České vysoké učení technické v Praze

Fakulta elektrotechnická

Moderní technologie Internetu

Hot Standby Router Protocol
(zajištění vysoké spolehlivosti výchozí brány)

Petr Milanov

listopad 2007

Zajištění vysoké spolehlivosti výchozí brány

1. Úvod

Jedním z požadavků zajištění vysoce spolehlivé síťové infrastruktury je eliminace výpadku výchozí brány (default gateway). Ve většině (menších a středně velkých) sítí je nasazena pouze jediná výchozí brána a její výpadek tudíž znemožní schopnost komunikace s okolními sítěmi (s okolním světem). Odstranění tohoto problému spočívá v nasazení více redundantních bran. V případě výpadku primární brány může její úkoly převzít brána záložní. Z důvodu efektivního využití síťové infrastruktury může být, za normálních podmínek (tj. „v bezporuchovém stavu“), uplatněn tzv. load-balancing, tedy vyvažovaní či distribuce zátěže mezi všechny nasazené brány.

Pro zajištění redundance výchozí brány se může použít například protokol Hot Standby Router Protocol (HSRP), což je proprietární protokol společnosti Cisco Systems (resp. se jedná o protokol původně vyvinutý společností Cisco Systems, který je v současné době již popsán v RFC 2281), nebo Virtual Router Redundancy Protocol (VRRP), který je definován konsorciem IEEE (Institute of Electrical and Electronics Engineers), konkrétně je popsán v RFC 2338 a 3768. Pro zajištění redundance s vyvažováním zátěže (load-balancing) lze využít protokolu Gateway Load Balancing Protocol (GLBP), což je opět proprietární protokol společnosti Cisco Systems.

2. Průběh komunikace v síťovém prostředí založeném na protokolu IP a technologii Ethernet

V dnešní době jsou pro komunikaci nejčastěji používány protokoly rodiny TCP/IP. Přitom nejčastější technologií lokální sítě je Ethernet. Pro adresaci stanic v prostředí TCP/IP se používají IP adresy. Pro adresaci v rámci Ethernetu to jsou MAC adresy. Aby mohla koncová stanice komunikovat s jinou, musí znát její IP adresu. Rovněž, v prostředí Ethernetu, musí znát i MAC adresu stanice, se kterou bude komunikovat – touto stanicí může být buď přímo ona stanice koncová, nebo ji může být výchozí brána, přes kterou bude vlastní komunikace probíhat. První případ, tedy přímá komunikace s koncovou stanicí i v rámci Ethernetového segmentu (z hlediska OSI modelu se jedná o komunikaci na druhé, linkové vrstvě) nastává tehdy, když jsou obě stanice připojeny do stejné sítě (či podsítě, z hlediska IP protokolu). Druhý případ pak nastává tehdy, když jsou obě stanice v sítích různých.

Skutečnost, zda obě stanice leží ve stejné síti určí stanice iniciující komunikaci z konfiguraci svého síťového rozhraní (pomocí své IP adresy a masky) a IP adresy stanice cílové. Pro automatické zjištění odpovídající MAC adresy se využívá protokolu ARP (Address Resolution Protocol). Stanice, která potřebuje zjistit MAC adresu k dané IP adrese, pošle všem ostatním stanicím na svém (lokálním) Ethernet segmentu zprávu zvanou ARP request (jedná se o broadcast), ve které uvede onu IP adresu stanice, se kterou chce komunikovat. Stanice s IP adresou uvedenou s ARP request odpoví pomocí zprávy ARP reply. Přišlou odpověď (tj. MAC adresu protější stanice získanou ze zprávy ARP reply) si žádající stanice uloží do své lokální keše pro pozdější, opakované, použití při vlastní komunikaci.

Jak již bylo výše zmíněno, každá komunikace mezi dvěma stanicemi nacházejícími se v různých sítích tedy probíhá přes výchozí bránu (router neboli směrovač). Tato brána je proto kritickým bodem propojujícím obě komunikující strany. Při jejím výpadku je ztracena veškerá možnost komunikace s jakoukoli stanici nacházející se mimo lokální síť. Pro zajištění spolehlivé síťové infrastruktury je proto nutné do sítě nasadit více výchozích bran, které budou schopny, při výpadku jedné (nebo více) z nich, se vzájemně zastoupit. Zotavení z výpadku musí být dostatečně rychlé, aby spojení navázaná síťovými protokoly nebyla ztracena a tím pádem nasazené služby či uživatelé tuto síť využívající výpadek vůbec nezaznamenali, popřípadě aby negativní důsledky tohoto výpadku byly co možná nejvíce minimalizovány.

2.1 Statická konfigurace výchozí brány

V mnoha případech je výchozí brána v konfiguraci síťového rozhraní koncové stanice nastavena staticky. Z tohoto důvodu, i za předpokladu nasazení více výchozích bran na jednom segmentu sítě, neexistuje, bez nasazení dalších specializovaných služeb, žádná možnost automatického zotavení se z výpadku této výchozí brány. Koncová stanice se statickou konfigurací neví o dalších, alternativních branách, které by mohla používat a proto ztratí možnost komunikovat s „okolním světem“.

Obdobné platí i pro konfiguraci dynamicky přiřazenou prostřednictvím DHCP serveru. Dále lze, v některých případech, na koncové stanici nakonfigurovat (ať už staticky, či přiřadit pomocí DHCP) více bran (například dvě), což přináší o něco větší míru spolehlivosti (dostupnosti). Ovšem toto řešení není příliš vhodné a svém důsledku tento problém ani neřeší (není z hlediska komunikace transparentní, je špatně škálovatelné a zotavení se z výpadku může trvat neúnosně dlouho).

2.2 Proxy ARP (RFC 1027)

Jednou z možností, jak dovolit koncové stanici komunikovat s ostatními stanicemi nacházejícími se vně její lokální síť, je tzv. proxy ARP (zástupné ARP). Proxy ARP je služba, která může být spuštěna na stanici mající přístup jak do lokální sítě, tak i do sítí dalších. Touto stanicí je typicky hraniční směrovač (router) a díky této službě plní funkci výchozí brány. Konfigurace stanic poté nemusí (neobsahuje) informaci o výchozí bráně. Způsob navazování komunikace se stanicí vně lokální síť pak probíhá následovně. Stanice iniciující komunikaci pošle ARP request, kterým chce zjistit MAC adresu k IP adrese cílové stanice. ARP request je vyslán jako broadcast, proto ho „vidí“ všechny stanice zapojené do daného segmentu, tj. vidí ho i stanice se zapnutou službou proxy ARP. Toto stanice se „podívá“ na IP adresu uvedenou v ARP requestu a zjistí, že se tato hledaná stanice nachází mimo lokální síť. Proto na tento ARP request odpoví svou vlastní MAC adresou (tj. pošle ARP response, ve kterém uvede, že její MAC adresa náleží k IP adrese uvedené v ARP requestu). Stanice, která poslala ARP request obdrží tuto odpověď a uvedenou MAC adresu si uloží do své lokální keše pro další použití při komunikaci. Tato stanice tedy vůbec nezjistí, že nekomunikuje přímo s cílovou stanicí a že ve skutečnosti jde veškerá komunikace přes stanici zástupnou, na které běží služba proxy ARP a která veškeré takto přijaté pakety (rámce) přeposílá dále k jejich skutečnému cíli.

Výhodou této metody je, že stanice může komunikovat se stanicemi vně její lokální segment i bez znalosti výchozí brány. Při případě, že stanice plnící funkci výchozí brány (stanice se spuštěnou službou proxy ARP) vypadne a že v daném segmentu je stanic se spuštěným proxy ARP více, může roli výchozí brány převzít stanice jiná. Z hlediska koncových stanic se toto děje téměř transparentně. Jediné, co koncová stanice zjistí je změna mapování MAC adresy k IP adrese, se kterou komunikuje. Toto mapování je však automatizováno prostřednictvím protokolu ARP.

Velkou nevýhodou je ale určitá doba, potřebná k tomu, aby vypršela platnost původní používané MAC adresy (tj. MAC adresy stanice, které vypadla z provozu). Po vypršení této doby je vždy vyslán nový ARP request pro obnovení mapování IP-MAC. Na tento nový dotaz již může odpovědět jiná výchozí brána (stanice provozující proxy ARP) a komunikace s vnějším světem je obnovena. Tato doba však může být poměrně dlouhá, takže může dojít ke ztrátě například navázaných TCP relací (typicky k této ztrátě dojde). Z hlediska real-time aplikací (tj. aplikací náročných na zpoždění a variabilitu zpoždění), jako je IP telefonie, je tato doba nutná k obnově komunikace nemyslitelně dlouhá.

3. Protokol HSRP (Hot Standby Router Protocol)

Protokol HSRP slouží k zajištění téměř okamžitého zotavení se z výpadku výchozí brány (někdy nazývané také jako first-hop k cíli). Toto zotavení se z výpadku je navíc zcela transparentní pro koncové, komunikující stanice. Protokol HSRP byl původně vyvinut společností Cisco Systems (tj. byl jejím proprietární protokolem), ale v současnosti však již je popsán v RFC 2281.

Protokol HSRP definuje tzv. standby skupinu směrovačů, ve které je jeden směrovač aktivní a plní roli výchozí brány. HSRP zajišťuje redundanci výchozí brány sdílením stejné IP a MAC adresy mezi všemi členy standby skupiny (tj. všechny redundantní brány „mají“ stejnou IP a MAC adresu). Tato adresa je nazývána jako virtuální. HSRP definuje tyto tři základní pojmy:

- Active router – směrovač, který se aktuálně (aktivně) účastní přenosu dat mezi dvěma komunikujícími stanicemi
- Standby router – primární záložní směrovač, který v případě výpadku převezme úkoly Active routeru
- Standby group – skupina všech směrovačů, na kterých běží HSRP a které společně emulují jeden virtuální směrovač (sekundární záložní směrovače)

V rámci každé HSRP skupiny (Standby group) existují následující entity:

- Jeden active router
- Jeden standby router
- Jeden virtual router
- Zbylé routery (směrovače)

Každý směrovač v HSRP group má svou roli a provádí specifickou činnost. HSRP active a standby směrovače posílají tzv. hello zprávy na multicast adresu 224.0.0.2, UDP port 1985.

3.1 Virtual router

Pod pojmem virtual router se myslí pouze IP a MAC adresa, která je sdílena mezi členy stejné HSRP skupiny a vystupuje jakožto „řádná IP a MAC adresa” výchozí brány (default gateway). Active router je zodpovědný za zpracování (směrování) rámců (paketů) zaslaných na MAC (IP) adresu virtual routeru.

3.2 Active Router

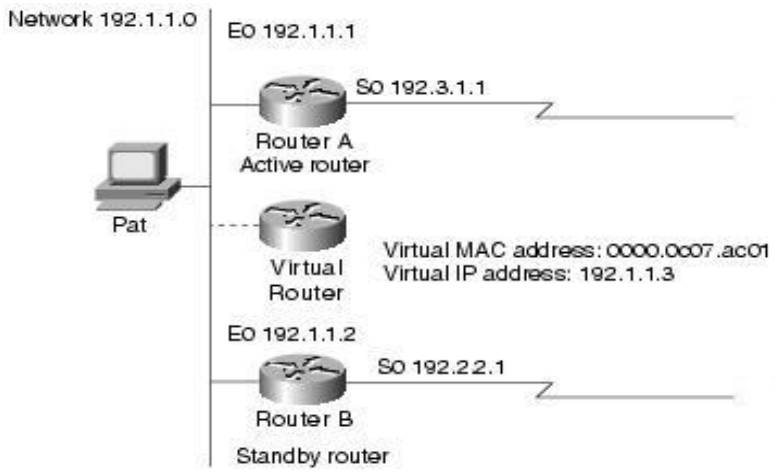
V rámci jedné HSRP skupiny je zvolen jeden směrovač jako aktivní (active router). Aktivní směrovač zajišťuje zpracování rámců zaslaných na MAC adresu virtual routeru. Tj. pokud koncová stanice zašle nějaké rámce přímo na MAC adresu virtuálního směrovače, aktivní směrovač tyto rámce přijme a dále zpracuje. Pokud koncová stanice pošle ARP dotaz na MAC adresu výchozí brány (tj. vlastně žádost o překlad IP adresy virtuálního směrovače na MAC adresu tohoto směrovače), zodpoví tento dotaz opět aktivní router.

3.3 ARP rezoluce při nasazení HSRP

IP adresa a její korespondující MAC adresa virtuálního směrovače jsou uloženy (spravovány) v ARP tabulce všech směrovačů ve stejné HSRP skupině (HSRP group). Pro potřeby HSRP se používají tzv. dobře známé (well-known) MAC adresy, které korespondují k používané IP adrese virtuálního směrovače. Například pro HSRP group 1 (HSRP skupiny jsou identifikovány celým číslem od 0 do 255) je odpovídající MAC adresa rovna 0000.0c07.ac01, kde 0000.0c07.ac__ je základ, ke kterému se přidá číslo HSRP skupiny zkonvertované do šestnáctkové soustavy (v tomto případě se přidá 01, jelikož 1_{10} je rovna 1_{16}).

3.4 HSRP standby

Funkcí HSRP standby routeru je monitorování stavu Active routeru. V případě zjištění výpadku Active routeru pak standby router okamžitě převezme roli aktivního směrovače a začne zpracovávat rámce přicházející na MAC adresu virtuálního routeru (převezme plnohodnotnou roli aktivního směrovače). Jak active router, tak standby router posílají hello zprávy, aby informovaly ostatní směrovače o svých rolích a o svém stavu. Za tímto účelem používají multicast adresu 224.0.0.2, UDP port 1985.



Obr. 1 – Topologie HSRP sítě
(zdroj: www.cisco.com)

3.5 Ostatní směrovače v HSRP skupině

HSRP skupina může, kromě active a standby routerů obsahovat i další směrovače. Tyto směrovače nemají speciálně označenou roli. Jejich úkolem je sledování hello zpráv, které si vyměňují active a standby routery patřící do stejné skupiny a v případě detekce jejich výpadku, který je implikován uplynutím maximální doby do příchodu další hello zprávy (tzv. hold interval), se mezi těmito směrovači provede volba nového (nových) active/standby routerů. Tyto směrovače si mezi sebou také vyměňují své hello zprávy (tzv. speak messages) a přeposílají pouze pakety odeslané přímo na jejich IP adresu (pakety poslané na IP adresu virtuální směrovače nepřeposílají).

Mezi další pojmy používané v rámci HSRP patří „hello interval" a „hold interval". Hello interval je interval mezi dvěma po sobě jdoucími hello zprávy, tj. doba, kterou směrovač čeká od odeslání jedné hello zprávy do odeslání následující hello zprávy („časovač" hello zpráv). Defaultní hodnota tohoto intervalu je rovna 3 vteřinám. Dalším pojmem je tzv. „hold interval". Jedná se o maximální dobu měřenou od přijetí hello zprávy, po kterou je směrovač, který zmiňovanou hello zprávu odeslal považován za bezproblémově fungujícího. Tedy pokud po přijetí poslední hello zprávy od nějakého směrovače uplyne doba hold intervalu, pak je tento směrovač považován za nefunkčního. Defaultní hodnota hold intervalu je rovna 10 vteřinám.

Pokud active router zhavaruje, standby router od něho přestane dostávat hello zprávy a po vypršení hold intervalu převezme jeho roli. Pokud se v rámci dané HSRP skupiny vyskytují i další směrovače, zahájí mezi sebou „boj" o roli nového standby routeru. V případě výpadku jak active, tak i standby směrovače, zahájí zbylé směrovače boj o obě tyto role. Protože nový active router začne zpracovávat (přeposílat) pakety, resp. rámce jdoucí na IP adresu, resp. MAC adresu virtuálního směrovače, je tato výměna rolí pro koncové stanice zcela transparentní.

3.6 Proces volby active a standby routeru

Proces volby rolí jednotlivých směrovačů v rámci HSRP skupiny je založen na prioritě směrovačů. Prioritou směrovače se rozumí hodnota parametru priority, která může nabývat hodnot v rámci intervalu <0; 255>, přičemž vyšší hodnota parametru znamená vyšší prioritu daného směrovače. Směrovač s nejvyšší prioritou (255 je nejvyšší možná priorita) bude zvolen do role active pro danou HSRP skupinu. Pokud existuje více směrovačů se stejnou hodnotou priority, tak bude jako active zvolen směrovač, který má nejvyšší IP adresu na HSRP interfejsu.

3.7 HSRP stavy

HSRP směrovač se může nacházet v jednom z následujících stavů:

- Initial
- Learn
- Listen
- Speak
- Standby
- Active

Initial je počáteční stav indikující, že HSRP zatím neběží. Do tohoto stavu směrovač přejde po změně konfigurace (vypnutí HSRP) či se v tomto stavu nachází při prvotním „nahození“ (zapnutí) rozhraní. Ve stavu learn se směrovač nachází během doby, kdy nezná informace potřebné k tomu, aby se mohl účastnit HSRP procesu. Do stavu listen se směrovač dostane, když se dozví IP adresu virtuálního routeru. V tomto stavu čeká na hello zprávy od ostatních směrovačů, které by se mohly nacházet ve stejné HSRP skupině. Smyslem tohoto stavu je tedy zjistit, zda pro danou skupinu již existuje aktivní (active) a záložní (standby) směrovač. Ve stavu speak směrovač aktivně posílá hello zprávy a účastní se volby active a standby routeru. Pokud se směrovač stane standby routerem, zastává roli záložního směrovače pro aktivní router. V roli active router zpracovává (přeposílá) pakety (rámce) poslané na IP (MAC) adresu virtuálního routeru.

Každý směrovač používá tři časově – active timer, standby timer a hello timer. Active timer slouží k monitorování stavu aktivního routeru. S každou přijatou hello zprávou od aktivního routeru je tento časovač vynulován. Pokud hodnota tohoto časovače převýší hold time interval, je aktivní router považován za nefunkčního. Obdobné platí pro standby timer, který slouží pro monitorování záložního směrovače. Hello timer pak slouží k plánování odesílání hello zpráv.

3.8 Optimalizace HSRP

HSRP umožňuje definovat, který ze směrovačů bude zastávat danou roli (resp. lze ovlivnit proces volby do těchto rolí), vyladit hodnoty časovačů a tím zajistit velmi rychlé zotavení se z výpadku aktivního směrovače. Rovněž dovoluje zotavit se i z výpadku rozhraní používaného (používaných) aktivním routerem pro zajištění komunikace s okolním světem.

Pro zajištění všech výše zmiňovaných vlastností slouží následující volby (parametry) – standby priorita, standby preempt, přizpůsobení časovačů (hello message timer, hold interval) a tzv. interface tracking (sledování rozhraní).

Pokud aktivní směrovač zhavaruje, záložní převezme jeho roli. V případě, že se původní aktivní router stane opět funkčním, setrvá nový aktivní router ve své roli, i když má (může mít) nižší prioritu než navrátivší se původní aktivní směrovač. HSRP standby preempt je funkce umožňující onomu původnímu aktivnímu směrovači navrátit se do své role i po svém výpadku. Navrácení do jeho původní role může být žádoucí z více důvodů, například z výkonnostního hlediska, či může mít daný směrovač „lepší spojení s okolním světem“ (linka s vyšší propustností, nižší latencí, apod.). Okamžité navrácení do aktivní role však nemusí být žádoucí. Po zavedení systému směrovače, resp. v okamžiku spuštění HSRP procesu, totiž tento směrovač nemusí mít dostatečné množství informací pro zajištění správného směrovaní průchozích paketů – dynamické směrovací protokoly potřebují určitý čas pro výměnu informací a finální konvergenci. Proto se k HSRP standby preempt pojí i parametr delay, kterým se dá definovat časový interval, po který směrovač po spuštění HSRP procesu vyčká, než znovu nabude role aktivního routeru.

Aby bylo zotavení se z výpadku aktivního směrovače co nejrychlejší, mohou být HSRP časovače (hello a hold interval) přizpůsobeny na velmi krátkou dobu, čímž se dá zajistit tzv. sub-second failover, tedy zotavení se z výpadku do jedné sekundy. Hello a hold intervaly pak po řadě nabývají hodnot kolem 250ms, resp. 800ms. Hodnoty těchto intervalů by ale neměly být extrémně malé, jelikož by mohlo dojít k poklesu stability HSRP skupiny. Směrovače by, v případě zatížení síťovým provozem, nemusely stihnout pravidelně odesílat a správě vyhodnocovat přijaté hello zprávy. To by následně způsobilo chybný předpoklad o výpadku nějakého ze směrovačů patřících do HSRP skupiny a chybné převzetí jeho role. Vyladění těchto intervalů je tedy kompromisem mezi rychlým zotavením se z výpadku a stabilitou HSRP skupiny (nasavení konkrétních hodnot hello a hold intervalů je tedy vhodné v reálném prostředí ověřit).

Sledování stavu rozhraní, tzv. interface tracking, dovoluje HSRP procesu automaticky snížit prioritu daného směrovače v případě výpadku rozhraní zajišťujícího konektivitu do „okolního světa“ (například rozhraní do sítě WAN; resp. libovolného rozhraní, které je HSRP procesem monitorováno). Výpadek tohoto rozhraní totiž nijak neovlivní dostupnost (dosažitelnost) a činnost rozhraní prostřednictvím kterého je daný směrovač připojen do sítě lokální (LAN) a na které je „mapováno“ rozhraní virtuálního směrovače. Výchozí brána je sice dostupná, ale konektivita do okolního světa však není (nemůže být) touto bránou zajištěna. Proto je žádoucí, aby v této situaci došlo k převolbě rolí HSRP směrovačů. Toho je dosaženo tím, že si směrovač, kterému vypadlo sledované rozhraní, sníží svou vlastní prioritu o určitou (v konfiguraci definovanou) hodnotu a roli aktivního routeru tak může převzít jiný směrovač, který má spojení s okolním světem zajištěno.

3.9 Problém s překladem síťových adres

Pokud je na směrovačích participujících v HSRP procesu prováděn překlad síťových adres (NAT – Network Address Translation), resp. překlad adres a portů (PAT – Port Address Translation), způsobí výpadek aktivního směrovače pád relací, které probíhaly právě přes aktivní směrovač a jejichž síťové adresy byly překládány. Výpadek navázaných relací nastává, i přes dostupnost všech stanic (díky převzetí funkce aktivního směrovače záložním), kvůli ztrátě překladové tabulky udržované (dynamicky) vypadnuvším směrovačem.

Řešením tohoto problému je nasazení „stavového předkladu adres“ (SNAT – Statefull NAT) společně s HSRP. SNAT dovoluje skupině směrovačů vzájemnou synchronizaci překladových tabulek. Směrovače si, kromě vlastního mapování překládaných IP adres, vyměňují rovněž i některé informace o stavu navázaných spojení (například stavové parametry TCP spojení). SNAP podporují například Cisco směrovače s IOS verzí 12.3 a vyšší.

3.10 HSRP verze 2

HSRP verze 2 přináší oproti první verzi několik vylepšení. Prvním vylepšením je propagovaní „milivteřinových“ hodnot hello a hold intervalů v rámci zpráv posílaných aktivním HSRP směrovačem. Toto zajišťuje mnohem větší stabilitu HSRP skupiny. Dalším vylepšením je rozšíření rozsahu hodnot pro identifikaci HSRP skupiny. První verze podporovala pouze hodnoty od 0 do 255, druhá verze přináší interval od 0 do 4095. S rozšíření tohoto intervalu samozřejmě souvisí i změna používaných virtuálních MAC adres. HSRPv1 postačoval k identifikaci skupiny pouze jeden (poslední) bajt MAC adresy. S rozšířením intervalu na 4096 možných hodnot bylo nutné zvětšit i počet bitů MAC adresy virtuálního routeru, které by sloužily k identifikaci dané skupiny, z původních 8 na 12. Nový rozsah MAC adres začíná hodnotou 0000.0C9F.F000 a končí 0000.0C9F.FFFF. Toto rozšíření rovněž umožnilo svázat hodnotu HSRP skupiny s číslem VLAN, které může nabývat rovněž hodnot od 0 do 4095 (alespoň v Cisco implementaci). V původní (první) verzi HSRP nebylo dále možné identifikovat zdroj hello zpráv, jelikož tyto zprávy byly odesílány se zdrojovou MAC adresou virtuálního routeru. Druhá verze rozšiřuje hlavičku této zprávy o šesti bajtový identifikátor zdroje (odesílatele) této zprávy. Tento identifikátor je typicky vyplňován skutečnou MAC adresou rozhraní odesílatele. Rovněž došlo ke změně multicast IP adresy, na kterou jsou HSRP zprávy odesílány. Původní adresa 224.0.0.2 mohla kolidovat se zprávami Cisco Group Management protokolu (CGMP). Druhá verze proto používá novou multicast IP adresu 224.0.0.102. HSRPv2 dále mění formát hlavičky paketu. Nový formát používá tzv. „type-length-value“ (TLV). Paket HSRP verze 2 přijatý směrovačem na němž běží HSRPv1 bude tuto hodnotu interpretovat jinak a daný paket zahodí (bude ho ignorovat), obdobné platí i pro opačně odeslanou zprávu. HSRPv2 tedy není kompatibilní s první verzí, tj. dvě zařízení provozující různé verze HSRP spolu nemohou komunikovat. Zároveň není

možné nad jedním rozhraním provozovat obě verze HSRP současně. Na různých rozhraních jednoho zařízení (routeru) však mohou současně běžet jak první, tak i druhá verze HSRP.

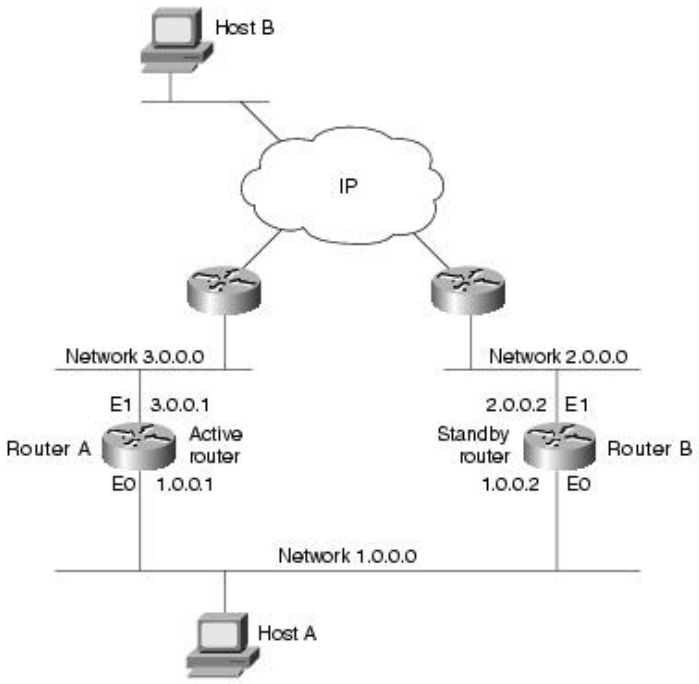
4. Porovnání HSRP s VRRP a GLBP

Protokol VRRP (Virtual Router Redundancy Protocol), definovaný organizací IETF (popsán v RFC 3768 a 3768), je alternativou k protokolu HSRP (jejich funkce je totožná, liší se pouze v nepodstatných detailech). Důvodem, proč nasadit VRRP namísto HSRP, může být zajištění kompatibility mezi zařízeními různých výrobců.

GLBP (Gateway Load Balancing Protocol) je proprietární protokol společnosti Cisco Systems. Oproti HSRP umožňuje lépe balancovat zátěž mezi všechny dostupné směrovače, které mohou plnit roli výchozí brány. HSRP totiž podporuje pouze jeden aktivní směrovač – rozkládání zátěže mezi více směrovačů je sice možné zajistit, řešení je ale těžkopádné a špatně škálovatelné (lze definovat více HSRP skupin, pro každou jiný aktivní směrovač a koncovým stanicím přidělovat různé adresy výchozí brány). V rámci jedné GLBP skupiny směrovačů vystupuje jeden jakožto „hlavní“ (tzv. active virtual gateway). Tento hlavní směrovač zpracovává veškeré ARP dotazy na MAC adresu výchozí brány (virtuální brány). Poté, dle nastaveného mechanizmu distribuce zátěže (např. dle vah jednotlivých směrovačů), bude „spoofovat” (podvrhovat) ARP odpovědi s MAC adresou nějakého směrovače ze stejné GLBP skupiny, který pak bude zajišťovat směrování rámců koncové stanice, která zaslala onen ARP dotaz. Pomocí vzájemného vyměňování zpráv mezi všemi směrovači GLBP skupiny je možné detekovat výpadek některého člena a převzat „jeho klienty“. Po vypršení platnosti ARP záznamu (mapování IP-MAC) uloženého v keši koncové stanice, jejíž výchozí brána zhavarovala, je na nový ARP dotaz navrácena platná MAC adresa stávajícího routeru vykonávajícího roli výchozí brány. GLBP tedy přináší více funkcí než HSRP. Nevýhodou je nedostupnost tohoto protokolu v platformách určených pro spíše menší a středně velké sítě (resp. produkty určené pro přístupovou či distribuční vrstvu sítě). Mezi Cisco produkty jej podporuje platforma Catalyst 6500, určená pro enterprise nasazení (rozsáhlé sítě, reps. páteřní vrstvu sítě). HSRP je oproti tomu podporován de facto napříč celým portfoliem Cisco síťových produktů (směrovači a multilayer přepínači).

5. Příklad sítě se zajištěnou vysokou spolehlivostí výchozí brány prostřednictvím HSRP (převzato z www.cisco.com)

Topologie sítě



Obr. 2 – Příklad nasazení HSRP v síti
(zdroj: www.cisco.com)

Všechny koncové stanice v síti jsou zkonfigurovány tak, že používají IP adresu virtuálního směrovače (v tomto případě 1.0.0.3) jakožto IP adresu své výchozí brány. V rámci sítě je, jako směrovací protokol, nasazen EIGRP (Enhanced Interior Gateway Routing Protocol).

Konfigurace směrovače A

```
hostname RouterA
!
interface ethernet 0
 ip address 1.0.0.1 255.0.0.0
 standby 1 ip 1.0.0.3
 standby 1 preempt
 standby 1 priority 110
 standby 1 timers 5 15
!
interface ethernet 1
 ip address 3.0.0.1 255.0.0.0
!
router eigrp 1
```

```
 network 1.0.0.0
 network 3.0.0.0
!
```

Konfigurace směrovače B

```
hostname RouterB
!
interface ethernet 0
 ip address 1.0.0.2 255.0.0.0
 standby 1 ip 1.0.0.3
 standby 1 preempt
 standby 1 timers 5 15
!
interface ethernet 1
 ip address 2.0.0.2 255.0.0.0
!
router eigrp 1
 network 1.0.0.0
 network 2.0.0.0
!
```

Popis jednotlivých HSRP příkazů

`standby 1 ip 1.0.0.3`

Spustí HSRP proces pro skupinu 1 a nastaví IP adresu virtuální směrovače této skupiny na hodnotu 1.0.0.3. Konfigurace všech routerů musí obsahovat tento příkaz, aby mohly společně spolupracovat (stejná skupina, stejná IP adresa virtuálního směrovače).

`standby 1 preempt`

Tento příkaz umožňuje směrovači stát se aktivním routerem pro danou HSRP skupinu (zde pro skupinu 1). V tomto případě se tedy aktivním směrovačem mohou stát oba – jak router A, tak i router B. Aktivním směrovačem se poté stane ten s vyšší prioritou.

`standby 1 priority 110`

Tímto příkazem lze ovlivnit proces volby rolí díky nastavení priority směrovače. Výchozí priorita je rovna 100. V tomto případě se tedy směrovač A stane (díky prioritě 110) aktivním routerem pro skupinu 1.

`standby 1 timers 5 15`

Nastavení délky intervalů pro plánování odesílání a kontrolu příchodů hello zpráv pro danou HSRP skupinu. Výchozí jednotkou je jedna vteřina. První hodnota udává délku hello intervalu (zde 5 vteřin), druhá poté délku hold intervalu (15 vteřin v tomto případě). Výchozí (defaultní) hodnoty jsou 3 vteřiny pro hello, resp. 10 vteřin pro hold interval. Pro natavení délky intervalu kratší než jedna vteřina lze použít volitelného parametru msec. Příkaz

`standby 1 timers msec 250 msec 800` by specifikoval nastavení 250ms pro hello, resp. 800ms pro hold interval.

Pozn.: Více podrobností o konfiguraci HSRP je možné nalézt ve veřejně přístupné dokumentaci společnosti Cisco Systems. Jeden z možných odkazů je uveden na konci tohoto dokumentu v seznamu zdrojů.

6. Ověření správné funkce HSRP

Funkčnost HSRP, resp. schopnost zotavit se z výpadku výchozí brány, lze ověřit například pomocí „debug" výpisů (hlášek) dostupných na většině síťových zařízení (v tomto případě by se sledovaly hlášky na HSRP směrovačích). Jinou možností ověření funkčnosti HSRP je sledování výpisu programu ping. Pomocí tohoto programu lze „nepřetržitě odesílat" ICMP echo request zprávy na nějakou stanici dostupnou právě přes výchozí bránu (která je de facto provozována HSRP směrovači) a sledovat hlášky o došlých odpovědích (ICMP echo reply). Součástí tohoto výpisu je i zpoždění došlé odpovědi. Hodnota tohoto parametru pak bude korelovat s vyladěním HSRP časovačů (hello a hold intervalů). Pokud budou hello a hold intervaly příliš dlouhé, dojde k vypršení limitu, po který se čeká na příchod ICMP echo reply zprávy a tato situace vyvolá vypsání (ping programem) jedné z hlášek o nedostupnosti cílové stanice. Takováto situace by ovšem, při bezproblémovém běhu HSRP a optimálním vyladění HSRP časovačů, neměla nikdy nastat. V případě bezeztrátového příjmu ICMP echo zpráv (při rozumně nastavené době čekání na odpověď – v rámci stejné lokální sítě například do jedné vteřiny) lze považovat výchozí bránu za vysoce dostupnou (HSRP směrovače fungují optimálně a bez problémů).

7. Závěr

Protokol HSRP je vhodný pro zajištění vysoké dostupnosti výchozí brány. V sítích, pro které je požadována vysoká spolehlivost a dostupnost, lze nasazení tohoto protokolu určitě doporučit.

Seznam literatury a zdrojů

[1] David Hucaby, *CCNP BCMSN Official Exam Certification Guide*, čtvrté vydání, Cisco Press, 2007

[2] Materiály ke školení Building Cisco Multilayer Switched Networks, verze 3.0, Cisco Systems, 2006

[3] David Davis, *Preserve NAT translations when a Cisco router fails (web article)*, 2006, http://articles.techrepublic.com.com/5100-1035_11-6065899.html

[4] Webové stránky společnosti Cisco Systems (www.cisco.com)

- Cisco IOS Software Releases 12.3T – Hot Standby Router Protocol Version 2 http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d21.html
- Using HSRP for Fault-Tolerant IP Routing http://www.cisco.com/en/US/tech/tk1330/technologies_design_guide_chapter09186a008066670b.html
- Catalyst 3750 Switch Software Configuration Guide, 12.2(25)SEE – Configuring HSRP http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_see/configuration/guide/swhsrp.html