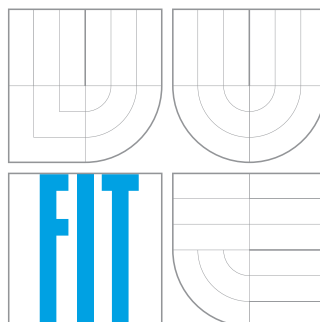


FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ



Protokol RIPng v prostředí OMNeT++

AUTOR PRÁCE

Bc. JIŘÍ TRHLÍK

VEDOUCÍ PRÁCE

Ing. VLADIMÍR VESELÝ

BRNO 2012

Obsah

1	Úvod	2
2	Směrovací protokol RIPng	3
2.1	Historie	3
2.2	Vlastnosti	3
2.3	Komunikace	4
2.3.1	Formát zprávy protokolu RIPng	4
2.3.2	Speciální typ RTE	5
2.4	Zprávy typu Response	5
2.4.1	Vytvoření zprávy typu Response	5
2.4.2	Zpracování zprávy typu Response	5
2.5	Zprávy typu Request	6
2.5.1	Zpracování zprávy typu Request	6
2.6	Časovače	7
2.7	Proces smazání cesty	7
3	Závěr	8
	Literatura	9

Kapitola 1

Úvod

Projekt OMNeT++ [7] poskytuje vyvojové a simulační prostředí pro tvorbu diskretních simulací. Usnadnění vytváření simulací z oblasti síťové komunikace poskytuje framework INET [4], jehož zkoumáním a rozšířením se zabývá projekt ANSA [1] na Fakultě informačních technologií Vysokého učení Technického v Brně. Projekt ANSA se zaměřuje na možnost modelování, simulací a analýzy počítačových sítí.

Cílem této práce je implementovat směrovací protokol RIPng v prostředí OMNeT++, přičemž tento protokol bude součástí frameworku INET.

Protokol RIPng je popsán v kapitole 2. Jsou zde uvedené vlastnosti tohoto protokolu a také jeho stručná historie.

Kapitola 2

Směrovací protokol RIPng

V této kapitole je stručně popsána historie protokolu RIP, ze kterého protokol RIPng vychází. Dále jsou zde popsány vlastnosti a specifikace protokolu RIPng. Přestože zmíněné protokoly sdílejí většinu vlastností, budou tyto vlastnosti vztaženy přímo k protokolu RIPng.

2.1 Historie

První specifikace protokolu RIP je popsána v RFC 1058 [3] z roku 1988. Samotný protokol RIP ale vznikl dříve (koncem 70. let) a je nejstarším používaným směrovacím protokolem. Rozšířil se díky své jednoduchosti, která předčila jeho nedostatky. Jedním z velkých nedostatků první verze protokolu RIP bylo směrování podle tříd IPv4 adres A, B nebo C. To neumožňovalo existenci různě velkých podsítí uvnitř jedné třídy IP adres.

Proto byla v roce 1993 vyvinuta druhá verze tohoto protokolu - RIPv2 (naposledy upravena v roce 1998 a popsána v RFC 2453 [6]). Ta odstraňuje třídnost tohoto protokolu – díky uvedení masky sítě v zasílaných aktualizacích – a navíc zavádí autentizaci.

Protokol RIPng je rozšířením protokolu RIPv2, jeho specifikaci lze nalézt v RFC 2080 [5] z roku 1997, a přináší podporu pro IPv6 sítě.

2.2 Vlastnosti

RIPng je vektorově orientovaný směrovací protokol, jehož specifikaci lze nalézt v [5], jak bylo uvedeno v předchozím odstavci.

Jako metriku používá počet skoků k cíli (Hop Count) a nejkratší cestu určuje pomocí Ford-Fulkerson (nebo také Bellman-Ford) algoritmu [2].

Tento protokol je určen pro jeden autonomní systém (AS)¹ a pro sítě střední velikosti. Do rozsáhlých a komplexních sítí není, díky svým limitacím a principům, příliš vhodný.

V samotném protokolu RIPng není specifikována autentizace, u které se předpokládá, že bude zajištěna jiným způsobem, např. pomocí IPsec².

¹Autonomní systém - množina IP sítí a směrovačů pod jednou technickou správou

²IPsec - Internet Protocol Security, <http://en.wikipedia.org/wiki/IPsec>.

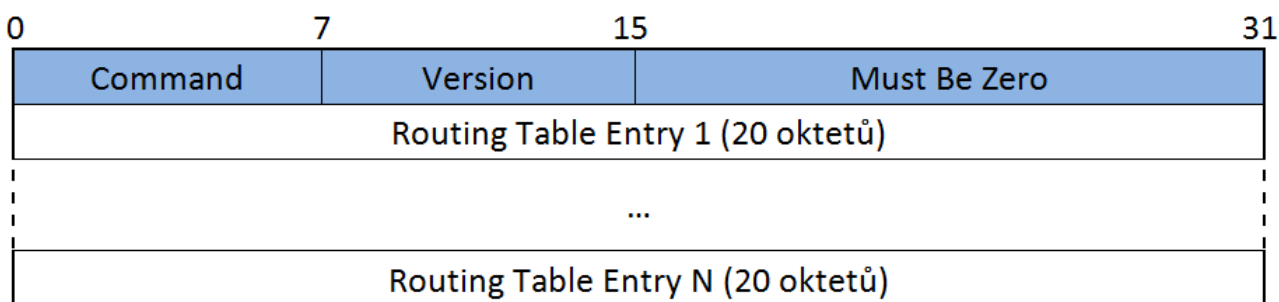
2.3 Komunikace

RIPng komunikuje pomocí transportního protokolu UDP¹ na portu 521 (dále také jako RIPng port). Aktualizace jsou zasílány na multicastovou skupinu FF02::9 (dále také jako multicastová adresa RIPng). Existují 2 základní typy zpráv:

- **Request** (požadavek) - kap. 2.5 a
- **Response** (odpověď) - kap. 2.4.

2.3.1 Formát zprávy protokolu RIPng

Zprávy zasílané protokolem RIPng mají strukturu, která je zobrazena na obrázku 2.1.



Obrázek 2.1: Formát zprávy protokolu RIPng

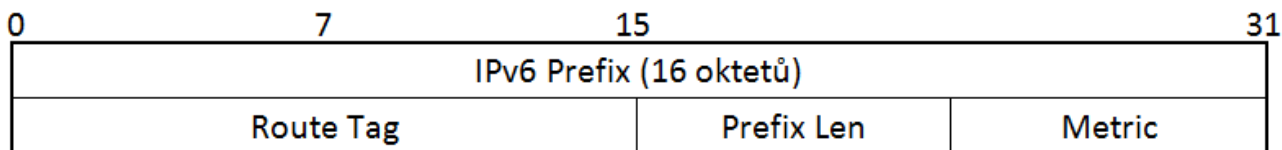
Pole **Command** obsahuje:

- **1**, pokud se jedná o zprávu typu **Response** nebo
- **2**, pokud jde o zprávu typu **Request**.

Pole **Version** obsahuje verzi protokolu (v současné době vždy **1**).

Poslední pole v hlavičce – **Must Be Zero** – musí být při odesílání zprávy nastaveno na **0** a ignorováno při přijmutí.

Záznamy o dostupných sítích jsou přenášeny v polích **Routing Table Entry** (dále také RTE). Formát pole RTE je na obrázku 2.2.



Obrázek 2.2: Formát pole RTE

Pole **IPv6 Prefix** obsahuje adresu sítě (prefix). **Route Tag** by měl obsahovat označení sítě - např. zda se jedná o síť distribuovanou z jiného protokolu. **Prefix Len** určuje délku prefixu. Pole **Metric** udává vzdálenost sítě (viz kap. 2.2), při ukládání RTE se tato vzdálenost většinou zvětší o jedna.

Maximální počet polí v jedné zprávě RIPng je omezen velikostí MTU² média, po kterém se přenáší RIPng zpráva, viz [5].

¹UDP - User Datagram Protocol [8]

²MTU - Maximum Transmission Unit, maximální velikost jednotky dat, která může být po médiu přenesena.

2.3.2 Speciální typ RTE

Protokol RIPng umožňuje určit další skok (*Next Hop*) pro RTE (jinak je určen ze zdrojové adresy zprávy). *Next Hop* se specifikuje jako RTE záznam, kde pole **IPv6 Prefix** určuje *Next Hop* adresu, pole **Route Tag** a **Prefix Len** je nastaveno na 0 a pole **Metric** má hodnotu 0xFF. Všechny RTE pod takovým záznamem mají potom *Next Hop* určen z tohoto záznamu. Jako *Next Hop* adresa musí být adresa typu link-local, jinak je ignorována a *Next Hop* se opět určí ze zdrojové adresy zprávy (totéž v případě, kdy *Next Hop* = 0:0:0:0:0:0:0:0).

2.4 Zprávy typu Response

Zprávy typu **Response** obsahují dostupné sítě (připojené přímo nebo naučené pomocí protokolu RIPng) a jsou vytvořeny a odeslány pokud:

- je nutné vygenerovat pravidelnou aktualizaci (tzv. *Regular Update Message*) - generuje se každých 30 sekund viz kap. 2.6,
- se změnila metrika cesty (tzv. *Triggered Update Message*),
- je přijata zpráva typu **Request**,

2.4.1 Vytvoření zprávy typu Response

Response zpráva se vytváří pro každou připojenou síť (každé rozhraní), pokud se jedná o *Regular Update Message* nebo *Triggered Update Message*. Rozdíl mezi těmito zprávami je v jejich obsahu. *Regular Update Message* musí obsahovat všechny dostupné sítě, zatímco *Triggered Update Message* může obsahovat pouze RTE ze směrovací tabulky u nichž se změnila metrika (např. síť se stala nedostupnou, tyto RTE mají nastaven *Route Change Flag*, viz kap. 2.7). Pro tyto typy zpráv je použita jako zdrojová adresa adresa příslušného rozhraní typu link-local (pokud má rozhraní více link-local adres, potom musí vybranou adresu používat po celou dobu, po které je dostupná), jako cílová adresa je nastavena multicastová skupina RIPng protokolu (FF02::9) a cílový port je RIPng port 521. Na každý RTE v těchto zprávách je aplikován *Split Horizon* – síť se neodešle na rozhraní, skrze které byla naučena, viz [5] – pro zamezení vytváření směrovacích smyček.

Pokud se vytváří **Response** zpráva, protože na ni byl přijat požadavek, odesílá se tato zpráva se zdrojem a cílem dle tabulky 2.1. Jestliže navíc požadavek obsahoval žádost na konkrétní RTE záznam (více o požadavcích v kapitole 2.5), v případě nalezení tohoto RTE záznamu, ve směrovací tabulce, se na něj neaplikuje *Split Horizon*.

Request Message		Response Message			
Zd. adr.	Zd. port	Zd. adr.	Zd. port	Cíl. adr.	Cíl. port
FF02::9	521	link-local	521	link-local	521
unicast	libovolný	global-unicast	521	Request zd. adr.	Request zd. port

Tabulka 2.1: Zdroj a cíl odpovědi na základě zdroje požadavku

V **Response** zprávě se nesmí objevit RTE s link-local adresou.

Po odeslání *Regular Update Message* nebo *Triggered Update Message* jsou všechny *Route Change Flag* resetovány.

2.4.2 Zpracování zprávy typu Response

Při přijmutí odpovědi se kontroluje zda:

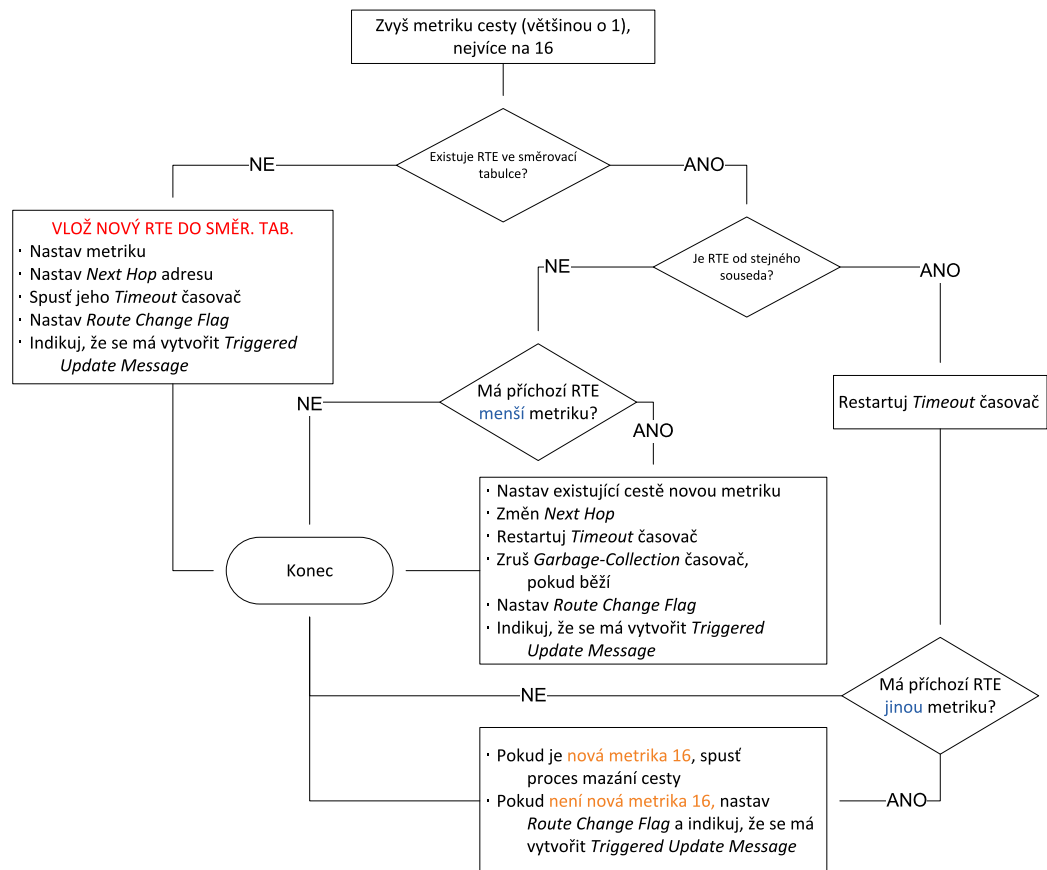
- je z RIPng portu,
- je zdrojová adresa typu link-local,

- není zdrojová adresa vlastní,
- je u zpráv *Regular Update Message* nebo *Triggered Update Message* nastaven hop-count na 255 - zpráva přišla od souseda.

Pokud některá podmínka nevyhoví kontrole, je odpověď zahozena.

Po kontrole hlavičky zprávy se prochází všechny RTE. Každý záznam se zkontroluje zda obsahuje validní IPv6 prefix (nesmí být multicast, či link-local adresa), délku prefixu (0-128) a metriku (0-16).

Každý RTE se zpracuje způsobem, který je znázorněn na obrázku 2.3.



Obrázek 2.3: Zpracování RTE ze zprávy typu Response

2.5 Zprávy typu Request

Zprávy typu Request obsahují požadavek na dostupné sítě a jsou většinou posílány, pokud:

- se spustil RIPng proces, který potřebuje zjistit všechny dostupné sítě,
- je potřeba diagnostikovat síť.

V prvním případě se požadavky odesílají jako multicast zpráva z RIPng portu. V případě druhém by měl být požadavek určen přímo – unicastovou adresou směrovače – a měl by být odeslán z jiného portu než je RIPng port.

2.5.1 Zpracování zprávy typu Request

Zpráva typu Request, stejně jako zpráva typu Response, obsahuje RTE.

RTE v tomto případě znamená požadavek, zda je síť určená tímto RTE dostupná pro daný směrovač. Pro každou takovou síť se k RTE nastaví příslušná metrika. Pokud požadovaná síť není dostupná je metrika nastavena na 16. Typ zprávy se změní na **Response** a zpráva je odeslána zpět.

Pokud požadavek obsahuje pouze jediný záznam RTE, který má všechna pole, mimo pole metriky, nastavena na **0** a metriku nastavenou na **16**, znamená to požadavek na zaslání všech dostupných sítí (v odpovědi se aplikuje *Split Horizon*).

2.6 Časovače

RIPng používá následující časovače:

- Každých 30 sekund se generuje *Regular Update Message*, viz kap. 2.4.
- Každý RTE má vlastní *Timeout* časovač o délce 180 sekund. Po vypršení tohoto časovače se spustí proces mazání cesty - viz kap. 2.7.
- Každý RTE má navíc *Garbage-Collection Time* časovač, který se spouští při procesu mazání cesty. Tento časovač má délku 120 sekund a po jeho vypršení se RTE odstraní ze směrovací tabulky.
- *Triggered Update* časovač, jehož délka je určena náhodně od 1 do 5 sekund. Tento časovač se spouští před odesláním *Triggered Update Message* a pokud se má odeslat další *Triggered Update Message*, odešle se až po uplynutí tohoto časovače.

2.7 Proces smazání cesty

Tento proces je spuštěn pro RTE ve směrovací tabulce, pokud:

- mu vypršel *Timeout* časovač nebo
- se mu nastavila metrika o délce 16.

Proces smazání cesty zahrnuje následující akce:

- spuštění *Garbage-Collection Time* časovače pro daný RTE,
- nastavení metriky na 16,
- nastavení *Route Change Flag*,
- indikace, že se má vytvořit *Triggered Update Message* zpráva, viz kap. 2.4.

Kapitola 3

Závěr

V rámci této práce byla provedena analýza prostředí OMNeT++ a frameworku INET, které dohromady poskytují funkce pro simulování síťové komunikace. Byly určeny možnosti frameworku INET a případně provedeny jeho úpravy pro implementaci protokolu RIPng a vytvoření testovací sítě.

Dále byla provedena analýza protokolu RIPng, jehož specifikace byla popsána, a implementována základní struktura RIPng do frameworku INET.

Tato práce vznikla za podpory projektu MŠMT CZ.1.07/2.3.00/09.0067 TeamIT – Budování konkurenceschopných výzkumných týmů pro IT v rámci projektu ANSA výzkumné skupiny Nes@FIT.

Literatura

- [1] Automated Network Simulation and Analysis. ANSA, 2012, [Online; navštíveno 30.8.2012].
URL <http://nes.fit.vutbr.cz/ansa/pmwiki.php>
- [2] Ford, L. R. J.; Fulkerson, D. R.: *Flows in Networks*. Princeton University Press, 1962, ISBN 9780691146676.
- [3] Hedrick, C.: Routing Information Protocol. RFC 1058, Internet Engineering Task Force (IETF), 1988.
- [4] Welcome to the INET Framework! INET FRAMEWORK, 2012, [Online; navštíveno 30.8.2012].
URL <http://inet.omnetpp.org/>
- [5] Malkin, G.: RIPng for IPv6. RFC 2080, Internet Engineering Task Force (IETF), 1997.
- [6] Malkin, G.: RIP Version 2. RFC 2453, Internet Engineering Task Force (IETF), 1998.
- [7] OMNeT++. OMNeT++, 2009, [Online; navštíveno 30.8.2012].
URL <http://www.omnetpp.org/>
- [8] Postel, J.: User Datagram Protocol. RFC 768, Internet Engineering Task Force (IETF), 1980.