ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 68 Nr kol. 1905

Jakub HORBACEWICZ, Ireneusz J. JÓŹWIAK, Jacek GRUBER
Politechnika Wrocławska

BADANIE KONWERGENCJI PROTOKOŁÓW REDUNDANCJI BRAMY DOMYŚLNEJ

Streszczenie. Zastosowanie mechanizmu redundancji bramy domyślnej zwiększa niezawodność sieci komputerowej. W artykule przedstawiono wyniki badań protokołów redundancji bramy domyślnej w przypadku awarii połączenia z jednym z dostawców usług internetowych w eksperymentalnej topologii sieciowej. Badanie pozwala wyznaczyć czas procesu konwergencji każdego z opisywanych protokołów. Im ten czas jest krótszy, tym rozwiązanie uznawane jest za lepsze.

Słowa kluczowe: sieć komputerowa, niezawodność, redundancja, brama domyślna, konwergencja.

FIRST HOP REDUNDANCY PROTOCOLS CONVERGENCE SURVEY

Summary. Use of the default gateway redundancy increases the reliability of a computer network. This paper presents results of the first hop redundancy protocols survey while losing connection to one of the ISP connected in experimental network topology. This test allows to determine the time of convergence processes of the described protocols. The shorter the time, the better the protocol is.

Keywords: computer network, reliability, redundancy, default gateway, convergence.

1. Wprowadzenie

Wszystkie współczesne systemy informatyczne zarządzania procesami wytwórczymi, zarządczymi i informacyjnymi egzystują w środowiskach komputerowych sieci intranetowych komputerowych sieci korporacyjnych, w większości komunikujących użytkowników i różnorodne procesy wytwórcze, zarządcze i biznesowe w architekturze klient-serwer i w długoterminowych systemach o architekturach opartych na paradygmatach

informatycznych procesów biznesowych. Sprawne i wydajne funkcjonowanie platformy sieciowej, jako środowiska funkcjonowania tych różnorodnych systemów informatycznych, ma tutaj znaczenie podstawowe. Z wielu powodów wydajnościowych, niezawodnościowych i funkcjonalnych bardzo istotne jest zapewnienie konwergencji bram (ang. gateways) środowisk sieci intranetowych z siecią globalną, najczęściej z Internetem. Technologia redundancji bramy domyślnej FHRP (ang. *First-hop redundancy protocols* lub *default-gateway redundancy protocols*) jest istotnym komponentem koncepcji niezawodnej sieci komputerowej, w której wykorzystywana jest brama domyślna [8]. Mechanizm pozwala na automatyczne przekazanie roli bramy domyślnej innemu, będącemu w gotowości, urządzeniu po awarii maszyny pierwotnie pełniącej tę funkcję. Każdy z opisywanych protokołów tworzy z kilku routerów fizycznych, pretendujących do roli bramy domyślnej, jeden router wirtualny, określany również mianem grupy. Do grupy przypisany jest wirtualny adres IP (ang. *Virtual Internet Protocol address*), który staje się adresem bramy domyślnej dla stacji roboczych działających w ramach segmentu sieci. Z wirtualnym adresem IP sprzężony jest wirtualny adres warstwy fizycznej MAC (ang. *Media Access Control address*) [8]. W ramach wirtualnego routera definiowana jest maszyna, która fizycznie pełni rolę bramy domyślnej i przekazuje pakiety na zewnątrz oraz do sieci lokalnej. Pozostałe z nich pracują w trybie gotowości, aby przejąć rolę aktywnej bramy w przypadku awarii routera pierwotnie pełniącego tę funkcję. Każdy protokół definiuje zbliżone mechanizmy odpowiedzialne za zarządzanie routerami wewnątrz grupy.

W artykule przedstawiono porównanie trzech protokołów redundancji bramy domyślnej FHRP: HSRP (ang. *Hot Standby Router Protocol*) [4], VRRP (ang. V*irtual Router Redundancy Protocol*) [5, 6, 7] oraz GLBP (ang. *Gateway Load Balancing Protocol*) [3], pod kątem czasu konwergencji. Konwergencja, inaczej zbieżność, zgodnie z definicją podaną w [9] rozumiana jest jako stan, w którym routery (węzły) w sieci komputerowej uzgadniają spójną informację na temat topologii sieci, do których są podłączone. Po wystąpieniu zmiany w topologii sieci, np. wywołanej awarią, zachodzi konieczność wystąpienia procesu konwergencji. W tym czasie węzły odrzucają ruch adresowany do lokalizacji zdalnych, do których trasa wiodła przez połączenie lub urządzenie, które uległo awarii, mimo istnienia innej ścieżki w układzie połączeń sieci komputerowej.

W badaniach jako kryterium przyjęto najkrótszy czas procesu konwergencji. Na jego podstawie będzie można wskazać, który z opisywanych protokołów jest najlepszy.

2. Opis środowiska testowego

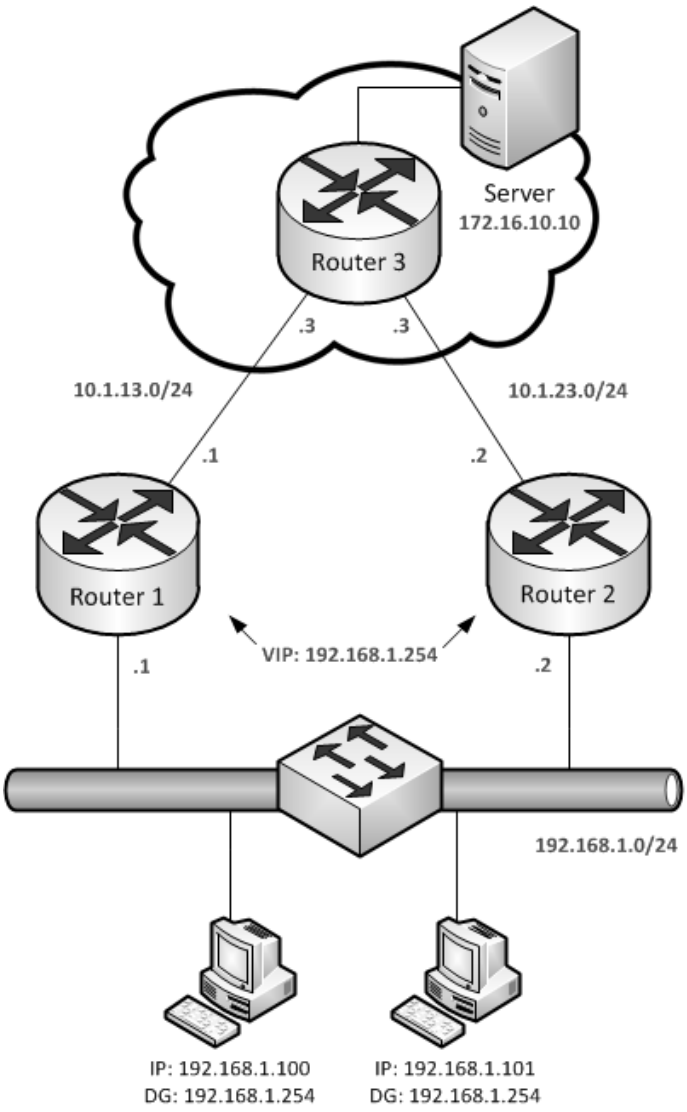
Topologia testowa, a więc model układu połączeń elementów sieci komputerowej, składa się kilku składników zaprezentowanych na rysunku 1. Pierwszy z nich to sieć lokalna

o adresie IP: 192.168.1.0/24, w której znajdują się stacje robocze oznaczone PC1, z adresem IP: 192.168.1.100, i PC2, z adresem IP: 192.168.1.101. Są one podłączone do przełącznika dostępowego (ang. *switch*). Połączenie pomiędzy przełącznikiem a routerami realizowane jest na zasadzie połączeń warstwy drugiej modelu OSI [2], co uzasadnia zastosowanie protokołów FHRP. Kolejnym elementem są dwa połączenia symulujące połączenia WAN (ang. *Wide Area Network*) z siecią zdalną o adresach IP: 10.1.13.0/24 oraz 10.1.23.0/24. Ostatni składnik to sieć odległa z serwerem o adresie IP: 172.16.10.10, do którego nawiązywane są połączenia ze stacji roboczych PC1 i PC2. Środowisko lokalnej sieci komputerowej bazuje na rozwiązaniu Ethernet [2].

Routery 1 oraz 2 są przy badaniu każdego protokołu konfigurowane jako jeden wirtualny router z wirtualnym adresem IP: 192.168.1.254. Na hostach PC1 i PC2 skonfigurowana jest brama domyślna, która wskazuje na adres wirtualny, co zostało zaznaczone na rysunku jako adres *DG* (z ang. *Default-Gateway*). Przy prawidłowo działającej sieci w każdym z przypadków Router 1 pełni rolę bramy domyślnej. Skonfigurowany jest on z wyższym priorytetem w ramach wirtualnego routera i przez niego przechodzi ruch wychodzący z sieci lokalnej o adresie IP: 192.168.1.0/24. Taki stan określony jest w dalszej części dokumentu mianem pierwotnego.

Usterka symuluje problem połączenia Routera 1 z Routerem 3. Komunikacja z Routerem 1 od strony sieci lokalnej jest możliwa, ale urządzenie nie jest w stanie wysyłać pakietów poza segment, a więc nie może pełnić funkcji bramy domyślnej. Do wykrycia opisywanej sytuacji zaimplementowano w systemie operacyjnym Routera 1 śledzenie interfejsu [1] od strony sieci zdalnej. Za pomocą tego sensora protokoły FHRP będą monitorować stan bramy domyślnej. W sytuacji kiedy połączenie do Routera 3 ulegnie awarii, Router 1 wygeneruje stosowny komunikat. Godzina jego wystąpienia będzie uznana za początek procesu konwergencji. Sytuacją pożądaną jest, aby po wystąpieniu awarii połączenia pomiędzy Routerem 1 i Routerem 3 nastąpiło przełączenie funkcji bramy domyślnej na Router 2. Takie działanie zmniejszy czas przerwy w działaniu sieci komputerowej.

Routery wchodzące w skład wirtualnego routera nieustająco komunikują się ze sobą. Pozwala im to na wykrycie ewentualnych awarii i zmianę roli bramy domyślnej na inny router wewnątrz grupy. Do komunikacji używane są pakiety typu *hello*, które powiadamiają resztę węzłów o istnieniu nadawcy. Pakiety te wysyłane są zgodnie z licznikiem (ang. *timer*) *hello*. Definiuje on czas, po którym router wysyła pakiet *hello*. Drugim licznikiem charakterystycznym dla każdego z opisywanych protokołów jest licznik *hold down*. Określa on czas, po którym dany węzeł uznawany jest za niedostępny. Licznik *hold down* zerowany jest każdorazowo po odebraniu pakietu *hello* od aktywnego węzła z grupy. Wartość licznika *hold down* jest większa niż *hello*, co oznacza, że aby uznać router za niedostępny, musi nastąpić brak dostarczenia co najmniej jednego pakietu *hello*.



Rys. 1. Topologia testowej sieci komputerowej
Fig. 1. Test network topology
Źródło: opracowanie własne.

W badaniach użyto dwóch zestawów liczników. Pierwszy jest zestawem domyślnym dla protokołów HSRP i GLBP, w którym licznik *hello* wyznacza czas 3 sekund, a licznik *hold down* 10 sekund. Drugi jest zestawem, w którym licznik *hello* ma wartość domyślną dla protokołu VRRP, a więc 1 sekundę. W protokole VRRP można ustalić jedynie odstęp dla wysyłania kolejnych pakietów typu *hello*. Wartość licznika *hold down* wyznaczana jest ze wzoru:

$$hdt = 3 \cdot hello + 1 - \frac{priorytet}{256}, \tag{1}$$

gdzie:

hdt – czas wyznaczony przez licznik *hold down timer*,

hello – czas wyznaczony przez licznika *hello*,

priorytet – priorytet interfejsu w grupie VRRP, priorytet $\in \langle 1,254 \rangle$ i priorytet $\in N$.

Aby uzyskać czas zbliżony do 10 sekund dla VRRP, przyjęto priorytet 3 dla routera pełniącego rolę pierwszej bramy i 1 po spadku spowodowanym awarią oraz priorytet 2 dla routera zastępczego. Dało to kolejno: 9,988 s (9,996 s po przełączeniu roli) i 9,992 s jako wartość licznika *hold down* dla użytych routerów. Drugi zestaw liczników to 1 sekunda odstępu pomiędzy kolejnymi pakietami *hello* i 4 sekundy dla licznika *hold down*. Aby uzyskać czas zbliżony do 4 sekund w przypadku VRRP, użyto tych samych priorytetów co w przypadku pierwszego zestawu. Dało to kolejno: 3,988 s (3,996 s po przełączeniu roli) i 3,992 s, jako wartości liczników *hold down* dla obu węzłów.

3. Przebieg badań czasu konwergencji protokołów FHRP

Każde badanie wykonano cztery razy, a wyniki przedstawiają średnią z tych prób. Wyniki o charakterze wyliczeniowym są zawsze zaokrąglone do części tysięcznej. Dane w formacie *hh:mm:ss.msc* wskazują na konkretną godzinę w dobie, gdzie: *hh* – godziny, *mm* – minuty, *ss* – sekundy, *msc* – milisekundy.

Tabela 1

Przykładowe dane dla badania czasu konwergencji protokołów FHRP

Protokół	Licznik *hello* [s]	Licznik *hold down* [s]	Zgłoszenie sensora [hh:mm:ss.msc]	Aktywacja Routera 2 [hh:mm:ss.msc]
HSRP	3	10	16:16:49.466	16:16:49.760
	1	4	16:49:19.831	16:49:24.683
VRRP	3	9,992	21:21:30.765	21:21:40.713
	1	3,992	22:32:30.611	22:32:34.067
GLBP	3	10	14:37:51.547	14:37:52.714
	1	4	16:13:31.553	16:13:31.746

Źródło: opracowanie własne.

Czas przełączenia na router zastępczy mierzony jest od chwili zgłoszenia przez sensor śledzenia, że interfejs jest nieaktywny, do momentu uzyskania przez router zastępczy roli bramy domyślnej. Tabela 1 przedstawia przykładowe dane mierzone dla obu zestawów liczników, dla wszystkich protokołów. Kolumna *Zgłoszenie sensora* przedstawia godzinę, w której śledzony interfejs uległ awarii. Kolejna, *Aktywacja Routera 2*, oznacza godzinę, w której router zastępczy przejął rolę bramy domyślnej dla sieci lokalnej. Na postawie danych, których przykład został zaprezentowany w tabeli 1, można wyliczyć średni czas konwergencji dla testowej sieci komputerowej, który w tym przypadku oznacza średni czas

przełączania roli bramy domyślnej pomiędzy routerami, w zależności od wartościowania liczników. Wyniki zapisano w tabeli 2.

Tabela 2

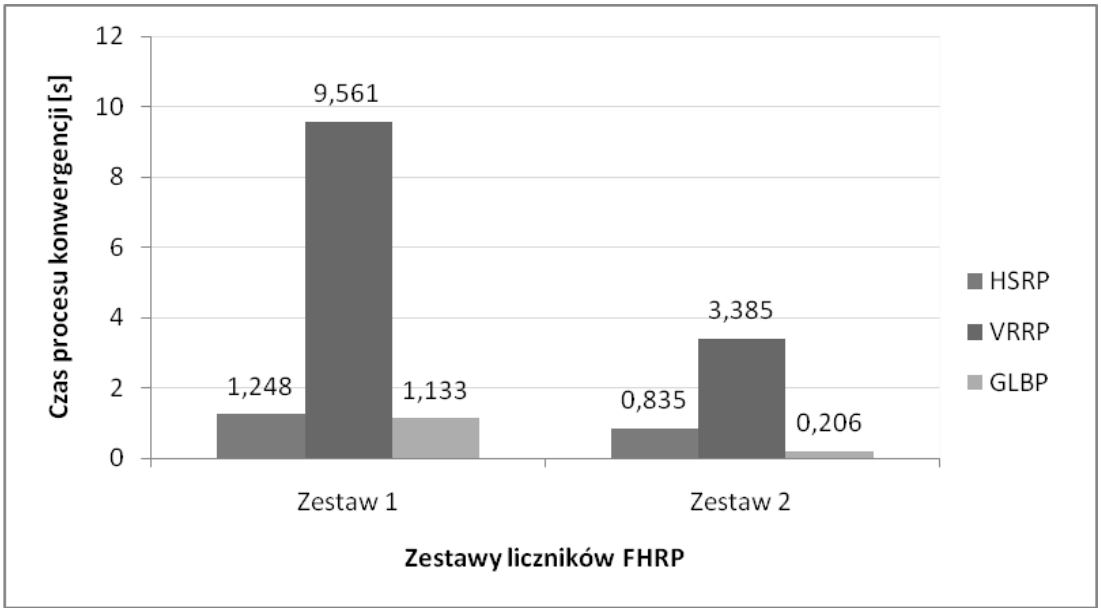
Wyniki badań czasu konwergencji dla protokołów FHRP

Protokół	Licznik *hello* [s]	Licznik *hold down* [s]	Średni czas przełączania routerów [s]
HSRP	3	10	1,248
	1	4	0,838
VRRP	3	9,992	9,561
	1	3,992	3,385
GLBP	3	10	1,133
	1	4	0,206

Źródło: opracowanie własne.

4. Podsumowanie

Porównanie średniego czasu przełączania routerów ilustruje rysunek 2. Na osi odciętych umieszczono kolejno dwa zestawy liczników opisanych szczegółowo w rozdziale 2. Czas procesu konwergencji, wyrażony w sekundach, zaznaczony jest na osi rzędnych.



Rys. 2. Czas procesu konwergencji protokołów FHRP w zależności od zestawów liczników
Fig. 2. Time of FHRP convergence based on sets of Times
Źródło: opracowanie własne.

Jak wynika z rysunku 2, przy każdym wartościowaniu zestawu liczników najgorzej wypada protokół VRRP. Jego czas konwergencji odpowiada w przybliżeniu licznikowi *hold down*, na którego podstawie, jako jedyny z badanych protokołów obsługiwał awarię zasymulowaną w artykule. Dla każdego z liczników *hello* można byłoby uzyskać w VRRP lepsze wartościowanie dla *hold down*, co nieznacznie poprawiłoby czasy konwergencji. Lepszy czas *hold down* można byłoby uzyskać, modyfikując priorytety routerów wchodzących w skład grupy VRRP. Uniemożliwiłoby to jednak sprawiedliwe porównanie protokołów. Zysk czasowy możliwy do osiągnięcia zawiera się w przedziale otwartym:

$$0 < x < y - 3 \cdot hello\,, \tag{2}$$

gdzie:
x – zysk czasowy dla zestawu,
hello – wartość licznika *hello* dla zestawu,
y – uzyskany wynik czasu konwergencji dla zestawu w badaniach opisanych w tabeli 2.

Protokół GLBP jest najlepszy dla przyjętego w artykule kryterium najkrótszego czasu procesu konwergencji. Jak wynika z przeprowadzonych badań, w przypadku usterek połączeń zewnętrznych, konwergencja jest zawsze krótsza niż zastosowany interwał wysyłania pakietów *hello*. Co więcej, przy konfiguracji domyślnej, w której stosowany jest algorytm karuzelowy Round-Robin [8], tylko $\frac{1}{n}$ urządzeń końcowych (gdzie n oznacza ilość routerów wchodzących w skład grupy GLBP i $n \leq 4$) dotkniętych zostaje skutkami awarii. Aby tak było w przypadku HSRP lub VRRP, zachodzi konieczność konfiguracji kilku równoczesnych grup, co nie jest tematem tej publikacji.

Bibliografia

1. Cisco Systems: Configuring Enhanced Object Tracking, https://www.cisco.com/en/US/docs/ios-xml/ios/ipapp/configuration/12-4t/ia p-eot.pdf.
2. Cisco Systems: Internetworking Technologies Handbook. Cisco Press, 2003, p. 64-76.
3. Cisco Systems: Gateway Load Balancing Protocol Overview. White Paper, http://www.cisco.com/en/US/prod/collateral/iosswrel/ ps6537/ps6550/prod_presentation0900aecd801790a3.pdf
4. Cole B., Li D., Li T., Morton P.: Cisco Hot Standby Router Protocol (HSRP). RFC 2281. IETF, 1998.
5. Higginson P., Hinden R., Hunt P., Knight S., Lindem A., Mitzel D., Shand M., Weaver D., Whipple D.: Virtual Router Redundancy Protocol. RFC 2338. IETF, 1998.

6. Hinden R., Ed.: Virtual Router Redundancy Protocol (VRRP). RFC 3768. IETF, 2004.
7. Nadas S., Ed.: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6. RFC 5798. IETF, 2010.
8. Tanenbaum A., Wetherall D.: Computer Networks. Prentice Hall, 2011, p. 282-465.
9. Teare D.: Implementing Cisco IP Routing (ROUTE). Foundation Learning Guide. Cisco Press, 2010, p. 25-30.

Abstract

Nowadays even the shortest outage during computer network operating is not acceptable because of the high-availability requirement of users, software and services. This paper describes the performance of mechanisms which are created to enhance network's reliability. It shows solution which provides the shortest network disruption within the first hop redundancy technique. First hop (default router) is a border router which is responsible for forwarding traffic outside the local segment. It provides survey of three protocols: HSRP, VRRP and GLBP. In this case the period of unavailability is associated with the time of the convergence process in which the network nodes agree on a coherent information about the networks which are used to forward traffic.