VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

MODELOVÁNÍ PROTOKOLŮ PRO REDUNDANCI BRÁNY

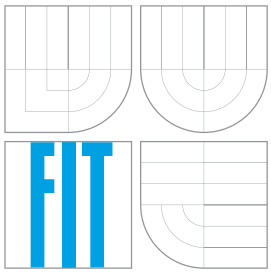
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. PETR VÍTEK

BRNO 2013

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

MODELOVÁNÍ PROTOKOLŮ PRO REDUNDANCI BRÁNY

MODELLING GATEWAY REDUNDANCY PROTOCOLS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. PETR VÍTEK

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. VLADIMÍR VESELÝ

BRNO 2013

Abstrakt

Tato diplomová práce se zabývá teoretickým rozborem FHRP protokolů. First Hop Redundancy Protocols jsou síťové protokoly, které jsou určeny pro ochranu výchozí brány a také pro zajištění vysoké dostupnosti v síti pomocí redundance směrovačů (bran). Čtenář se nejen seznámí s protokoly VRRP, HSRP a GLBP, ale také se dozví způsoby jejich konfigurace na reálných zařízeních společnosti Cisco. Dále popisuje implementaci protokolu VRRP v simulačním prostředí OMNeT++. Výsledek implementace je ověřen na sadě testovacích topologiích.

Abstract

This master's thesis report deals with the theoretical analysis of FHRP. First Hop Redundancy Protocols are network protocols which are designed to protect the default gateway and also to ensure high availability in the network by using redundancy. The reader becomes familiar with protocols VRRP, HSRP and GLBP and also learn the way how to configure them to on real Cisco devices. It also describes how implement VRRP int the simulated enviroment of OMNeT++. The result of the implementation is verified in the test topologies.

Klíčová slova

FHRP, First Hop Redundancy Protocol, VRRP, Virutal Router Redundancy Protocol, HSRP, Hot Standby Router Protocol, GLBP, Gateway Load Balancing Protocol, Cisco, OMNeT++, INET, simulace

Keywords

FHRP, First Hop Redundancy Protocol, VRRP, Virutal Router Redundancy Protocol, HSRP, Hot Standby Router Protocol, GLBP, Gateway Load Balancing Protocol, Cisco, OMNeT++, INET, simulation

Citace

Petr Vítek: Modelování protokolů pro redundanci brány, diplomová práce, Brno, FIT VUT v Brně, 2013

Modelování protokolů pro redundanci brány

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Vladimíra Veselého

.....
Petr Vítek
22. května 2013

Poděkování

Tyto řádky patří hlavně mému vedoucímu Ing. Vladimíru Veselému, který mi pomohl s realizací mé diplomové práce. Jako poděkování použiji jednoduchou rovnici: Dobré jídlo = dobrá nálada = dobré zdraví. Jedním z těchto zdravých jídel je i má oblíbená rybka - pečený pstruh. V následujících řádcích bych Vám rád popsal jeho přípravu. Pro jeho realizaci potřebujeme 1 rybu (ideálně tedy toho pstruha), 40g másla, sůl, pepř, cca 8 snítek tymiánu a citron. Plech vymažeme máslem, aby se ryba při pečení nepřichytila. Vykuchaného a očištěného pstruha důkladně osušíme, osolíme a opepříme z obou stran. Vložíme do něj 2 snítky tymiánu. Takto připraveného pstruha položíme na vymazaný plech a dáme do péct do trouby rozehřáté přibližně na 160 stupňů zhruba na 10minut. Poté můžeme servírovat na talíř, nesmíme zapomenout přidat citrón k ochucení. Přílohu přenechám kreativitě kuchaře.

Obsah

Kapitola 1

Úvod

1.1 Počítačové sítě

V dnešní době každá organizace disponuje počítačovými systémy, které usnadňují její chod. Ve většině případů je nemožné si jejich fungování bez těchto zařízení představit. Tyto systémy jsou propojeny počítačovou sítí, jenž umožňuje uživatelům využívat její služby v kanceláři, na cestách nebo z pohodlí domova. Historie počátku sítí sahá až do 60. let 20. století, kdy začaly první pokusy s komunikací počítačů. První počítačové sítě sloužily pro sdílení strojového času a propojovaly velké sálové počítače s jednotlivými terminály, které sloužily pro vstup a výstup dat. Nevýhodou mainframe počítačů byl princip jedné chyby. Pokud počítač "spadnul" stal se nepřístupným nikomu. Nikdo se nemohl k datům dostat a nikdo také nemohl dokončit rozdělanou práci. Použití osobních počítačů tento problém obešlo.

Spolu s revolucí osobních počítačů nastoupily lokální sítě LAN (Local Area Network), ve kterých si uživatelé mohli vyměňovat soubory, zprávy a také přistupovat ke společným síťovým prostředkům jako jsou například databázové servery nebo síťové tiskárny.

Uživatelé se na počítačových sítích stali svým způsobem závislí a očekávají od ní nejvyšší možnou spolehlivost. Už při návrhu sítě by pro každého síťového inženýra měla být eliminace jednotlivých poruchových míst prioritou. Mezi tato problematická místa patří také výchozí brána, která pro určitou stanici nebo skupinu stanic zprostředkovává spojení s vnějším světem. Kvůli těmto problémům byly navrženy protokoly pro redundanci brány FHRP (First Hop Redundancy Protocols), jenž slouží k zajištění vysoké dostupnosti pomocí redundance.

1.2 Struktura práce

Práce se zaměřuje na bližší popis současných protokolů FHRP, jenž pomocí speciálních mechanismů zajišťují spolehlivost při jejím selhání. Struktura práce je následující:

V kapitole 2 je teoretický rozbor redundantních protokolů, popisuje základní mechanismy a principy redundance bran. Konkrétně se zaměřuje na protokoly VRRP, HSRP a GLBP. V závěru kapitoly se nachází také stručný přehled vlastností těchto protokolů.

Kapitola 3 se zaměřuje na konfiguraci FHRP protokolů ve směrovačích Cisco. Čtenáři se představí všechny základní příkazy s vysvětlením jejich možností a parametrů. Pro každý příkaz je uvedena jeho syntaktická podoba doplněná o ilustrační příkad jeho nastavení.

V kapitole 4 se nachází popis simulačního prostředí OMNeT++ a také rozšiřující knihovny INET, která přináší funkcionalitu IP sítí.

Následuje 5 kapitola, zde se nachází popis návrh modulu VRRP a jsou vysvětleny všechna úskalí implementace do prostředí OMNeT++.

Kapitola 6 zobrazuje proces simulace implementovaného modulu. Jsou představeny testovací topologie, následovány analýzou událostí v čase a porovnání s reálnými zařízeními v laboratoři.

Poslední 7 kapitola shrnuje dosažené výsledky obsahu práce a zaměřuje se i na budoucí vývoj.

Kapitola 2

Protokoly pro redundanci brány

Maximální dostupnost síťové infrastruktury je v dnešní době informačních technologií běžným požadavkem. Jedna z priorit pro zajištění spolehlivosti počítačové sítě je eliminace výpadku výchozí brány. V malých a středních sítích je ve většině případů pouze jediná výchozí brána a její výpadek znemožní schopnost komunikace s okolními sítěmi. Odstranění těchto problémů spočívá v nasazení protokolu typu FHRP, tedy protokolu pro redundanci brány. FHRP umožňuje v případě selhání převzetí funkcí jednoho zařízení jiným zařízením v dané síti.

Spojení mezi zařízeními, které se nacházejí v různých sítích, probíhá přes výchozí bránu. Tato brána je kritickým bodem spojujícím obě komunikující strany. Při jejím výpadku je ztracena veškerá výměna informací s jakýmkoliv zařízením umístěným mimo lokální síť. Pro zajištění vysoké spolehlivosti je nutné nasadit více výchozích bran, které budou schopny při výpadku jedné z nich se vzájemně zastoupit. Zotavení z výpadku musí být dostatečně rychlé, aby navázaná spojení se síťovými protokoly nebyla ztracena a negativní důsledky takového výpadku byly co možná nejvíce minimalizovány.

V případě technologie Ethernet jsou nejčastěji používaným řešením protokoly VRRP (Virtual Router Redundancy Protocol), HSRP (Hot Standby Router Protocol) nebo GLBP (Gateway Load Balancing Protocol). Protokoly HSRP a GLBP jsou proprietární protokoly společnosti Cisco. Zatímco VRRP proprietárním protokolem není, a proto je dostupný i u zařízení jiných výrobců.

Dříve než byly první First Hop Redundancy Protocols k dispozici, počítačové sítě spoléhaly na techniku Proxy ARP a také statickou konfiguraci výchozí brány.

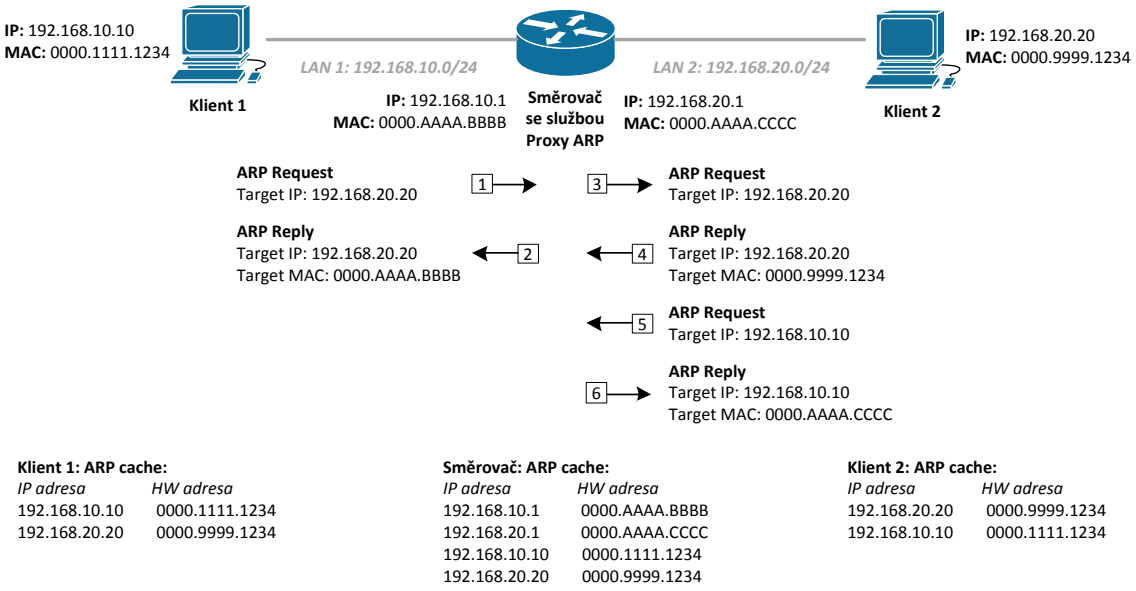
2.1 Statická konfigurace výchozí brány

V konfiguraci síťového rozhraní koncové stanice je výchozí brána nastavena staticky. Za předpokladu použití několika výchozích bran v rámci jednoho segmentu sítě neexistuje bez využití dalších specializovaných služeb žádná možnost automatického zotavení z výpadku výchozí brány. Koncová statnice neví o dalších alternativních branách, které by mohla použít, a proto ztrácí možnost komunikovat se stanicemi v jiných segmentech počítačové sítě.

2.2 Proxy ARP

Proxy ARP (popsaný v RFC 1027 [10]) je technika umožňující propojit několik lokálních sítí, jejichž zařízení mezi sebou komunikují pomocí protokolu ARP (Address Resolution Protocol). ARP se nedostane za hranici lokální sítě, služba Proxy ARP, spuštěna na hraničním směrovači, toto omezení odstraňuje a zařízení je schopno plnit funkci výchozí brány.

Komunikace se stanicí vně lokální síť probíhá následovně (obrázek 2.1). Koncové zařízení odešle `ARP Request` obsahující IP adresu stanice, se kterou chce komunikovat. Dotaz je rozeslán všem zařízením v lokální síti, zde se ovšem hledaná stanice nenachází. Hraniční směrovač zjistí, že se hledaná stanice nachází mimo lokální síť, proto odpoví tazateli svoji vlastní MAC adresou. Zdrojová stanice, která poslala `ARP Request`, si MAC adresu uvedenou v odpovědi uloží do své lokální paměti pro další použití při komunikaci. Koncová stanice nezjistí, že komunikace neprobíhá přímo s cílovou stanicí, ale jde přes směrovač se službou Proxy ARP, která přeposílá pakety k jejich skutečnému cíli.



Obrázek 2.1: Princip činnosti Proxy ARP

Výhodou této metody je, že stanice mezi sebou mohou komunikovat i bez znalosti výchozí brány. V situaci, kdy je v síti více stanic se službou Proxy ARP, může roli výchozí brány převzít jiná stanice při jejím výpadku. Tato činnost je pro koncové stanice téměř transparentní. Jediné co stanice zaregistruje je změna mapování MAC adresy na IP, které je automaticky provedeno prostřednictvím protokolu ARP.

Nevýhodou je doba potřebná k tomu, aby vypršela platnost původní používané MAC adresy. Po vypršení této doby je vyslán nový `ARP Request` pro mapování IP adresy na MAC. Na tento dotaz již může odpovědět jiná brána a komunikace je obnovena. Tato doba však může být poměrně dlouhá, takže může dojít ke ztrátě navázaných relací.

2.3 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol je otevřený standard popsaný v RFC 5798 [11] pro VRRPv3 a v RFC 3768 [9] pro VRRPv2, podporuje redundanci směrovačů na základě volebního procesu mezi zařízeními pracujícími jako členy jedné logické skupiny nazývané Virtual Router.

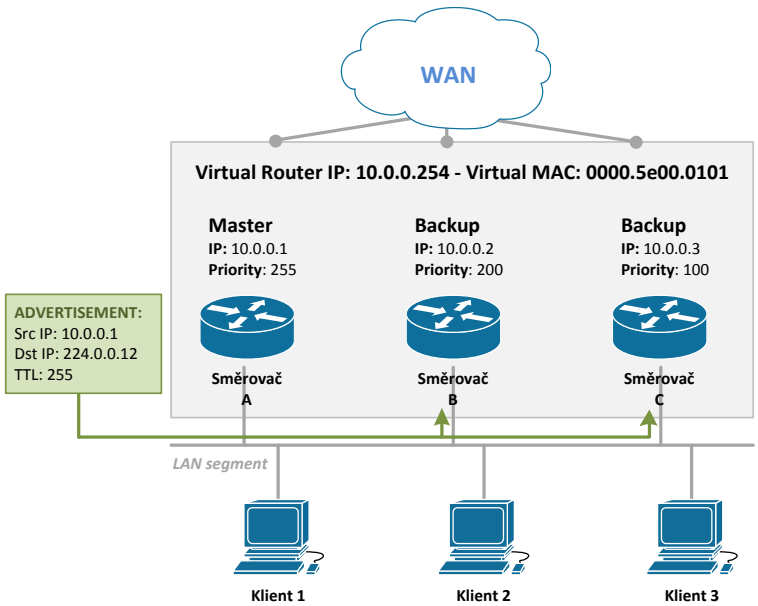
Virtual Router obsahuje dva nebo více směrovačů s nastavenou virtuální IP adresou, kterou může obsahovat jeden z členů skupiny jako primární IP adresu na svém síťovém rozhraní. Virtuální IP adresu je také možné nakonfigurovat tak, aby nebyla shodná s žádnou jinou adresou v síti. Taková adresa se nazývá plovoucí nebo čistě virtuální IP adresa. Výhodou tohoto nastavení je poskytnutá flexibilita, která umožňuje správci sítě změnit adresy reálných zařízení bez nutnosti překonfigurovat samotný virtuální směrovač.

Směrování paketů ve Virtual Router zajišťuje Master, kterým se stává směrovač s nejvyšší prioritou. Jestliže je virtuální IP adresa rovna primání IP adrese rozhraní, tak se směrovač automaticky stává Master a je mu nastavena priorita 255.

Master v pravidelných intervalech rozesílá ohlášení `ADVERTISEMENT`, čímž záložním směrovačům deklaruje svoji funkčnost. Backup může převzít roli Master nejen v případě jeho selhání, ale také pokud má vyšší hodnotu priority a preemce není zakázána.

Všechny zprávy jsou odesílány na multicastovou adresu, jejíž hodnota pro IPv4 je `224.0.0.12` a `FFE02::12` pro IPv6. Zdrojová adresa paketu je vždy primární IP adresa rozhraní, ze kterého je ohlášení odesláno. V sítích IPv6 je zdrojová adresa unicastová adresa rozhraní link-local. Na L2 vrstvě je paketu přiřazena virtuální MAC adresa, u které podrobnosti vysvětluji v kapitole 2.3.4 Virtual Router MAC Address.

Tyto pakety jsou zasílány vždy s `TTL = 255` a nejsou předávány pomocí směrovače. Pokud z nějakého důvodu směrovač přijme paket s nižší hodnotou `TTL` je daný paket zahozen.



Obrázek 2.2: Ukázka zapojení VRRP

Protokol VRRP přidává do počítačové sítě následující benefity [1]:

- **Redundance**
  Umožňuje konfigurovat více směrovačů jako výchozí bránu, čímž snižuje možnost selhání sítě v jediném bodě.

- **Load Sharing**
  Konfigurace VRRP takovým způsobem, aby provoz od klientů dělila mezi více směrovači a tím rovnoměrně rozložil zátěž.

- **Vícenásobný virtual router**
  VRRP podporuje až 255 virtuálních směrovačů (skupin VRRP) na fyzickém rozhraní. Podpora vícenásobných IP adres umožňuje implementovat redundanci a sdílení zátěže v topologii sítě LAN.

- **Vícenásobné IP adresy**
  Virtuální směrovač může spravovat více IP adres včetně sekundárních. Je-li na ethernetovém rozhraní nastaveno více podsítí, může být VRRP nakonfigurováno pro každý segment.

- **Preemce**
  Umožňuje převzít záložnímu směrovači s nejvyšší prioritou všechny funkce Master směrovače.

- **Advertisement protokol**
  VRRP používá speciální multicastovou adresu (`224.0.0.18`) přiřazenou organizací IANA (Internet Assigned Numbers Authority) pro zasílání zpráv. Toto řešení minimalizuje počet směrovačů, jenž musí v segmentu identifikovat VRRP pakety.

- **Sledování objektů**
  Poskytuje způsob, jak zjistit volbu nejvhodnějšího Master ovlivňováním priority záložních směrovačů na základě sledování objektů jako je stav rozhraní nebo IP směrování.

Do VRRPv3 bylo přidáno:

- **Podpora IPv6**
  VRRPv3 podporuje IPv4 i IPv6 adresy, zatímco VRRPv2 umožňuje využít pouze IPv4 adresy. Spolupráce VRRPv2 a VRRPv3 je možná, ale je doporučována pouze v případě přechodu od jedné verze ke druhé.

2.3.1 Základní pojmy

V této části vysvětluji základní pojmy VRRP, jejichž osvětlení je nutné pro pochopení dalších informací v této kapitole.

- **VRRP Router**
  Směrovač se spuštěným Virtual Router Redundancy Protocol.

- **Virtual Router**
  Abstraktní objekt řízený VRRP působí jako výchozí směrovač pro počítače v síti. Skládá se z Virtual Router ID a jedné nebo více přidružených IPv4 / IPv6 adres.

- **Virtual Router Master**
  Směrovač, jehož IP adresa na rozhraní odpovídá virtuální IP adrese nebo také směrovač s nejvyšší hodnotou priority. Stará se o směrování paketů.

- **Virtual Router Backup**
  Množina VRRP směrovačů, kteří naslouchají, zda je Master v provozu a plní své funkce. Pokud po určitý časový interval od směrovače neobdrží žádné ohlášení, jeden z nich přebírá všechny jeho povinnosti.

- **Virtual Router ID - VRID**
  Číselná identifikace konkrétního virtuálního směrovače. VRID musí být jedinečný v daném segmentu sítě.

2.3.2 Proces převzetí

Dynamické převzetí služeb při selhání v případě, kdy Master není k dispozici, používá tři časovače:

- **Advertisement interval** je časový interval mezi ohlášeními. Výchozí hodnota je 1 sekunda.

- **Master down interval** je čas zálohy o nedostupnosti směrovače Master. Výchozí hodnota se počítá jako $(3 \cdot \textit{Advertisement interval}) + \textit{skew interval}$

- **Skew time** $\frac{256-\textit{priorita}}{256}$ ms zaručuje volbu nového Master, stane se jím Backup s největší prioritou.

Všechny VRRP směrovače patřící do jednoho Virtual Router musí mít stejnou hodnotu Advertisement interval. Pokud se liší, směrovač přijatá oznámení zahodí.

Tabulka 2.1 uvádí kroky převzetí služeb Master z obrázku .

Krok	Popis
1	Směrovač A v roli Master posílá ohlášení každou sekundu.
2	Selhání směrovače A, zapříčiní konec ohlášení.
3	Směrovače B i C nedostávají ohlášení, čekají na vypršení Master down intervalu před přechodem do stavu Master. Ve výchozím nastavení je Master down interval 3 sekundy + skew time.
4	Protože skew time je nepřímo uměrný prioritě Master down intervalu směrovače B je menší než u směrovače C. Směrovač B má hodnotu skew time 3,2s, směrovač C 3,6s.
5	Směrovač B přejde do stavu Master po uplynutí 3,2s ve kterém začne posílat ohlášení.
6	Směrovač C přijímá ohlášení od nového Master, resetuje Master down interval a zůstává ve stavu Backup.

Tabulka 2.1: Převzetí služeb Master

V případě dobrovolného ukončení práce směrovače Master na účasti ve virtuálním routeru odesílá ohlášení se speciální hodnotou priority (`Priority = 0`). Obdrží-li Backup směrovače takové ohlášení, nečekají na vypršení časovačů, ale ihned se pustí do volby nového Master.

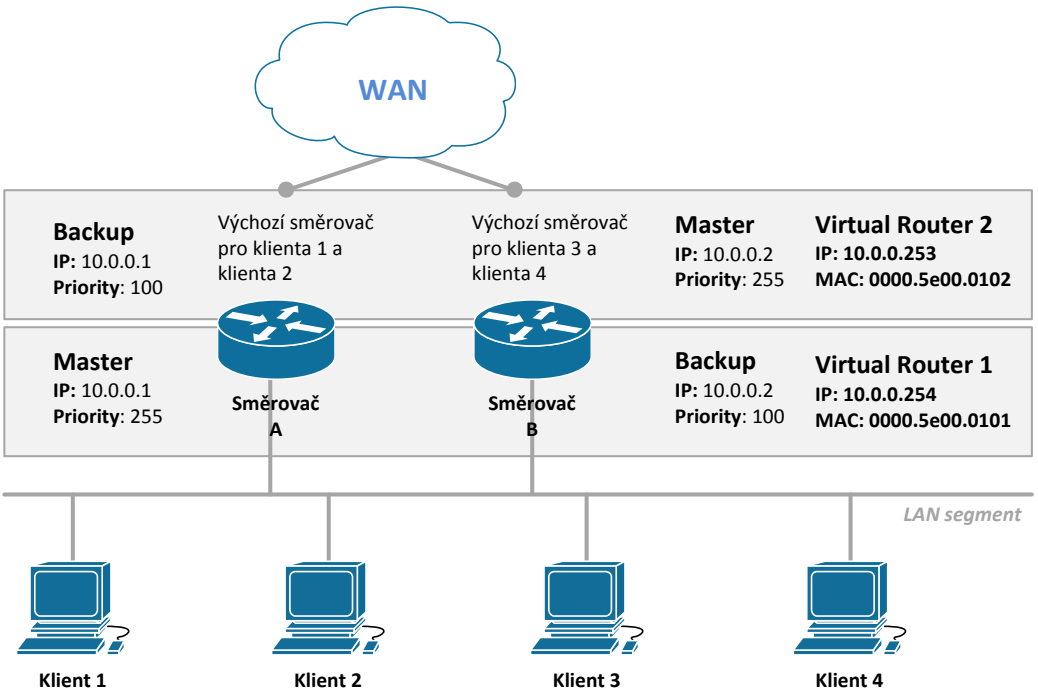
2.3.3 Load Sharing

Na obrázku 2.2 jsou směrovače B i C zcela nečinné v době, kdy se nachází v Backup stavu. Obě zařízení jsou čistě redundantní. Za určitých okolností nemusí být toto uspořádání nejlepší. Ponecháním nevyužitého síťového zařízení ztrácíme cenné zdroje. Za těchto okolností můžeme nastavit směrovač B jako výchozí bránu pro některé hostitele - klient 3 a 4. V této konfiguraci je provoz klientů předán směrovači A a provoz klientů 3 a 4 předán směrovači B.

Výhodou tohoto uspořádání je vytvoření schéma load sharing. V této konfiguraci se provoz pocházející ze sítě neposílá výlučně do jednoho směrovače, ale je sdílen mezi A i B.

Chceme-li vytvořit toto nastavení, musíme definovat dva virtuální směrovače. Obrázek 2.3 ilustruje toto nastavení. Směrovač A je Master pro Virtual Router 1 a backup pro Virtual Router 2. Pro Virtual Router 2 je směrovač B Master a směrovač A Backup. V případě selhání jednoho routeru je možné zpozorovat určitou degradaci síťových služeb.

Mezi další výhody paralelního použití obou směrovačů je jednodušší detekce selhání zařízení. Je mnohem snažší odhalit selhání aktivního zařízení než zařízení, které je v pasivním režimu monitorování.



Obrázek 2.3: Ukázka zapojení Load Sharing

2.3.4 Virtual Router MAC adresa

MAC adresa směrovače s implementovaným VRRP je přiřažena ve formátu `IEEE 802 MAC` a má následující tvar:

```
IPv4: 00-00-5E-00-01-{VRID}
```

`IPv6: 00-00-5E-00-02-{VRID}`

První tři oktety jsou přiřazeny organizací IANA. Další dva uvádějí adresu bloku přiřazenou VRRP pro IPv4 / IPv6 protokol. Poslední oktet {`VRID`} je identifikátor virtuálního směrovače, umožňuje využití až 255 virtuálních směrovačů v síti.

V případě ARP požadavku klienta na IP adresu Virtual Router směrovač Master musí odpovědět virtuální MAC adresou. Směrovač, který je ve stavu Backup, tedy záložní směrovač, na tento požadavek nereaguje.

2.3.5 Bezpečnost

Aktuální verze protokolu VRRPv3 neobsahuje žádnou interní autentizaci. V dřívější verzi specifikace VRRPv2 byly zahrnuty tři hlavní metody autentizace: bez ověřování, jednoduché prosté textové heslo a silná autentizace IP ověřování pomocí Message Digest 5 (MD5) HMAC.

Z provozních zkušeností a další analýzy se zjistilo, že neposkytují dostatečné zabezpečení pro překonání zranitelnosti a při chybně nakonfigurovaném tajemství dochází k mnohonásobnému zvolení Master. Mají-li směrovače v jedné skupině odlišná hesla, Backup přijaté ohlášení zahazuje a po vypršení Master Down intervalu přechází do stavu Master.

Vzhledem k povaze protokolu VRRP, i když byla ohlášení kryptograficky chráněna, nezabrání útočníkovi vystupovat jako Master. Zapříčiní to stejný problém jako u chybně nastaveného hesla - několikanásobný Master. Autentizace zpráv měla zabránit neprátelskému uzlu, aby poslal všechny řádně pracující směrovače do Backup stavu. Avšak několikanásobný Master způsobuje stejné narušení bezpečnosti, jako když nejsou směrovače kryptograficky chráněny. I v případě, že útočník nemůže napadnout VRPP, může narušit ARP.

Nicméně obsahuje mechanismus (kontrola `TTL = 255` při přijetí), který chrání před vložením zpráv `ADVERTISMENT` ze vzdálené sítě. Toto omezí většinu zranitelností na místní útoky.

VRRP neposkytuje důvěrnost zpráv, která není nutná pro jeho správnou funkci. Neexistují žádné informace, které by měly být ve zprávách utajeny před ostatními uzly v síti LAN.

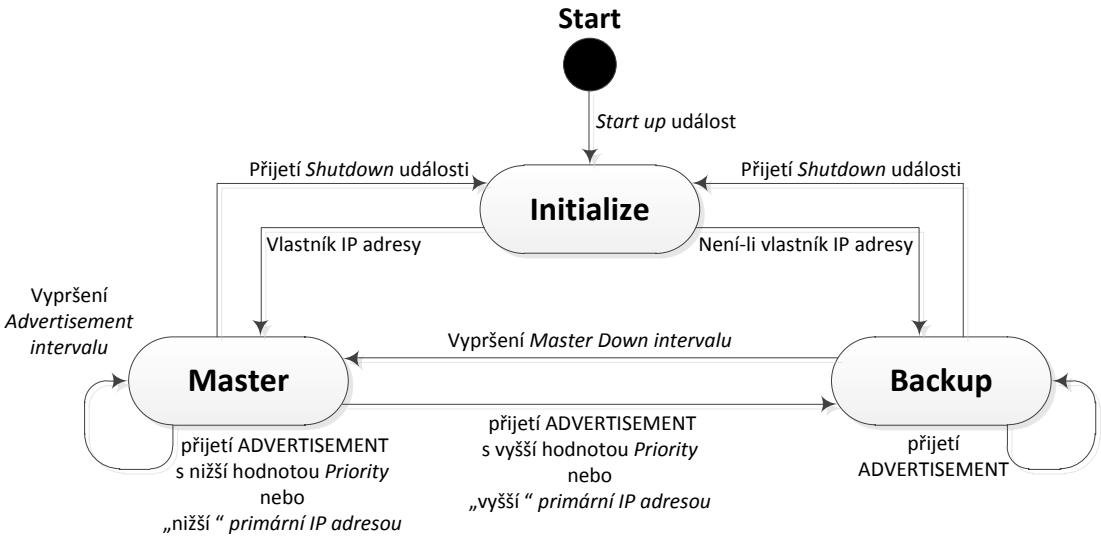
2.3.6 Stavový automat

Jak je vidět z obrázku 2.4, směrovač se může nacházet v jednom ze tří stavů:

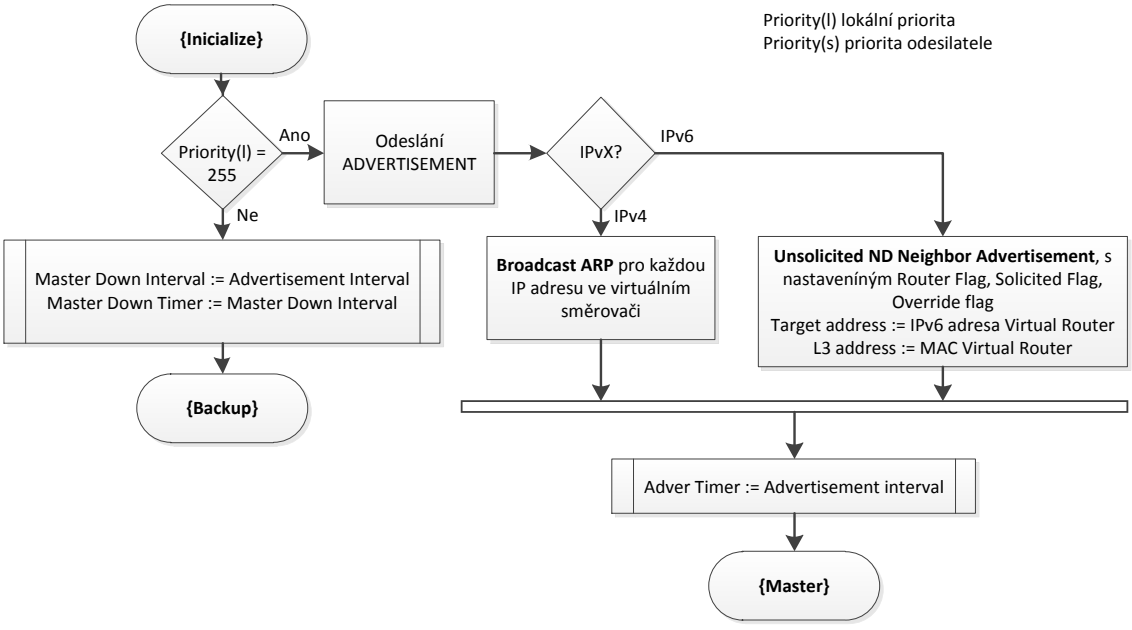
- Initialize
- Master
- Backup

Stav Initialize

Účelem tohoto stavu (obrázek 2.5) je čekat na spouštěcí akci. Po přijetí této události je zkontrolována hodnota priority. Ta pokud je rovna 255, odešle oznámení a přejde do stavu Master, v opačném případě do stavu Backup.



Obrázek 2.4: Stavový automat VRRP



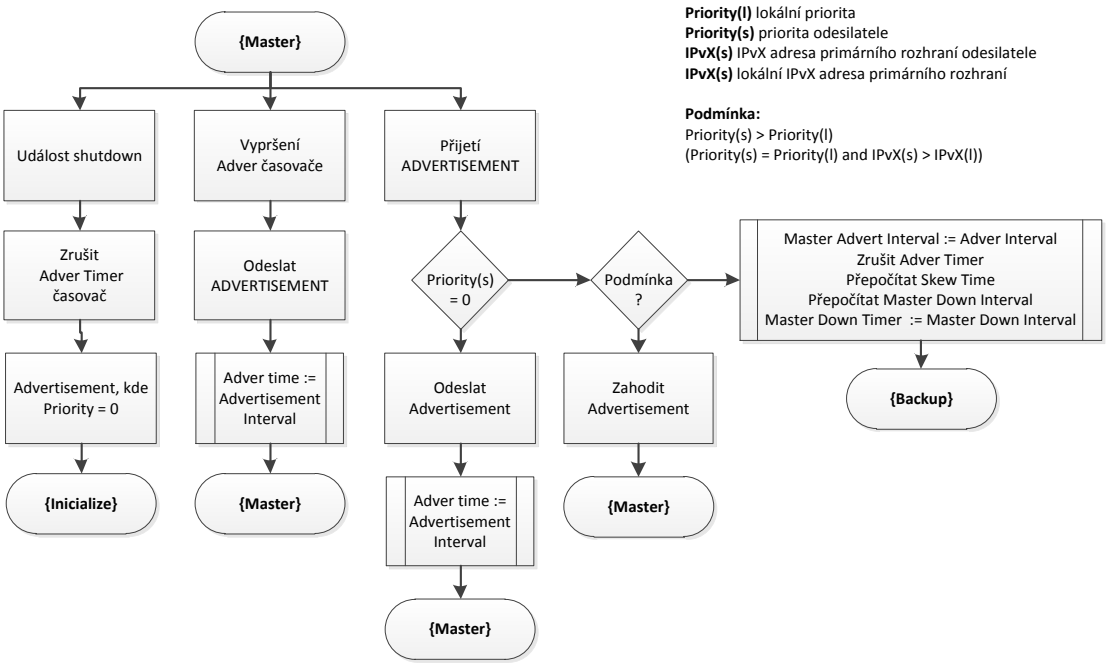
Obrázek 2.5: Průběh činnosti ve stavu Initialize

Stav Master

Zatímco se směrovač nachází ve stavu Master (obrázek 2.6), pracuje jako výchozí brána pro koncové stanice v rámci LAN sítě. Odpovídá na žádosti spojené s IP adresou virtuálního směrovače a také pravidelně odesílá ohlášení - `ADVERTISEMENT`. Interval mezi ohlášeními je možno upravit, ve výchozím nastavení je 1 sekunda.

V přídadě, kdy obdrží `ADVERTISEMENT`. provede následující:

- Porovnání priorit, jestliže lokální priorita je menší, přejde do stavu Backup
- Priority mají stejnou hodnotu a dojde tedy k porovnání lokální IP adresy a IP adresy odesilatele, na jehož výsledku se rozhodne, zda zůstane ve svém stavu nebo přejde do stavu Backup.

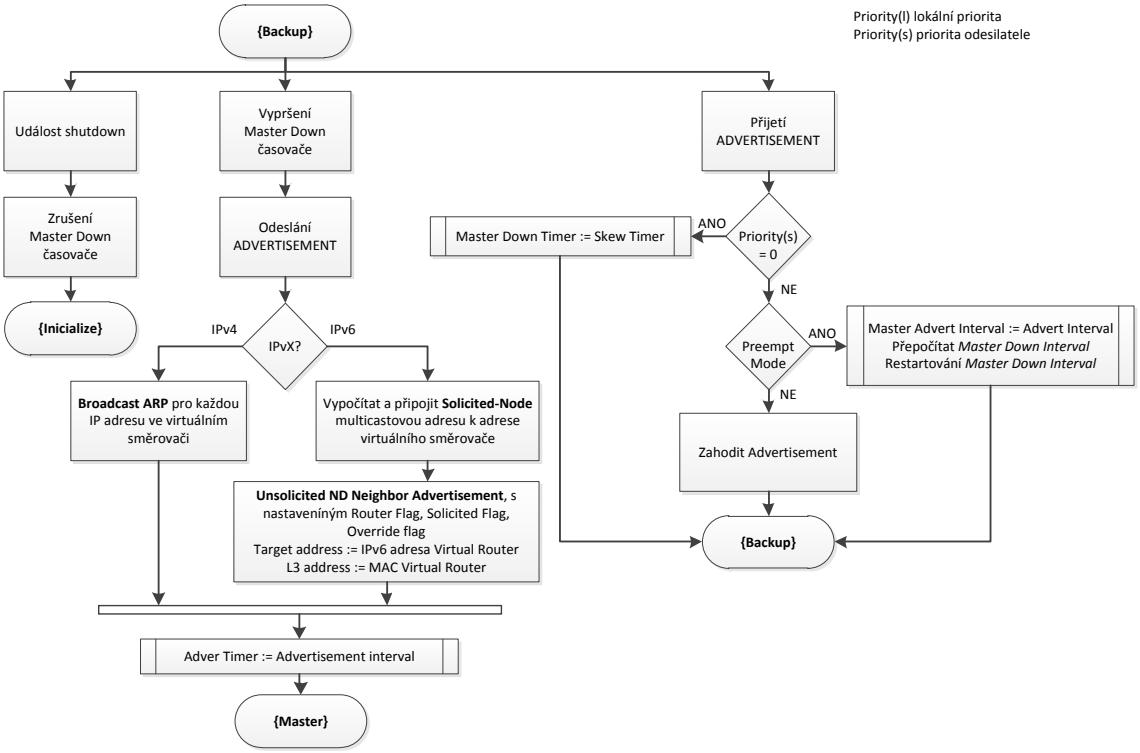


Obrázek 2.6: Průběh činnosti ve stavu Master

Stav Backup

Během Backup stavu (obrázek 2.7) se směrovač neúčastní provozu. Pouze sleduje VRRP oznámení od Master a vykonává následující:

- Jestliže není přijato oznámení po předem stanoveném časovém intervalu, pak provede přechod do stavu Master.
- Zjistí-li směrovač ve výchozím stavu, že má vyšší prioritu než aktuální Master, dojde k předání rolí, tj. aktuální Master přenechá svoji roli. Toto chování lze vypnout.



Obrázek 2.7: Průběh činnosti ve stavu Backup

2.3.7 Struktura paketu

Veškeré informace, které posílá směrovač Master jsou v položkách za IP hlavičkou.

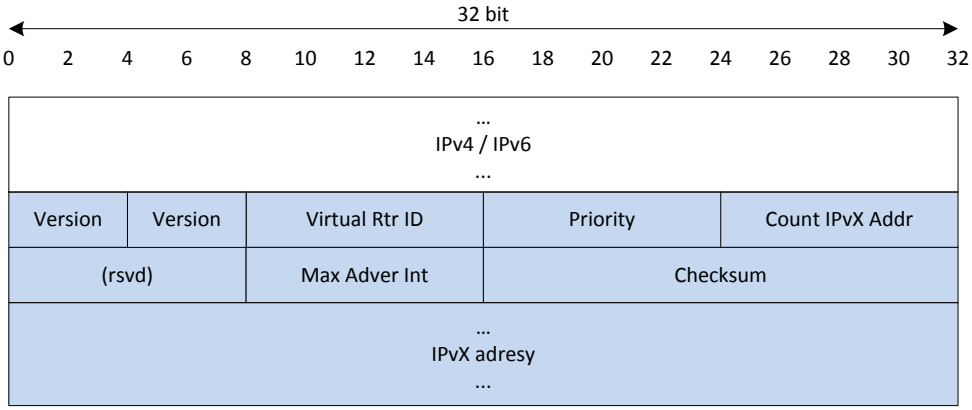
Relevantní položky IP hlavičky:

- **Source address**
  Primární IPv4 / IPv6 adresa rozhraní, ze kterého byl paket odeslán.
- **Destination address**
  Multicastová adresa přiřazena IANA pro VRRP je:

  ```
  IPv4: 224.0.0.18
  IPv6: FF02::12
  ```

  Tato adresa je určena pro lokální multicast, paket s touto cílovou adresou nesmí směrovač přeposlat bez ohledu na jeho TTL / Hop Limit.
- **TTL / Hop Limit**
  Hodnota této položky musí být nastavena na hodnotu 255. VRRP směrovač, který obdrží ohlášení s nižší hodnotou, musí tento paket zahodit.
- **Protocol / Next header**
  Číslo IP protokolu přiřazené IANA pro VRRP je 112 (dekadicky).

Struktura VRRP paketu je znázorněna na obrázku 2.8.



Obrázek 2.8: Struktura VRRP paketu

- **Version**
  Verze VRRP protokolu, který vygeneroval paket.
- **Type**
  Typ VRRP paketu. Jediný možný typ je `ADVERTISEMENT`, zadaný binární číslicí 1. Pakety neznámého typu jsou zahozeny.
- **Virtual Rtr ID (VRID)**
  Jednoznačně identifikuje virtuální směrovač v lokální síti.
- **Priority**
  Priorita VRRP směrovače, který vyslal paket. Vyšší hodnota znamená vyšší prioritu. Pole je 8bitový bez znamenkový integer.
- **Count IPvX address**
  Počet adres obsahující VRRP oznámení. Minimální hodnota je 1.
- **Rsvd**
  Toto pole musí být při odeslání nasteveno na 0 a při příjmu ignorováno.
- **Maximum Advertisement Interval (Max Adver Int)**
  Udává časový interval pro ohlášení, po kterém je odeslán oznamovací paket o dostupnosti směrovače. Výchozí hodnota je 1 sekunda.
- **Checksum**
  Kontrolní součet sloužící k detekci poškození dat ve zprávě. V době výpočtu je hodnota nastavena na 0.
- **IPvX Address**
  Jedna nebo více IP adres asociovaných s virtuálním směrovačem, jejichž počet udává pole Count IPvX address.

2.4 Hot Standby Router Protocol

Protokol Hot Standby Router Protocol je proprietární protokol společnosti Cisco [4], který je ale také popsán v RFC 2281 [8].

HSRP je svým principem velmi podobný protokolu VRRP (kapitola 2.3), jejich funkce jsou téměř totožné a liší se pouze v detailech. Směrovače jsou organizovány do skupin, ve kterých jeden směrovač plní roli výchozí brány, tzv. Active Router.

Active Router plní totožnou funkci jako Master u Virtual Router, zajišťuje správu paketů zasílaných na MAC adresu výchozí brány. HSRP využívá následující MAC adresu `00-00-0c-9f-fc-{GID}`, kde `{GID}` je číslo skupiny v hexadecimálním tvaru.

Oproti protokolu VRRP zavádí roli Standby, jejíž funkcí je monitorování stavu Active Router. V případě detekce jeho výpadku Standby okamžitě přebírá roli Active a začíná zpracovávat pakety odesílané na virtuální IP adresu výchozí brány. Active i Standby směrovače posílají Hello zprávy, aby informovaly ostatní členy skupiny o svém stavu.

Architektura protokolu dovoluje využít i další směrovače. Ty ale nemají přiřazenu žádnou speciální roli, jejich úkolem je sledovat Hello zprávy od Active i Standby a v případě detekce jejich výpadku je vybrán nový Active respektive Backup.

HSRP používá širší spektrum odesílaných zpráv:

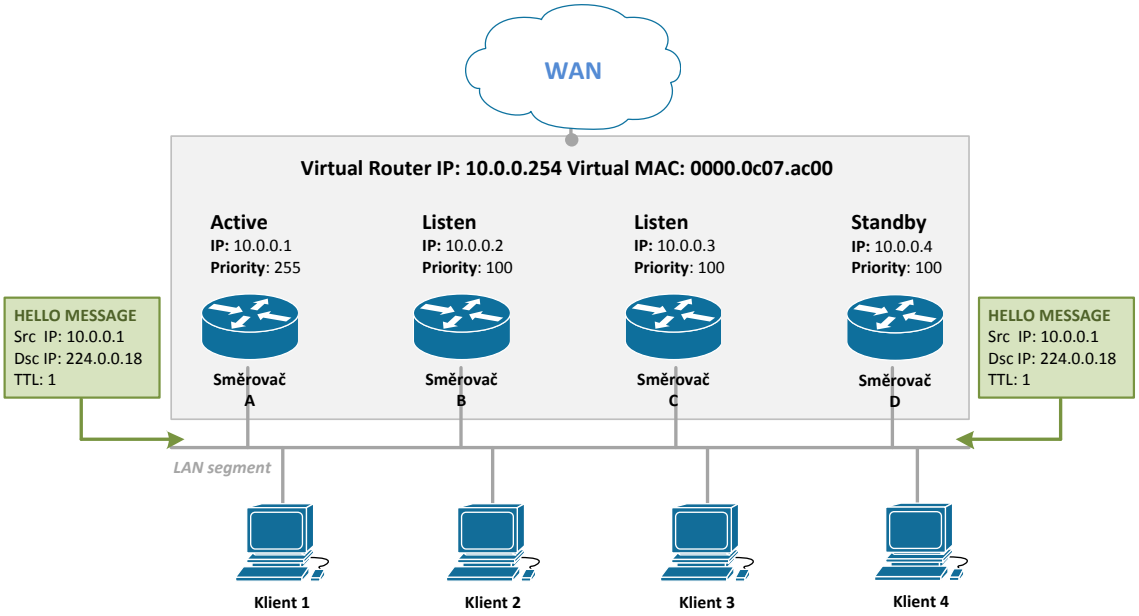
- **Hello** - pomocí zprávy Hello informuje Active i Backup ostatní směrovače o své aktivitě, může je také informovat o prioritách a hodnotách některých intervalů.
- **Coup** - zpráva od Standby směrovači Active, jestliže chce převzít jeho roli, tzn. Standby má vyšší prioritu.
- **Resign** - zprávu posílá Active router, pokud již nadále nechce / nemůže pokračovat ve své roli.

Tyto zprávy jsou odesílány na multicastovou adresu `224.0.0.2` pomocí protokolu UDP a portu `1985`.

Virtuální IP adresa nesmí být shodná s žádnou IP adresou. To je zásadní rozdíl oproti VRRP, kde IP adresa mohla být adresa reálného rozhraní směrovače. S tím také souvisí proces volby jednotlivých rolí, který spoléhá na priority jednotlivých směrovačů.

HSRP přináší následující benefity:

- **Redundance**
  HSRP využívá systém redundance, který je časem ověřený a nasazovaný v rozsáhlých sítích.
- **Rychlé převzetí služeb při selhání**
  Poskytuje transparentní a rychlé převzetí služeb při selhání směrovače.
- **Preemce**
  Preemce umožní směrovači Standby zpožděný přechod do role Active.
- **Autentizace**
  HSRP Message Digest 4 (MD5) algoritmus ověřování chrání HSRP proti spoffing a používá průmyslový standard algoritmu MD5 pro zlepšení spolehlivosti a bezpečnosti.



Obrázek 2.9: Ukázka zapojení HSRP

2.4.1 HSRP verze 2

HSRP ve druhé verzi přináší několik změn a vylepšení [5]. Prvním výrazným vylepšením je rozšíření rozsahu hodnot pro identifikaci skupiny z 0-255 v první verzi na 0-4095. S rozšířením intervalu souvisí i změna virtuální MAC adresy. Nová MAC adresa má tvar `0000.0e9f.f{GID}`, kde k identifikaci Standby skupiny slouží posledních 12 bitů.

V první verzi nebylo možné identifikovat zdroj Hello zprávy, protože tyto zprávy byly odesílány se zdrojovou MAC adresou virtuálního směrovače. Ve druhé verzi byla rozšířena hlavička zprávy o 6-ti bajtové pole. Toto pole je vyplněno reálnou MAC adresou rozhraní odesilatele.

Mezi další změny patří změna multicastové adresy, na kterou jsou zprávy odesílány. Multicastová adresa HSRPv1 `224.0.0.2` koliduje s protokolem Cisco Group Management Protocol (CGMS).

Kooperace HSRPv1 a HSRPv2 není možná, protože HSRPv2 používá formát hlavičky TLV tzv. type-length-value. Tyto pakety se zaměřují na optimalizaci rychlosti a velikosti přenesených dat. Zpráva HSRPv2 přijatá směrovačem s HSRPv1 bude ignorována a zahozena, toto platí i pro opačně odeslané zprávy.

2.4.2 Základní pojmy

Mezi pojmy používané v HSRP patří:

- **Active Router**
  Směrovač, který momentálně směruje pakety ve Standby Group.
- **Standby Router**
  Primární záložní směrovač.
- **Standby Group**
  Množina směrovačů, které společně představují virtuální směrovač.

- **Hello Time**
  Interval mezi po sobě jdoucími Hello zprávami z daného směrovače, tedy doba po kterou Active nebo Standby čeká od odeslání jedné Hello zprávy do odeslání další. Ve výchozím nastavení je hodnota intervalu rovna 3 sekundám.

- **Hold Time**
  Interval mezi obdržením Hello zprávy a prohlášením o selhání zařízení. Pokud po přijetí poslední zprávy Hello uplyne doba intervalu Hold Time, je daný směrovač považován za nefunkční.

2.4.3 Časovače a intervaly

Každý HSRP směrovač obsahuje tři časovače Active, Standby a Hello. HSRP konverguje, když dojde k selhání, to závisí na nastavení hodnot Hello Time a Hold Time. Ve výchozím nastavení mají hodnotu 3 sekundy a 10 sekund, to znamená, že Hello paket je odesílán každé 3 sekundy a pokud neobdrží Standby paket po dobu 10 sekund, je odesilatel prohlášen za nedostupného.

- **Časovač Active** se používá ke sledování Active router. S každou přijatou Hello zprávou je časovač anulován. Dosáhne-li hodnoty intervalu Hold time je Active router prohlášen za nedostupný.

- **Časovač Standby** využívá stejného principu jako časovač Active, ale pro Standby Router.

- **Časovač Hello** je určen k plánování odesílání Hello zpráv.

Vysoké hodnoty intervalů Hello Time a Hold Time způsobují vysokou prodlevu před převzetím funkcí a naopak extrémně malé hodnoty mohou mít za následek snížení stability HSRP skupiny. Směrovače by v tomto případě nemusely v důsledku zatížení stihnout odesílat či správně zpracovávat přijaté Hello zprávy. To by způsobilo chybné vyhodnocování výpadku a "neoprávněné"převzetí jeho role. Nastavení intervalů je kompromisem mezi stabilitou skupiny a rychlým zotavením z výpadku.

2.4.4 Proces volby a převzetí rolí

Proces volby rolí je založen na prioritě směrovačů. Priorita může nabývat hodnot v rámci intervalu 0 až 255, přičemž vyšší hodnota znamená vyšší prioritu. Pokud existují zařízení se stejnou hodnotou priority, vítězí to s vyšší IP adresou na rozhraní.

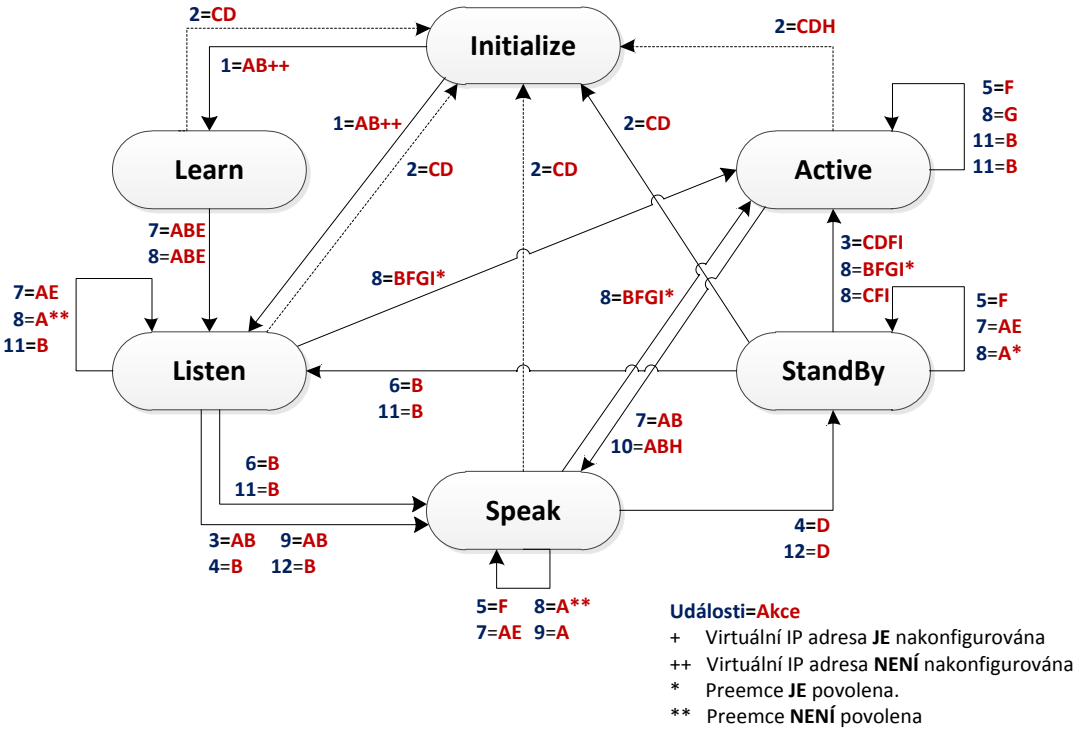
Obrázek 2.9 zobrazuje Standby Group s číslem 10, kterou tvoří 4 zařízení. Směrovač A má prioritu 255 a proto plní funkci Active router. Zbylé 3 směrovače se stejnou hodnotou priority mezi sebou volí Standby, tím se stává díky vyšší IP adrese `10.0.0.4` směrovač D.

Jestliže současný Active selže, Standby přestává dostávat Hello zprávy a po dosažení časovače Active intervalu Hold Time (10s) přebírá funkce Active router. Směrovače B i C, jenž se aktuálně nacházejí ve stavu Listen, zahájí volbu nového Standby, jakmile časovač Standby nabude intervalu Hold Time (10s). Tím se stává s vyšší IP adresou směrovač C. Na konci volby směrovač D plní funkce Active router, směrovač C je novým Standby a B se nachází ve stavu Listen.

2.4.5 Stavový automat

HSRP Směrovač se může nacházet v jednom z těchto stavů: Initial, Learn, Listen, Speak, Standby nebo Active. Obrázek 2.10 zobrazuje stavový automat protokolu HSRP, kde jednotlivé události jsou popsány v tabulce 2.2 a reakce na ně v podobě akcí v tabulce 2.3.

- **Initial**
  Počáteční stav indikující, že HSRP zatím neběží. Do toho stavu směrovač přejde po změně konfigurace nebo při povolení rozhraní.
- **Listen**
  Směrovač zná virtuální IP adresu, ale není ani Active ani Standby router.
- **Speak**
  Ve stavu speak odesílá pravidelné Hello zprávy a aktivně se podílí na volbě Active nebo Standby router. Do Speak stavu nemůže směrovač vstoupit, pokud má virtuální IP adresu.
- **Standby**
  Směrovač je hlavním kandidátem, aby byl další Active router. Posílá pravidelně Hello zprávy. Maximálně jeden člen ve skupině se nachází ve stavu Standby.
- **Active**
  Ve stavu Active router zpracovává pakety posílané na adresu virtuálního směrovače.



Obrázek 2.10: Stavový automat HSRP

Událost	Popis
1	HSRP je nakonfigurováno a síťové rozhraní povoleno.
2	Rozhraní nebo HSRP je vypnuto.
3	Časovač Active vypršel. Časovač je nastaven na hodnotu Hold time při přijetí poslední zprávy od Active router.
4	Časovač Standby vypršel. Časovač je nastaven na hodnotu Hold time při přijetí poslední zprávy od Standby router.
5	Časovač Hello vypršel. Časovač pro pravidelné odesílání Hello zpráv vypršel.
6	Příjem Hello zpráv od směrovače ve stavu Speak s vyšší prioritou.
7	Příjem Hello zpráv od Active router s vyšší prioritou.
8	Příjem Hello zpráv od Active router s nižší prioritou.
9	Příjem Resign zprávy do Active Router.
10	Příjem Coup zprávy od směrovače s vyšší prioritou.
11	Příjem Hello zprávy od Standby router s vyšší prioritou.
12	Příjem Hello zprávy od Standby router s nižší prioritou.

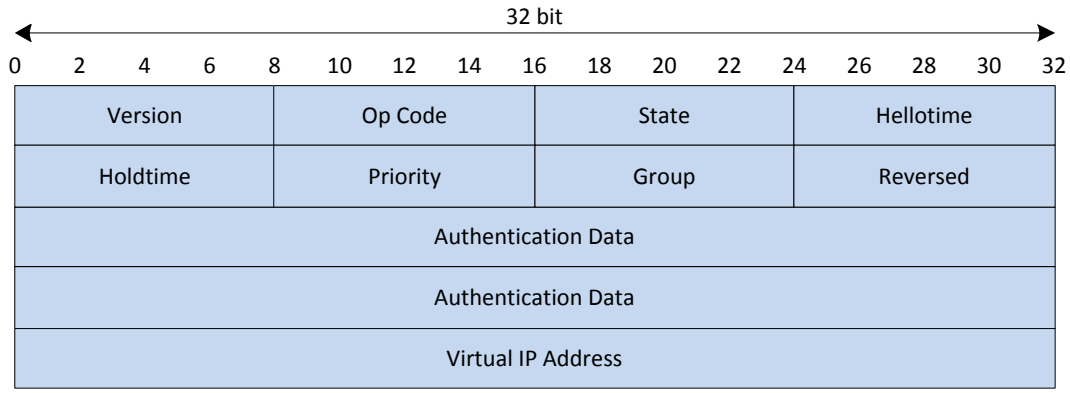
Tabulka 2.2: Události stavového automatu

Akce	Popis
A	Pokud k této akci dojde v důsledku přijetí ověřené zprávy Hello od Active Router je časovač Active nastaven na hodnotu v Hello zprávě, v opačném případě je používána lokální hodnota Hold time. Časovač Active je spuštěn.
B	Pokud k této akci dojde v důsledku přijetí ověřené zprávy Hello od Standby Router je časovač Standby nastaven na hodnotu v Hello zprávě, v opačném případě je používána lokální hodnota Hold time. Časovač Standby je spuštěn.
C	Časovač Active byl zastaven.
D	Standby časovač byl zastaven.
E	Tato akce je přijata, pokud je ověřená zpráva přijata od Active router. Jestliže není virtuální IP adresa této skupiny nastavena ručně, může se jí dozvědět ze zprávy, z níž se může také naučit hodnoty Hello time a Hold time.
F	Směrovač posílá Hello zprávu s aktuálním stavem, Hello time a Hold time.
G	Směrovač odesílá Coup zprávu s cílem informovat Active Router, že je k dispozici směrovač s vyšší prioritou.
H	Směrovač odesílá zprávu Resign, aby umožnil dalšímu směrovači stát se Active Routerem.
I	Směrovač vysílá paket ARP Reply, ve kterém inzeruje virtuální IP a MAC adresu.

Tabulka 2.3: Akce stavového automatu

2.4.6 Struktura paketu

Formát paketu definovaným standardem RFC 2281.



Obrázek 2.11: Struktura HSRP paketu

Význam jednotlivých položek je následující:

- **Version**
  Verze HSRP protokolu.
- **OpCode**
  Typ HSRP zprávy:
  - 0 - Hello
  - 1 - Coup
  - 2 - Resign
- **State**
  Aktuální stav, ve kterém se odesilatel paketu nachází:
  - 0 - Initial
  - 1 - Learn
  - 2 - Listen
  - 4 - Speak
  - 8 - Standby
  - 16 - Active
- **Hello time**
  Význam tohoto pole je pouze ve zprávách Hello. Směrovač se může hodnotu naučit z ověřených zpráv od Active router. Výchozí hodnota jsou 3 sekundy.
- **Hold time**
  Hodnota v Hello zprávách označuje množství času v sekundách, která určuje dobu platnosti Hello zprávy. Doporučovaná hodnota je alespoň trojnásobek hodnoty Hello time, ve výchozím nastavení je 10 sekund.

- **Priority**
  Pole jehož hodnota se využívá pro volbu Active nebo Standby směrovače. Při porovnávání směrovačů vítězí ten jenž má vyšší hodnotu. Jsou-li shodné rozhoduje vyšší IP adresa.

- **Group**
  Číselný identifikátor HSRP. Pro Token Ring je rozsah 0 až 2, pro ostatní média 0 až 255.

- **Authentication Data**
  Toto pole obsahuje textové heslo o velikosti 8 znaků, ve výchozím nastavení má hodnotu `0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00` (cisco).

- **Virtual IP Address**
  Virtuální adresa skupiny HSRP. V případě, že směrovač nemá manuálně zadanou virtuální adresu, může se ji naučit z Hello zprávy od Active router. To je umožněno poze pokud je Hello zpráva autentizována.

2.5 Gateway Load Balancing Protocol

Nyní víme jak může být VRRP/HSRP efektivní při poskytování redundantních bran. Rozložení provozu můžeme dosáhnout pouze vícenásobným použitím skupin. Je potřeba určit rozdělení koncových stanic mezi virtuální směrovače. Každá skupina stanic musí být směrována na příslušný virtuální směrovač. Takovéto sdílení zátěže je poněkud těžkopádné.

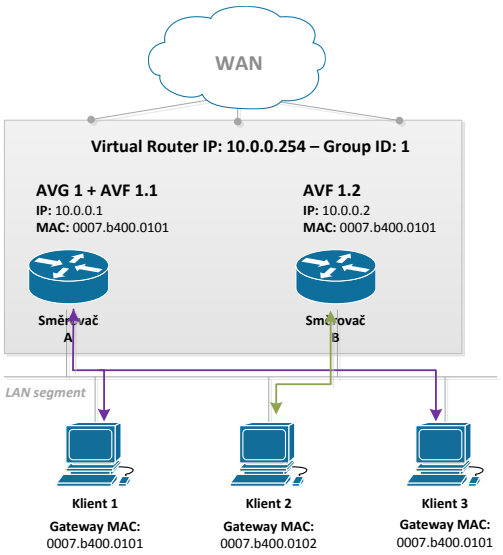
Gateway Load Balancing Protocol (GLBP) [3] je propriotární Cisco protokol navržen tak, aby překonal stávající redundantní protokoly. GLBP chrání datový provoz při výpadku směrovače stejně jako VRRP či HSRP ale zároveň umožňuje sdílení zátěže mezi skupinou směrovačů.

Vyrovnání zátěže tzv. Load Balancing je technika, při niž se po překročení určité prahové hodnoty síťového provozu na primární lince odkloní část provozu na jinou, sekundární linku. Vyrovnání zátěže se podobá redundanci, protože také po vzniku definované události dochází k přesunu síťového provozu jinam a rovněž součástí konfigurované sítě musí být druhé, alternativní zařízení. Při vyrovnání zátěže toto zařízení nemusí být nutně pouze redundantní, ale může normálně fungovat i bez havárie primárního zařízení.

Rozhraní GLBP jsou organizovány do skupin, které určují jejich příslušnost k virtuálnímu směrovači. Členové skupiny si zvolí jeden směrovač jako `Active Virtual Router` (AVG), zbylí členové působí jako zálohy pro výpadek AVG. Funkce AVG je přiřazení virtuální adresy MAC každému členu skupiny. Všechny směrovače přijímají odpovědnost za směrování paketů posílaných na virtuální MAC adresu, která mu byla přidělena AVG. Tyto směrovače se označují Active Virtual Forwarder (AVF).

GLBP poskytuje redundanci virtuálních bran stejným způsobem jako HSRP. Jeden směrovač je v roli AVG, další ve Standby roli a zbývající směrovače jsou ve stavu Listen. Pokud výchozí brána AVG selže, směrovač v pohotovostním režimu Standby převezme jeho roli a stává se novým Active Virtual Gateway.

Komunikace probíhá na portu UDP portu `3222` prostřednictvím Hello zpráv odesílaných ve výchozím nastavení každé 3 sekundy na multicastovou adresu `224.0.0.102`.



Obrázek 2.12: Ukázka zapojení GLBP

Protokol GLBP přináší do počítačové sítě následující benefity:

- **Automatický Load Balancing**
  Síťový provoz je sdílen mezi dostupnými bránami dle stanoveného algoritmu vyrovnávání zátěže.
- **Vícenásobný virtuální směrovač**
  GLBP umožňuje až 1024 virtuálních směrovačů (GLBP skupin) na každém fyzickém rozhraní a až čtyři virtuální AVF na skupinu.
- **Převzetí aktivní role**
  Redundance GLBP umožňuje převzetí aktivní role záložnímu směrovači s nejvyšší prioritou.
- **Autentizace**
  Pro zvýšení spolehlivosti, bezpečnosti a ochrany proti GLBP-spoofing je používán algoritmus Message Digest 5 (MD5). Směrovač jenž obsahuje jiný autentizační řetězec než ostatní směrovače ve skupiny, bude ignorován.
- **Jednoduchá konfigurace**
  Konfigurace protokolu je velmi jednoduchá. Každý směrovač v GLBP skupině musí mít nastaveno číslo skupiny a virtuální IP adresu. Všechny ostatní parametry mohou být naučeny.

Na uvedené topologii (obrázek 2.12) je směrovač A pro GLBP skupinu 1 AVG a je také odpovědný za virtuální IP adresu `10.0.0.1`. Směrovač A je také AVF pro virtuální MAC `0007.b400.0101`. Směrovač B je členem stejné skupiny a je určen AVF pro virtuální MAC adresu `0007.b400.0102`. Klient 1 má výchozí `bránu 10.0.0.254` s MAC adresou `0007.b400.0101`. Klient 2 má stejnou IP adresu výchozí brány, ale s MAC adresou `0007.b400.0102`, protože směrovače sdílí zátěž přenosového pásma mezi sebou.

2.5.1 Základní pojmy

V úvodu GLBP jsem vysvětlil pojmy Active Virtual Router a Active Virtual Forwarder, mezi další pojmy patří:

- **Virtual Forwarder (VF)**
  Abstraktní entita v rámci GLBP brány, která přijímá odpovědnost za virtuální MAC adresu.
- **Primary Virtual Forwarder (PVF)**
  Virtual Forwarder, jemuž byla přiřazena virtuální MAC adresu od AVG.
- **Secondary Virtual Forwarder (SVF)**
  Virtual Forwarder, který se naučil virtuální MAC adresu z Hello zprávy.

2.5.2 Load Balancing metody

GLBP používá následující metody vyrovnání zátěže viz konfigurace cisco [2]:

- **Žádná**
  Situace kdy není zvolená žádná metoda.
- **Round Robin**
  Požadavky na MAC adresu výchozí brány, jsou v jednom cyklu postupně uvedeny všechny MAC adresy AVF.
- **Vážený**
  Váha GLBP rozhraní určuje poměr provozu v rámci skupiny směrovačů. Vyšší váha znamená vyšší provoz tohoto rozhraní směrovače. Hodnota váhy slouží k nastavení relativních poměrů mezi AVF.
- **Podle koncových stanic**
  Každý klient, který generuje `ARP Request` pro virtuální adresu směrovače, vždy dostane v odpovědi stejnou virtuální MAC adresu. Není doporučováno pro malý počet koncových stanic. Čím větší je počet hostitelů, tím je menší pravděpodobnost nerovnováhy provozu.

Load Balancing podle metody koncových stanic se používá v aplikacích, kde je potřeba sledovat datové toky (např. při použití NAT). Round robin je výchozí metoda, která je vhodná pro všechny ostatní požadavky. Vážená metoda je vhodná v případě, kdy máme zařízení s různými možnostmi bran.

2.5.3 Časovače a intervaly

Intervaly Hello Time a Hold Time u GLBP mají obdobný význam jako u protokolu HSRP. Použití těchto intervalů jsem již vysvětloval u protokolu HSRP (kapitola 2.4.3), a proto se zde zaměřím pouze na dva nové intervaly Redirect time a Secondary Hold time.

- **Redirect time**
  Doba, po kterou AVG přesměrovává hostitele na AVF. Cílem je pokračovat ve zpracování nových ARP požadavků dle aktuálního návrhu vyrovnávání zatěže, v očekávání, že se nedostupný VF vrátí do stavu online. Pokud k tomu dojde v průběhu intervalu Redirect, získá VF svoje předchozí zatížení.

- **Secondary Hold time**
  Doba po kterou zůstává sekundární Virtual Forwarder (SVF) v platnosti při nedostupnosti primárního VF. SVF je odstraněn při intervalu Secondary Hold. Jakmile je SVF ostraněn, load balancing metoda upraví rozdělení provozu mezi zbývající VFS. Výchozí hodnota je 1 hodina v rozsahu 40 minut až 18 hodin.

Oba intervaly se směrovač obvykle naučí od svého AVG, jestliže nem je použit ručně zadaný interval.

2.5.4 Virtuální MAC adresy

Skupina GLBP umožňuje až čtyři virtuální MAC adresy pro skupinu. Primární AVG je odpovědný za přiřazení MAC adres každému členu skupiny. Směrovačům jsou přidělovány virtuální MAC adresy postupně. Ostatní směrovače, které objeví AVG prostřednictvím Hello zprávy, se nazývají sekundární AVF.

Virtuální adresa v protokolu GLBP má následující tvar

`00-07-B4-XX-XX-XX`

Kde `XX-XX-XX` odpovídá nejnižším 24 bitům. Prvních 6 bitů tohoto úseku má hodnotu 0, následujících 10 bitů uvádí číslo skupiny a posledních 8 bitů odpovídá číslu Virtual Forwarder.

Protokol umožňuje až 1024 skupin a 255 Virtual Forwarder, ale konfigurace je v současné době omezena pouze na 4 (01 až 04) Virtual Forwarder na redundantní skupinu.

2.5.5 Stavy VG a VF

Směrovač v roli virtuální brány se může nacházet v jednom z následujících stavů:

- **Disabled** - Směrovač s GLBP konfigurací, ale nebyla mu přiřazena ani se nanaučil virtuální IP adresu.
- **Initial** - Konfigurace GLBP není kompletní, přestože VF zná virtuální IP adresu.
- **Listen** - VG příjmá pravidelné zprávy Hello, jakmile je Standby nebo Active nedostupný přechází do stavu Speak.
- **Speak** - VG se pokouší přejít do stavu Standby nebo Active.
- **Standby** - Směrovač je připraven přejít do stavu Active, při vypršení intervalu Hold time.
- **Active** - Stav ve kterém směrovač odpovídá na ARP dotazy spojené s virtuální IP adresou.

Pro Virtual Forwarder existují následující čtyři stavy:

- **Disabled** - Virtuální MAC adresa nebyla naučena ani přiřazena. Tento stav je přechodný, protože VF ve stavu disabled jsou smazány.
- **Initial** - VF zná virtuální MAC, ale jeho konfigurace není kompletní.
- **Listen** - VF přijímá Hello zprávy a je připraven přejít do stavu Active, bude-li současný AVF prohlášen za nedostupný.
- **Active** - Označuje směrovač AVF, je odpovědný za předávání paketů zasílaných na virtuální MAC adresu VF.

2.5.6 Struktura paketu

Jak je vidět na obrázku 2.13, GLBP využívá ve svých paketech dvě struktury TLV. První TLV obsahuje informace související s AVG, tj. hodnoty jednotlivých intervalů Hello, Hold, Redirect i Timeout, dálé virtuální IP adresu a svůj stav a prioritu virtuální brány v rámci GLBP skupiny.

Druhá struktura obsahuje informace vztahující se k AVF. Mezi tato data patří virtuální MAC adresa, stav a hodnota váhy VF.

```
Frame 49: 102 bytes on wire (816 bits), 102 bytes captured
IPv4, Src: 10.0.0.1 (10.0.0.1), Dst: 224.0.0.102 (224.0.0.102)
User Datagram Protocol, Src Port: glbp (3222), Dst Port: glbp
(3222)
Gateway Load Balancing Protocol
Version?: 1
Unknown1: 0
Group: 1
Unknown2: 0000
Owner ID: d0:00:16:8e:00:00 (d0:00:16:8e:00:00)
TLV l=28, t=Hello

     Type: Hello (1)
     Length: 28
     Unknown1-0: 00
     VG state?: Listen (4)
     Unknown1-1: 00
     Priority: 100,
     Unknown1-2: 0000
     Helloint: 3000
     Holdint: 10000
     Redirect: 600
     Timeout: 14400
     Unknown1-3: 0000
     Address type: IPv4 (1)
     Address length: 4
     Virtual IPv4: 10.0.0.254 (10.0.0.254)

TLV l=20, t=Request/Response?

     Type: Request/Response? (2)
     Length: 20
     Forwarder?: 2
     VF state?: Active (32)
     Unknown2-1: 00
     Priority: 135
     Virtualmac: Cisco_00:01:02 (00:07:b4:00:01:02)
```

Obrázek 2.13: Ukázka paketu zachyceným programem Wireshark

2.6 Shrnutí

Všechny tři protokoly patří do skupiny protokolu FHRP. Díky standardu IETF umožňuje protokol VRRP zajistit kompatibilitu v počítačových sítích s různými výrobci síťových zařízení. Oproti tomu HSRP i GLBP je možno použít pouze v případě, kdy členové logické skupiny jsou zařízení z portfolia společnosti Cisco.

VRRP i HSRP zajišťují téměr stejnou funkcionalitu a liší se především v detailech jednotlivých protokolů. Naproti nim GLBP umožňuje lépe balancovat zátěž mezi všechny dostupné směrovače, které budou plnit funkci výchozí brány. Protokoly VRRP i HSRP podporují pouze jeden aktivní směrovač (Master u VRRP, Active v případě HSRP) a sdílení zátěže formou Load Sharing je težkopádné a špatně škálovatelné.

	VRRP		**HSRP**		**GLBP**
	VRRPv2	*VRRPv3*	*HSRPv1*	*HSRPv2*	
Standard	RFC 3768	RFC 5798	Cisco i RFC 2281		Cisco
IPv6	Ne	Ano	Ano		Ano
Transportní protokol	IP 112		UDP 1985	UDP 2029	UDP 3222
Multicastová adresa	224.0.0.18		224.0.0.2	224.0.0.102	224.0.0.102
Adresa MAC	0000.5e00.01__		0000.0c07.ac__	0000.0c9f.f___	Přiřazeno AVG
Rozsah skupin	0-255		0-255	0-4095	0-+1024
Časovače	Advertisement Interval Master Down Interval Skew Interval		Hello - 3s Hold - 10s		Hello - 3s Hold - 10s
Stavy	Master, Backup		Active, Standby, Listen		AVG, AVF
Autentizace	Ano	Ne	Ano		Ano
Funkce					
Defaultní preemce	Ano		Ano		Ano
Object tracking	Ano		Ano		Ano

Tabulka 2.4: Vlastnosti FHRP

Kapitola 3

Podpora FHRP na Cisco zařízeních

V předcházející kapitole jsem se věnoval teoretickému rozboru základních protokolů FHRP. V této kapitole předvedu konfiguraci těchto protokolů na reálných zařízeních společnosti Cisco. Vybral jsem si směrovače značky Cisco, protože jimi jsou primárně vybaveny školní laboratoře.

Společnost Cisco do svých směrovačů a přepínačů vkládá operační systém Cisco IOS. IOS je množina směrovacích, přepínacích a propojovacích telekomunikačních funkcí integrovaných do operačního systému. V této kapitole jsou popsány příkazy FHRP pro verzi Cisco IOS Release 12.4(16), který je podporován např. směrovači Cisco řady 3800, 2800 nebo 1800.

Každý popsaný příkaz obsahuje syntaxi, textový popis a příklad použití. Z popisu byly vynechány příkazy zajišťující vyšší stupně zabezpečení, protože vyžadují podrobnější znalost prostředí IOS. Kategorie volitelných příkazů pro volitelné přízpůsobení chování všech protokolů by měla být nastavena před samotným povolením protokolu. Zabrání se tím situaci neočekávaného přebírání rolí.

Funkčnost FHRP, resp. schopnost zotavit se z výpadku výchozí brány, lze ověřit např. pomocí příkazu `debug`, který je dostupný pro všechny tři protokoly. Jinou možností ověření je sledování příkazu `ping`, s jehož pomocí lze nepřetržitě odesílat `Echo Request ICMP` zprávy na libovolnou stanici dostupnou přes výchozí bránu. Hodnota parametru zpoždění přijaté odpovědi odpovídá vyladění časovačů. Pokud budou intervaly příliš dlouhé, dojde k vypršení limitu, po který se čeká na doručení `ICMP Echo Reply` a to zapříčiní nedostupnost cílové stanice. Tata situace by ovšem po správném nastavení časovačů neměla nastat.

3.1 Konfigurace rozhraní

Aby mohlo rozhraní pracovat s protokoly FHRP, musí mít přiřazenu IP adresu a musí být aktivní. Tato adresa je nutná pro zpracování IP provozu a musí být nastavena.

```
Router(config)# interface interface-type interface-number
Router(config-if)# ip address ip-address mask
Router(config-if)# no shutdown
```

3.2 VRRP

Operační systém Cisco IOS 12.4 podporuje pouze protokol VRRPv2, který se povoluje a nastavuje pro konkrétní rozhraní směrovače, tj. všechny příkazy až na vyjímky se zadávají v konfiguraci síťového rozhraní a začínají klíčovým slovem `vrrp`.

3.2.1 Povolení a zakázání

Skupina a IP adresa se konfiguruje na všech směrovačích, které VRRP používají. Použitá IP adresa je adresa, kterou budou stanice v síti používat jako adresu výchozí brány. Volba *group* slouží k nastavení více skupin na jednom směrovači. Díky tomu je možné zajistit redundanci. Parametr `secondary` udává, že záložní IP adresa je sekundární adresou. Toto nastavení se využívá v případě, kdy je rozhraní připojeno k síti, která zajišťuje směrování i pro sekundární síť.

`vrrp` *group ip-address* `[secondary]`

Příklad:
`Router(config-if)# vrrp 10 192.168.0.254`

Zákázáním VRRP skupiny na rozhraní umožňuje zastavit protokol při zachování stavající konfigurace.

`vrrp` *group* `shutdown`

Příklad:
`Router(config-if)# vrrp 10 shutdown`

3.2.2 Volitelná nastavení

Description

Příkazem `description` se nastavuje až 80 znaků dlouhý popis skupiny, má pouze lokální význam.

`vrrp` *group* `description` *text*

Příklad:
`Router(config-if)# vrrp 10 description working group 10`

Priority

Nastavením priority rozhraní a skupiny je možné určit, který směrovač bude sloužit jako primární směrovač skupiny. Do role Master bude zvolen směrovač s nejvyšší prioritou. Pokud jsou priority shodné, je zvolen směrovač s vyšší primární IP adresou. Výchozí priorita je 100.

`vrrp` *group* `priority` *level*

Příklad:
`Router(config-if)# vrrp 10 priority 150`

Převzetí aktivní role

Příkaz `preempt` umožní směrovači převzít funkci aktivního směrovače s vyšší prioritou. Po zapnutí směrovačů dochází k volbě aktivního směrovače. Pokud později dojde k připojení dalšího směrovače s vyšší prioritou, nebo pokud aktivní směrovač vypadne a znovu naběhne, nestane se už aktivním směrovačem, pokud nemá nastaveno, aby úlohu aktivního směrovače převzal. Volba `delay` umožňuje nastavit zpoždění v sekundách, po němž směrovač převezme funkci od stávajícího Master směrovače. Ve výchozím nastavení je povoleno okamžité převzetí.

`vrrp` *group* `preempt [delay minimum` *seconds*`]`

Příklad:

```
Router(config-if)# vrrp 10 preempt
Router(config-if)# vrrp 10 preempt delay minimum 400
```

Časovače

Interval po sobě jdoucích ohlášení lze ovlivňovat příkazem `timers` s parametrem *advertise*. Jednotka intervalu je uvedena v sekundách, po uvedení klíčového slova `msec` se mění na milisekundy. Výchozí hodnota je 1 sekunda.

`vrrp` *group* `timers` *advertise* `[msec]` *interval*

Příklad:

```
Router(config-if)# vrrp 10 timers advertise 4
```

Pokud mají směrovače nastaveny rozdílné hodnoty intervalu, nebude Backup přijímat ohlášení a přejde do stavu Master. Tomuto chování lze zabránit uvedením příkazu `timers` s parametrem *learn* na všech Backup směrovačích, pomocí něhož se inverval ohlášení naučí od Master směrovače.

`vrrp` *group* `timers` *learn*

Příklad:

```
Router(config-if)# vrrp 10 timers learn
```

Object tracking

Object tracking umožňuje sledovat objekty na zařízení jako je například stav rozhraní (`line-protocol`), IP směrovaní (`ip | ip6 routing`), dosažitelnost IP cesty a reagovat v případě, kdy sledovaný objekt změní stav. Tato funkce umožňuje zvýšit dostupnost sítě a zkrátit dobu zotavení.

`track` *object-number* `interface` *type number* {`line-protocol | {ip | ip6} routing`}

Příklad:

```
Router(config-if)# track 2 interface serial 6 line-protocol
```

Číslo objektu *object-number* je použito u příkazu `vrrp track`, který umožnuje upravovat hodnotu priority.

`vrrp` *group* `track` *object-number* `[decrement` *priority*`]`

Příklad:
`Router(config-if)# vrrp 10 track 2 decrement 20`

Jestliže VRRP skupina obsahuje IP adresu vlastníka, tzn. priorita má fixní hodnotu 255, nemůže být priorita jakkoliv snížena.

3.2.3 Monitorování a verifikace

Pro kontrolu správné funkčnosti protokolu existují dva příkazy `show vrrp` a `debug vrrp`.

`show vrrp [all | brief | interface]`

Příkazem zobrazíme informace o roli směrovače, informace o časovačích a jejich intervalech. Přepínač `all` zobrazuje informace o všech VRRP skupinách v rámci směrovače nebo pomocí `interface` zobrazí pouze vybrané rozhraní.

```
Router# show vrrp
FastEthernet0/0 - Group 10
State is Master
Virtual IP address is 192.168.1.254
Virtual MAC address is 0000.5e00.000a
Advertisement interval is 1.000 sec
Preemption enabled
Priority is 150
Master Router is 192.168.1.254 (local), priority is 200
Master Advertisement interval is 1.000 sec
Master Down interval is 3.218 sec
```

3.3 HSRP

Proprietární protokol HSRP je podporován v obou jeho verzích pod klíčovým slovem `standby`. Výchozí verze je HSRPv1. Chování HSRP je možno definovat pro fyzický port, rozhraní VLAN nebo EtherChannel.

3.3.1 Povolení a zakázání

Vlastní zapnutí HSRP na rozhraní se provádí příkazem:

`standby` *group-member* `ip` *ip-address* `[secondary]`

Příklad:
`Router(config-if)# standby 10 ip 192.168.0.254`

Kde *group-member* je číslo skupiny, může nabývat hodnot 0 až 255, kdy 0 je defaultní a nemusí se zadávat. IP adresa je virtuální adresa brány, kterou zadávají klienti při konfiguraci sítě jako adresu výchozí brány.

Pro vypnutí HSRP skupiny se používá příkaz:

`no standby` *group-member* `ip` *ip-address*

Příklad:
`Router(config-if)# no standby 10 ip 192.168.0.254`

3.3.2 Volitelná nastavení

Priority

Příkaz `standby priority` je ekvivalentem příkazu `vrrp priority` (kapitola 3.2.2), tzn. směrovač s nejvyšší hodnotou ve skupině bude plnit funkce Active směrovače. Výchozí priorita má hodnotu 100.

`standby` *group-member* `priority` *level*

Příklad:
`Router(config-if)# standby 10 priority 150`

Verze

Implicitně Cisco směrovače používají HSRP verze 1. HSRP verzi je možné změnit příkazem:

`standby version {1 | 2}`

Příklad:
`Router# standby version 2`

Název

Příkaz `standby name` umožňuje nastavit název HSRP skupiny.

`standby` *group-member* `name`

Příklad:
`Router# standby 1 name WorkGroup`

Adresa MAC

Následující příkaz slouží ke specifikaci virtuální MAC adresy. Je však doporučováno tento příkaz nepoužívat, ale místo toho využít výchozí well-known MAC adresy HSRP.

`standby` *group-member* `mac-address` *mac-address*

Příklad:
`Router# standby 1 mac-address 4000.1000.1060`

Převzetí aktivní role

Význam příkazu `standby preempt` je stejný jako u protokolu VRRP, popsaný v kapitole 3.2.2. HSRP k parametru *minimum* navíc přidává další dva *reload* a *sync*.

`standby` *group-member* `preempt [delay [minimum` *seconds* `| reload` *seconds* `| sync` *seconds*`]]`

Příklad:
`Router# standby 1 preempt delay 300`

Minimum i *reload* odloží převzetí aktivní role směrovačem s vyšší prioritou, ale *reload* pouze při opětovném načtení směrovače. Parametr *sync* zpozdí převzetí tak, aby redundantní klienti stihli odpovědět. Po vypršení tohoto intervalu dochází k převzetí bez ohledu na aktuální stav redundantních směrovačů.

Časovače

Příkazem `standby timers` se nastavuje interval, v němž směrovač odesílá hello pakety, kterými sděluje svůj stav, a dále interval, po němž je směrovač prohlášen za nefunkční. Hodnota časovače hold by měla být vždy alespoň trojnásobek hodnoty hello. Nastavení časovačů aktivního směrovače skupiny vždy přepíše případná jiná nastavení ostatních směrovačů. Výchozí nastavení jsou 3 sekundy pro časovač hello a 10 sekund pro časovač hold.

`standby` *group-member* `timers [msec]` *hello-time* `[msec]` *hold-time*

Příklad:
`Router# standby 1 timers 5 15`

Přesměrování ICMP

Odesílání zpráv ICMP Redirect s virtuální IP adresu jako IP adresou brány se nastaví příkazem:

`standby redirects {enable | disable}`

Příklad:
`Router# standby redirects enable`

Autentizace

Autentizace záložní skupiny se nastavuje příkazem `authentication text`. Všechny směrovače ve skupině musí mít nastaveny stejný řetězec. Pokud směrovač nemá řetězec nastaven správně, nebude moci fungovat jako aktivní ani záložní směrovač.

`standby` *group-member* `authentication text` *word*

Příklad:
`Router# standby 1 authentication word secret`

Při změně hesla je doporučováno změnit řetězec *word* u aktivního směrovače jako poslední, zabrání se tím jakékoliv změně stavu. Změněn by měl být nejpozději do vypršení intervalu `Hold time`. Tento postup zaručuje, že záložní směrovače nemají čas převzít roli Active.

3.3.3 Monitorování a verifikace

Kontrolu správného průběhu protokolu HSRP lze provádět pomocí příkazu `show standby`

```
show standby [BVI | FastEthernet | Port-channel | all | brief |
capability | delay | internal | redirect]
```

nebo pomocí debugovacích informací `debug standby`.

```
Router# show standby
State is Speak
Virtual IP address is 192.168.1.254
Active virtual MAC address is 0000.0c07.ac00
Local virtual MAC address is 0000.0c07.ac00 (v1 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.804 secs
Preemption enabled
Active router is 192.168.1.1, priority 100 (expires in 8.920
sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Fa0/0-0"(default)
```

3.4 GLBP

Protokol GLBP je stejně jako HSRP proprietárním protokolem společnosti Cisco, který byl navržen tak, aby byl snadno konfigurovatelný. Minimálně jeden směrovač ve skupině musí mít nakonfigurovánu virtuální IP adresu, která bude použita pro celou skupinu. Všechny ostatní parametry se mohou směrovače naučit. Konfigurační příkazy začínají klíčovým slovem `glbp`.

3.4.1 Povolení a zakázání

V případě, kdy chceme aktivovat protokol GLBP pro skupinu *group-member*, použijeme následující příkaz:

`glbp` *group-member* `ip` *ip-address* `[secondary]`

Příklad:
`Router(config-if)# glbp 10 ip 192.168.0.254`

V opačném případě, tedy pro deaktivace skupiny *group-member* použijeme příkaz:

`no glbp` *group-member* `ip` *ip-address*

Příklad:
`Router(config-if)# no glbp 10 ip 192.168.0.254`

3.4.2 Volitelná nastavení

Priority

Každému směrovači ve skupině *group-member* lze přiřadit číselnou prioritu v rozmezí 0-255. Podle této hodnoty se následně rozhoduje, který z routerů převezme činnost AVG, pokud se aktivní AVG stane nedostupným.

`glbp` *group-member* `priority` *level*

Příklad:
`Router(config-if)# glbp 10 priority 150`

Převzetí aktivní role

Povolení nebo zákázání převzetí aktivní role směrovačem s vyšší prioritou se konfiguruje příkazem:

`glbp` *group-member* `forwarder preempt [delay minimum` *seconds*`]`

Příklad:
`Router(config-if)# glbp 1 forwarder preempt delay minimum 300`

Volitelný `delay minimum` definuje počet sekund, o které se směrovač zpozdí před převzetím role AVF. Rozsah hodnot je 0 až 3600s s výchozí hodnotou 30s.

Časovače

Úpravu intervalu *redirect*, během kterého bude AVG nadále přesměrovávat klienty na AVF, se provádí příkazem `glbp timers`. V počátečním nastavení je rovna 300s. Druhá hodnota *timeout* specifikuje počet sekund, po kterých se sekundární virtuální odesilatel stává neplatným. Ve výchozím stavu má hodnotu 14400s (4h).

`glbp` *group-member* `timers redirect` *redirect timeout*

Příklad:
`Router(config-if)# glbp 1 timers redirect 1800 28800`

Intervaly *hello-time* i *hold-time* mají stejný význam i výchozí hodnoty jako u protokolu HSRP, kapitola 3.3.2.

`glbp` *group-member* `timers [msec]` *hello-time* `[msec]` *hold-time*

Příklad:
`Router(config-if)# standby 1 timers 5 15`

Směrovače, na kterých nejsou hodnoty časovačů nakonfigurovány, se mohou dozvědět tyto hodnoty z aktivní virtuální brány. Časovače nastavené na AVG vždy potlačí všechna ostatní nastavení časovačů. Všechny směrovače ve skupině by měly používat stejné hodnoty intervalů.

Load Balancing metoda

Příkaz `glbp weighting` umožňuje výběr metody vyvažování zátěže, jejíž princip jsem vysvětlil v kapitole 2.5.2. Ve výchozím nastavení se využívá metoda `round-robin`.

`glbp` *group-member* `load-balancing [host-dependent | round-robin | weighted]`

Příklad:
`Router(config-if)# glbp 1 load-balancing host-dependent`

Pro metodu `weighted` je nutné nastavit počáteční hodnoty vah *maximum* jednotlivých rozhraní, tyto váhy následně určují poměr účasti rozhraní na síťovém provozu.

`glbp` *group-member* `weighting` *maximum* `[lower` *lower*`] [upper` *upper*`]`

Příklad:
`Router(config-if)# glbp 1 weighting 150`

Object tracking

Metoda vyvažování zátěže pomocí nastavených vah se často používá ve spojení s technologií sledování objektů.

Parametry *lower* i *upper* u příkazu `glbp weighting` jsou prahové hodnoty rozhraní, které mají smysl nastavovat pouze u dynamicky měnících se vah. V případě, kdy se sníží hodnota váhy rozhraní pod stanovenou mez *lower*, přesměrování se zakáže. V opačném případě, jestliže se hodnota zvýší nad horní mez *upper*, přesměrování bude opět povoleno.

Změnu váhy rozhraní, na základě sledovaného čísla objektu *object-number*, nastavíme příkazem:

`glbp group weighting track` *object-number* `[decrement` *value*`]`

Příklad:
`Router(config-if)# glbp 10 weighting track 2 decrement 5`

Parametr `decrement` snižuje hodnotu *value* brány, pokud sledovaný objekt *object-number* změní svůj stav.

3.4.3 Monitorování a verifikace

Správné nastavení parametrů protokolu můžeme ověřit příkazem `show glbp`

`show glbp [BVI | FastEthernet | Port-channel | all | brief | capability | delay | internal | redirect]`

nebo pomocí debugovacích informací `debug glbp`. Použití diagnostických příkazů by se mělo používat pouze při odstraňování potíží, protože objem získaných informací může mít za následek výrazné snížení výkonu.

Pro zobrazení debugovacích zpráv o podmínkách GLBP byl vytvořen následující příkaz:

```
debug condition glbp interface-type interface-number group
[forwarder]
```

Kde atributy *interface-type interface-number* identifikují rozhraní, pro něž bude poskytován výstup, *group* specifikuje skupinu směrovačů a `forwarder` je číslo v rozsahu 1 až 255 sloužící k identifikaci virtuální MAC adresy.

```
Router# show glbp
FastEthernet0/0 - Group 10
State is Active
2 state changes, last state change 23:50:33
Virtual IP address is 10.21.8.10
Hello time 5 sec, hold time 18 sec
Next hello sent in 4.300 secs
Redirect time 600 sec, forwarder time-out 7200 sec
Authentication MD5, key-string
Preemption enabled, min delay 60 sec
Active is local
Standby is unknown
Priority 254 (configured)
Weighting 105 (configured 110), thresholds: lower 95, upper 105
Track object 2 state Down decrement 5
Load balancing: host-dependent
There is 1 forwarder (1 active)
Forwarder 1
State is Active
1 state change, last state change 23:50:15
MAC address is 0007.b400.0101 (default)
Owner ID is 0005.0050.6c08
Redirection enabled
Preemption enabled, min delay 60 sec
Active is local, weighting 105
```

Kapitola 4

Simulační prostředí

V této kapitole je krátce představeno simulační prostředí OMNeT++, ve kterém je projekt vyvíjen. Dále představuji INET Framework, jenž přináší implementaci základních síťových zařízení a protokolů.

4.1 OMNeT++

OMNeT++ [7] je modulární, objektově orientovaný framework určený pro simulaci diskrétně-událostních sítí. Díky jeho flexibilní architektuře je vhodný pro řešení mnoha problémů od modelování protokolů, multiprocesorů až po distribuované či paralelní systémy.

Základním prvkem simulací v prostředí OMNeT++ je hierarchický systém modulů. Jedná se o uživatelem definové části simulace, které lze kombinovat. Komunikace mezi jednotlivými moduly probíhá zasíláním zpráv prostřednictvím bran. Ty jsou definovány jako rozhraní mezi modulem a zbytkem simulačního prostředí.

OMNeT++ je distribuován v otevřené podobě prostřednictvím zdrojových kódů, je proto platformě nezávislý a lze jej provozovat na různých operačních systémech. Aplikace je poskytována pro akademické a nekomerční využití zdarma. Verze pro komerční použití je šířena pod názvem OMNEST.

Velkou výhodou OMNetT++ je dostupnost celé řady volně dostupných frameworků, které rozšiřují jeho funkcionalitu.

4.2 INET

INET [6] je open source knihovna rozšiřující simulační nástroj OMNeT++. Svým zaměřením určen pro simulaci komunikace v datových sítích založených na různých technologiích od metalických, optických až po bezdrátová média.

Architektura INET frameworku vychází z OMNeT++, místo modulů zde vystupují síťová zařízení, jejich rozhraní a protokoly v nich implementovaných. Zpráva vzniká na nejvyšší vrstvě a postupně se zapouzdřuje dle modelu TCP/IP do nejnižší vrstvy, kde se na rozhraní odešle jinému zařízení.

Mezi implementované protokoly patří například UDP, TCP, SCTP, IP, IPv6, Ethernet, PPP, 802.11, MPLS, OSPF a další.

Kapitola 5

Návrh a implementace

V následující kapitole se věnuji návrhu a implementaci protokolu VRRP verze 2. Tento protokol jsem si zvolil kvůli jeho podpoře velkou škálou výrobců síťových zařízení.

5.1 Analýza OMNeT++ a INET

Před vlastní implementací protokolu VRRP bylo potřeba provést analýzu zdrojových kódů knihovny INET a zjistit jaké prostředky poskytuje pro implementaci.

Základem protokolu je virtuální síťová IP adresa a virtuální MAC adresa. Z teoretického rozboru VRRP víme, že na jednom rozhraní můžeme mít až 255 virtuálních směrovačů tzn. 255 virtuálních MAC adres. Toto je největší omezení INETu pro jakýkoliv FHRP. V třídě `EtherMacBase` je vytvořena jedna jediná MAC adresa a nad ní je definováno rozhraní specifikované třídou `InterfaceEntry`, která může obsahovat pouze jednu IP adresu (třída `IPv4Data` resp. `IPv6Data`).

VRRP používá pro aktualizaci tabulek přepínačů zprávy typu `ARP Gratuitous`. Tyto zprávy pak mohou být `Request` i `Reply`. Mají následující tvar:

```
Sender MAC address: 02:02:02:02:02:02 (02:02:02:02:02:02)
Sender IP address: 192.168.1.1 (192.168.1.1)
Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)
Target IP address: 192.168.1.1 (192.168.1.1)
```

Takto specifikované zprávy nelze prostřednictvím modulu `ARP` odeslat.

5.2 Implementace podpůrných technologií

V předcházející kapitole jsem popisoval nejkritičtější omezení, které brání v implementaci protokolů FHRP. V této kapitole se zaměřím na jejich řešení.

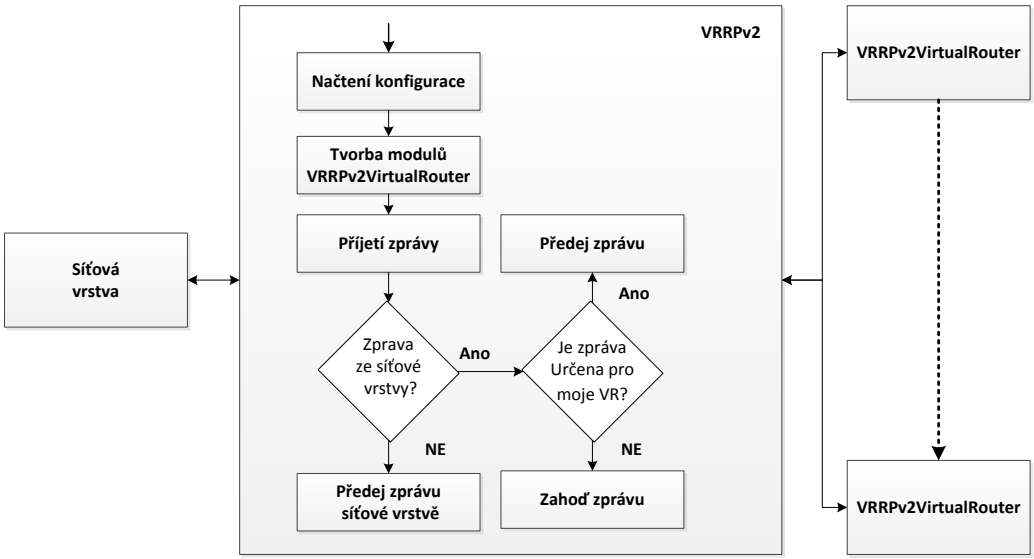
Pro řešení tzv. „Multiple MAC“ jsem vytvořil novou třídu `AnsaInterfaceEntry`, která je potomkem třídy `InterfaceEntry`. Tato nová třída rozšiřuje původní o metody pro práci s objekty `VirtualForwarder`, specifikované stejnojmenou třídou. `VirtualForwarder` je třída definující vektor `IPv4Address` pro vloženou adresu MAC. Síťové rozhraní je pak schopno odesílat i přijímat rámce obsahující jinou MAC adresu, než kterou má nastavenou na svém rozhraní. Tímto ale všechny problémy nekončí, bylo potřeba propagovat `VirtualForwarder` do modulů a s hodnotami v nich uložených pracovat. Konkrétně jsem upravovat třídy modulů: `IPv4` a `ARP`.

5.3 Návrh architektury

VRRP je protokol síťové vrstvy, navazuje na modul síťové vrstvy `Network Layer`. Modul `NetworkLayer` je nutné upravit tak, aby pakety označené protokolovým číslem 112 zasílal do modulu VRRPv2.

Protokol VRRP je komplikovaný z pohledu, že může obsahovat až 255 instancí virtuálního směrovače na jednom rozhraní. Každá instance má vlastní číslo skupiny a vlastní MAC a IP adresu. Vytvářet všech 255 virtuální směrovačů na rozhraních by bylo značně neefektivní. Z toho důvodu bylo potřeba navrhnout systém dynamického vytváření instancí virtuálního směrovače na základě konfigurace.

Pro činnost VRRP jsem navrhl dva moduly `VRRPv2` a `VRRPv2VirtualRouter`. Moduly jsou implementovány jako samotné třídy C++ a obsahují všechny potřebné metody pro správnou funkci protokolu. Obrázek zachycuje navrženou architekturu.



Obrázek 5.1: Návrh architektury modulů VRRPv2 a VRRPv2VirtualRouter

5.4 Modul VRRPv2

Modul VRRPv2 je hlavním prostředkem pro poskytnutí redundance protokolu VRRP. Primární úlohou je načítat konfigurační soubor (kapitola 5.7) a na základě jeho analýzy dynamicky vytváří virtuální směrovače (moduly `VRRPv2VirtualRouter`). Síťová vrstva (modul `Network Layer`) předává pakety adresované na port IP 112 do rozhraní tohoto modulu. Zde se provádí kontrola přijatého oznámení k příslušnosti virtuálního směrovače obsahující tento modul. Bude-li tato zpráva učena pro jim spravovaný virtuální směrovač, předá mu ji. V opačném případě zprávu zahazuje.

Modul VRRPv2 tedy slouží jako komunikační brána, která zprostředkovává komunikaci modulů `VRRPv2VirtualRouter` s modulem síťové vrstvy. Ohlášení odesílaná z virtuálních směrovačů bez žádné kontroly předává síťové vrstvě.

Výše popsaný postup je jediná činnost, kterou modul VRRP vykonává. Všechna ostatní logika je přesunuta do modulu `VRRPv2VirtualRouter`.

5.5 Modul VRRPv2VirtualRouter

Hlavní částí implementace protokolu VRRP je modul `VRRPv2VirtualRouter`. Ten si nejprve nastaví výchozí hodnoty virtuálního směrovače a poté je při čtení konfigurace upravuje dle uživatele. Následuje přihlášení rozhraní do multicastové skupiny a vytvoření virtuální MAC adresy.

V této fázi už je modul připraven a přechází do stavu `Initialize` a následně podle konfigurace do stavu `Backup` nebo `Master`.

5.5.1 Odesílání a přijímání zpráv

Při přijetí ohlášení je nutné provést několik typů kontrol. První z nich je kontrola hodnoty `TTL`. Ta musí být rovna 255, pokud obsahuje nižší hodnotu znamená to, že paket již prošel přes nějaký směrovač a je zahozen.

Kontrola příslušnosti paketu virtuálnímu směrovači byla již provedena v modulu `VRRPv2`. Ostatní kontroly hodnot typu autentizace, minimální velikost paketu a hodnoty checksum nebyly implementovány.

Před odesláním ohlášení `ADVERTISEMENT` modul musí nastavit IP hlavičku. Konkrétně se jedná o hodnotu cílové MAC adresy, zde je vložena hodnota virtuální MAC adresy. Dále je přidána zdrojová IP adresa jako primární IP adresa rozhraní a také port `112`. Celý paket je odesílán na multicastovu adresu VRRP.

5.6 Zprávy Advertisement

Definice zpráv se nachází v souboru `VRRPv2Advertisement.msg`. Definici zpráv jsem zachoval dle RFC 3768 i když jsou některá pole nevyužitá nebo mají nulovou hodnotu. Při překladu kódů se automaticky vygeneruje nový zdrojový soubor odpovídají definici zpráv. Soubor `VRRPv2Advertisement.msg` vypadá následovně:

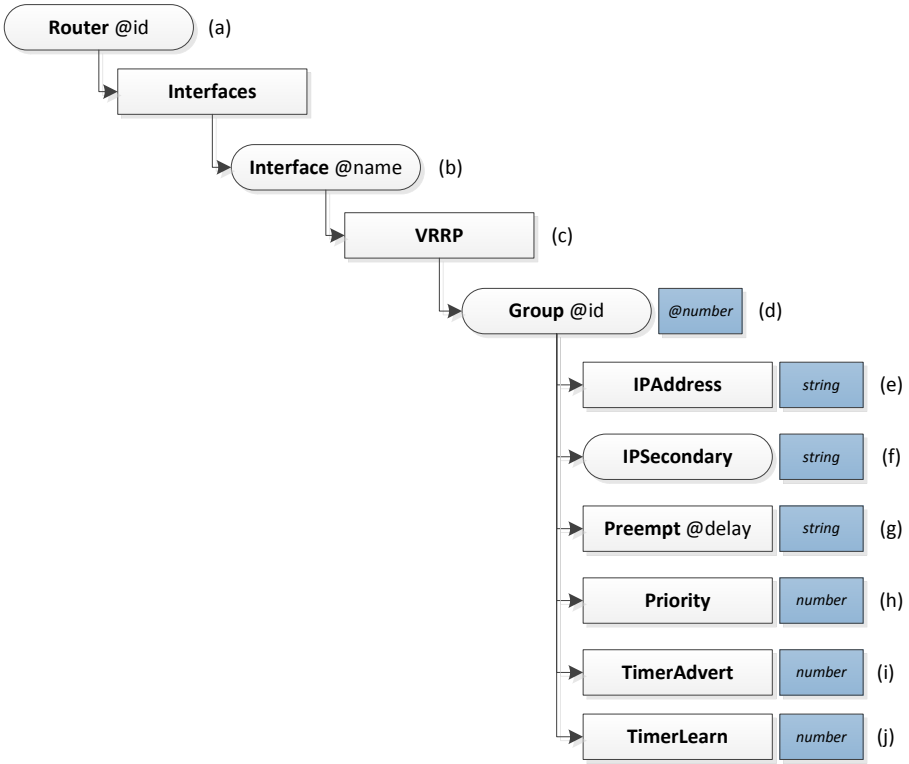
```
enum VRRP_TYPE
{
     VRRPADVERTISEMENT = 1;
}
packet VRRPv2Advertisement
{
     unsigned char version;
     unsigned char type = VRRPADVERTISEMENT;
     unsigned char vrid;
     unsigned char priority;
     unsigned char countIPAddrs;
     unsigned char authType;
     uint16_t checksum;
     unsigned char adverInt;
     IPv4Address addresses[];
}
```

Standard RFC 3768 [9] specifikuje položky `version` a `type` jako pole o velikosti 4 bity. Implementační jazyk C++ neobsahuje datový typ pro tuto velikost. Řešením by bylo vložení obou polí do jedné proměnné a pomocí bitových posuvů rozlišovat hodnoty. Tato implementace ale snižuje přehlednost a proto jsem se využil větší datový typ `unsigned char` (8 bitů). Použití větších datových typů, nijak neovlivní průběh simulace

5.7 Konfigurace

Konfigurační soubor je zapsán ve značkovacím jazyce XML. Tento formát se zpracovává prostřednictvím již vytvořeného modulu `DeviceConfigurator`, jehož autorem je Marek Černý. Modul jsem rozšířil o dvě metody `loadVRRPv2Config()` a `loadVRRPv2VirtualRouterConfig()`. První zmíněnou metodu používá modul `VRRP`, druhá slouží k definování parametrů virtuálních směrovačů.

Strukturu konfigurace popisuje obrázek 5.2.



Obrázek 5.2: Struktura konfigurace VRRP v XML

(a) Identifikace sekce směrovače pro který náleží konfigurace vložených elementů.

(b) Výběr rozhraní. Parametr `name` specifikuje název rozhraní.

(c) Konfigurace protokolu VRRP pro rozhraní `Interface@name` na směrovači `Router@id`.

(d) Definice instance Virtual Router s povinným parametrem ID identifikujícím příslušnost k virtuálnímu směrovači.

(e) Virtuální IP adresa, kterou uživatelé zadávají jako výchozí adresu brány.

(f) Sekundární IP adresy.

(g) Volitelný popis VR.

(h) Hodnota priority zařízení ve virtuálním směrovači.

(i) Povolení či zakázání preemce, volitelný parametr `@delay` umožňuje odložit převzetí aktivní funkce.

(j) Nastavení časovače Avertisement Timer, pro pravidelné odesílání ohlášení.

(k) Tento parametr umožňuje učení intervalu Advertisement.

V prvním fázi modul `VRRP` načítá konfigurační soubor, vyhledá v něm všechny elementy `<VRRP>` nastavených u rozhraní. Po kontrole minimální konfigurace `<Group>` dynamicky vytváří modul `VRRPv2VirtualRouter` jemuž předá identifikátor skupiny (parametr elementu `group`) a číslo rozhraní na kterém poběží (`InterfaceId`). Minimální konfigurací se rozumí identifikátor skupiny a virtuální IP adresa, bez těchto hodnot by nebylo možné správně vytvořit virtuální směrovač.

Virtual router při své inicializaci vyhledá pomocí XPath svoji konfiguraci na základě předaných parametrů. Poté hodnotami definovanými uživatelem upraví své výchozí hodnoty. Příklad konfiguračního souboru se nachází v příloze C.

Kapitola 6

Simulace

V této kapitole provádím porovnání chování simulace vůči reálné síti. Popisuji zde analýzu jednotlivých událostí, zaměřuji se především na změny stavů protokolu VRRP a na zprávy `ADVERTISEMENT`, které odesílá směrovač ve stavu Master.

Validace proběhla srovnáním síťové komunikace s relevantní topologií v simulátoru Cisco zařízení GNS3. Dále jsem pro analýzu zpráv využil software Wireshark. Pro snadnější verifikaci jsem na Cisco zařízeních povolil debugování protokolu VRPP viz kapitola 3.2.3.

6.1 Zotavení z výpadku

V této simulaci jsem se pokusil ověřit, zda správně funguje proces zotavení z výpadku výchozí brány a její následné obnovení činnosti. Byla navrhnuta topologie dle obrázku 6.1, kde pro lokální síť `192.168.10.0` představují směrovače `GW1` a `GW2` výchozí bránu pro komunikaci s ostatními sítěmi. Všem zařízením byly nastaveny znázorněné IP adresy. Celý konfigurační soubor XML lze nalézt v příloze C s ekvivalentním nastavením Cisco směrovačů příloze D.

Pro jednoduchost bylo použito statické směrovaní. `GW1` a `GW2` obsahují defaultní cestu na směrovač `ISP`, ten obsahuje cesty k síti `192.168.10.0` přes `GW1` i `GW2`.

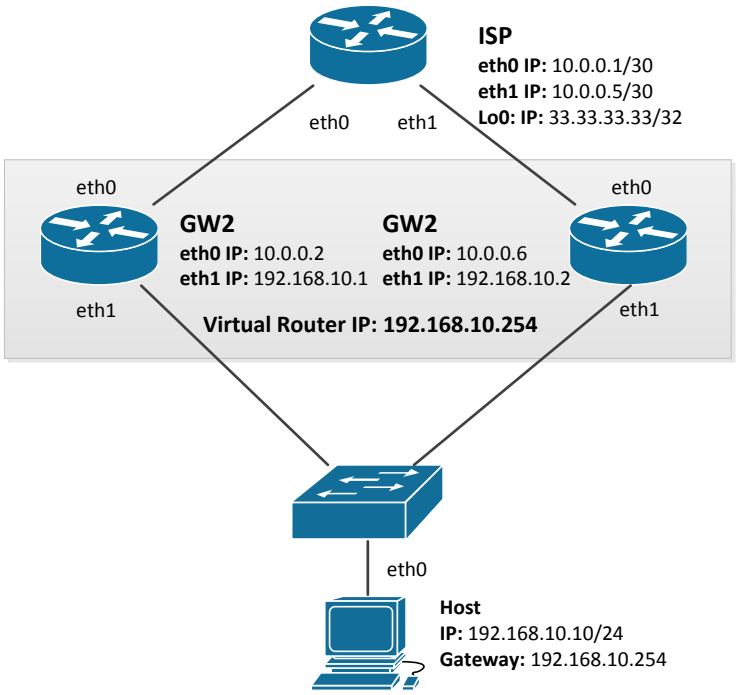
6.1.1 Analýza událostí

Volba směrovače Master

V prvním kroku začíná proces inicializace zařízení, které načítají konfigurační soubor XML, nastavení parametrů zařízení a síťových rozhraní. Jakmile jsou zařízení připravena začíná volba nového směrovače Master:

- Virtuální IP adresu nemá žádný směrovač ve skupině 10 nastavenu na svém rozhraní a z tohoto důvodu oba přechází do stavu Backup. Výstup zpráv modulů:

```
GW1(vrrp-configuration)# IPAddress:192.168.10.254 IPSecondary:{}
Priority:100 Preempt:Y TimerAdvertise:1 TimerLearn:-
GW1# %VRRP-6-STATECHANGE: eth1 Grp10 state Init -> Backup
GW2(vrrp-configuration)# IPAddress:192.168.10.254 IPSecondary:{}
Priority:100 Preempt:Y TimerAdvertise:1 TimerLearn:-
GW2# %VRRP-6-STATECHANGE: eth1 Grp10 state Init -> Backup
```



Obrázek 6.1: Testovaná topologie

- Směrovačům vyprší intervaly Master Down a téměř současně přechází do stavu Master. Oba odesílají `ADVERTISEMENT` na multicastovou adresu `224.0.0.18` a následně `ARP Gratuitous`.

```
** Event #21 T=3.609375 Network.GW1.vrrp.VR_102_10 (VRRPv2VirtualRouter,
id=81), on selfmsg 'MasterDownTimer' (cMessage, id=61)
GW1# Grp 10 sending Advertisement checksum 0xaf4c
GW1# %VRRP-6-STATECHANGE: eth1 Grp10 state Backup -> Master
** Event #22 T=3.609375 Network.GW2.vrrp.VR_102_10 (VRRPv2VirtualRouter,
id=82), on selfmsg 'MasterDownTimer' (cMessage, id=63)
GW2# Grp 10 sending Advertisement checksum 0xaf4c
GW2# %VRRP-6-STATECHANGE: eth1 Grp10 state Backup -> Master
```

- `GW1` i `GW2` navzájem obdrží své ohlášení `ADVERTISEMENT`. Porovnávají lokální priority s hodnotou obdrženou ve zprávě. Na základě priorit se nepodařil určit, kdo má být Master a přichází na řadu porovnávání IP adres. Zde má nižší IP adresu `GW1` tzn. přechází do stavu Backup. `GW2` zůstává jako Master a v intervalu Advertisement odesílá pravidelná ohlášení

- V čase 3.609375s od inicializace protokolu jsou směrovače ve svých rolích

```
** Event #88 T=3.609388539998 Network.GW2.vrrp.VR_102_10
(VRRPv2VirtualRouter, id=82)
GW2# Grp 10 Advertisement priority 100, ipaddr 192.168.10.254
** Event #89 T=3.609388539998 Network.GW1.vrrp.VR_102_10
(VRRPv2VirtualRouter, id=81)
GW1# Grp 10 Advertisement priority 100, ipaddr 192.168.10.254
GW1# Grp 10 Event - Advert higher or equal priority
GW1# %VRRP-6-STATECHANGE: eth1 Grp10 state Master -> Backup
```

Pro porovnání uvádím výpis příkazu `debug event` na zařízeních `GW1` a `GW2`

```
GW1#
Mar 1 07:21.683: VRRP: Grp 10 Event - Interface UP
Mar 1 07:21.683: %VRRP-6-STATECHANGE: Fa1/0 Grp 10 state Init -> Backup
Mar 1 07:25.295: VRRP: Grp 10 Event - Master down timer expired
Mar 1 07:25.295: %VRRP-6-STATECHANGE: Fa1/0 Grp 10 state Backup -> Master
Mar 1 07:26.659: %VRRP-6-STATECHANGE: Fa1/0 Grp 10 state Master -> Backup

GW2#
Mar 1 07:21.183: VRRP: Grp 10 Event - Interface UP
Mar 1 07:21.187: %VRRP-6-STATECHANGE: Fa1/0 Grp 10 state Init -> Backup
Mar 1 07:24.799: VRRP: Grp 10 Event - Master down timer expired
Mar 1 07:24.799: %VRRP-6-STATECHANGE: Fa1/0 Grp 10 state Backup -> Master
```

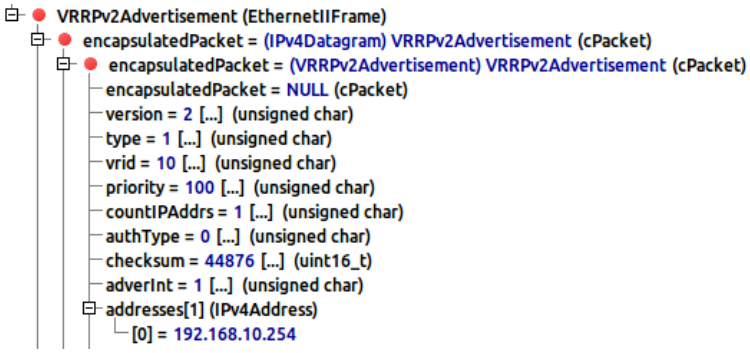
Paket `ADVERTISEMENT` zachycený nástrojem Wireshark:

```
Frame 26: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: IETF-VRRP-VRID_0a (00:00:5e:00:01:0a), Dst:
IPv4mcast_00:00:12 (01:00:5e:00:00:12)
Internet Protocol Version 4, Src: 192.168.10.2 (192.168.10.2), Dst:
224.0.0.18 (224.0.0.18)
Virtual Router Redundancy Protocol
Version 2, Packet type 1 (Advertisement)
0010 .... = VRRP protocol version: 2
.... 0001 = VRRP packet type: Advertisement (1)
Virtual Rtr ID: 10
Priority: 100 (Default priority for a backup VRRP router)
Addr Count: 1
Auth Type: No Authentication (0)
Adver Int: 1
Checksum: 0xaf4c [correct]
IP Address: 192.168.10.254 (192.168.10.254)
```

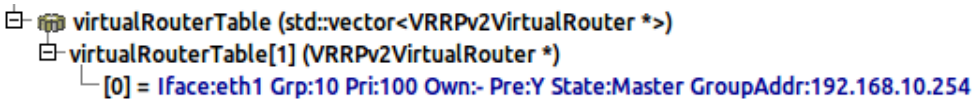
Paket `ADVERTISEMENT` ze simulace:

Komunikace s výchozí bránou

V čase t=5 už mají směrovače definovány své role. klient Host vysílá ping na adresu výchozí brány `192.168.10.254`. Obrázek 6.3 zachycuje stav VRRP na směrovači `GW2`.

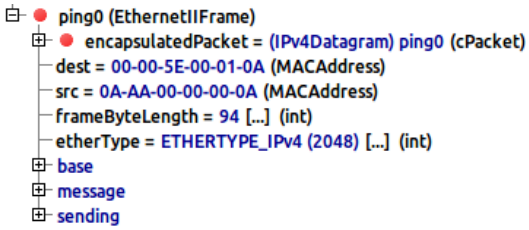


Obrázek 6.2: Advertisement paket



Obrázek 6.3: Grafické znázornění informace VRRP.

- Host ve své ARP tabulce nemá záznam pro zařízení `192.168.10.254` proto nejprve odesílá `ARP Request`, který je adresován jako broadcast, aby zjistil MAC adresu cíle.
- Dotaz dorazí oběma směrovačům `GW1` i `GW2`, avšak odpovídá pouze `GW2` zprávou `ARP Reply` s virtuální MAC adresou (obrázek 6.4)
- Nyní už obě zařízení znají vzájemné MAC adresy a komunikace začíná.

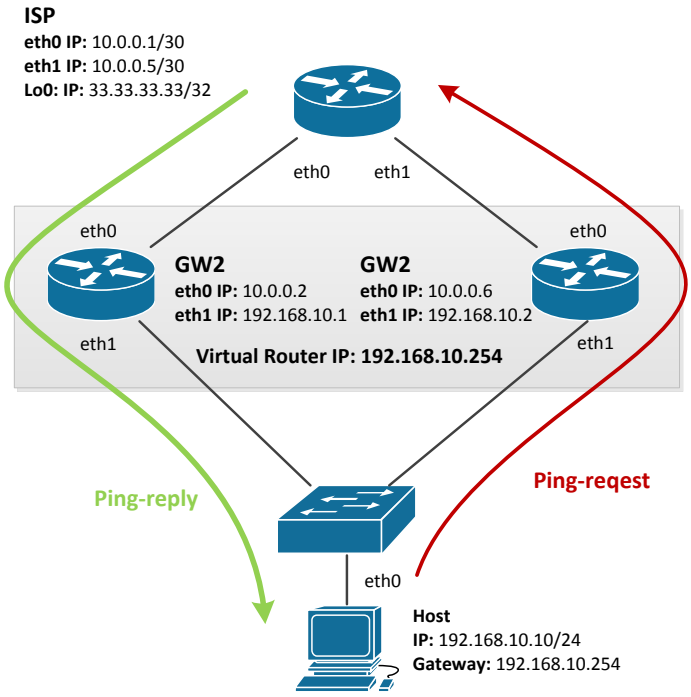


Obrázek 6.4: Ping paket na výchozí bránu

Komunikace mimo lokální síť

V čase t=15 `Host` provádí `ping` mimo lokální sít na IP adresu `33.33.33.33`, kterou obsahuje směrovače `ISP` na svém rozhraní Loopback0. Ve výchozím nastavení mají směrovače povolenou techniku Proxy ARP (kapitola 2.2) proto ji nechávám povolenou i na směrovačích v OMNeT++.

- Adresa `33.33.33.33` není adresou lokální sítě, `Host` tudíž bude odesílat zprávy na adresu přes výchozí bránu. ARP záznam pro výchozí bránu již zná z předchozí komunikace.
- `GW2` obsahuje statický směrovací záznam na `ISP`, díky němu vybírá cestu pro adresu `33.33.33.33` ze směrovací tabulky.



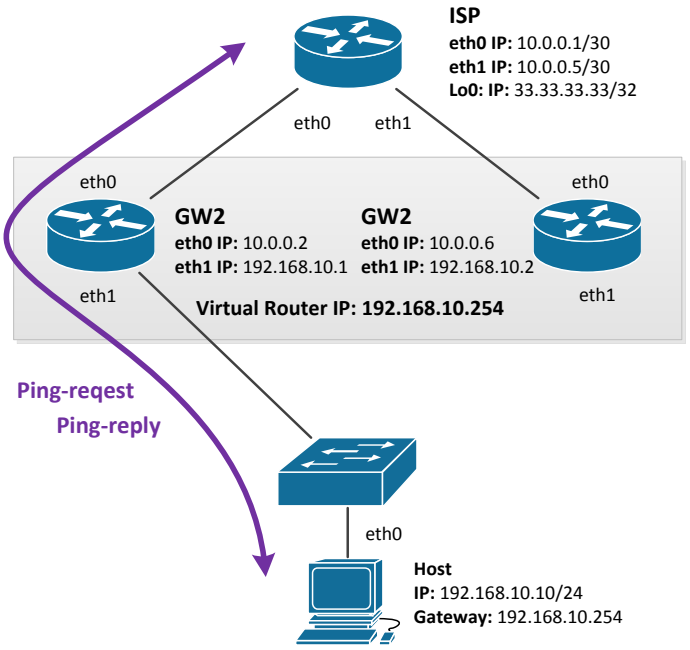
Obrázek 6.5: Testovaná topologie - Komunikace mimo lokální síť

- Směrovač `ISP` pro odpověď vybírá první záznam pro síť `192.168.10.0` ze směrovací tabulky. Ten odkazuje na směrovač `GW1` a na který odesílá odpověď. `GW1` předává zprávu zařízení `Host`.
- Paket `ping0-request` probíhá od zařízení `Host` ke směrovači `ISP` přes výchozí bránu `GW2` a odpověd `ping0-reply` prochází přes směrovač `GW1`.

Zotavení z výpadku

OMNeT++ neposkytuje metody ekvivalentní vypnutí rozhraní nebo rovnou celého směrovače. Z toho důvodu bude výpadek představovat odpojení kabelu mezi směrovačem `GW2` a přepínačem `SW`.

- `Host` komunikuje prostřednictvím `ping-request` respektive `ping-reply` se směrovačem `ISP`.
- V čase t = 20 dochází k výpadku `GW2`.
- `GW1` přestává dostávat pravidelná ohlášení, nedochází tudíž k restartování časovače Master Down.
- `Host` stále odesílá zprávy na zprávy ale do vypršení intervalu Master Down nedostává odpovědi.



Obrázek 6.6: Testovaná topologie - Zotavení z výpadku

```
** Event #1427 T=23.218777079996 Network.GW1.vrrp.VR_102_10
(VRRPv2VirtualRouter, id=82), on selfmsg 'MasterDownTimer' (cMessage,
id=709)
GW1# Grp 10 sending Advertisement checksum 0xaf4c
GW1# %VRRP-6-STATECHANGE: eth1 Grp10 state Backup -> Master
```

- V čase T=23.218s `GW1` zaregistruje výpadek `GW2`. Odesílá první `ADVERTISEMENT` i `ARP Gratuitous` a přechází do stavu Master.
- Switch začíná přeposílat pakety vedoucí k `ISP` na port, kde je připojený `GW1`. Ten přijímá zprávy ale v současné době nemá odpovídající ARP záznamy a zahájí proces jejichž získávaní.
- Komunikace je plně obnovena v čase t=24s

Zotavení z výpadku

Zatímco byl směrovače `GW2` odpojen od lokální sítě, jeho rozhraní `eth1` zůstává ve stavu Master. Po jeho opětovném připojení, pokračuje v odesílání svých ohlášení a dochází k činnosti jako při aktivaci protokolu VRRP (kapitola 6.1.1) tedy volba směrovače Master. Komunikace je tedy opět směrována přes zařízení `GW2`.

Kapitola 7

Závěr

Tato práce se zabývala problematikou současných protokolů redundance výchozí brány. Krátce jsem představil simulační nástroj OMNeT++ a knihovnou INET. Cílem práce bylo rozšířit knihovnu INET o protokol redundance brány. Ač jsou si protokoly VRRP a HSRP velmi podobné, tak jsem si jako implementační protokol vybral VRRP kvůli jeho specifikaci v RFC a také pro jeho podporu napříč různými výrobci. Navržené rozšíření bylo implementováno a jeho odpovídající korektnost byla porovnána s reálnou sítí.

Informace o principech redundance jsem čerpal především ze specifikací RFC a pro Cisco protokoly z materiálů dostupných na webu společnosti Cisco. Ačkoliv jsou specifikace RFC velmi dobře popsány, ne vždy poskytovaly odpovědi na mé otázky. Proto se zde vyplatilo ochytávání komunikace zařízení nástrojem Wireshark a výpisy ladících informací jednotlivých protokolů. Praktické chování protokolů jsem zkoumal jak ve školní laboratoři, tak i v simulátoru GNS3. Konfigurace reálných zařízení mi byla inspirací při navrhování odpovídající XML konfigurace.

Navržený modul VRRP lze použít přo vytváření simulací počítačových sítí nad protokolem IPv4. Díky podpoře scénářů lze analyzovat v čase detekce výpadků zařízení a přebírání funkcí nedostupných směrovačů.

Další vývoj spatřuji v protokolu VRRP verze 3. Oba protokoly VRRPv2 i VRRPv3 mají identickou IPv4 část. VRRP ve třetí verzi navíc přidává podporu funkcionality IPv6 sítí. S implementací třetí verze do prostředí OMNeT++ souvisí ale úprava knihovny INET, konkrétně modulů obsažených v síťové vrstvě NetworkLayer6. Možnosti dalšího rozšiřování je celá řada, ať už HSRP nebo protokol GLBP jehož funkcionalita značně převyšuje jak VRRP tak i HSRP.

Tato práce mi umožnila nabýt znalosti FHRP protokolů, se kterými jsem se doposud nesetkal. Rozšířil jsem si povědomí o ostatních aspektech spolehlivosti v počítačových sítích. Podrobně jsem se seznámil s prostředím OMNeT++, což mi umožnilo doplnit své dovednosti v oblasti modelování a simulace.

Literatura

[1] Configuring VRRP. http://www.cisco.com/en/US/docs/ios-xml/ipapp_fhrp/configuration/12-4/fhpvrrp.html, [cit. 2013-05-20].

[2] Gateway Load Balancing Protocol. http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_glbp2.html, [cit. 2013-05-20].

[3] Gateway Load Balancing Protocol Overview. http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6550/prod_presentation0900aecd801790a3_ps6600_Products_Presentation.html, [cit. 2013-05-20].

[4] Hot Standby Router Protocol Features and Functionality. http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml, [cit. 2013-05-20].

[5] Hot Standby Router Protocol (HSRP): Frequently Asked Questions. http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800a9679.shtml, [cit. 2013-05-20].

[6] INET Framework for OMNeT++. http://inet.omnetpp.org/doc/INET/inet-manual-draft.pdf, [cit. 2013-05-20].

[7] A. Varga: *aj.: OMNeT++ User Manual. OpenSim Ltd.* 2010.

[8] B. Cole, P. Morton, D. Li: Cisco Hot Standby Router Protocol (HSRP). RFC 2281. http://tools.ietf.org/html/rfc2281, Březen 2010 [cit. 2013-05-20].

[9] R. Hinden: Virtual Router Redundancy Protocol (VRRP). RFC 3768. http://www.ietf.org/rfc/rfc5798.txt, Duben 2004 [cit. 2013-05-20].

[10] S. Carl-Mitchell, J. S. Quarterman: Using ARP to Implement Transparent Subnet Gateway. RFC 1027. http://www.ietf.org/rfc/rfc1027.txt, Říjen 1987 [cit. 2013-05-20].

[11] S. Nadas, Ed. Ericsson: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. RFC 5798. http://www.ietf.org/rfc/rfc5798.txt, Březen 2010 [cit. 2013-05-20].

Příloha A

Seznam zkratek

ARP	Address Resolution Protocol
AVF	Active Virtual Forwarder
AVG	Active Virtual Gateway
CGMP	Cisco Group Management Protocol
GLBP	Gateway Load Balancing Protocol
HSRP	Hot Standby Routing Protocol
IANA	Internet Assigned Numbers Authority
IP	Internet Protocol
MAC	Media Access Control
MD5	Message-Digest algorithm
NAT	Network Address Translation
PVF	Primary Virtual Forwarder
SVF	Secondary Virtual Forwarder
TLV	Type length value
TTL	Time to live
UDP	User Datagram Protocol
VF	Virtual Forwarder
VG	Virtual Gateway
VRID	Virtual Router ID
VRRP	Virtual Router Redundancy Protocol
XML	Extensible Markup Language

Příloha B

Obsah CD

/ansa/src/ansa/vrrpv2/*	Zdrojové kódy
/ansa/examples/ansa/vrrpv2/*	Simulační scénáře a konfigurační soubory
/tex	Zdrojové soubory této práce
/vsp	Zdrojové soubory obrázků a diagramů
/projekt.pdf	PDF verze práce
/readme.txt	Obsah DVD

Příloha C

Konfigurační soubor XML

```
<Devices>
     <Router id="33.33.33.33">
          <Interfaces>
               <Interface name="lo0">
                    <IPAddress>33.33.33.33</IPAddress>
                    <Mask>255.255.255.255</Mask>
               </Interface>
               <Interface name="eth0">
                    <IPAddress>10.0.0.1</IPAddress>
                    <Mask>255.255.255.252</Mask>
               </Interface>
               <Interface name="eth1">
                    <IPAddress>10.0.0.5</IPAddress>
                    <Mask>255.255.255.252</Mask>
               </Interface>
          </Interfaces>
               <Routing>
                    <Static>
                         <Route>
                              <NetworkAddress>192.168.10.0</NetworkAddress>
                              <NetworkMask>255.255.255.0</NetworkMask>
                              <NextHopAddress>10.0.0.2</NextHopAddress>
                         </Route>
                         <Route>
                              <NetworkAddress>192.168.10.0</NetworkAddress>
                              <NetworkMask>255.255.255.0</NetworkMask>
                              <NextHopAddress>10.0.0.6</NextHopAddress>
                         </Route>
                    </Static>
               </Routing>
     </Router>
```

```
<Router id="192.168.10.1">
     <Interfaces>
          <Interface name="eth0">
               <IPAddress>10.0.0.2</IPAddress>
               <Mask>255.255.255.252</Mask>
          </Interface>
          <Interface name="eth1">
               <IPAddress>192.168.10.1</IPAddress>
               <Mask>255.255.255.0</Mask>
               <VRRP>
                    <Group id="10">
                         <IPAddress>192.168.10.254</IPAddress>
                    </Group>
               </VRRP>
          </Interface>
     </Interfaces>
     <Routing>
          <Static>
               <Route>
                    <NetworkAddress>33.33.33.33</NetworkAddress>
                    <NetworkMask>255.255.255.255</NetworkMask>
                    <NextHopAddress>10.0.0.1</NextHopAddress>
               </Route>
          </Static>
     </Routing>
</Router>


<Router id="192.168.10.2">
     <Interfaces>
          <Interface name="eth0">
               <IPAddress>10.0.0.6</IPAddress>
               <Mask>255.255.255.252</Mask>
          </Interface>
          <Interface name="eth1">
               <IPAddress>192.168.10.2</IPAddress>
               <Mask>255.255.255.0</Mask>
               <VRRP>
                    <Group id="10">
                         <IPAddress>192.168.10.254</IPAddress>
                    </Group>
               </VRRP>
          </Interface>
     </Interfaces>
     <Routing>
          <Static>
               <Route>
```

```
                    <NetworkAddress>33.33.33.33</NetworkAddress>
                    <NetworkMask>255.255.255.255</NetworkMask>
                    <NextHopAddress>10.0.0.5</NextHopAddress>
                </Route>
            </Static>
        </Routing>
    </Router>


    <Host id="192.168.10.10">
        <Interfaces>
            <Interface name="eth0">
                <IPAddress>192.168.10.10</IPAddress>
                <Mask>255.255.255.0</Mask>
            </Interface>
        </Interfaces>
        <DefaultRouter>192.168.10.254</DefaultRouter>
    </Host>
</Devices>
```

Příloha D

Konfigurace zařízení Cisco

```
GW1#show running-config | section interface
interface FastEthernet0/0
     ip address 10.0.0.2 255.255.255.252
     duplex auto
     speed auto
interface FastEthernet1/0
     ip address 192.168.10.1 255.255.255.0
     duplex auto
     speed auto
     vrrp 10 ip 192.168.10.254


GW1#show running-config | section ip route
ip route 33.33.33.33 255.255.255.255 10.0.0.1
```

```
GW2#show running-config | section interface
interface FastEthernet0/0
     ip address 10.0.0.6 255.255.255.252
     duplex auto
     speed auto
interface FastEthernet1/0
     ip address 192.168.10.1 255.255.255.0
     duplex auto
     speed auto
     vrrp 10 ip 192.168.10.254


GW1#show running-config | section ip route
ip route 33.33.33.33 255.255.255.255 10.0.0.5
```

```
ISP#show running-config | sect interface
interface Loopback0
     ip address 33.33.33.33 255.255.255.255
interface FastEthernet0/0
     ip address 10.0.0.1 255.255.255.252
     duplex auto
     speed auto
interface FastEthernet1/0
     ip address 10.0.0.5 255.255.255.252
     duplex auto
     speed auto
ISP#show running-config | sect ip route
ip route 192.168.10.0 255.255.255.0 10.0.0.2
ip route 192.168.10.0 255.255.255.0 10.0.0.6
```