

Protokol IPv6, část 2

Obsah přednášky

Průzkum okolí

- Objevování susedů

- Detekce dosažitelnosti

- Objevování směrovačů

- Autokonfigurace

Podpora mobility

- Domácí agent

- Komunikace přes domácího agenta

- Optimalizace cesty

Závěrečné poznámky

Průzkum okolí

- angl. Neighborhood discovery (ND)
- RFC 2461
- Překlady mezi L2 a L3 adresami, autokonfigurace, apod.
- Ekvivalenty službám ARP, RARP, DHCP v IPv4.
- Složky ND
 - Zjišťování L2 adres uzlů v lokální síti a udržování překladových tabulek
 - Kontrola dosažitelnosti sousedů.
 - Detekce duplicitních adres.
 - Hledání směrovačů.
 - Autokonfigurace – stavová a bezstavová

Typu ICMP paketů pro ND

- Neighbor solicitation (NS – výzva sousedovi)
- Neighbor advertisement (NA – ohlášení souseda)
- Router solicitation (RS – výzva směrovači)
- Router advertisement (RA – ohlášení směrovače)
- Redirect (přesměrování)
 - V případě, že směrovač zná krašší cestu než přes sebe.
 - Podobné přesměrování v IPv4.

Hledání linkových adres z IPv6 adres (ND)

- Řešeno pomocí vysílání do multicastové skupiny.
 - Vyčleněn prefix FF02:0:0:0:0:1:FF00::/104.
 - Multicastová skupina pro danou IPv6 adresu: prefix + posledních 24 b z IPv6 adresy.

Příklad

```
FF02:0:0:0:0:1:FF00::/104 +  
28BC:FA3D:21:AA37:1:66FE:9AA4:D678 =  
FF02:0:0:0:0:1:FFA4:D678
```

Hledání linkových adres z IPv6 adres (ND)

- Řešeno pomocí vysílání do multicastové skupiny.
 - Vyčleněn prefix FF02:0:0:0:0:1:FF00::/104.
 - Multicastová skupina pro danou IPv6 adresu: prefix + posledních 24 b z IPv6 adresy.
 - Každý uzel musí poslouchat v multicastové skupině (skupinách) odpovídající jeho IPv6 adrese (adresám).
 - 24 bitů z IPv6 adresy zaručuje, že v dané skupině bude poslouchat velmi málo (typicky 0 nebo 1) uzel.

- Hledající zkonstruuje adresu skupiny z prefixu a IPv6 adresy a do ní pošle **neighborhood solicitation**.
 - Obsahuje hledanou adresu.
 - Vysílající připojí svoji L2 adresu.
- Naslouchající s hledanou IPv6 adresou reaguje pomocí **neighbor advertisement**.
 - Obsahuje hledané IPv6 a L2 adresy.
 - Možné příznaky:
 - R (Router) ... odesílatel je směrovač,
 - S (Solicited) ... ohlášení je vyžádanou reakcí (záznamy je možno aktualizovat bez vyžádání!),
 - O (Override) ... nová informace má přepsat eventuální staré záznamy (měl by být nastaven u nevyžádaných NA a vyžádaných NA, které nebyly poslány na anycastovou adresu).

Formáty paketů NS a NA

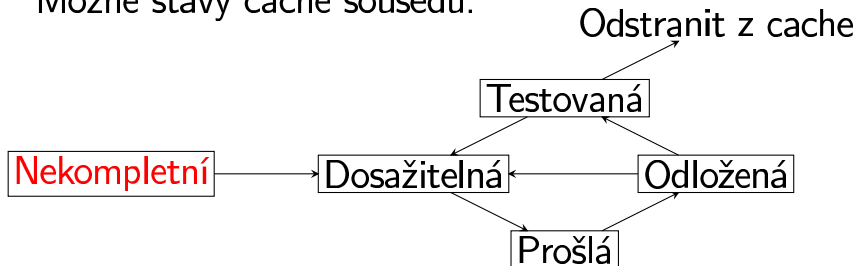
- Neighbor Solicitation
 - IPv6 hlavička
 - Zdrojová adresa: IP adresa odesílajícího rozhraní (ev. nspecifická :: v případě hledání duplicit)
 - Cílová adresa: multicastová nebo unicastová adresa cíle
 - Max. počet hopů: 255
 - Priorita: 15
 - ICMP hlavička
 - Type: 135
 - Code: 0
 - Zdrojová L2 adresa odesílatele, je-li známa (pokud existuje, tak povinně v multicastových a doporučeně v unicastových zprávách)

Neighbor Advertisement

- IPv6 hlavička
 - Zdrojová adresa: IP adresa odesílajícího rozhraní
 - Cílová adresa: jedna z následujících možností
 - a) adresa uzlu, který zaslal NS zprávu
 - b) multicastová adresa všech lokálních uzlů pro nespécifickou původní zdrojovou adresu a pro nevyžádané NA
 - Max. počet hopů: 255
 - Priorita: 15
- ICMP hlavička
 - Type: 136
 - Code: 0
 - Příznaky: R, S, O.
 - "Cílová adresa": u vyžádaných NA je to zdroj NS, u nevyžádaných adresa uzlu, jehož L2 adresa se změnila (nikdy ne multicastová adresa!)
 - Volby: pokud má uzel přidělenou L2 adresu, musí být zahrnuta

Detekce dosažitelnosti

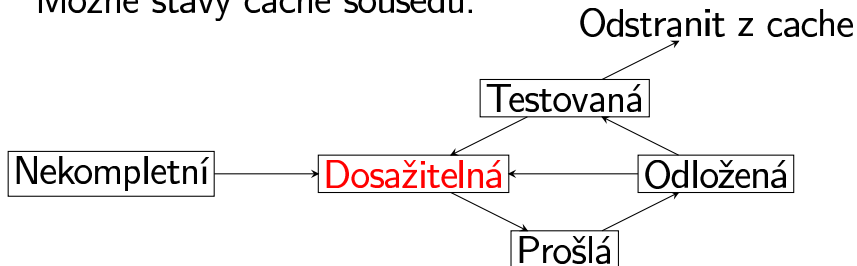
Možné stavy cache sousedů:



L2 adresa není známa. Spouští se proces hledání L2 adresy. Odesílání NS probíhá multicastem.

Detekce dosažitelnosti

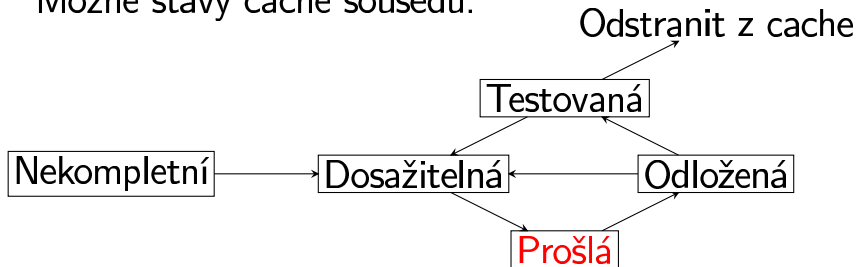
Možné stavy cache sousedů:



Soused žije, „normální“ stav, t.j. záznam v cache není expirovaný.

Detekce dosažitelnosti

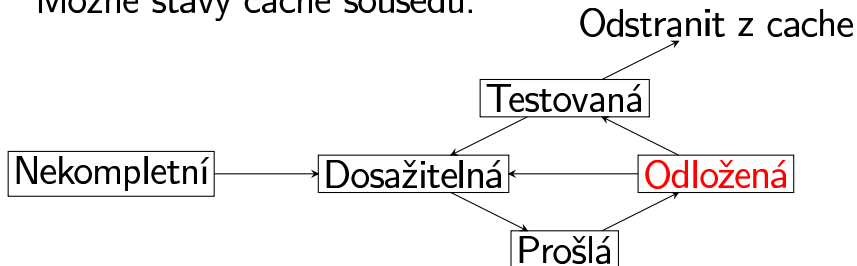
Možné stavy cache sousedů:



Vypršela expirační doba záznamu v cache.
Pokud se se sousedem nekomunikuje, nic se neděje.

Detekce dosažitelnosti

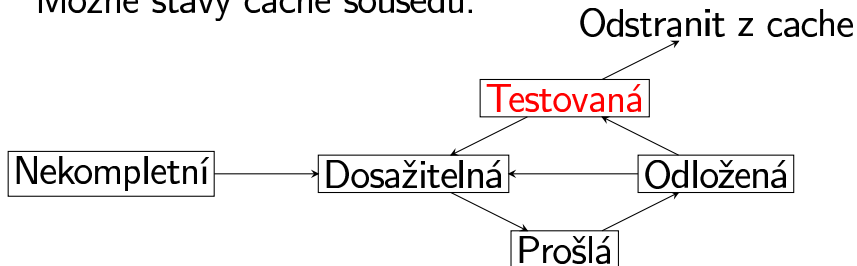
Možné stavy cache sousedů:



Čeká se na potvrzení živosti vyšší komunikační vrstvou (např. TCP). Pokud není potvrzeno, přejde se na proaktivní testování.

Detekce dosažitelnosti

Možné stavy cache sousedů:



Proaktivní testování dosažitelnosti pomocí NS odesílaných unicastem. Po neúspěšných opakováních je záznam vyřazen z cache.

Inverzní objevování sousedů

- angl. Inverse Neighbor Discovery (IND)
- V situaci, kdy je známa L2 adresa a není známa IPv6 adresa.
- Na výzvu (solicitation) reaguje uzel oznámením (advertisement), který obsahuje jednu či více jeho IPv6 adres.
- Zasíláno unicastem.

Objevování směrovačů

- Založeno na výzvěch a oznamech směrovačů (RS a RA)
 - Základní pilíř bezstavové autokonfigurace.
- Výzva směrovači (RS)
 - Směrovače odpovídají oznamem (RA)
 - Ignorováno normálními uzly (ne-směrovači)
 - Podmínky přijetí směrovačem:
 - Maximální počet hopů = 255
 - Korektní autentizace (má-li AH) a kontrolní součet
 - ICMP má délku ≥ 8 a ICMP kód = 0
 - Použité volby mají nenulovou délku

- Struktura výzvy RS
 - Pole IPv6 hlavičky
 - Max. počet skoků je 255
 - Priorita je 15
 - Zdrojová adresa je buď unicastová nebo nspecifikovaná adresa
 - Cílová adresa je zpravidla multicastová adresa směrovačů
 - Pole ICMP hlavičky
 - Type 133
 - Code 0
 - Může obsahovat adresu odesílatele, je-li známa

- Oznam směrovače (RA)
 - Posílány v náhodných intervalech každým směrovačem do přímo připojených sítí nebo jako reakce na výzvu směrovači (RS).
 - Obsahuje specifické informace o směrovači, zejména
 - MTU,
 - prefixy,
 - L2 adresa rozhraní.
 - V případě, že se jedná o reakci na RS, RA obsahuje veškerou volitelnou informaci (zejména všechny validní prefixy).
 - Uzly si tyto informace cachují.

- Struktura oznamu RA
 - Pole IPv6 hlavičky
 - Max. počet hopů je 255
 - Priorita 15
 - Volitelně obsahuje také L2 adresu odesílajícího rozhraní.
 - Cílová adresa je buď multicast nebo unicast (podle toho, jestli se jedná o reakci na RS).

- Struktura oznamu RA (pokračování)

- Pole ICMP hlavičky

- Type 134
- Code 0
- Příznaky

M ... Managed address configuration (použití stavové konfigurace pro IP adresu)

O ... Other stateful configuration (použití stavové konfigurace pro ostatní parametry)

- Router lifetime ... udává, jak dlouho je ještě ochoten směrovač fungovat jako implicitní v sekundách, jinak 0.
- Trvání dosažitelnosti a interval opakování.
- Další volitelné informace důležité pro autokonfiguraci budou diskutovány dále.

Autokonfigurace

- Dva typy
 - Stavová (DHCPv6, podobné DHCP pro IPv4)
 - Bezstavová (RFC 1971, nemá ekvivalent v IPv4)
 - Kombinuje lokálně dostupnou informaci s informacemi propagovanými směrovači. Směrovač oznamuje v RA reagujících na RS všechny prefixy dostupné v dané síti, které jsou spojeny s lokálně generovanou adresou (např. MAC nebo její jedinečný hash).
- Vzájemně se mohou doplňovat
 - Získání IPv6 adresy bezstavovou autokonfigurací, ostatní parametry stavovou.

Bezstavová autokonfigurace

- Informace v RA důležité pro autokonfiguraci
 - Směrovač poskytne informaci o tom, jestli je ochoten fungovat jako implicitní.
 - **Seznam prefixů.**
 - U každého prefixu je uvedena jeho **délka**, **doba platnosti** a **doba preferování** (0xffffffff znamená nekonečnou trvanlivost).

Životní cyklus prefixu

Preferovaný → Odmítaný (deprecated) → Neplatný

- Adresa je ve stavu předběžná (tentative)
- Proveďte se detekce duplicitních adres
 - mandatorní, přístup „důvěřuj ale prověřuj“
 - použije se NS s nspecifickou zdrojovou adresou (::) pro cílovou adresu, kterou chci použít
 - pokud dostanu NA, nsmím adresu rozhraní přiřadit
 - není 100% spolehlivé (např. při přerušení spoje po vyslání NS)
- Pokud vše prošlo, adresa se nastaví jako platná.

Podpora mobility

- IETF draft “Mobility support in IPv6” (Únor 2003)

Problém

Naivní odpojení se a nové zapojení do sítě s sebou nese potenciální změnu IP adresy, což znemožňuje spojitou činnost všech vyšších protokolů.

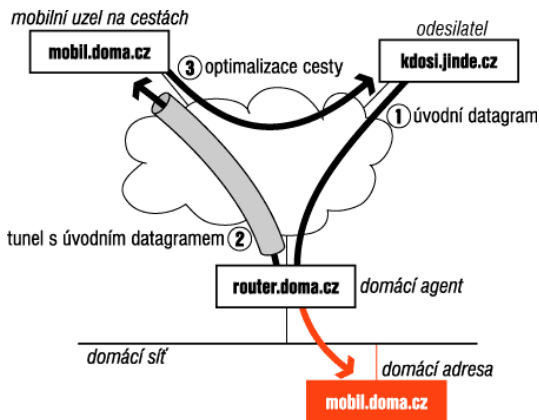
- Princip řešení
 - Stabilní **domovská adresa**, nezávislá na způsobu připojení
 - Uzel komunikuje prostřednictvím této domovské adresy
 - Změna umístění uzlu transparentní pro vyšší vrstvy

Základní pojmy

- **Domovská adresa** – odpovídá „domácímu“ (výchozímu) umístění uzlu
- **Care-of adresa** – konkrétní IPv6 adresa, kterou uzel získá při pohybu
 - Uzel může mít současně více care-of adres
 - Mezi domovskou a každou care-of adresou se musí ustavit **vazba** (binding)
- **Korespondující uzly** – spolu komunikující uzly
 - Korespondující uzel se může dozvědět aktuální care-of adresu prostřednictvím odpovídající vazby (correspondent binding procedure)

Přístupy k řešení

- Přes domácího agenta
- Pomocí optimalizace cesty



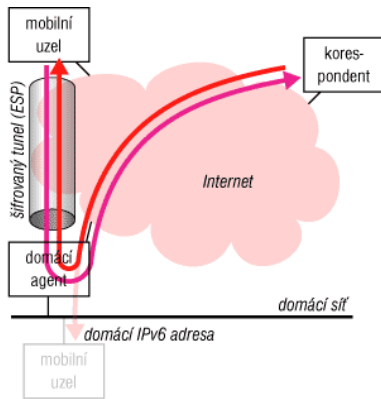
Domácí agent

- Udržuje cache vazeb a seznam domovských agentů
- Zpracovává vazby
 - Primární care-of adresa
 - Změna (přeregistrace) care-of adresy
 - Smazání care-of adresy
- Podpora nalezení adresy domovského agenta
- Změna prefixu domovské sítě

- Zpracování paketů
 - Zachytávání paketů pro mobilní uzly
 - Neighbor Advertisements jménem mobilního uzlu
 - Zpracování zachycených paketů
 - Tunelování paketů na care-of adresu
 - Nepřeposílá pakety pro link-local adresu mobilního uzlu
 - Pouze multicastové adresy s globálním rozsahem přeposílány jsou
 - Podpora přihlášení do multicastových skupin
 - DHCPv6 pro mobilní uzly
 - Přeposílání paketů z mobilních uzlů
 - Ochrana Return routability paketů

Komunikace přes domácího agenta

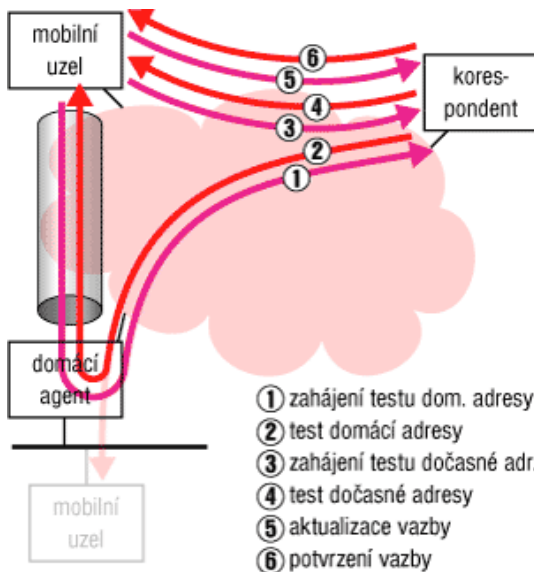
- Používá domovského agenta (směrovač)
- Proxy Neighbor Discovery – zachycení paketů určených pro mobilní uzel
- Oboustranné tunelování přes domovský směrovač
- Používá IPv6 zapouzdření a šifrování (ESP) pro přenos dat (tunelování)



Optimalizace cesty

- Korespondující uzly komunikují přímo (po iniciaci tunelem)
- Původní zabezpečení pomocí IPsec (do r. 2000)
 - Problém s neexistencí všepokrývající PKI infrastruktury (korespondent může být kdokoli)
- Return routability procedure (od draftu z r. 2002, nyní RFC 3775)
 - Ověří, že nabídnutá care-of adresa patří deklarovanému uzlu
 - Dvě dvojice zpráv:
 - Home Test Init (HoTI, 1) a Care-of test Init (CoTI, 3) (výzvy)
 - Home test (HoT, 2) a Care-of test (CoT, 4) (odpovědi)

Return routability procedure (RRP)



Zabezpečení RRP

- Mobilní uzel (MN) pošle HoTI pro získání home keygen tokenu.
- MN pošle CoTI pro získání care-of keygen tokenu.
- Korespondující uzel vygeneruje tokeny pomocí svého interního klíče K_{cn}
 - home keygen token :=
 $\text{First}(64, \text{HMAC_SHA1}(K_{cn}, (\text{home address}, \text{nonce}, 0)))$
 - care-of keygen token :=
 $\text{First}(64, \text{HMAC_SHA1}(K_{cn}, (\text{care-of address}, \text{nonce}, 1)))$

- Korespondující uzel odešle **tokeny** a **nonce indexy** ve zprávách HoT a CoT.
- Mobilní uzel spojí oba keygen tokeny a vytvoří vlastní klíč
$$K_{bm} := \text{SHA1}(\text{home keygen token}, \text{care-of keygen token})$$
- K_{bm} se používá pro autentizaci aktualizace vazeb.
- Klíč pro zrušení vazby je
$$K_{bm} := \text{SHA1}(\text{home keygen token})$$

Aktualizace vazeb

- Mobilní uzel pošle Binding Update (BU) zprávu
 - care-of adresa jako zdrojová, adresa korespondujícího uzlu jako cílová
 - parametry: domovská adresa, pořadové číslo BU, home nonce index, care-of nonce index, $\text{HMAC_SHA1}(K_{bm}, (\text{care-of address}, \text{CN address}, \text{BU}))$
- Korespondující uzel si spočte K_{bm} s využitím nonce indexů a ověří platnost vazby.
- Pokud projde, aktualizuje cache.

Literatura

- příslušná RFC: 1886, 1887, 1971, 1981, 2373, 2461, 2874, 3775
- Satrapa P., IPv6, Neocortex, Praha, 2002
- Web IPv6, CESNET, <http://www.ipv6.cz/> a server Lupa
 - ... posloužil jako zdroj obrázků (s poděkováním P. Satrapovi!)