

LABORATORIUM NR 6

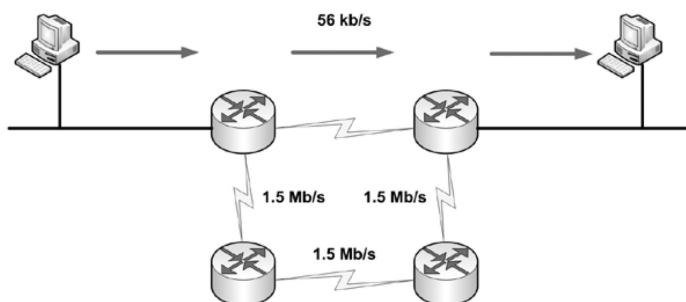
Celem ćwiczenia jest poznanie i porównanie konfiguracji routingu dynamicznego na bazie protokołu RIPv2 oraz RIPv6.

Protokół routingu RIP.

Protokół RIP (ang. Routing Information Protocol) opisany po raz pierwszy w dokumencie RFC 1058 przeszedł ewolucję od klasowego protokołu routingu RIP w wersji 1 (RIP v1) do bezklasowego protokołu routingu RIP w wersji 2 (RIP v2). W celu zapobieżenia nieskończonym pętlom routingu, w protokole RIP ograniczono liczbę dopuszczalnych przeskoków na ścieżce od źródła do celu do 15. Gdy router otrzymuje aktualizację routingu zawierającą nową albo zmienioną pozycję, zwiększa wartość metryki o 1, aby uwzględnić siebie jako przeskok na ścieżce. Jeśli wartość metryki przekroczy 15, cel w sieci jest uznawany za niedostępny.

Działanie protokołu RIP

Na rysunku poniżej ścieżka o prędkości 56 kb/s między dwoma hostami używającymi górnych routerów jest równa dwóm skokom. Niższa, zastępcza ścieżka, używająca trzech łączy T1 (1.5 Mb/s) jest równa czterem skokom. Ponieważ wybór ścieżki przez RIP jest oparty wyłącznie na liczbie skoków, w tym przypadku wybrane zostanie łącze o prędkości 56 kbps, a nie znacznie szybsze łącze T1.



Konfiguracja protokołu RIPv1

Polecenie `router rip` uaktywnia protokół RIP jako protokół routingu. Następnie używane jest polecenie `network` określające, na których interfejsach ma działać protokół RIP. Proces routingu wiąże określone interfejsy adresami sieciowymi rozpoczyna wysyłanie odbieranie aktualizacji RIP na tych interfejsach.

Protokół RIP wysyła aktualizacje routingu w regularnych odstępach czasu. Po odebraniu aktualizacji tras zawierającej zmianę pozycji router aktualizuje swoją tablicę routingu, aby uwzględnić nową trasę. Odebrana wartość metryki dla ścieżki jest zwiększana o 1, a jako następny przeskoczek w tablicy routingu jest wskazywany interfejs źródłowy tej aktualizacji.

Na routerach RIP jest przechowywana informacja tylko o najlepszej ścieżce do celu, ale w przypadku ścieżek o równych kosztach przechowywanych może być ich kilka. W przypadku większości protokołów routingu aktualizacje są generowane czasowo oraz zdarzeniowo. Protokół RIP jest sterowany czasowo, ale w implementacji firmy Cisco tego protokołu w przypadku wykrycia zmiany wysyłane są wyzwalane aktualizacje. Bez takich aktualizacji protokół RIP działałby mniej efektywnie.

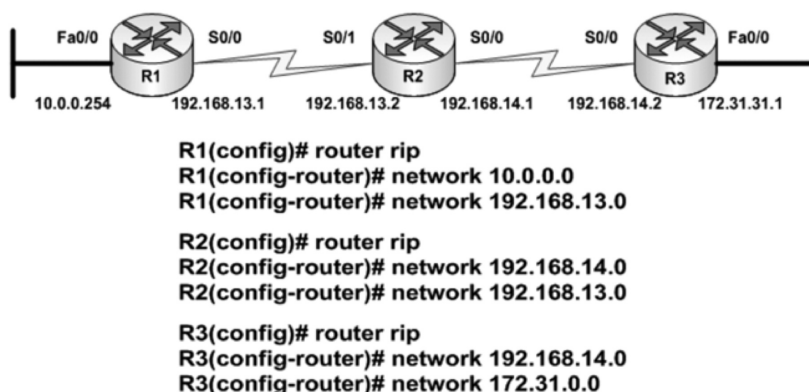
Po aktualizacji tablicy z powodu zmiany konfiguracji router natychmiast wysyła aktualizacje tras, aby poinformować inne routery o tej zmianie. Aktualizacje te, zwane aktualizacjami wyzwalanymi, są wysyłane dodatkowo oprócz aktualizacji zaplanowanych wysyłanych przez router RIP.

Aby włączyć protokół RIP, należy w trybie konfiguracji globalnej użyć następujących poleceń:

Router(config)# router rip – włącza proces routingu RIP,

Router(config-router)# network numer_sieci – tworzy powiązanie sieci z procesem RIP

Proces konfiguracji RIPv1 ilustruje rysunek poniżej:



Konfiguracja protokołu RIPv2

W wersji protokołu RIPv2 wprowadzono następujące rozszerzenia:

1. Możliwość przenoszenia dodatkowych informacji o routingu pakietów.
2. Mechanizm uwierzytelniania zabezpieczający tablice routingu.
3. Obsługa techniki masek podsieci o zmiennej długości (VLSM).

Aby włączyć protokół RIPv2, należy w trybie konfiguracji globalnej użyć następujących poleceń:

Router(config)# router rip – włącza proces routingu RIP

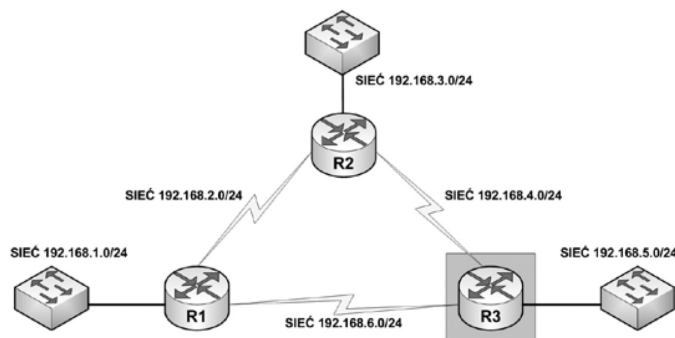
Router(config)# version 2

Router(config-router)# network numer_sieci – tworzy powiązanie sieci z procesem RIP

Weryfikowanie konfiguracji protokołu RIP

A. Polecenie *show ip route* umożliwia sprawdzenie, czy trasy odbierane od sąsiednich urządzeń używających protokołu RIP znajdują się w tablicy routingu. W danych

wyjściowych polecenia należy poszukać tras RIP, które są oznaczone literą R. Należy pamiętać o tym, że uzyskanie zbieżności trochę trwa, więc trasy mogą nie pojawić się natychmiast.



R3#show ip route

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Gateway of last resort is not set

```
R 192.168.1.0/24 [120/1] via 192.168.6.2, 00:00:05, Serial0/0/0
R 192.168.2.0/24 [120/1] via 192.168.6.2, 00:00:05, Serial0/0/0
R 192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:05, Serial0/0/1
C 192.168.4.0/24 is directly connected, Serial0/0/1
C 192.168.5.0/24 is directly connected, FastEthernet0/0
C 192.168.6.0/24 is directly connected, Serial0/0/0
```

B. Polecenie `show ip protocols` pokazuje, które protokoły routingu przenoszą ruch IP w routerze. Danych tych można użyć do sprawdzenia ustawień konfiguracji protokołu RIP. Najczęściej sprawdzane są następujące elementy konfiguracji:

1. Konfiguracja protokołu RIP.
2. Wysyłanie i odbieranie aktualizacji protokołu RIP przez właściwe interfejsy.
3. Ogłaszanie właściwych sieci przez router.

R3#show ip protocols

```
Routing Protocol is "rip"
(**output omitted**)
```

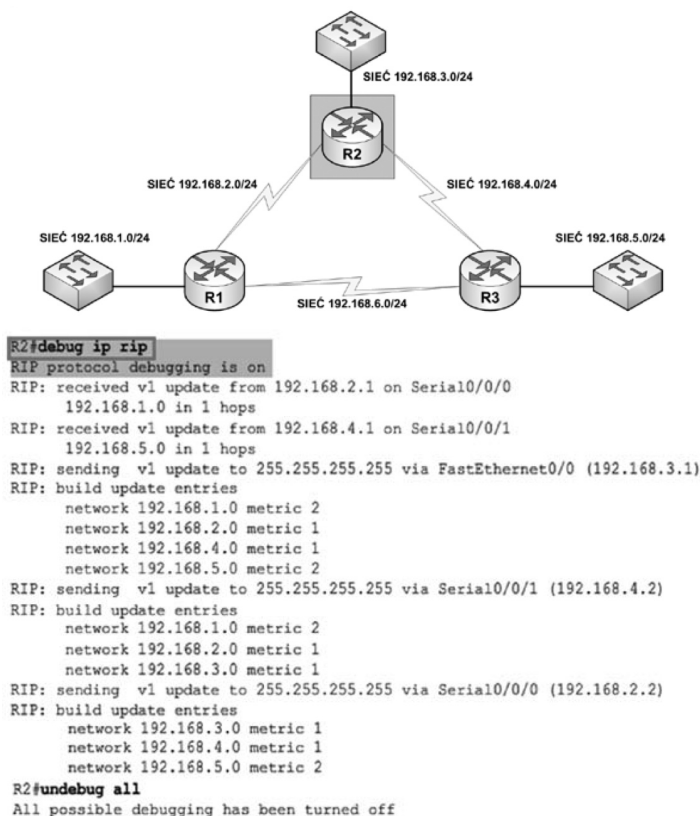
```
Redistributing: rip
Default version control: send version 1, receive any version

Interface          Send Recv Triggered RIP Key-chain
FastEthernet0/0     1     1 2
Serial0/0/0         1     1 2
Serial0/0/1         1     1 2

Automatic network summarization is in effect
Routing for Networks:
 192.168.4.0
 192.168.5.0
 192.168.6.0

Routing Information Sources:
 Gateway         Distance      Last Update
 192.168.6.2     120           00:00:10
 192.168.4.2     120           00:00:18
Distance: (default is 120)
```

- C. Polecenie `debug ip rip` umożliwia diagnostykę takich problemów, jak nieciągłość podsieci lub powielone sieci. Objawem takich problemów może być router, który ogłasza metrykę mniejszą niż sam odebrał dla danej sieci.



Protokół RIPng

Protokół RIPng (ang. Routing Information Protocol Next Generation) jest protokołem wewnętrznej bramy (ang. Interior Gateway Protocol – IGP), który korzysta z algorytmu wektora odległości w celu określenia najlepszej trasy do miejsca docelowego, korzystając z liczby przeskoków jako metryki. RIPng jest następcą protokołu RIPv2 ale tylko dla protokołu IPv6.

Elementami wspólnymi dla obu protokołów są:

- Wykorzystanie algorytmu Bellmana-Forda podczas wyboru najkrótszej ścieżki do celu.
- Ograniczenia promienia działania protokołu do 15 skoków.
- Wykorzystania UDP do wysyłania informacji o routingu oraz okresowych rozgłoszeń.

Główne różnice między protokołami RIPv2 i RIPng to:

- Informacje o routingu RIPng przenoszone są w pakietach IPv6 (1).
- Adresem źródłowym każdego komunikatu o trasach jest adres lokalny łącza interfejsu, z którego wiadomość ta jest wysyłana (2).
- Adresem docelowym wiadomości jest adres grupowy wszystkich routerów RIPng (3).
- Numer portu UDP wykorzystywany przy wysyłaniu i odbieraniu informacji o routingu to 521 (4).
- W komunikatach wykorzystywane są 128-bitowe prefiksy (5).

- Adresy następnego skoku używają 128 bitów zamiast 32 bitów (jak w IPv4).

Różnice (z uwzględnieniem punktów podanych w nawiasach) ilustruje rysunek poniżej.

No.	Time	Source	Destination	Protocol	Info
66	98.738000	fe80::c603:11ff:fe00:ff02::1	ff02::1	ICMPv6	Router advertisement
69	103.075000	fe80::c603:11ff:fe00:ff02::9	ff02::9	RIPng	ve Response
74	114.984000	fe80::c603:11ff:fe00:ff02::1	ff02::1	ICMPv6	Router advertisement
78	129.704000	fe80::c603:11ff:fe00:ff02::9	ff02::9	RIPng	ve Response
87	159.284000	fe80::c603:11ff:fe00:ff02::9	ff02::9	RIPng	ve Response

Internet Protocol Version 6	(1)
0110 = Version: 6	
[0110 = This field makes the filter "ip.version == 6" possible: 6]	
.... 1110 0000 = Traffic class: 0x000000e0	
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000	
Payload length: 112	
Next header: UDP (0x11)	
Hop limit: 255	
Source: fe80::c603:11ff:fe00:0 (fe80::c603:11ff:fe00:0) (2)	
Destination: ff02::9 (ff02::9) (3)	
User Datagram Protocol	Src Port: ripng (521), Dst Port: ripng (521)
Source port: ripng (521)	
Destination port: ripng (521) (4)	
Length: 112	
Checksum: 0xb220 [correct]	
[Good Checksum: True]	
[Bad Checksum: False]	
RIPng	
Command: Response (2)	
Version: 1	
IP Address: 2010:aabc:ffed:f::/64	Metric: 1 (5)
IP Address: 2010:aabc:ffed:f::	
Tag: 0x0000	
Prefix length: 64	
Metric: 1	
IP Address: 1997:bb09:ddca::/64	Metric: 1 (5)
IP Address: 1997:bb09:ddca::	
Tag: 0x0000	
Prefix length: 64	
Metric: 1	

Konfiguracja protokołu RIPng

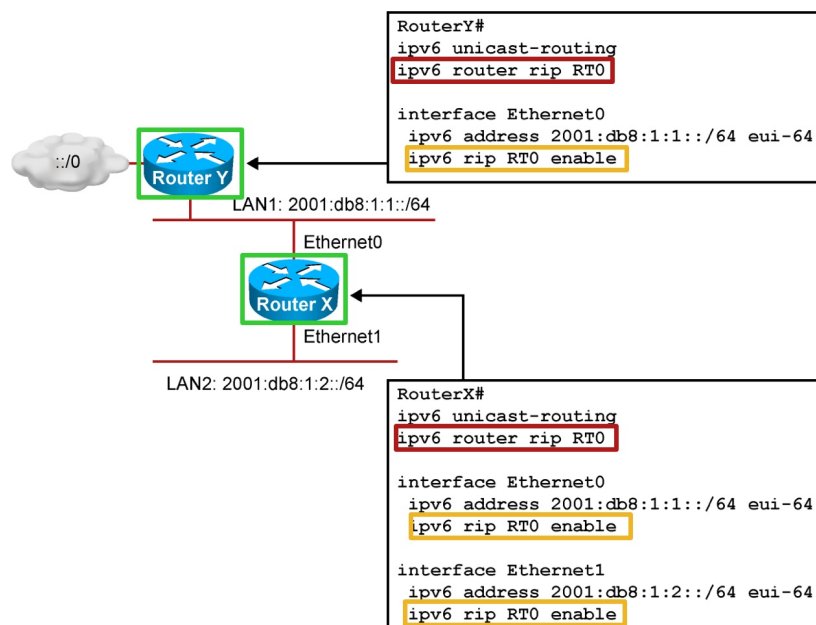
Poniżej zebrane są podstawowe polecenia służące do konfiguracji protokołu RIPng na routerach Cisco:

RouterX(config)# ipv6 router rip tag - włącza proces routingu RIPng

RouterX(config-if)# ipv6 rip tag enable - tworzy powiązanie interfejsu z procesem RIPng

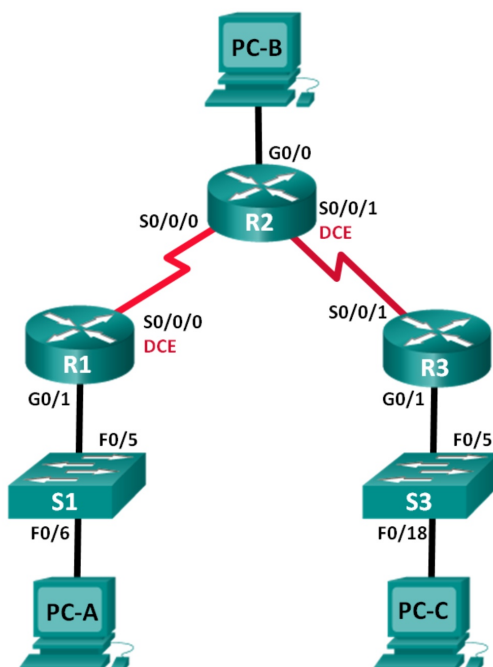
RouterX# show ipv6 rip - wyświetla status procesów RIPng

RouterX# show ipv6 route rip - wyświetla trasy RIPng w tablicy routingu



PRZEBIEG ĆWICZENIA

UWAGA: W sprawozdaniu muszą znaleźć się wszystkie elementy (pytania, polecenia) wyróżnione kolorem czerwonym.



Uwaga:

podane na rysunku nazwy interfejsów proszę traktować jako przykładowe i w trakcie wykonywania ćwiczenia uwzględniać typ użytych routerów i switchy (pomiń ustawienia vlan-ów na S1 oraz S2)

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Ćwiczenie należy rozpocząć od utworzenia fizycznej sieci zgodnej z rysunkiem powyżej. Proszę zastosować adresację zgodnie z tabelą powyżej.

1. Wstępna konfiguracja routerów i komputerów PC.

A. Konfiguracja routerów R1, R2, R3.

- Wyłącz DNS lookup.
- Przypisz nazwy do routerów zgodnie z topologią na rysunku powyżej.
- Skonfiguruj logging synchronous na konsoli routera.
- Skonfiguruj łącza szeregowo (clock rate na DCE) analogicznie jak w poprzednich ćwiczeniach.
- Skonfiguruj adresy IP na interfejsach routera zgodnie z tabelą powyżej.

B. Konfiguracja interfejsów komputerów PC.

- Skonfiguruj statycznie adresy IP na interfejsach komputerów zgodnie z tabelą adresacji powyżej.

C. Sprawdzenie połączeń.

Poprawnie wykonane punkty A oraz B powinny pozwolić na:

- Pingowanie pomiędzy komputerem PC a interfejsem bezpośredniego routera.
- Pingowanie pomiędzy bezpośrednio połączonymi interfejsami routerów.

W przypadku braku połączeń należy, przed realizacją kolejnych zadań, sprawdzić poprawność dokonanej konfiguracji.

2. Konfiguracja i weryfikacja protokołu RIPv2.

A. Na routerze R1, skonfiguruj protokół RIPv2 i rozgłoś właściwe sieci.

```
R1# config t
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# passive-interface g0/1
R1(config-router)# network 172.30.0.0
R1(config-router)# network 10.0.0.0
```

UWAGA: Polecenie *passive-interface* wstrzymuje odbieranie uaktualnień (update) na określonym interfejsie. Pozwala to zapobiegać pętlom routingu. Należy jednak pamiętać iż sieci obsługiwane przez interfejs wskazany przez *passive-interface* wciąż są rozgłaszane w uaktualnieniach i przesyłane dalej do sieci LAN.

B. Skonfiguruj RIPv2 na routerze R3 analogicznie jak dla R1. Zablokuj rozsyłanie updatów na interfejsie LAN.

C. Skonfiguruj RIPv2 na routerze R2. Nie rozgłaszaj sieci 209.165.201.0.

Wyjaśnij dlaczego w przypadku konfiguracji routera R2 nie dodano wymagania użycia polecenia *passive-interface* w odniesieniu do G0/0

D. Sprawdź działanie protokołu RIPv2 na routerach. Wykorzystaj w tym celu polecenia: `debug ip rip`, `show ip protocols` oraz `show run`. Przykład wyniku działania polecenia `show ip protocols` dla routera R1 jest przedstawiony poniżej:

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv  Triggered RIP  Key-chain
  Serial0/0/0         2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway            Distance    Last Update
  10.1.1.2            120
Distance: (default is 120)
```

E. Bazując na informacjach uzyskanych poleceniem `debug ip rip` na routerze R2, zaznacz na zrzucie ekranowym te fragmenty, które potwierdzają, że protokół RIPv2 działa.

Po skończeniu obserwacji podaj komendę `undebug all` by wyłączyć debugging.

F. Bazując na informacjach uzyskanych poleceniem `show run` na routerze R3, zaznacz na zrzucie ekranowym te fragmenty, które potwierdzają, że protokół RIPv2 działa.

2. Automatyczna sumaryzacja tras

A. Sieci LAN przyłączone do routerów R1 oraz R3 są sieciami nieciągłymi. Proszę zweryfikować, że tablica routingu na R2 zawiera dwie ścieżki, każda o równym koszcie, do sieci 172.30.0.0/16. Ponadto R2 wskazuje tylko na jeden klasowy adres 172.30.0.0 i nie ma wiedzy o podsieciach w tej sieci.

```
R2# show ip route
<Output omitted>
  10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.2/32 is directly connected, Serial0/0/0
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.2/32 is directly connected, Serial0/0/1
R       172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
          [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
  209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.201.0/24 is directly connected, GigabitEthernet0/0
L       209.165.201.1/32 is directly connected, GigabitEthernet0/0
```


Z kolei w tablicy routingu na routerze R1 zawarte są tylko jego własne podsieci dla sieci 172.30.0.0. Router R1 nie posiada określonych tras do podsieci 172.30.0.0 przyłączonych do R3.

```
R1# show ip route
<Output omitted>
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/0/0
L       10.1.1.1/32 is directly connected, Serial0/0/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.10.0/24 is directly connected, GigabitEthernet0/1
L       172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

Analogicznie, router R3 ma w tablicy routingu wpisy związane ze "swoimi" podsieciami w sieci 172.30.0.0. Router R3 nie posiada wiedzy o trasach do podsieci w sieci 172.30.0.0 przyłączonych do routera R1.

```
R3# show ip route
<Output omitted>
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
L       10.2.2.1/32 is directly connected, Serial0/0/1
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.30.30.0/24 is directly connected, GigabitEthernet0/1
L       172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

W sprawozdaniu umieść wynik działania polecenia *debug ip rip* na routerze R2 i zaznacz fragmenty, które potwierdzają, że router R3 nie wysyła rozgłoszeń o podsieciach w sieci 172.30.0.0 a wyłącznie o zsumaryzowanej trasie do sieci 172.30.0.0/16.

B. W celu wyłączenia automatycznej sumaryzacji tras należy wykorzystać polecenie *no auto-summary*. Należy użyć to polecenie na wszystkich trzech routerach.

```
R1(config)# router rip
R1(config-router)# no auto-summary
```

Następnie należy wydać polecenie *clear ip route ** w celu wyczyszczenia tablicy routingu.

```
R1(config-router)# end
R1# clear ip route *
```

Odczekaj ok 30s i sprawdź tablice routingu na wszystkich routerach. W sprawozdaniu umieść te tablice routingu i zaznacz miejsca potwierdzające, że podsieci w sieci 172.30.0.0 są rozgłaszane poprawnie (tj. bez automatycznej sumaryzacji).

Włącz *debug ip rip* na routerze R2 w celu obserwacji rozgłoszeń RIP.

Po ok. 60 sekundach wydaj polecenie `no debug ip rip`.

Wypisz rozgłoszenia RIP otrzymane od R3.

3. Konfiguracja i rozgłaszanie tras domyślnych w protokole RIPv2.

- A. Na routerze R2 skonfiguruj statyczną trasę domyślną (trasę do sieci 0.0.0.0 0.0.0.0), wykorzystując polecenie `ip route`. Trasa ta ma kierować na interfejs G0/0 routera R2 i tym samym ma symulować połączenie z siecią zewnętrzną, np internetem (tzw. ustawienie Gateway of Last Resort).

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

R2 będzie teraz rozgłaszać tę trasę do innych routerów tylko jeśli konfiguracja RIPv2 zawierać będzie polecenie `default-information originate`.

```
R2(config)# router rip
```

```
R2(config-router)# default-information originate
```

Umieść w sprawozdaniu tablicę routingu dla R1 potwierdzająca propagację trasy domyślnej. Czy w tak skonfigurowanej sieci wszystkie pingi kończą się sukcesem ?

4. Podstawowa konfiguracja protokołu RIPv2

- A. W topologii sieciowej jak poprzednio należy skonfigurować interfejsy routerów i komputerów PC zgodnie z tabelą poniżej. Przy konfiguracji należy wykorzystać wiadomości z poprzednich dwóch ćwiczeń.

Device	Interface	IPv6 Address / Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

B. W przypadku RIPng nie wykorzystuje się polecenia **network** (interfejsy mogą mieć wiele adresów). Konfiguracja RIPng odnosi się do interfejsu i indywidualnie nazwanych procesów (potencjalnie wielu) RIPng. W poniższym przykładzie dla routera R1 proces taki nazwano Test1.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```

C. Skonfiguruj RIPng dla interfejsu szeregowego na routerze R2 przypisując procesowi nazwę Test2. Nie konfiguruj RIPng dla interfejsu G0/0.

D. Skonfiguruj RIPng dla wszystkich interfejsów na routerze R3 i skojarz z nazwą procesu Test3.

E. Zweryfikuj konfigurację RIPng na routerach za pomocą poleceń: **show ipv6 protocols**, **show run**, **show ipv6 rip database** oraz **show ipv6 rip process name**. W sprawozdaniu umieść wyniki działania tych poleceń dla routera R3.

F. Spróbuj poleceń ping pomiędzy wszystkimi komputerami PC. Czy wszystkie pingu zakończyły się sukcesem a jeśli nie to dlaczego ?

5. Propagacja trasy domyślnej w RIPng.

A. Na routerze R2 dodaj statyczną trasę domyślną do sieci ::0/64. Wykorzystaj w tym celu polecenie **ipv6 route**. Poniżej podaj wprowadzone polecenie ze wszystkimi parametrami.

B. Rozgłaszanie tras domyślnych w RIPng jest analogiczne jak w RIPv2 dla protokołu IPv4. Polecenie ma składnię: **ipv6 rip <process name> default-information originate**
Na routerze R2 należy wydać polecenia:

```
R2(config)# int s0/0/0
R2(config-rtr)# ipv6 rip Test2 default-information originate
R2(config)# int s0/0/1
R2(config-rtr)# ipv6 rip Test2 default-information originate
```

C. Umieść w sprawozdaniu tablice routingu dla R1, R2 oraz R3.

D. Wykonaj test ping z PC-A oraz z PC-C pod adres 2001:DB8:ACAD:B::B/64
Czy oba pingu zakończyły się sukcesem? _____

**SPRAWOZDANIE NALEŻY UMIEŚCIĆ NA DROPBOX W KATALOGU
/Laboratorium/Sprawozdania/<dzień tygodnia_godz. rozpoczęcia zajęć>**

**PLIK SPRAWOZDANIA PROSZĘ NAZWAĆ WEDŁUG SCHEMATU:
Spr6_<nazwisko studenta wykonującego sprawozdanie>.pdf**

PREFEROWANY FORMAT PLIKU: PDF