- volby pro všechny/volby pro cíl - jedná se o standardní nepovinné volby známé z protokolu IPv4. V IPv6 však byly rozšířeny na volby pro cíl a volby pro všechny prvky na cestě, aby se prvky na cestě nemusely zabývat prohledáváním voleb, které pro ně nejsou určeny
- explicitní směrování – stejně jako v IPv4 lze u paketu určit, přes které směrovače má procházet a to buďto striktním vyjmenováním jednoznačné sekvence směrovačů nebo volným určením jen několika z nich.
- Fragmentace – hlavička nesoucí informace, podle kterých lze složit fragmenty původně jediného paketu, který však musel být z důvodu malého MTU u odesílatele fragmentován na větší počet menších paketů (fragmentů). Je důležité vědět, že IPv6 nedovoluje z důvodu

šetření výkonu fragmentaci na směrovačích, kvůli kompatibilitě se softwarem počítajícím s IPv4 však umožňuje fragmentovat alespoň odesílateli.
- Autentizace odesílatele
- Šifrování obsahu
- Mobilita – hlavička nesoucí informace týkající se komunikace s uzly, které mají svou původní IP adresu, avšak právě hostují v cizí síti.

Propojení hlaviček se děje pomocí pole "Další hlavička", umístěném jednak v základní hlavičce a jednak na pevné pozici v každé z rozšiřujících hlaviček. V poli Další hlavička je vždy uveden typ rozšiřující hlavičky, která bude následovat (formou pevně definovaných kódů rozšiřujících hlaviček). Protože rozšiřující hlavičky mohou mít různou délku, je na pevné pozici na začátku každé z nich uvedena její délka, takže i při zpracování neznámých hlaviček je vždy zřejmé, kde začíná hlavička další. U poslední rozšiřující hlavičky (nebo přímo v základní hlavičce, pokud paket rozšiřující hlavičky nemá) je uveden kód protokolu 4. vrstvy stejně, jako tomu bývalo v poli Protocol hlavičky IPv4. Bližší popis mechanismu řetězení a detailní strukturu nejpoužívanějších rozšiřujících hlaviček lze nalézt např. v [3].

1.2.4 Podpůrné protokoly IPv6

1.2.4.1 ICMPv6

Protokol IPv4 používá ke své funkci dva pomocné (služební) protokoly: ARP a ICMP. Protokol ARP (Address Resolution Protocol, RFC826) slouží k mapování IP adres na adresy spojové vrstvy (MAC adresy); protokol ICMP (Internet Control Message Protocol, RFC792) informuje o zvláštních stavech během šíření paketu sítí. Pro použití v souvislosti s protokolem IPv6 byly oba zmíněné protokoly modifikovány a sloučeny do jediného protokolu ICMPv6.

1.2.4.3 DNS a IPv6 adresy

Zatímco adresy IPv4 byli správcové a dokonce i někteří uživatelé schopni si zapamatovat, u šestnáctibajtových adres IPv6 je to již velmi problematické. O to důležitější je mít možnost používat doménová jména a mapovat je na IPv6 adresy pomocí systému DNS. Pro mapování doménového jména na IPv6 adresu byl nově zaveden záznam AAAA (označení vyjadřuje fakt, že IPv6 adresa je čtyřikrát delší než IPv4 adresa uváděná v klasických A záznamech). Pro mapování IPv6 adresy na doménové jméno se používá osvědčená konstrukce se záznamem typu PTR, kdy se jednotlivé hexadecimální číslice IPv6 adresy zapíší zprava doleva a za tento zápis se připojí doména ip6.arpa.
Během vývoje se také objevily záznamy typu A6 a DNAME, umožňující snadnější změnu adresace, resp. lepší delegování provádění změn jak pro dopředné tak reverzní dotazy. V praxi se však jejich používání nevžilo. Podrobnější informaci o těchto typech záznamů lze nalézt např. v [2].

1.2.5 Pokročilé vlastnosti protokolu IPv6

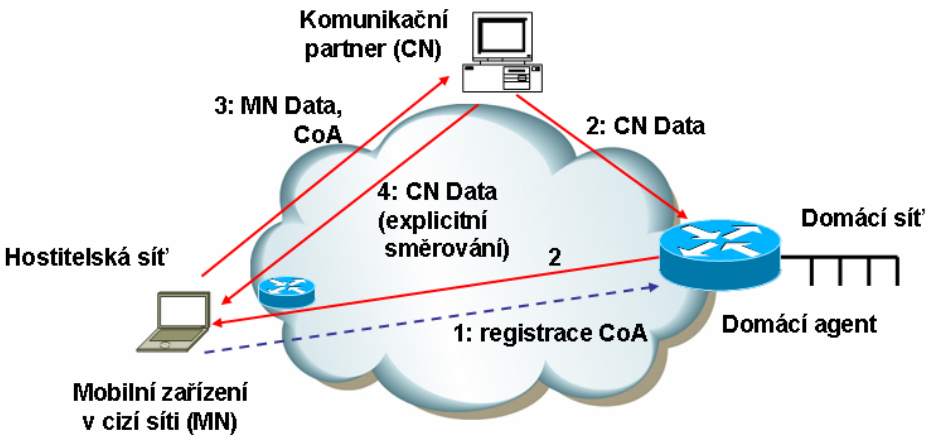
1.2.5.1 Bezpečnost

Data přenášena původním protokolem IPv4 nebyla nijak šifrována ani autentizovována. To znamená, že si data na cestě mohl nejen kdokoli přečíst, ale také je pozměnit nebo dokonce podvrhnout vyslání dat z nějaké IP adresy, aniž by se o tom příjemce mohl dozvědět. Proto byly postupně vyvíjeny různé mechanismy, jak data šifrovat, zajistit jejich integritu (tj. zabránit modifikaci na cestě) a autentizovat zdroj dat, tedy ověřit zda data skutečně vyslat zdroj, který to o sobě v paketu tvrdí. Pro účely zabezpečení na síťové vrstvě OSI modelu je v současné době v prostředí IPv4 de facto standardem protokol IPSec (kap. 1.5.3.2.1), který je volitelným doplňkem IPv4. Protokol IPv6 standard IPSec integruje a předepisuje jeho implementaci jako povinnou (což se však bohužel dnes u mnohých implementací stále neděje). Protože mechanismy zajištění bezpečnosti u IPv6 jsou prakticky totožné jako u standardu IPSec, odkazujeme čtenáře na kapitolu 1.5.3.2.1, kde jsou jeho principy popsány detailněji.

1.2.5.2 Mobilita

V dnešní době je vcelku běžné, že uživatel může (po více či méně silné autentizaci) připojovat své mobilní zařízení postupně do různých sítí podle toho, jak se s tímto zařízením pohybuje. Nicméně protože adresace v protokolu IP má hierarchický charakter (adresa sítě-adresa uzlu), není možné, aby si zařízení ponechalo stále tutéž adresu – její síťová část musí odpovídat adrese sítě, do které je právě připojeno. V mnoha případech, kdy uživatel zařízení chce vystupovat jen jako klient síťových služeb, toto není problémem. Zařízení si pouze vyžádá při připojení do sítě pronájem vhodné adresy protokolem DHCP a z pohledu uživatele vše funguje automaticky. Jiná situace však nastává, když má být mobilní zařízení serverem a jako takové být neustále dostupné pod jednou a toutéž IP adresou, registrovanou v DNS pod určitým všeobecně známým doménovým jménem.

Uvedený případ lze řešit právě s podporou technologie Mobile IP, která je na rozdíl od protokolu IPv4, kde je poskytována formou dodatečného rozšíření (viz RFC3220), do IPv6 přímo vestavěna (RFC3775). Princip spočívá v tom, že aktuální polohu každého mobilního uzlu neustále sleduje jeden ze směrovačů v síti, kam mobilní uzel patří, když uživatel není na cestách (tzv. domácí síť). Tento pověřený směrovač se nazývá Domácí agent (Home Agent, HA). Jestliže se mobilní stanice přesune do cizí sítě, zaregistruje u svého domácího agenta adresu, pod kterou bude po dobu pobytu v této cizí síti dostupná. Tato adresa je označována jako Care-Of Address (CoA). Domácí agent pak všechny pakety došlé na adresu stanice, která právě dočasně hostuje v cizí síti, přeposílá na zaregistrovanou adresu CoA (obr. 1.16). Odpovědi mobilní stanice partnerovi, který s ní komunikuje (tzv. correspondent node), již samozřejmě jdou přímou cestou. Existuje zde také možnost, aby mobilní stanice v cizí síti sdělila svému partnerovi pomocí speciální volby svou dočasnou COA adresu a partner pak posílal všechny pakety přímo na ní s použitím hlavičky explicitního směrování. Před entitami transportní vrstvy však musí zůstat veškeré tyto mechanismy samozřejmě utajeny.



Obr. 1.16 – Princip podpory mobility

Pro reálnou použitelnost MobileIP je nutné zajistit autentizaci všech zúčastněných komponent, aby nemohlo například dojít k podvržení registrace u domácího agenta a tím ke stažení provozu pro jistou stanici na stanici útočníka. K tomu může být velmi dobře využito standardních mechanismů pro autentizaci, případně šifrování, obsažených v IPv6.

Všimněme si na závěr, že na rozdíl od implementace Mobile IP v IPv4 nepředpokládá implementace v IPv6 vůbec existenci cizích agentů (foreign agents).

1.2.5.3 Podpora zabezpečení kvality služby

Kvalita služby na úrovni rozlišovaných služeb (Differentiated Services, kap. 1.4.1.4) je v IPv6 zajišťována stejným způsobem, jako v IPv4. Pole Třída provoz lze strukturovat stejně, jako pole DSCP v hlavičce IPv4 s tím, že další zpracování s ohledem na zajištění kvality služby je již věcí správy front směrovačů, případně i přepínačů.

Se zajištění kvality služby souvisí i pole Flow Label v hlavičce IPv6 paketu, zmíněné již v kapitole 1.2.3.1. Hlavním smyslem tohoto pole je omezení prohledávání směrovacích tabulek na směrovačích, kterými prochází jistý datový tok. Jestliže zdrojová stanice zajistí, že bude paketům každého takovéhoto datového toku přidělovat vždy stejnou a od jiných datových toků se lišící hodnotu a tuto vkládat do pole Flow Label, může každý směrovač provést vyhledání ve směrovací tabulce pouze jedenkrát a výsledek vložit pro další použití do paměti cache. Ta již může být organizovaná jako paměť asociativní a je vždy prohlížena předtím, než bude zahájeno náročné vyhledávání ve směrovací tabulce. Záznamy v cache paměti tak budou mít tvar n-tic

<zdrojová adresa, flow label, next_hop_IP, výstupní_rozhraní, hlavička_spojové_vrstvy>

Ukládání položky Flow Label i se zdrojovou adresou je nezbytné, protože přidělování hodnot Flow Label se děje na jednotlivých zdrojových stanicích nezávisle. Předpřipravení hlavičky spojové

vrstvy pro výstupní rozhraní může směrování opět urychlit, protože odpadá potřeba opakovaného prohledávání ARP tabulky výstupního rozhraní.
S podporou kvality služby souvisí pole Flow Label tak, že pomáhá identifikovat pakety téhož datového toku, s nimiž mohou směrovače na cestě zacházet jistým jednotným způsobem, který může směrovačům vhodným způsobem signalizovat zdroj datového toku. Konkrétní mechanismy jsou však dosud pouze ve stádiu návrhů.

1.2.6 Směrování a protokol IPv6

Pro směrování v sítích s IPv6 lze samozřejmě využít léty prověřené mechanismy používané v současné době v sítích s protokolem IPv4. Mimo statického směrování se tak ve světě IPv6 se tak setkáme jak se směrovacími protokoly třídy vektoru vzdáleností (distance-vector), tak s protokoly založenými na stavu linek (link-state), se stejnými výhodami a nevýhodami jako u IPv4. Nemůžeme však přímo převzít ty směrovací protokoly z prostředí IPv4, které počítaly s jediným konkrétním formátem adres – adresami IPv4. Těch je bohužel většina. Proto musely být některé protokoly reimplementovány (např. RIPNG (RFC2080), který nahradil původní RIP) nebo byly vypracovány nové verze (např. u OSPF může adresy protokolu IPv6 nést až implementace OSPF verze 3). Pro směrování IPv6 mezi autonomními systémy se s výhodou používá BGP verze 4+, který bývá často označován jako Multiprotocol BGP a je schopen nést formou atributů prefixy síťových adres v nejrůznějších formátech, mezi jinými i IPv6.

1.2.7 Současný stav podpory protokolu IPv6

Reálná situace s IPv6 je v současné době taková, že přechod z IPv4 na IPv6 probíhá velmi pozvolna. Je tomu tak proto, že původně prorokovaný akutní nedostatek adres IPv4 se stal méně ožehavým zavedením jejich efektivnějšího přidělování a širokým využíváním překladu adres. Také ostatní pokročilé mechanismy vestavěné do IPv6 jsou v současné době nabízeny formou dodatečných standardů (IPSec, Mobile IP) již i v IPv4. Protože pro uživatele v současné době nepřináší přechod na IPv6 přímý užitek, za který by byli ochotni zaplatit, raději (stejně jako poskytovatelé, kteří nechtějí zbytečně zasahovat a investovat do fungující infrastruktury) vyčkávají. Existují pouze ostrůvky používající spolu s protokolem IPv4 i IPv6, avšak globální konektivita mezi všemi sítěmi Internetu pomocí IPv6 ještě z daleka vybudována není. V moderních operačních systémech (Linux, Windows XP) i na kvalitnějších směrovačích je však více či méně široká implementace IPv6 k dispozici a jen vývoj v oblasti ukáže, kdy a zda vůbec bude IPv6 hlavním síťovým protokolem v Internetu

1.2.7.1 Možnosti přechodu z protokolu IPv4

Návrhářům protokolu IPv6 bylo od začátku jasné, že přechod z IPv4 na IPv6 není technicky ani organizačně uskutečnit skokově. Předpokládá se, že se IPv6 bude v Internetu zavádět postupně a jak stanice, tak směrovače budou ještě dlouhou dobu schopny pracovat současně s původním IPv4 i nově zaváděným IPv6. Pro postupný přechod z IPv4 na IPv6 byly navrženy následující mechanismy:

- Dvojí protokolový zásobník – zařízení má implementovováno paralelně podporu jak IPv4, tak IPv6 a umožňuje komunikovat oběma těmito protokoly
- Tunelování – tunelováni paketů IPv6 v paketech IPv4 přes části sítě, které IPv6 dosud nepodporují. Zde samozřejmě musíme řešit překlad mezi adresami IPv6 sítí a adresami koncových bodů IPv4 tunelů, za kterými se tyto sítě ukrývají. V nejjednodušším případě lze toto přiřazení konfigurovat staticky.
- Překlad protokolů – vzájemná konverze paketů mezi protokoly IPv4 a IPv6 pomocí speciální brány.

V praxi se v současné době setkáme nejčastěji s prvními dvěma způsoby.