6. Routing z wykorzystaniem stanu łącza, OSPF

6.1. Routing stanu łącza a routing wektora odległości

Zasada działania protokołów routingu według stanu łącza jest inna niż w przypadku protokołów działających na podstawie wektora odległości. Na poniższych rysunkach przedstawiono cechy obu rodzajów protokołów:

Protokół	Przykłady	Cechy
Według wektora odległości	RIP v1 i RIP v2 IGRP (ang. Interior Gateway Routing Protocol)	• Kopiuje tablice routingu do sąsiadów. • Często dokonuje aktualizacji. • Protokoły RIP v1 i RIP v2 jako metryki używają licznika przeskoków. • Korzysta z obrazu sieci z perspektywy sąsiadów. • Jest wolno zbieżny. • Umożliwia powstanie pętli routingu. • Jest łatwy w konfigurowaniu i w administrowaniu. • Ma duże zapotrzebowanie na pasmo.
Według stanu łącza	OSPF (ang. Open Shortest Path First) IS-IS (ang. Intermediate-System to Intermediate-System)	• Używa algorytmu Shortest Path. • Aktualizacje są wyzwalane zdarzeniami. • Wysyła pakiety o stanie łącza do wszystkich routerów w sieci. • Korzysta ze wspólnego obrazu sieci. • Jest szybko zbieżny. • Jest mniej podatny na powstawanie pętli routingu. • Jest trudniejszy do skonfigurowania. • Wymaga większej ilości pamięci i mocy obliczeniowej niż protokoły działające według wektora odległości. • Ma mniejsze zapotrzebowanie na pasmo niż protokoły działające według wektora odległości.

Algorytm routingu według stanu łącza utrzymuje skomplikowaną bazę danych zawierającą informacje o topologii sieci. Podczas gdy algorytmy działające w oparciu o wektor odległości gromadzą ogólne informacje na temat odległych sieci i nie dają wiedzy na temat odległych routerów, algorytm routingu według stanu łącza dysponuje pełną informacją o odległych routerach i ich wzajemnych połączeniach.

6.2. Sposoby utrzymywania informacji o routingu

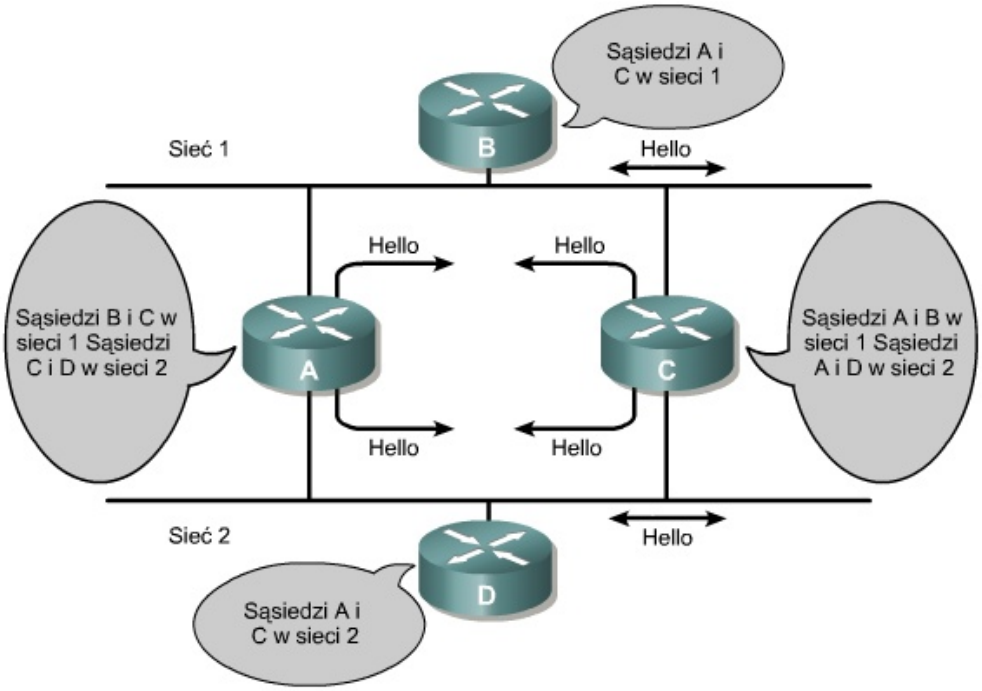
Protokoły routingu według stanu łącza korzystają z następujących elementów:

- ogłoszeń LSA (*Link-State Advertisement*);
- bazy danych o topologii;
- algorytmu SPF (*Shortest Path First*);
- drzewa SPF;
- tablicy routingu tras.

Protokoły routingu z wykorzystaniem stanu łącza zostały zaprojektowane w celu eliminacji ograniczeń protokołów routingu opartych na wektorze odległości. Protokoły działające na podstawie wektora odległości wymieniają informacje aktualizujące jedynie z bezpośrednimi sąsiadami, podczas gdy protokoły routingu według stanu łącza wymieniają informacje o routingu na znacznie większym obszarze.

Wymiana pakietów LSA (oprócz pakietów *Hello*) jest wyzwalana przez wystąpienie zdarzenia w sieci, nie jest natomiast cykliczną aktualizacją. Przyspiesza to proces osiągania zbieżności, ponieważ nie trzeba czekać na upłynięcie limitu czasu na wielu zegarach.

Określanie sąsiedztwa pomiędzy routerami odbywa się za pomocą rozsyłania pakietów *Hello*. Każdy router wysyła okresowo pakiety *Hello* do przyległych sąsiadów, informując je o swoim istnieniu i sprawnym działaniu. Mechanizm ten umożliwia wykryć, że dany router przestał odpowiadać.



Łącze jest równoważne interfejsowi routera. Stan łącza jest opisem interfejsu oraz relacji z sąsiednimi routerami. Opis interfejsu może na przykład zawierać adres IP interfejsu, maskę podsieci, typ sieci, do której jest przyłączony, routery dołączone do danej sieci itp. Zbiór stanów poszczególnych łączy stanowi bazę danych stanów łączy, która jest nazywana **bazą danych o topologii**. Baza danych stanów łączy służy od obliczania najlepszych tras w

sieci. Routery wykorzystują w tym celu algorytm Dijkstry (**Shortest Path First**). Algorytm ten tworzy **drzewo SPF**, którego korzeniem jest lokalny router. Następnie w drzewie SPF są wyszukiwane najlepsze ścieżki, które zostają umieszczone w **tablicy routingu**.

6.3. Zalety i wady routingu według stanu łącza

Zalety:

- Przy wyborze tras przez sieć protokoły routingu według stanu łącza używają metryki kosztu. Metryka kosztu odzwierciedla przepustowość łączy na tych trasach;
- Protokoły routingu według stanu łącza używają wyzwalanych aktualizacji oraz rozpływowego przekazywania pakietów LSA, aby móc natychmiast powiadamiać wszystkie routery w sieci o zmianach jej topologii. Prowadzi to do szybkiej zbieżności;
- Każdy router dysponuje pełnym i zsynchronizowanym obrazem sieci. Z tego powodu powstawanie pętli routingu jest bardzo utrudnione;
- Routery dokonują wyboru najlepszych tras na podstawie najświeższych informacji;
- Każdy router dysponuje przynajmniej topologią własnego obszaru sieci. Ta cecha pozwala rozwiązywać pojawiające się problemy;
- Protokoły routingu według stanu łącza obsługują notacje CIDR i VLSM.

Wady:

- Wymagają większej ilości pamięci i mocy obliczeniowej niż protokoły działające na podstawie wektora odległości. Na skutek tego koszty ich stosowania w organizacjach dysponujących mniejszym budżetem i starszym sprzętem są znacznie wyższe;
- Wymagają ściśle hierarchicznego projektu sieci, gdzie sieć jest podzielona na mniejsze obszary w celu zmniejszenia tablic topologii;
- Wymagają pracy administratora dobrze rozumiejącego działanie tych protokołów;
- Podczas początkowego procesu wykrywania sieć jest zalewana pakietami LSA. Proces ten może znacząco zmniejszyć możliwość przesyłania danych w sieci. Może to w widoczny sposób obniżyć wydajność sieci.

6.4. Protokół OSPF — główne cechy

Protokół wyszukiwania najkrótszej ścieżki OSPF (*Open Shortest Path First*) jest protokołem IGP (routing w obrębie jednego systemu autonomicznego). Został on dokładnie opisany w dokumencie RFC 2328 (druga wersja OSPF). Swoją popularność w sieciach IP zawdzięcza kilku cechom. Jest rozwiązaniem bezklasowym, w pełni obsługującym techniki CIDR i VLSM. Doskonale poddaje się skalowaniu. Gwarantuje krótki czas konwergencji sieci i brak pętli. Nie ma zatem zdefiniowanej maksymalnej liczby przeskoków. Udostępnia mechanizm uogólniania tras i oznaczania tras zewnętrznych, podobnie jak EIGRP. W sieciach, w których wymagany jest dodatkowy poziom zabezpieczeń, można w taki sposób skonfigurować routery OSPF, aby w trakcie komunikacji z innymi urządzeniami tego typu korzystały z uwierzytelnienia. Komunikaty w OSPF korzystają z TCP/IP. Przy wymianie komunikatów LSA, OSPF korzysta z rozgłaszania grupowego. Umożliwia także podział sieci na obszary, ograniczając rozgłaszanie pakietów LSA tylko do nich.

Prawdopodobnie najważniejszym powodem tak dużej popularności OSPF jest fakt, że rozwiązanie stało się otwartym standardem i jest stosowane od dłuższego czasu. Jego obsługa jest uwzględniana przez niemal wszystkich dostawców urządzeń sieciowych. Z tego względu doskonale nadaje się do zastosowania jako protokół routingu w sieciach zbudowanych z urządzeń różnych firm.

6.5. Algorytm stanu łącza

OSPF używa algorytmu stanu łącza by zbudować i wyliczyć najkrótsze trasy do wszystkich znanych sieci. Algorytm ten jest skomplikowany. Poniżej przedstawiono tylko główne założenia i cechy tego algorytmu:

1. Podczas inicjalizacji lub podczas jakiejkolwiek zmiany w sieci, router generuje pakiet LSA, który zawiera informacje o wszystkich łączach routera.

2. Każdy router, który otrzymuje taki pakiet, wykorzystuje go do uaktualnienia informacji w swojej bazie danych topologii i przesyła ten pakiet do pozostałych routerów (*flooding*).

3. Na podstawie bazy danych topologii budowane jest drzewo najkrótszych ścieżek we wszystkich możliwych dostępnych kierunkach. Do tego celu używany jest algorytm Dijkstry. Na podstawie danych z tego drzewa konstruowana jest tablica routingu.

4. W przypadku gdy żadna zmiana w sieci się nie pojawia, OSPF praktycznie się nie komunikuje (oprócz słanych regularnie małych pakietów Hello).

6.6. Pojęcie kosztu – metryka w OSPF

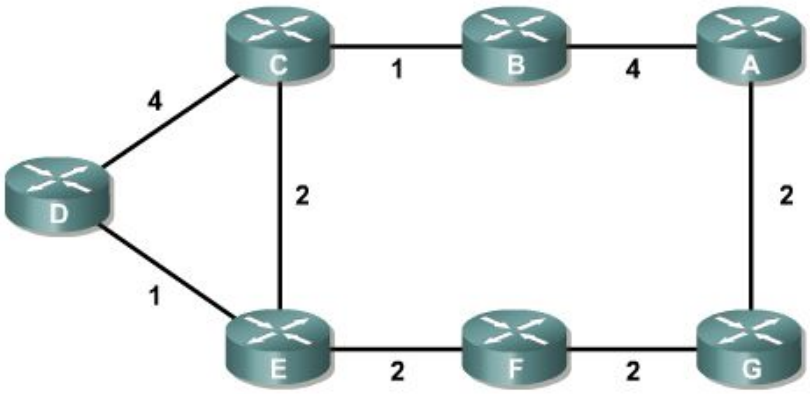
OSPF korzysta z tak zwanych kosztów, przypisanych do każdego łącza (czyli interfejsu) o maksymalnej wartościach z przedziału: 1..65535. Koszt ten domyślnie jest odwrotnie proporcjonalny do szerokości pasma na danym łączu - jest obliczany na podstawie wzoru 10^8/przepustowość, gdzie przepustowość jest wyrażona w b/s.

Typ łącza a przepustowość	Koszt
56-kbps Łącze szeregowe	1785
T1 1.544-Mbps Łącze szeregowe	64
E1 2.048-Mbps Łącze szeregowe	48
4-Mbps Token Ring	25
Ethernet 10 Mb/s	10
16-Mbps Token Ring	6
100-Mbps Fast Ethernet , FDDI	1

W protokole OSPF routery rozpowszechniają koszty pojedynczych łączy, a nie całych tras, tak jak to miało miejsce w RIP czy EIGRP - co za tym idzie nie ma sprecyzowanej maksymalnej wartości kosztu całej trasy.

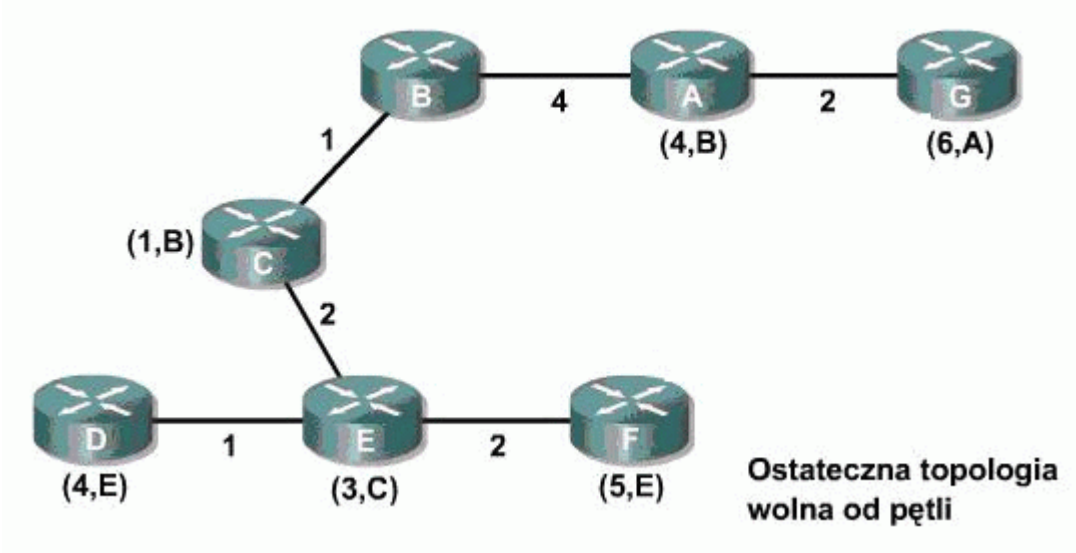
6.7. Algorytm SPF (Shortest Path First)

W przypadku algorytmu SPF najlepszą trasą jest trasa o najniższym koszcie. Algorytm ten został opracowany przez Edsgera Dijkstrę, informatyka holenderskiego, i został opublikowany w roku 1959. Algorytm przedstawia sieć jako zbiór węzłów połączonych przez łącza punkt-punkt. Każdemu łączu jest przypisany koszt. Każdy węzeł ma nazwę. Każdy węzeł dysponuje pełną bazą danych wszystkich łączy, tak więc jest mu znana pełna informacja o topologii fizycznej. Wszystkie bazy danych stanów łączy znajdujące się w danym obszarze są identyczne.



A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

Tablica na powyższym rysunku przedstawia informacje otrzymane przez węzeł B. Otrzymał on informację, że jest połączony z węzłem A łączem o koszcie 4 oraz z węzłem C łączem o koszcie 1.



Następnie algorytm SPF wyznacza topologię wolną od zapętleń, używając danego węzła jako punktu początkowego i odwołując się do posiadanych informacji o przyległych węzłach. Na powyższym rysunku przedstawiono drzewo SPF obliczone dla węzła B. Najlepsza ścieżka do węzła D prowadzi przez węzeł E i ma koszt równy 4. Informacja ta jest zapisywana w pozycji trasy w węźle B, przez który będzie przekazywany ruch do węzła C. W przypadku tej sieci OSPF pakiety z węzła B do węzła D będą przekazywane z B do C, E i następnie do D.

6.8. Pojęcia obszarów i routerów brzegowych w OSPF

Jednym z najważniejszych elementów standardu OSPF jest koncepcja obszaru (*area*) stanowiąca jednocześnie największą trudność przy konfigurowaniu routerów OSPF (wykorzystanie protokołu OSPF w dużych, skalowalnych sieciach wymaga uwzględnienia tego faktu już na etapie ich projektowania). Sieć OSPF można podzielić na obszary, które są łączone za pomocą routerów brzegowych (ABR - *Area Border Router*). Zadanie routerów brzegowych polega na uogólnieniu tras, które są przekazywane poza dany obszar. Dzięki takiemu rozwiązaniu routery z jednego obszaru nie muszą przetwarzać danych LSA istotnych dla routerów innego obszaru, co znacznie zwiększa stabilność pracy sieci i skraca czas konwergencji. Dodatkowo ograniczeniu ulega wykorzystanie pamięci oraz procesora, niezbędnych do obsługi protokołu OSPF w routerze.

Poprawna praca protokołu OSPF zależy od właściwego przydziału adresów IP dla poszczególnych obszarów sieci. Konieczne jest bowiem uogólnienie tras do danego obszaru przy przekazywaniu ich do innego obszaru sieci. Wynikiem procedury uogólniania nie musi być pojedyncza trasa do danego obszaru, ale należy pamiętać, że im mniej komunikatów LSA trzeba rozesłać między obszarami, tym lepszy będzie efekt skalowania OSPF.

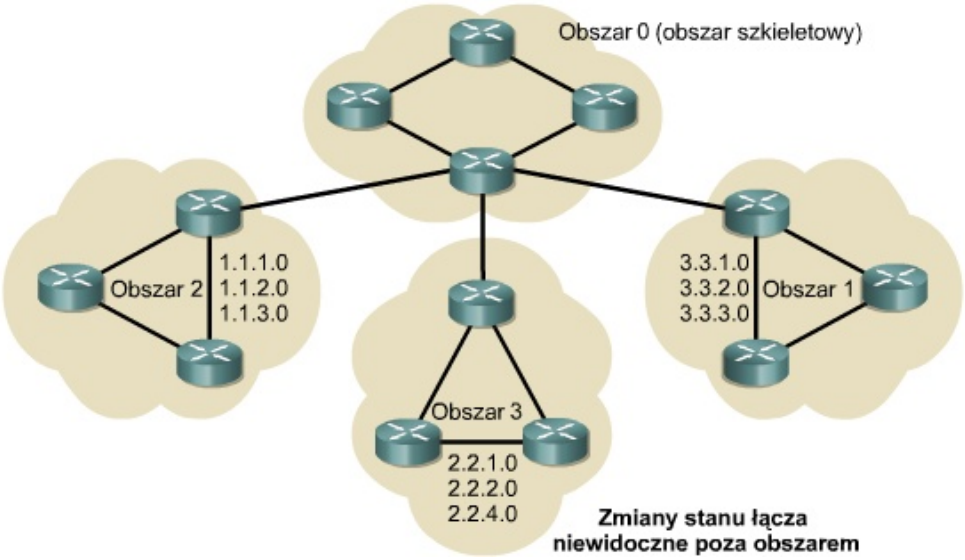
Każdy obszar ma 32-bitowy identyfikator, który często jest zapisywany w postaci dziesiętnej z poszczególnymi bitami rozdzielonymi kropkami (tak samo jak adresy IP). Każda sieć OSPF musi zawierać obszar o identyfikatorze 0 (*Area 0*) lub 0.0.0.0, tzw. obszar szkieletowy, a każdy router ABR musi być należeć do obszaru 0. Rozwiązanie to wymusza hierarchiczny projekt sieci OSPF. Jedyne odstępstwo od tej grupy dotyczy sieci złożonych z jednego obszaru. W takim wypadku obszar ten może mieć dowolny identyfikator, choć nie

zaleca się nadawania mu wartości innych niż zero, gdyż może to utrudnić ewentualne późniejsze wydzielenie innych obszarów sieci.

Wszystkie routery w ramach jednego obszaru mają wspólną bazę danych topologii. Rozgłaszanie pakietów LSA i wyliczanie tras za pomocą algorytmu SPF jest ograniczone do obszarów.

Można wprowadzić następujący podział routerów:

- routery wewnętrzne (IR – *Internal Router*) – to routery, których wszystkie interfejsy należą do jedngo obszaru;
- routery brzegowe (ABR) – to routery, których interfejsy należą do róznych obszarów;
- routery brzegowe systemu autonomicznego (ASBR – *Autonomous System Boundary Router*) – to routery, które pełnią funkcje bram (redystrybucja) pomiędzy OSPF a innymi protokołami routingu (IGRP, EIGRP, RIP, BGP, statyczny) lub innymi instancjami routingu OSPF.



6.9. Sąsiedzi w OSPF

Routery, które dzielą wspólny segment sieci mogą stać się sąsiadami. Pakiety Hello pomagają wykryć sąsiednie routery. Routery stają się sąsiadami jeżeli informacje o nich są wymieniane w pakietach Hello.

Następujące warunki muszą być spełnione by dwa routery mogły zostać sąsiadami:

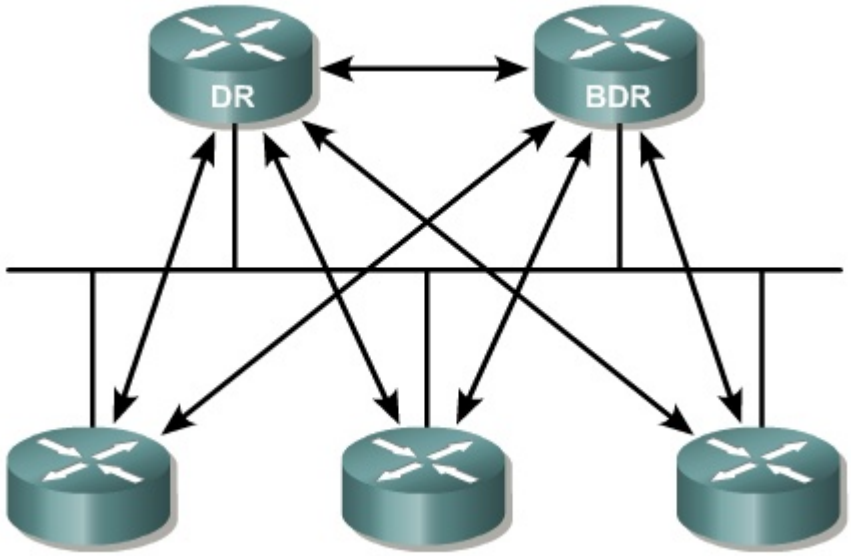
- dwa routery muszą mieć ten sam identyfikator obszaru na sąsiadujących interfejsach. Oczywiście interfejsy muszą należeć do tej samej podsieci i mieć tą samą maskę;
- jeśli włączone jest uwierzytelnianie, interfejsy muszą wymieniać to samo hasło;

- liczniki czasowe muszą się zgadzać: czas pomiędzy wysłaniem dwóch kolejnych pakietów Hello oraz czas przetrzymania, czyli czas, po którego upłynięciu zgłaszana jest niedostępności routera o ile nie napływa od niego żaden komunikat Hello.

6.10. Przyleganie w OSPF

Routery możemy nazwać przyległymi jeśli są sąsiednie i wymieniają się informacjami o topologii. Aby zminimalizować ilość przesyłanych informacji w danym segmencie sieci wielodostępowej, OSPF wybiera router, który zaczyna pełnić role routera desygnowanego (DR – *Designated Router*) i drugi router, który zaczyna pełnić rolę zastępczego desygnowanego routera (BDR – *Backup Designated Router*). Jak sama nazwa wskazuje: jeśli router DR przestanie działać, to BDR przejmuje jego rolę. Dzięki takiemu rozwiązaniu routery mają centralny punkt (router DR) z którym wymieniają informacje o sieci, zamiast wymieniać te informacje ze wszystkimi routerami w danym segmencie.

Aby zagwarantować, że oba routery — DR i BDR — widzą wszystkie stany łączy wysyłane przez wszystkie routery w segmencie, używany jest adres grupowy przeznaczony dla wszystkich routerów desygnowanych, 224.0.0.6. Router DR wysyła informacje o stanie łącza do wszystkich pozostałych routerów OSPF w segmencie za pomocą adresu grupowego 224.0.0.5.



Routery desygnowane mają znaczenie tylko wtedy, gdy do jednego wspólnego medium (np. segmentu Ethernet) przyłączonych jest kilka routerów OSPF. W przypadku sieci punkt-punkt istnieją tylko dwa routery i nie jest wybierany ani router DR, ani BDR. Oba routery są w pełni przyległe do siebie.

6.11. Komunikat OSPF Hello

W warstwie 3 modelu OSI pakiety *Hello* są wysyłane na adres grupowy 224.0.0.5. Pakiety *Hello* są wysyłane domyślnie co 10 sekund w sieciach rozgłoszeniowych, zaś w sieciach punkt-punkt co 30 sekund.

W sieciach wielodostępowych protokół *Hello* służy do wyboru wyznaczonego routera (DR) i zapasowego routera desygnowanego (BDR).

Nagłówek komunikatu OSPF (24 oktety):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	39	31
WERSJA (1)								TYP								DŁ. NAGŁÓWKA															
ADRES IP ROUTERA ŹRÓDŁOWEGO																															
IDENTYFIKATOR OBSZARU																															
SUMA KONTROLNA																TYP UWIERZYTELNIANIA															
UWIERZYTELNIANIE (oktety 0-3)																															
UWIERZYTELNIANIE (oktety 4-7)																															

Opis pól:

WERSJA – wersja protokołu;
TYP:

Typ	Opis
1	Testowanie połączenia (*Hello*)
2	Opis topologii sieci (*Database Description*)
3	Prośba o status łączy (*Link-State Request*)
4	Aktualizacja stanu łączy (*Link-State Update*)
5	Potwierdzenia przyjęcia informacji o stanie łączy (*Link-State Acknowledgment*)

ADRES IP ROUTERA ŹRÓDŁOWEGO – określa adres IP nadawcy komunikatu;
IDENTYFIKATOR OBSZARU – 32-bitowy identyfikator obszaru;
TYP UWIERZYTELNIANIA:

Typ	Opis
0	Brak uwierzytelniania
1	Zwykłe hasło

Dane komunikatu OSPF *Hello*:

Komunikat ten jest wysyłany aby ustalić aktualną osiągalność sąsiadów.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	39	31
MASKA SIECI																															
CZAS PRZETRZYMANIA																OKRES HELLO								PRIORYTET						
DESYGNOWANY ROUTER																															
ZAPASOWY DESYGNOWANY ROUTER																															
ADRES IP SĄSIADA (1)																															

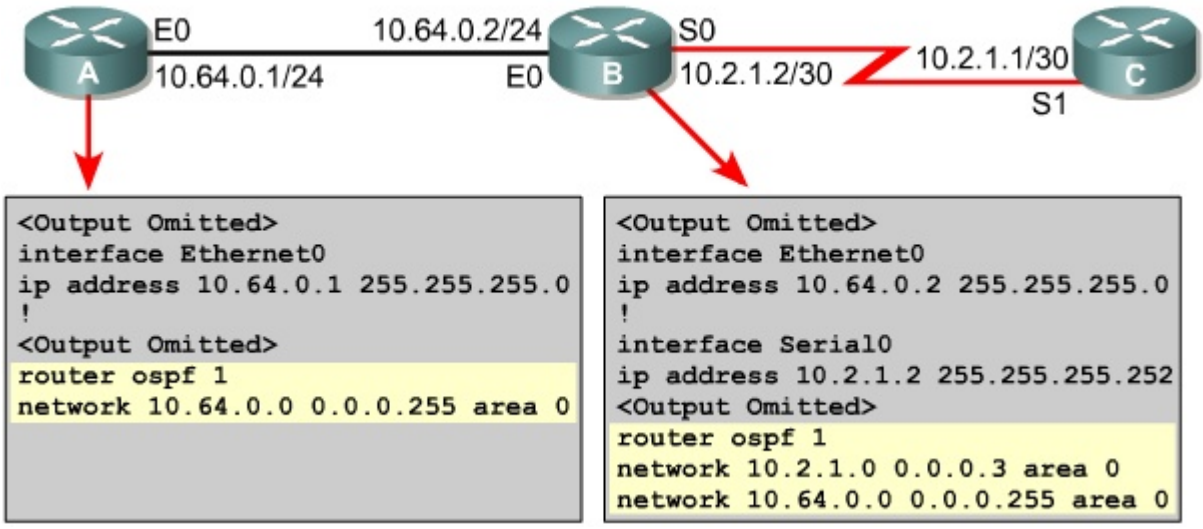
ADRES IP SĄSIADA (2)
...
ADRES IP SĄSIADA (n)

Opis pól:

MASKA SIECI – maska sieci, przez którą przechodził ten komunikat;
CZAS PRZETRZYMANIA – czas (sekundy), po jakim nie zgłaszający się sąsiad zostanie uznany za niedostępny;
OKRES HELLO - okres (sekundy) pomiędzy komunikatami *Hello*
PRIORYTET – określa priorytet danego routera;
DESYGNOWANY ROUTER – adres IP wyróżnionego routera znanego nadawcy;
ZAPASOWY DESYGNOWANY ROUTER – adres IP zapasowego wyróżnionego serwera sieci;
ADRES IP SĄSIADA (n) – adres IP n-tego sąsiada, od którego nadawca otrzymał ostatnio komunikat *Hello*.

6.12. Konfigurowanie procesu routingu protokołu OSPF

Konfigurowanie protokołu OSPF wymaga włączenia procesu routingu OSPF na routerze oraz podaniu adresów sieci i informacji o obszarach:



Aby włączyć routing OSPF, należy użyć polecenia konfiguracji globalnej o składni:

```
Router(config)#router ospf id-procesu
```

Identyfikator procesu jest liczbą używaną do identyfikacji procesu routingu OSPF na routerze. Na tym samym routerze można jednocześnie uruchomić wiele procesów OSPF. Liczba ta może przyjmować wartości z przedziału od 1 do 65 535. Większość administratorów sieci używa tego samego identyfikatora procesu w całym systemie autonomicznym, ale nie jest to obowiązkowe. W praktyce informacje o identyfikatorze

procesu nie opuszczają nawet routera, dlatego dopuszcza się definiowanie różnych wartości identyfikatora w różnych routerach należących do tego samego systemu autonomicznego.

W protokole OSPF sieci IP są ogłaszane w następujący sposób:

```
Router(config-router)#network adres maska-blankietowa area id-obszaru
```

Polecenie network area	Opis
adres	Może to być adres sieci, podsieci lub interfejsu. Stanowi informację dla routera, na których łączach należy oczekiwać ogłoszeń oraz na których łączach ogłaszać informacje.
maska-blankietowa	Jest to odwrotna maska, która służy do określania sposobu odczytywania adresu. Maska zawiera bity blankietowe, w których 0 oznacza dopasowanie, a 1 - nieistotność. Na przykład adres 0.0.255.255 oznacza dopasowanie dwóch pierwszych bajtów. Odpowiadająca mu maska podsieci byłaby 16-bitową maską 255.255.0.0. Maska blankietowa 0.0.0.0 jest używana do określania adresu interfejsu.
identyfikator-obszaru	Wartość ta określa obszar, który ma być powiązany z adresem. Może to być liczba lub też wartość o postaci zbliżonej do adresu IP. W przypadku obszaru szkieletowego identyfikator musi wynosić 0.

Ogólnie identyfikatory obszarów mogą przybierać wartości z przedziału od 0 do 4294967295.

Mechanizm OSPF przetwarza identyfikator obszaru jako 32-bitowe pole niezależne od tego, czy został on wyznaczony za pomocą jednej cyfry czy czterech wartości dziesiętnych rozdzielonych kropkami. Nic nie stoi na przeszkodzie, żeby stosować obydwa sposoby zapisu. Zaleca się jednak wybranie jednego z nich i konsekwentnie używane we wszystkich urządzeniach sieciowych.

6.13. Konfigurowanie adresu pseudosieci (loopback) OSPF i priorytetu routera

Po uruchomieniu procesu OSPF w systemie Cisco IOS najwyższy lokalny aktywny adres IP jest używany jako własny identyfikator routera OSPF (RID). W przypadku braku aktywnego interfejsu proces OSPF nie zostanie uruchomiony. Jeśli interfejs aktywny zostanie wyłączony, proces OSPF utraci identyfikator routera i w związku z tym przestanie działać aż do ponownego włączenia interfejsu.

Aby zapewnić stabilność działania protokołu OSPF, przez cały czas powinien istnieć aktywny interfejs procesu OSPF. W tym celu można skonfigurować interfejs pętli zwrotnej (lopback), będący interfejsem logicznym. Po skonfigurowaniu interfejsu loopback, protokół OSPF używa jego adresu jako identyfikatora routera, niezależnie od jego wartości. W

przypadku routera z więcej niż jednym interfejsem loopback jako identyfikatora routera protokół OSPF używa najwyższego adresu IP interfejsu loopback.

Aby utworzyć i przypisać adres IP do interfejsu loopback, należy użyć następujących poleceń:

```
Router(config)#interface loopback liczba
Router(config-if)#ip address adres-ip maska-podsieci
```

Zaleca się, aby interfejsy pętli zwrotnej były używane na wszystkich routerach, na których uruchomiono protokół OSPF. Interfejs loopback powinien zostać skonfigurowany przy użyciu adresu o 32-bitowej masce podsieci równej 255.255.255.255. Ta 32-bitowa maska podsieci jest nazywana maską hosta, ponieważ określa ona sieć składającą się z jednego hosta. Gdy protokół OSPF musi ogłosić sieć pętli zwrotnej, zawsze ogłasza ją jako trasę do hosta o 32-bitowej masce.

```
! Create the loopback 0 interface
Sydney3(config)#interface loopback 0
Sydney3(config-if)#ip address 192.168.31.33
255.255.255.255
Sydney3(config-if)#exit
! Remove loopback 0 interface
Sydney3(config)#no interface loopback 0
Sydney3(config)#
01:47:27: %LINK-5-CHANGED: Interface Loopback0, changed
state to administratively down
```

Jeśli sieć dla danego interfejsu jest typu rozgłoszeniowego, domyślnym priorytetem protokołu OSPF jest 1. Router o najwyższym priorytecie zostaje wybrany routerem DR, zaś kolejny router o najwyższym priorytecie zostaje wybrany BDR. Jeśli priorytety OSPF są takie same, protokół OSPF wybiera router DR na podstawie identyfikatora routera (RID). Wybierany jest router o najwyższej wartości identyfikatora. Priorytety mogą przyjmować wartości z przedziału od 0 do 255. Po zakończeniu wyborów routery DR i BDR zachowują swoje funkcje, nawet jeśli do sieci dodano routery o wyższych wartościach priorytetu OSPF.

Wartość priorytetu OSPF można zmienić, wydając polecenie konfiguracji interfejsu **ip ospf priority**, który bierze udział w routingu OSPF:

```
Router(config-if)#ip ospf priority liczba
```

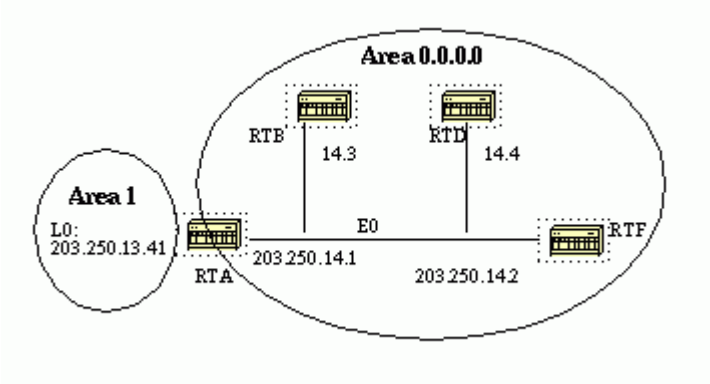
```
Sydney1(config)#interface fastethernet 0/0
Sydney1(config-if)#ip ospf priority 50
Sydney1(config-if)#end
Sydney1#
00:21:57: %SYS-5-CONFIG_I: Configured from console
by console
```

Dzięki poleceniu:

```
Router#show ip ospf neighbor interfejs
```

można zapoznać się z informacjami o stanie sąsiednich routerów należących do tego segmentu. Urządzenia oznaczane jako DROTHER są zwykłymi urządzeniami sąsiednimi.

Spójrzmy na przykład konfiguracji poniższej sieci i wyniki poleceń show:




```
RTA#
hostname RTA

interface Loopback0
 ip address 203.250.13.41 255.255.255.0


interface Ethernet0
 ip address 203.250.14.1 255.255.255.0

router ospf 10
 network 203.250.13.41 0.0.0.0 area 1
 network 203.250.0.0 0.0.255.255 area 0.0.0.0


RTF#
hostname RTF
interface Ethernet0
 ip address 203.250.14.2 255.255.255.0

router ospf 10
 network 203.250.0.0 0.0.255.255 area 0.0.0.0
```

Konfiguracje routerów RTB i RTD są podobne do konfiguracji routera RTF.

```
RTA#show ip ospf interface e0
Ethernet0 is up, line protocol is up
  Internet Address 203.250.14.1 255.255.255.0, Area 0.0.0.0
```

```
      Process ID 10, Router ID 203.250.13.41, Network Type
BROADCAST, Cost:
    10
      Transmit Delay is 1 sec, State BDR, Priority 1
      Designated Router (ID) 203.250.15.1, Interface address
203.250.14.2
      Backup Designated router (ID) 203.250.13.41, Interface
address
    203.250.14.1
      Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
        Hello due in 0:00:02
      Neighbor Count is 3, Adjacent neighbor count is 3
        Adjacent with neighbor 203.250.15.1  (Designated
Router)
    Loopback0 is up, line protocol is up
      Internet Address 203.250.13.41 255.255.255.255, Area 1
      Process ID 10, Router ID 203.250.13.41, Network Type
LOOPBACK, Cost: 1
      Loopback interface is treated as a stub Host


    RTF#show ip ospf interface e0
    Ethernet0 is up, line protocol is up
      Internet Address 203.250.14.2 255.255.255.0, Area 0.0.0.0
      Process ID 10, Router ID 203.250.15.1, Network Type
BROADCAST, Cost: 10
      Transmit Delay is 1 sec, State DR, Priority 1
      Designated Router (ID) 203.250.15.1, Interface address
203.250.14.2
      Backup Designated router (ID) 203.250.13.41, Interface
address
    203.250.14.1
      Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
        Hello due in 0:00:08
      Neighbor Count is 3, Adjacent neighbor count is 3
        Adjacent with neighbor 203.250.13.41  (Backup
Designated Router)


    RTD#show ip ospf interface e0
    Ethernet0 is up, line protocol is up
      Internet Address 203.250.14.4 255.255.255.0, Area 0.0.0.0
      Process ID 10, Router ID 192.208.10.174, Network Type
BROADCAST, Cost:
    10
      Transmit Delay is 1 sec, State DROTHER, Priority 1
```

```
      Designated Router (ID) 203.250.15.1, Interface address
203.250.14.2
      Backup Designated router (ID) 203.250.13.41, Interface
address
    203.250.14.1
      Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
        Hello due in 0:00:03
      Neighbor Count is 3, Adjacent neighbor count is 2
        Adjacent with neighbor 203.250.15.1  (Designated
Router)
        Adjacent with neighbor 203.250.13.41  (Backup
Designated Router)


    RTB#show ip ospf interface e0
    Ethernet0 is up, line protocol is up
      Internet Address 203.250.14.3 255.255.255.0, Area 0.0.0.0
      Process ID 10, Router ID 203.250.12.1, Network Type
BROADCAST, Cost: 10
      Transmit Delay is 1 sec, State DROTHER, Priority 1
      Designated Router (ID) 203.250.15.1, Interface address
203.250.14.2
      Backup Designated router (ID) 203.250.13.41, Interface
address
    203.250.14.1
      Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
        Hello due in 0:00:03
      Neighbor Count is 3, Adjacent neighbor count is 2
        Adjacent with neighbor 203.250.15.1  (Designated
Router)
        Adjacent with neighbor 203.250.13.41  (Backup
Designated Router)
```

Spójrzmy na informacje o interfejsie e0 na routerze RTA. Interfejs ten znajduje się w obszarze 0.0.0.0, proces OSPF ma wartość 10, a ID routera to 203.250.13.41. Interfejs ten pełni rolę BDR dla tego obszaru.

Interfejs routera RTF został wybrany na DR ze względu na najwyższy RID w danym obszarze (priorytet jest tutaj domyślny i wynosi 1). W taki sam sposób interfejs routera RTA został wybrany na BDR.. Routery RTB i RTD mają status DROTHER.

Należy zwrócić uwagę na liczbę sąsiadów i liczbę przyległych routerów. Routery RTB i RTD mają po trzech sąsiadów i po dwa routery przyległe (DR i BDR). Natomiast RTA i RTF mają po trzech sąsiadów i po trzy routery przyległe. Wynika to z faktu, że pełnią one rolę routerów DR i BDR.

Spójrzmy jeszcze na wynik poniższego polecenia:

```
RTD#show ip ospf neighbor

    Neighbor ID    Pri State          Dead Time  Address
Interface

    203.250.12.1    1  2WAY/DROTHER  0:00:37   203.250.14.3
Ethernet0
    203.250.15.1    1  FULL/DR       0:00:36   203.250.14.2
Ethernet0
    203.250.13.41   1  FULL/BDR      0:00:34   203.250.14.1
Ethernet0
```

6.14. Modyfikowanie kosztu w protokole OSPF

Dla poprawnej pracy protokołu OSPF ważne jest, aby przepustowość interfejsu była ustalona prawidłowo.

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 64
```

Domyślną przepustowością interfejsów szeregowych w urządzeniach Cisco jest 1,544 Mb/s, czyli 1544 kb/s.

Domyślnym kosztem przypisywanym łączu 100 Mb/s jest najniższa wartość kosztu równa 1. W przypadku sieci 100 Mb/s i Gigabit Ethernet te domyślne wartości kosztu, o ile nie zostaną zmienione, mogą spowodować wybór mniej efektywnej ścieżki. Aby zmienić domyślną wartość pasma odniesienia należy zastosować polecenie:

```
Router(config-router)#auto-cost reference-bandwidth mbps
```

Równie dobrze można po prostu zmienić przypisany koszt do danego interfejsu:

```
Router(config-if)#ip ospf cost liczba
```

6.15. Konfigurowanie uwierzytelniania w protokole OSPF

Domyślnie router przyjmuje, że informacje o routingu nadchodzą od tego routera, który powinien je przysłać. Router zakłada również, że przesyłana informacja nie została zmieniona w trakcie przesyłania.

Aby to zagwarantować, można tak skonfigurować routery znajdujące się w danym obszarze, aby przeprowadzały wzajemne uwierzytelnianie.

Każdy interfejs OSPF może udostępniać klucz uwierzytelniający, który jest przeznaczony dla routerów wysyłających informacje OSPF do innych routerów znajdujących

się w danym segmencie. Klucz uwierzytelniający, zwany również hasłem, jest tajną wartością wspólną dla routerów. Klucz ten jest używany do generowania danych uwierzytelniających przesyłanych w nagłówku pakietu OSPF. Hasło może mieć długość do ośmiu znaków. Do konfigurowania uwierzytelniania protokołu OSPF służy polecenie o następującej składni:

```
Router(config-if)#ip ospf authentication-key hasło
```

Po skonfigurowaniu hasła należy włączyć funkcję uwierzytelniania:

```
Router(config-router)#area numer-obszaru authentication
```

W przypadku prostego uwierzytelniania hasło jest wysyłane tekstem jawnym.

Zaleca się jednak, aby wiadomości uwierzytelniające były przesyłane w postaci zaszyfrowanej. W celu wysłania wiadomości uwierzytelniających w postaci zaszyfrowanej i zapewnienia większego bezpieczeństwa jest używane słowo kluczowe **message-digest**. Słowo kluczowe MD5 określa typ algorytmu mieszającego używanego do tworzenia sygnatury wiadomości, zaś pole typu szyfrowania określa stosowaną metodę szyfrowania, gdzie 0 oznacza brak szyfrowania, a 7 — zastrzeżoną metodę szyfrowania.

Składnia polecenia konfigurowania interfejsu wygląda następująco:

```
Router(config-if)#ip ospf message-digest-key id-klucza
md5 [typ-szyfrowania] klucz
```

Podany id-klucza jest identyfikatorem i przybiera wartość z przedziału od 1 do 255. Klucz jest hasłem alfanumerycznym o długości do szesnastu znaków. Routery sąsiednie muszą używać takiego samego identyfikatora klucza o tej samej wartości.

Następujące polecenie jest używane w trybie konfigurowania routera:

```
Router(config-router)#area id-obszaru authentication
message-digest
```

```
Sydney1(config-if)#ip ospf message-digest-key 1 md5 7
asecret
Sydney1(config-if)#exit
Sydney1(config)#router ospf 1
Sydney1(config-router)#area 0 authentication message-
digest
Sydney1(config-router)#end
Sydney1#
```

Uruchamiając opcję uwierzytelniania w danym obszarze, trzeba włączyć jej obsługę we wszystkich routerach należących do tego obszaru.

Istnieje możliwość zdefiniowania różnych kluczy dla poszczególnych interfejsów routera lub jednego hasła wykorzystywanego w całej sieci. Najważniejsze jest to, by wszystkie interfejsy należące do jednego segmentu sieci korzystały z tego samego klucza OSPF.

6.16. Konfigurowanie zegarów protokołu OSPF

Aby móc wymieniać informacje, routery OSPF muszą używać tych samych wartości czasu między pakietami *Hello* oraz czasu przetrzymania w ramach danego segmentu sieci. Domyślnie wartość czasu przetrzymania jest cztery razy większa niż czas między pakietami *Hello*. Oznacza to, że router może podjąć cztery próby wysłania pakietu *Hello*, zanim zostanie uznany za wyłączony (martwy).

Wartości zegarów mogą być zmienione przez administratora sieci. Usprawiedliwieniem zmiany wartości zegarów może być tylko poprawa wydajności sieci OSPF. Należy tak zmieniać wartość zegarów, aby odpowiadały wartościom na sąsiednich routerach.

Aby skonfigurować interwał pakietów *Hello* oraz czas przetrzymania, należy użyć następujących poleceć:

```
Router(config-if)#ip ospf hello-interval sekundy
Router(config-if)#ip ospf dead-interval sekundy
```

6.17. Propagowanie domyślnej trasy w protokole OSPF

Routing OSPF zapewnia istnienie wolnych od zapętleń tras do wszystkich sieci w domenie. Aby osiągnąć sieć znajdującą się poza domeną, protokół OSPF musi wiedzieć o tej sieci lub też musi mieć domyślną trasę.

Praktycznym rozwiązaniem jest dodanie domyślnej trasy do routera OSPF połączonego z siecią zewnętrzną. Trasa ta może być redystrybuowana między wszystkimi routerami znajdującymi się w danym systemie autonomicznym dzięki zwykłym aktualizacjom OSPF.

Skonfigurowana trasa domyślna jest używana przez router do utworzenia bramy ostatniej szansy. Składnia konfiguracji statycznej trasy domyślnej używa adresu sieci 0.0.0.0 oraz maski podsieci 0.0.0.0:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [interfejs | adres-następnego-przeskoku]
```

Następująca instrukcja konfiguracyjna dokona propagacji tej trasy do wszystkich routerów w danym obszarze OSPF:

```
Router(config-router)#default-information originate
```

Wszystkie routery w obszarze OSPF poznają trasę domyślną, jeśli jest aktywny interfejs routera brzegowego do bramy domyślnej.

6.18. Sprawdzanie konfiguracji protokołu OSPF

Do sprawdzania konfiguracji protokołu OSPF można użyć szeregu poleceń **show**. Na poniższym rysunku przedstawiono te polecenia.

Polecenie	Opis
`show ip protocol`	Służy do wyświetlania parametrów zegarów, filtrów, metryk, sieci oraz innych informacji dotyczących routera traktowanego jako całość.
`show ip route`	Służy do wyświetlania tras znanych routerowi i opisu metody ich poznania. Jest to jeden z najlepszych sposobów sprawdzania połączenia między lokalnym routerem a resztą intersieci.
`show ip ospf interface`	Służy do sprawdzenia, czy interfejsy zostały skonfigurowane w odpowiednich obszarach. Jeśli nie podano adresu pseudosieci (loopback), rolę identyfikatora routera pełni interfejs o najwyższym adresie. Wyświetla również wartości zegarów, takich jak zegar pakietów hello, oraz prezentuje relacje przylegania.
`show ip ospf`	Służy do wyświetlania liczby wskazującej, ile razy został użyty algorytm SPF. Wyświetla również interwał aktualizacji stanu łącza w przypadku braku zmian w topologii.
`show ip ospf neighbor detail`	Służy do wyświetlania szczegółowej listy sąsiadów, ich priorytetów oraz stanu (na przykład init, exstart lub full).
`show ip ospf database`	Służy do wyświetlania zawartości bazy danych o topologii uaktualnianej przez router. Wyświetla również identyfikator routera oraz identyfikator procesu OSPF. Używając odpowiednich słów kluczowych, można wyświetlić bazy danych różnych typów. Szczegółowe informacje dotyczące słów kluczowych można znaleźć na stronie www.cisco.com.

Na poniższym rysunku przedstawiono polecenia przydatne podczas rozwiązywania problemów z protokołem OSPF.

Polecenie	Opis
`debug ip ospf events`	Raportuje wszystkie zdarzenia OSPF
`debug ip ospf adj`	Raportuje zdarzenia dotyczące przylegania OSPF