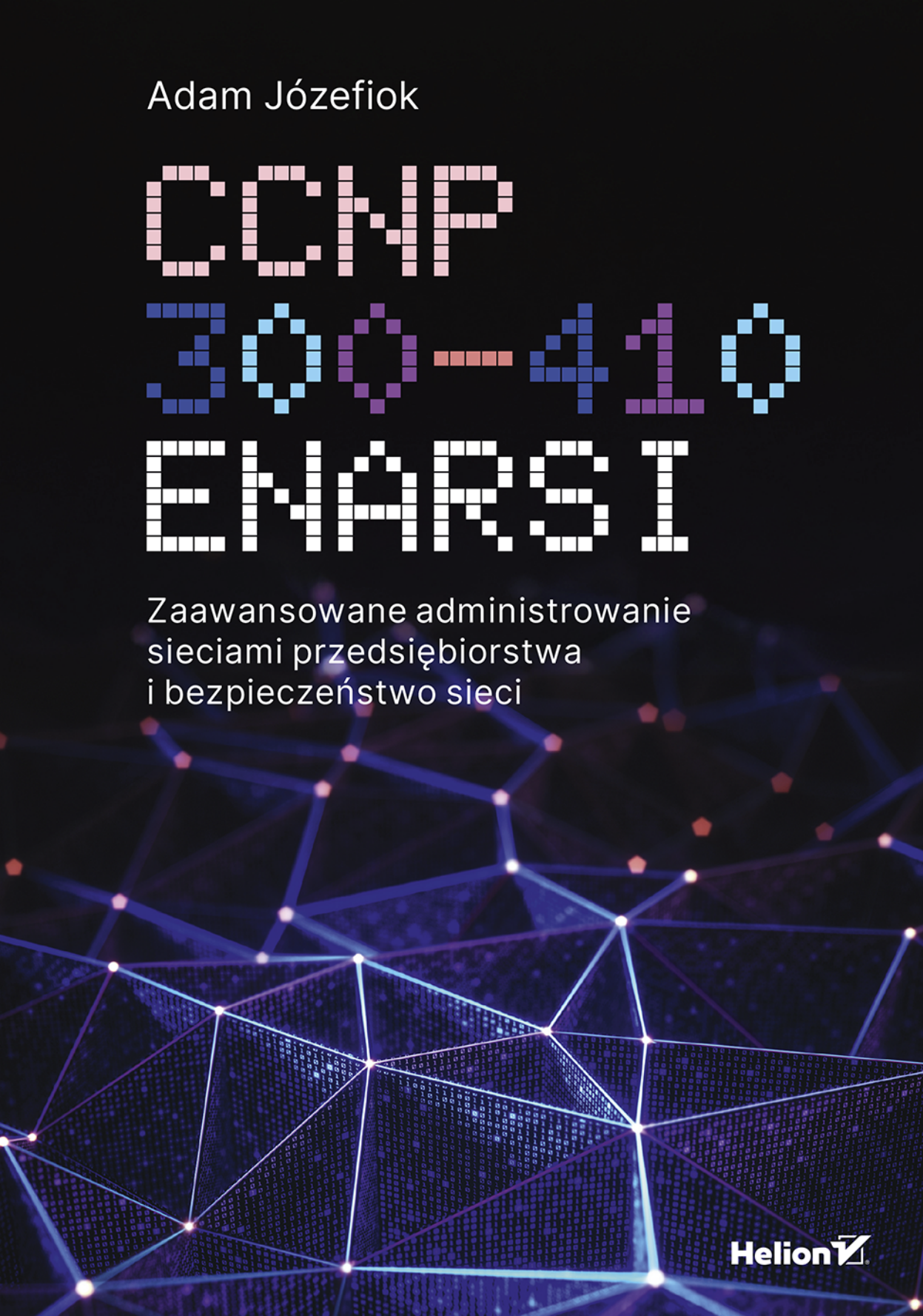
Adam Józefiok

CCNP 300-410 ENARSI

Zaawansowane administrowanie sieciami przedsiębiorstwa i bezpieczeństwo sieci



Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/cc300e
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-1318-9

Printed in Poland.

Spis treści

ROZDZIAŁ 7.

Protokół OSPFv3

Podstawowe informacje

Protokół OSPFv3 jest opisany w RFC 5340. Używa on adresów multicastowych `FF02::5` i `FF02::6` (komunikacja routerów desygnowanych). W OSPFv3 adresami źródłowymi dla pakietów mogą być adresy `link-local`.

Również w OSPFv3 trzeba skonfigurować identyfikator routera, tak zwany *router ID*. Jeśli w sieci wykorzystywany jest tylko protokół IPv6, to trzeba pamiętać o ręcznym przypisaniu identyfikatora poleceniem `router-id` *`[identyfikator_x.x.x.x]`*, wydanym w trybie konfiguracji globalnej routera.

W OSPFv2 można było pominąć ten etap, ponieważ router miał takie ID jak adres IPv4 interfejsu `loopback` lub najwyższy adres IP interfejsu z przypisanym adresem IPv4.

Jeżeli routery są podłączone do sieci wielodostępowej, to w routingu OSPFv3 także wybierane są routery `DR` i `BDR`. Tak samo jak w OSPFv2, jest to określane na podstawie najniższego identyfikatora routera.

W OSPFv3 nie powinno zdziwić Cię na przykład to, że po interfejsie może się pojawić wiele prefiksów, które OSPF ogłosi, ale też na jednym łączu może pojawić się wiele instancji OSPFv3. Ponadto w OSPFv3 stosowane jest znacząco lepsze uwierzytelnianie, które wykorzystuje IPSec.

W protokole OSPFv3 występuje dziewięć typów `LSA` i generalnie pełnią podobne funkcje, tyle że nazwy niektórych zmieniono. Poniżej przedstawiam ich listę z przyporządkowanym w nawiasie typem oraz krótkim opisem.

Router `LSA` (`0x2001`) to podstawowy typ `LSA`, opisujący stan oraz koszt interfejsów routera dla danego obszaru. Czyli można powiedzieć, że służy do wymiany informacji o dostępnych ścieżkach. `LSA` typu 1. informuje o stanie połączeń w zakresie ich aktywności, jak również o sąsiadach, z którymi router ma relację OSPFv3. Ten typ `LSA` zawiera między innymi informację RID oraz pole `Flags`. Tego pola używa się do oznaczenia dodatkowych funkcji routera, na przykład `ABR` czy `ASBR`. Zauważyłeś zapewne, że w IPv6 identyfikatory typów komunikatów są oznaczane heksadecymalnie. Tak więc wartość `0x2000` to podstawowy format `LSA`, a ostatnia cyfra opisuje po prostu typ komunikatu.

`Network LSA` (`0x2002`) jest używany i generowany przez router, który w danej sieci pełni funkcję routera `DR`. Tak więc zwykle ten typ komunikatu występuje w sieciach wielodostępowych, gdzie routery `DR` i `BDR` są wybierane. Ten komunikat informuje nie tylko o routerach bezpośrednio podłączonych do `DR`, ale również o adresie IP danego segmentu sieci i prefiksie.

Zasada działania sieci wielodostępowych w protokole IPv6 jest w zasadzie taka sama jak w IPv4. Tak więc router DR odgrywa rolę routera, który w imieniu wszystkich routerów podłączonych do danego segmentu sieci przesyła informacje dotyczące konkretnych informacji związanych z routingiem. Komunikat network LSA zawiera między innymi takie dane jak ID routera DR, adres i maska sieci oraz lista routerów OSPFv3 podłączonych do danego segmentu sieci.

Inter-Area Prefix LSA (0x2003) generują routery graniczne w IPv6, które przesyłają je pomiędzy obszarami. Jest odpowiednikiem LSA summary w OSPFv2. W OSPFv3 ten typ komunikatu tworzą routery ABR, gdyż są w stanie propagować trasy do innych obszarów. LSA typu 3. rozgłasza prefiksy sieciowe z innych obszarów, aby te mogły zaktualizować swoje tablice routingu, natomiast nie jest to tak, że komunikaty te zawierają pełne informacje o topologii. Zwykle LSA zawiera RID routera ABR rozgłaszającego LSA, prefiks sieci, jego długość oraz koszt służący do obliczenia najlepszej trasy do prefiksu transmitowanego w LSA.

Inter-Area Router LSA (0x2004) jest odpowiedzialny za generowanie międzyobszarowych LSA i przesyłanie ich do innych obszarów. Pełni funkcję podobną do Summary LSA w OSPFv2. Komunikat tego typu generują routery ABR oraz ASBR. Dzięki przesyłaniu tego typu komunikatów routery znajdujące się w innym obszarze są w stanie odnaleźć poprawne ścieżki do sieci docelowych. Istotna rola tych komunikatów to również poinformowanie routerów, których pakiety mają osiągnąć sieci zdalne, o konieczności przesłania pakietów przez routery ASBR. Zwykle LSA typu 4. mają w swoich komunikatach ID routera ABR, ID routera ASBR oraz koszt.

AS-External LSA (0x4005) jest odpowiedzialny za ogłaszanie tras domyślnych lub tras uzyskanych przez redystrybucję. Jest wykorzystywany w OSPFv3 do rozgłaszania tras do sieci zewnętrznych, spoza domeny OSPF. W zasadzie dzięki tego typu komunikatom routery różnych systemów autonomicznych lub różnych protokołów routingu mogą się ze sobą komunikować. Rozgłaszaniem komunikatów typu 5. zajmuje się router ASBR, który przez wygenerowanie tego typu komunikatu informuje inne routery wewnątrz domeny OSPF o dostępnych trasach zewnętrznych. Zwykle komunikat typu 5. zawiera takie informacje jak ID routera ASBR, prefiks sieci zewnętrznej, metryka i dodatkowo pole flagi określające, czy metryka jest typu 1. czy 2. Typ 1. metryki oznacza metrykę wewnętrzną dla routerów OSPF, a metryka typu 2. oznacza metrykę zewnętrzną. Czasem jeśli w sieci funkcjonuje technologia NAT, wówczas w komunikacie typu 5. może znaleźć się informacja na temat translacji.

Group Membership LSA (0x2006) jest LSA typu 6., w którym OSPFv3 może rozgłaszać informacje o grupach multicastingowych. OSPFv3 może dzięki temu dowiadywać się, które z routerów znajdują się w jakich grupach. Nie warto przeznaczać więcej czasu na wyjaśnienie działania tego typu, gdyż nie jest obecnie używany.

Type-7 LSA (0x2007) przesyłają routery graniczne znajdujące się w obszarze NSSA. Jak wiesz, NSSA importuje trasy zewnętrzne, ale też ogranicza działania LSA typu 5. NSSA importuje trasy spoza OSPF, ale ogranicza rozprzestrzenianie tych tras w głąb domeny OSPF. W zamian ABR przekształca je na typ 5. Można powiedzieć, że ten typ komunikatu to kompromis między zwykłymi obszarami a obszarami *stub*.

Link LSA (0x0008) jest przesyłany pomiędzy sąsiadami OSPFv3 na jednym łączu. Jest o tyle specyficznym LSA, że działa jedynie w OSPFv3. Rozgłasza informacje o adresach IPv6 i identyfikatorze interfejsu przypisanego do routera. Jest rozgłaszany tylko na podłączonym łączu i nie jest przekazywany poza to łącze. Jest to dosyć istotny komunikat, gdyż przekazuje informacje o adresach IPv6, prefiksy i RID, czyli dane, które są kluczowe w budowaniu topologii OSPFv3.

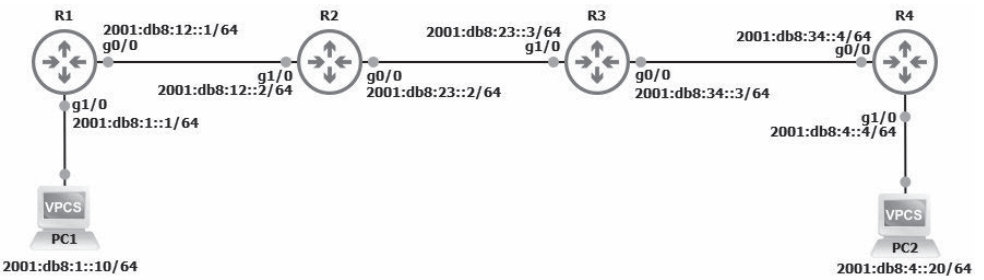
Intra-Area Prefix LSA (0x2009) rozgłasza informacje o prefiksach IPv6 w obrębie jednego obszaru OSPFv3. Protokół OSPFv3 oddzielnie przesyła informacje o topologii oraz o adresach IPv6. Typ 9. służy właśnie do przesyłania informacji o prefiksach. Ten typ komunikatu działa wyłącznie w IPv6 i tylko w obrębie jednego obszaru.

Sposób działania wygląda tak, że na przykład router RX działający w obszarze 0 OSPFv3 ma przypisane do swoich interfejsów adresy IPv6. Generuje oczywiście LSA typu 1., aby rozgłosić informacje o swojej topologii w obrębie obszaru. Ponadto generuje LSA typu 9., aby przekazać informacje o prefiksach IPv6, takich jak 2001:db8:1011::/64, przypisanych do jego interfejsów. Inne routery w tym obszarze uczą się o tych prefiksach, co pozwala im na dokładne zbudowanie topologii IPv6.

Protokół OSPFv3 wykorzystuje dodatkowe typy pakietów LSA (typ 8. i typ 9.), gdyż nieco inaczej wyglądają prefiksy w sieci, która stosuje IPv6. Te LSA są więc używane do ich przenoszenia. OSPFv3 nie umieszcza prefiksów w nagłówku pakietu OSPF. Powyższa lista, jak widzisz, jest bardzo podobna do tej pochodzącej z IPv4, a większość LSA pełni identyczną funkcję.

Konfiguracja OSPFv3

Zanim zagłębimy się w dalsze omówienie OSPFv3, wykonajmy konfigurację sieci pokazanej na rysunku 7.1.



RYSUNEK 7.1. Sieć OSPFv3

Zabieramy się zatem do konfigurowania protokołu OSPFv3 we wskazanej sieci. Nie zapomnij najpierw uruchomić obsługi IPv6 poleceniem ipv6 unicast-routing. Możesz zacząć od dowolnego routera, ale poniżej przedstawiam konfigurację rozpoczętą od R1.

```
R1(config)#ipv6 unicast-routing
```

Teraz możemy przejść do konfiguracji routingu OSPF. W pierwszym kroku nadaj routerowi odpowiedni identyfikator, tak zwane *router-id*. W trybie konfiguracji globalnej

wydaj polecenie `ipv6 router ospf 1`. Zauważ, że router od razu wskazuje ostrzeżenie o braku możliwości automatycznego przypisania identyfikatora. Musisz więc zrobić to ręcznie, przez wpisanie w konfiguracji routingu polecenia `router-id` *`[identyfikator_w_formie_adresu_IPv4]`*. Ja stosuję zasadę, że jeśli router nazywa się `R1`, to identyfikator powinien odzwierciedlać jego nazwę, dlatego dla `R1` identyfikatorem jest `1.1.1.1`, dla `R2` jest to `2.2.2.2` itd.

Następnym krokiem jest przypisanie interfejsu do określonego obszaru (`area`). Pamiętaj, że zawsze w sieci musi być tak zwany *backbone area*, czyli obszar zerowy, do którego muszą być dołączone wszystkie pozostałe obszary. Przejdź teraz do konfiguracji interfejsu routera, który ma uczestniczyć w działaniu OSPF, i wydaj polecenie `ipv6 ospf 1 area 0`. Podany interfejs stanie się członkiem `area 0`.

```
R1(config)#ipv6 router ospf 1
R1(config-rtr)#
*Jun 22 11:40:15.799: %OSPFv3-4-NORTRID: Process OSPFv3-1-IPv6 could not pick a router-id,
➥please configure manually
R1(config-rtr)#router-id 1.1.1.1
R1(config-rtr)#exit
R1(config)#int g0/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#int g1/0
R1(config-if)#ipv6 ospf 1 area 0
R1(config-if)#
```

Analogiczną konfigurację należy wykonać na pozostałych routerach w sieci.

Po nawiązaniu relacji sąsiedzkiej przez routery możesz sprawdzić poleceniem `show ipv6 ospf neighbors`, czy wszystko w konfiguracji działa poprawnie. Jak pokazałem na poniższym listingu, z poziomu routera `R1` widać sąsiada, którym jest router `R2` o RID `2.2.2.2`.

```
R1#show ipv6 ospf neighbor
            OSPFv3 Router with ID (1.1.1.1) (Process ID 1)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
2.2.2.2           1   FULL/BDR        00:00:34    4               GigabitEthernet0/0
R1#
```

Po przypisaniu wszystkich interfejsów do odpowiednich obszarów możesz wydać polecenie `show ipv6 ospf interface brief`, aby sprawdzić poprawność ich przypisania.

```
R1#show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Gi1/0        1     0               4          1     DR    0/0
Gi0/0        1     0               3          1     DR    1/1
R1#
```

Z powyższego listingu wynika, że interfejsy `g0/0` i `g0/1` są w `area 0`. Ponadto kolumna `State` informuje, że router został routerem desygnowanym (przy interfejsie `g0/0` i `g1/0` jest status `DR`).

Jeśli chodzi o konfigurację tras domyślnych, to w IPv6 również przeprowadza się ją znanym Ci już poleceniem `default-information originate`.

Jak więc mogłeś się przekonać, konfiguracja protokołu OSPFv3 jest bardzo prosta i intuicyjna.

Interfejs pasywny w OSPFv3

Podobnie jak w OSPFv2 należy zabezpieczyć interfejsy, do których router nie jest podłączony, przed dystrybuowaniem przez te interfejsy komunikatów `hello`. Odpowiedzialna jest za to funkcjonalność `passive-interface`. Pierwszy sposób skonfigurowania tej funkcjonalności to wydanie w konfiguracji routingu polecenia `passive-interface` *[adres_IP_interfejsu_do_zablokowania]*.

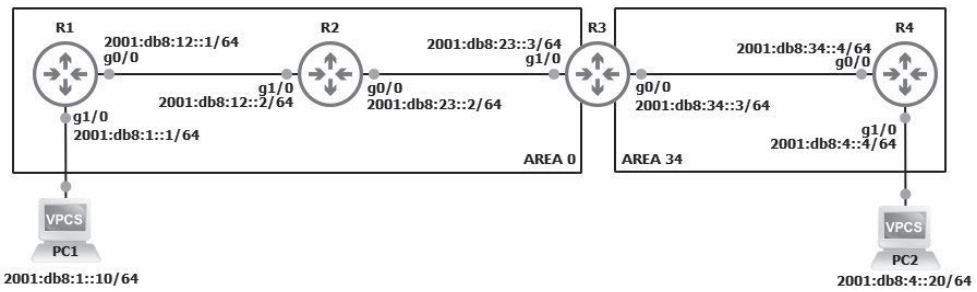
```
R1(config)#router ospfv3 1
R1(config-router)#passive-interface g1/0
R1(config-router)#
```

Drugi sposób to posłużenie się w konfiguracji routingu poleceniem `passive-interface default`, a następnie wyłączenie `passive-interface` na interfejsach, na których nie powinien być włączony. Ten sposób jest lepszy w sytuacji, kiedy sieć nie jest jeszcze skonfigurowana i dopiero rozpoczynasz konfigurację.

```
R1(config)#router ospfv3 1
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface g0/0
R1(config-router)#
```

Konfiguracja wielu obszarów

Zmodyfikujmy jeszcze naszą sieć IPv6 z protokołem OSPFv3 tak, aby znajdowały się w niej dwa obszary. Oczywiście widzimy na rysunku 7.2 sieć z dwoma obszarami: 0 oraz 34.



RYSUNEK 7.2. OSPFv3 wieloobszarowy

Konfiguracja wielu obszarów w OSPFv3 w zasadzie jest banalnie prosta. Należy bowiem podczas konfigurowania interfejsu wskazać obszar, w którym się ten interfejs znajduje, tak jak pokazano to na poniższym listingu. Jeden interfejs routera `R3`, to jest `g1/0`, znajduje się w obszarze `0`, a interfejs `g0/0` w obszarze `34`, dlatego konfiguracja wygląda tak:

```
R3(config)#int g0/0
R3(config-if)#ipv6 ospf 1 area 34
R3(config-if)#
```

Oczywiście na routerze R4 należy przeprowadzić analogiczną konfigurację. Po tym możesz wyświetlić tablicę routingu, aby sprawdzić, jak działa OSPF wieloobszarowy w sieci IPv6. Tablica routingu routera `R4` zawiera już wpisy `OI` pochodzące z innego obszaru.

```
R4#show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
<POMINIĘTO>
OI  2001:DB8:1::/64 [110/4]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
OI  2001:DB8:12::/64 [110/3]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
OI  2001:DB8:23::/64 [110/2]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
R4#
```

Sumaryzacja w IPv6 OSPF

W OSPFv3 również jest możliwość sumaryzacji sieci, jednak należy pamiętać, że taka sumaryzacja musi być wykonana na routerze ABR. Tym routerem w naszej niewielkiej sieci jest router R3. Zanim jednak wykonamy prostą sumaryzację, jeszcze raz zerknijmy do tablicy routera R4, który jak widzisz, zawiera trzy wpisy z innego obszaru. Spróbujemy w kolejnym kroku zsumaryzować te sieci do jednego zapisu.

```
R4#show ipv6 route ospf
<POMINIĘTO>
OI  2001:DB8:1::/64 [110/4]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
OI  2001:DB8:12::/64 [110/3]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
OI  2001:DB8:23::/64 [110/2]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
R4#
```

Po przejściu do konfiguracji routera R3 przejdź w trybie konfiguracji routingu OSPFv3 poleceniem `address-family ipv6 unicast` dalej, do ustawień `address family (AF)`. Następnym poleceniem `area` *[obszar_sumaryzacji]* `range` *[adres_IPv6_zsumaryzowany]* włącz sumaryzację.

```
R3(config)#router ospfv3 1
R3(config-router)#address-family ipv6 unicast
R3(config-router-af)#area 0 range 2001:db8:0:0::/32
R3(config-router-af)#
```

Po ponownym wyświetleniu tablicy routingu routera R4 widać tylko jeden zsumaryzowany wpis.

```
R4#show ipv6 route ospf
<POMINIĘTO>
OI  2001:DB8::/32 [110/4]
     via FE80::C803:7FF:FE5F:8, GigabitEthernet0/0
R4#
```

Zmiana typu sieci

Podobnie jak w OSPFv2, również w OSPFv3 jest możliwość manipulowania typem sieci. Oczywiście typ sieci musi być zmieniony po obydwu stronach połączenia. Aby sprawdzić, jaki typ sieci jest włączony na interfejsach routera R1, wydaj polecenie `show ospfv3 interface brief`. Zauważ, że w kolumnie `State` mamy w pierwszym wierszu DR, a w drugim BDR. Wniosek jest prosty: typ interfejsu to BROADCAST, gdyż w tym typie wybierane są właśnie te routery.

```
R1#show ospfv3 interface brief
Interface    PID   Area            AF          Cost  State Nbrs F/C
Gi1/0        1     0               ipv6        1     DR    0/0
Gi0/0        1     0               ipv6        1     BDR   1/1
R1#
```

Ale zajrzyjmy jeszcze do parametrów interfejsu g0/0 w kontekście OSPF. Tutaj możemy tylko potwierdzić, że typ sieci to faktycznie BROADCAST oraz że router został wybrany jako BDR.

```
R1#show ipv6 ospf int g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::C801:7FF:FE1F:8, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, local address FE80::C802:7FF:FE3F:1C
  Backup Designated router (ID) 1.1.1.1, local address FE80::C801:7FF:FE1F:8
<POMINIĘTO>
R1#
```

Zmiana typu interfejsu odbywa się w konfiguracji interfejsu. Należy wydać polecenie ospfv3 network i podać odpowiedni typ, na przykład point-to-point.

```
R1(config)#int g0/0
R1(config-if)#ospfv3 network point-to-point
R1(config-if)#
```

Po zmianie typu po obydwu stronach połączenia teraz polecenie show ospfv3 interface brief zwraca informację, że na interfejsie g0/0 mamy już status P2P.

```
R1#show ospfv3 interface brief
Interface    PID   Area            AF          Cost  State Nbrs F/C
Gi1/0        1     0               ipv6        1     DR    0/0
Gi0/0        1     0               ipv6        1     P2P   1/1
R1#
```

Polecenia weryfikujące OSPFv3

Jeśli pojawia się problem z działaniem OSPFv3, to oczywiście polecenia weryfikujące są nieodzowną częścią analizy. W pierwszej kolejności możesz użyć polecenia show ospfv3 interface [interfejs]. Pozwoli Ci ono zlokalizować problemy w zakresie działania interfejsu. Ponadto dowiesz się, w jakiej roli pracuje interfejs. Zauważ, że w przypadku IPv6 routery do identyfikacji obok RID używają również adresów *IPv6 link-local*.

```
R1#show ospfv3 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Link Local Address FE80::C801:7FF:FE1F:8, Interface ID 3
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, local address FE80::C802:7FF:FE3F:1C
  Backup Designated router (ID) 1.1.1.1, local address FE80::C801:7FF:FE1F:8
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Graceful restart helper support enabled
  Index 1/1/1, flood queue length 0
```

```
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

Przydatnym poleceniem jest `show ospfv3 interface brief`. Pozwala Ci szybko zweryfikować problemy związane z interfejsami. Dzięki temu będziesz mógł się skupić na konkretnym interfejsie.

```
R1#show ospfv3 interface brief
Interface    PID   Area            AF         Cost  State Nbrs F/C
Gi1/0        1     0               ipv6       1     DR    0/0
Gi0/0        1     0               ipv6       1     BDR   1/1
R1#
```

Jeśli chodzi bazę `LSA`, to spójrzmy na przykładowy wpis pochodzący z bazy routera `R1`. Aby wyświetlić wpisy, należy użyć polecenia `show ospfv3 database`. Dodatkowo można podać odpowiedni argument, na przykład `router`.

Od razu w oczy rzuca się pozycja `Options`, zawierająca pewne skróty. Są to pola bitowe opcji dodatkowych opisujące możliwości routera.

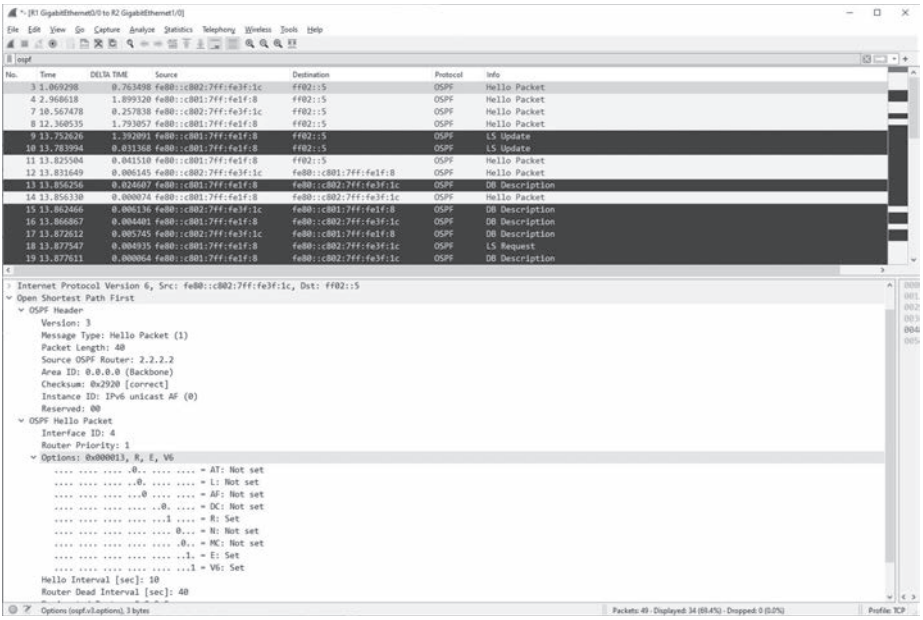
```
R1#show ospfv3 database router
          OSPFv3 1 address-family ipv6 (router-id 1.1.1.1)
               Router Link States (Area 0)
  LS age: 421
  Options: (V6-Bit, E-Bit, R-bit, DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 1.1.1.1
  LS Seq Number: 8000000C
  Checksum: 0x3DE
  Length: 40
  Number of Links: 1

    Link connected to: another Router (point-to-point)
      Link Metric: 1
      Local Interface ID: 3
      Neighbor Interface ID: 4
      Neighbor Router ID: 2.2.2.2
<POMINIĘTO>
R1#
```

Bity omówione poniżej są umieszczane wewnątrz pakietu OSPFv3 (rysunek 7.3). Zauważ, że w tym przypadku mamy zaznaczony pakiet `hello`, ale pole to występuje również w innych pakietach `LSA`.

`V6-Bit` to nic innego jak bit informujący o tym, że na routerze uruchomiony jest proces routingu dla IPv6.

`E-bit` to informacja, że router jest w stanie przetwarzać pochodzące z zewnątrz pakiety `LSA`. Jeśli na przykład na routerze mamy zaimplementowany obszar *stub*, to wtedy wartość tego bitu wynosi `0` (`clear`). Aby nastąpiła relacja sąsiedzka, wartość tego bitu musi się zgadzać po obydwu stronach połączenia.



RYSUNEK 7.3. Dodatkowe bity w komunikacie hello

Bit `R-bit` jest informacją na temat aktywności routera. Jeśli jest ustawiony na `1`, wówczas jest to informacja o aktywnym uczestnictwie w przekazywaniu ruchu. Jeśli jest ustawiony na `0`, wtedy router nie będzie używany jako tranzytowy, będzie natomiast w stanie przesyłać i odbierać `LSA`.

Kolejny bit to `DC-bit`, który jest informacją, że router może zablokować przesyłanie komunikatów `hello` przez dany interfejs. Obecnie ze względu na szybkość działania współczesnych sieci komputerowych ten bit rzadko jest wykorzystywany i zwykle jest ustawiony na `0`.

Ponadto mogą wystąpić jeszcze dwa bity, `MC-bit` oraz `N-bit`. Pierwszy wskazuje na to, że router może obsłużyć multiemisję w OSPF, tak zwaną technologię **MOSPF**. Obecnie też nie jest używany. Drugi jest informacją o możliwościach obsłużenia przez router `LSA` typu 7. Bit ten jest wykorzystywany w obszarach `NSSA` i wtedy routery obsługujące te obszary muszą mieć ustawioną obsługę tego bitu po obydwu stronach połączenia.

Warto, abyś wiedział, że w OSPFv3 istnieją dwa dodatkowe typy `LSA`: 8. oraz 9. Typ 8. `LSA` działa tylko i wyłącznie na łączu lokalnym. Jest odpowiedzialny za dostarczenie sąsiadowi informacji o adresach lokalnych łącza. `LSA` typu 9. są przesyłane w ramach jednego obszaru i zwykle zawierają informacje na temat adresacji sieci tranzytowej, przez którą przechodzą pakiety OSPF. Oba te typy działają tylko w sieciach IPv6 i nie występują w IPv4.

Konfiguracja uwierzytelniania w OSPFv3

Podczas korzystania z OSPFv3 również masz możliwość skonfigurowania uwierzytelniania, ale i szyfrowania. Dzieje się tak, ponieważ ten protokół oferuje IPsec, dlatego istnieją dwie możliwości, z których będziesz mógł skorzystać. Pierwsza to uwierzytelnianie nagłówka (ang. *authentication header*). Zobacz, jak wygląda konfiguracja, która zresztą jest niezwykle prosta.

W konfiguracji interfejsu łączącego router R1 z routerem R2 wydaj polecenie `ipv6 ospf authentication ipsec spi` *`[numer_indeksu] [metoda]`*. Identyfikator SPI (ang. *Security Parameter Index*) możesz wybrać dowolny, ale zaleca się wybranie numeru od 256 do 4096, gdyż ten zakres jest zarezerwowany przez TCP/IP na cele tworzenia tuneli ręcznych. Następnie wybierz metodę SHA1 (staraj się nie wybierać MD5) i wpisz klucz w formacie heksadecymalnym. Aby wygenerować klucz, możesz użyć dowolnego generatora SHA1 online. Pełne polecenie, które należy wydać także po drugiej stronie połączenia, wygląda tak: `ipv6 ospf authentication ipsec spi 256 sha1 0e18f44c1fec03ec4083422cb58ba6a09ac4fb2a`.

```
R1(config)#int g0/0
R1(config-if)#ipv6 ospf authentication ipsec spi ?
  <256-4294967295>  SPI
R1(config-if)#ipv6 ospf authentication ipsec spi 256 ?
  md5   Use MD5 authentication
  sha1  Use SHA-1 authentication
R1(config-if)# ipv6 ospf authentication ipsec spi 256 sha1
0e18f44c1fec03ec4083422cb58ba6a09ac4fb2a
R1(config-if)#
*Jun 22 22:39:40.594: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Pamiętaj, że po włączeniu uwierzytelniania routery muszą ponownie nawiązać relację sąsiedzką, dlatego przez chwilę połączenie będzie niedostępne. Musisz to uwzględnić w trakcie konfigurowania sieci w przedsiębiorstwie. Kiedy routery od nowa ustanowią sąsiedztwo, możesz poleceniem `show crypto ipsec policy` sprawdzić lokalne ustawienia szyfrowania.

```
R1#show crypto ipsec policy
Crypto IPsec client security policy data
Policy name:      OSPFv3-256
Policy refcount:  1
Inbound  AH SPI:  256 (0x100)
Outbound AH SPI:  256 (0x100)
Inbound  AH Key:  0E18F44C1FEC03EC4083422CB58BA6A09AC4FB2A
Outbound AH Key:  0E18F44C1FEC03EC4083422CB58BA6A09AC4FB2A
Transform set:    ah-sha-hmac
R1#
```

Konfiguracja szyfrowania w OSPFv3

To teraz wypróbujmy jeszcze konfigurację drugiej metody, jaką jest szyfrowanie. Metoda ta jest dostępna, ponieważ OSPFv3 potrafi szyfrować całe pakiety i enkapsulować je jako ESP (ang. *Encapsulating Security Payload*). Konfiguracji szyfrowania również dokonuje się w konfiguracji interfejsu, poleceniem `ipv6 ospf encryption ipsec spi 256` *`[metoda_szyfrowania] [klucz]`* `sha1` *`[klucz]`*. I jak poprzednio w celu wygenerowania kluczy możesz posłużyć się wieloma stronami online, które oferują tego typu usługi.

Poniżej znajduje się listing z przykładową konfiguracją. Jeśli chcesz ją zaimplementować w przykładzie, to najpierw będziesz musiał usunąć poprzednią.

```
R1(config-if)#ipv6 ospf encryption ipsec spi 256 esp aes-cbc 256 40F60C0EB2BDD5A457129B16DA
↪891C69C2E9FEBC1D7F8A67B06B146077760CF9 sha1 f941e1206abd4a2d8889da67be10151f429d95dc
R1(config-if)#
*Jun 22 22:46:50.986: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

Po sprawdzeniu konfiguracji poleceniem `show crypto ipsec policy` możesz zauważyć, że metoda szyfrowania się zmieniła.

```
R1#show crypto ipsec policy
Crypto IPsec client security policy data
Policy name:      OSPFv3-256
Policy refcount:  1
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   F941E1206ABD4A2D8889DA67BE10151F429D95DC
Outbound ESP Auth Key:   F941E1206ABD4A2D8889DA67BE10151F429D95DC
Inbound  ESP Cipher Key: 40F60C0EB2BDD5A457129B16DA891C69C2E9FEBC1D7F8A67B06B146077760CF9
Outbound ESP Cipher Key: 40F60C0EB2BDD5A457129B16DA891C69C2E9FEBC1D7F8A67B06B146077760CF9
Transform set:    esp-256-aes esp-sha-hmac
R1#
```

Jak więc widzisz, protokół OSPFv3 konfiguruje się niemal identycznie jak OSPFv2. Również funkcjonują niezwykle podobnie. Dlatego myślę, że przedstawiona wiedza wystarczy Ci do tego, aby samodzielnie ten protokół skonfigurować i na podstawie informacji z OSPFv2 później z powodzeniem nim administrować.

Skorowidz

C

D

E

F

L

M

N

O

P

R

S

T

U

V

W

Z

CCNP 300-410 ENARSI

Dziwne, u mnie też nie działa...

Rola administratora sieci komputerowej zaczyna się od jej skonfigurowania, jednak na tym absolutnie się nie kończy. Dalej musi on zadbać o to, by sieć działała poprawnie — jeśli cokolwiek pójdzie nie tak, administrator szybko dowie się o tym od użytkowników, którzy będą oczekiwać, że równie szybko przywróci ją do stanu poprzedniego. Drobnostka, jeśli problem okazuje się błahy i prosty do rozwiązania. Prawdziwe wyzwanie zaczyna się wtedy, kiedy naprawa usterki wymaga dogłębnej znajomości sieci, jej silnych i mocnych stron, a także metod radzenia sobie z awariami. Na szczęście powstała ta książka.

Najnowsza pozycja autorstwa Adama Józefioka pozwoli Ci nie tylko poznać swoją sieć komputerową w najdrobniejszych szczegółach. Dowiesz się również, jak sobie radzić, gdy detal, z którego istnienia co prawda zdajesz sobie sprawę, ale którego nie bierzesz pod uwagę jako źródła ewentualnych problemów, nagle zaczyna sprawiać kłopoty. Przyswajając wiedzę teoretyczną zawartą w książce i trenując na jej podstawie umiejętności praktyczne, przygotujesz się równocześnie do zdania egzaminu CCNP ENCOR, a tym samym do zdobycia kolejnego certyfikatu przydatnego w Twojej rozwijającej się karierze administratora sieci komputerowych.

Adam Józefiok

Ukończył studia doktoranckie na Politechnice Śląskiej w Gliwicach, na Wydziale Automatyki, Elektroniki i Informatyki. Specjalizuje się w tematyce sieci komputerowych (przełączanie, routing, bezpieczeństwo i projektowanie), jest autorem publikacji polskich i zagranicznych z tej dziedziny. Brał udział w konferencjach naukowych (krajowych i międzynarodowych) dotyczących sieci komputerowych. Jest pracownikiem naukowym Katedry Sieci i Systemów Komputerowych Politechniki Śląskiej. Na co dzień administruje również bezpieczeństwem urządzeń sieciowych, konfiguruje między innymi urządzenia sieciowe (Cisco, HP), utrzymuje sieci WAN. Przez siedem lat kierował komórką realizacji wsparcia usług IT. Ma wieloletnie doświadczenie w pracy jako administrator sieci i projektant sieci komputerowych.
Przez lata projektował serwerownie i tworzył projekty okablowania. Opracowywał procedury i dokumentacje projektowe. Na koncie ma wiele zrealizowanych projektów w zakresie zakupu sprzętu IT wraz z prowadzeniem procedur przetargowych, wdrożeniem, wykonaniem dokumentacji i testami. Posiada certyfikaty: CCNA Security, CCNP Routing and Switching, Cisco CCDP, CCNAV, jak również certyfikat instruktorski Cisco CCAI, certyfikaty ITIL i PRINCE2.
Jego pasją jest pisanie książek, praca ze studentami i szeroko rozumiana dydaktyka.

Helion

helion.pl

HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej! ▶

ISBN 978-83-289-1318-9

9 788328 913189

Cena: 169,00 zł