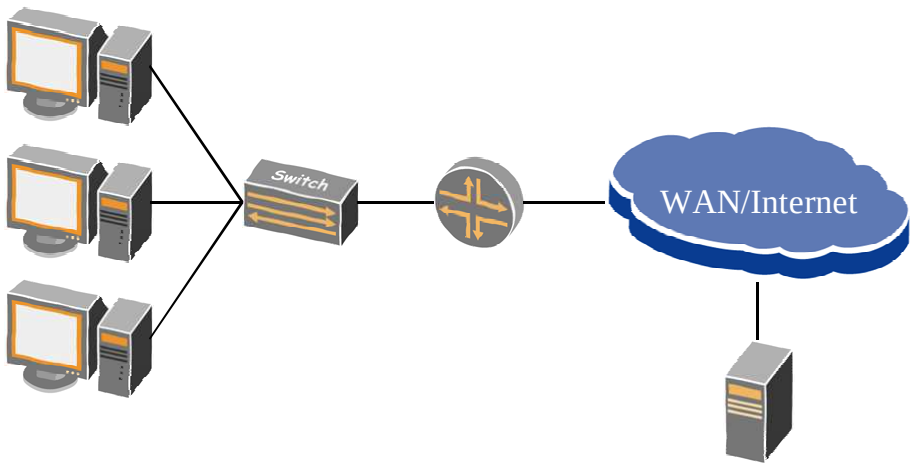
Zapewnianie niezawodności w sieciach IP – problem bramy domyślnej

1. Wstęp

W przetwarzaniu informacji w systemach teleinformatycznych kładzie się obecnie duży nacisk na bezpieczeństwo. Jedną z kluczowych kwestii związanych z bezpieczeństwem jest dostępność – zapewnienie możliwości przetwarzania informacji zgromadzonej w systemie, zgodnie z wymaganiami użytkownika. Współczesne systemy i sieci komputerowe buduje się w oparciu o wiele różnych urządzeń. Projektując sieć komputerową pod kątem zapewnienia ciągłości działania – a więc dostępności – należy starać się uwzględnić parametry niezawodności w każdej warstwie modelu odniesienia ISO/OSI. Przedstawimy metody zabezpieczania dostępności z zastosowaniem mechanizmów dostępnych w warstwie sieciowej (L3 – Network) – rozwiązanie problemu zapewnienia dostępu do bramy domyślnej.

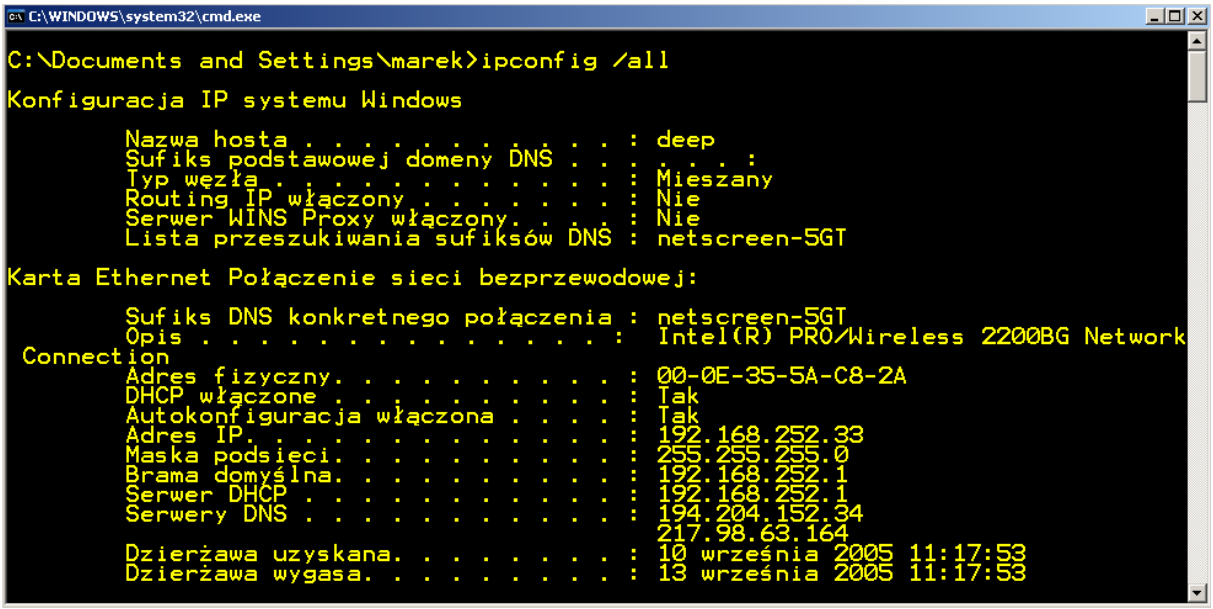
2. Konfiguracja parametrów sieciowych stacji

W przykładowej sieci (rys. 1) mamy komputery, które podłączone są za pomocą kart sieciowych do przełącznika warstwy 2. Przełącznik podłączony jest do routera, który umożliwia komunikację z innymi sieciami, w tym na przykład z Internetem.



Rysunek 1 Przykładowa sieć komputerowa

Stacje w sieci muszą mieć skonfigurowany adres IP, oraz w celu komunikacji z innymi sieciami – adres bramy do tej sieci lub też adres bramy domyślnej, która służy do komunikacji ze wszystkimi sieciami, poza własną. Przykładowa konfiguracja parametrów sieciowych stacji jest przedstawiona na rysunku 2.



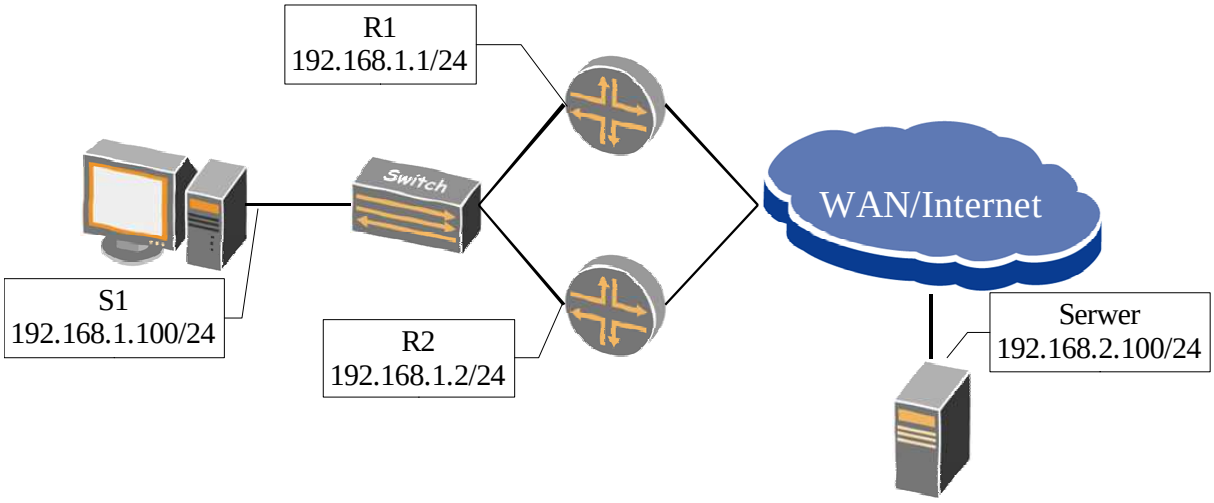
Rysunek 2 Konfiguracja stacji w sieci

W sieci o adresie 192.168.252.0/24 stacje będą porozumiewały się bez pośrednictwa bramy. Gdy jednak zajdzie potrzeba dostępu do stacji o innym adresie, ruch zostanie skierowany do bramy domyślnej. Metod wyboru bramy domyślnej i zapewnienia do niej dostępu jest wiele. Można na każdej stacji w sieci uruchomić instancję protokołu routingu dynamicznego – większość współczesnych systemów operacyjnych (Unix, Windows 2k, 2k3) jest wyposażona w narzędzia obsługujące na przykład takie protokoły IGP, jak RIP i OSPF. Jednakże uruchomienie routingu dynamicznego wiąże się z dodatkowym obciążeniem zasobów komputera, jak również z nakładem pracy osób obsługujących system informatyczny. Można również zastosować inne mechanizmy, które nie wymagają ani dodatkowych zasobów, ani specjalnego nakładu pracy administracyjnej związanej z konfiguracją każdej ze stacji.

3. Proxy ARP

ARP czyli Adress Resolution Protocol jest jednym z podstawowych mechanizmów używanych w sieci IP. Protokół ten umożliwia przypisanie adresu fizycznego warstwy 2 do adresu IP. Mechanizmy działania tego protokołu opisane są w dokumencie RFC826. Gdy stacja w sieci chce się skomunikować z inną stacją, wysyła zapytanie do wszystkich

odbiorców znajdujących się w danej sieci – *Kto ma adres IP XXX.YYY.ZZZ.TTT?* Stacja która ma nadany taki adres, odpowiada i komunikacja może zostać nawiązana. Gdy odpowiedzi nie ma, to oczywiście połączenia nawiązać się nie da. Środowisko, w którym demonstrowane będą wszystkie przykłady, przedstawione jest na rysunku 3.



Rysunek 3 Sieć testowa - konfiguracja

Korzystając z tego mechanizmu można pytać o wszystkie stacje – wtedy odpowiadać musiałaby brama, która ma dostęp do stacji spoza konkretnej sieci lokalnej. Mechanizm ten nosi nazwę Proxy ARP i opisany jest w dokumencie RFC1027. W celu uruchomienia mechanizmu Proxy ARP na stacji, należy ustawić adres bramy domyślnej taki sam, jak adres interfejsu, z którego brama jest osiągalna.

```
[root@webdallas ~]# ip route add default via 192.168.1.100
[root@webdallas ~]# ip route
192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.100
default via 192.168.1.100 dev eth1
```

Przykład 1 Ustawienie trasy domyślnej

Gdy jednak spróbujemy osiągnąć serwer w innej sieci, nie uzyskamy odpowiedzi. Można za pomocą narzędzia `tcpdump` zaobserwować zachowanie stosu protokołów. Po wydaniu polecenia `ping` 192.168.2.100 komputer wysyła do wszystkich stacji w podsieci zapytanie ARP o stację, która ma adres 192.168.2.100 – jednakże w sieci nie ma takiego komputera – w końcu to sieć o adresie 192.168.1.0/24, a zapytanie jest o stację z sieci 192.168.2.0. W tablicy przypisań adresów sprzętowych do adresów IP (tablica ARP) adres 192.168.2.100 jest oznaczony jako niekompletny (*incomplete).*

```
[root@webdallas ~]# ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
From 192.168.1.100 icmp_seq=1 Destination Host Unreachable
From 192.168.1.100 icmp_seq=2 Destination Host Unreachable
From 192.168.1.100 icmp_seq=3 Destination Host Unreachable

--- 192.168.2.100 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss, time 5000ms

[root@webdallas ~]# tcpdump -vvni eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
10:46:22.238486 arp who-has 192.168.2.100 tell 192.168.1.100
10:46:23.238327 arp who-has 192.168.2.100 tell 192.168.1.100
10:46:24.238176 arp who-has 192.168.2.100 tell 192.168.1.100

[root@webdallas ~]# arp -en
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.2              ether   00:05:85:C3:11:D0   C                     eth1
192.168.1.1              ether   00:05:85:CA:0C:D0   C                     eth1
192.168.2.100                    (incomplete)                              eth1
```

Przykład 2 Próba połączenia bez włączonego Proxy ARP na bramach

Aby zapewnić komunikację należy włączyć mechanizm Proxy ARP na bramie w sieci lokalnej. Po włączeniu Proxy ARP na routerach R1 oraz R2 komunikacja od razu zachodzi. Można zaobserwować odpowiedź na icmp echo request (ping).

```
[root@webdallas ~]# ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=0 ttl=63 time=8.18 ms
64 bytes from 192.168.2.100: icmp_seq=1 ttl=63 time=2.22 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=63 time=2.21 ms

--- 192.168.2.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 2.211/4.206/8.181/2.811 ms, pipe 2


[root@webdallas ~]# tcpdump -vvnei eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
12:27:47.057465 00:01:02:e2:6d:d6 > Broadcast, ethertype ARP (0x0806), length 42:
arp who-has 192.168.2.100 tell 192.168.1.100
12:27:47.063363 00:05:85:c3:11:d0 > 00:01:02:e2:6d:d6, ethertype ARP (0x0806),
length 60: arp reply 192.168.2.100 is-at 00:05:85:c3:11:d0
12:27:47.063399 00:01:02:e2:6d:d6 > 00:05:85:c3:11:d0, ethertype IPv4 (0x0800),
length 98: IP (tos 0x0, ttl  64, id 0, offset 0, flags [DF], proto 1, length: 84)
192.168.1.100 > 192.168.2.100: icmp 64: echo request seq 0
12:27:47.065519 00:05:85:c3:11:d0 > 00:01:02:e2:6d:d6, ethertype IPv4 (0x0800),
length 98: IP (tos 0x0, ttl  63, id 57967, offset 0, flags [none], proto 1, length:
84) 192.168.2.100 > 192.168.1.100: icmp 64: echo reply seq 0

[root@webdallas ~]# arp -en
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:05:85:CA:0C:D0   C                     eth1
192.168.1.2              ether   00:05:85:C3:11:D0   C                     eth1
192.168.2.100            ether   00:05:85:C3:11:D0   C                     eth1
```

Przykład 3 Próba połączenia z włączonym Proxy ARP na bramach

Komputer ma w swojej tablicy ARP jako adres zdalnej stacji 192.168.2.100 adres bramy R2 (192.168.1.2) – wobec tego cała komunikacja do sieci odległych będzie przechodziła przez tę właśnie bramę. Włączenie mechanizmów Proxy ARP w routerach Juniper Networks odbywa się per interfejs logiczny.

```
[edit]
root@R1# show interfaces fe-0/0/0
unit 0 {
    proxy-arp;
    family inet {
        address 192.168.1.1/24;
    }
}

[edit]

root@R2# show interfaces fe-0/0/0
unit 0 {
    proxy-arp;
    family inet {
        address 192.168.1.2/24;
    }
}
```

Przykład 4 Ustawienie Proxy ARP na bramach

Mechanizm ten zapewnia również wysoką dostępność bramy domyślnej – w przypadku awarii jednego z routerów ruch będzie przekierowywany przez drugi router. Po odpięciu interfejsu routera R2 przez pewien czas nie ma komunikacji.

```
[root@webdallas ~]# ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
64 bytes from 192.168.2.100: icmp_seq=8 ttl=63 time=37.9 ms
64 bytes from 192.168.2.100: icmp_seq=9 ttl=63 time=2.05 ms

--- 192.168.2.100 ping statistics ---
12 packets transmitted, 4 received, 66% packet loss, time 11001ms
rtt min/avg/max/mdev = 2.053/11.162/37.992/15.490 ms, pipe 2


[root@webdallas ~]# tcpdump -vvnei eth1
11:59:10.429448 00:01:02:e2:6d:d6 > 00:05:85:c3:11:d0, ethertype IPv4 (0x0800),
length 98: IP (tos 0x0, ttl  64, id 7, offset 0, flags [DF], proto 1, length: 84)
192.168.1.100 > 192.168.2.100: icmp 64: echo request seq 7
11:59:11.430260 00:01:02:e2:6d:d6 > Broadcast, ethertype ARP (0x0806), length 42:
arp who-has 192.168.2.100 tell 192.168.1.100
11:59:11.464968 00:05:85:ca:0c:d0 > 00:01:02:e2:6d:d6, ethertype ARP (0x0806),
length 60: arp reply 192.168.2.100 is-at 00:05:85:ca:0c:d0
11:59:11.465001 00:01:02:e2:6d:d6 > 00:05:85:ca:0c:d0, ethertype IPv4 (0x0800),
length 98: IP (tos 0x0, ttl  64, id 8, offset 0, flags [DF], proto 1, length: 84)
192.168.1.100 > 192.168.2.100: icmp 64: echo request seq 8
11:59:11.467259 00:05:85:ca:0c:d0 > 00:01:02:e2:6d:d6, ethertype IPv4 (0x0800),
length 98: IP (tos 0x0, ttl  63, id 39547, offset 0, flags [none], proto 1, length:
84) 192.168.2.100 > 192.168.1.100: icmp 64: echo reply seq 8


[root@webdallas ~]# arp -en
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.2              ether   00:05:85:C3:11:D0   C                     eth1
192.168.1.1              ether   00:05:85:CA:0C:D0   C                     eth1
192.168.2.100            ether   00:05:85:CA:0C:D0   C                     eth1
```

Przykład 5 Uszkodzenie routera R2 – przełączenie na R1

Czas ten jest potrzebny na usunięcie przez system operacyjny wpisu z tablicy ARP, przyporządkowującego adresowi IP zdalnej stacji adres MAC routera R2.

Proxy ARP ma jednak poważną wadę w zakresie zapewniania wysokiej dostępności – czas przebudowy topologii (czas zbieżności) jest dosyć długi. Związane to jest z czasem okresowego opróżniania tabeli ARP na stacjach. Na ogół czas ten wynosi kilka minut. Można oczywiście w konfiguracji systemu operacyjnego czas ten zmniejszyć, jednakże będzie to powodować konieczność częstego odpytywania ARP, co generuje dodatkowy ruch w sieci. Jednakże jest to mechanizm bardzo prosty w implementacji i dostępny praktycznie na wszystkich znanych platformach.

4. ICMP Router Discovery Protocol (*IRDP*)

IRDP jest mechanizmem, który umożliwia bramom rozgłaszanie informacji przeznaczonej dla stacji w danym segmencie sieci – informacji o bramie domyślnej. Każda z bram, która ma uruchomioną instancję protokołu IRDP wysyła do grupy multikastowej 224.0.0.1 (wszystkie stacje w danym segmencie) informację o adresie bramy domyślnej. Administrator ma możliwość skonfigurowania preferencji konkretnej trasy oraz czasu życia informacji o tej trasie. Większość współczesnych systemów operacyjnych zapewnia wsparcie dla protokołu IRDP. Konfiguracja wspomnianych mechanizmów w routerach Juniper Networks wygląda następująco:

```
[edit]
root@R1# show protocols
router-discovery {
    interface fe-0/0/0.0 {
        lifetime 900;
    }
    address 192.168.1.1 {
        advertise;
        priority 50;
    }
}


[edit]
root@R2# show protocols
router-discovery {
    interface fe-0/0/0.0 {
        lifetime 900;
    }
    address 192.168.1.2 {
        advertise;
        priority 100;
    }
}
```

Przykład 6 IRDP – konfiguracja R1 oraz R2

Po uruchomieniu IRDP routery R1 oraz R2 będą rozgłaszać okresowo informację o dostępności tras domyślnych, odpowiednio przez adres 192.168.1.1 z priorytetem 50 oraz przez adres 192.168.1.2 z priorytetem 100. Czas życia każdej z informacji o trasie domyślnej został ustawiony na 900 sekund (15 minut) wobec domyślnego ustawienia na 30 minut (zgodnie z RFC). Po uruchomieniu na stacji narzędzia odpowiedzialnego za obsługę protokołu IRDP (w systemach typu unix program rdisc) można wymusić wysłanie przez routery informacji o trasach. Komunikat z żądaniem jest wysyłany przez stację do grupy multikastowej 224.0.0.2 (wszystkie routery w danym segmencie).

```
[root@webdallas ~]# rdisc -svt
Sending solicitation to 224.0.0.2
ICMP Router Advertise from 192.168.1.2, lifetime 900
        address 192.168.1.2, preference 0x64
ICMP Router Advertise from 192.168.1.1, lifetime 900
        address 192.168.1.1, preference 0x32

[root@webdallas ~]# tcpdump -vvni eth1
tcpdump: listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
13:34:33.659680 IP (tos 0x0, ttl   1, id 2, offset 0, flags [DF], proto 1, length:
28) 192.168.1.100 > 224.0.0.2: icmp 8: router solicitation
13:34:35.681055 IP (tos 0x0, ttl   1, id 49116, offset 0, flags [none], proto 1,
length: 36) 192.168.1.2 > 192.168.1.100: icmp 16: router advertisement lifetime
15:00 1: {192.168.1.2 100}
13:34:35.694907 IP (tos 0x0, ttl   1, id 25836, offset 0, flags [none], proto 1,
length: 36) 192.168.1.1 > 192.168.1.100: icmp 16: router advertisement lifetime
15:00 1: {192.168.1.1 50}

[root@webdallas ~]# ip route
192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.100
default via 192.168.1.2 dev eth1

root@webdallas ~]# ip ro get 192.168.2.0/24
192.168.2.0 via 192.168.1.2 dev eth1  src 192.168.1.100
    cache  mtu 1500 advmss 1460 metric10 64

Po awarii R2

[root@webdallas ~]# rdisc -tv
ICMP Router Advertise from 192.168.1.1, lifetime 0
        address 192.168.1.1, preference 0x32

[root@webdallas ~]# ip route
192.168.1.0/24 dev eth1  proto kernel  scope link  src 192.168.1.100
default via 192.168.1.1 dev eth1
default via 192.168.1.2 dev eth1

[root@webdallas ~]# ip ro get 192.168.2.0/24
192.168.2.0 via 192.168.1.1 dev eth1  src 192.168.1.100
    cache  mtu 1500 advmss 1460 metric10 64
```

Przykład 7 Funkcjonowanie IRDP

Wybrana została trasa preferowana, przez router 192.168.1.2 – w przypadku jego awarii po pewnym czasie w tablicy routingu stacji zostanie zainstalowana trasa pochodząca od

pozostałego, funkcjonującego routera. Wadą protokołu IRDP, podobnie jak w przypadku Proxy ARP jest bardzo długi czas konwergencji sieci.

5. Virtual Router Redundancy Protocol (*VRRP*)

VRRP jest odmienną od przedstawionych powyżej koncepcją zapewnienia dostępu do bramy domyślnej i jest opisany szczegółowo w dokumencie RFC3768. Tworzony jest jeden lub wiele wirtualnych routerów (do 255), widocznych w danym segmencie sieci lokalnej. Każdemu z routerów wirtualnych (grupie VRRP) jest przypisany wirtualny adres IP (obsługiwany jest na razie tylko Ipv4) oraz odpowiedni adres MAC. Adres ten ma zawsze postać **00-00-5E-00-01-GG**, gdzie **GG** to numer grupy VRRP (numer routera wirtualnego). VRRP używa do komunikacji protokołu IP 112 oraz grupy multikastowej 224.0.0.18. Charakterystyczne jest ustawienie pola TTL w nagłówku datagramu IP na 255. Wśród routerów należących do danej grupy wybierany jest jeden, który będzie uczestniczył w przekazywaniu ruchu (Master). Pozostałe routery w grupie pełnią funkcję urządzeń zapasowych (Backup). Router Master wysyła okresowo informacje o swoim stanie. W przypadku jego awarii, co objawiać się będzie brakiem informacji, jeden z routerów zapasowych przejmie jego rolę w przekazywaniu ruchu. Wybór routera Master odbywa się w drodze negocjacji pomiędzy członkami danej grupy. Uruchomienie podstawowej konfiguracji VRRP w routerach Juniper Networks odbywa się per adres IP przypisany do interfejsu logicznego.

```
[edit]
root@R1# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.1/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
            }
        }
    }
}

[edit]
root@R2# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.2/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
            }
        }
    }
}
```

Przykład 8 VRRP – konfiguracja podstawowa R1 oraz R2

Po zatwierdzeniu konfiguracji można sprawdzić, który router ma status Master oraz jak wyglądają komunikaty VRRP.

```
root@R1# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           backup     D 2.994
                         vip   192.168.1.254
                         mas   192.168.1.2

root@R2# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.2      up           master     A 0.934
                         vip   192.168.1.254


[root@webdallas ~]# tcpdump -vvni eth1
14:01:41.560677 IP (tos 0xc0, ttl 255, id 5278, offset 0, flags [none], proto 112,
length: 40) 192.168.1.2 > 224.0.0.18: VRRPv2, Advertisement, vrid 100, prio 100,
authtype none, intvl 1s, length 20, addrs: 192.168.1.254
14:01:42.770511 IP (tos 0xc0, ttl 255, id 5280, offset 0, flags [none], proto 112,
length: 40) 192.168.1.2 > 224.0.0.18: VRRPv2, Advertisement, vrid 100, prio 100,
authtype none, intvl 1s, length 20, addrs: 192.168.1.254

W przypadku awarii R2

root@R1# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           master     A 0.576
                         vip   192.168.1.254
```

Przykład 9 VRRP – status R1 oraz R2 oraz

Routerem Master jest R2, który co jedną sekundę wysyła informację o stanie do pozostałych routerów w grupie VRRP. Po awarii R2 rolę routera aktywnego przejmuje R1.

VRRP ma wiele zaawansowanych funkcjonalności. Jedną z nich jest możliwość zabezpieczenia się przed błędem administratora polegającym na podpięciu wadliwie skonfigurowanego routera. Służy do tego mechanizm uwierzytelniania członków grupy.

```
[edit]
root@R1# show interfaces
fe-0/0/0 {
    unit 0 {
        family inet {
            address 192.168.1.1/24 {
                vrrp-group 100 {
                    virtual-address 192.168.1.254;
                    authentication-type simple;
                    authentication-key "$9$kPfzOBEcyK5Q1h"; ## SECRET-DATA
                }
            }
        }
    }
}
```

Przykład 10 VRRP – konfigurowanie prostego uwierzytelnienia

Po zdefiniowaniu uwierzytelnienia na R1 należy taką samą operację przeprowadzić dla pozostałych członków grupy. W przeciwnym razie VRRP nie będzie funkcjonować poprawnie.

```
root@webdallas ~]# tcpdump -vvni eth1
14:11:35.300004 IP (tos 0xc0, ttl 255, id 904, offset 0, flags [none], proto 112,
length: 40) 192.168.1.1 > 224.0.0.18: VRRPv2, Advertisement, vrid 100, prio 100,
authtype simple, intvl 1s, length 20, addrs: 192.168.1.254 auth "clico^@^@^@"
14:11:35.578398 IP (tos 0xc0, ttl 255, id 6101, offset 0, flags [none], proto 112,
length: 40) 192.168.1.2 > 224.0.0.18: VRRPv2, Advertisement, vrid 100, prio 100,
authtype none, intvl 1s, length 20, addrs: 192.168.1.254


root@R1# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           master     A 0.255
                         vip   192.168.1.254


root@R1> monitor start vrrpd

*** vrrpd ***
Feb 28 02:48:49 Mismatch of auth type expected simple got none on fe-0/0/0.0

Po skonfigurowaniu uwierzytelnienia na R2 VRRP znów funkcjonuje poprawnie

root@R1> show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           backup     D 2.585
                         vip   192.168.1.254
                         mas   192.168.1.2


Przykład 11 VRRP – funkcjonowanie prostego uwierzytelnienia
```

Za pomocą sniffera sieciowego można bez problemu wejść w posiadanie hasła uwierzytelniającego routery w grupie VRRP. W związku w tym proste uwierzytelnienie może ochronić przed błędem konfiguracyjnym, ale już nie przed atakiem (np. Man-In-the-Middle), gdy napastnik będzie próbował dodać "swój" router do sieci. W celu zapobieżenia tego typu sytuacjom można zastosować algorytm kryptograficzny MD5. Przykładowa konfiguracja w systemie JUNOS przedstawiona jest poniżej.

```
[edit]
root@pepsi43# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.1/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
                authentication-type md5;
                authentication-key "$9$e8IW87aJDikPLxZj"; ## SECRET-DATA
            }
        }
    }
}


Przykład 12 VRRP – konfigurowanie uwierzytelnienia MD5
```

Grupa VRRP będzie funkcjonowała poprawnie tylko wtedy, gdy mechanizmy kryptograficzne potwierdzą prawidłowość przesyłanych danych. Algorytm MD5 wykorzystywany jest wraz z protokołem AH.

```
root@webdallas ~]# tcpdump -vvni eth1
14:15:45.565382 IP (tos 0xc0, ttl 255, id 6495, offset 0, flags [none], proto 51,
length: 64) 192.168.1.2 > 224.0.0.18: AH(spi=0xabababab,sumlen=16,seq=0x2): VRRPv2,
Advertisement, vrid 100, prio 100, authtype ah, intvl 1s, length 20, addrs:
192.168.1.254
```

Przykład 13 VRRP – uwierzytelnienie MD5 – wykorzystanie AH

Kolejnym przydatnym mechanizmem zaimplementowanym w VRRP jest możliwość ustawienia priorytetu poszczególnych routerów w grupie i przez to wymuszenie, który z nich będzie routerem Master. Wybierany jest router z wyższym priorytetem. Przykładowa konfiguracja w systemie JUNOS oraz funkcjonowanie priorytetów są przedstawione poniżej.

```
[edit]
root@R1# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.1/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
                priority 120;
            }
        }
    }
}

[edit]
root@R2# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.2/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
                priority 100;
            }
        }
    }
}

[edit]
root@R1# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           master     A 0.500
                         vip   192.168.1.254

[edit]
root@R2# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.2      up           backup     D 3.307
                         vip   192.168.1.254
                         mas   192.168.1.1
```

Przykład 14 VRRP – priorytety

Z wykorzystaniem priorytetów można zaimplementować bardzo użyteczny mechanizm – śledzenie stanu pozostałych interfejsów routera. W momencie, gdy na przykład interfejs łączący router z siecią szkieletową przestanie funkcjonować, automatycznie zostanie zmniejszony priorytet dla danej grupy VRRP. Pozwoli to przejąć funkcję Mastera temu, kto ma funkcjonujące interfejsy do wskazanych sieci.

```
[edit]
root@pepsi43# show interfaces fe-0/0/0
unit 0 {
    family inet {
        address 192.168.1.1/24 {
            vrrp-group 100 {
                virtual-address 192.168.1.254;
                priority 120;
                track {
                    interface fe-0/0/1.0 priority-cost 30;
                }
            }
        }
    }
}


[edit]
root@R1# run show vrrp
Interface   Unit  Group  Type  Address          Int state    VR state   Timer
fe-0/0/0    0     100    lcl   192.168.1.1      up           master     A 0.500
                         vip   192.168.1.254
[edit]
root@R1# set interfaces fe-0/0/1 disable

[edit]
root@R1# commit
commit complete


root@R1# run show vrrp detail


Physical interface: fe-0/0/0, Unit: 0, Address: 192.168.1.1/24
  Index: 66, SNMP ifIndex: 36, VRRP-Traps: disabled
  Interface state: up, Group: 100, State: backup
  Priority: 90, Advertisement interval: 1, Authentication type: none
  Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 192.168.1.254
  Dead timer: 3.257s, Master priority: 100, Master router: 192.168.1.2
  Virtual router uptime: 00:12:18
  Tracking: enabled
    Current priority: 90, Configured priority: 120
    Interface tracking: enabled, Interface count: 1
      Interface            Int state     Priority cost
      fe-0/0/1.0           down          30


Przykład 15 VRRP – śledzenie stanu interfejsów
```

Ponieważ konfiguracja protokołu VRRP odbywa się per adres IP, a adresy przypisywane są do interfejsów logicznych, można zdefiniować wiele grup VRRP i przypisać je do interfejsów skojarzonych z tagami VLAN. Możliwa jest taka konfiguracja, że router pełni rolę Master dla jednego interfejsu VLAN i rolę routera zapasowego dla innych VLAN-ów. Pozwala to

również na rozkład obciążenia pomiędzy poszczególnymi routerami. Przykładowa konfiguracja interfejsów VLAN (IEEE802.1Q) w systemie JUNOS przedstawiona jest poniżej.

```
[edit]
root@R1# show interfaces fe-5/0/0
vlan-tagging;
unit 100 {
    vlan-id 100;
    family inet {
        address 10.0.10.1/24 {
            vrrp-group 10 {
                virtual-address 10.0.10.254;
                priority 200;
            }
        }
    }
}
unit 200 {
    vlan-id 200;
    family inet {
        address 10.0.20.1/24 {
            vrrp-group 20 {
                virtual-address 10.0.20.254;
                priority 100;
            }
        }
    }
}
```

Przykład 16 VRRP – interfejsy VLAN

Możliwa jest również konfiguracja zapewniająca rozkład obciążenia w ramach jednej sieci lokalnej bez zastosowania VLAN-ów.

```
[edit]
root@R1# show interfaces fe-5/0/0
unit 0 {
    family inet {
        address 10.0.100.1/24 {
            vrrp-group 100 {
                virtual-address 10.0.100.1;
                priority 200;
            }
            vrrp-group 200 {
                virtual-address 10.0.100.2;
                priority 150;
            }
        }
    }
}
```

Przykład 17 VRRP – interfejsy VLAN

W takim przypadku administator definiuje bramę domyślną dla części stacji, wskazując adres wirtualnego routera w pierwszej grupie VRRP i dla innej części stacji, wskazując adres

wirtualnego routera w kolejnej grupie VRRP. Jest to może prymitywny, ale bardzo skuteczny sposób na rozkład obciążenia pomiędzy routerami. Warto zwrócić uwagę na jeden aspekt funkcjonowania VRRP w implementacji dostępnej na platformie Juniper Networks – w domyślnej konfiguracji urządzenia nie odpowiadają na żądania skierowane do adresu wirtualnego (np. nie da się uzyskać odpowiedzi na polecenie *ping addres_wirtualny*).

```
root@R1# run show vrrp detail
Physical interface: fe-0/0/0, Unit: 0, Address: 192.168.1.1/24
  Index: 66, SNMP ifIndex: 36, VRRP-Traps: disabled
  Interface state: up, Group: 100, State: backup
  Priority: 90, Advertisement interval: 1, Authentication type: none
  Preempt: yes, Accept-data mode: no, VIP count: 1, VIP: 192.168.1.254
  Dead timer: 3.257s, Master priority: 100, Master router: 192.168.1.2
  Virtual router uptime: 00:12:18
```

Przykład 18 VRRP – akceptowanie zapytań

Gdy niezbędne jest włączenie tej funkcjonalności należy w definicji grupy VRRP dodać polecenie *accept-data*.

6. Podsumowanie

Przedstawiony przegląd metod zapewniających dostęp do bramy domyślnej nie wyczerpał wszystkich obecnych możliwości technologicznych. Administratorom zawsze pozostaje wspomniane uruchomienie protokołów routingu dynamicznego na stacjach i serwerach. Z przedstawionych mechanizmów na największą uwagę zasługuje VRRP, który zapewnia największą elastyczność i łatwość konfiguracji, która praktycznie w całości jest wykonywana po stronie administratora sieci komputerowej. Na stacjach wystarczy ustawić adres bramy (również za pomocą DHCP).

Marek Krauze,
JNCIS-M & JNCIA-J