

## Redundancja w sieci LAN dla IP domyślnej bramy

Chciał bym przybliżyć w tym artykule w bardzo krótki sposób grupę protokołów, które umożliwiają redundancję dla bramy domyślnej skonfigurowanej na urządzeniach końcowych.

Protokoły te to:

**HSRP** – Hot Standby Router Protocol (Cisco proprietary)

**VRRP** – Virtual Router Redundancy Protocol (RFC3768)

**GLBP** – Global Load Balancing Protocol (Cisco proprietary)

Są to protokoły, które bardzo łatwo można skonfigurować w swojej sieci i zapewnić redundancję dla urządzenia, które posiada adres IP bramy domyślnej. Co ciekawe nie są to protokoły szeroko znane przez „samouków”, a moim zdaniem mogą być bardzo pomocne, bo oprócz redundancji można przy ich pomocy zapewnić load-balancing ruchu wychodzącego do Internetu poprzez kilka niezależnych łączy bez protokołu BGP.

Na początek krótkie wprowadzenie w problem redundancji bramy domyślnej. Weźmy na przykład komputer z systemem operacyjnym Windows. W konfiguracji IP możemy wprowadzić tylko jeden adres IP dla bramy domyślnej (routera, który zapewni nam połączenie z innymi podsieciami). W przypadku awarii tego routera nasz komputer nie będzie w stanie wysłać pakietów do podsieci innej niż jego własna. Pierwsza myśl, jaka się nasuwa to uruchomić protokół routingu dynamicznego pomiędzy naszym komputerem a kilkoma routerami, z których każdy będzie w stanie zapewnić redundancję dla routingu domyślnego. Pomysł dobry i wykonalny, ale niezbyt wygodny do zrealizowania, szczególnie gdy świadczymy usługę dostępu do Internetu dla „szarych” abonentów, którzy niekoniecznie muszą wiedzieć co to jest protokół routingu dynamicznego, do czego się go używa i jak go skonfigurować na swoim komputerze. Tutaj przychodzą nam właśnie z pomocą wspomniane wcześniej protokoły do zapewnienia redundancji bramy domyślnej. Wykorzystują one fakt, że w ramach jednej podsieci IP (także do domyślnej bramy) transmisja zawsze realizowana jest bezpośrednio przy użyciu adresów MAC. Najpierw host wykonuje mapowanie adresu IP za pomocą protokołu ARP na adres MAC, po czym tworzona jest ramka i transmitowana bezpośrednio do urządzenia docelowego. Możemy wykorzystać ten fakt do naszych celów. I znowu – najprostszym rozwiązaniem wydaje się przypisanie tego samego adresu MAC na dwóch różnych urządzeniach. Niestety w przypadku takiej konfiguracji problem będzie stwarzał switch. Switch przełącza ramki na podstawie docelowych adresów MAC. Informacje o tym, jaki adres MAC przypisany jest do jakiego portu przechowuje w tablicy przełączania. W tablicy tej jeden adres MAC może być przypisany tylko do jednego portu. W takim przypadku ruch przełączany będzie tylko do jednego urządzenia, którego – to zależy, które z nich jako ostatnie wysłało pakiet w kierunku switcha (aktualizacja tablicy przełączania na switchu realizowana jest w oparciu o źródłowy adres MAC przychodzącej ramki. Jeśli ten sam adres MAC pojawi się na innym porcie niż switch ma zapisane, stary wpis w tablicy przełączania jest kasowany, a w jego miejsce wprowadzany jest nowy). Protokoły redundancji bramy domyślnej stosują inną technikę, mianowicie tworzony jest wirtualny adres MAC oraz skojarzony z nim wirtualny adres IP. Para wirtualnych adresów może wędrować pomiędzy różnymi routerami, ale w jednym i tym samym czasie przypisana może być tylko do jednego z nich (HSRP oraz VRRP, GLBP działa troszkę inaczej). Tak więc konfigurujemy routery w taki sposób, aby dzieliły między sobą jeden adres MAC oraz skojarzony z nim adres IP, a na stacjach roboczych wskazany adres IP konfigurujemy jako adres IP domyślnej bramy.

Zanim zaczniemy konfigurację – na początek trochę informacji o protokole HSRP:

- Wirtualny adres IP z wirtualnym adresem MAC są przypisane zawsze do routera „Active”, który nadzoruje pracę całej grupy HSRP i jest wybierany na podstawie najwyższego priorytetu (domyślny priorytet ma wartość 100), jeśli priorytety wszystkich routerów w grupie są równe na podstawie najwyższego adresu IP,
- Routery, które są w stanie „Standby” nasłuchują komunikatów hello pochodzących od routera „Active”, które są rozsyłane standardowo co 3 sekundy. W przypadku gdy trzy kolejne pakiety nie

dotrą do celu – przyjmuje się że router „Active” uległ awarii. Wtedy spośród routerów „Standby” wybierany jest jeden, który przejmuje jego rolę i przejmuje na siebie wirtualną adresację (MAC oraz IP). Czas przełączenia to około 10s.

- Jeśli zajdzie taka sytuacja że router, który miał status „Active” i uległ awarii, a następnie został ponownie uruchomiony i pojawił się w sieci, to protokół HSRP domyślnie nie wykonuje przełączenia powrotnego. Znaczący to, że taki router po powrocie stanie się routerem „Standby” do czasu gdy aktywny router ulegnie awarii. Można jawnie skonfigurować, że życzymy sobie aby taki router stał się po powrocie znowu routerem „Active”. Do konfiguracji tej funkcjonalności służy polecenie „preempt”.

- Bardzo ciekawą funkcjonalnością jest możliwość śledzenia stanu interfejsów po stronie sieci WAN, bądź stanu wpisów w tablicy routingu. Jeśli ulegnie awarii łącze WAN, to pomimo, że router będzie widoczny od strony sieci LAN i będzie działał poprawnie, nie pozwoli nam na dostęp do Internetu, bo łącze WAN nie będzie funkcjonować. Protokół HSRP pozwala więc śledzić status łącza WAN i w przypadku jego awarii możliwe jest obniżenie priorytetu routera o wskazaną wartość, co spowoduje (w przypadku poprawnego ustawienia) wybór nowego routera „Active”, czyli przełączenie ruchu na router, który ma podłączone inne, sprawne łącze WAN.

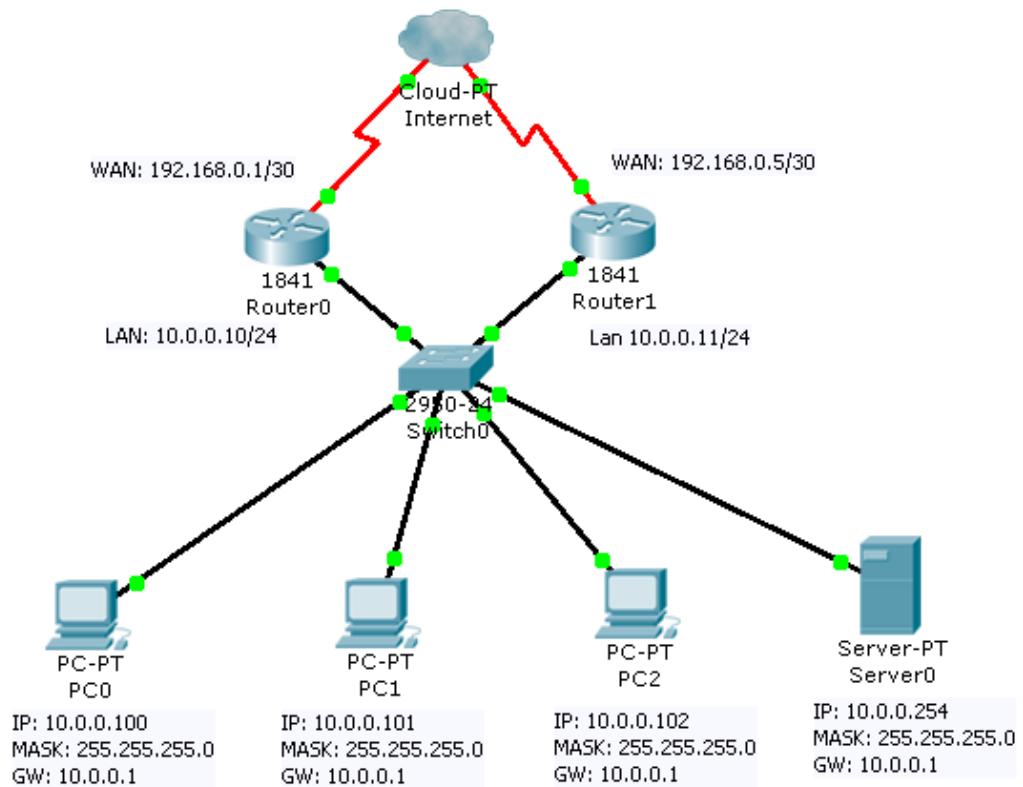
- Na pojedynczym interfejsie routera można skonfigurować maksymalnie do 255 grup HSRP. Jak się za chwile przekonamy może to mieć znaczenie w przypadku, gdy będziemy chcieli wykorzystać HSRP do load-balancingu.

- Wirtualne adresy MAC przypisane do protokołu HSRP, to 00:00:0C:07:AC:xx, gdzie xx to numer grupy HSRP zapisany w systemie szesnastkowym (stąd maksymalnie 255 możliwych do skonfigurowania grup HSRP).

- Wirtualny adres IP routera powinien być przyznany z tej samej podsieci co standardowy adres IP na interfejsie, ale musi być od niego różny.

- Można się zabezpieczyć przed nieautoryzowanym przekierowaniem ruchu przy pomocy autentykacji MD5 (key chain)

Ufff, to chyba wszystkie najważniejsze informacje. Poniżej przedstawiam przykładowy schemat sieci i przykładową konfigurację protokołu HSRP (przyznam się, że do stworzenia schematu sieci użyłem Cisco Packet Tracera, ale gdybyśmy chcieli poćwiczyć omawiane tutaj protokoły, to niestety nie pomoże on nam ☹, polecam GNS-a ☺):



Konfiguracja Router0:

```
track 10 interface Serial0/0 line-protocol
```

```
interface FastEthernet0/0
ip address 10.0.0.10 255.255.255.0
standby 1 ip 10.0.0.1
standby 1 priority 110
standby 1 preempt
standby 1 track 10 decrement 20
end
```

Konfiguracja Router1:

```
interface FastEthernet0/0
ip address 10.0.0.11 255.255.255.0
standby 1 ip 10.0.0.1
standby 1 preempt
end
```

Możemy sprawdzić, czy nasz protokół HSRP działa poprawnie śledząc logi na konsoli

```
*Mar 1 00:07:21.231: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
```

bądź wydając polecenie:

```
Router1#show standby
FastEthernet0/0 - Group 1
State is Standby
  1 state change, last state change 00:06:04
Virtual IP address is 10.0.0.1
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.480 secs
Preemption enabled
Active router is 10.0.0.10, priority 110 (expires in 7.248 sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Fa0/0-1" (default)
```

To cała konfiguracja. Jak widać nie jest wcale skomplikowana 😊 dodatkowo na routerze "Router0" dodane zostało śledzenie status interfejsu serial0/0. W przypadku awarii tego interfejsu router automatycznie zmniejszy swój priorytet o 20 (ze 110 na 90), wtedy „Router1” stanie się routerem „Active”, bo jego priorytet wynosi 100.

```
Router0#conf t
Router0(config)#int s0/0
Router0(config-if)#shutdown
```

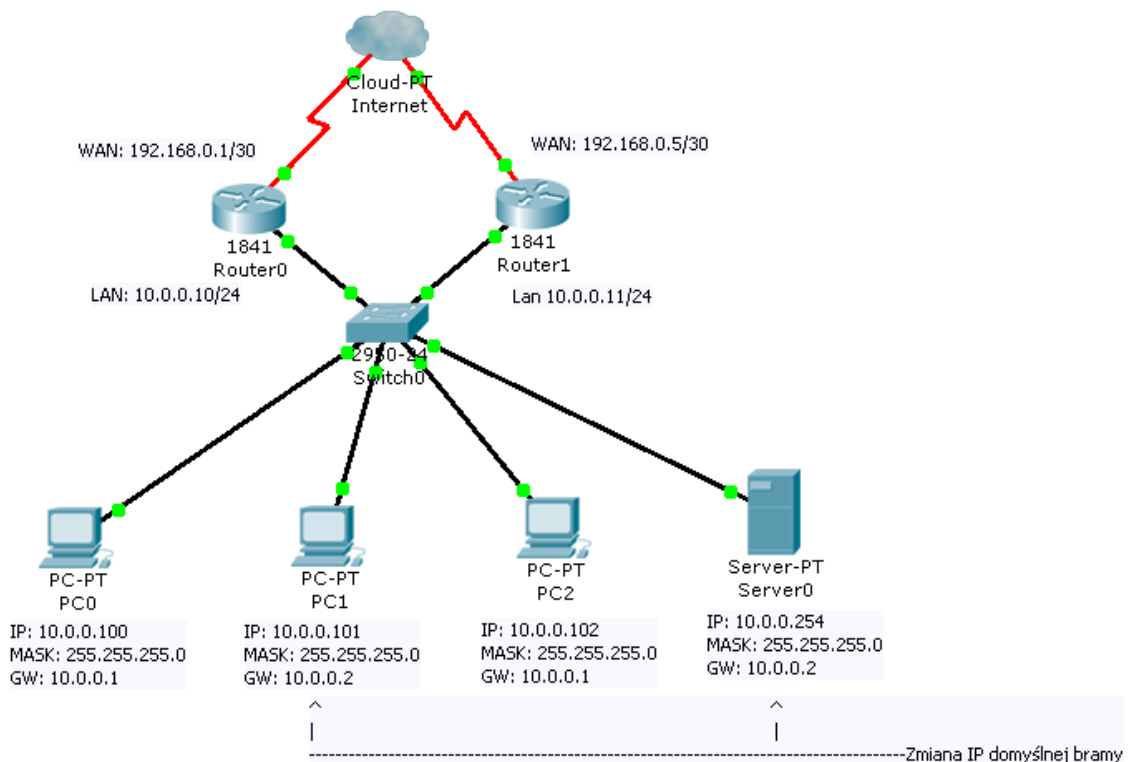
```
*Mar 1 00:16:45.443: %TRACKING-5-STATE: 10 interface Se0/0 line-protocol Up->Down
*Mar 1 00:16:45.671: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:16:45.831: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Active -> Speak
*Mar 1 00:16:47.443: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively
down
*Mar 1 00:16:48.443: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state
to down
*Mar 1 00:16:55.827: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Speak -> Standby
```

A na "Router1" mamy:

```
*Mar 1 00:16:46.763: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Active
```

Jest to zabezpieczenie na wypadek awarii łącza WAN.

Teraz przykład konfiguracji HSRP z „pseudo” load-balancingiem. Na początek schemat sieci:



Sieć wygląda identycznie, tylko proszę zwrócić uwagę na fakt, że na części hostów został ustawiony IP domyślnej bramy na 10.0.0.1, natomiast na pozostałych 10.0.0.2. Jest to bardzo ważne. Teraz konfiguracja naszych routerów:

Konfiguracja Router0:

```
track 10 interface Serial0/0 line-protocol
```

```
interface FastEthernet0/0
 ip address 10.0.0.10 255.255.255.0
 standby 1 ip 10.0.0.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 10 decrement 20
 standby 2 ip 10.0.0.2
 standby 2 preempt
 end
```

Konfiguracja Router1:

```
track 10 interface Serial0/0 line-protocol
```

```
interface FastEthernet0/0
 ip address 10.0.0.11 255.255.255.0
 standby 1 ip 10.0.0.1
 standby 1 preempt
```

```
standby 2 ip 10.0.0.2
standby 2 priority 110
standby 2 preempt
standby 2 track 10 decrement 20
end
```

Proszę zwrócić uwagę na to, że na jednym interfejsie mamy skonfigurowane dwie grupy HSRP. Grupa 1 jako router „Active” ze względu na priorytet wybierze Router0, natomiast grupa 2 jako „Active” wybierze Router1. Tak więc hosty, które mają ustawioną domyślną bramę na IP 10.0.0.1 będą wychodzić domyślnie przez Router0, a hosty, które mają ustawioną domyślną bramę na IP 10.0.0.2 będą wychodzić domyślnie przez Router1. Tak więc osiągniemy pewnego rodzaju load-balancing. Dodatkowo, jeśli któreś łącze WAN, bądź któryś router ulegnie awarii, wszystkie hosty zostaną przełączone na router, który jeszcze pracuje.

```
Router0#sh standby
FastEthernet0/0 - Group 1
State is Active
  5 state changes, last state change 00:07:49
Virtual IP address is 10.0.0.1
Active virtual MAC address is 0000.0c07.ac01
  Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.264 secs
Preemption enabled
Active router is local
Standby router is 10.0.0.11, priority 100 (expires in 8.720 sec)
Priority 110 (configured 110)
  Track object 10 state Up decrement 20
Group name is "hsrp-Fa0/0-1" (default)
FastEthernet0/0 - Group 2
State is Standby
  4 state changes, last state change 00:06:10
Virtual IP address is 10.0.0.2
Active virtual MAC address is 0000.0c07.ac02
  Local virtual MAC address is 0000.0c07.ac02 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.248 secs
Preemption enabled
Active router is 10.0.0.11, priority 110 (expires in 8.076 sec)
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Fa0/0-2" (default)
```

Oczywiście w ramach protokołu HSRP można budować redundancje używając więcej niż tylko dwóch routerów, pamiętajmy jednak, że tylko jeden z nich może być routerem „Active” w ramach jednej grupy HSRP. Dzięki takiej konfiguracji nasi użytkownicy będą mieli nieprzerwany dostęp do Internetu nawet w przypadku awarii, natomiast my będziemy mieć spokojny sen ☺. Trochę problemu może przysporzyć rozkładanie ruchu poprzez przydzielanie ręczne użytkowników do korzystania z jednej bądź drugiej domyślnej bramy, ale na szczęście problem ten został już rozwiązany w protokole GLBP, ale zanim do niego przejdziemy, krótki opis VRRP.

HSRP to standard Cisco, nie można go więc spotkać poza routerami Cisco. VRRP to otwarty protokół opisany w RFC3768, który jest odpowiednikiem HSRP, ale troszkę się od niego różni, poniżej podstawowe różnice:

- VRRP używa innego zakresu wirtualnych adresów MAC: 00:00:5E:00:01:xx, gdzie xx to numer grupy VRRP. Przyznam też że jestem tutaj nieco w kropce. Każde ze źródeł, które wyszukałem opisuje ten adres MAC jako adres multicastowy, podczas gdy te same źródła definiują adresy multicastowe jako adresy, które mają najmłodszy bit pierwszego bajtu ustawiony na „1”, tak zwany I/G bit (Individual=0, Group=1). Przykładowe źródło, które tutaj cytuję to: „**CCIE Routing and Switching Certification Guide**” Fourth Edition, Wendell Odom, Rus Healy, Denise Donohue. Muszę jeszcze trochę głębiej poszperać ☺ I temat zgłębić.
- VRRP używa innego mechanizmu na śledzenie status interfejsów,
- VRRP domyślnie ma włączone „preemption”, podczas, gdy HSRP nie.
- VRRP używa innych terminów na określenie routera aktywnego („Master”), niż HSRP („Active”).
- W przypadku VRRP wirtualny adres IP, to fizyczny adres IP jednego z routerów.

Przykładowa konfiguracja równoważna konfiguracji z pierwszego przykładu z HSRP:

Konfiguracja Router0:

```
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 vrrp 1 ip 10.0.0.1
 vrrp 1 priority 110
end
```

Konfiguracja Router1:

```
interface FastEthernet0/0
 ip address 10.0.0.11 255.255.255.0
 vrrp 1 ip 10.0.0.1
end
```

O tym, że VRRP działa można się przekonać śledząc logi z konsoli obu routerów,

```
*Mar 1 00:57:56.687: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Init -> Master
```

```
*Mar 1 00:58:08.403: %VRRP-6-STATECHANGE: Fa0/0 Grp 1 state Init -> Backup
```

Bądź wydając stosowne polecenie.

```
Router0#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 10.0.0.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255
  Master Router is 10.0.0.10 (local), priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec
```

Jeszcze uwaga dotycząca priorytetów. Router, którego adres IP jest używany jako wirtualny adres IP domyślnie otrzymuje priorytet 255, pozostałe routery mają domyślny priorytet 100. No i jeszcze jedna mała niespodzianka:

```
track 10 interface Serial0/0 line-protocol
```

```
Router0#conf t
Router0(config-if)#vrrp 1 track 10 decrement 20
% tracking not supported on IP address owner
```

Należy niestety zastosować inne sposoby na śledzenie status interfejsów.

Na koniec został nam do omówienia ostatni z protokołów redundancji domyślnej bramy: GLBP. Jest to tak jak HSRP rozwiązanie firmowe Cisco. W stosunku do HSRP zasadniczo różni się tym, że potrafi automatycznie realizować load-balancing, ale po kolei:

- load-balancing może być realizowany na maksymalnie cztery routery w ramach jednej grupy GLBP.
- W przypadku GLBP wszystkie routery uczestniczą w przekazywaniu ruchu. Zarządza nimi „GLBP Active Virtual Gateway (AVG). Każdy z routerów otrzymuje swój unikalny wirtualny adres MAC, inaczej niż w HSRP i VRRP, gdzie tylko jeden (aktywny) z routerów dysponuje wirtualnymi adresami MAC + IP. Natomiast nadzorcą jest AVG. Nadzorca wybierany jest na podobnych zasadach jak w HSRP. Do zadań nadzorca (i tylko nadzorca) należy odpowiadanie na zapytania ARP. W odpowiedziach na zapytanie ARP dotyczące adresu MAC domyślnej bramy AVG podaje na przemian adresy MAC wszystkich aktywnych routerów w ramach grupy GLBP. Powoduje to sytuacje, kiedy różne komputery klientów w odpowiedzi na zapytanie ARP o MAC domyślnej bramy otrzymują różne odpowiedzi, pomimo, że IP domyślnej bramy jest takie samo.
- Wirtualne adresy MAC związane z GLBP to 00:07:B4:00:xx:yy gdzie xx to numer grupy GLBP natomiast yy to numer routera w ramach grupy.
- Cisco pozwala na konfiguracje do 1024 grup GLBP w ramach fizycznego interfejsu i do 4 routerów w ramach jednej grupy.

W przypadku, gdy jeden z routerów w ramach grupy GLBP ulega awarii, jego wirtualny adres MAC jest przejmowany przez AVG, a odpowiedzi na zapytania ARP przestają go uwzględniać. Jeśli awarii ulegnie router AVG, w jego miejsce wybierany jest nowy AVG, który przejmuje MAC poprzednika (obsługując jednocześnie swój, poprzednio przydzielony).  
Pozostaje jeszcze przykład konfiguracji:

Konfiguracja Router0:

```
track 10 interface Serial0/0 line-protocol
```

```
interface FastEthernet0/0
ip address 10.0.0.10 255.255.255.0
glbp 1 ip 10.0.0.1
glbp 1 priority 110
glbp 1 preempt
glbp 1 weighting track 10 decrement 20
end
```



Konfiguracja Router1:

```
interface FastEthernet0/0
ip address 10.0.0.11 255.255.255.0
glbp 1 ip 10.0.0.1
end
```

start GLBP w logach routerów widać następująco:

```
*Mar 1 01:20:10.687: %GLBP-6-STATECHANGE: FastEthernet0/0 Grp 1 state Standby -> Activera
*Mar 1 01:20:20.687: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 1 state Listen ->
Activepre
```

```
*Mar 1 01:20:26.459: %GLBP-6-FWDSTATECHANGE: FastEthernet0/0 Grp 1 Fwd 2 state Listen ->
Active
```

```
Router0#show glbp
FastEthernet0/0 - Group 1
State is Active
  2 state changes, last state change 00:03:52
Virtual IP address is 10.0.0.1
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.736 secs
Redirect time 600 sec, forwarder timeout 14400 sec
Preemption enabled, min delay 0 sec
Active is local
Standby is 10.0.0.11, priority 100 (expires in 7.844 sec)
Priority 110 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
  Track object 10 state Up decrement 20
Load balancing: round-robin
Group members:
  c000.1a38.0000 (10.0.0.10) local
  c001.1a38.0000 (10.0.0.11)
There are 2 forwarders (1 active)
Forwarder 1
State is Active
  1 state change, last state change 00:03:42
MAC address is 0007.b400.0101 (default)
Owner ID is c000.1a38.0000
Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100
Forwarder 2
State is Listen
MAC address is 0007.b400.0102 (learnt)
Owner ID is c001.1a38.0000
Redirection enabled, 599.268 sec remaining (maximum 600 sec)
Time to live: 14399.264 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 10.0.0.11 (primary), weighting 100 (expires in 9.260 sec)
```

Jak widać możliwości konfiguracyjnych mamy bez liku – o ile wybraliśmy sprzęt Cisco 😊 jeśli nie – pozostaje nam tylko VRRP.

A mnie pozostaje tylko życzyć wszystkim spokojnego snu, gdy HSRP, VRRP lub GLBP będzie pracować za nas.

Paweł Kucharczyk

