Adam Józefiok

CCNA 200-120

ZOSTAŃ ADMINISTRATOREM SIECI KOMPUTEROWYCH CISCO

- Co siedzi w sieci, czyli wstęp do sieci komputerowych
- Jak sterować ruchem bitów, czyli routery, przełączniki i technologie sieciowe
- Z czym to się je, czyli ćwiczenia praktyczne z budowania i obsługi sieci

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/sikoci
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-246-9101-2

Printed in Poland.

Spis treści

Rozdział 12.

Routing pomiędzy sieciami VLAN

Teraz, kiedy omawiamy routery, możemy na chwilę powrócić do sieci VLAN, a ściślej do umożliwienia komunikacji między nimi. Jak wiesz, komunikacja we VLAN-ach odbywa się w warstwie drugiej ISO OSI. Na tym poziomie, jeśli dwa urządzenia znajdują się w różnych VLAN-ach, nie ma możliwości komunikacji między nimi. Ze względu na znajdujący się 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, natomiast trafiając do interfejsu przełącznika, otrzymuje znakowanie i od tej chwili może komunikować się z pozostałymi urządzeniami w tej samej sieci VLAN.

Odseparowany od siebie ruch 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 w prosty sposób to zrealizować i na jednym fizycznym urządzeniu oddzielić ruch płynący z poszczególnych działów.

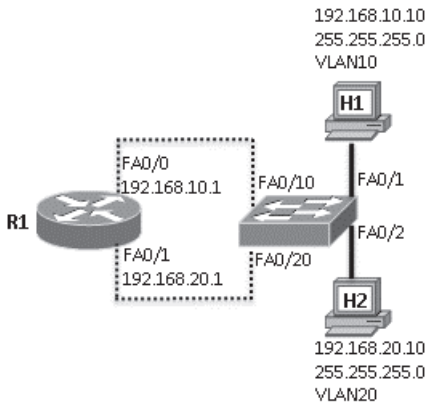
Oczywiście, odseparowanie od siebie stacji roboczych lub serwerów sprawi, że wiele aplikacji nie będzie ze sobą współdziałać. Dlatego wprowadzenie rozwiązania opartego na warstwie trzeciej jest konieczne do tego, aby umożliwić im komunikację, jednak w sposób w pełni kontrolowany i zapewniający pozbycie się zbędnych rozgłoszeń. Trzeba wspomnieć, że możliwość komunikacji sieci VLAN między sobą daje jedynie zastosowanie urządzenia warstwy trzeciej routera lub przełącznika.

Za chwilę zostanie omówiony każdy z trzech możliwych scenariuszy, w których będzie możliwość komunikowania się stacji roboczych znajdujących się w różnych sieciach VLAN. Na konkretnych przykładach przekonasz się, która z metod będzie dla Ciebie bardziej optymalna lub szybsza w implementacji.

Metoda klasyczna

Metoda klasyczna, tak ją nazwijmy, polega na skierowaniu ruchu z sieci VLAN do routera. Spójrz na poniższy rysunek (rysunek 12.1). Znajdują się na nim dwie stacje robocze. Stacja robocza H1 znajduje się w sieci VLAN10 i podsieci 192.168.10.0/24, natomiast stacja H2 jest w sieci VLAN20 i podsieci 192.168.20.0/24. Jeśli w sieci nie będzie routera, te dwie stacje nie mogą się ze sobą komunikować. Oczywiście, pierwszy powód to taki, że znajdują się w różnych podsieciach, ale najważniejszym powodem jest to, że znajdują się w różnych sieciach VLAN.

Rysunek 12.1.
Routing pomiędzy sieciami VLAN — model klasyczny



Aby te dwie stacje robocze mogły się ze sobą komunikować, użyjemy routera R1. Jest on wyposażony w 2 interfejsy FastEthernet i ta funkcjonalność w tym przypadku jest konieczna. Rozwiązanie klasyczne 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 przejdźmy do konfiguracji przełącznika. Poleceniem vlan [numer_sieci_vlan] utwórz dwie sieci VLAN: VLAN10 oraz VLAN20.

```
S1(config)#vlan 10
S1(config-vlan)#vlan 20
S1(config-vlan)#
```

W kolejnym kroku przypisz interfejs fa0/1 do sieci VLAN10, a interfejs fa0/2 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.

```
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#int fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10
S1(config-if)#int fa0/2
```

```
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20
S1(config-if)#
```

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

```
S1#show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                         active    Fa0/1
20   VLAN0020                         active    Fa0/2
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
S1#
```

Teraz, kiedy interfejsy podłączone do stacji roboczych są już w odpowiednich sieciach VLAN, w kolejnym kroku przypisz do sieci VLAN interfejsy prowadzące do routera R1.

```
S1(config)#int fa0/10
S1(config-if)#switchport access vlan 10
S1(config-if)#int fa0/20
S1(config-if)#switchport access vlan 20
S1(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.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shut
*Apr 10 19:03:15.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface
↪FastEthernet0/0, changed state to up
R1(config-if)#int fa0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
*Apr 10 19:03:39.907: %LINEPROTO-5-UPDOWN: Line protocol on Interface
↪FastEthernet0/1, changed state to up
R1(config-if)#
```

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

```
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.10.1    YES manual up                    up
FastEthernet0/1            192.168.20.1    YES manual up                    up
Serial0/1/0                unassigned      YES NVRAM  administratively down down
Serial0/1/1                unassigned      YES NVRAM  administratively down down
Serial0/3/0                unassigned      YES NVRAM  administratively down down
R1#
```

Po zakończeniu konfiguracji wyświetl na routerze tablicę routingu. Aby tego dokonać, wpisz polecenie `show ip route`. Tablica routingu przedstawia w pierwszej części legendę zawierającą symbole wraz z ich rozwinięciem. Następnie na samym końcu znajdują się dwa wiersze.

Spójrz na pierwszy wiersz, zawierający literę `C`, oznaczającą źródło wpisu. Litera `C` oznacza `connected`, czyli wpis pochodzi z sieci bezpośrednio podłączonej. Następnie jest podana podsieć, której 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 podany na końcu identyfikator oznacza interfejs, którym musi zostać przesłany pakiet, aby trafił właśnie do tej podsieci.

```
R1#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, FastEthernet0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/1
R1#
```

Reasumując, pierwszy wpis oznacza, że sieć `192.168.10.0/24` jest bezpośrednio podłączona do routera R1, a prowadzi do niej interfejs `fa0/0`. Jeśli spojrzysz na rysunek 12.1, przekonasz się, że jest to prawda. Ponadto sieć `192.168.20.0/24` również jest podłączona bezpośrednio do routera R1, ale przez interfejs `fa0/1`.

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, ponieważ obie stacje znajdują się w różnych sieciach i różnych domenach rozgłoszeniowych. Stacja robocza H1 ma jednak 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 więc komunikacja.

Ramka trafia do interfejsu routera R1. Router, dekapsulując ramkę, wyłania pakiet i sprawdza w nim, że adresem docelowym jest `192.168.20.10`. Router sprawdza 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 fa0/1, zgodnie z zapisem w tablicy routingu. Oczywiście, pakiet jest ponownie umieszczany w ramce i wysyłany po uprzednim procesie ARP przez interfejs fizyczny. Ramka otrzymuje znakowanie VLAN20 i trafia do stacji roboczej H2.

Po zakończonej konfiguracji routera i przełączników możesz wykonać testowy ping ze stacji H1 do stacji H2. Jak widzisz w poniższym listingu, stacja H2 odpowiada pomyślnie.

```
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>
```

Ponadto na stacji roboczej H1 wydaj polecenie tracert [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.

```
H1>tracert 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>
```

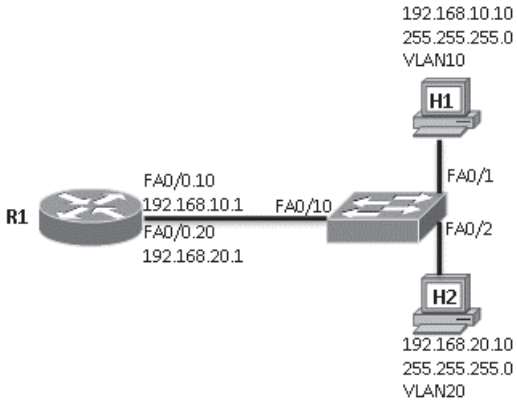
Podsumujmy metodę klasyczną. Jak zauważyłeś, w przypadku dwóch sieci VLAN właściwie nie ma problemu, aby taką metodę wprowadzić do sieci. Jednak każda kolejna sieć VLAN wymaga odrębnego interfejsu na routerze oraz przełączniku. W przypadku 20 sieci VLAN ciężko będzie w ten sposób zrealizować routing pomiędzy sieciami VLAN.

Router-on-a-stick

Metoda *router-on-a-stick* przypomina metodę klasyczną, jednak tutaj do komunikacji przełącznika z routerem wykorzystany jest jeden przewód. Dzięki temu rozwiązuje się problem z dużą liczbą potrzebnych interfejsów w przypadku zastosowania wielu sieci VLAN. Pojawia się za to inny, który w przypadku dużego ruchu, niestety, będzie nie do ominięcia. W żargonie to zjawisko nazywa się *bottleneck* (wąskie gardło). Jak można się spodziewać, duża ilość ruchu sieciowego przesyłanego przez stacje robocze spowoduje dość duże obciążenie interfejsu; jest to bez wątpienia duży minus tej metody. Jednak w niewielkich sieciach rozwiązanie *router-on-a-stick* jest bardzo dobrym podejściem do tematu, szczególnie jeśli firma posiada tylko przełączniki warstwy drugiej.

Na poniższym rysunku (rysunek 12.2) jest sieć komputerowa, w której połączenie pomiędzy routerem a przełącznikiem realizowane jest za pomocą jednego przewodu. Przejdźmy więc do konfiguracji i szczegółowego omówienia działania tej metody.

Rysunek 12.2.
Metoda router-on-a-stick



Tym razem konfigurację rozpocznijmy od routera R1. Poleceniem `show ip interface brief` wyświetl listę wszystkich interfejsów. Zauważ, że interfejs `fa0/0`, do którego podpięty jest przełącznik, jest uruchomiony, ale nie ma adresu IP. Jest to wbrew pozorom poprawne. Gdyby interfejs posiadał adres IP, należy go wcześniej usunąć poleceniem `no ip address`.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES manual up                    up
FastEthernet0/1            unassigned      YES manual up                    down
Serial0/1/0                unassigned      YES NVRAM  administratively down down
Serial0/1/1                unassigned      YES NVRAM  administratively down down
Serial0/3/0                unassigned      YES NVRAM  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 bazie identyfikatora interfejsu fizycznego tworzy się podinterfejs dla każdej sieci VLAN.

Aby utworzy podinterfejs, 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 praktyka jest zalecana, ponadto dzięki niej łatwo zachować porządek.

Jeśli więc mamy sieć `VLAN10`, komenda tworząca podinterfejs będzie wyglądała następująco: `interface fa0/0.10`. Po utworzeniu podinterfejsu znajdziesz się w trybie jego konfiguracji. Zanim przypiszesz do niego adres IP, konieczne jest wskazanie enkapsulacji oraz podanie identyfikatora sieci VLAN. Uczyń to poleceniem `encapsulation dot1q [identyfikator_sieci_vlan]`. Dopiero po tej czynności możesz przypisać dowolny

adres IP. Podanie enkapsulacji jest ważne, bowiem interfejs routera dzięki temu wie, jak obsłużyć znakowane ramki, które będą do niego wysyłane. Ponadto musi wiedzieć, jak znakować ramki, które on sam będzie wysyłał do sieci.

Pamiętaj, że adres ten będzie adresem domyślnej bramy dla wszystkich stacji roboczych z tej podsieci i znajdujących się w tej sieci VLAN. Przypisanie adresu IP odbywa się poleceniem, które już znasz: `ip address [adres_ip] [maska_podsieci]`. Poniższy listing przedstawia konfigurację obydwu podinterfejsów dla sieci `VLAN10` i `VLAN20`.

```
R1(config)#int fa0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-subif)#
R1(config)#int fa0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-subif)#
```

Poleceniem `show ip interface brief` jeszcze raz wyświetl listę interfejsów. Pojawiły się na niej dwa dodatkowe podinterfejsy posiadające adres IP. Interfejs fizyczny `fa0/0` nie ma adresu.

```
R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES manual up                    up
FastEthernet0/0.10         192.168.10.1    YES manual up                    up
FastEthernet0/0.20         192.168.20.1    YES manual up                    up
FastEthernet0/1            unassigned      YES manual up                    down
Serial0/1/0                unassigned      YES NVRAM  administratively down down
Serial0/1/1                unassigned      YES NVRAM  administratively down down
Serial0/3/0                unassigned      YES NVRAM  administratively down down
R1#
```

W kolejnym kroku przejdź do konfiguracji przełącznika. Zakładam, że sieci VLAN są już utworzone oraz przypisane są do nich interfejsy, do których podpięte są stacje robocze. Dlatego interfejs `fa0/10` należy jedynie ustawić do pracy jako `trunk` poleceniem `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.

```
S1(config)#int fa0/10
S1(config-if)#switchport mode trunk
S1(config-if)#
*Mar  1 01:40:33.011: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/10, changed state to down
*Mar  1 01:40:36.023: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/10, changed state to up
S1(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 są dostępne.

```
R1#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, FastEthernet0/0.10
C    192.168.20.0/24 is directly connected, FastEthernet0/0.20
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* wysłane ze stacji roboczej ramki 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 więc prawidłowo je 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 `fa0/0.10` 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 trzeciej

Przełączanie w warstwie trzeciej prezentuje nieco inne podejście. W warstwie 2. odbywało się wyłącznie na podstawie adresów MAC. Wszystkie inne czynności dostosowywane były właśnie do tych identyfikatorów. W warstwie 3. przełączanie odbywa się na podstawie adresów IP, czyli warstwy 3. Ze względu na to, że praca odbywa się w warstwie 3., przełączniki mają również wiele innych funkcjonalności, jakie posiadają routery. Mogą więc z powodzeniem przejmować część ruchu sieciowego na siebie, bez angażowania routerów.

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

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

Samo przełączanie wykorzystuje dwie funkcjonalności: *Forwarding Information Base* (FIB) oraz *adjacency table* (tablica przylegania).

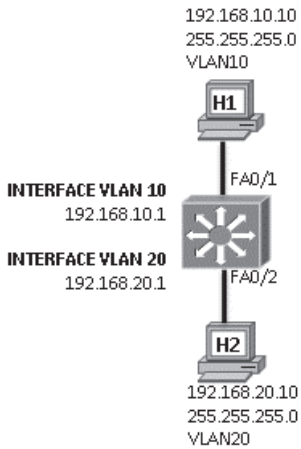
`FIB` jest czymś w rodzaju tablicy używanej do przesłania pakietu w inne miejsce w sieci. Przypomina swoim działaniem tablicę routingu, na podstawie której routery podejmują decyzję o przesłaniu pakietu do innej podsieci. Tablica `FIB` zawiera więc co najmniej adres podsieci oraz interfejs, który osiąga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

Adjacency table zawiera wpisy dotyczące adresów warstwy drugiej, wykorzystywane m.in. na użytek `FIB` i będące pomocą do przesłania informacji dalej.

Przełączniki warstwy 3. wyglądają identycznie jak ich młodsi koledzy z warstwy 2. Posiadają fizyczne interfejsy, których liczba zależy od zakupionego modelu przełącznika. Do celów przełączania w warstwie trzeciej mają możliwość skonfigurowania interfejsów SVI (ang. *Switch Virtual Interface*). Jest to wirtualny interfejs, który umożliwia komunikację pomiędzy sieciami VLAN.

Kolejna z metod komunikacji pomiędzy sieciami VLAN oparta jest więc na przełącznikach warstwy trzeciej. Spójrz na poniższy rysunek (rysunek 12.3), na którym widzisz tylko przełącznik, już bez udziału routera.

Rysunek 12.3. *Komunikacja pomiędzy sieciami VLAN z wykorzystaniem przełącznika L3*



Najpierw musisz na przełączniku warstwy trzeciej uruchomić funkcjonalność routingu. W trybie konfiguracji globalnej wydaj 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]`.

Następnie 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`. Znajdują się w niej 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 trzeciej jest najszybsze i najbardziej optymalne. Nie generuje dodatkowego ruchu, odciąża routery, jest proste w konfiguracji i umożliwia dowolne kierowanie ruchu za pomocą ACL, o których będziesz mógł jeszcze przeczytać. Oczywiście, przełączniki L3 są rozwiązaniem droższym.

Skorowidz

A

B

C

D

E

F

G

H

I

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ż

Sieci komputerowe dawno już oplotły cały świat. Nawet w cieniu peruwiańskiej dżungli można znaleźć kafejkę internetową, nie mówiąc o bardziej cywilizowanych okolicach. Każda firma potrzebuje swojej własnej sieci, dostosowanej do jej potrzeb. Twoja nie jest wyjątkiem. Teraz masz szansę nauczyć się samodzielnie budować wyspecjalizowane sieci komputerowe i zarządzać nimi tak, jak uznasz za stosowne. Z tą książką poznasz wszystkie niezbędne elementy sieci i zorientujesz się, jak najsensowniej ich używać. A potem, jeśli będziesz chciał, będziesz mógł przystąpić do egzaminu CCNA i zostać profesjonalnym „pająkiem"!

Materiał zawarty w książce Adama Józefioka jest ułożony w taki sposób, by krok po kroku wprowadzić Cię w świat sieci komputerowych. Znajdziesz tu informacje o modelach sieci, konfiguracji podstawowych urządzeń Cisco i programach niezbędnych do posługiwania się sieciami. Odkryjesz, czym różnią się od siebie poszczególne typy sieci i technologie przesyłania danych, zrozumiesz zasady działania routingu statycznego i dynamicznego, nauczysz się obsługiwać protokoły sieciowe. A potem wykorzystasz te wiadomości w serii praktycznych ćwiczeń — i będziesz gotowy sprostać wyzwaniom każdej sieci!

- Modele sieci, Ethernet, program Wireshark i emulator GNS3
- Wprowadzenie do systemu operacyjnego iOS i konfiguracja urządzeń Cisco
- Adresacja IPv4 oraz IPv6
- Przełączniki sieciowe oraz sieci VLAN
- Protokół STP i jego następcy
- Wprowadzenie do routerów Cisco
- Routing pomiędzy sieciami VLAN, statyczny i dynamiczny
- Listy ACL, Network Address Translation (NAT) oraz DHCP
- Redundancja w sieci i wykorzystanie nadmiarowości
- Technologie sieci WAN oraz sieci VPN
- Słownik pojęć z wyjaśnieniami

Odkryj fascynujące tajemnice sieci komputerowych!

Helion

Partner wydania
WSTI Wyższa Szkoła Technologii Informatycznych w Katowicach

25531 numer katalogowy
księgarnia internetowa
http://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900

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

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

ISBN 978-83-246-9101-2
9 788324 691012

Informatyka w najlepszym wydaniu
cena: 99,00 zł