

Adam Józefiok

CCNP 300-410 ENARSI

Zaawansowane administrowanie
sieciami przedsiębiorstwa
i bezpieczeństwo sieci

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Copyright © Helion S.A. 2025

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wstęp	9
ROZDZIAŁ 1. Komunikacja w sieciach komputerowych	11
Adresowanie w sieciach	11
Przydzielanie adresu IPv4	12
Rozwiązywanie problemów z DHCP	18
Adresowanie IPv6	20
Rodzaje adresów IPv6	21
Proces EUI-64	22
Adresy typu multicast	26
Funkcjonalność SLAAC	28
Konfiguracja routera jako bezstanowego serwera DHCPv6	31
Konfiguracja routera jako połączeniowego serwera DHCPv6	34
Komunikacja w sieciach	40
IPv6 First Hop Security	43
Działanie przełączników w kontekście wykorzystania CEF	55
Technologia CEF	57
ROZDZIAŁ 2. Routing w sieciach	63
Manipulowanie trasami routingu	63
Dystans administracyjny	64
Listy ACL	67
Listy prefiksów	72
Redystrybucja OSPF do EIGRP	75
Redystrybucja EIGRP-EIGRP	79
Redystrybucja OSPF-OSPF	82
Listy offsetowe	83
Mapy trasy	85
Sumaryzacja tras	95
Routing oparty na politykach	98
Konfiguracja i działanie VRF	101
Funkcjonalność BFD	106
Rozwiązywanie problemów związanych z redystrybucją	109
Przykład 1.	110
Przykład 2.	112
ROZDZIAŁ 3. Protokół EIGRP w sieciach IPv4 i rozwiązywanie problemów	114
Konfiguracja EIGRP	115
Zapobieganie pętli routingu	119
Rodzaje pakietów EIGRP	120

Metryka w EIGRP	122
Interfejs pasywny	125
Rozgłaszanie tras	126
Uwierzytelnianie tras w EIGRP	126
Konfiguracja routera stub w EIGRP	127
Alternatywna konfiguracja EIGRP (nazywany EIGRP)	130
Osiąganie zbieżności w EIGRP	131
Rozwiązywanie problemów z protokołem EIGRP	134
Problem 1. Brak komunikacji pomiędzy stacjami roboczymi	141
Problem 2. Brak komunikacji i problem z trasami	147
ROZDZIAŁ 4. Protokół routingu EIGRPv6	150
Podstawowa konfiguracja EIGRPv6	150
Konfiguracja alternatywna EIGRPv6	151
Weryfikacja routingu EIGRPv6	153
Pakiety EIGRPv6	154
Sumaryzacja w EIGRPv6	158
Włączenie uwierzytelniania w EIGRPv6	159
Rozwiązywanie problemów w EIGRPv6	163
Polecenia weryfikujące	163
Rozwiązywanie typowych problemów w EIGRPv6	164
ROZDZIAŁ 5. Protokół routingu OSPF	172
Informacje wstępne o OSPF	172
ID obszaru	173
Identyfikator routera	174
Konfiguracja protokołu OSPF	174
Baza LSDB	179
Wymiana informacji pomiędzy routerami	181
OSPF w sieciach wielodostępowych	186
Designated Router i Backup Designated Router	186
Wybór routerów DR i BDR	187
Proces elekcji — wymiana LSA	189
Statusy po nawiązaniu relacji sąsiedztwa	192
Routery DR i BDR w połączeniu punkt – punkt	193
Typy sieci w OSPF	195
Uwierzytelnianie w OSPF	198
Alternatywna konfiguracja protokołu OSPF	201
Wielooobszarowy OSPF	204
Typy przesyłanych pakietów LSA	205
Typy obszarów i tras wykorzystywanych przez OSPF	215
Wybór odpowiedniego typu obszaru	221
Metryka w OSPF	226
Sieć nieciągła	230

ROZDZIAŁ 6. Rozwiązywanie problemów z protokołem OSPFv2	234
Przykład 1.	234
Przykład 2.	236
Przykład 3.	238
Zmiana czasów	241
Konfiguracja passive-interface	242
Przykład 4.	242
Zmiana identyfikatora routera	246
Przykład 5.	247
Filtrowanie w OSPF na podstawie listy dystrybucyjnej	249
Filtrowanie obszarów	249
Równoważenie obciążenia w OSPF	250
ROZDZIAŁ 7. Protokół OSPFv3	252
Podstawowe informacje	252
Konfiguracja OSPFv3	254
Interfejs pasywny w OSPFv3	256
Konfiguracja wielu obszarów	256
Sumaryzacja w IPv6 OSPF	257
Zmiana typu sieci	257
Polecenia weryfikujące OSPFv3	258
Konfiguracja uwierzytelniania w OSPFv3	260
Konfiguracja szyfrowania w OSPFv3	262
ROZDZIAŁ 8. Rozwiązywanie problemów w OSPFv3	263
Przykład 1.	263
Przykład 2.	265
Przykład 3.	266
ROZDZIAŁ 9. Protokół BGP. Działanie i konfiguracja	269
Wprowadzenie do BGP	269
Podstawowa konfiguracja protokołu BGP	277
Polecenia weryfikujące działanie BGP	282
Analiza problemu w BGP	285
Uwierzytelnianie w BGP	285
Rozgłaszanie prefiksów w BGP	286
Rodzaje BGP: Internal BGP (iBGP)	288
iBGP i problemy skalowalności	297
Rodzaje BGP: External BGP (eBGP)	302
eBGP Multihop	302
Łączy redundantne w eBGP	305
Rozgłaszanie sieci w BGP	306
Redystrybucja w BGP	309
Zaawansowana konfiguracja protokołu BGP IPv4	312
Sumaryzacja i autosumaryzacja w BGP IPv4	312
Sposoby filtrowania tras w BGP	315
Filtrowanie i grupowanie tras w BGP	328

Atrybuty w BGP i ich rola	337
Atrybut Local Preference	342
Atrybut Origin Code	346
Atrybut MED	347
ROZDZIAŁ 10. BGP i protokół IPv6	350
IPv6 w BGP czyli Multiprotocol BGP (MP-BGP)	350
Aktywacja MP-BGP dla sieci IPv6	350
Aktywacja MP-BGP dla sieci z prefiksami IPv6	352
Zastosowanie mechanizmu route reflector w BGP IPv6	355
Konfiguracja filtrowania prefiksów i map tras w BGP IPv6	357
Uwierzytelnianie w BGP IPv6 i funkcja filtrowania tras	359
Filtrowanie tras BGP za pomocą standardowych ACL IPv6	363
ROZDZIAŁ 11. Rozwiązywanie podstawowych problemów w BGP	365
Problem 1.	365
Problem 2.	367
ROZDZIAŁ 12. Sieć MPLS. Zastosowanie, konfiguracja i rozwiązywanie problemów	371
Wprowadzenie do MPLS	371
Konfiguracja MPLS	374
Wymiana danych MPLS	383
MPLS Layer 3 VPN	388
VRF dla MPLS	390
Routing pomiędzy routerami PE i CE	394
Konfiguracja iBGP w sieci ISP	395
Weryfikacja MPLS VPN oraz omówienie ruchu	397
Rozwiązywanie problemów w sieciach MPLS	405
Problem 1.	405
Problem 2.	407
Problem 3.	409
Problem 4.	411
Problem 5.	414
ROZDZIAŁ 13. Technologia Dynamic Multipoint Virtual Private Network (DMVPN)	418
Informacje na temat IPsec	418
Zachowanie integralności	420
Uwierzytelnianie	421
Sieci VPN	421
Konfiguracja DMVPN bez IPsec	423
Analiza pakietów	432
Konfiguracja DMVPN z IPsec	434
Analiza pakietów	439
ROZDZIAŁ 14. Rozwiązywanie problemów z bezpieczeństwem	442
Problemy z funkcjami bezpieczeństwa routera	442
Listy ACL i rozwiązywanie problemów	442
Funkcjonalność uRPF (unicast Reverse Path Forwarding)	454
Funkcjonalność CoPP	457

ROZDZIAŁ 15. Zarządzanie urządzeniami i rozwiązywanie problemów	467
Dostęp do urządzeń	467
Transfer plików pomiędzy urządzeniami	468
Tworzenie serwera TFTP na routerze i transfer plików	468
Transfer plików przez HTTP	471
Transfer plików przez Secure Copy Protocol (SCP)	473
Rozwiązywanie problemów z SNMP	474
Konfiguracja SNMPv2c	476
Konfiguracja SNMPv3	479
Rozwiązywanie problemów z wykorzystaniem logowania zdarzeń	481
Funkcja debugowania	484
Powiadomienie o zmianach w konfiguracji	485
Funkcjonalność IP SLA — działanie i rozwiązywanie problemów	487
Wykorzystanie i działanie NetFlow	497
Konfiguracja NetFlow na routerze	498
Zakończenie	501
Skorowidz	503

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 oznaczają 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.

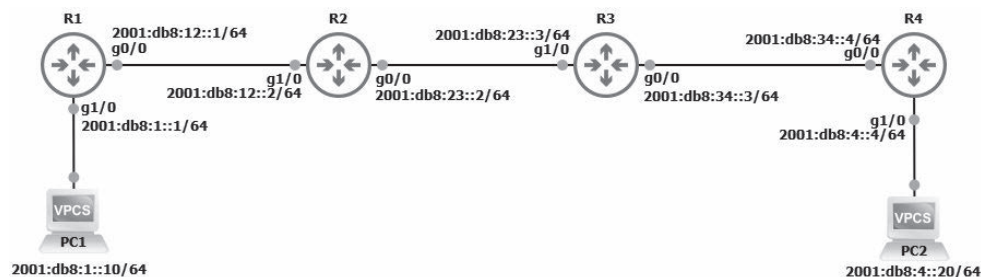
Intra-Area Prefix LSA (0x2009) rozgłasza informacje o prefiksach IPv6 w obrębie jednego obszaru OSPFv3. Protokół OSPFv3 oddzielnie przesyła informacje o topologii oraz o adresach IPv6. Typ 9. służy właśnie do przesyłania informacji o prefiksach. Ten typ komunikatu działa wyłącznie w IPv6 i tylko w obrębie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



RYСУNEK 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]`.

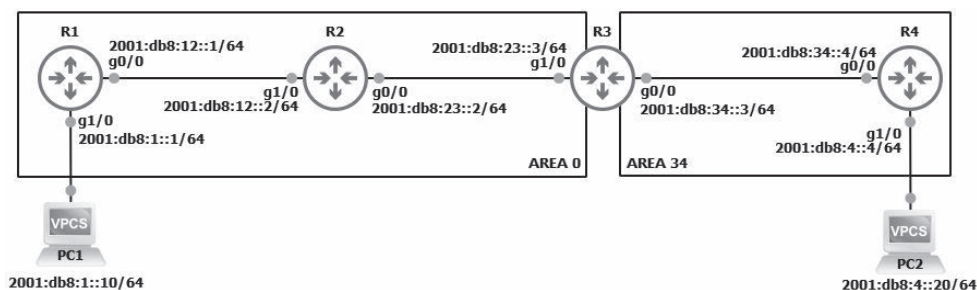
```
R1(config)#router ospfv3 1
R1(config-router)#passive-interface g1/0
R1(config-router)#
```

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 0I 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 o 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

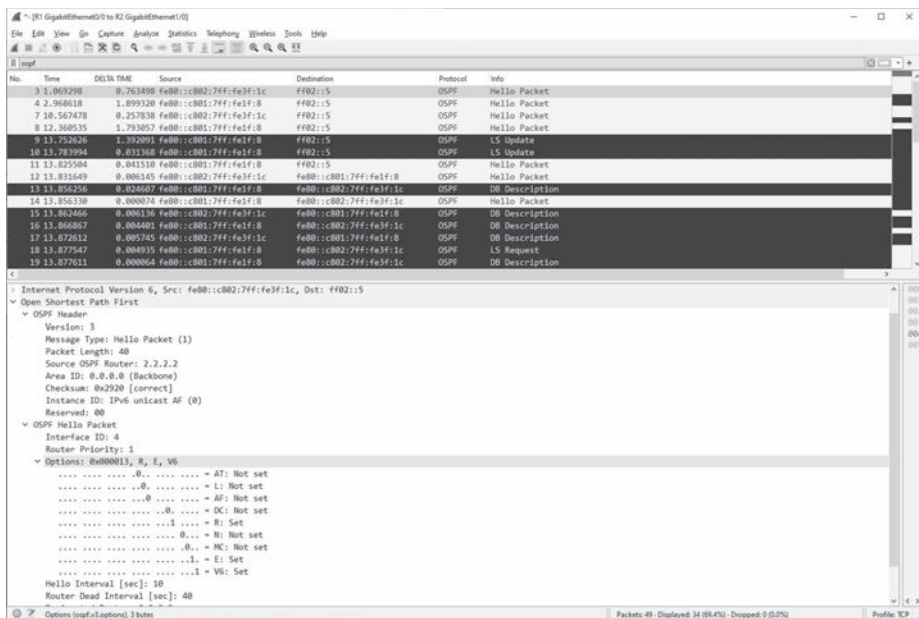
Link connected to: another Router (point-to-point)
Link Metric: 1
Local Interface ID: 3
Neighbor Interface ID: 4
Neighbor Router ID: 2.2.2.2
<POMINIĘTO>
R1#

```

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 przysyłać 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 przysyłane 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
↪891C69C2E9FEBBC1D7F8A67B06B146077760CF9 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: 40F60C0EB2BDD5A457129B16DA891C69C2E9FEB1D7F8A67B06B146077760CF9
Outbound ESP Cipher Key: 40F60C0EB2BDD5A457129B16DA891C69C2E9FEB1D7F8A67B06B146077760CF9
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

A

ABR, Area Border Router, 204
ACL, Access Control List, 442
AD, administrative distance, 64
adres
 anycast, dowolny, 22
 APIPA, 18
 global, globalny, 21
 GUA, 30
 IPv4, 11
 IPv6, 20
 link-local, lokalnego łącza, 22
 loopback, lokalnej pętli, 22
 MAC, 13, 23
 multicast, grupowy, 21
 unspecified, nieokreślony, 21
adresy typu multicast, 26
agent przekazujący, relay agent, 36
AH, Authentication Header, 419
aktualizacje wyzwalane, triggered updates, 120
algorytm
 link state, 172
 MD5, 199
 SPF, 172
algorytmy haszujące, 420
APIPA, Automatic Private IP Addressing, 18
ARP, 26, 41
AS, Autonomous System, 270
ASBR, Autonomous System Boundary Router, 205
AS-PATH, 321
atak typu
 ARP spoofing, 50
 DDoS, 457
 DoS, 454
 fałszywego serwera DHCPv6, 49
 IP spoofing, 50, 454
 Man In The Middle, 44, 159
atrybut
 AS-Path, 272, 345
 atomic aggregate, 273
 local preference, 273
 Local Preference, 342, 344
 MED, 347
 Next-hop, 273
 Origin, 273
 Origin Code, 346
 Weight, 338, 340

atrybuty
 ścieżki, path attributes, 272
 w BGP, 337
autosumaryzacja, 312

B

baza danych LSDB, 179
BDR, Backup Designated Router, 186
bezpieczeństwo sieci, 44
 funkcjonalność CoPP, 457
 listy ACL, 442
 mechanizm uRPF, 454
bezzastanowy serwer DHCPv6, 31
BFD, Bidirectional Forwarding Detection, 106
 działanie, 106, 109
 konfiguracja, 107
 OSPF, 107
BGP, Border Gateway Protocol, 269
 adresacja IPv6, 350
 analiza problemu, 285
 atrybuty, 272, 274, 337
 direct peering, 275
 działanie, 270
 filtrowanie tras, 315, 316, 321, 323, 328
 funkcjonalność maximum-prefix, 336
 grupowanie sąsiadów, 337
 grupowanie tras, 328
 IPv4, 312
 IPv6, 352
 filtrowanie prefiksów, 357
 filtrowanie tras, 363
 mechanizm route map, 324, 357
 mechanizm route reflector, 297, 355
 sumaryzacja, 354
 uwierzytelnianie, 359
 komunikaty, 272
 konfederacje, 300
 konfiguracja podstawowa, 277
 konfiguracja zaawansowana, 312, 352
 maszyna stanowa, 276
 multihop peering, 275
 pętle routingu, 299
 polecenia weryfikujące, 282
 protokół eBGP, 302
 protokół iBGP, 288
 redystrybucja, 309
 rodzaje relacji, 275
 rozgłaszanie prefiksów, 286

BGP, Border Gateway Protocol
 rozgłaszanie sieci, 306
 rozwiązywanie problemów, 365
 uwierzytelnianie, 285
 Binding Table, 52
 broadcast, 195

C

CE, Customer Edge, 389
 CEF, Cisco Express Forwarding, 56–58
 CoPP, Control Plane Policing, 457
 konfiguracja, 458
 monitorowanie działania, 463
 czas wstrzymania, hold down timer, 120

D

DAD, Duplicate Address Detection, 24
 debugowanie warunkowe, conditional
 debugging, 484
 DHCP, Dynamic Host Configuration Protocol, 11
 działanie serwera, 17
 przydzielanie adresu IPv4, 12
 rozwiązywanie problemów, 18
 SLA, 493
 DHCPv6
 Guard, 47
 komunikaty, 37
 serwer bezstanowy, 31
 router jako klient, 34
 weryfikacja ustawień, 34
 serwer stanowy, 34
 agent przekazujący dane, 36
 weryfikacja ustawień, 35
 DMVPN, Dynamic Multipoint VPN, 418
 analiza pakietów, 432, 439
 konfiguracja bez IPsec, 423
 konfiguracja z IPsec, 434
 dostęp do urządzeń, 467
 DR, Designated Router, 186
 drother, 186, 189
 DUAL, Diffusing Update Algorithm, 114
 dystans administracyjny, AD, 64

E

eBGP, External BGP, 271, 302
 łączy redundantne, 305
 Multihop, 302
 edytor nano, 53
 EGP, Exterior Gateway Protocols, 269
 EIGRP, Enhanced Interior Gateway Routing
 Protocol, 75, 79, 87, 114, 425
 błędy konfiguracyjne, 147
 brak komunikacji, 141, 147
 interfejs pasywny, 125
 konfiguracja, 115
 alternatywna, 130
 interfejsu pasywnego, 131
 routera stub, 127

metryka, 122
 osiągnięcie zbieżności, 131
 pętle routingu, 119
 rodzaje pakietów, 120
 rozgłaszanie tras, 125
 rozwiązywanie problemów, 134
 uwierzytelnianie tras, 126
 zużycie pasma, 134
 EIGRPv6
 konfiguracja, 150
 konfiguracja alternatywna, 151
 polecenia weryfikujące, 163
 rodzaje pakietów, 154
 rozwiązywanie problemów, 164
 sumaryzacja, 158
 uwierzytelnianie, 159
 uwierzytelnianie HMAC SHA2-256, 162
 weryfikacja routingu, 153
 ESP, Encapsulating Security Payload, 261, 419

F

falszywe komunikaty RA, 46
 FEC, Forwarding Equivalence Class, 373
 FHS, First Hop Security, 43
 FIB, Forwarding Information Base, 58, 372
 filtrowanie
 obszaru, area filtering, 249
 pakietów, 357
 prefiksów, 357
 tras, 249, 359
 tras w BGP, 315, 321, 323, 328, 363
 tras w OSPF, 249
 FSM, Finite State Machine, 275
 funkcja filtrowania tras, 359
 funkcjonalność
 agent przekazujący, 17, 36
 BFD, 106
 Binding Table, 52
 CoPP, 457
 debugowanie warunkowe, 484
 DHCPv6 Guard, 47
 grupowanie tras, 328
 IP SLA, 487
 IPv6 Source Guard, 50
 key chain, 360
 maximum-prefix, 336
 ND Inspection, 52
 passive-interface, 135, 148, 242, 256
 PBR, 98, 99
 PE-CE routing, 388
 powiadomienie o zmianach w konfiguracji, 485
 prefix-list, 249
 RA Guard, 44
 RA Snooping, 53
 redystrybucja, 76
 route map, 86, 324
 route reflector, 355
 SLAAC, 28
 Snooping DHCPv6, 50
 stub, 128

stubby, 221
 sumaryzacja tras, 95, 158
 tracking, 494
 Traffic Engineering, 373
 uRPF, 454
 VRF, 97, 101

G

GUA, Global Unicast Address, 30

H

haszowanie, 421
 HMAC SHA2-256, 162
 HTTP, 472

I

iBGP, Internal BGP, 271, 288
 konfiguracja, 289, 296
 konfiguracja w ISP, 395
 problem skalowalności, 297
 identyfikator
 obszaru, Area ID, 173
 routera, router ID, 174, 246, 252
 SPI, 261
 IKE, Internet Key Exchange, 420
 integralność danych, 420
 interfejs pasywny, 131, 256
 IOS Peer Groups, 337
 IP LFA, IP Loop-Free Alternate, 387
 IP SLA, IP Service Level Agreement, 487
 działanie, 487
 funkcjonalność tracking, 494
 konfiguracja, 493
 responder, 491
 rozwiązywanie problemów, 487
 testy UDP jitter, 490
 IPsec, 418
 IPv4, 11
 przydzielanie adresów, 12
 IPv6, 20
 adresy typu multicast, 26
 First Hop Security, 43
 funkcjonalność SLAAC, 28
 nagłówki, 21
 początek komunikacji, 29
 proces EUI-64, 22
 przydzielanie adresów, 22
 rodzaje adresów, 21
 Source Guard, 50
 w BGP, 350
 ISP
 konfiguracja iBGP, 395
 konfiguracja OSPF, 396

K

komunikacja, 40
 komunikat, *Patrz także* pakiet
 BGP
 KEEPALIVE, 272
 NOTIFICATION, 272
 OPEN, 272
 UPDATE, 272, 287
 DHCP, 12, 17
 Ack, 15
 Decline, 17
 Discover, 13, 14, 17
 Inform, 17
 NAK, 17
 Offer, 13, 14, 17
 Release, 17
 Request, 17
 DHCPv6, 37
 Advertise, 37, 38
 Confirm, 38
 Decline, 40
 Information-request, 40
 Neighbour Advertisement, 27
 Network Solicitation, 27
 Rebind, 39
 Reconfigure, 40
 Relay-forward, 40
 Relay-replay, 40
 Release, 40
 Renew, 38
 Reply, 39
 Request, 37, 38
 Solicit, 37
 Solicited-Node Address, 27
 EIGRP
 Query, 122, 127
 Update, 90, 121
 EIGRPv6
 Query, 156
 Update, 157
 ICMPv6, 24
 Neighbour Advertisement, 24
 Network Solicitation, 24
 LS Update, 209
 NHRP Registration Request, 425
 RA, Router Advertisement, 28–36, 44, 53
 RS, Router Solicitation, 28, 29
 RSVP-TE, 373
 State DROTHER, 188
 syslog, 481
 Type: Transit, 189
 komunikaty
 NDP, 52
 NLRI, 286
 konfederacja, confederation, 300
 konsola logowania, logging console, 481

L

LDP, Label Distribution Protocol, 372, 383, 386, 401
 LER, Label Edge Router, 372
 LFIB, Label Forwarding Table, 372
 LIB, Label Information Base, 373, 384
 listy
 ACL, 91, 249, 321, 363, 442
 extended ACL, 68, 316, 443, 445
 konfiguracja, 68, 71, 445, 447
 reflective ACL, 68
 rozwiązywanie problemów, 448
 standard ACL, 67, 442, 443
 dystrybucyjne, 249
 offsetowe, offset-lists, 83
 oparte na czasie, 446
 prefiksów, prefix lists, 72, 323, 327, 453
 loopback, 195
 LSA, Link State Advertisement, 172
 typy pakietów, 205
 Type 1, Router link, 208
 Type 2, Network link, 209
 Type 3, Summary link, 211
 Type 4, ASBR Summary, 213, 215
 Type 5, External Routes, 215, 216
 Type 7, NSSA External Summary, 225
 LSAck, Link State Acknowledgment, 173
 LSDB, Link State Database, 179
 LSP, Label Switched Path, 383
 LSP, Link State Packet, 172
 LSR, Label Switching Router, 372
 LSR, Link State Request, 172
 LSU, Link State Update, 172

M

maksymalny dystans, max distance, 119
 mapy trasy, route maps, 85, 324
 konfiguracja, 87, 91, 93, 94
 maszyna stanowa BGP, 276
 MED, Multi Exit Discriminator, 347
 metryka
 w EIGRP, 122
 w OSPF, 226
 MOSPF, Multicast Open Shortest Path First, 205, 260
 MP-BGP, Multiprotocol BGP, 350
 aktywacja dla IPv6, 350, 352
 MPLS, Multiprotocol Label Switching, 371
 etykiety do pakietów, 385
 konfiguracja, 374
 Layer 3 VPN, 388
 problem powolnej odpowiedzi, 387
 protokół LDP, 383
 rozwiązywanie problemów, 405–17
 VPN, 396
 analiza trasy, 400
 weryfikacja, 397
 wymiana etykiet, 401

VRF, 390
 weryfikacja iBGP, 398
 wymiana danych, 383

N

NA, Neighbor Advertisement, 52
 NA, Network Advertisement, 24
 narzędzie
 fake_dhcp6, 48
 fake_router6, 44
 parasite6, 51
 radvd, 53
 syslog, 481
 nazywany EIGRP, 130
 ND, Neighbor Discovery, 22
 Neighbor Discovery Inspection, 52
 NetFlow
 działanie, 497
 konfiguracja, 498
 NLRI, Network Layer Reachability Information, 272, 286
 nonbroadcast, 195
 NS, Neighbor Solicitation, 52
 NS, Network Solicitation, 24
 NSSA, Not So Stub Area, 205

O

obszar
 NSSA, 217, 224
 stub area, 216, 222
 stubby OSPF, 221
 totally stub, 217, 223
 tranzytowy, transit area, 231
 TSNSSA, 217, 225
 opóźnienie, delay, 77
 OSPF, Open Shortest Path First, 75, 82, 172
 baza LSDB, 179
 filtrowanie tras, 249
 ID obszaru, 173
 ID routera, 174
 konfiguracja, 174
 konfiguracja alternatywna, 201
 metryka, 226
 relacja sąsiedztwa, 192
 routery DR i BDR, 186, 187, 191, 193
 równoważenie obciążenia, 250
 statusy interfejsu, 178
 statusy urządzeń, 192
 typy pakietu, 181
 typy sieci, 195
 uwierzytelnianie, 198
 w sieci point-to-point, 193
 w sieciach wielodostępowych, 186
 wielooobszarowy, 204
 konfiguracja, 205
 redystrybucja tras statycznych, 219
 sieć nieciągła, 230
 typy obszarów, 215

OSPF, Open Shortest Path First
 wieloobszarowy
 typy pakietów LSA, 205, 208
 typy tras, 215
 wirtualne połączenia, 231
 wybór typu obszaru, 221
 wymiana pakietów LSA, 207
 wymiana informacji, 181
 OSPFv2
 częstotliwość wysyłania pakietów, 241
 filtrowanie obszarów, 249
 konfiguracja passive-interface, 242
 lista dystrybucyjna, 249
 rozwiązywanie problemów, 234
 zmiana identyfikatora routera, 246
 OSPFv3, 252
 interfejs pasywny, 256
 konfiguracja, 254
 szyfrowania, 261
 uwierzytelniania, 260
 wielu obszarów, 256
 polecenia weryfikujące, 258
 rozwiązywanie problemów, 263
 sumaryzacja, 257
 zmiana typu sieci, 257

P

pakiet
 AS-External-LSA, 205
 BGP Update, 332, 334
 database description, 172
 Hello Ack, 120
 hello, 154, 160, 182, 241
 ICMP, 378
 Keepalive, 351, 352
 LDP, 384
 LSA, 172, 179, 185, 189, 205
 LSack, 173, 190
 LSP, 172
 LSR, 172
 LSU, 172
 MOSPF-LSA, 205
 Network-LSA, 205
 NSSA-External-LSA, 205
 query, 121, 156
 reply, 121, 156, 157
 Router-LSA, 205
 SNMP, 480
 Summary-LSA, 205
 update, 121, 155–157
 PBR, Policy Based Routing, 98
 PDM, Protocol-Dependent Module, 114
 PE, Provider Edge, 389
 PE-CE routing, 388
 pętle routingu, 119, 299
 PHP, Penultimate Hop Popping, 384
 PHR, Penultimate Hop Router, 384
 PIM, Protocol Independent Multicast, 455
 podpis elektroniczny, digital signature, 421
 podzielony horyzont, split horizon, 120

polecenia weryfikujące
 BGP, 282
 EIGRPv6, 153, 163
 OSPF, 177
 OSPFv3, 258
 polecenie
 aaa new-model, 473
 accept-lifetime, 360
 access-list [numer_listy] [permit lub deny]
 [adres_źródłowy], 67, 68, 443
 address-family [ipv4_lub_ipv6] unicast auto-
 nous-system [numer_AS], 97, 130
 ipv4, 351, 391
 ipv4 vrf [nazwa_VRF], 394, 396
 ipv6 autonomous-system [numer_AS], 152
 ipv6 unicast, 257, 358
 vpn4, 396
 af-interface [interfejs], 98, 131, 152, 160
 aggregate-address
 [adres_IPv6_zsumaryzowany], 314
 summary-only, 355
 archive, 486
 area [numer_obszaru_sumaryzowanej_sieci]
 [adres_sieci_po_sumaryzacji] [maska_po_
 sumaryzacji], 229
 authentication, 198
 authentication message-digest, 200
 nssa default-information-originate, 224
 stub no-summary, 223
 nssa no-summary, 225
 range [adres_IPv6_zsumaryzowany], 257
 authentication
 mode hmac-sha-256 [hasło], 162
 mode md5, 160
 pre-share, 434
 auto-cost reference-bandwidth [Mb/s], 78, 226
 autonomous-system [numer_AS_dla_EIGRP], 395
 auto-summary, 95, 314
 bandwidth [szerokość_pasma_w_kb/s], 226,
 424
 bfd all-interfaces, 108
 bgp
 bestpath med missing-as-worst, 348
 cluster-id, 299
 confederation identifier [ID_konfederacji],
 301
 default local-preference [wartość], 344
 log-neighbor-changes, 358
 router-id [router_ID], 278, 338, 351
 class [nazwa], 458, 460
 clear
 access-list counters, 319
 ip bgp *, 277, 318, 335
 ip eigrp neighbors, 125, 137
 ip ospf process, 174, 246
 control-plane, 459
 crypto
 ipsec profile [nazwa_profilu], 434
 ipsec transform-set TRANSPORT esp-aes
 esp-sha-hmac, 434
 isakmp policy 1, 434

- polecenie
 - debug [argument], 484
 - condition interface [interfejs], 485
 - eigrp packets, 136
 - ip bgp, 277
 - ip dhcp server events, 19
 - ip dhcp server packet, 19
 - ip ospf [numer_procesu] adj, 235, 237
 - ip ospf hello, 484
 - ip ospf packet, 181
 - ipv6 nd, 23
 - default-information
 - always metric-type 1, 220
 - originate, 206, 255
 - deny global-autoconf, 52
 - description [opis], 392
 - device-role
 - host, 46
 - node, 54
 - router, 46
 - dhcp [adres_serwera_dhcp], 493
 - dir, 469
 - distance ospf external 250, 368
 - distribute-list
 - [numer_listy] [kierunek_in/out], 318, 320
 - prefix [nazwa_listy] [kierunek], 73
 - route-map [nazwa_mapy]
 - [kierunek_in_lub_out], 89
 - eigrp
 - router-id [identyfikator_IPv4], 150, 152
 - stub, 128
 - stub connected, 129
 - enable secret, 486
 - frequency [liczba_sekund], 489
 - hidekeys, 487
 - icmp-echo, 489
 - interface tunel [identyfikator_interfejsu], 424
 - ip access-group 1 ?, 69, 444
 - ip access-list extended [nazwa], 99
 - ip authentication mode eigrp 1 md5, 126
 - ip bandwidth-percent eigrp [numer_procesu] [procent], 134
 - ip cef, 374
 - ip dhcp excluded address, 18
 - ip flow
 - egress, 498
 - ingress, 498
 - ip flow-export
 - destination [IP_kolektora] 2055, 498
 - version [wersja], 498
 - ip helper-address [adres_IP_serwera_DHCP], 16
 - ip http
 - authentication local, 472
 - secure-server, 472
 - server, 472
 - ip mtu [MTU], 425
 - ip next-hop-self, 426
 - ip nhrp
 - authentication [hasło], 425
 - map multicast, 428
 - map multicast dynamic, 425
 - network-id [identyfikator], 425
 - registration no-unique, 431
 - ip ospf [numer_procesu] [numer_obszaru], 202
 - authentication-key [podanie_hasła], 198
 - cost [koszt], 226
 - dead-interval [sekundy], 179, 196, 241
 - hello-interval [sekundy], 179, 196, 241
 - message-digest-key [numer_klucza] md5 [hasło], 200
 - network [typ_sieci], 196
 - network point-to-point, 194
 - priority [wartość_od_0_do_255], 186, 191
 - ip pim sparse-mode, 455
 - ip policy route-map [nazwa_mapy], 100
 - ip prefix-list [nazwa] [permit/deny] adres, 73, 250
 - ip route vrf [nazwa] [adres_docelowy] [maska] [adres_IP_kolejnego_skoku], 105
 - ip scp server enable, 474
 - ip sla [id], 490, 495
 - ?, 488
 - schedule 1 start-time ?, 489
 - ip summary-address eigrp 1 [zsumaryzowana_sieć], 96
 - ip ttl-exception, 377
 - ip verify unicast source
 - reachable-via any, 457
 - reachable-via rx, 455
 - ip vrf [numer_lub_nazwa], 102, 103
 - ipconfig /release6, 40
 - ipv6 address autoconfig, 34
 - ipv6 authentication mode eigrp 1 md5, 161
 - ipv6 dhcp
 - pool [nazwa_puli], 35
 - relay destination [adres_serwera], 36
 - server [nazwa_puli], 32, 35
 - ipv6 eigrp [numer_systemu_autonomicznego], 151
 - ipv6 enable, 24, 25, 34
 - ipv6 nd
 - manager-config-flag, 35
 - other-config-flag, 32
 - raguard attach-policy HOSTY, 47
 - raguard attach-policy ROUTERY, 47
 - ipv6 ospf 1 area 0, 255
 - ipv6 ospf
 - authentication ipsec spi [numer_indeksu] [metoda], 261
 - encryption ipsec spi 256 [metoda_szyfrowania] [klucz] sha1 [klucz], 261
 - network point-to-point, 266
 - ipv6 router
 - eigrp [numer_systemu_autonomicznego], 150
 - ospf 1, 255
 - ipv6 unicast-routing, 30, 150, 254, 350
 - key [ID klucza], 360
 - key chain [nazwa_łańcucha], 126, 161, 360
 - key-string [hasło], 126, 161, 360

- logging
 - buffered [wartość_bufora], 482
 - host [adres_ip_hosta], 484
 - size [liczba_wpisów], 486
 - synchronous level [numer_poziomu_komunikatów], 482
 - trap [rodzaj_komunikatu], 484
- mac-address [nowy_adres_MAC], 23
- match, 341
- maximum-paths [liczba_tras], 251
- maximum-paths ibgp 2, 397
- mpls
 - ip, 374, 408
 - label range [dolny_zakres] [górny_zakres], 385
 - ldp router-id Loopback0 force, 387, 406
- neighbor [adres_IP_sąsiada]
 - activate, 396, 415, 416
 - disable-connected-check, 303
 - ebgp-multihop [wartość_ttl], 304
 - maximum-prefix [maksymalna_liczba_prefiksów], 336
 - password [hasło_klucza], 286
 - peer-group [nazwa_grupy], 337
 - prefix-list [lista] [kierunek], 323
 - remote-as [numer_AS_sąsiada], 278, 297, 326
 - route-map [nazwa_mapy] [kierunek in/out], 326, 331, 341
 - route-reflector-client, 297
 - send-community [standard | extended | both], 330, 396
 - update-source [IP_źródłowy], 292
- netsh interface ipv6
 - set privacy state=disabled, 27
 - show neighbors, 28
- network [adres_do_rozgłoszenia] [wild-card_mask] [obszar] , 72, 175
- next-hop-self, 294
- no ip mtu, 245
- no ip ospf network, 240
- no ipv6 nd managed-config-flag, 31
- no mpls ip, 385
- no neighbor [adres_ip] disable-connected-check, 304
- no passive-interface [interfejs], 242
- no router eigrp [identyfikator_AS], 97
- notify syslog, 486
- offset-list ?, 84
- ospfv3 network, 258
- passive-interface [adres_IP_interfejsu_do_zablokowania] , 131, 256
- passive-interface default, 242, 256
- permit link-local, 52
- ping [adres_ip] -l [długość_wiadomości] -c [liczba_prób], 100, 460
- police ?, 458
- policy-map [nazwa_polityki], 460
- rd [typ/identyfikator:identyfikator], 391
- redistribute [rodzaj_protokołu] [numer_procesu], 311
 - bgp, 395
 - connected, 346
 - connected route-map [nazwa_mapy], 94, 347
 - ospf [numer_procesu] metric [metryka], 77, 113, 311
 - static subnets metric [wartość_metryki] metric-type 1, 220
 - static, 126
 - static subnets, 220
- request-data-size [bajty], 490
- remote-as, 291
- route-map [nazwa] [warunek] [numer_sekwencyjny], 86, 91, 324
- router bgp [numer_AS], 278
- router eigrp [numer_procesu] [parametr_dodatkowy], 97, 115, 128, 130, 152
- router ospf [numer_procesu] vrf [nazwa_VRF], 105, 175, 396
- router-id [identyfikator_w_formie_adresu_ip], 115, 175, 246, 252, 255
- route-target export, 391
- send-lifetime, 360
- service, 483
- set, 341
 - as-path prepend [identyfikatory_systemów_autonomicznych], 345
 - community no-advertise, 331
 - community no-export, 329
 - ipv6 next-hop [adres_IPv6_sąsiada], 353
 - local-preference [wartość], 344
 - metric [dane_do_metryki], 94
 - origin igp, 347
- sh ip bgp summ, 369
- sh run | s router bgp, 415
- sh run | section ospf, 235
- sh runn | section authentication, 237
- sh runn | section ipv6 ospf, 264
- show access-list, 99, 248
- show access-lists, 444
- show adjacency
 - detail, 60
 - summary, 60
 - vlan 99 detail, 61
- show archive log config all, 487
- show archive log config all provisioning, 487
- show bfd neighbors, 108
- show bfd neighbors details, 108
- show bgp
 - ipv4 unicast neighbors [adres_IP_sąsiada], 281, 283
 - ipv4 unicast summary, 282, 336
 - ipv6 unicast summary, 356, 361
- show cdp neighbors, 165
- show cef not-cef-switched, 61
- show crypto
 - engine connections active, 436
 - ipsec policy, 261, 262
 - isakmp sa detail, 437
 - map, 437
- show debug condition, 485
- show dmvpn, 438
- show eigrp address-family ipv6 interfaces, 164

polecenie

- show int fa0/0 | incl bia, 25
- show interface [identyfikator_interfejsu], 122, 123
- show interface g0/0 | include bia, 23
- show ip access-lists, 69
- show ip bgp [adres_sieci], 315
 - bestpath, 287
 - neighbors [adres_sasiada] received-routes, 286
 - neighbors [adres_sasiada]
 - advertised-routers, 317, 413
 - summary, 278, 291
 - vpn4 all, 398
 - vpn4 all summary, 415
- show ip cache flow, 498
- show ip cef, 60
- show ip cef adjacency glean, 61
- show ip dhcp
 - binding, 18, 493, 494
 - conflict, 18
 - snooping binding, 53
- show ip eigrp
 - interface, 145
 - interfaces, 136, 431
 - neighbor, 110, 116
 - neighbors, 139, 144
 - neighbors detail, 129
 - topology [adres_sieci], 83, 117
 - topology all-links, 85
- show ip flow export, 499
- show ip http client all, 471
- show ip interface brief, 142
- show ip nhrp, 428, 429
- show ip ospf
 - database, 180, 208, 211
 - database asbr-summary, 214
 - database external, 215
 - database network, 210
 - database nssa-external, 226
 - database router, 209
 - database summary, 212
 - int brief, 368
 - interface [identyfikator_interfejsu], 177, 193, 196, 203, 241
 - interface brief, 177, 232, 239
 - neighbor, 178, 192, 204, 243
 - virtual-links, 232, 236, 238
- show ip policy, 100
- show ip prefix-list [nazwa], 73, 74, 453
- show ip protocols, 125, 145, 246, 394
- show ip route [konkretny_adres], 141, 308
 - eigrp, 74, 77
 - ospf, 176
 - static, 126
 - vrf [nazwa], 104
- show ip rp [adres_sieci], 456
- show ip sla
 - application, 492
 - configuration, 490
 - responder, 491
 - statistics, 492
- show ip vrf, 392, 393
- show ip vrf interface, 411
- show ipv6 dhcp
 - binding, 35
 - guard policy, 49
 - interface [interfejs_przekazujacy], 37
 - pool, 34, 35
- show ipv6 eigrp
 - interfaces, 153, 169
 - neighbors, 163, 167, 169
- show ipv6 int
 - fa0/0, 25
 - g0/0 | inc FF|EE|joinet|global, 24
- show ipv6 neighbors, 153
- show ipv6 ospf
 - int brief, 264
 - interface brief, 255
 - neighbor, 264–267
 - neighbors, 255
- show ipv6 protocols, 152, 154, 163, 167
- show ipv6 route [szukana_siec], 153, 164
- show ipv6 snooping policies, 50, 52, 55
- show key chain BGP_ KEYCHAIN, 361
- show logging, 482
- show mpls
 - forwarding-table, 375
 - ldp binding, 386
 - ldp neighbor, 407, 408, 412
- show ospfv3
 - database, 259
 - interface [interfejs], 258
 - interface brief, 257–259
- show policy-map control-plane, 459, 463
- show route-map, 99, 341
- show running-config, 450
- show running-config | section router eigrp, 143
- show snmp, 478
 - community, 478
 - user, 479
- show tcp brief, 276
- show vrf, 102
 - detail, 410
 - interface, 410
- shutdown, 189
- snmp-server
 - community
 - [nazwa_łańcucha_środowiskowego_snmp]
 - ro [nazwa_lub_numer_listy_ACL], 477
 - contact [kontakt], 477
 - enable traps, 477
 - host
 - [adres_ip_stacji_odbierajacej_komunikaty_snmp] version 2c [nazwa_łańcucha], 477
 - location [nazwa_lokalizacji], 477
- sudo
 - nano /etc/radvd.conf, 53
 - parasite6 eth0 -l, 50
 - radvd, 54

- summary-address
 - [adres_ipv6_zsumaryzowany/długość_prefiksu], 98, 158, 171
 - terminal monitor, 481, 484
 - tftp-server disk0:running-config, 469
 - trace, 124
 - traceroute, 101
 - track 1 ip sla 1 reachability, 496
 - tracking
 - disable, 55
 - enable, 54
 - tunnel
 - source [interfejs_źródłowy_tunelu], 426
 - key [wartość_klucza], 426
 - protection ipsec profile [nazwa_profilu], 434
 - udp-jitter [IP_docelowe] [PORT] source-ip [IP_źródłowe] num-packet [liczba_pakietów] interval [czas], 490
 - undebg all, 484
 - username, 472
 - vrf
 - definition [nazwa], 391
 - forwarding [nazwa_VRF], 392
 - proces
 - EUI-64, 22
 - neighbor discovery, ND, 22
 - program
 - Kiwi Syslog, 476
 - PuTTY, 482
 - Wireshark, 189
 - protokoły
 - haszujące, 419
 - negocjacyjne, 419
 - ochrony procesu wymiany kluczy, 419
 - symetrycznego szyfrowania, 419
 - protokół
 - ARP, 26, 42
 - BFD, 106
 - BGP, 269
 - DHCP, 11
 - eBGP, 271
 - EIGRP, 75
 - EIGRPv6, 150
 - iBGP, 271
 - IPsec, 418
 - IPv4, 11
 - IPv6, 20
 - LDP, 383
 - OSPF, 75
 - OSPFv2, 234
 - OSPFv3, 252
 - PIM, 455
 - RSVP-TE, 373
 - SCP, 473
 - SNMP, 475
 - TFTP, 468
 - przełączanie procesowe, process switching, 59
 - przełączany wirtualny interfejs, SVI, 58
 - przełączniki, 56
 - wielowarstwowe, 56
 - przepustowość, bandwidth, 77
- ## R
- RA, Router Advertisement, 44, 52
 - Guard, 44
 - Snooping, 53
 - ramka ICMP, 42
 - redystrybucja, redistribution, 76
 - EIGRP-EIGRP, 79
 - OSPF do EIGRP, 75
 - OSPF-OSPF, 82
 - rozwiązywanie problemów, 109
 - tras statycznych, 219
 - w BGP, 309
 - relacja sąsiedztwa, 192
 - router
 - ABR, 204, 228
 - ASBR, 205
 - BDR, 186, 187, 191, 193
 - CE, 389, 394
 - DR, 186, 187, 191, 193
 - PE, 389, 394
 - stub, 127
 - routing, 63
 - oparty na politykach, PBR, 98
 - równoważenie obciążenia, load balancing, 251
 - RR, Route Reflectors, 297, 355
 - RS, Router Solicitation, 52
 - RSVP-TE, 373
 - RTP, Reliable Transport Protocol, 114
- ## S
- scalanie tras, 388
 - SCP, Secure Copy Protocol, 473
 - serwer
 - DHCPv6
 - bezstanowy, 31
 - stanowy, 34
 - HTTP, 472
 - TFTP, 468
 - sham-link OSPF, 390
 - siatka połączeń, full mesh, 297
 - sieci wielodostępowe, 186
 - sieć
 - ISP, 395
 - MPLS, 371
 - nieciągła, 230
 - redundantna, 305
 - typu
 - broadcast, 195
 - loopback, 195
 - nonbroadcast, 195
 - point-to-multipoint, 195
 - point-to-point, 193, 195
 - VPN, 388, 421
 - SLA, 493
 - SLAAC, Stateless Address Autoconfiguration, 28, 52, 53

SNMP

- działanie, 475
- rozwiązywanie problemów, 474

SNMPv2

- konfiguracja, 476

SNMPv3

- konfiguracja, 479

Snooping DHCPv6, 50**SPF, Shortest Path First, 172****SPI, Security Parameter Index, 261****stan łączy, link state, 172****stanowy serwer DHCPv6, 34****sumaryzacja, 95**

- automatyczna, 96
- dla różnych instancji, 97
- dynamiczna, 312
- na routerze ABR, 228
- ręczna, 96
- statyczna, 312
- w BGP IPv4, 312
- w BGP IPv6, 354
- w IPv6 OSPF, 257

SVI, Switched Virtual Interface, 58**szyfrowanie, 419**

- asymetryczne, 420
- w OSPFv3, 261

T**tabela dystansów administracyjnych, 64****tablica**

- przełączania, forwarding table, 58
- routingu, control plane, 43, 58
- sąsiedztwa, adjacency table, 58
- topologii, topology table, 117

TFTP

- kody błędów, 470
- transfer plików, 468

TLV, Type, Length, Value, 272**transfer plików**

- przez HTTP, 471
- przez SCP, 473
- za pomocą TFTP, 468

trasy statyczne, static route, 64, 219**typy**

- obszarów, 215, 221
- pakietów LSA, 205
- tras, 216

U**UDP jitter, 490****uRPF, unicast Reverse Path Forwarding, 454****urząd certyfikacji, CA, 420****urządzenia**

- konfigurowanie, 467, 468
- transfer plików, 468

usługi

- bezstanowe, stateless services, 30
- stanowe, statefull services, 30

uwierzytelnianie, 421

- nagłówek, authentication header, 260
- w BGP, 285
- w BGP IPv6, 359
- w EIGRP, 126
- w EIGRPv6, 159
- w OSPF, 198
- w OSPFv3, 260

V**VPN, Virtual Private Network, 388, 421**

- w MPLS, 396, 398

VRF, Virtual Routing and Forwarding, 101

- dla MPLS, 390
- działanie, 101
- konfiguracja, 103

W**wielookszarowy OSPF, 204****wirtualne łączy, 231****wykrywanie zdublowanych adresów, 24****wrażenia regularne, regular expressions, 321****Z****zapytanie ARP, 41****zatrucie trasy, route poisoning, 119****zdarzenia, 481****znaki specjalne, 322**

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion 

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 dokumentację 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



Cena: 169,00 zł