

Sniffer OSPFv2 a OSPFv3

Dokumentace projektu pro předmět Síťové aplikace a správa sítí

Martin Knapovský

VUT FIT Brno

xknapo02@stud.fit.vutbr.cz

Obsah

[Úvod 3](#_Toc310102792)

[Směrovací protokoly 3](#_Toc310102793)

[OSPF 3](#_Toc310102794)

[Typy zpráv protokolu OSPF 3](#_Toc310102795)

[Databázové informace 4](#_Toc310102796)

[Popis programu 4](#_Toc310102797)

[Spuštění 5](#_Toc310102798)

[Implementace 5](#_Toc310102799)

[Moduly 5](#_Toc310102800)

[Logické části programu 5](#_Toc310102801)

[Použitá Literatura 7](#_Toc310102802)

[Metriky projektu 7](#_Toc310102803)

[Příloha – Parametry překladu programu 8](#_Toc310102804)

# Úvod

Cílem projektu bylo implementovat aplikaci pro odposlech OSPF zpráv podporující IPv4 a IPv6 LSA topologické informace a po ukončení tohoto programu i exportér OSPFv3 LSA topologických informací. Aplikace je implementována v programovacím jazyku C pro prostředí FreeBSD/Linux.

# Směrovací protokoly

Směrovací protokoly zahrnují sadu procesů, datových struktur, algoritmů a zpráv, které slouží k přenosu informací mezi směrovači. Umožňují tak směrovači se autonomně rozhodnout o tom, na který výstup odešle zprávy, které nejsou určeny pro zařízení k němu přímo připojená, ale pro zařízení, ke kterým pomocí směrovacích protokolů získal cestu.

Směrovací protokoly se rozdělují na *Distance Vector* a *Link State* protokoly. Distance Vector protokoly jsou vhodné pro menší sítě, ve kterých není potřeba znát síťovou topologii. Pro výpočet nejlepší cesty používají Bellman-Fordův algoritmus a mezi typické zástupce patří protokoly RIPv1, RIPv2, IGRP, EIGRP. Oproti tomu Link State protokoly vytváří kompletní pohled na topologii sítě a umožňují tak efektivnější směrování v rozsáhlejších sítích.

## OSPF

Open Shortest Path First, neboli zkráceně OSPF je Link State směrovací protokol využívající Dijkstrova algoritmu stejného názvu. Byl vyvinut jako náhrada protokolu RIP, zahrnuje koncept oblastí a pomocí výše zmíněného algoritmu vytváří kompletní topologii sítě. To mu umožňuje nasazení ve větších, hierarchicky strukturovaných sítích s možností pozdějšího růstu.

Protokol za svou dobu prošel několika inovacemi. Původní OSPFv1 byl pouze experimentální, ktežto OSPFv2, který byl vyvinut Johnem Moyem v roce 1991 se dočkal okamžitého nasazení na poli počítačových sítí. Nejnovější revize OSPFv3 zahrnuje podporu IPv6 a zjednodušuje některé ze zpráv, které používá jeho předchůdce.

## Typy zpráv protokolu OSPF

Následující tabulka uvádí typy zpráv protokolu OSPFv2 a OSPFv3.

|  |  |  |
| --- | --- | --- |
| Kód zprávy | Typ zprávy | Popis |
| 0x01 | Hello | Slouží k objevení sousedů a navázání spojení mezi směrovači. |
| 0x02 | Database Description | Obsahuje zkracený seznam databáze směrovacích informací. |
| 0x03 | Link-State Request | Požadavek na směrovací informace. |
| 0x04 | Link-State Update | Odpověď na požadavek obsahující směrovací informace. |
| 0x05 | Link-State Acknowledgment | Potvrzení příjmu směrovacích informací. |

## Databázové informace

Informace o databázi směrovače jsou distribuovány ve formě zpráv *Link-State Advertisments* (LSA), které jsou obsaženy ve zprávě typu *Link-State Update.* Zde jsou již typy zpráv různých revizí více odlišné. V následující tabulce jsou uvedeny typy zpráv a jejich popis pro OSPFv3.

|  |  |  |
| --- | --- | --- |
| Kód zprávy | Typ zprávy | Popis |
| 0x2001 | Router-LSA | Popis stavu a metriky rozhranní směrovače. |
| 0x2002 | Network-LSA | Popis všech směrovaču připojených k danému spoji. |
| 0x2003 | Inter-Area-Prefix-LSA | Popis cest a prefixů v jiných oblastech. |
| 0x2004 | Inter-Area-Router-LSA | Původcem těchto zpráv jsou hraniční směrovače informující ostatní hraniční směrovače v jiných oblastech o vnitřních cestách. |
| 0x4005 | AS-External-LSA | Slouží pro popis implicitní cesty. |
| 0x2006 | Neschváleno |  |
| 0x2007 | NSSA-LSA | Vysílány hraničními směrovači k popisu vzdálených lokací mimo autonomní systém. |
| 0x0008 | Link-LSA | Pro každý fyzický spoj je generána zpráva tohoto typu, která poskytuje informace směrovačům na daném spoji o adresách typu *link-local* a prefixech. |
| 0x2009 | Intra-Area-Prefix-LSA | Určeno pro šíření informací o prefixech spojených s místní adresou směrovače, síťovým segmentem, nebo připojeným tranzitním síťovým segmentem. |

# Popis programu

Program zachytává zprávy na naslouchaném ethernetovém rozhranní v promiskuitním módu a vypisuje informace v nich obsažené. Tyto informace zahrnují výpis hlavičky ethernetového rámce, výpis hlavičky IP packetu a dále hlavičku, typ zprávy popř. další doplňující informace OSPF ve zprávě obsažené. Po ukončení programu zasláním signálu SIGINT je programem vypsána OSPFv3 topologie z odposlechnutých zpráv.

Spuštění

Pro spuštění je potřeba programu pomocí parametru zadat rozhranní, na kterém bude naslouchat pomocí přepínače *–i* následujícím způsobem :

*./myospfsniffer –i eth1*

,kde *eth1* je rozhranní, na kterém se bude naslouchat. Pro výpis nápovědy je možné použít přepínač *–h*.

## Implementace

### Moduly

Program je rozčleněn do několika modulů :

sys - obsahuje funkce pro tisk nápovědy, ethernetových a ip hlaviček a dále funkce pro tisk IPv4 a IPv6 adres a jejich prefixů

const - definice kostant použitých v programu

binary - makro pro převod čísla z binární reprezentace do reprezentace programovacího jazyka C

ospfv2 - struktury a funkce pro výpis OSPFv2 informací

ospfv3 - struktury a funkce pro výpis OSPFv3 informací

ospfv3\_db - struktury a funkce pro záznam a výpis OSPFv3 topologie

main - samotný program

### Logické části programu

#### Odposlech zpráv na rozhranní

Pro odposlech byla použita knihovna *libpcap*, bez použití filtrace, což umožnilo zpracovat přijaté zprávy přímo v programu a vypsat tak přesné pořadové číslo tak, jak to dělá například program *Wireshark*. Pro použití filtru je však možné změnit definici *FILTER\_EXP*, v hlavičkovém souboru *main.h*. Stejně tak je možné zapnout/vypnout výpis ladících informací pomocí definice *DEBUG*, v hlavičkovém souboru *const.h*. Seznam dalšího nastavení překladu programu je obsažen v příloze 1.

#### Zpracování

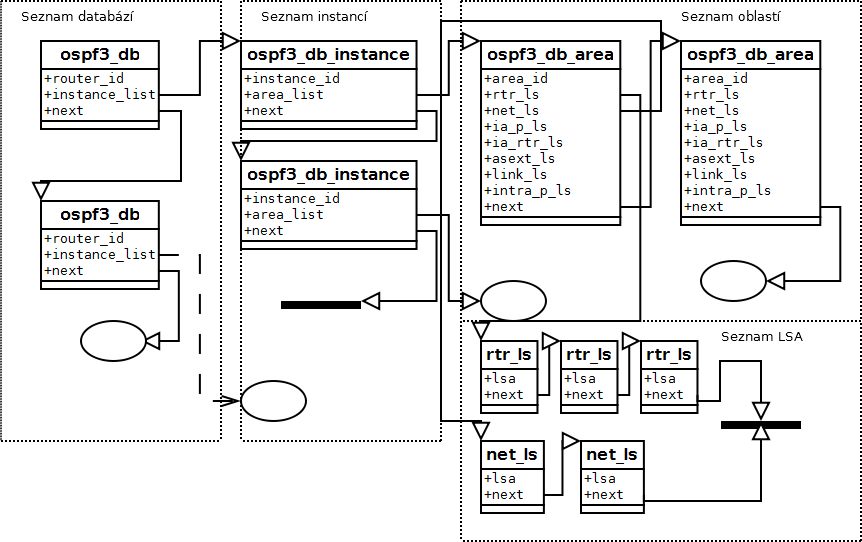
O zpracování zprávy se stará funkce *got\_packet*, která postupně rozlišuje struktury zprávy dle jejího typu (IPv4/IPv6, OSPF typy zpráv), vypisuje celé tyto struktury na standartní výstup a ukládá relevantní informace do databáze za použití dříve uvedených modulů. Formát výpisu zprávy lze změnit pomocí změny definic *ETHERNET\_FORMAT, IP\_FORMAT, OSPF\_HEADER\_FORMAT, OSPF\_TYPE\_FORMAT, OSPF\_LSA\_HEADER\_FORMAT* a *OSPF\_LSA\_FORMAT*.

#### Tisk LSA

Je vhodné zmínit funkce pro tisk *print\_ospf2\_lsa* a *print\_ospf3\_lsa.* Tyto funkce přijímají jako parametr ukazatel na hlavičku LSA části OSPF zprávy, samostatně pak rozlišují typ předaného LSA a prostřednictvým pomocných funkcí tisknou LSA na standartní výstup. Problém nastává u struktur zprávy, které nemají přesně danou velikost jako například pole *prefix* u OSPFv3 Inter-Area-Prefix LSA, kde je nutné tuto velikost zjistit a pracovat s pamětí pouze v rozsahu zprávy. Dále se ve zprávách vyskytují pole, která se mohou opakovat. Je opět nutné ze zprávy zjistit počet opakování a tisknout pouze relevantní informace.

#### Databáze topologických informací

Databáze topologických informací je rozčleněna do několika struktur. Je vhodné rozlišovat informace od různých směrovačů, jejichž informace byla na rozhranní odposlechnuta a dále identifiční číslo instance procesu OSPF, která dané informace ze směrovače vyslala. LSA informace mohou patřit do různých oblastí a mohou být různého typu, což je potřeba pro efektivní prohledávání databáze také rozlišit. Vzhledem k tomu, že předem nevíme kolik routerů/instancí/oblastí budou odposlechnuté zprávy obsahovat, byly pro implementaci databáze zvoleny jednosměrně vázané seznamy. Na následujícím diagramu je znázorněna struktura databáze.



Obr. 1 – Struktura Databáze

Topologická databáze je po zaslání signálu *SIGINT* celá vytištěna na standartní výstup ve formátu blížícímu se výpisu topologické databáze na směrovačích Cisco.

# Použitá Literatura

* RFC5340, RFC2328
* Přednášky CCNA2

# Metriky projektu

3061 řádků kódu

# Příloha – Parametry překladu programu

Program je spustitelný na operačních systémech FreeBSD a Linux. Pro překlad na operačním systému FreeBSD použijte GNU Make bez parametrů.

*> gmake*

Pro překlad na operačním systému Linux je potřeba dodat parametr *linux*.

*> make linux*

V následující tabulce jsou uvedena různá nastavení programu, kterými lze změnit chování programu.

|  |  |
| --- | --- |
| Nastavení | Popis |
| PRINT\_IP | výpis IP hlaviček |
| PRINT\_ETHERNET | výpis Ethernetových hlaviček |
| PRINT\_PACKET\_NUMBER | výpis pořadového čísla packetu |
| PRINT\_OSPF\_NUMBER | výpis pořadového čísla OSPF zprávy |
| IP\_PRETTY\_PRINT | zapne výpis zkraceného tvaru IP adres a prefixů |
| DEBUG | zapne výpis ladících zpráv |
| ETHERNET\_FORMAT | odsazení výpisu Ethernetové hlavičky |
| IP\_FORMAT | odsazení výpisu IP hlavičky |
| OSPF\_HEADER\_FORMAT | odsazení výpisu OSPF hlavičky |
| OSPF\_TYPE\_FORMAT | odsazení výpisu OSPF zprávy (Hello, DBU, ...) |
| OSPF\_LSA\_HEADER\_FORMAT | odsazení výpisu LSA hlavičky |
| OSPF\_LSA\_FORMAT | odsazení výpisu LSA zprávy |
| PRINT\_LLS | zapne výpis LLS bloku |

Tato nastavení se provádějí změnou definic v hlavičkovém souboru *const.h*.