Adam Józefiok

CCNA 200-125

Zostań administratorem sieci komputerowych **Cisco**

Helion

Opieka redakcyjna: Ewelina Burska
Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Materiały graficzne na okładce zostały wykorzystane za zgodą Shutterstock.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/ccn125
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-3280-5

Printed in Poland.

Spis treści

Rozdział 13.

Routing pomiędzy sieciami VLAN

Przy okazji omawiania routerów możemy na chwilę powrócić do sieci VLAN, a ściślej mówiąc, do komunikacji pomiędzy nimi. Jak wiesz, komunikacja we VLAN-ach odbywa się w warstwie 2. OSI. Na tym poziomie, jeśli dwa urządzenia znajdują się w różnych VLAN-ach, nie ma możliwości komunikacji między nimi. Ze względu na występujący w każdej ramce identyfikator sieci VLAN ruch na poziomie logicznym jest odseparowany, mimo że urządzenia na poziomie fizycznym podłączone są do tego samego przełącznika. Każda z ramek zostaje wysłana ze stacji roboczej nieoznakowana, a trafiając do interfejsu przełącznika, otrzymuje znakowanie i od tej chwili może komunikować się z pozostałymi urządzeniami w tej samej sieci VLAN.

Odseparowanie ruchu w poszczególnych sieciach VLAN jest bardzo dobrym rozwiązaniem, ogranicza bowiem zalewanie sieci rozgłoszeniami, pochodzącymi chociażby z protokołu ARP czy DHCP. Ponadto sieci VLAN separują od siebie stacje robocze, które nie powinny móc się ze sobą komunikować. Załóżmy, że firma ma kilka działów. Każdy z nich realizuje inne zadania, a co za tym idzie, każdy z pracowników powinien mieć dostęp do danych tylko ze swojego działu. Dzięki sieciom VLAN możesz to zagwarantować i na jednym fizycznym urządzeniu oddzielić ruch płynący z poszczególnych działów.

Oczywiście odseparowanie od siebie stacji roboczych lub serwerów sprawi, że wiele aplikacji nie będzie ze sobą współdziałać. Dlatego wprowadzenie rozwiązania opartego na warstwie 3. jest konieczne do tego, aby umożliwić im komunikację, jednak w sposób w pełni kontrolowany i zapewniający pozbycie się zbędnych rozgłoszeń. Trzeba wspomnieć, że wzajemna komunikacja sieci VLAN jest możliwa jedynie dzięki zastosowaniu urządzeń warstwy 3. routera lub przełącznika.

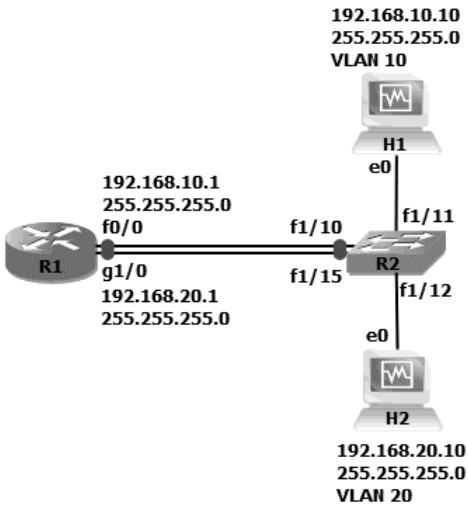
Za chwilę zostaną omówione trzy metody na umożliwienie komunikowania się stacji roboczych znajdujących się w różnych sieciach VLAN. Dzięki analizie przykładów będziesz mógł się przekonać, która z nich jest dla Ciebie optymalna.

Każdą metodę postaram się wyjaśnić na podstawie projektów, które możesz wykonać samodzielnie w programie GNS3. Będzie Ci do tego potrzebny router Cisco 3745, o którym wspominałem we wcześniejszych rozdziałach.

Metoda klasyczna

Metoda klasyczna polega na skierowaniu ruchu z sieci VLAN do routera. Spójrz na poniższy rysunek 13.1. Przedstawia on dwie stacje robocze. Stacja robocza `H1` znajduje się w sieci `VLAN10` i podsieci `192.168.10.0/24`, a stacja `H2` jest w sieci `VLAN20` i podsieci `192.168.20.0/24`. Jeśli w sieci nie będzie routera, te dwie stacje nie będą mogły się ze sobą komunikować. Stanie się tak, ponieważ znajdują się one w różnych podsieciach oraz, co najważniejsze, w różnych sieciach VLAN.

Rysunek 13.1.
Routing pomiędzy sieciami VLAN — model klasyczny



Aby te dwie stacje robocze mogły się ze sobą komunikować, użyjemy routera `R1`. Jest on wyposażony w dwa interfejsy. Pierwszy z nich to `FastEthernet`, a drugi to `GigabitEthernet`. W naszym przykładzie są konieczne właśnie dwa interfejsy. Celowo wybrałem dwa różne, abyś mógł po prostu przetrenować rozmaite możliwe przypadki. Metoda klasyczna wymaga bowiem tego, aby każdy z interfejsów routera należał do określonej sieci VLAN i był bramą domyślną dla wszystkich stacji w tej podsieci. Interfejs `fa0/0` posiada więc adres IP `192.168.10.1` i jest domyślną bramą dla wszystkich urządzeń znajdujących się w sieci `VLAN10`.

Najpierw jednak wykonajmy konfigurację przełącznika, którym tak naprawdę jest router 3745. Celowo nie zmieniałem nazwy, żebyś bez problemu mógł się orientować w całym ćwiczeniu. Aby utworzyć nowe sieci VLAN na tym emulowanym przełączniku, użyj w trybie uprzywilejowanym polecenia `vlan database`. Następnie poleceniem `vlan [numer_sieci_vlan]` utwórz nową sieć `VLAN10` i `VLAN20`. Aby zapisać ustawienia, wydaj polecenie `exit`.

```
R2#vlan database
R2(vlan)#vlan 10
VLAN 10 added:
    Name: VLAN0010
R2(vlan)#vlan 20
VLAN 20 added:
    Name: VLAN0020
R2(vlan)#exit
APPLY completed.
Exiting....
R2#
```

Czasami podczas emulowania przełącznika w programie GNS3 po wydaniu polecenia `exit` może pojawić się błąd. Należy wtedy wyjść z konfiguracji VLAN poleceniem `abort`, a następnie wydać polecenie `format flash:`. Po wykonaniu tej czynności i sformatowaniu pamięci flash wszystko powinno już działać prawidłowo. W tym miejscu chciałbym jeszcze przypomnieć, że w rzeczywistym przełączniku konfigurację sieci VLAN przeprowadza się poleceniem `vlan [numer_sieci_vlan]` w trybie konfiguracji globalnej, a więc już bez wspomnianego polecenia `vlan database`.

W kolejnym kroku przypisz interfejs `fa1/10` do sieci `VLAN10`, a interfejs `fa1/15` do sieci `VLAN20`. Pamiętaj, aby określić przeznaczenie interfejsu, wykorzystując polecenie `switchport mode access`. Następnie poleceniem `switchport access vlan [symbol_sieci_vlan]` przypisz interfejs do określonej sieci VLAN.

```
R2(config)#int f1/10
R2(config-if)#switchport mode access
R2(config-if)#switchport access vlan 10
R2(config-if)#int f1/15
R2(config-if)#switchport mode access
R2(config-if)#switchport access vlan 20
R2(config-if)#
```

Używając polecenia `show vlan-switch`, a w rzeczywistym przełączniku `show vlan brief`, sprawdź, czy interfejsy znajdują się w odpowiednich sieciach VLAN.

```
R2#show vlan-switch
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/0, Fa1/1, Fa1/2, Fa1/3
                                                Fa1/4, Fa1/5, Fa1/6, Fa1/7
                                                Fa1/8, Fa1/9, Fa1/11, Fa1/12
                                                Fa1/13, Fa1/14
10   VLAN0010                         active    Fa1/10
20   VLAN0020                         active    Fa1/15
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        1002   1003
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
```

```
1002 fddi   101002     1500  -      -      -        -    -        1      1003
1003 tr     101003     1500  1005   0      -        -    srb      1      1002
1004 fdnet  101004     1500  -      -      1        ibm  -        0      0
1005 trnet  101005     1500  -      -      1        ibm  -        0      0
R2#
```

Teraz kiedy interfejsy prowadzące do routera są już w odpowiednich sieciach VLAN, przypisz do sieci VLAN interfejsy prowadzące do stacji roboczych.

```
R2(config)#int f1/11
R2(config-if)#switchport mode access
R2(config-if)#switchport access vlan 10
R2(config-if)#int f1/12
R2(config-if)#switchport mode access
R2(config-if)#switchport access vlan 20
R2(config-if)#
```

Pamiętaj, że interfejsy routera będą domyślną bramą dla całego ruchu pochodzącego z określonej sieci VLAN. Przydziel odpowiednie adresy IP do interfejsów routera i uruchom interfejsy. Zauważ, że np. interfejs `fa0/0` routera `R1` posiada adresację pochodzącą z tej samej podsieci co stacja robocza `H1`, ponadto znajduje się w tej samej sieci VLAN. Na stacjach roboczych ustaw też adresy IP i adresy bram domyślnych.

```
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#int g1/0
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
```

Za pomocą polecenia `show ip interface brief` wyświetl listę interfejsów i sprawdź, czy wszystkie przypisane adresy IP się zgadzają oraz czy interfejsy zostały uruchomione i są w stanie `up`.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
GigabitEthernet1/0     192.168.20.1    YES manual up                    up
Serial2/0              unassigned      YES unset  administratively down down
Serial2/1              unassigned      YES unset  administratively down down
Serial2/2              unassigned      YES unset  administratively down down
Serial2/3              unassigned      YES unset  administratively down down
GigabitEthernet3/0     unassigned      YES unset  administratively down down
R1#
```

Po zakończeniu konfiguracji wyświetl na routerze tablicę routingu, wpisując polecenie `show ip route`. w Pierwsza część tablicy routingu przedstawia legendę zawierającą symbole wraz z ich rozwinięciem. Na samym końcu znajdują się cztery wiersze.

Spójrz na pierwszy z nich, zawierający literę `C`, oznaczającą źródło wpisu. Litera `C` pochodzi od określenia `connected`, co wskazuje na wpis z sieci bezpośrednio podłączonej. Następnie podana jest podsieć, której ów wpis dotyczy. W tym przypadku jest to `192.168.10.0/24`. Za adresem sieci znajduje się wyrażenie `is directly connected` („jest

bezpośrednio podłączona"). Natomiast identyfikator zamieszczony na końcu oznacza interfejs, którym musi zostać przesłany pakiet, aby trafił właśnie do tej podsieci. Litera L wskazuje na adres lokalnego interfejsu podłączonego właśnie do tej sieci. Jest to dodatkowa informacja, która pozwala odnaleźć się w gąszczu podsieci.

```
R1#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, FastEthernet0/0
L        192.168.10.1/32 is directly connected, FastEthernet0/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet1/0
L        192.168.20.1/32 is directly connected, GigabitEthernet1/0
R1#
```

A zatem pierwszy wpis oznacza, że sieć 192.168.10.0/24 jest bezpośrednio podłączona do routera R1, prowadzi zaś do niej interfejs fa0/0. Jeśli spojrzysz na rysunek 13.1, przekonasz się, że jest to prawda. Ponadto sieć 192.168.20.0/24 również jest podłączona bezpośrednio do routera R1, ale przez interfejs g1/0.

Co się jednak stanie, kiedy po tej konfiguracji stacja H1 wykona ping do stacji H2?

W takim przypadku stacja H1 musi uzyskać adres MAC stacji roboczej H2. Jest to niemożliwe, gdyż obie stacje znajdują się w różnych sieciach i różnych domenach rozgłoszeniowych. Stacja robocza H1 ma jednakże podaną w ustawieniach protokołu TCP/IP domyślną bramę, którą jest interfejs fa0/0 routera R1. Wysyła więc rozgłoszenie ARP do sieci, podając jako docelowy adres IP domyślnej bramy. Ponieważ stacja robocza oraz interfejs routera znajdują się w tej samej sieci VLAN (tej samej domenie rozgłoszeniowej), ramka trafia do interfejsu routera i router przesyła adres MAC swojego interfejsu. Rozpoczyna się zatem komunikacja.

Stacja robocza za każdym razem musi posiadać ustawienia domyślnej bramy. Jeśli stacja nie może wykonać komunikacji poza sieć, a sprawdzasz to poleceniem ping, to otrzymasz na konsoli komunikat: *Destination host unreachable* („host docelowy nieosiągalny"). Jest to klasyczny, najłatwiejszy sposób weryfikacji.

Ramka trafia do interfejsu routera R1. Router, dekapsulując ramkę, wyłania pakiet i sprawdza w nim, że adresem docelowym jest 192.168.20.10. Router bada więc tablicę routingu i dopasowuje adres docelowy do wpisów w tablicy. Okazuje się, że adres IP jest częścią podsieci 192.168.20.0/24, dlatego router odsyła pakiet przez interfejs g1/0, zgodnie z zapisem w tablicy routingu. Pakiet jest ponownie umieszczany w ramce i, po wcześniejszym przeprowadzeniu procesu ARP, wysyłany przez interfejs fizyczny. Ramka otrzymuje znakowanie VLAN20 i trafia do stacji roboczej H2.

Po zakończeniu konfiguracji routera i przełączników możesz wykonać testowy `ping` ze stacji `H1` do stacji `H2`. Jak widzisz na poniższym listingu, stacja `H2` odpowiada bez problemu.

```
H1>ping 192.168.20.10
Badanie 192.168.20.10 z 32 bajtami danych:
Odpowiedź z 192.168.20.10: bajtów=32 czas=1ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=2ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=1ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=2ms TTL=64
Statystyka badania ping dla 192.168.20.10:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 2 ms, Maksimum = 5 ms, Czas średni = 3 ms
H1>
```

Teraz na stacji roboczej `H1` wydaj polecenie `tracert –d [adres_IP]`, podając adres IP stacji `H2`. Zauważ, że w wyniku pojawia się właśnie adres IP interfejsu `fa0/0` routera `R1`. Przez ten interfejs zostaje przesłany pakiet. Użyty w poleceniu parametr `–d` sprawia, że w wynikach polecenia nie będą rozwiązywane nazwy własne. Wynik polecenia otrzymuje się w takim przypadku znacznie szybciej.

```
H1>tracert -d 192.168.20.10
Tracing route to 192.168.20.10 over a maximum of 30 hops:
  1    1 ms      0 ms      0 ms      192.168.10.1
  2    0 ms      0 ms      0 ms      192.168.20.10
Trace complete.
H1>
```

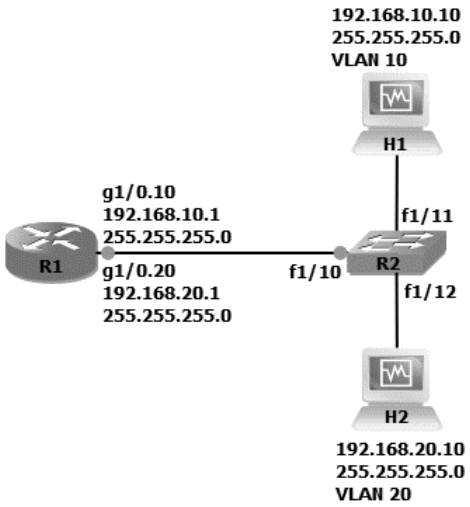
Pora na podsumowanie informacji dotyczących metody klasycznej. Jak zauważyłeś, w przypadku dwóch sieci VLAN właściwie nie ma przeszkód, aby zastosować tę metodę. Jednak każda kolejna sieć VLAN wymaga odrębnego interfejsu na routerze i przełączniku. Oznacza to, że przy 20 sieciach VLAN trudno będzie w ten sposób zrealizować routing pomiędzy sieciami VLAN.

Router-on-a-stick

Kolejna metoda, *router-on-a-stick*, przypomina metodę klasyczną, jednak tutaj do komunikacji przełącznika z routerem wykorzystany jest jeden przewód. Rozwiązuje to problem związany z dużą liczbą interfejsów potrzebną w przypadku zastosowania wielu sieci VLAN. Pojawia się za to inna trudność, która przy dużym ruchu niestety będzie nie do pokonania. Zjawisko to nosi nazwę *bottleneck* (wąskie gardło). Jak można się spodziewać, duża ilość ruchu sieciowego przesyłanego przez stacje robocze spowoduje dość duże obciążenie interfejsu; jest to bez wątpienia spory minus tej metody. Jednak w niewielkich sieciach *router-on-a-stick* jest bardzo dobrym rozwiązaniem, szczególnie jeśli firma posiada tylko przełączniki warstwy 2.

Na poniższym rysunku 13.2 pokazano sieć komputerową, w której połączenie pomiędzy routerem a przełącznikiem realizowane jest za pomocą jednego przewodu. Przejdźmy więc do konfiguracji i szczegółowego omówienia działania prezentowanej tu metody.

Rysunek 13.2. *Metoda router-on-a-stick*



Tym razem konfigurację rozpoczniemy od routera `R1`. Poleceniem `show ip interface brief` wyświetl listę wszystkich interfejsów. Zauważ, że interfejs `GigabitEthernet1/0`, do którego podpięty jest przełącznik, nie ma adresu IP. Jest to wbrew pozorom poprawne. Gdyby interfejs posiadał adres IP, należałoby go usunąć poleceniem `no ip address`.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
GigabitEthernet1/0     unassigned      YES unset  administratively down down
Serial2/0              unassigned      YES unset  administratively down down
Serial2/1              unassigned      YES unset  administratively down down
Serial2/2              unassigned      YES unset  administratively down down
Serial2/3              unassigned      YES unset  administratively down down
GigabitEthernet3/0     unassigned      YES unset  administratively down down
R1#
```

Ponieważ mamy jeden fizyczny przewód, a do podłączenia dwie sieci VLAN, wykorzystamy funkcjonalność opartą na podinterfejsach (*subinterfaces*). Polega ona na tym, że na podstawie identyfikatora interfejsu fizycznego tworzy się podinterfejs dla każdej sieci VLAN.

Aby to zrobić, w konfiguracji globalnej wydaj polecenie `interface [identyfikator_interfejsu_fizycznego] . [identyfikator_sieci_vlan]`.

Podanie identyfikatora sieci VLAN w powyższym poleceniu jest opcjonalne. Może to być dowolna wartość, niekoniecznie identyfikator sieci VLAN. Jednak przedstawiona tu praktyka jest zalecana, gdyż dzięki niej łatwo zachować porządek.

Jeśli więc mamy sieć VLAN10, komenda tworząca podinterfejs będzie wyglądała następująco: `interface g1/0.10`. Po utworzeniu podinterfejsu znajdziesz się w trybie jego konfiguracji. Zanim przypiszesz do niego adres IP, musisz wskazać enkapsulację oraz podać identyfikator sieci VLAN. Uczyń to poleceniem `encapsulation dot1q [identyfikator_sieci_vlan]`. Teraz możesz już przypisać dowolny adres IP. Podanie enkapsulacji jest ważne, gdyż interfejs routera dzięki temu wie, jak obsłużyć znakowane ramki, które będą do niego wysyłane. Ponadto musi on wiedzieć, jak znakować ramki, które sam będzie wysyłał do sieci.

Pamiętaj, że adres ten będzie adresem domyślnej bramy dla wszystkich stacji roboczych występujących w tej podsieci i znajdujących się w tej sieci VLAN. Przypisanie adresu IP odbywa się przy użyciu polecenia, które już znasz: `ip address [adres_ip] [maska_podsieci]`. Konfigurację obydwu podinterfejsów dla sieci VLAN10 i VLAN20 przedstawia poniższy listing. Na sam koniec przejdź do fizycznego interfejsu g1/0 i uruchom go poleceniem `no shutdown`.

```
R1(config)#int g1/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#int g1/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#
R1(config)#int g1/0
R1(config-if)#no shutdown
R1(config-if)#
```

Za pomocą polecenia `show ip interface brief` jeszcze raz wyświetl listę interfejsów. Pojawiły się na niej dwa dodatkowe podinterfejsy posiadające adres IP. Interfejs fizyczny g1/0 nie ma adresu.

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
GigabitEthernet1/0     unassigned      YES unset  up                    up
GigabitEthernet1/0.10  192.168.10.1    YES manual up                    up
GigabitEthernet1/0.20  192.168.20.1    YES manual up                    up
Serial2/0              unassigned      YES unset  administratively down down
Serial2/1              unassigned      YES unset  administratively down down
Serial2/2              unassigned      YES unset  administratively down down
Serial2/3              unassigned      YES unset  administratively down down
GigabitEthernet3/0     unassigned      YES unset  administratively down down
R1#
```

W kolejnym kroku przejdź do konfiguracji przełącznika. Zakładam, że sieci VLAN są już utworzone i mają przypisane interfejsy, do których podpięte są stacje robocze. Dlatego interfejs f1/10 należy jedynie ustawić do pracy jako `trunk`, korzystając z polecenia `switchport mode trunk`. Ustawienie interfejsu jako `trunk` sprawi, że będzie on przekazywał ruch płynący z różnych sieci VLAN. Nie można więc tego interfejsu ustawić do pracy w konkretnym VLAN-ie.

```
R2(config)#int f1/10
R2(config-if)#switchport mode trunk
R2(config-if)#
```

Wyświetlenie tablicy routingu routera R1 pokazuje informacje podobne do tych, które pojawiły się w poprzedniej metodzie. Obie sieci w tablicy są oznaczone jako bezpośrednio podłączone, zmieniły się jedynie interfejsy, przez które sieci są dostępne.

```
R1#show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1/0.10
L        192.168.10.1/32 is directly connected, GigabitEthernet1/0.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet1/0.20
L        192.168.20.1/32 is directly connected, GigabitEthernet1/0.20
R1#
```

Tym razem wykonaj test ping pomiędzy stacjami roboczymi (ze stacji H1 do stacji H2), które bez problemu powinny się ze sobą komunikować.

```
 C:\>ping 192.168.20.10
Badanie 192.168.20.10 z 32 bajtami danych:
Odpowiedź z 192.168.20.10: bajtów=32 czas=5ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=3ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=4ms TTL=64
Odpowiedź z 192.168.20.10: bajtów=32 czas=2ms TTL=64
Statystyka badania ping dla 192.168.20.10:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 2 ms, Maksimum = 5 ms, Czas średni = 3 ms
C:\>
```

W przypadku zastosowania metody *router-on-a-stick* ramki wysłane ze stacji roboczej są znakowane na interfejsie przełącznika i przesyłane przez połączenie trunk do routera. Dzięki temu, że na każdym z podinterfejsów routera wskazałeś enkapsulację oraz podałeś identyfikator VLAN, ramki są kierowane do odpowiedniego podinterfejsu routera. Router może je więc prawidłowo zinterpretować i przesłać dalej na podstawie tablicy routingu.

Polecenie tracert wydane ze stacji H1 do stacji H2 pokazuje drogę pakietów przez bramę domyślną 192.168.10.1, czyli adres podinterfejsu g1/0.10 routera R1.

```
H1>tracert 192.168.20.10
Tracing route to 192.168.20.10 over a maximum of 30 hops:
  1   1 ms      0 ms      1 ms      192.168.10.1
  2   10 ms     10 ms     0 ms      192.168.20.10
Trace complete.
H2>
```

Przełączanie w warstwie 3.

Przełączanie w warstwie 3. wygląda nieco inaczej niż w warstwie 2., gdzie odbywało się wyłącznie na podstawie adresów MAC. Wszystkie inne czynności dostosowywane były właśnie do tych identyfikatorów. W warstwie 3. przełączanie następuje na podstawie adresów IP, czyli warstwy 3. Ze względu na to, że praca odbywa się w warstwie 3., przełączniki posiadają również wiele innych funkcjonalności routerów. Mogą więc z powodzeniem przejmować część ruchu sieciowego, tak by routery nie musiały być angażowane.

Do realizowania przełączania w warstwie 3. przełączniki używają CEF (ang. *Cisco Express Forwarding*).

Przełącznik L3 wykonuje przełączanie nie na podstawie mikroprocesora, ale przy użyciu układu cyfrowego (tzw. ASIC). Dlatego jeśli przełącznik podejmuje decyzję o przesłaniu pakietu w warstwie 3., to do wyznaczania trasy używa konkretnego pakietu (pierwszego); pozostałe pakiety z danej transmisji zostają przekazane przy pomocy warstwy 2.

Przełączanie wykorzystuje dwie funkcjonalności: *Forwarding Information Base* (FIB) oraz *adjacency table* („tablicę przylegania").

`FIB` jest czymś w rodzaju tablicy używanej do przesyłania pakietu w inne miejsce w sieci. Przypomina swoim działaniem tablicę routingu, na której podstawie routery podejmują decyzję o przesłaniu pakietu do innej podsieci. Tablica `FIB` zawiera więc co najmniej adres podsieci oraz interfejs, który osiąga tę podsieć.

Adjacency table obejmuje wpisy dotyczące adresów warstwy 2., wykorzystywane m.in. w `FIB` i pomocne w trakcie przesyłania informacji dalej.

Przełączniki warstwy 3. wyglądają tak samo jak ich młodsi koledzy z warstwy 2. Posiadają fizyczne interfejsy, których liczba zależy od modelu przełącznika. W celu wykonywania przełączania w warstwie 3. mają możliwość skonfigurowania interfejsów SVI (ang. *Switch Virtual Interface*). Są to wirtualne interfejsy, które pozwalają na komunikację pomiędzy sieciami VLAN.

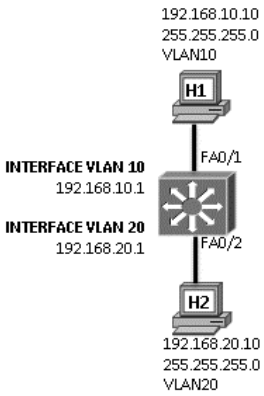
Opisywana metoda komunikowania się sieci VLAN między sobą oparta jest więc na przełącznikach warstwy 3. Na poniższym rysunku 13.3 pokazano tylko przełącznik; nie ma tu już natomiast routera.

Najpierw na przełączniku warstwy 3. musisz uruchomić funkcjonalność routingu. W trybie konfiguracji globalnej wydaj więc komendę `ip routing`.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ip routing
S1(config)#
```

Następnie utwórz sieci `VLAN10` oraz `VLAN20` i przypisz do nich odpowiednie interfejsy. W kolejnym kroku utwórz wirtualne interfejsy dla sieci `VLAN10` oraz `VLAN20`. Służy do tego standardowa komenda `interface [identyfikator_interfejsu]`.

Rysunek 13.3.
Komunikacja pomiędzy sieciami VLAN z wykorzystaniem przełącznika L3



Teraz do każdego z interfejsów wirtualnych przypisz odpowiedni adres IP. Będzie to adres domyślnej bramy, którą podasz na stacjach roboczych `H1` i `H2`.

```
S1(config)#
S1(config)#interface vlan 10
S1(config-if)#ip address 192.168.10.1 255.255.255.0
S1(config-if)#exit
S1(config)#interface vlan 20
S1(config-if)#ip address 192.168.20.1 255.255.255.0
S1(config-if)#
```

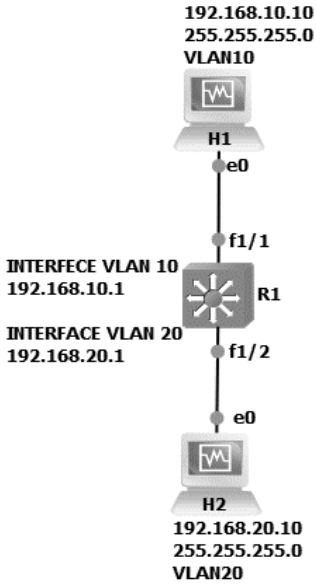
Po przypisaniu adresów IP do interfejsów możesz na przełączniku wyświetlić tablicę routingu. Użyj tego samego polecenia co na routerze, czyli `show ip route`. W tablicy znajdują się dwie podsieci bezpośrednio podłączone oraz interfejsy wyjściowe `VLAN10` i `VLAN20`.

```
S1#show ip route
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
S1#
```

Bez wątpienia rozwiązanie oparte na przełącznikach warstwy 3. jest optymalne. Nie generuje dodatkowego ruchu, odciąża routery, jest proste w konfiguracji i umożliwia dowolne kierowanie ruchu za pomocą ACL, o których więcej przeczytasz w dalszej części tej książki. Niestety opisywana metoda jest dość droga.

Jeśli przedstawioną powyżej konfigurację chcesz przetrenować w GNS3, możesz to uczynić, wykorzystując router 3745 z modułem przełącznika (patrz rysunek 13.4). Utwórz ten sam model w programie GNS3, przeciągając na obszar roboczy wspomniany router



Rysunek 13.4. *Projekt sieci z przełącznikiem L3 wykonany w GNS3*

oraz dwie stacje robocze. Nadaj im odpowiednie adresy IP, nie zapominając o poprawnym adresie domyślnej bramy. Następnie przejdź do konfiguracji routera. W projekcie zmieniona została dodatkowo ikona routera.

Jeśli utworzyłeś projekt, w pierwszej kolejności powinieneś sformatować w GNS3 pamięć flash. W tym celu wydaj polecenie `format flash:`. Dzięki temu nie pojawi się błąd w trakcie tworzenia sieci VLAN i nie narazisz się na niepotrzebne kłopoty. Błąd nie musi się pokazać w każdej takiej sytuacji, ale jeśli wykonasz formatowanie, będziesz miał gwarancję, że nie wystąpi.

```
R1#format flash:
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "flash:".  Continue? [confirm]
Current Low End File System flash card in flash will be formatted into DOS File
↪System flash card!  Continue? [confirm]
Format: Drive communication & 1st Sector Write OK...
Writing Monlib sectors.
.....................................................................................
Monlib write complete
Format: All system sectors written. OK...
Format: Total sectors in formatted partition: 8049
Format: Total bytes in formatted partition: 4121088
Format: Operation completed successfully.
Format of flash complete
R1#
```

Teraz możesz przejść do właściwej konfiguracji. Wydaj polecenie `vlan database` i utwórz w konfiguracji sieci VLAN dwie nowe sieci. Następnie poleceniem `apply` zapisz wprowadzone dane.

Jak widzisz, w GNS3 konfiguracja jest nieco odmienna, ale dzięki temu, że wiesz, jak wygląda, będziesz mógł przećwiczyć nowo nabyte umiejętności bez konieczności posiadania rzeczywistego przełącznika.

```
R1#vlan database
R1(vlan)#vlan 10
VLAN 10 modified:
R1(vlan)#vlan 20
VLAN 20 modified:
R1(vlan)#apply
APPLY completed.
R1(vlan)#exit
APPLY completed.
Exiting....
R1#
```

Teraz do każdego interfejsu VLAN, czyli `VLAN10` oraz `VLAN20`, przypisz odpowiednie adresy IP, zgodnie z poniższym listingiem.

```
R1(config)#int vlan 10
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#int vlan 20
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
```

Ostatnia czynność w tej konfiguracji to dodanie do odpowiednich sieci VLAN interfejsów naszego przełącznika, do których podłączone zostały wirtualne stacje. Aby to zrobić, przejdź do konfiguracji odpowiednich interfejsów i wydaj polecenie `switchport access vlan [siec_VLAN]`. Teraz stacje bez problemu powinny się ze sobą komunikować.

```
R1(config-if)#int f1/1
R1(config-if)#switchport access vlan 10
R1(config-if)#
R1(config-if)#int f1/2
R1(config-if)#switchport access vlan 20
R1(config-if)#
```

Skorowidz

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

S

Ś

T

U

V

W

X

Z

Ż

Szeroko zarzuć sieci i zdaj egzamin CCNA 200–125!

Szybkie sieci komputerowe oplotły świat w zawrotnym tempie. Jeszcze kilkanaście lat temu w Polsce niemal wszyscy posługiwali się modemami podpiętymi do kabli telefonicznych. Dane przepychały się przez te sieci długo i bez gwarancji, że w ogóle uda się je ściągnąć, zanim zerwie się połączenie. Dziś używamy diametralnie innych sieci, a internet jest nam potrzebny niemal w każdej chwili życia: do sprawdzenia pogody, trasy dojazdu czy informacji na dowolny temat. Nagła utrata połączenia bywa dużym utrudnieniem, dlatego właśnie tak bardzo potrzebni są kompetentni administratorzy sieci komputerowych.

Jeśli chcesz zostać takim administratorem — albo już nim jesteś, ale masz potrzebę uaktualnienia swojej wiedzy — czym prędzej sięgnij po tę książkę. Znajdziesz tu odpowiedzi na wszystkie pytania z prestiżowego egzaminu CCNA 200–125. Nie tylko nauczysz się wszystkiego, co musisz wiedzieć o typach sieci, protokołach, przełącznikach, routingu, adresacji, listach ACL, logowaniu zdarzeń, raportowaniu i bezpieczeństwie, lecz także będziesz gotów zdać ten egzamin i otrzymać cenny certyfikat CCNA. Ta książka zawiera wiadomości podane na przykładach i konkretach, a oprócz nich jej autor proponuje ćwiczenia praktyczne. Pozwolą Ci one sprawdzić wiedzę i wyobrazić sobie różne sytuacje, które mogą dotyczyć także Twojej sieci. Czytaj, ucz się i śmiało podejdź do egzaminu CCNA 200–125!

- Informacje wstępne o sieciach komputerowych, modele sieci i Ethernet
- Zastosowanie programu Wireshark i emulator GNS3
- Wprowadzenie do systemu operacyjnego iOS i konfiguracja urządzeń Cisco
- Adresacja IPv4 oraz IPv6, protokół STP i jego nowsze wersje
- Przełączniki sieciowe, sieci VLAN i routing pomiędzy sieciami VLAN
- Routing statyczny, dynamiczny i tablice routingu
- Routing dynamiczny — protokoły: RIP, OSPF, EIGRP
- Listy: ACL, Network Address Translation (NAT) i DHCP
- Redundancja w sieci i wykorzystanie nadmiarowości
- Technologie sieci WAN i VPN oraz protokół routingu BGP
- Logowanie zdarzeń, raportowanie, zarządzanie bezpieczeństwem sieci
- Obsługa Cisco Configuration Professional
- Ćwiczenia praktyczne

CCNA 200–125 — certyfikat na wyciągnięcie ręki!

Helion

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

ISBN 978-83-283-3280-5

9 788328 332805

Informatyka w najlepszym wydaniu

cena: 199,00 zł