Dokumentácia projektu

Programovanie sieťovej služby

Router Advertisement

ISA 2010/2011

Milan Kubík
xkubik17@stud.fit.vutbr.cz
V Brne, 29. novembra 2010

Zadanie

Cieľom projektu bolo naštudovať automatickú konfiguráciu v protokole IPv6 a vytvoriť aplikáciu schopnú odchytávať Router Advertisement pakety, pričom táto dokáže zachytené pakety upraviť a odoslať ich naspäť na sieť. Program nesmie skolabovať pri prijatí paketu s rozširujúcou hlavičkou.

Zo zachyteného paketu bolo potrebné zistiť základné prenášané údaje ako zdrojová a cieľová IP adresa, router lifetime, príznaky[1], a detailné informácie o prenášaných sieťových prefixoch.

Rozšírenie zadania

Implementovaný program okrem informácií o sieťových prefixoch spracováva aj MTU, source-link layer a target-link layer položky RA paketu

Pri spustení s voliteľným parametrom *-s* program vygeneruje Router Solicitation paket a odošle ho na zadané rozhranie.

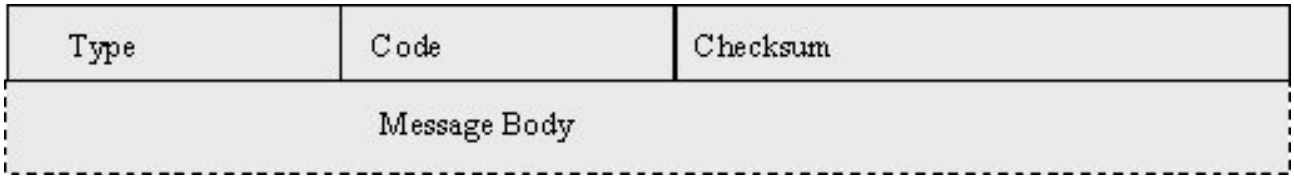
1 Bude uvedené v popise RA paketu

Teoretický základ

Internet control message protocol – ICMP

Protokol ICMP je režijným protokolom internetu. Používa sa na prenos chybových, testovacích a iných prevádzkových informácií. Je nedeliteľnou súčasťou implementácie IP protokolu.

ICMPv6 je implementáciou pre IPv6 protokol. Samotná špecifikácia možností je pomerne rozsiahla a pokrýva ju niekoľko RFC dokumentov. Všetky ICMP správy majú jednotný základ, ktorý nesie jednotlivé položky podľa ich konkrétneho typu.



Obrázok 1: Formát ICMPv6 hlavičky

Typ určuje základný druh správy bližšie identifikovaný jej kódom. Správy sú rozdelené do dvoch tried. Správy s typom z intervalu 0 až 127 sú určené na signalizáciu chybových stavov a správy s typom z intervalu 128 až 255 sú určené na informačné účely[2]. V našom prípade nás zaujímajú iba niektoré vyššie typy ICMP správ.

Neighbor discovery

V IPv4 sa na zistenie fyzickej adresy partnera používa protokol ARP (Address Resolution Protocol). Funguje na základe posielania výziev na broadcastovú adresu, na ktorú vlastník IP adresy, ktorej MAC adresa je požadovaná reaguje.

Ekvivalent funkčnosti ARP je v prípade IPv6 priamo súčasťou tohto protokolu. Okrem rezolúcie fyzickej adresy navyše dokáže riešiť niekoľko ďalších problémov ako sú vyhľadávanie smerovačov, šírenie informácií o parametroch siete a ďalších, potrebných pre automatickú konfiguráciu adresy, overovanie dosiahnuteľnosti susedných zariadení či zaistenie bezkonfliktnosti adresy.

Automatická konfigurácia

IPv6 ponúka dva druhy automatickej konfigurácie. Stavovú a bezstavovú. Stavová konfigurácia je klasický spôsob, kedy existuje v sieti dedikovaný server, spravujúci konfiguráciu a tú na požiadanie poskytuje klientom. Je to mechanizmus podobný ARP či DHCP. V IPv6 týmto spôsobom pracuje DHCPv6. Klient na obecnú adresu odošle svoju požiadavku a server mu oznámi parametre siete.

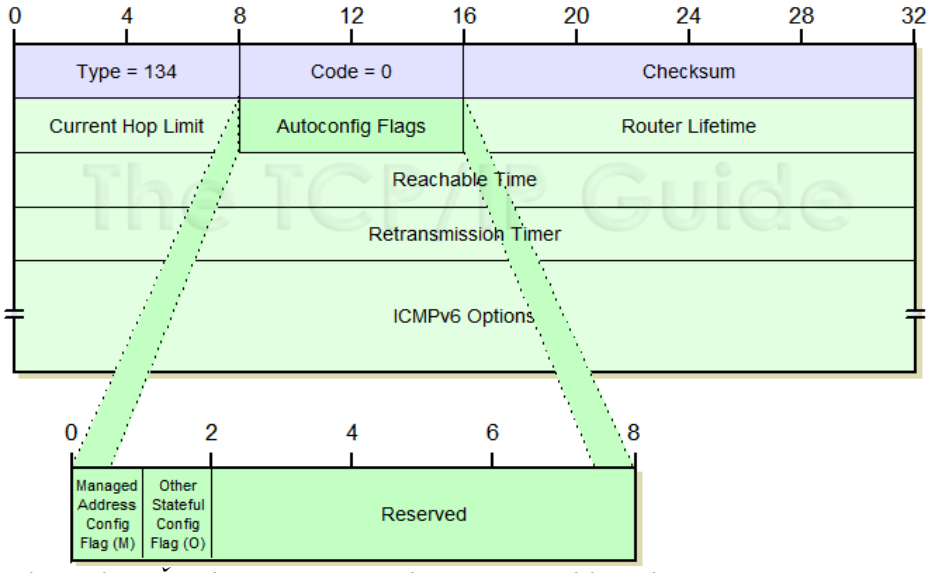
Oproti tomu, bezstavová konfigurácia je založená na tom, že v sieti sú prítomné smerovače, ktoré majú všetky potrebné informácie a s určitým intervalom ich šíria na sieť. Práve pripojenému počítaču stačí chvíľu načúvať alebo si o konfiguráciu aktívne požiadať.

2 http://www.iana.org/assignments/icmpv6-parameters

Router advertisement

Oznámenia smerovača sú základným nástrojom pre bezstavovú konfiguráciu. V náhodných intervaloch ich posiela každý smerovač do všetkých sietí, ku ktorým je pripojený.

Oznámenia smerovača sú šírené pomocou ICMP protokolu. V základnej hlavičke je niekoľko dôležitých informácií, samotné adresy siete sú ale šírené ako položky, ktoré voliteľne nasledujú základnú hlavičku. Významnú úlohu hrá položka hlavičky obsahujúca niekoľko riadiacich príznakov.



Obrázok 2: Štruktúra Router Advertisement hlavičky

Typ ICMP 134 označuje Router Advertisement paket. Kontrolným súčtom je Internet checksum.

Dôležitou položkou správy je *router lifetime*, určujúci počet sekúnd, počas ktorých daný router bude implicitným pre uzlu danej siete. *Current hop limit* udáva pre uzly v sieti, akým maximálnym počtom skokov obmedzovať životnosť nimi vytváraných datagramov.

Prvé dva bity sa týkajú nastavenia DHCPv6. Ich kombinácia určuje akým spôsobom bude uzol siete nastavený.

M príznak – managed, oznamuje, že o konfiguráciu sa stará DHCP.

O príznak – other, určuje, či ostatné informácie, ako napríklad adresy lokálnych DNS servrov sú tiež šírené s DHCPv6.

Managed	Other	význam
1	-	DHCP poskytuje všetky informácie
0	1	Kombinované nastavenie, adresa, prefix a routovanie bezstavovo, zbytok DHCP
0	0	DHCP nie je k dispozícii

Tabuľka 1: Význam kombinácií

Je definovaných niekoľko ďalších príznakov:

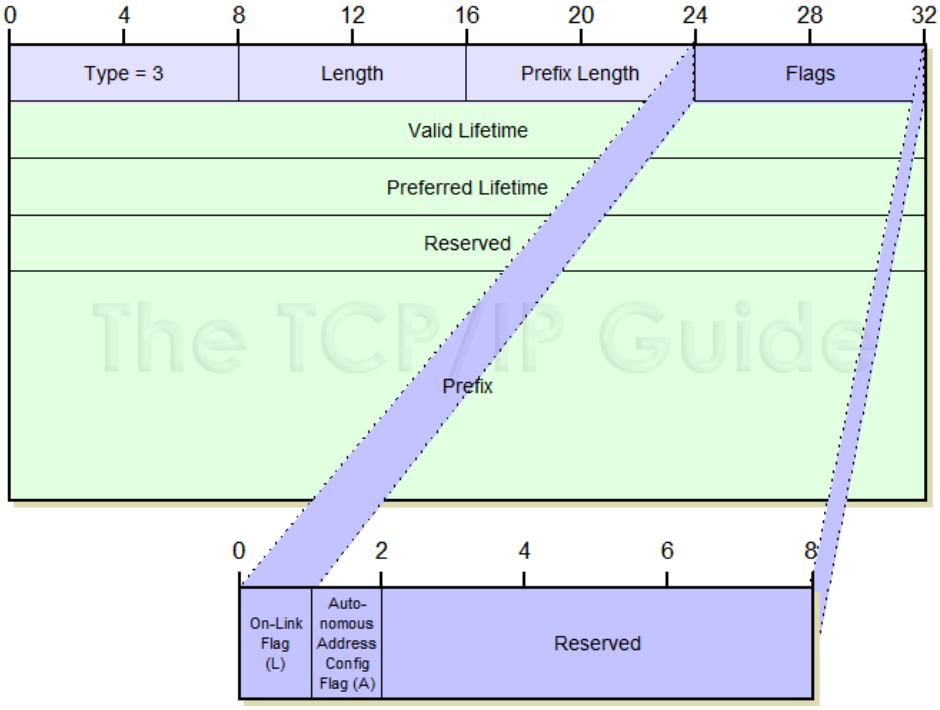
- `H - Mobile IPv6 Home Agent`
- `Prf - Router Selection Preferences`
- `P - Neighbor Discovery Proxy`

Router Selection Preference **–** používa sa na označenie priority pri smerovaní v sieťach, ktoré daný smerovač obsluhuje. Bližší popis je obsahom RFC 4191.

neighbor discovery proxy – príznak pre experimentálny protokol

Prefixy adries

Sú hlavným nástrojom bezstavovej konfigurácie. Nakoľko uzly na jednej fyzickej sieti môžu byť organzované do viacero logických sietí, môžu smerovače v jednej správe šíriť viacero prefixov.



Obrázok 3: RA prefix voľba

Dĺžka prefixu udáva, koľko bitov prefixu je platných. *Valid* a *preffered* lifetime sú hodnoty určujúce platnosť daného prefixu a dobu, kedy sú v platnosti adresu vytvorené pomocou tohto prefixu. V oboch prípadoch hodnota 0xffffffff znamená neobmedzenú dobu.

RA obsahuje tri príznaky, jednobitové on-link a autonomouse, určujúce, či adresa odvodená z prefixu má byť považovaná za lokálnu adresu a či daný prefix možno použiť pre automatické vytvorenie adresy. Posledný príznak R – router address bol doplnený pre potreby mobilných zariadení. Ak je nastavený, prefix obsahuje kompletnú adresu smerovača.

Určenie adresy

Uzol zahajuje priradenie adresy tým, že si vygeneruje základnú linková adresu s prefixom ff80::/10, pripojí identifikátor svojho rozhrania. O unikátnosti takto pridelenej adresy sa presvedčí poslaním Neighbor solicitation ostatným uzlom na sieti a hľadá vlastníka práve vygenerovanej adresy. Ak sa žiaden uzol neozve, pridelená adresa je unikátna.

Pre pokračovanie v prideľovaní adresy uzol potrebuje poznať informácie o sieti. Má dve možnosti. Buď pasívne počkať na plánované oznámenie smerovača, alebo oň aktívne požiadať, pomocou *Router Solicitation*. ZA prijatého oznámenia sa dozvie, či má použiť bezstavovú konfiguráciu pre pridelenie vlastnej adresy a ostatné informácie o sieti. Pokiaľ áno, spojí prefix so sebou vygenerovanou adresou, ktorá už bola overená na duplicitu. Na duplicitu sa rovnakým spôsobom testuje aj stavovo pridelená adresa.

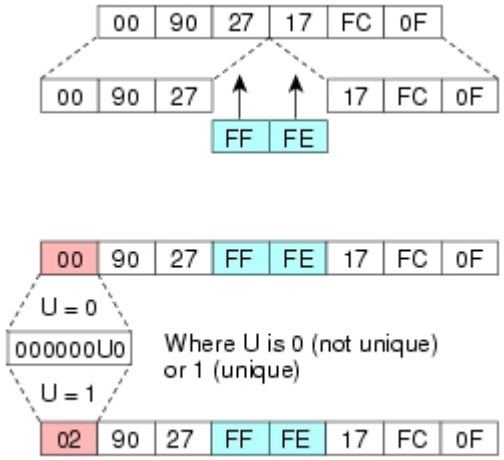
Identifikátor rozhrania a modifikované EUI-64

Základná podoba identifikátoru je odvodená od IEEE EUI-64. Je to štandard pre určovanie globálnych identifikátorov pre počítačové siete. Ich dĺžka je 64 bitov a odpovedá vyhradenému priestoru v IPv6 adrese.

V najjednoduchšom prípade rozhranie EUI-64 identifikátor pridelený má. Ten sa do adresy prevezme s úpravou jednoho bitu. Druhý najmenej významný bit určuje, či ide o celosvetovo unikátnu adresu – bit je nastavený na 0, alebo o lokálnu adresu – bit na 1.

Modifikované EUI-64 tento bit invertuje. Tzn. 0 predstavuje lokálny identifikátor a 1 globálny.

Samotné určenie identifikátora pri určení adresy etheretovej či wi-fi karty prebieha za použitia ich MAC 48 bitovej MAC adresy, kedy sa za prvé tri oktety (v polovici) vloží hodnota 0xfffe a nastaví sa príznak na druhom najmenej významnom bite.



Obrázok 4: Modifikované EUI-64

Popis implementácie

Program sa spúšťa z príkazovej riadky s jedným povinným a dvoma[3] voliteľnmi parametrami

rasniffer -i <interface> [-r] [-s]

Povinná voľba interface určuje, na ktorej sieťovej karte budú RA oznamy sledované, voľba -r znamená, že program odchytené pakety upraví a odošle späť. Voľba -s spôsobí, že program po svojom spustení odošle jeden Router Solicitation paket.

Program je logicky rozdelený do niekoľkých modulov. Sú to hlavná aplikácia, sniffer, modul pre posielanie dát a modul pre získanie MAC adresy.

Po odchytení paketu knižnicou pcap, je tento spolu s parametrami príkazového riadka predaný snifferu, ktorý prechádza cez obsah paketu a spracováva ho. Z IPv6 hlavičky prečíta potrebnú dvojicu IP adries, v prípade potreby preskočí rozširujúce IPv6 hlavičky, čím sa dostane k obsahu ICMPv6.

Ak je daným ICMP paketom ohlásenie smerovača, program z neho číta potrebné informácie a vypisuje ich na štandardný výstup. V spracovaní volieb, ak voľbu nepozná, oznámi to na štandardný chybový výstup a pokračuje v činnosti. Keďže volieb nie je dopredu určený počet, prechod cez ne je iteratívny a obmedzený informáciou o dĺžke paketu z IP hlavičky.

3 Rozšírené o Router Solicitation

Posielanie paketu je realizované úpravou paketu prijatého. Tým pádom program môže podvrhovať sebou upravené informácie do všetkých lokálnych logických sietí. Samotná požadovaná úprava je vymaskovanie dvoch bitov v správe. Následne je správa odoslaná cez RAW soket na multicastovú adresu ff02::1, do tejto skupiny patria všetky uzly na lokálnej linke.

Program takto ale prijme svoj vlastný paket. Potenciálne zacyklenie a zahltenie linky je ošetrené kontrolou MAC adresy odosielateľa porovnanej voči MAC adrese sieťovej karty na ktorej sa počúva.

Zhrnutie

V súčasnej podobe program odosiela pakety s upravenou preferenciou na nízku. Potenciálne však môže upravovať ktorúkoľvek časť RA paketu podľa potreby. Týmto spôsobom sa môže pokúsiť previesť na seba komunikáciu v sieti ako nový prioritný router a sledovať komunikáciu na sieti, čo predstavuje isté bezpečnostné riziko.

Pri diagnostickom použití podáva informácie o konfigurácii siete a smerovačoch.

Program je preložiteľný a funkčný na GNU/Linux (písané na Arch linuxe) a freeBSD systémoch. Testovanie prebiehalo za pomoci poskutnutého obrazu freeBSD, ochytávaním paketov na sieti kolejnet a nástroja radvd.

Zoznam použitej literatúry

SATRAPA, Pavel. *Internetový protokol IPv6* [online]. 2. vydanie. Praha : CZ.NIC, z. s. p. o., 2008 [cit. 2010-11-29]. Dostupné z WWW: <http://knihy.nic.cz/>. ISBN 978-80-904248-0-7.

STEVENS, Richard W; FENER, Bill; RUDOFF, Andrew M . *UNIX Network Programming : Vol. 1, the sockets networking API* . 3rd ed. Boston : Addison-Wesley , 2004. xxiii, 991 s. ISBN 0-13-141155-1.

NETWORK WORKING GROUP, *Internet Protocol, Version 6 (IPv6) Specification* [online], 1998, [cit. 2010-11-29]. Dostupné z www: <http://tools.ietf.org/html/rfc2460>

NETWORK WORKING GROUP, *Neighbor Discovery for IP version 6 (IPv6)* [online], 2007, [cit. 2010-11-29]. Dostupné z www: <http://tools.ietf.org/html/rfc4861>

NETWORK WORKING GROUP, *IPv6 Router Advertisement Flags Option* [online], 2008, [cit. 2010-11-29]. Dostupné z www: <http://tools.ietf.org/html/rfc2460>

CELTDRA, Aragoen. *Routemyworld.com* [online]. 2009 [cit. 2010-11-29]. BSCI: IPv6 Addressing Architecture. Dostupné z WWW: <http://routemyworld.com/2009/02/05/bsci-ipv6-addressing-architecture/>.