Protokol GLBP

Projekt do předmětu Správa počítačových systémů

Radim Poloch (pol380), Jan Prokop (pro266)

7.6.2007

Obsah

1 Úvod **3**
1.1 Technologie GLBP 3
1.1.1 Příklad topologie GLBP 3
1.1.2 Přiřazení virtuální MAC adresy v GLBP 4
1.1.3 Priorita v GLBP 4
1.1.4 Váhy v GLBP 4
1.1.5 Výhody GLBP 4
2 Postup při testování **5**
2.1 Schéma implementované topologie 5
2.2 Analýza chování síťovým analyzátorem 6
2.3 Testování různých nastavení loadbalancingu u protokolu GLBP 6
2.4 Ověřování náhrady AVG jedním z AVF (v případě výpadku linky u AVG) 6
3 Výsledky testování **7**
3.1 Anylýza chování síťovým analyzátorem 7
3.1.1 Popis prostředí Etherealu 7
3.2 Testování různých nastavení loadbalancingu u protokolu GLBP 8
3.3 Ověřování náhrady AVG jedním z AVF (v případě výpadku linky u AVG) 8
4 Závěr **8**
5 Přílohy **9**
A) Konfigurace routeru 9
B) Konfigurace PC 10

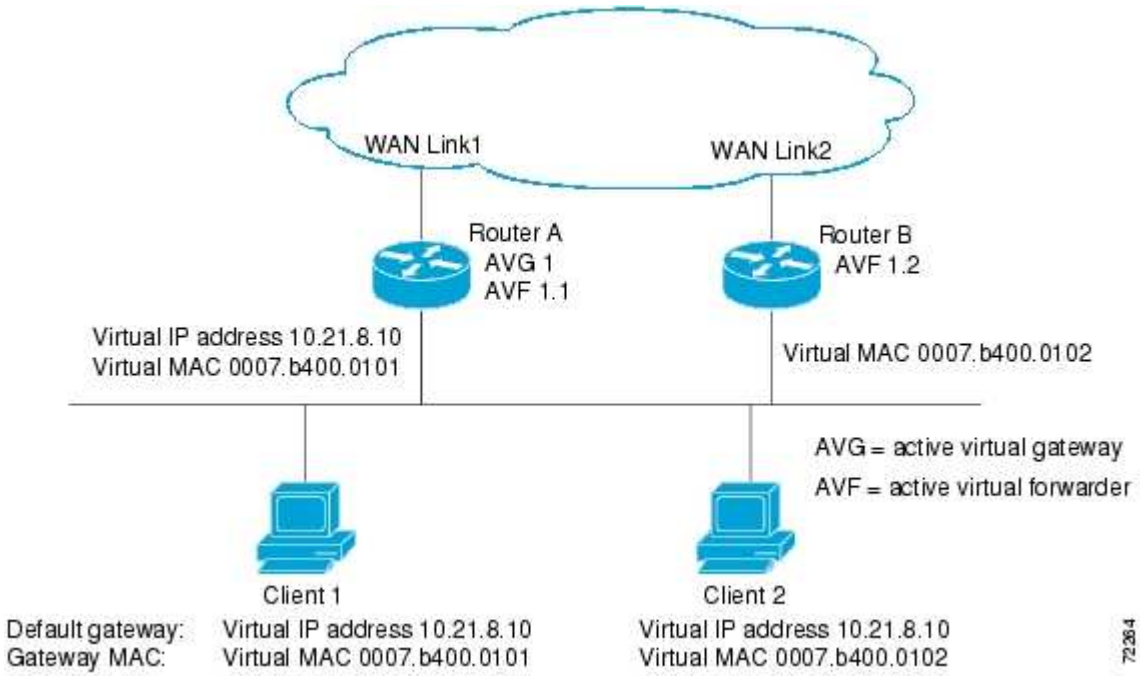
1 Úvod

GLBP (Gateway Load Balancing Protocol) zajišťuje automatickou náhradu routeru nastaveného jako výchozí brána připojených stanic linkou vedenou přes záložní router(y). Několik výchozích bran se zkombinuje a celek pak nabízí jedinou virtuální bránu, přičemž zátěž se může dělit mezi všechny routery ve skupině. Routery mohou vzájemně působit jako podpůrní členové GLBP skupiny a při výpadku hlavního routeru mohou převzít řízení protokolu. GLBP poskytuje jedinou virtuální IP adresu a více virtuálních MAC adres. Všechna zařízení mají nakonfigurováno směrování na tuto stejnou IP adresu, přičemž na směrování packetů se podílejí všechny routery (vždy právě jeden vybraný) ve virtuální skupině. Členové skupiny mezi sebou komunikují pomocí zpráv hello, které si posílají každé 3 vteřiny na multicast adresu 224.0.0.102.

1.1 Technologie GLBP

Členové GLBP zvolí jeden router jako aktivní virtuální bránu (AVG). Ostatní členové pak působí jako záložní AVG, pokud aktivní vypadne. AVG přiřadí virtuální MAC adresu každému routeru ze skupiny GLBP. Každý router přijímá zodpovědnost za směrování packetů poslaných na virtuální MAC adresu, který mu přiřadil AVG. Tyto routery jsou pak aktivní virtuální přeposílatelé pro jejich virtuální MAC adresy (AVFs). AVG je zodpovědný za vyřízení dotazů ARP, které přijdou na virtuální adresu. Sdílení zátěže je dosaženo tím, že AVG v odpovědi na ARP dotaz zasílá různé virtuální MAC adresy (odpovídající různým routerům ve skupině).

1.1.1 Příklad topologie GLBP



Router A je AVG pro tuto GLBP skupinu a je zodpovědný za virtuální IP adresu 10.21.8.10. Router A je také AVF pro virtuální MAC adresu 0007.b400.0101. Router B je členem stejné GLBP skupiny a je nastaven jako AVF pro virtuální MAC adresu 0007.b400.0102. Client 1 má nastavenou výchozí bránu na IP adresu 10.21.8.10 a MAC adresu 0007.b400.0101. Client 2 sdílí stejnou IP adresu výchozí brány (10.21.8.10), ale přijímá MAC adresu 0007.b400.0102, za účelem rozdělení zátěže.

Pokud se router A stane nedostupným, Client 1 neztratí přístup do WAN, protože router B převezme zodpovědnost za směrování packetů zaslaných na virtuální MAC adresu routeru A (AVF 1.1) a také za směrování packetů zaslaných na jeho vlastní MAC adresu (AVF 1.2). Router B také převezme roli AVG pro celou GLBP skupinu. Komunikace pro členy GLBP skupiny pokračuje nezávisle na selhání routeru ve skupině.

1.1.2 Přiřazení virtuální MAC adresy v GLBP

GLBP povoluje maximálně 4 virtuální MAC adresy v rámci skupiny. AVG je zodpovědný za přiřazování MAC adres každému ze členů skupiny. Routerům jsou přidělovány MAC adresy sekvenčně. V každé skupině mohou být maximálně 4 routery (4 MAC adresy). Virtuální směrovač (AVF), kterému je přiřazena virtuální MAC adresa routerem AVG, je označen primární virtuální směrovač. Ostatní členové si sami vyžádají virtuální MAC adresu poté, co detekují AVG pomocí jimi posílaných hello zpráv (na adresu AVG). Tyto AVF označujeme jako sekundární.

1.1.3 Priorita v GLBP

Každému routeru ve skupině lze přiřadit číselná priorita v rozmezí 0-255. Podle této priority se pak rozhoduje, který z routerů převezme činnost AVG, pokud se aktivní AVG stane nedostupným.

1.1.4 Váhy v GLBP

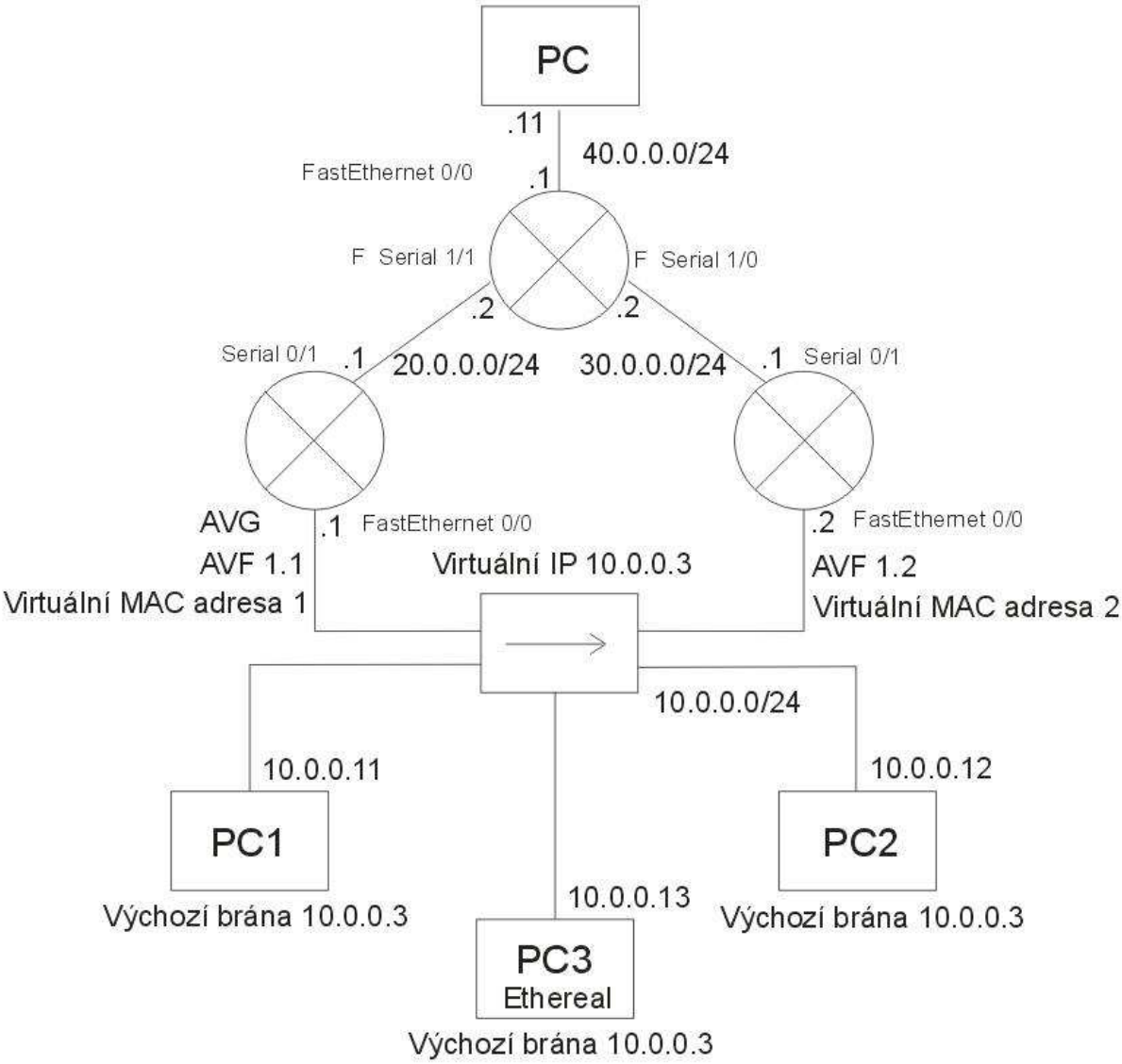
GLBP používá schéma vah pro rozhodnutí datové propustnosti odchozích linek jednotlivých routerů ve skupině. Na základě váhy se rozhodne, přes který router bude směrování probíhat a kolik klientů bude obsluhovat. Hranice mohou být nastaveny tak, aby přerušily přeposílání rámců v případě, že váha klesne pod určitou úroveň. V okamžiku, kdy váha zpětně přeroste jinou hranici, je přeposílání rámců automaticky obnoveno. Váhy mohou být automaticky přizpůsobovány pomocí sledování aktuálního stavu zatížení (tracking).

1.1.5 Výhody GLBP

- Sdílení zátěže
- Podpora velkého počtu GLBP skupin na jednom rozhraní (až 1024)
- Systém priorit a váh
- Autentifikace

2 Postup při testování

2.1 Schéma implementované topologie



Obrázek 2.1.1

2.2 Analýza chování síťovým analyzátorem

Na PC3 připojeném k HUBu zaznamenáme provoz packetů v síti pomocí programu Ethereal. Zachycené packety profiltrujeme (na základě cílové adresy – multicast adresa GLBP) a získáme tak přehled o přenosu Hello zpráv mezi routery ve skupině. Získaná data analyzujeme a pokusíme se dekódovat obsah zpráv.

2.3 Testování různých nastavení loadbalancingu u protokolu GLBP

Při nastavování parametrů protokolu lze vybrat způsob, na základě kterého bude balancování přenášených packetů prováděno. GLBP poskytuje tři možnosti: Round-Robin (každý virtuální směrovač se může během požadavku stát zodpovědným za vyřízení požedavku), Host dependent (požadavky z jednoho zařízení obstará vždy stejný směrovač), Weighting (směrovač je přiřazen zařízení podle zadaných parametrů váhování). Budeme zkoumat, jak se které nastavení chová při zahlcování sítě pingy, případně pak flood pingy. Budeme je odesílat z PC1 – 3 na rozhraní horního routeru (40.0.0.1), ke kterému je připojené horní PC (40.0.0.11). Tak můžeme pomocí příkazu “debug ip packet“ na rozhraní routeru (40.0.0.1) sledovat příchozí packety včetně cesty, kterou na toto rozhraní došly.

2.4 Ověřování náhrady AVG jedním z AVF *(v případě výpadku linky u AVG)*

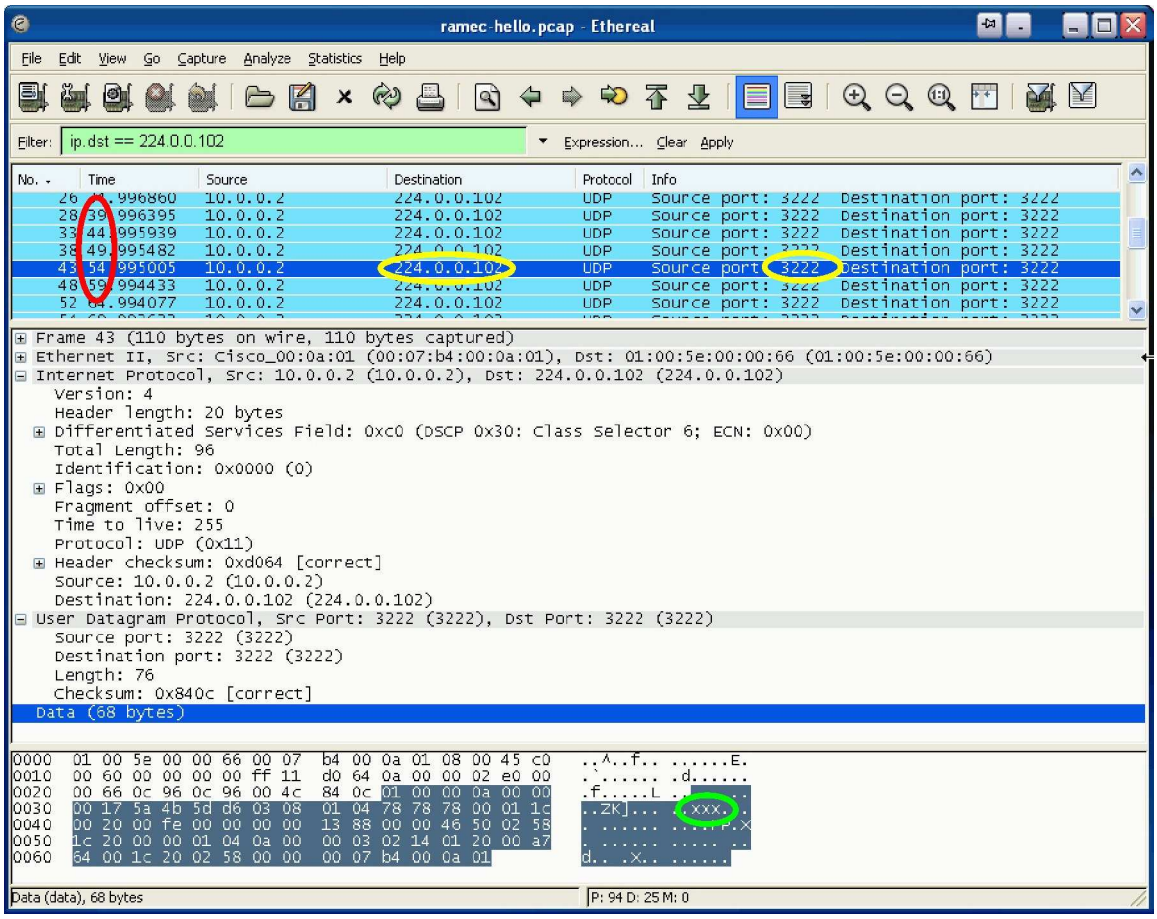
Předpokládáme, že v případě výpadku linky u AVG bude tato funkce přebrána jedním z AVF. Tuto skutečnost ověříme tak, že během provozu odpojíme rozhraní Serial, které spojuje AVG s horním routerem. Dále pak po uplynutí hold down timu zkontrolujeme, zda byl probíhající přenos pingů přesměrován na AVF.

3 Výsledky testování

3.1 Anylýza chování síťovým analyzátorem

Po zapojení topologie dle uvedeného schématu byly zachytávány packety programem Ethereal spuštěném na PC3.

Výpis zachycených Hello zpráv, které se periodicky posílaly mezi routery v nastaveném intervalu 5s:



3.1.1 Popis prostředí Etherealu

Vidíme, že zprávy chodí pravidelně na multicast adresu 224.0.0.102, protokolem UDP na port 3222. Zprávy zasílají pouze routery AVF (v tomto případě router 10.0.0.2). V zelené elipse vidíme authentification text (xxx), který byl nastaven pro naši GLBP skupinu a přenáší se v čistě textové podobě. Konkrétní formát dat packetu Cisco nezveřejňuje.

3.2 Testování různých nastavení loadbalancingu u protokolu GLBP

Nastavení GLBP bylo testováno zvlášť na routerech Cisco 2800 Series (2 měření) a zvlášť na routerech Model Cisco 1751 (1 měření).

U této části testování nebylo dosaženo očekávaných výsledků. Ačkoli byly vyzkoušeny všechny tři možnosti balancování, ani u jedné z nich se nepodařilo zajistit očekávaný průběh. Ačkoli GLBP byl prokazatelně aktivní, pingy a flood pingy posílané na FastEthernetové rozhraní horního routeru z dolních počítačů byly směrovány vždy pouze přes AVG. Výchozí brána počítačů v HUBu byla nastavena na virtuální IP GLBP skupiny. Zpátky byly packety vráceny na základě směrování RIP, které bylo na routerech konfigurováno.

3.3 Ověřování náhrady AVG jedním z AVF (v případě výpadku linky u AVG)

V této fázi jsme zjistili výsledky zcela odpovídající našim teoretickým předpokladům. V případě výpadku linky u AVG bylo spojení po uplynutí maximálně námi nastaveného času obnoveno pomocí linky AVF. Tento čas se počítá na základě hold down timu od chvíle, kdy byla nedoručena poslední Hello zpráva. Maximální doba obnovení spojení je tedy hold down time + interval mezi Hello zprávami. Zvolený AVF router (podle priority nakonfigurované v GLBP nebo podle jeho číslování) tak přebral funkci AVG a směrování obstarával sám. Po opětovném zapojení rozpojené linky se přenos vrátil zpět na původní AVG. Opět zde byla časová prodleva (redirect time – viz. popis v příloze) nastavená při konfiguraci protokolu.

4 Závěr

Jak již vyplývá z výsledků našeho měření, podařilo se nám sestavit a zapojit topologii pro otestování protokolu, ale nedočkali jsme se všech očekávaných výsledků. Balancování se nám nepodařilo zprovoznit tak, aby skutečně vyvažovalo zatížení linek.

Vše ostatní se nám však podařilo zachytit dle požadavků a protokol fungoval dle našich předpokladů, ať už jde o zasílanou komunikaci přes Hello zprávy, nebo o náhradu AVG či funkčnost virtuální IP adresy brány.

5 Přílohy

A) Konfigurace routeru

Výpis „show run“ routeru AVG

```
interface FastEthernet0/0
ip address 10.0.0.1 255.255.255.0
speed auto
glbp 10 ip 10.0.0.3
glbp 10 timers 5 18
glbp 10 timers redirect 600 7200
glbp 10 priority 254
glbp 10 load-balancing host-dependent
glbp 10 authentication text xxx
no glbp 10 forwarder preempt
!
interface Serial0/0
no ip address
shutdown
!
interface Serial0/1
ip address 20.0.0.1 255.255.255.0
!
interface ATM1/0
no ip address
shutdown
no atm ilmi-keepalive
dsl operating-mode auto
!
router rip
network 10.0.0.0
network 20.0.0.0
```

Význam jednotlivých parametrů příkazů GLBP je slovně uveden ve výpisu show glbp (níže).

Výpis „show glbp“

FastEthernet0/0 - Group 10
State is Active
2 state changes, last state change 00:37:40
Virtual IP address is 10.0.0.3
Hello time 5 sec, hold time 18 sec
Next hello sent in 4.120 secs
Redirect time 600 sec, forwarder time-out 7200 sec
Preemption disabled
Active is local
Standby is unknown
Priority 254 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: host-dependent
There is 1 forwarder (1 active)
Forwarder 1
State is Active
1 state change, last state change 00:37:22
MAC address is 0007.b400.0a01 (default)
Owner ID is 0008.e3fb.a67c
Redirection enabled
Preemption disabled
Active is local, weighting 100
Arp replies sent: 6

B) Konfigurace PC

Konfigurace PC1

ifconfig eth0 10.0.0.11 netmask 255.255.255.0
route add default gw 10.0.0.3