Konfigurace – autokonfigurace a DHCPv6

Jsou dva typy automatické konfigurace :

- Stavová
- Bezstavová

Stavová konfigurace

Základem stavové konfigurace je server spravující konfigurační parametry, které pak klientům na požádání sděluje. Podobné mechanismy se používají již dlouho – od RARP přes BOOTP až k dnešnímu DHCP.

Pro účely stavové konfigurace IPv6byl navržen protokol DHCPv6. V novějších textech o IPv6 se přestává termín „stavová konfigurace“ používat a uvádí se DHCPv6.

Princip všech zmíněných mechanismů je podobný – **počítač rozešle na obecnou adresu dotaz ohledně svých komunikačních parametrů a server mu je ve své odpovědi sdělí.** Zahrnují potřebné informace pro zapojení do sítě:

- IP adresu
- prefix podsítě (dříve maska, nyní dle dosahu více prefixů)
- implicitní záznam do směrovací tabulky (gateway)
- adresu DNS serveru
- další informace (add DHCP serveru)

Bezstavová konfigurace

***Bezstavová konfigurace* představuje zcela nový způsob**. Je založena na tom, že **v síti jsou směrovače, které vědí potřebné.** Čas od času všem sdělí, **jaká je zdejší situace – pomocí tzv. „ohlášení směrovače“**. **Nově připojenému počítači stačí jen chvíli poslouchat nebo o tyto informace aktivně požádat.** Hlavním cílem bezstavové konfigurace je **automatické určení vlastní adresy uzlu.**

Je popsána v RFC 4862: *IPv6 Stateless Address Autoconfiguration*. S touto tématikou souvisí i automatická konfigurace směrování, která je oficiálně řazena do objevování sousedů. Proto je popsána také zde.

Bezstavová konfigurace - autokonfigurace

Ohlášení směrovače (Router advertisement)

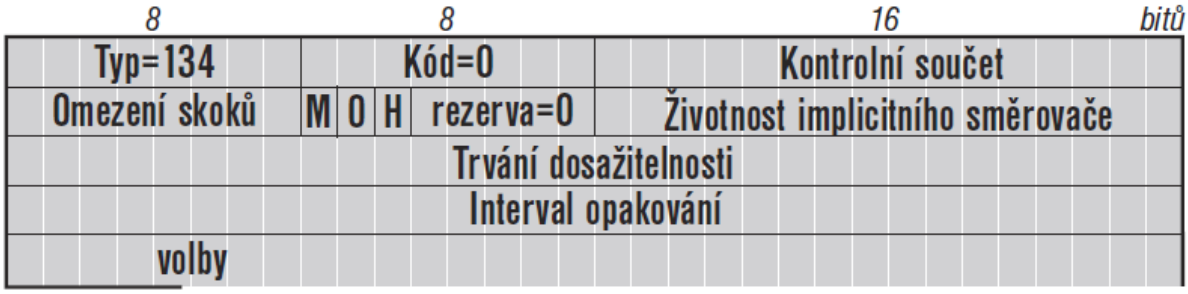
***Ohlášení směrovače (Router advertisement) posílá* v náhodných intervalech každý směrovač**, a to do všech sítí, k nimž je připojen. Náhodnost přestávky mezi ohlášeními má za cíl omezit dopady případných nešťastných časových souher (kdy dvě ohlášení v nevhodném intervalu po sobě způsobí zmatení).

Ohlášení směrovače připomíná hlášení, která jsme zvyklí slýchat na nádraží. „Na . . . tou kolej přijel vlak z Prahy, pravidelný příjezd 14:30. Vlak dále pokračuje Brno a …k.“. Po jeho absolvování vědí všichni zúčastnění – cestující ve vlaku, v ostatních vlacích i na nádraží – co se děje a jak to bude pokračovat.

Po obdržení ohlášení směrovače vědí připojené počítače (viz. obr níže)

- v jaké jsou síti
- jak se zde komunikuje

- kdo je **implicitní směrovač** (gateway)



***Ohlášení směrovače (Router advertisement)* se posílá pomocí ICMP**. Typ 134

Nejsou zde adresy zdejších sítí, protože jsou umístěny mezi volbami.

Důležitá je ***Životnost implicitního směrovače (Router Lifetime)*- jedná se o čas (v sekundách)** a udává, jak dlouho ještě tento směrovač hodlá sloužit jako implicitní pro uzly z této sítě.
Je-li hodnota nulová, směrovač nemá být používán jako implicitní.

Omezení skoků (Cur Hop Limit) oznamuje zdejším uzlům, jak mají omezovat životnost odesílaných datagramů **– jakou hodnotu vkládat do položky s maximálním počtem skoků**.

Následuje **osm příznaků,** jsou **definovány tři**. První dva se týkají DHCPv6.

Příznak *M (Managed address configuration, stavová konfigurace adres)* oznamuje, že adresy i další komunikační parametry přidělí DHCPv6.

Příznak *O (Other stateful configuration, stavová konfigurace ostatních parametrů)*, který rozhoduje o použití DHCPv6 pro ostatní parametry sítě, jako jsou například adresy lokálních DNS serverů.

Významy možných kombinací příznaků M a O shrnuje tabulka

M	*O*	*význam*
1	–	DHCPv6 poskytne vše
0	1	kombinovat bezstavovou konfiguraci (pro adresu, prefix a směrování) s DHCPv6 (pro ostatní parametry)
0	0	DHCPv6 není k dispozici

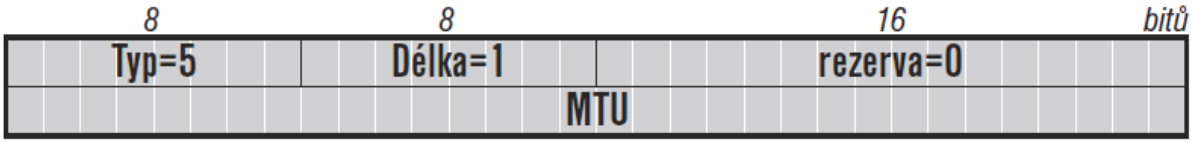
Příznak *H (Home agent, domácí agent)* slouží pro podporu mobility a byl doplněn v RFC 3775. Směrovač jeho nastavením sděluje, že je ochoten pro místní síť pracovat jako domácí agent.
Více najdete ve zmiňované publikaci pana Satrapy.

Poslední dva údaje pevné části ohlášení **ovlivňují detekci dosažitelnosti sousedů. Oba jsou časové a jejich hodnota je uvedena v milisekundách.**

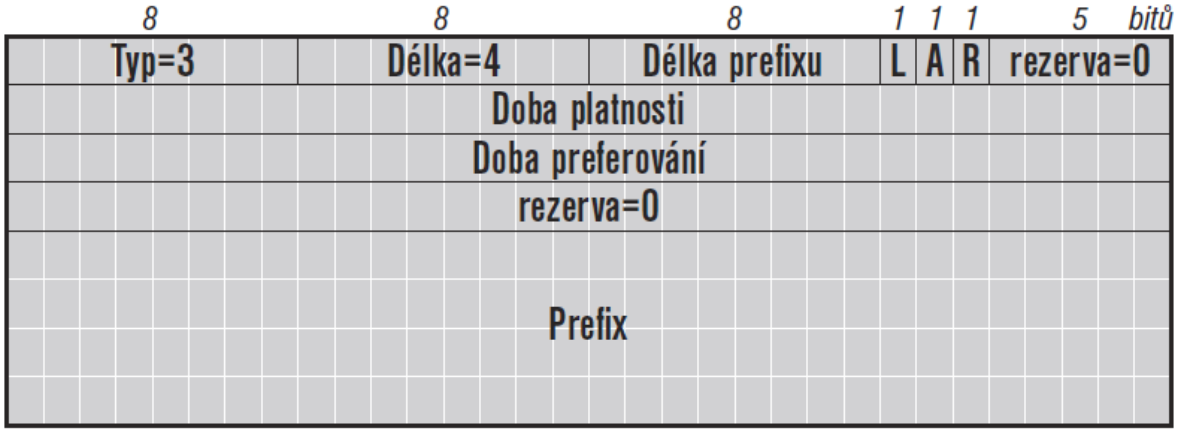
Trvání dosažitelnosti (Reachable Time) říká, jak dlouho má být uzel považován za dosažitelný poté, co byla ověřena jeho momentální dosažitelnost.

Interval opakování (Retrans Timer) je interval mezi dvěma výzvami sousedovi.

Ve *Volbách*
- může směrovač sdělit svou linkovou adresu
- ohlásit MTU této sítě



- připojí po jedné volbě pro každý prefix IP adres
- prefixy adres, které se v dané síti používají



Počítá se s tím, že jedna fyzická síť může sloužit několika různým logickým sítím a má několik prefixů.

Volba informace o prefixu (Prefix Information)*je výše*

***Prefix – je k*líčový**

Délka prefixu (Prefix Length) - **udává, kolik bitů z prefixu je platných.** Obvyklou hodnotou by mělo být 64.

Doba platnosti (Valid Lifetime) udává, jak dlouho prefix platí

Doba preferování (Preferred Lifetime) jak dlouho mají být preferovány adresy vzniklé automatickou konfigurací z tohoto prefixu.

Oba časové údaje jsou uvedeny v sekundách. V obou případech hodnota 0xffffffff znamená nekonečnou trvanlivost.

Oba údaje stanoví dobu trvání jednotlivých fází v životě adresy vytvořené bezstavovou autokonfigurací.

Po vzniku je adresa *preferována (preferred)*. To znamená, že ji počítač může používat podle libosti.

Po vypršení *Doby preferování* se adresa stává *odmítanou (deprecated)*. Tato adresa je sice nadále platná, ale počítač by se jí měl pokud možno vyhýbat. Může ji použít například při pokračování již probíhající komunikace, pokud by přechod na jinou (preferovanou) působil potíže.

Po uplynutí *Doby platnosti* se adresa stává *neplatnou*. Počítač ji nesmí používat a měl by odstranit její přiřazení odpovídajícímu rozhraní. Neplatná adresa jako by vůbec nebyla.

Příznak *L (on-Link, na lince)* znamená, že prefix lze používat k rozhodování, který uzel je lokální – tedy přímo dosažitelný linkovou vrstvou – a který nikoli.

Příznak *A (Autonomous address-configuration, autonomní konfigurace adres)*, prefix lze použít k automatické konfiguraci vlastní adresy.
Zde se skrývá **možnost vypnout (zakázat) bezstavovou konfiguraci.** Pokud všechny směrovače u **všech prefixů ve svých ohlášeních vynulují příznak *A*, počítače nemají k dispozici žádné**

adresy, které by si mohly přidělit. Zůstanou odkázány na DHCPv6 a lokální linkové adresy, které si přidělují automaticky.

Naopak pokud některé prefixy mají **nastaven příznak A a i příznak M, může počítač použít obě cesty k získání adresy – stavovou i bezstavovou**

Příznak *R (Router address, adresa směrovače)* byl doplněn pro potřeby podpory mobilních zařízení. Je-li nastaven, **obsahuje položka *Prefix* kompletní globální adresu směrovače.** Pro potřeby automatické konfigurace si z ní místní stroje vezmou jen prefix sítě a identifikátor rozhraní budou ignorovat.

Ovšem domácí agenti spolupracující s mobilními uzly zde najdou kompletní adresy svých kolegů. Ty pak mohou poslat uzlu na cestách, když bude dynamicky hledat domácího agenta.

Určení vlastní adresy

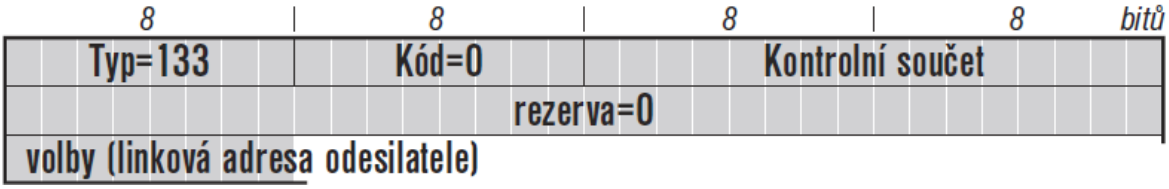
Každé KZ musí především znát svou vlastní IP adresu.

Automatické stanovení vypadá následovně:

- Uzel si **vytvoří svou lokální linkovou adresu.** Ke standardnímu prefixu lokálních linkových adres fe80::/10 připojí identifikátor svého rozhraní, jehož vygenerování nepředstavuje žádný problém.

- **Detekce duplicitních linkových adres** (málo pravděpodobné, že by stejnou lokální adresu mělo více uzlů, ale je potřeba se o tom přesvědčit**). Použije se standardní objevování sousedů. Uzel rozešle výzvu sousedovi,** v níž hledá vlastníka adresy, kterou sám sobě vygeneroval. **Pokud dorazí ohlášení souseda, vznikne potíž. Znamená to, že někdo má stejný identifikátor rozhraní a automatická konfigurace tudíž nemůže pokračovat dál.** V normálním případě však bude odezva negativní a uzel si vytvořenou lokální linkovou adresu přidělí.

- **Získání informací o okolí - ohlášení směrovače** – počká nebo o ně požádá **prostřednictvím *Výzvy směrovači* Typ 133 (ICMP 133)**



  Z příznaků v *Ohlášení směrovače* se dozví, zda má použít stavovou konfiguraci pro svou adresu a další parametry sítě.
- U každého ze zdejších prefixů uveden příznak, **zda se pro tento prefix má použít bezstavová konfigurace adres**. Pokud ano, **připojí si k prefixu svůj identifikátor rozhraní a tuto adresu si přidělí**. Už ji netestuje, protože jednoznačnost lokálního prefixu byla prověřena hned v počáteční fázi, když si uzel přiděloval lokální linkovou adresu.

Jednoznačnost se testuje u adres konfigurovaných manuálně nebo získaných prostřednictvím stavové konfigurace. Použije se výše popsaný postup – uzel pošle výzvu sousedovi se svou vlastní adresou.

Konfigurace směrování

V IP verze 6 se jednotlivé uzly dovedou naučit i směrování ve své síti.

Předpokládá se, že si uzel bude udržovat následující datové struktury:

- **Cache cílů (Destination Cache)** obsahuje směrovací informace pro konkrétní cílové adresy. Ke každému cíli je v této tabulce umístěna první adresa po cestě k němu (next hop). Datagramy směřující k uvedenému cíli se mají předat na tuto adresu.
- **Seznam prefixů (Prefix List)** slouží k posuzování, kdo je a kdo není umístěn ve stejné síti.
- **Seznam implicitních směrovačů (Default Router List)** obsahuje informace o všech směrovačích, které ve svém ohlášení nastavily příznak implicitního směrovače.

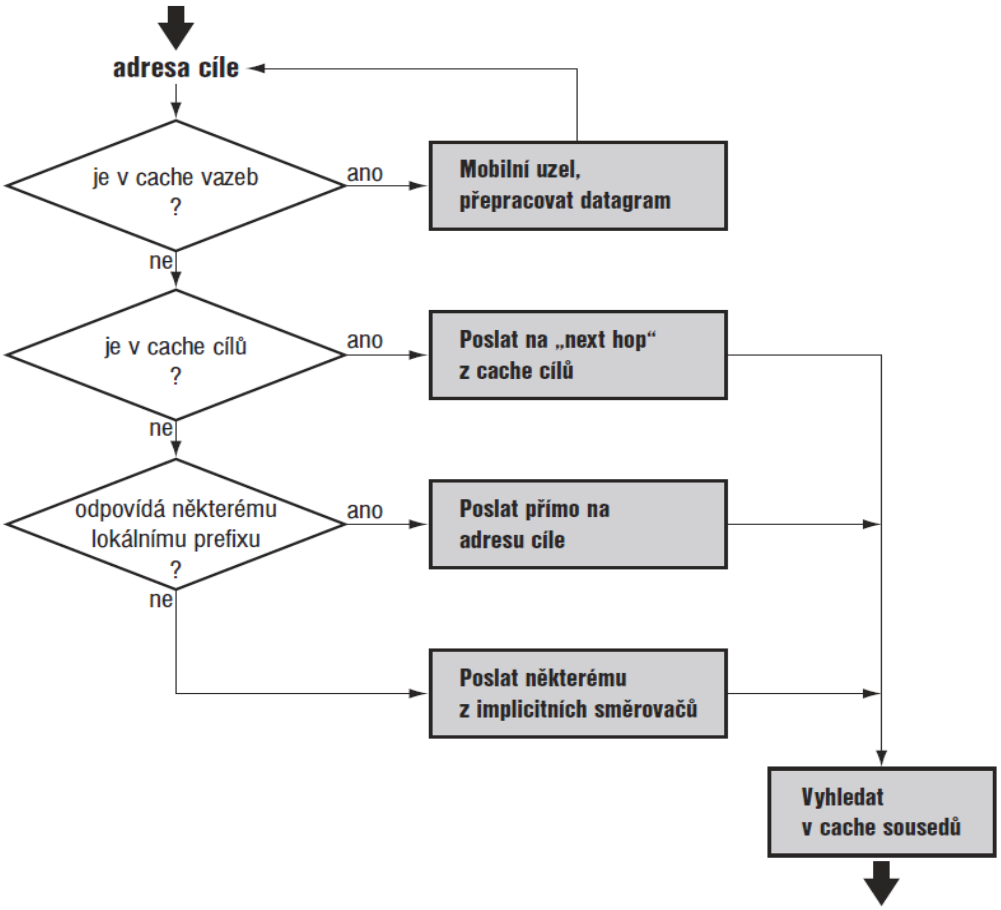
Seznam prefixů a seznam implicitních směrovačů představují obecný mechanismus (ipv4 – směrovací tabulka netstat –r).

Cache cílů uvádí výjimky z obecného mechanismu. Datové struktury jsou ideové, lze je realizovat také všechny v jednom – například směrovací tabulkou.

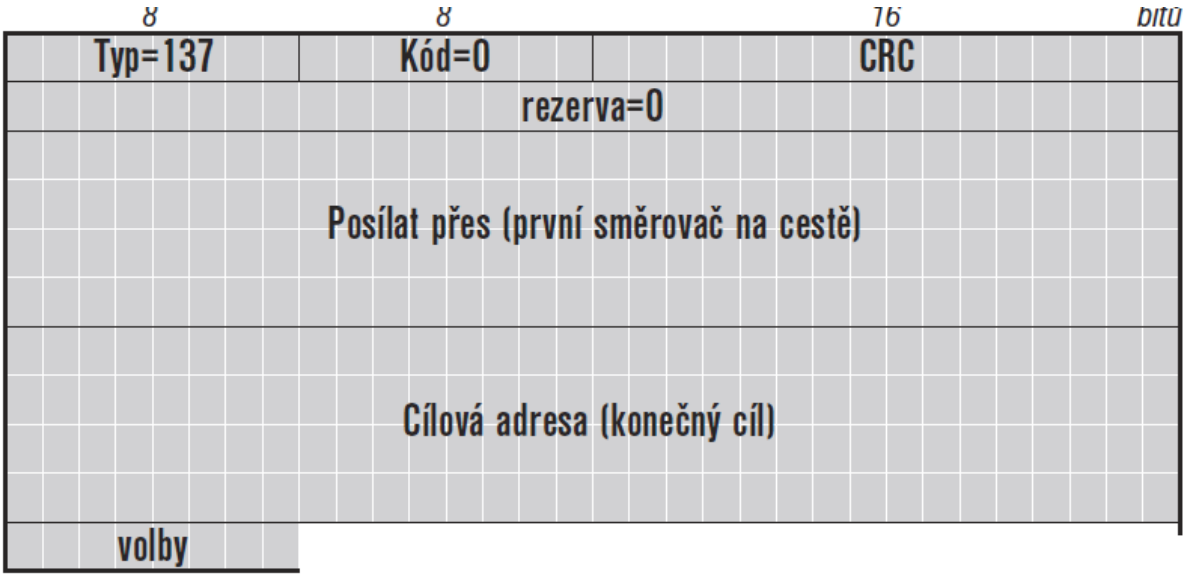
Podpora mobility přidává ještě cache vazeb, říká, že dotyčný počítač momentálně pobývá na úplně jiné adrese. To znamená, že datagram bude zcela přepracován (změní se cílová adresa a přibude hlavička *Směrování*)

Když je rozhodnuto o příjemci datagramu, přijde na cache sousedů (viz. objevování sousedů)**,** v níž se bude hledat jeho fyzická (linková) adresa.(dříve ARP)

Celý postup při odesílání datagramu je níže



- cache cílů, zda tato adresa není explicitně definována. Pokud ano, použije ji.
- srovná adresu cíle s jednotlivými položkami v seznamu prefixů. Podle nich určí, zda se jedná o adresu lokální či vzdálenou. Pro vzdálenou použije jeden z implicitních směrovačů. **Zvolí-li nevhodný směrovač nebo je daný cíl ve skutečnosti lokální, pošle směrovač odesilateli paketu ICMP zprávu *Přesměrování*.** Údaje v ní obsaženy si odesilatel poznamená do cache cílů, aby příště posílal datagramy určené tomuto cíli vhodnější cestou.



Formát přesměrování obsahuje nejzákladnější informace: *Cílovou adresu (Destination Address)* a *Posílat přes (Target Address)*, což je adresa směrovače (nebo cíle samotného), na kterou se mají posílat datagramy určené pro tento cíl.

Do voleb lze zařadit fyzickou adresu směrovače (pokud ji odesilatel přesměrování zná) a hlavičku datagramu, který přesměrování vyvolal. Její velikost je omezena tak, aby celkově datagram s přesměrováním nepřekročil délku 1280 B.

Informace o adrese místního DNS serveru

Pro úplnost zbývá **adresa místního DNS serveru**, na nějž se má obracet se svými dotazy. Základní **mechanismy objevování sousedů zde nepomohou, DNS nechávají stranou.** To je nedostatek, protože při rozkošné podobě IPv6 adres je počítač bez funkčního DNS téměř nepoužitelný.

Postupem času se **objevila tři možná řešení**, jejichž rozbor najdete v RFC 4339: *IPv6 Host Configuration of DNS Server Information Approaches*.

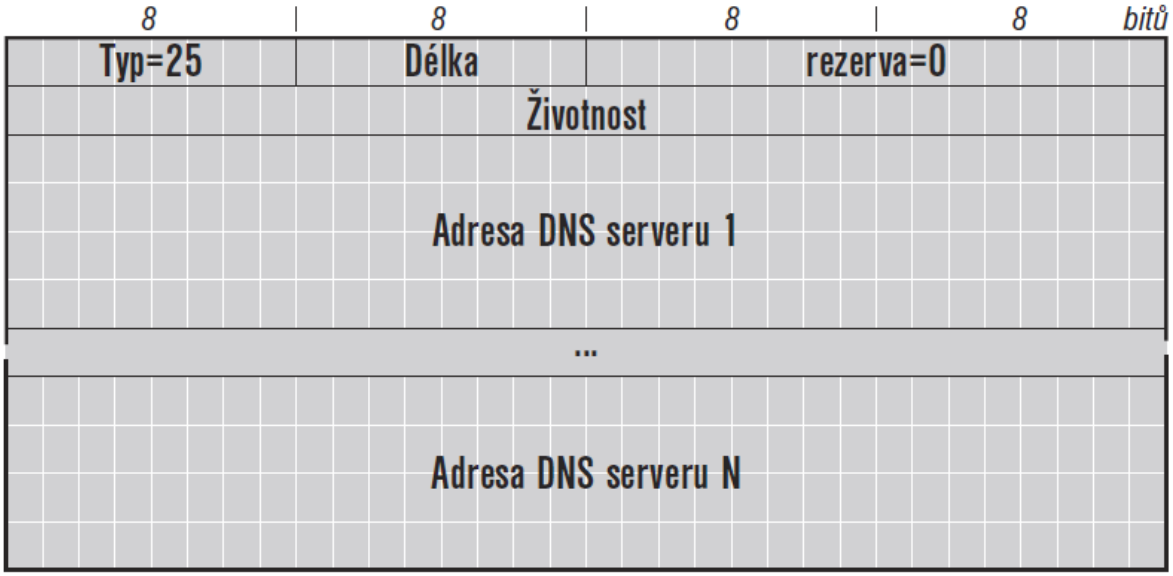
- **informace o DNS (i případné další) do bezstavové autokonfigurace doplnit stavovou cestou**. K tomu slouží příznak O v ohlášení směrovače,

- **definovat pevné adresy pro místní DNS servery**, které bude znát každý klient. Pokud se nic nedozví jinou cestou, například ze své konfigurace či z DHCP, bude se klient prostě obracet na tyto standardní adresy. Přišel s ní *draft-ohta-preconfigured-dns*, který se od roku 2004 nevyvíjí. Počítal s využitím výběrových adres lokálních pro místo – site local a ty jsou zakázané.

- **doplnit informace o lokálních DNS serverech přímo do bezstavové automatické konfigurace, konkrétně do ohlášení směrovače.** Výslednou podobu tohoto rozšíření

shrnuje RFC 5006: *IPv6 RouterAdvertisement Option for DNS Configuration (zatím experimentální)*.

Zavádí novou volbu pro ohlášení směrovače, pojmenovanou ***Rekurzivní DNS server*** *(Recursive DNSServer, RDNSS)*. Její obsah je velmi jednoduchý (viz. níže). Poskytuje adresy místních serverů v libovolném počtu (je odvozen z *Délky*) a počet sekund jejich *Životnosti*. Dá se očekávat, že během doby životnosti dorazí další ohlášení směrovače, které ji prodlouží.



Problém je, že objevování sousedů a automatická konfigurace jsou implementovány hluboko v operačním systému. Jejich úpravy proto nejsou snadné a navíc představují riziko pro stabilitu.

Stavová konfigurace - DHCPv6

Automatická konfigurace s DHCP je v IPv4 běžnou záležitostí.
Pomocí *Dynamic Host Configuration Protocolu (DHCP)* startující počítač získá všechny potřebné údaje (IP adresu, masku podsítě, adresu DNS serveru a implicitní směrovač pro odchozí provoz).

DHCP je všudypřítomné

- typický operační systém bývá po instalaci nastaven na jeho použití
- pomocí DHCP se konfigurují síťové tiskárny
- najdete je v podnikových sítích i v domácnostech (protože ADSL modem funguje jako DHCP server pro počítače připojené k němu Ethernetem či Wi-Fi).

DHCP má čtyři fáze:

1. **Objevování (discover):** Klient pošle všesměrově (čili na IP adresu 255.255.255.255) dotaz obsahující jeho ethernetovou adresu (BootP).

2. **Nabídka (offer):** Servery, k nimž se dotaz dostane (často bývá jeden, ale obecně jich může být libovolné množství), nahlédnou do svých tabulek, zda pro tohoto klienta mají nějaké použitelné parametry. Pokud ano, pošlou mu nabídku „Ode mne bys mohl mít tohle. . . “

3. **Požadavek (request):** Klient posbírá nabídky, vybere si jednu a příslušnému serveru pošle požadavek, v němž žádá o přidělení nabídnutých parametrů.

4. **Potvrzení (acknowledge):** Server mu potvrdí, že jeho žádosti vyhověl.

Tím okamžikem může klient začít příslušné parametry používat.

Přidělení parametrů je pouze dočasné (v terminologii DHCP se jedná o pronájem, lease), po vypršení platnosti musí klient požádat o prodloužení nebo získat zcela nové parametry.

V IPv6 se tento přístup nazývá **stavovou konfigurací a zajišťuje jej nová verze DHCP.**

Změny protokolu vlivem IPv6 prostředí:

- IPv6 nezná oznamovací (broadcast) adresy
- každá stanice si umí sama nastavit lokální linkovou adresu, takže odpadá vazba na adresy nižších komunikačních vrstev (Ethernet apod.).

Vzhledem k všeobecnému rozšíření DHCP a spoustě zkušeností s jeho provozem je překvapující, že **definice nové verze protokolu vznikala dlouho.** Od prvního návrhu *draft-ietf-dhc-dhcpv6-00* do výsledného RFC uběhlo **osm a půl roku**! V roce 2003 jsme se konečně dočkali RFC 3315: *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*.

Účastníci DHCP

Na DHCPv6 se podílejí tři kategorie zařízení:

- ***klient*** je stroj, který chce získat informace;
- ***server*** je ten, kdo mu je poskytne;
- ***zprostředkovatel (relay)*** zprostředkovává styk mezi nimi, pokud se klient a server nacházejí na různých linkách.

Společný pojem ***agent* - zahrnovány servery a zprostředkovatelé**. Agent je zkrátka někdo, kdo poskytne DHCP odpověď (ať už svou vlastní či zprostředkovanou) a sídlí na lokální lince.

DUID – identifikace klienta

Významnou roli v DHCP hraje identifikace – jak **serverů,** tak především **klientů**.
Dříve se k tomuto účelu používala ethernetová adresa,

DHCPv6 zavádí pojem *DHCP Unique Identifier (DUID)*. Jedná se o jednoznačný identifikátor účastníka DHCP. Jeden DUID má každý klient i server. Měl by být pokud možno stálý a neměnit se ani při výměně síťové karty počítače.

Autoři protokolu vzdali snahu o vytvoření univerzálního identifikátoru, který by vyhověl ve všech případech. Je definováno několik způsobů, jak DUID lze vytvořit. Navíc připustili do budoucna rozšiřování sortimentu typů DUID.

Identifikátor přidělený výrobcem

Podmínku stálosti snadno splňuje **identifikátor přidělený výrobcem.** Předpokládá, že výrobce přidělí zařízení jednoznačnou identifikační hodnotu (výrobní číslo). DUID je pak tvořen touto hodnotou a doménou výrobce.

Dva definované typy využívají linkovou adresu.

- první kombinuje linkovou adresu s časem vytvoření a předpokládá, že zařízení má k dispozici zapisovatelnou paměť. Čili že si DUID jednou vygeneruje, uloží do této paměti a pak bude trvale používat tutéž uloženou hodnotu.
- druhý z definovaných typů používá samotnou linkovou adresu a odpovídá praxi ze světa IPv4. Na rozdíl od něj by ale měl stejný DUID používat pro všechna síťová rozhraní, jež chce pomocí DHCPv6 konfigurovat. Výměnou síťové karty se tento typ DUID změní.

Identifikační IA asociace (identity association, IA) – IAID – identifikace rozhraní

Jedná se o **shluk konfiguračních informací přidělených jednomu rozhraní**, opatřený jednoznačným identifikátorem (IAID).

Tyto identifikátory přiděluje klientský počítač každému rozhraní, pro něž chce použít DHCPv6. Měl by být konzistentní a neměnit se v čase. Čili by si je buď měl **ukládat do trvanlivé paměti nebo používat takový algoritmus pro jejich vytváření, který zajistí pokaždé stejné hodnoty**.

Identifikace v DHCPv6:

- klient je jednoznačně identifikován svým DUID,
- rozhraní v rámci klienta jsou rozlišována prostřednictvím IA. S IA jsou také spojeny přidělované parametry(některé však mohou stát i mimo IA, pokud jsou obecné pro celého klienta).

Fáze DHCPv6

Základní fáze DHCPv6 dialogu se proti předchůdci nijak významně nezměnily.
Klient se poptá po dostupných parametrech, dostane nabídky, jednu si vybere a se serverem si dohodne její přidělení.

Konfigurace začíná hledáním vstřícných serverů. Jelikož na začátku klient neví nic o síti, ve které se nachází, posílá své počáteční zprávy na standardní skupinové adresy.

Pro DHCPv6 byly definovány následující standardní skupinové adresy:

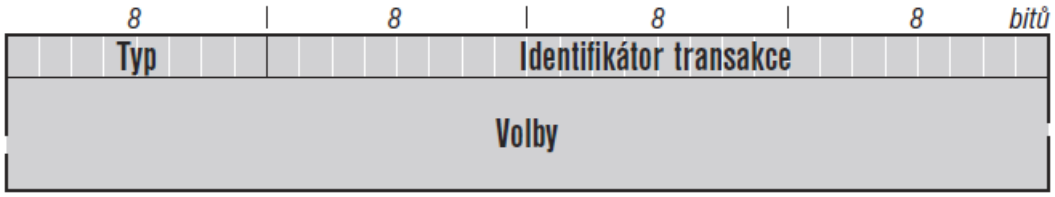
- všichni DHCP agenti a servery ff02::1:2
- všechny DHCP servery ff05::1:3

Klient zahájí svou činnost tím, že vytvoří IA pro svá rozhraní a opatří je jednoznačnými identifikátory.

Výzva (solicit)

Na adresu všech DHCP agentů (ff02::1:2 - má dosah jen v rámci linky) pak pošle ***výzvu (solicit)***, ke které přibalí svůj DUID i všechny IA.

Významem výzvy je „hledám všechny DHCP servery, které jsou ochotny mi poskytnout adresu“. Aby systém fungoval, musí být v každé lokální síti umístěn alespoň jeden agent. Součástí výzvy je i *lokální linková adresa* (s prefixem fe80::), kterou si klient přidělil.



Ve srovnání se staršími verzemi návrhu byl naprosto minimalizován. Skoro všechny informace byly přesunuty do voleb, zůstaly jediné dvě společné položky:

Typ identifikující o jakou zprávu se vlastně jedná

1	výzva (solicit)
2	ohlášení serveru (advertise)
3	žádost (request)
4	potvrzení (confirm)
5	obnovení (renew)
6	převázání (rebind)
7	odpověď (reply)
8	uvolnění (release)
9	odmítnutí (decline)
10	rekonfigurace (reconfigure)
11	žádost o informace (information request)
12	předání (relay forward)
13	zprostředkovaná odpověď (relay reply)

Identifikátor transakce (Transaction-id)**,** který umožňuje párovat dotazy a odpovědi.

Pokud výzvu obdrží server, rovnou klientovi odpoví. Znamená to, že sídlí společně s klientem na téže lince a pro doručení odpovědi proto použije jeho lokální linkovou adresu.

Ohlášení serveru (advertise)

Odpovědí na výzvu je ***ohlášení serveru (advertise)*****.** Jeho součástí **bývá *preference*, která udává ochotu serveru poskytnout své služby danému klientovi.** Zároveň server přibalí **konfigurační parametry, které by přidělil jednotlivým IA**. V podstatě říká „Kdybych já dostal tento požadavek, nabídl bych toto. . . “

Zprostředkovatel má konfigurován seznam serverů, kterým má předávat dotazy (součástí tohoto seznamu může být i obecná skupinová adresa všech DHCP serverů daného místa ff05::1:3). Dorazí-li k němu výzva, předá ji na všechny adresy ze seznamu.

Zprostředkovatel zabalí dotaz do nové zprávy **typu *předání (relay forward)*,** v níž uvede svou vlastní adresu. Server svou odpověď zabalí do podobné zprávy (***zprostředkovaná odpověď, relay reply***) a pošle zpět zprostředkovateli. Ten vybalí data a předá je opět na lokální linkovou adresu klienta.

Klient posbírá doraziví ohlášení a vytvoří si tak seznam DHCP serverů, které má k dispozici. Klient by měl dát přednost tomu, kdo má nejvyšší preferenci.

DHCP *žádost (request)*

Když si klient vybral server, nastává **druhá fáze: získání komunikačních parametrů.** Odešle **DHCP *žádost(request)*** *a v* ní uvede DUID serveru, kterému je určena (identifikátor získal z jeho ohlášení).

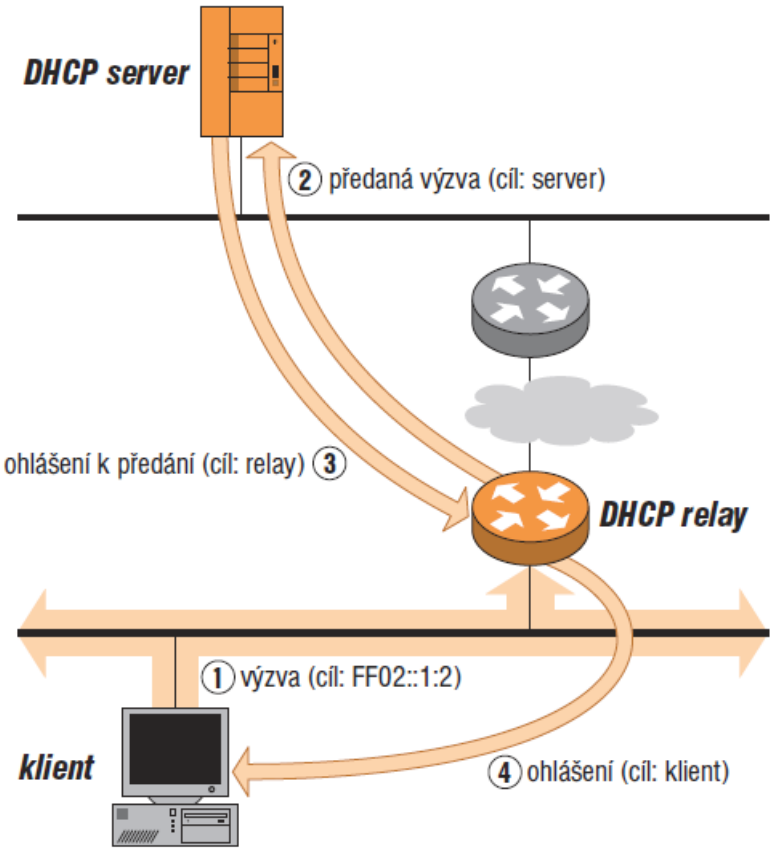
Zprávu opět pošle na obecnou adresu všech DHCP agentů. Stále ještě nezná zdejší síť, takže neví, jak doručit konkrétně adresovaný datagram. Servery, kterých se netýká, žádost ignorují.

Odpověď (reply).

Cílový server žádost vyhodnotí a pošle **zpět *odpověď (reply)***. Při přidělování adresy server bere v úvahu především linku (fyzickou síť), ke které je klient připojen, a DUID klienta. Především podle těchto dvou informací vybere adresu (či adresy), které oznámí klientovi.

Součástí odpovědi je i stav, kterým sděluje, zda žádosti vyhověl nebo ne (a z jakého důvodu). Odmítnutí by mělo být velmi nepravděpodobné.

Komunikace opět může proběhnout přímo nebo přes zprostředkovatele.
Zprostředkovaná žádost a odpověď v DHCPv6 je níže



DHCP zpráva odmítnutí (decline)

Klient si přidělené adresy ověří (standardním postupem pro detekci duplicitních adres) a pokud zjistí, že je někdo již používá, může je odmítnout.

Životnost adres

Stejně jako v IPv4 jsou adresy přidělovány na časově omezenou dobu. Po jejím uplynutí musí klient **požádat o prodloužení.**

- nejprve žádá server, který adresu přidělil (**zpráva *obnovení, renew***).
- pokud neodpovídá, obrátí se na všechny dostupné servery, zda některý z nich není ochoten adresu prodloužit (***převázání, rebind***).

Když klient **končí svou síťovou existenci**, měl by o tom server informovat zprávou ***uvolnění (release)*****,**aby mohla být jeho adresa přidělena případnému novému zájemci.

Návrat klienta do sítě.

Například po restartu, usnutí a probuzení počítače či jeho dočasném fyzickém odpojení. V takovéto situaci si klient musí ověřit, jestli jeho stávající síťové parametry jsou správné.
Pošle na adresu všech DHCP agentů zprávu ***potvrzení* (*confirm*),** v níž sdělí aktuální parametry svých IA. Příslušný server reaguje *odpovědí*, ve které platnost přiřazení potvrdí nebo naopak odmítne.

Konfigurace vyžádaná serverem

Aktivita v DHCP typicky vychází od klienta. Jsou **případy, kdy vyvolání konfiguračního dialogu požaduje server.** Například došlo ke změně síťových parametrů a server chce, aby se klienti přizpůsobili nové situaci.

DHCP server rozešle zprávu ***rekonfigurace* (*reconfigure***). **Posílá se individuálně každému z klientů, kterých se týká.** Jelikož si server vede přehled o přidělených parametrech, bez problémů si v něm najde potřebné adresy.

Klient pak reaguje odesláním požadavku na *obnovení* svých parametrů a server ve své *odpovědi* sdělí vše potřebné.

Bezpečnost DHCPv6

Aneb jak se bránit proti partyzánským serverům poskytujícím nesmyslné údaje či proti změnám DHCP zpráv při přenosu.

Protokol za tímto účelem zavádí **volbu *Autentizace (Authentication)*.** Pokud klient chce ověřovat pravost DHCP komunikace, přibalí ji hned k úvodní výzvě.

V ní určí, jaké metody pro ověřování chce používat, **základní je HMAC v kombinaci s MD5.** Server následně připojí autentizační informace ke svému ohlášení a i dále bude tato volba součástí vyměňovaných zpráv.

Obsahuje digitální podpis, díky němuž může příjemce ověřit jak totožnost odesilatele (zná klíč), tak obsah zprávy.

Slabinou tohoto mechanismu je, že staví na symetrické kryptografii, kde obě strany používají stejný klíč. Vyžaduje konfiguraci na obou stranách – klient musí znát klíč pro komunikaci se serverem a server musí znát stejný klíč pro komunikaci s daným klientem.

V praxi bude mít DHCPv6 server uloženy klíče všech známých klientů, což vyžaduje neustálou aktualizaci a navíc představuje bezpečnostní riziko při kompromitaci serveru. **Autentizační prvky DHCPv6 jsou spíše teoretickou než reálně použitelnou konstrukcí.**

Výrazně jednodušší je situace při **zabezpečení komunikace mezi agenty a servery**. K ní dochází v době, kdy oba účastníci již mají nastaveny síťové parametry a normálně komunikují. Lze použít IPsec Agentů i serverů bývá v síti málo, takže i související konfigurace bude poměrně jednoduchá.

Bezstavové DHCPv6

Hlavní nevýhodou bezstavové automatické konfigurace je velmi **omezený sortiment informací,** které lze jejím prostřednictvím získat.Nejpalčivější je absence adres místních DNS serverů, ale občas by se klientům hodily i jiné věci.

Proto obsahuje bezstavová konfigurace možnost, jak doplnit další součásti konfigurace jiným (stavovým) způsobem.

K tomuto účelu slouží kombinace voleb M=0 a O=1. Znamená, že počítač si má adresu a směrování nastavit bezstavově a doplnit k nim další informace získané stavovým protokolem.

K tomuto účelu slouží bezstavové DHCPv6 definované v RFC 3736: *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*.

Jedná se o *velmi* zjednodušenou verzi DHCPv6.
Přebírá formáty zpráv i pravidla chování všech účastníků, ovšem snaží se o maximální jednoduchost a díky tomu snadnou implementovatelnost.
Používá jen dva typy DHCP zpráv:

- žádost o informace
- odpověď.

Také sortiment dostupných voleb je značně omezen.

Celá transakce začíná odesláním zprávy ***Žádost o informace (Information request)* ze strany klienta.**
Její součástí je volba identifikující parametry, které požaduje.

Server sestaví *Odpověď (Reply)* a pošle ji klientovi, který informace v ní obsažené využije..

Vzájemná komunikace je jednodušší, protože na rozdíl od klasického DHCPv6 klient již má (bezstavově) nastavenu adresu a směrování.

Bezstavové DHCPv6 je jednodušší nejen pro implementátory, ale také pro správce. Zpravidla bude třeba poskytovat klientům v místní síti jen adresy lokálních DNS serverů, které bývají pro všechny stejné a příliš se nemění.

Lze očekávat, že konfigurace bezstavového DHCPv6 serveru bude obsahovat pár řádků a vydrží roky.

Jak tedy konfigurovat?

Každá z dostupných variant má své klady a zápory.

Bezstavová konfigurace láká svou jednoduchostí. Nikdo nemusí nic nastavovat (v implicitní konfiguraci operačních systémů a zařízení bývá zapnutá), stroj se prostě zapojí do sítě a funguje. Tedy funguje za předpokladu, že nějak získá informace o DNS. Ty lze doplnit bezstavovým DHCPv6, ovšem v tomto případě už bych byl velmi opatrný v prohlášeních o jeho všeobecné podpoře a rozšíření na straně klientů.

Druhou možností je vyvěsit návod pro ruční konfiguraci, který bude sice stejný pro všechny, takže relativně snadno vytvořitelný, ale není bezpracný.

Druhým problémem bezstavové konfigurace je, že některým správcům sítí při slovech „nikdo nemusí nic nastavovat, zařízení se prostě zapojí do sítě a funguje“ vyráží studený pot na čele. Chaos v síti.

Divocí uživatelé zapojující bez jakékoli kontroly a evidence nejrůznější aparáty. Jak v takové situaci řešit problémy, které způsobí?

Protipólem je stavová konfigurace, čili regulérní DHCPv6. Umožňuje udržovat v síti jakýs takýs pořádek, dodá počítačům kompletní informace, ale pokud se chcete vyhnout náhodně přidělovaným adresám, musíte si udržovat databáze počítačů v síti.

Správa takového systému je pracná, navíc implementace DHCPv6 jsou pořád ještě méně časté a méně kvalitní.

Názor p.Satrapy:

Kdybych si měl zavěštit do budoucna, očekával bych spíše příklon k plug-and-play přístupu. Tedy buď bezstavovou konfiguraci doplněnou bezstavovým DHCPv6 pro zbývající parametry, nebo plnohodnotné DHCPv6 v liberálním nastavení typu „přidělím adresu každému, kdo si o ni řekne“. O pořádek v síti se pak postará autentizace uživatelů protokolem IEEE 802.1X nebo podobným – počítač sice dostane síťové parametry volně, ale jeho komunikace bude zablokována, dokud *uživatel* neprokáže svou totožnost.