ADAM JÓZEFIOK

CCNA 200-301

ZOSTAŃ ADMINISTRATOREM SIECI KOMPUTEROWYCH CISCO

Helion

Redaktor prowadzący: Małgorzata Kulik

Recenzja naukowa: prof. dr hab. inż. Tadeusz Czachórski, dyrektor Instytutu Informatyki Teoretycznej i Stosowanej Polskiej Akademii Nauk (IITiS PAN),
dr hab. inż. Bartłomiej Zieliński, prof. Politechniki Śląskiej

Projekt okładki: Studio Gravite / Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki
Grafika na okładce została wykorzystana za zgodą Shutterstock.com

Helion SA
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/ccn301
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-7168-2

Printed in Poland.

Spis treści

Rozdział 14.

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 ramka zostaje wysłana ze stacji roboczej nieoznakowana, a trafiając do interfejsu przełącznika, otrzymuje oznakowanie i od tej chwili może się komunikować 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 pracownik 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, 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.

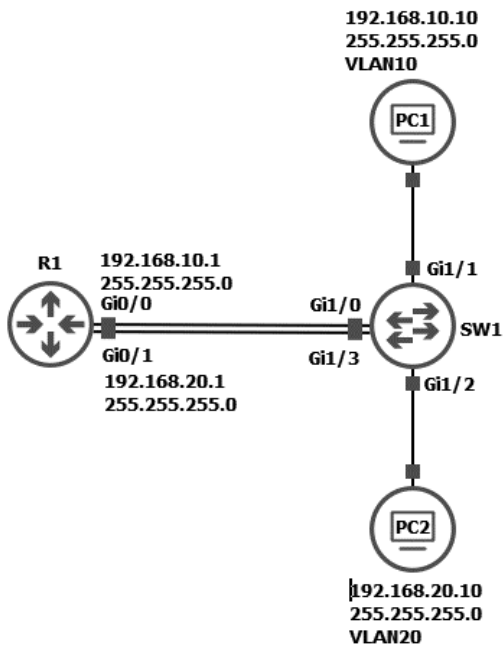
Za chwilę omówię trzy metody, które umożliwiają komunikowanie się stacji roboczych znajdujących się w różnych sieciach VLAN. Dzięki analizie przykładów zorientujesz się, która z nich jest dla Ciebie optymalna.

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 w poprzednich rozdziałach.

Metoda klasyczna

Metoda klasyczna polega na skierowaniu ruchu z sieci VLAN do routera. Spójrz na rysunek 14.1. Przedstawia on dwie stacje robocze. Są to stacje VPC użyte w programie GNS3, ale możesz również użyć własnych wirtualnych maszyn. 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 14.1. *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: `GigabitEthernet0/0` i `GigabitEthernet0/1`. W naszym przykładzie są konieczne właśnie dwa interfejsy. Metoda klasyczna wymaga, aby każdy interfejs routera należał do określonej sieci VLAN i był bramą domyślną dla wszystkich stacji w tej podsieci. Interfejs `g0/0` ma więc adres IP `192.168.10.1` i jest domyślną bramą dla wszystkich urządzeń znajdujących się w sieci `VLAN10`.

Najpierw jednak skonfigurujmy przełącznik warstwy 2, czyli klasyczny przełącznik Cisco, którego już używaliśmy w innych zadaniach. Aby na tym emulowanym przełączniku utworzyć nowe sieci VLAN, `VLAN10` i `VLAN20`, użyj w trybie uprzywilejowanym polecenia `vlan` *`[numer_sieci_vlan]`*. Polecenie `exit` powoduje zapisanie ustawień.

```
SW1(config)#vlan 10
SW1(config-vlan)#exit
SW1(config)#vlan 20
SW1(config-vlan)#exit
SW1(config)#
```

W kolejnym kroku przypisz interfejs g1/1 do sieci VLAN10, a interfejs g1/2 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.

```
SW1(config)#int g1/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#int g1/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#
```

Używając polecenia show vlan brief, sprawdź, czy interfejsy znajdują się w odpowiednich sieciach VLAN.

```
SW1#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/0, Gi0/1, Gi0/2, Gi0/3
                                                Gi1/0, Gi1/3, Gi2/0, Gi2/1
                                                Gi2/2, Gi2/3, Gi3/0, Gi3/1
                                                Gi3/2, Gi3/3
10   VLAN0010                         active    Gi1/1
20   VLAN0020                         active    Gi1/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
SW1#
```

Następnie, zanim przejdziesz do konfiguracji routera, zobacz, czy ze stacji H1 można wykonać ping do stacji H2. Jak widać na poniższym listingu, jest to niemożliwe.

```
H1> ping 192.168.20.10
host (192.168.10.1) not reachable
H1>
```

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

```
SW1(config)#int g1/0
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit
SW1(config)#int g1/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(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 na

przykład interfejs g0/0 routera R1 ma 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. Stację VPCS skonfigurujesz za pomocą komendy `ip` *`[adresIP] [maska] [adresIP_domyslnej_bramy]`*, np. `ip 192.168.10.10 255.255.255.0 192.168.10.1`. Zajmijmy się teraz routerem R1.

```
R1(config)#int g0/0
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 g0/1
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
GigabitEthernet0/0         192.168.10.1    YES manual up                    up
GigabitEthernet0/1         192.168.20.1    YES manual up                    up
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
R1#
```

Po zakończeniu konfiguracji wyświetl na routerze tablicę routingu, wpisując polecenie `show ip route`. 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`, która oznacza źródło wpisu. Litera `C` pochodzi od słowa `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 fraza `is directly connected` (jest bezpośrednio podłączona). Natomiast identyfikator umieszczony na końcu oznacza interfejs, którym musi zostać przesłany pakiet, aby trafił właśnie do tej podsieci. Litera `L` wskazuje na adres lokalnego interfejsu podłączonego 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
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
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, GigabitEthernet0/0
```

```
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet0/1
L        192.168.20.1/32 is directly connected, GigabitEthernet0/1
R1#
```

A zatem pierwszy wpis oznacza, że sieć `192.168.10.0/24` jest bezpośrednio podłączona do routera `R1`, prowadzi zaś do niej interfejs `g0/0`. Jeśli spojrzysz na rysunek 14.1, przekonasz się, że jest to prawda. Ponadto sieć `192.168.20.0/24` również jest podłączona bezpośrednio do routera `R1`, ale przez interfejs `g0/1`.

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 `g0/0` 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 mieć 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 `g0/1`, zgodnie z zapisem w tablicy routingu. Pakiet jest ponownie umieszczany w ramce i, po wcześniejszym przeprowadzeniu procesu ARP, wysyłany przez interfejs fizyczny. Ramka otrzymuje oznakowanie `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.

```
PC1> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=63 time=34.222 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=63 time=13.447 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=63 time=16.257 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=63 time=15.582 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=63 time=17.787 ms
PC1>
```

Teraz na stacji roboczej `H1` wydaj polecenie `trace` *`[adres_IP]`*, podając adres IP stacji `H2`. Zauważ, że w wyniku pojawia się właśnie adres IP interfejsu `g0/0` routera `R1`. Przez ten interfejs zostaje przesłany pakiet.

```
PC1> trace 192.168.20.10
trace to 192.168.20.10, 8 hops max, press Ctrl+C to stop
```

```
  1   192.168.10.1   14.031 ms  13.028 ms  10.330 ms
  2   192.168.20.10   18.993 ms
PC1>
```

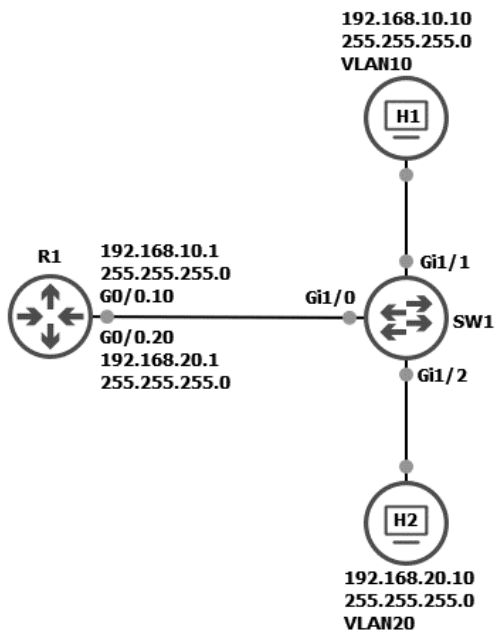
Pora na podsumowanie informacji dotyczących metody klasycznej. Jak zauważyłeś, w przypadku dwóch sieci VLAN właściwie nie ma przeszkód, aby zastosować tę metodę. Jednak każda kolejna sieć VLAN wymaga odrębnego interfejsu na routerze i przełączniku. Oznacza to, że przy 20 sieciach VLAN trudno będzie w 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, duży ruch sieciowy generowany przez stacje robocze spowoduje dość duże obciążenie interfejsu, co jest bez wątpienia sporym minusem tej metody. Jednak w niewielkich sieciach *router-on-a-stick* jest bardzo dobrym rozwiązaniem, szczególnie jeśli firma posiada tylko przełączniki warstwy 2.

Na rysunku 14.2 pokazałem 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. Możesz do tego ćwiczenia wykorzystać poprzednie, ale wymaż konfigurację routera i przełącznika, aby łatwiej Ci było dokonywać nowych ustawień.

RYSUNEK 14.2. *Metoda router-on-a-stick*



Tym razem konfigurację rozpoczniemy od routera R1. Poleceniem show ip interface brief wyświetl listę wszystkich interfejsów. Interfejs GigabitEthernet0/0, do którego podpięty jest przełącznik, nie ma adresu IP. Jest to wbrew pozorom poprawne. Gdyby interfejs miał adres IP, należałoby go usunąć poleceniem no ip address.

```
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES manual administratively down down
GigabitEthernet0/1         unassigned      YES manual administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
R1#
```

Sprawdźmy też, czy pomiędzy stacjami roboczymi jest komunikacja. Wykonaj ping ze stacji H1 do stacji H2.

```
H1> ping 192.168.20.10
host (192.168.10.1) not reachable
H1>
```

Oczywiście komunikacja nie działa. Stacje są w różnych podsieciach, została również usunięta wszelka konfiguracja urządzeń, które zapewniały komunikację tych dwóch stacji.

Ponieważ mamy jeden fizyczny przewód, a do podłączenia dwie sieci VLAN, wykorzystamy funkcjonalność opartą na podinterfejsach (ang. *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 g0/0.10. Po utworzeniu podinterfejsu znajdziesz się w trybie jego konfiguracji. Zanim przypiszesz do niego adres IP, musisz wskazać enkapsulację oraz podać identyfikator sieci VLAN. Zrób 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 oznakowane 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 g0/0 i uruchom go poleceniem no shutdown.

```
R1(config)#int g0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#int g0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#
```

Wyświetl teraz poleceniem `show ip interface brief` listę skonfigurowanych wcześniej interfejsów. Zauważ, że mają adresy IP, ale nie są aktywne. Dzieje się tak, ponieważ interfejs fizyczny `g0/0` nie został włączony.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES manual administratively down down
GigabitEthernet0/0.10      192.168.10.1    YES manual administratively down down
GigabitEthernet0/0.20      192.168.20.1    YES manual administratively down down
GigabitEthernet0/1         unassigned      YES manual administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
R1#
```

Włącz interfejs `g0/0`, aby uruchomić również pozostałe podinterfejsy.

```
R1(config)#int g0/0
R1(config-if)#no shutdown
R1(config-if)#
```

Za pomocą polecenia `show ip interface brief` ponownie wyświetl listę interfejsów. Tym razem wszystko jest już uruchomione. Interfejs fizyczny `g0/0` nie ma adresu, ale jest włączony.

```
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES manual up                    up
GigabitEthernet0/0.10      192.168.10.1    YES manual up                    up
GigabitEthernet0/0.20      192.168.20.1    YES manual up                    up
GigabitEthernet0/1         unassigned      YES manual administratively down down
GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
R1#
```

W kolejnym kroku przejdź do konfiguracji przełącznika i jeszcze raz przypisz interfejsy do odpowiednich sieci VLAN, jeśli wcześniej usunąłeś konfigurację. Dodatkowo interfejs `g1/0` 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. Jeśli w trakcie zmiany interfejsu na tryb `trunk` pojawi się komunikat `Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode`, należy zmienić enkapsulację na interfejsie z trybu automatycznego na tryb ustawiony manualnie.

```
SW1(config)#int g1/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
```

```
SW1(config-if)#int g1/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit
SW1(config)#int g1/0
SW1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured
↪to "trunk" mode.
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#
```

Przejdź jeszcze na chwilę do konsoli routera i wyświetl tablicę routingu. 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
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
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, GigabitEthernet0/0.10
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L        192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
R1#
```

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

```
H1> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=63 time=39.416 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=63 time=17.031 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=63 time=16.691 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=63 time=15.701 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=63 time=19.622 ms
H1>
```

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 podinterfejsie routera wskazałeś enkapsulację i podałeś identyfikator VLAN, ramki są kierowane do odpowiedniego podinterfejsu routera. Router może je więc prawidłowo zinterpretować i przesłać dalej na podstawie tablicy routingu.

Polecenie `trace` wydane ze stacji `H1` do stacji `H2` pokazuje drogę pakietów przez bramę domyślną `192.168.10.1`, czyli adres podinterfejsu `g0/0.10` routera `R1`.

```
H1> trace 192.168.20.10
trace to 192.168.20.10, 8 hops max, press Ctrl+C to stop
 1   192.168.10.1   15.199 ms  17.172 ms  8.022 ms
 2   192.168.20.10   16.607 ms
H1>
```

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 mają 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), a pozostałe pakiety z danej transmisji zostają przekazane za pomocą warstwy 2.

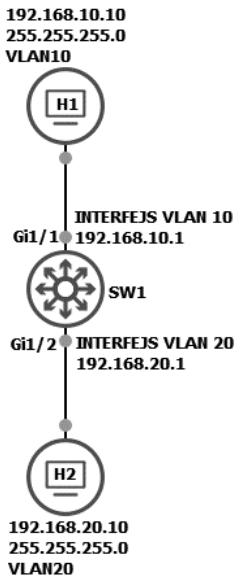
Przełączanie wykorzystuje dwie funkcjonalności: *Forwarding Information Base* (FIB) i *adjacency table* (tablica przylegania).

`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. Mają 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 rysunku 14.3 został pokazany tylko przełącznik, nie ma tu już natomiast routera. Przełącznik, którego tu używam, to ten sam, którego używałem wcześniej, jednak dla zachowania przejrzystości schematu zmieniłem jego ikonę, tak aby kojarzył się z przełącznikiem warstwy 3.



RYSUNEK 14.3. *Komunikacja pomiędzy sieciami VLAN z wykorzystaniem przełącznika L3*

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

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#ip routing
SW1(config)#
```

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

Teraz do każdego z interfejsów wirtualnych przypisz odpowiedni adres IP. Będzie to adres domyślnej bramy, którą podasz na stacjach roboczych `H1` i `H2`. Zauważ, że dopiero po wydaniu komendy `no shutdown` interfejsy zostają uruchomione i przełączają się w stan przesyłania danych.

```
SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.10.1 255.255.255.0
SW1(config-if)#no shut
*Feb 26 14:49:30.834: %LINK-3-UPDOWN: Interface Vlan10, changed state to up
*Feb 26 14:49:31.841: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10,
↪changed state to up
SW1(config-if)#exit
SW1(config)#interface vlan 20
SW1(config-if)#ip address 192.168.20.1 255.255.255.0
SW1(config-if)#no shut
*Feb 26 14:50:41.747: %LINK-3-UPDOWN: Interface Vlan20, changed state to up
*Feb 26 14:50:42.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20,
↪changed state to up
SW1(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`.

```
SW1#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
       a - application route
       + - 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, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
SW1#
```

Można po raz kolejny sprawdzić, czy komunikacja pomiędzy stacjami roboczymi działa prawidłowo. Jak pokazuje poniższy listing, komunikacja działa.

```
H1> ping 192.168.20.10
84 bytes from 192.168.20.10 icmp_seq=1 ttl=63 time=3.207 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=63 time=3.908 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=63 time=7.155 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=63 time=3.210 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=63 time=4.269 ms
H1>
```

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.

Skorowidz

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

Q

R

S

Ś

T

U

V

W

X

Y

Z

ZOSTAŃ PROFESJONALNYM ADMINISTRATOREM SIECI CISCO

- **Poznaj teoretyczne podstawy działania sieci komputerowych**
- **Naucz się praktycznie konfigurować urządzenia sieciowe**
- **Dowiedz się, jak tworzyć i rozbudowywać sieci Cisco**

Sieci komputerowe oplotły dosłownie cały świat, obecnie korzystają z nich miliardy użytkowników, a liczba urządzeń podłączonych do internetu znacznie przekracza populację Ziemi. Rewolucja informatyczna stała się możliwa właśnie dzięki powszechnej dostępności do sieci — to dzięki niej ludzie mogą bez kłopotu korzystać z zasobów zgromadzonych w najsłynniejszych bibliotekach i największych bazach danych, w dowolnej chwili sprawdzać najnowsze informacje ze świata, wygodnie słuchać muzyki i oglądać materiały wideo, w mgnieniu oka dokonywać transakcji finansowych czy łączyć się ze znajomymi mieszkającymi w najodleglejszych zakątkach kuli ziemskiej.

Sieci przeszły długą drogę od czasu zestawienia pierwszych połączeń między komputerami, bez wątpienia czeka je też dalszy burzliwy rozwój. Jeśli chcesz mieć w nim udział i związać swoją karierę z budową lub utrzymaniem sieci, sięgnij po książkę *CCNA 200-301. Zostań administratorem sieci komputerowych Cisco*. Dzięki tej monografii poznasz teoretyczne podstawy funkcjonowania sieci i nauczysz się konfigurować je w praktyce. Niezależnie od tego, czy marzysz o pracy administratora infrastruktury sieciowej, czy chcesz zapoznać się z tematem w ramach studiów informatycznych, ten podręcznik pomoże Ci postawić pierwsze kroki, opanować niezbędną wiedzę, nabyć doświadczenia, zdać egzamin CCNA i… zdobyć upragniony certyfikat Cisco!

- **Egzaminy i ścieżka certyfikacji firmy Cisco**
- **Podstawy działania sieci komputerowych**
- **Najważniejsze narzędzia administratora sieci**
- **System operacyjny iOS i konfiguracja urządzeń Cisco**
- **Protokoły sieciowe oraz adresacja IPv4 i IPv6**
- **Routing statyczny, dynamiczny i między sieciami VLAN**
- **Translacja adresów sieciowych i DHCP**
- **Zabezpieczanie sieci i zapewnianie jakości obsługi**
- **Konfiguracja sieci bezprzewodowych**
- **Projektowanie i automatyzacja sieci**
- **Zarządzanie sieciami**

ŚMIAŁO WKROCZ NA ŚCIEŻKĘ CERTYFIKACJI CCNA!

DR 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 polskich oraz zagranicznych publikacji z tej dziedziny. Brał udział w konferencjach naukowych (krajowych oraz międzynarodowych) dotyczących sieci komputerowych. Posiada certyfikaty: CCNA Security, CCNP Routing and Switching, Cisco CCDP, CCNAV oraz certyfikat instruktorski Cisco CCAI, jak również certyfikaty ITIL i PRINCE2. Jego pasją jest pisanie książek, praca ze studentami i szeroko rozumiana dydaktyka.

Helion

helion.pl

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

ISBN 978-83-283-7168-2

9 788328 371682