

Adam Józefiok



CCNA 200-125

Zostań administratorem sieci komputerowych **Cisco**



Helion 

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Copyright © Helion 2017

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Wprowadzenie	13
Rozdział 1. Kilka słów wstępu	15
Firma Cisco	15
Certyfikacja i egzamin	16
CCNA — tematyka i materiał	18
Sprzęt do nauki	21
Dokumenty RFC	22
Rozdział 2. Informacje wstępne o sieciach komputerowych	25
Podstawy sieci komputerowych	25
Reguły działania sieci (komunikacja)	26
Proces komunikacji i wykorzystanie protokołów sieciowych	28
Przesyłanie danych w sieci	29
Pojęcie protokołu sieciowego	31
Liczby w sieciach komputerowych	32
Organizacje standaryzujące	34
Rodzaje sieci komputerowych	35
Model pracy klient-serwer	35
Sieć bezprzewodowa	35
Sieć SAN	36
Sieci lokalne i sieci rozległe	36
Sieć internet	38
Urządzenia sieciowe	39
Okablowanie sieci przedsiębiorstwa	45
Typowa sieć komputerowa w domu (telewizja kablowa, DSL)	49
Media transmisyjne (miedziane, światłowodowe, bezprzewodowe)	50
Projektowanie sieci	64
Rozdział 3. Modele sieci i pojęcie sieci Ethernet	71
Model TCP/IP	71
Warstwa aplikacji	72
Warstwa transportu	73
Warstwa internetowa	73
Warstwa dostępu do sieci	73
Model OSI	74
Warstwa aplikacji	74
Warstwa prezentacji	75
Warstwa sesji	76

Warstwa transportu	76
Warstwa sieci	80
Warstwa łącza danych	89
Warstwa fizyczna	92
Podstawy sieci Ethernet	94
CSMA/CD	94
Adresowanie w Ethernetcie	96
Protokół ARP	97
Dodanie wpisu statycznego ARP	99
Komunikacja poza domyślną bramę	100
Niebezpieczeństwa związane z ARP	101
Rozdział 4. Zastosowanie programu Wireshark	103
Omówienie najważniejszych funkcji programu Wireshark	104
Działanie komunikacji DNS	108
Rozmiar okna TCP oraz three-way handshake	118
Działanie protokołu ARP	120
Rozdział 5. Emulator GNS3	135
Informacje na temat programu GNS	135
Pobieranie, instalacja i najważniejsze funkcje	137
Ważniejsze funkcje i opcje	139
Obszar roboczy GNS3	157
Połączenie dwóch wirtualnych stacji w programie GNS3	158
Przygotowanie IOS	160
Dodawanie routerów do obszaru roboczego i zmiana ustawień	168
Podłączenie routerów i uruchomienie prostej sieci	172
Konfiguracja programu SuperPuTTY	174
Połączenie z urządzeniem sieciowym	175
Połączenie z urządzeniem wirtualnym	175
Wydanie polecenia wielu urządzeniom naraz	177
Zmiana nazwy zakładki	179
Rozdział 6. Wprowadzenie do systemu operacyjnego IOS i podstawowa konfiguracja urządzeń Cisco	181
Proces uruchamiania urządzenia	181
System operacyjny IOS	183
Podłączenie do urządzenia	184
Zarządzanie urządzeniem	186
Tryby pracy	187
System pomocy	188
Przeglądanie konfiguracji	191
Wstępna konfiguracja routera Cisco wraz z zabezpieczeniami	194
Konfiguracja oraz opis interfejsu	198
Zarządzanie konfiguracją	199
Połączenie wirtualnego routera z siecią rzeczywistą za pomocą obiektu Cloud	203
Zarządzanie systemem IOS	217
Uruchomienie TFTP na routerze	220
Wykorzystanie programu Wireshark w GNS3	222
Rozdział 7. Adresacja IPv4	225
Informacje wstępne o protokole IPv4	225
Pojęcia adresu sieci, adresu hosta i adresu rozgłoszeniowego	226
Ping na adres rozgłoszeniowy sieci	226
Typy adresów (prywatne, publiczne)	227

Binarna reprezentacja adresu IP	229
Zamiana liczb dziesiętnych na binarne	231
Zamiana liczb binarnych na dziesiętne	238
Podział sieci według liczby wymaganych podsieci	243
Podział klasy C	244
Podział klasy B	251
Podział klasy A	256
Podział sieci na podsieci — liczba hostów w każdej sieci	260
Podział klasy C	260
Podział klasy B	264
Podział klasy A	266
Podział sieci na podsieci — nierówna wielkość hostów w każdej podsieci	267
Reverse engineering	277
Rozdział 8. Przełączniki sieciowe — podstawy działania i konfiguracji	281
Model hierarchiczny	281
Przełącznik warstwy drugiej	283
Tablica adresów MAC	286
Podłączanie urządzeń do przełącznika	292
Metody przełączania ramek	293
Podstawowa konfiguracja przełącznika	294
Konfiguracja adresu IP i domyślnej bramy	296
Zmiana parametrów interfejsów i wyłączenie interfejsów nieużywanych	300
Zapisanie konfiguracji	301
Włączenie protokołu SSH	302
Emulowany przełącznik w GNS3	309
Wykorzystanie w GNS3 obiektu Ethernet switch	312
Rozdział 9. Przełączniki sieciowe — Port Security	315
Przygotowanie konfiguracji i informacje wstępne	316
Konfiguracja Port Security	317
Wywołanie zdarzenia bezpieczeństwa	324
Uruchomienie interfejsu po zdarzeniu bezpieczeństwa	325
Funkcja autouruchamiania interfejsu	327
Zmiana adresu MAC karty sieciowej	327
Rozdział 10. Sieci VLAN	331
Działanie sieci VLAN	331
Konfiguracja sieci VLAN	334
Prywatne sieci VLAN	338
Połączenia typu trunk	338
Protokół VTP	342
Ograniczenia VTP	346
Ustalanie hasła i innych parametrów	347
Usuwanie konfiguracji VLAN	349
VTP Pruning	350
Rozdział 11. Protokół STP i jego nowsze wersje	353
Algorytm działania STP	355
Rozszerzenie protokołu STP, czyli protokół PVST	366
Konfiguracja PVST	369
Protokół RSTP	371
Konfiguracja RSTP	372

Rozdział 12. Wprowadzenie do routerów Cisco	377
Działanie routera i jego budowa	377
Budowa routera	380
Wstępna konfiguracja routera	383
Omówienie protokołu CDP	398
Protokół LLDP	401
Własne menu na routerze	401
Rozdział 13. Routing pomiędzy sieciami VLAN	403
Metoda klasyczna	404
Router-on-a-stick	408
Przełączanie w warstwie 3.	412
Rozdział 14. Routing statyczny	417
Wprowadzenie do routingu statycznego	417
Sumaryzacja tras statycznych	421
Default route	424
Najdłuższe dopasowanie	426
Floating Static Route	427
Rozdział 15. Routing dynamiczny i tablice routingu	431
Rodzaje protokołów routingu dynamicznego	432
Wymiana informacji i działanie protokołów	434
Protokoły distance vector	435
Protokoły link state	436
Tablica routingu routera	436
Proces przeszukiwania tablicy routingu	439
Tablica routingu stacji roboczej	447
Rozdział 16. Adresacja IPv6	451
Wstępne informacje na temat protokołu IPv6	451
Zamiana liczb	453
Rozdział 17. Routing dynamiczny — protokół RIP	477
Charakterystyka i działanie protokołu RIPv1	477
Konfiguracja RIPv1	479
Charakterystyka i konfiguracja protokołu RIPv2	485
Konfiguracja RIPv2	486
Podstawy protokołu RIPv2	490
Konfiguracja protokołu RIPv2	490
Rozdział 18. Routing dynamiczny — protokół OSPF	497
Protokół OSPFv2	497
Pakiety hello	498
Konfiguracja protokołu OSPF	502
Zmiana identyfikatora routera	506
Stany interfejsów i relacje sąsiedzkie	509
Wymiana informacji pomiędzy routerami — obserwacja	510
Metryka w OSPF	518
Zmiana czasów	525
Konfiguracja passive-interface	527
Rozgłaszanie tras domyślnych	527
OSPF w sieciach wielodostępowych	528
Wybór routerów DR i BDR	529
Statusy po nawiązaniu relacji sąsiedztwa	535

Uwierzytelnianie w OSPF	538
Wielobszarowy OSPF	541
Typy przesyłanych pakietów LSA	543
Konfiguracja wielobszarowego OSPF	543
Protokół OSPFv3	554
Konfiguracja OSPFv3	554
Rozdział 19. Routing dynamiczny — protokół EIGRP	561
Protokół EIGRPv4	561
Konfiguracja EIGRP	563
Konfiguracja routera stub w EIGRP	589
Protokół EIGRPv6	594
Rozdział 20. Listy ACL	601
Rodzaje list ACL	603
Konfiguracja standardowych list ACL	604
Przykład 1.	604
Przykład 2.	609
Przykład 3.	611
Przykład 4. (lista standardowa nazywana)	614
Konfiguracja rozszerzonych ACL	618
Przykład 5.	618
Przykład 6.	621
Przykład 7.	623
Przykład 8.	625
Przykład 9.	628
Listy ACL w IPv6	629
Przykład 10.	630
Przykład 11.	631
Przykład 12.	632
Przykład 13.	632
Rozdział 21. Network Address Translation (NAT) oraz DHCP	635
Static NAT (translacja statyczna)	636
Dynamic NAT (translacja dynamiczna)	640
PAT — Port Address Translation	641
Konfiguracja routera R1 jako serwera DHCP	643
DHCP Snooping	644
Przykład	650
Konfiguracja routera R1 jako serwera DHCPv6 (SLAAC)	651
Konfiguracja routera jako serwera DHCPv6 (bezstanowego DHCPv6)	653
Konfiguracja routera jako serwera DHCPv6 (połączeniowy DHCPv6)	655
NAT dla IPv6	657
Rozdział 22. Redundancja w sieci i wykorzystanie nadmiarowości	659
Konfiguracja protokołu HSRP	661
Przygotowanie przykładowej sieci w programie GNS3	661
Konfiguracja HSRP	663
Konfiguracja VRRP	673
Konfiguracja GLBP	682
EtherChannel	685
Konfiguracja EtherChannel	687

Rozdział 23. Technologie sieci WAN oraz sieci VPN	691
Sieci WAN — informacje ogólne	691
Technologie sieci WAN	692
Frame Relay	692
ISDN	693
PPP	694
DSL	694
Przykładowy model sieci WAN	696
Konfiguracja enkapsulacji w przykładowym modelu punkt-punkt	696
Technologia Frame Relay	702
Konfiguracja Frame Relay (hub-and-spoke)	705
Konfiguracja multipoint	707
Konfiguracja Frame Relay point-to-point	716
Samodzielna konfiguracja przełącznika Frame Relay	720
Technologia VPN	724
Szyfrowanie w VPN	725
Algorytmy szyfrowania w VPN	726
Zachowanie integralności	729
Uwierzytelnianie	732
Implementacja VPN site-to-site na routerze Cisco za pomocą CLI	735
Tunel GRE w site-to-site	745
Opis działania SSL/TLS	749
Konfiguracja dostępu przez przeglądarkę	750
Konfiguracja dostępu przez klienta VPN	752
Rozdział 24. Protokół routingu BGP — podstawy	755
Informacje wstępne na temat protokołu BGP	755
Nawiązywanie relacji pomiędzy routerami BGP będącymi sąsiadami	757
Nawiązywanie relacji pomiędzy routerami BGP niebędącymi bezpośrednimi sąsiadami	759
Przeglądanie tablic routingu i wymiana informacji o sieciach	761
Rozdział 25. Logowanie zdarzeń, raportowanie, zarządzanie bezpieczeństwem sieci za pomocą 802.1x oraz QoS	765
Rozwiązywanie problemów z działaniem sieci	765
Wprowadzenie	766
Rozwiązywanie problemów z interfejsami	768
Narzędzie debugowania	769
Sprawdzanie komunikacji	771
Odwzorowanie nazw	774
Testowanie łącza z siecią internet	775
Testowanie połączenia w sieci lokalnej za pomocą narzędzia iperf	776
Logowanie zdarzeń i raportowanie	778
Obsługa logów systemowych syslog	779
Wykorzystanie SNMP	783
Wykorzystanie i działanie NetFlow	795
Konfiguracja funkcjonalności span port	801
Użycie uwierzytelniania 802.1x dla stacji roboczej	804
Konfiguracja 802.1x	805
Quality of Service — QoS	810
Rodzaje kolejkowania	810
Usługi chmury	812

Rozdział 26. Obsługa Cisco Configuration Professional	815
Program Cisco Configuration Professional CCP	815
Instalacja programu CCP	816
Uruchomienie CCP Express na routerze w GNS3	816
Konfiguracja CCP na stacji roboczej i podłączenie do routera uruchomionego w programie GNS3	819
Rozdział 27. Ćwiczenia praktyczne	833
Rozdział 28. Słownik pojęć z wyjaśnieniami	875
Zakończenie	903
Literatura	905
Skorowidz	907

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.

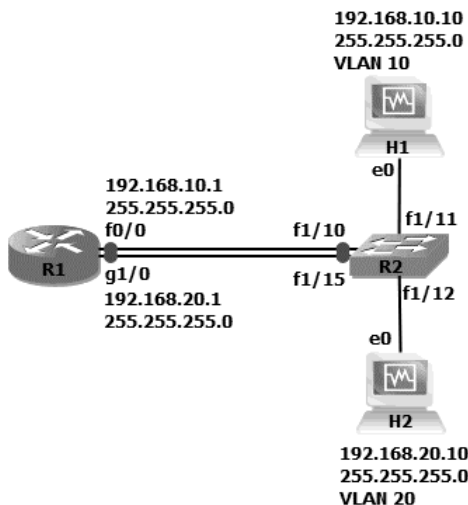
Każdą metodę postaram się wyjaśnić na podstawie projektów, które możesz wykonać samodzielnie w programie GNS3. Będzie Ci do tego potrzebny router Cisco 3745, o którym wspominałem we wcześniejszych rozdziałach.

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 przetestować 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, I - 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, dekapując ramkę, wyłania pakiet i sprawdza w nim, że adresem docelowym jest 192.168.10. 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 błędzenia 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>
```

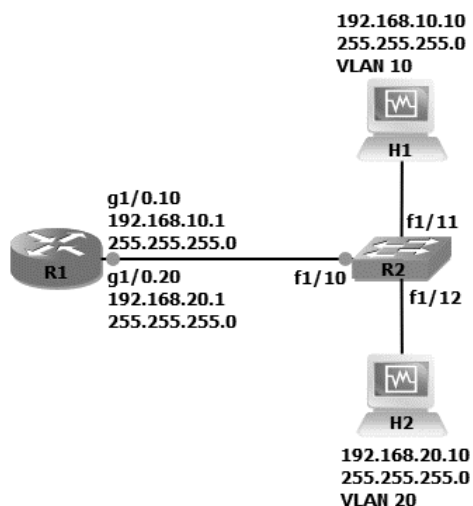
Pora na podsumowanie informacji dotyczących metody klasycznej. Jak zauważyłeś, w przypadku dwóch sieci VLAN właściwie nie ma przeszkód, aby zastosować tę metodę. Jednak każda kolejna sieć VLAN wymaga odrębnego interfejsu na routerze i przełączniku. Oznacza to, że przy 20 sieciach VLAN trudno będzie w 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` wyświetli 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 (*subinterfejsy*). 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]`.



Wskazówka

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. Uczyni 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 wyświetli 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 błędzenia 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:
  0  0 ms    0 ms    0 ms    192.168.10.1
  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 młodszy 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.

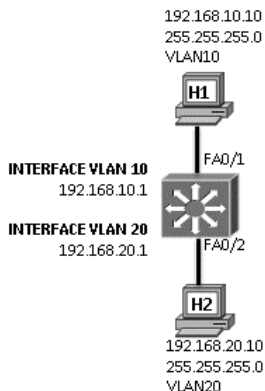
Opisywana metoda komunikowania się sieci VLAN między sobą oparta jest więc na przełącznikach warstwy 3. Na poniższym rysunku 13.3 pokazano tylko przełącznik; nie ma tu już natomiast routera.

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

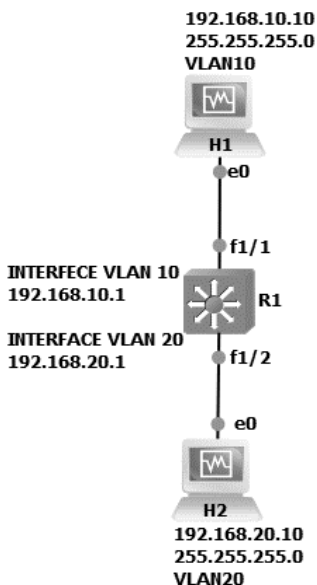
C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
S1#
```

Bez wątpienia rozwiązanie oparte na przełącznikach warstwy 3. jest optymalne. Nie generuje dodatkowego ruchu, obciąża 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 przetestować w GNS3, możesz to uczynić, wykorzystując router 3745 z modulem 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 zmieniła 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 przeciwiczyć 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

3CDaemon, 211, 780

A

access attack, *Patrz:* atak dostępu

Access Control List, *Patrz:* ACL

access point, *Patrz:* punkt dostępu

achieving convergence, *Patrz:* sieć komputerowa zbieżność

ACL, 66, 601, 641, 650

IPv6, 629, 630, 631, 632

kierunek działania, 606

komentarz, 608

konfiguracja, 602, 603, 604,

605, 607, 609, 611, 614,

618, 619, 621, 623, 626,

628

deny, 601, 607, 621

permit, 601, 603

numer, 603, 605

rodzaj, 603, 604

rozszerzona, 603

konfiguracja, 618, 619,

621, 626, 628

nazywana, 623, 625, 626

standardowa, 603, 616

edytowanie, 612, 613

konfiguracja, 604, 605,

606, 607, 609, 611, 614

nazywana, 614

usuwanie, 612

adjacency table, *Patrz:* tablica przylegania

Administrative Distance, *Patrz:* dystans administracyjny

adres

IP, 27, 38, 82, 105, 109, 112, 644

docelowy, 115, 123

nadawcy, 73, 78, 80

odbiorcy, 73, 78, 80

reprezentacja binarna,

229, 230

wirtualny, *Patrz:* adres VIP

źródłowy, 115

IPv4, 82, 116, 453

prywatny, 83, 84, 227,

228, 635

przypisanie

automatyczne, 87

przypisanie ręczne, 86

publiczny, 227, 228, 640

zarezerwowany, 84

IPv6, 453, 454, 456, 469,

635, 656

global, 455

link-local, 456

loopback, 455

multicast, 455, 460

skracanie, 455

unspecified, 455

lokalnego łącza, 229

MAC, 40, 89, 96, 115, 315

broadcast, 97

docelowy, 97, 123, 378

DYNAMIC, 321

falszywy, 101

karta sieciowa, 327

multicast, 97

najniższy, 358

sprawdzenie, 41

STATIC, 321, 322

wirtualny, 660, 665, 682

zapis, 96

pętli zwrotnej, 229

rozgłoszeniowy sieci, 226,

230, 645, 648

sieci, 226, 232

readresacja, 232

wyznaczanie, 230

Temporary IPv6, 463

translacja, *Patrz:* translacja,

NAT

unicastowy, 648

URL, 72, 109

VIP, 660, 661, 663

algorytm

3DES, 727, 728

AES, 727, 728, 737

algorytm

DES, 727

DH, 734

DSA, 732

DUAL, 561

ECDSA, 732

hashujący, 729, 730

HMAC, 731

IDEA, 727, 728

MD5, 539, 729, 737

RC, 727, 728

RSA, 732

SHA, 729, 737

SPF, 497, 500

STA Spanning-Tree

Algorithm, 355, 357

ANSI, 34

application layer,

Patrz: warstwa aplikacji

Area ID, *Patrz:* obszar identyfikator

- ARP, 462
 inverse, 710
 poisoning, 101
 spoofing, 101
 wpis statyczny, 99
- atak, 67
 ARP spoofing, 101
 brute force, 728
 DDoS, 69
 DHCP Consumption Attack, 645
 DoS, 66, 69
 dostępu, 69
 buffer overflow attack, 69
 man-in-the-middle attack, 69
 passwords attack, 69
 ping of death, 70
 smurf attack, 70
 trust exploitation attack, 70
 hasło, 69
 man-in-the-middle, 69, 668, 731
 rekoniesans, *Patrz:*
 rekoniesans
 wewnętrzny, 66, 67
 zewnętrzny, 66, 67
- ATM, 695
 ATP, 692
 attenuation, *Patrz:* tłumienie
 authenticator, 804
 Autonomus System AS, *Patrz:*
 system autonomiczny
 availability, *Patrz:* dostępność
- B**
- backbone area, *Patrz:* obszar zerowy
 bajt, 33, 34
 band, *Patrz:* pasmo
 bandwidth, *Patrz:* przepustowość
 banner motd, 198
 bencka, *Patrz:* kabel koncentryczny
 bezpieczeństwo, 66, 67, 315, 483, 497, 601, 779, 804
 atak, *Patrz:* atak certyfikat, 749, 750, 752
 specjalizacja, 67
 zarządzanie, 67
 złamanie zasad, 324, 325
- bezprzewodowe, *Patrz też:* sieć komputerowa bezprzewodowa
 bit, 33, 34, 93
 bluetooth, 63
 błąd pola metryki, 436
 brama domyślna, 82, 85, 100, 115, 122
 adres, 468
 broadcast, *Patrz:* adres rozgłoszeniowy sieci
 broadcast domain, *Patrz:* domena rozgłoszeniowa
 broadcast multiaccess, *Patrz:* sieć komputerowa wielodostępowa
 broadcast storm, *Patrz:* burza rozgłoszeniowa
 bufor
 przepełnienie, 69
 wewnętrzny, 782, 783
 building backbone cabling, *Patrz:* sieć komputerowa okablowanie szkieletowe
 burza rozgłoszeniowa, 354
 bus topology, *Patrz:* sieć komputerowa topologia magistrali
 BYOD, 45
 byte, *Patrz:* bajt
- C**
- CAT-OS, 184
 CBWFQ, 812
 CCP, 815
 instalacja, 820
 konfiguracja, 820
 interfejsu, 822
 routingu statycznego, 823
 router
 konfiguracja, 822, 823, 829
 monitorowanie, 828
 zabezpieczenie, 825
 CCP Express, 816
 instalacja, 816
 konfiguracja, 818
 certyfikat
 CCENT, 16
 CCIE, 18
 CCNA, 16, 18
 CCNA R&S, 16
 CCNAX, 16
- chmura, 812
 CIR, 703
 circuit switched, *Patrz:* przełączanie obwodów
 Cisco Configuration Professional, *Patrz:* CCP
 Cisco Express Forwarding, 380, 412
 Cisco Networking Academy, 15
 cloud, *Patrz:* chmura
 coaxial cable, *Patrz:* kabel koncentryczny
 cold start, 434
 Committed Information Rate, *Patrz:* CIR
 confidentiality, *Patrz:* dane zapewnienie poufności
 congestion, *Patrz:* przeciążenie
 convergence, *Patrz:* sieć komputerowa osiągnięcie zbieżności
 CP Express, 815
 Cpulimit, 138
 CSMA/CA, 95
 CSMA/CD, 94, 95
- D**
- dane
 integralność, 67, 726, 729
 kompresja, 75
 multipleksowanie, 77
 nieznakowane, 339
 przesyłanie, 73
 segment, *Patrz:* segment szyfrowanie, *Patrz:* szyfrowanie
 VoIP, 811
 wideo, 812
 zapewnienie poufności, 67, 726, 727
 Data Link Connection Identifier, *Patrz:* DLCI
 dead interval, 500
 debugowanie, 769
 komunikat, 769, 770, 779
 protokołu ICMP, 769
 wyłączanie, 770
 decoding, *Patrz:* odkodowanie
 default route, *Patrz:* trasa domyślna
 dekapsulacja, 94
 delay, *Patrz:* opóźnienie

DHCP Snooping, 644, 646, 647
 dioda LED, *Patrz:* LED
 DLCI, 693, 703, 706
 DMVPN, 725
 domena
 kolizja, *Patrz:* kolizja
 domena
 rozwłoszeniowa, 27, 95, 100, 364
 ograniczenie, 27
 dostępność, 29, 31, 67
 drother, 501, 533
 drzewo SPF, 500
 DSL, 38, 694
 Dynamips, 136
 dystans administracyjny, 427, 497

E

egzamin certyfikujący, 16, 17
 koszt, 18
 pytania, 19, 20
 EIR, 693
 emulator GNS3, *Patrz:* GNS3
 encoding, *Patrz:* kodowanie
 enkapsulacja, 96, 339, 340, 696
 HDLC, 693, 697
 PPP, 693, 697, 699, 700
 established ACL, 604
 EtherChannel, 686, 687, 688, 689
 Ethernet, 40, 58, 94, 123, 388
 adresowanie, 96
 ramka, 90, 91
 Excess Information Rate, 693
 extended ACL, *Patrz:* ACL
 rozszerzona
 extended star topology, *Patrz:*
 sieć komputerowa topologia
 rozszerzonej gwiazdy
 external threat, *Patrz:* atak
 zewnętrzny
 extranet, 37

F

FastEthernet, 58
 firewall, 66
 fluktuacje, 811
 Forwarding Information Base,
 Patrz: tablica FIB
 frame, *Patrz:* ramka

Frame Relay, 692, 696, 702, 703
 chmura, 702
 CIR, *Patrz:* CIR
 EIR, *Patrz:* EIR
 hub-and-spoke, 705, 716, 720
 konfiguracja, 709, 710, 712, 713
 mapa, 711
 multipoint, 705, 707
 point-to-point, 705, 716, 720
 stały obwód wirtualny,
 Patrz: PVC

G

gniazdo
 abonenckie, 46, 47
 RJ-45, 46, 56
 GNS3, 123, 135, 136, 161, 222, 396, 405
 działanie, 139
 emulowane urządzenia, 136
 instalacja, 137
 interfejs, 136
 konfiguracja, 139, 140, 141, 155
 GNS3
 łączenie wirtualnych stacji, 158
 obszar roboczy, 157, 158
 pobieranie, 137
 Google DNS, 83
 Graphical Network Simulator,
 Patrz: GNS3
 GRE, 745, 746

H

haker, 67
 hasło, 69
 horizontal cabling, *Patrz:* sieć
 komputerowa okablowanie
 poziome
 horyzont podzielony, 436
 hub, *Patrz:* koncentrator

I

IaaS, 813
 IEEE, 34
 IETF, 22, 34

Infrastructure as a Service,
 Patrz: IaaS
 integralność, *Patrz:* dane
 integralność
 integrity, *Patrz:* dane
 integralność
 interfejs, 72
 autouruchamianie, 327
 Frame Relay, 721
 inside, 637
 konfiguracja, 316, 317, 318, 319, 320, 321
 loopback, 207, 421, 465, 499, 577
 monitorowanie, 768, 802, 803
 outside, 637
 pasywny, 583
 przechwytywania, 106
 przeciwstawny, 61
 span port, 802, 803
 SVI, 412
 tryb duplex, 96, 768
 uruchamianie, 325, 326, 327
 wewnętrzny, *Patrz:* interfejs
 inside
 wirtualny, 421
 zewnętrzny, *Patrz:* interfejs
 outside
 internal threat, *Patrz:* atak
 wewnętrzny
 internet, 38, 44, 73
 dostawca, *Patrz:* ISP
 dostęp, 38
 usługa, 44
 wielkość, 44
 internet layer, *Patrz:* warstwa
 internetowa
 Internetwork Operating System,
 Patrz: IOS
 intranet, 37
 Intrusion Prevention Systems,
 Patrz: IPS
 IOS, 161, 164, 182, 184
 kopiowanie do routera, 213, 214, 215
 kopiowanie do serwera, 211, 215
 obraz, 163
 polecenie niepoprawne, 190, 191
 system pomocy, 188, 189, 190
 wersja, 217, 218, 219

- iperf, 777
 IPS, 66
 IPv4, *Patrz:* protokół IPv4
 IPv6, *Patrz:* protokół IPv6
 IRDA, 63
 ISDN, 692, 693
 ISDN BRI, 693
 ISDN PRI, 693
 ISO, 34
 ISOC, 34
 ISP, 50
- J**
- jitter, 811
- K**
- kabel
 crossover, 57
 koncentryczny, 53, 59
 krosowniczy, 49
 rollover, *Patrz:* kabel odwrócony
 sieciowy, 46
 światłowodowy, *Patrz:* światłowód, medium transmisyjne kabel światłowodowy, technologia światłowodowa
 z przeplotem, *Patrz:* kabel crossover
- KALI LINUX, 645
- karta
 NIC, *Patrz:* karta sieciowa rozszerzeń, 734
 sieciowa, 29, 39, 56, 57
 adres, 40, 41
 bezprzewodowa, 39, 64
 producent, 41, 42
 światłowodowa, 46
 wirtualna, 152, 153
 zmiana adresu MAC, 327
 WIC, 696
 Wi-Fi, *Patrz:* karta sieciowa bezprzewodowa
- klient
 AnyConnect, 752
 FTP, 72, 75
 pocztowy, 32
 RADIUS, 804
 syslog, 780
 VPN, 725, 752
- klucz
 asymetryczny, 729
 negocjacja, 734
 prywatny, 732
 publiczny, 750
 sesji, 750
 tajny, 733, 737
 kodowanie, 28, 52
 kolejowanie, 812
 kolizja, 94, 95, 96
 komentarz ACL, 608
 komunikacja, 26
 broadcast, 26, 27, 353
 burza rozgłoszeniowa, 354
 grupowa, *Patrz:* komunikacja multicast
 jednostkowa, *Patrz:* komunikacja unicast
 multicast, 26, 27
 rozgłoszeniowa, *Patrz:* komunikacja broadcast
 unicast, 26
 urządzeń redundantnych, 660
 w sieci VLAN, 403
 bottleneck, 408
 router, 404, 406
 router-on-a-stick, 408
 wąskie gardło, 408
 wąskie gardło, 408, 811
- komunikat, 394
 ACK, 118
 DHCP ACK, 645
 DHCP Discover, 644, 645, 647
 DHCP Offer, 645
 ICMP packet debugging is on, 769
 poziom, 779
 przesyłanie, 781, 782
 RA, 468, 469, 652
 Router Advertisement, *Patrz:* komunikat RA
 Routing Protocol, 504
 SYN, 118
 SYN-ACK, 118
- koncentrator, 43, 94, 281
 VPN, 733
- koń trojański, 66, 68
 kradzież tożsamości, 66
- L**
- LAG, 687
 LAR, 703
- laser, 60, 61
 leased line, *Patrz:* linia dzierżawiona
 LED, 60, 61
 level 1 parent route, *Patrz:* trasa nadrzędna pierwszego poziomu
 level 1 route, *Patrz:* trasa pierwszego poziomu
 level 2 child route, *Patrz:* trasa podrzędna drugiego poziomu
 liczba
 binarna, 229, 453, 454
 obliczanie, 231, 235
 parzystość, 243
 zamiana na dziesiętne, 238, 240
 szesnastkowa, 41, 96, 453, 454
- licznik wstrzymania, 436
- linia
 dzierżawiona, 691, 693, 702
 stale podłączona, 693
- link state database, *Patrz:* LSDB
 LLQ, 812
 LMI, 703
 Local Access Rate, *Patrz:* LAR
 Local Area Network, *Patrz:* sieć komputerowa LAN
 Local Management Interface, *Patrz:* LMI
 log systemowy, 779
 loopback, *Patrz:* pętla zwrotna
 LSDB, 498, 514, 541
 Lucent Connector, *Patrz:* złącze LC
- M**
- maska podsieci, 82, 83, 84
 długość, 434
 stała, 228
 zmienna, 228, 478
- IPv4, 452, 453
 IPv6, 452, 453
 odwrotna, 502, 503
 zsumaryzowanej, 422, 423, 473
- maszyna wirtualna, 138
 dysk twardy, 144
 dysk USB, 153
 karta sieciowa, 152, 153
 łączenie, 158
 pamięć RAM, 150

tworzenie, 142, 144, 147
 uruchamianie, 147
 ustawienia, 149, 151, 152, 153, 154
 Maximum Transmission Unit, *Patrz:* MTU
 medium transmisyjne, 26, 28, 29, 31
 bezprzewodowe, 50, 63
 kabel
 miedziany, 50, 51, 52, 53, *Patrz też:* sieć komputerowa
 okablowanie miedziane, skrętka
 światłowodowy, 50, *Patrz też:* światłowód, technologia światłowodowa
 metoda
 dynamiczne dostosowanie okien, 119
 wstrzymywania potwierżeń, 119
 Microsoft Hyper-V, 142
 model
 AAA, 806
 DoD TCP/IP, 71
 model
 OSI, 71, 74
 TCP/IP, 71, 72, 73
 warstwa, 72, *Patrz też:* warstwa
 modem, 695
 monitoring, 766, 768, 769, 771, 773, 775, 776, 779, 780, 782, 783, 790, 793, 795, 801, 802
 OOB, 779
 in-band, 779
 out-of-band, 779
 most główny, 357, 360, 686
 wybór, 357, 358
 zmiana, 369, 371
 MPLS, 692
 MTU, 81
 multimode fiber, *Patrz:* światłowód wielomodowy

N

nadmiarowość, 353
 NAT, 635, 650
 dynamic, *Patrz:* translacja dynamiczna

IPv6, 657
 konfiguracja, 637
 overloaded, *Patrz:* PAT static, *Patrz:* translacja statyczna
 natowanie, 228, 642
 nazwa DNS, 105, 106, 109, 115
 neighbor table, *Patrz:* tablica sąsiadów
 NetFlow, 795, 796
 network access layer, *Patrz:* warstwa dostępu do sieci
 Network Address Translation, *Patrz:* NAT
 network diameter,
Patrz: średnica sieci
 Nmap, 69
 noise, *Patrz:* szum
 Npcap, 138
 NX-OS, 184

O

obszar, 499, 541
 identyfikator, 499, 503
 konfiguracja, 499, 500
 zerowy, 556
 obwód, 693
 przełączanie, *Patrz:* przełączanie obwodów
 PVC, 693
 SVC, 693
 odkodowanie, 28
 opóźnienie, 29, 30, 432, 811
 oprogramowanie
 antywirusowe, 66
 fałszywe, 66
 jako usługa, *Patrz:* SaaS
 snifujące, 69, 138, 801
 organizacja standaryzująca, 34

P

PaaS, 813
 packet switched, *Patrz:* przełączanie pakietów
 pakiet, 73, 89, 378
 database description, 498
 DBD, 498
 długość, 511
 hello, 578, 579
 hello, 498, 500, 562, 660
 interwał, 500, 525
 ICMP, 70

IP, 225
 Destination IP Address, 226
 header, 225
 Protocol, 225
 Source IP Address, 226
 Time-to-Live, 225
 LSA, 500, 501, 533
 typ, 543
 LSAck, 498
 LSP, 498
 LSR, 498
 LSU, 498
 otrzymanie, 510
 przechwytywanie, 138
 przełączanie, *Patrz:* przełączanie pakietów
 query, 562
 ścieżka, 73
 transport, 81
 typ, 498
 update, 562, 580
 wielkość, 81
 maksymalna, *Patrz:* MTU
 znakowanie, 812
 panel krosowniczy, 47, 48, 49
 pasmo, 29
 PAT, 641
 konfiguracja, 641, 642, 650
 patch cord, *Patrz:* kabel krosowniczy
 patch panel, *Patrz:* panel krosowniczy
 Permanent Virtual Circuit, *Patrz:* PVC
 pętla, 353, 354, 435
 zapobieganie, 436, 561
 hold down timer, 562
 max distance, 561
 route poisoning, 562
 split horizon, 562, 706, 715
 triggered updates, 562
 pętla zwrotna, 229
 physical topology, *Patrz:* sieć komputerowa topologia fizyczna
 Platform as a Service, *Patrz:* PaaS
 podinterfejs, 706
 podsieć, 226, 228
 sumaryczna, 421
 podwarstwa LCP/NCP, 694
 PoE, 21

- poison reverse, 478
- polecenie
 - aaa authentication dot1x
 - default group radius, 806
 - aaa authorization network
 - default group radius, 806
 - aaa new-model, 806
 - abort, 405
 - access-list, 603
 - arp, 98, 99, 100
 - authentication, 737
 - auto-cost reference-
 - bandwidth, 517
 - banner motd, 198
 - błędne, 393
 - channel-group mode, 687
 - clear ip dhcp binding, 648
 - clear ip ospf process, 499
 - copy running-config tftp, 212
 - copy tftp running-config, 213
 - crypto isakmp policy, 736
 - crypto map, 739
 - debug cdp events, 770
 - debug cdp packets, 770
 - debug ip icmp, 769
 - debug ip ospf adj, 552
 - debug ip rip, 487
 - debug ipv6 rip, 495
 - default-information
 - originate, 549
 - deny ip host, 623
 - do show interface, 325, 326
 - duplex, 768
 - enable, 187
 - enable secret, 194, 196
 - encapsulation frame-relay, 721
 - encryption, 737
 - erase startup-config, 201
 - errdisable recovery cause
 - psecure, 327
 - errdisable recovery interval, 327
 - exit, 405
 - extended ping, 771, 772
 - format flash, 405
 - frame-relay map, 711
 - frame-relay switching, 721
 - glbp ip, 682
 - hash, 737
 - hostname, 194, 383
 - interface, 198
 - interface loopback, 421
 - ip access-list, 603
 - ip access-list extended, 626
 - ip access-list standard, 642
 - ip address dhcp, 641
 - ip bandwidth-percent eigrp, 586
 - ip dhcp excluded-address, 643
 - ip dhcp pool, 643
 - ip dhcp snooping, 646
 - ip dhcp snooping limit rate, 647
 - ip domain-lookup, 774
 - ip flow-export destination, 796
 - ip helper-address, 650
 - ip hold-time eigrp, 585
 - ip nat, 637
 - ip nat inside, 637
 - ip nat outside, 637
 - ip ofsp dead-interval, 500
 - ip ospf hello-interval, 500, 525
 - ip ospf priority, 501
 - ip route, 85
 - ipconfig, 82, 85
 - ipconfig /displaydns, 109
 - ipconfig /flushdns, 110
 - ipconfig -all, 327
 - ipv6 address, 464
 - ipv6 dhcp relay destination, 657
 - ipv6 dhcp server, 654, 656
 - ipv6 nd manager-config-flag, 656
 - ipv6 nd other-config-flag, 654
 - ipv6 rip enable, 492
 - ipv6 unicast-routing, 464, 469, 652, 654, 655
 - key chain, 588, 670
 - logging buffered, 782
 - logging console, 782
 - logging host, 781
 - logging source-interface, 781
 - logging synchronous, 383
 - logging synchronous level, 780
 - menu, 401
 - monitor session, 802
 - neighbor, 757, 760
 - netsh interface ipv4 show
 - subinterfaces, 81
 - netstat, 79, 80, 81
 - network, 502, 762
 - no access-list, 621
 - no debug ip icmp, 770
 - no hostname, 194
 - no ip domain, 393
 - no ipv6 nd managed-config-
 - flag, 652
 - no ipv6 nd other-config-flag, 652
 - no shutdown, 199, 325
 - nslookup, 774
 - ntp server, 392
 - passive-interface default, 526
 - permit tcp, 626
 - ping, 69, 70, 97, 100, 112, 116, 226, 475, 771
 - router-id, 499, 507
 - send, 394
 - serwer, 113
 - sh ipv6 route, 465
 - show cdp entry, 399
 - show cdp neighbors, 398
 - show controllers, 698
 - show crypto ipsec sa, 740, 743
 - show crypto isakmp, 740
 - show crypto isakmp peers, 741
 - show crypto isakmp policy, 737
 - show etherchannel summary, 688, 689
 - show frame-relay map, 711
 - show glbp brief, 684
 - show interface, 768
 - show ip bgp, 761
 - show ip bgp summary, 758, 760
 - show ip dhcp conflict, 650
 - show ip dhcp snooping, 647
 - show ip eigrp interface
 - detail, 585
 - show ip eigrp neighbor, 565
 - show ip eigrp topology, 565, 571, 590
 - show ip eigrp topology
 - all-links, 574
 - show ip flow export, 797
 - show ip interface, 608
 - show ip interface brief, 688
 - show ip nat translations, 642
 - show ip ospf database, 514
 - show ip ospf interface brief, 515, 550

- show ip ospf neighbor, 509, 534, 545
- show ip protocols, 551
- show ip route, 437, 761
- show ip route eigrp, 567
- show ip ssh, 395
- show ipv6 dhcp binding, 656
- show ipv6 dhcp pool, 654
- show ipv6 int brief, 465
- show ipv6 interface, 466
- show ipv6 protocols, 491
- show ipv6 rip database, 495
- show ipv6 route, 470, 491
- show ipv6 route rip, 493
- show port security, 320
- show port-security, 316, 320
- show process, 795
- show runn, 492
- show running-config, 193, 195
- show spanning-tree, 355, 357, 359, 363, 686
- show standby, 665
- show users, 393
- show version, 191
- show vlan, 334
- show vlan brief, 335, 336, 405
- show vlan-switch, 405
- show vtp status, 343
- shutdown, 325
- snmp-server community, 785
- snmp-server contact, 786
- snmp-server enable traps, 786
- snmp-server group, 788
- snmp-server host, 786
- snmp-server location, 786
- snmp-server user, 789
- ssh, 395
- switchport access vlan, 336
- switchport mode access, 317, 336, 806
- switchport port-security, 317, 318, 319
- title, 401
- traceroute, 69, 771, 773
- tracert, 506, 518, 521, 773
- track, 679
- tunnel mode gre ip, 746
- undebug all, 770
- vlan, 405
- vrrp, 674
- vrrp timers advertise msec, 678
- połączenie
 - nadmiarowe, 354, 355
 - port tagowany, 339
 - tag vlan, 339
 - testowanie, 775, 776, 777
 - trunk, 316, 317, 332, 338, 339, 340
- port
 - aktualnie używany, 79
 - alternatywny, *Patrz:* port typ alternate
 - desygnowany, *Patrz:* port typ designated
 - dobrze znany, 78
 - docelowy, 73, 78
 - główny, 359, *Patrz:* port typ root
 - niedesygnowany, *Patrz:* port typ non-designated
 - numer, 77
 - priorytet, 357, 361
 - RS232, 184
 - tagowany, 339
 - trusted, 646
 - typ, 359
 - alternate, 359, 363
 - designated, 359, 360, 363
 - non-designated, 359
 - root, 359, 360
 - untrusted, 646, 647
 - zablokowany, 359
 - źródłowy, 73
- Port Address Translation, *Patrz:* PAT
- Port Security, 315
 - działanie, 324, 325
 - konfiguracja, 317, 318, 319, 320, 321
 - omijanie, 327
 - uruchamianie, 322, 323
- PortFast, 364, 365
- poufność, *Patrz:* dane
- zapewnienie poufności
- powłoka zdalna, 397
- priorytetyzacja, 811
- propagacja, 51
- protokół, 28, 31
 - 3DES, 727, 728
 - 802.1.x, 804, 805, 806, 807
 - AES, 727, 728
 - AH, 727
 - AHP, 629
 - ARP, 97, 100, 120, 378, 388, 461, 462
 - atak, 101
 - tablica, *Patrz:* tablica ARP
 - bezklasowy, 497
 - bezpołączeniowy, 225
 - BGP, 433, 755
 - eBGP, 755
 - iBGP, 755
 - konfiguracja, 756
 - szybkość, 756, 761
 - bramy
 - wewnętrznej, 433
 - zewnętrznej, 433, 434
 - CDP, 398, 400
 - CHAP, 700
 - DES, 727
 - DH, 727, 728
 - DHCP, 75
 - DHCPv6, 469, 651
 - bezstanowy, 653, 654
 - połączeniowy, 655, 656
 - distance vector, 435, 477, 478, 561, 594
 - DNS, 75
 - DTP, 316
 - EAP, 805
 - EAPOL, 805
 - EIGRP, 27, 433, 561, 586, 660, 714
 - FD, 567, 572, 573
 - FS, 573
 - interfejs pasywny, 583
 - konfiguracja, 563, 564
 - load balancing, 586, 587
 - metryka, 566, 567, 568, 569, 570, 571
 - pakiet, 562
 - RD, 567, 572, 573
 - routera stub, 589, 592, 593
 - sumaryzacja, 574, 575, 576, 577, 578
 - tablica routingu, 567, 571
 - tablica sąsiadów, 565
 - tablica topologii, 565, 566, 572
 - trasa domyślna, 584
 - uwierzytelnianie, 588
 - zmiana czasów, 585, 586
 - EIGRPv6, 594, 596
 - enkapsulacji, 725
 - ESP, 629, 727
 - FTP, 75
 - GLBP, 660, 661
 - konfiguracja, 682, 684

- protokół
 - hashujący, 727
 - HSRP, 660, 661
 - czas, 668
 - hasło, 668
 - konfiguracja, 661, 663, 665, 668, 671, 672
 - priorytet, 666
 - uwierzytelnianie, 668
 - uwierzytelnianie MD5, 670
- HTTP, 72, 74
- ICMP, 88, 116, 117, 628, 629, 630
 - debugowanie, *Patrz:* debugowanie protokołu ICMP
 - komunikat, 89
- IDEA, 727, 728
- IGRP, 433, 561
- IKE, 729, 734
 - Phase 1, 734, 739
 - Phase 2, 734
 - SA, 734
 - security associations, 729
- interakcja, 32
- IP, 32, 80, 81, 89, 659
- IPsec, 726
- IPv4, 97, 225, 451, 452
- IPv6, 66, 225, 451, 452, 462, 629, 657
 - diagnostyka, 475
 - grupa, 460
 - neighbour discovery, 456
 - podział sieci, 473, 474
 - proces, 456
- ISAKMP, 729
- IS-IS, 433
- klasowy, 477, 561
- komunikacyjny, 726
- LACP, 687
- LCP, 697, 699
- link state, 436, 497, 541
- LLDP, 401
- LMI, 713
- MD5, 727
- NCP, 699
- negocjacyjny, 727
- NTP, 390, 391, 392
- operatora, 725
- OSPF, 433, 497, 499, 527
 - konfiguracja, 502, 503, 505, 542, 543, 544, 545, 546, 548, 549, 550, 551
- metryka, 517, 523
- passive-interface, 526
- restart, 499
- trasa domyślna, 548, 549
- trasa statyczna, 550
- uwierzytelnienie, 537, 538
- uwierzytelnienie MD5, 539
- w sieci wielodostępowej, 528
- weryfikacja, 550, 551
- wieloobszarowy, 541, 542, 543, 544, 545, 546, 548, 549, 550
- wybieranie routera, 501
- OSPFv3, 553
 - konfiguracja, 554, 556, 558
- PAGP, 687
- PAP, 699
- PCP, 629
- POP3, 32, 75
- PPP, 694, 699
 - konfiguracja, 700
 - uwierzytelnienie CHAP, 699, 700, 701
 - uwierzytelnienie PAP, 699, 701
- przenoszenia, 725
- PVST, 366
 - konfiguracja, 369, 371
- RADIUS, 805
- redundancji, 661
- RIP, 432, 434, 438, 477
 - dystans administracyjny, 478
- RIPng, 490
 - debugowanie, 495
 - konfiguracja, 490, 491, 492
 - trasa domyślna, 493, 494
- RIPv1, 477
 - bezpieczeństwo, 483, 484
 - debugowanie, 482
 - konfiguracja, 479, 480, 481, 482, 483
 - trasa domyślna, 483
 - wyłączenie rozgłaszania, 484
- RIPv2, 485
 - debugowanie, 487, 488, 489
 - konfiguracja, 485, 486, 487, 488, 489
- routingu, 27, 432, 433
- RSTP, 353, 371, 372, 375
- RTP, 561
- SEAL, 727
- SHA, 727
- SMTP, 32, 75
- SNMP, 783, 784
 - analiza, 790, 794
 - konfiguracja, 784, 785, 786, 788, 789, 794
 - poziom zabezpieczeń, 784
- SSH, 387, 395
- SSL, 75
- STP, 353, 354, 364, 685
 - algorytm, 355, 357
 - PortFast, *Patrz:* PortFast status, 363
- symetrycznego szyfrowania, 727
- TCP, 32, 73, 76, 77
 - flow control, 118
 - three-way handshake, 118, 120
- TCP/IP, 726
 - serwer DNS, 113
- telnet, 630
- transportowy, 805
- UDP, 73, 76, 77, 115, 116, 490, 779
- VRRP, 660, 661
 - częstotliwość, 678
 - konfiguracja, 673, 674, 675, 676
 - rozgłoszenie, 677
 - track, 679
 - uwierzytelnianie, 678
- VTP, 342, 343
 - hasło, 347
 - ograniczenie, 346
 - VTP Pruning, 350
 - wersja, 343
- X.25, 695
- PRTG, 790, 798
- przeciążenie, 811
- przełączanie
 - obwodów, 691, 692
 - pakietów, 691, 692
- przełącznik, 21, 30, 42, 49, 95, 281, 378, 801
- CEF, 412
- Cisco 2960, 22
- Cisco 3550, 21
- enkapsulacja, 339
- Frame Relay, 692, 693, 720

interfejs, 315
 konfiguracja, 316
 przeciążenie, 811
 revision number, 342
 tryb pracy, *Patrz:* tryb pracy warstwa
 dostępu, 281, 282
 dystrybucji, 281
 rzenia, 282
 wymiana ramek, 317, 321
 przepływ ruchu, 795
 przepustowość, 29, 30, 432, 811
 przestój, 31
 punkt dostępu, 64
 PuTTY, 174
 PVC, 704
 full mesh, 704
 hub-and-spoke, 704, 705, 708, 716
 partial mesh, 705

Q

QEMU, 138
 QoS, 810, 811
 Quality of Service, *Patrz:* QoS

R

radius-server host, 806
 ramka, 89
 802.11, 89
 adresacja, 91
 BPDU, 357, 363
 dekapsulacja, 92,
 Patrz: dekapulacja
 długość, 115
 enkapsulacja,
 Patrz: enkapsulacja
 ethernetowa, 89, 90, 91, 96, 332
 filtrowanie, 120, 121
 Frame-Relay, 89
 PPP, 89
 priorytetyzacja, 811
 przechwytywanie, 138
 przełączanie, 43
 rozgłoszeniowa
 ARP, 97, 98, 121
 tagowanie, 331
 zawartość, 115
 ransomware, 68
 reconnaissance attack,
 Patrz: rekonesans

redundancja, 659, 660
 reflective ACL, 604
 rekonesans, 68, 69
 relacja sąsiedztwa,
 Patrz: sąsiedztwo
 RFC, 22
 ring topology, *Patrz:* sieć komputerowa topologia pierścienia
 robak, 66, 68
 root bridge, *Patrz:* most główny
 router, 30, 43, 49, 50, 73, 377
 ABR, 542, 543, 547
 AIM, 733
 ASBR, 542, 543
 BDR, 501, 528, 529, 531, 554
 BGP, 756, 757, 759, 761
 brzegowy, 480
 budowa, 380
 dioda, 381
 gniazdo, 382
 interfejs, 382
 pamięć, 381
 CEF, 380
 czas bezczynności, 396
 distance vector, 435
 DR, 501, 516, 528, 529, 531, 533, 554
 działanie, 378, 380
 fast switching, 380
 ID, 499, 501, 506, 507, 508, 509
 identyfikator, 499, 501, 506, 507, 508, 509, 529, 530, 554, 556, 563
 interfejs, 198, 199, 200
 jako agent przekazujący dane serwera DHCPv6, 656
 jako serwer DHCP, 643
 jako serwer DHCPv6, 468, 469, 652, 655
 konfiguracja, 194, 378, 379, 383, 384, 386
 NAT, 228
 lista sąsiadów, 501
 łączenie, 386
 mapowanie nazw, 774
 menu własne, 401
 obszar, *Patrz:* obszar priorytet, 500, 501, 529
 process switching, 380

przeciążenie, 811
 restart, 202
 router-on-a-stick, 333, 408
 serwera DHCPv6, 653
 sprzętowy, 22
 stan
 active, 660, 661, 666, 667
 standby, 660
 statystyki, 795, 796, 797, 799, 800
 stub, 589, 592, 593
 system operacyjny, 815
 tablica
 najdłuższe dopasowanie, 426
 testowanie połączenia, 389
 wirtualny, 136, 163, 396
 interfejs, 166
 karta rozszerzeń, 170
 konfigurowanie, 166, 168
 łączenie, 172
 pamięć, 170
 podłączenie do sieci rzeczywistej, 203, 204
 wartość Idle PC, 171
 wylogowanie, 396
 zarządzanie zdalne, 397
 zużycie procesora, 795
 routing, 73, 85, 436
 dynamiczny, 73, 431, 432, 466, 477, 490
 klasowy, 434
 pętla, 478
 RIPng, 467, 490
 statyczny, 73, 417, 418, 469, 545
 tablica, 92, 127, 128, 377, 379, 380, 436, 470, 518, 567, 571, 761
 cold start, 434
 initial exchange, 434
 minimalizowanie, 422
 przeszukiwania, 439
 stacji roboczej, 447, 448
 struktura, 437, 438
 wpis automatyczny, 379
 wpis dynamiczny, 379
 wpis statyczny, 379
 wieloobszarowy, 542
 routing table, *Patrz:* routing tablica

S

- SaaS, 813
- sąsiedztwo, 498, 500, 507, 509, 535, 578, 579
- segment, 80
 - TCP, 77
 - UDP, 77
- segmentacja, 119
- serwer, 42
 - czasu, 391, 392
 - DHCP, 87, 468, 643, 644
 - helper-address, 648
 - unieruchomienie, 645
 - DNS, 113, 774
 - alternatywny, 113
 - domyślny, 113
 - odpowiedź, 115, 116
 - preferowany, 113
 - wewnętrzny, 651
 - FTP, 75
 - intranetowy, 37
 - NTP, 391, 392
 - RADIUS, 806
 - syslog, 780, 781, 829
 - TFTP, 211, 213
 - VPN, 733
- serwera
 - DHCP, 82
 - DHCPv6, 655
- sesja, 76
- shielded twisted-pair,
 - Patrz:* skrętka ekranowana
- sieć komputerowa, 25, 35
 - analiza ruchu, 103, 104, 107, 138
 - atak, *Patrz:* atak bezpieczeństwa,
 - Patrz:* bezpieczeństwo
 - bezczynowa, 35, 63, 64
 - domowa, 49
 - emulator, 123
 - extranet, *Patrz:* extranet
 - internet, *Patrz:* internet
 - intranet, *Patrz:* intranet
 - klient-serwer, 35
 - LAN, 36, 46, 228, 273
 - łączenie, 692, 693
 - okablowanie, 45, 46, 52,
 - Patrz też:* medium transmisyjne
 - Ethernet, 58, 59
 - miedziane, 53
 - poziome, 52, 53
 - szkieletowe, 52
 - okablowanie pionowe,
 - Patrz:* sieć komputerowa
 - okablowanie szkieletowe
 - osiągnięcie zbieżności, 31
 - podział na podsieci, 243, 244, 246, 248, 251, 253, 255, 256, 257, 259, 277, 278
 - liczba hostów, 260, 263, 264, 265, 266, 267, 270, 273
 - prędkość, 32, 34
 - przechwytywanie, 104, 107
 - przedsiębiorstwa, 45
 - reverse engineering, 277, 278
 - SAN, 36
 - schemat, *Patrz:* sieć
 - komputerowa topologia
 - single-homed, 756
 - średnica, *Patrz:* średnica sieci
 - topologia, 440
 - fizyczna, 64
 - gwiazdy, 64
 - logiczna, 64, 65
 - magistrali, 64, 65
 - pierścienia, 64, 65
 - rozszerzonej gwiazdy, 64
 - VLAN, 331, 342, 344, 366, 403
 - domena rozgłoszeniowa, 332
 - działanie, 332
 - identyfikator, 346
 - komunikacja, 403, 404, 406, 408
 - konfiguracja, 334, 335, 336, 338, 342
 - natywny, 339, 341
 - prywatna, 338
 - usuwanie, 349
 - VTP Pruning, 350
 - VPN, *Patrz:* VPN
 - WAN, 37, 273, 691, 692
 - wielodostępowa, 528
 - WIFI, *Patrz:* WIFI
 - WLAN, 63
 - zbieżność, 432, 435, 436, 525, 537, 564, 585, 586, 591, 723
 - sieć satelitarna, 36, 38
 - single-mode fiber, *Patrz:* światłowód jednomodowy
 - skrętka, 53, 60
 - crossover, 57
 - ekranowana, 53, 54
 - kategoria, 55
 - niekranowana, 53, 54
 - SLAAC, 468, 469, 652, 655
 - Snowden Edward, 66
 - Software as a Service,
 - Patrz:* SaaS
 - SOHO, 37, 43
 - Solar Winds Response, 138
 - split-horizon, 478
 - spyware, 66
 - SSL, 749
 - stacja robocza, 39
 - tablica routingu, 447, 448
 - standard, 34
 - ACL, *Patrz:* ACL standardowa
 - IEEE 802.11, 63
 - IEEE 802.1D, 354
 - IEEE 802.1Q, 332
 - IEEE 802.3, 94
 - IEEE jako 802.1AB, 401
 - RFC1157, 784
 - RFC1631, 635
 - RFC1901, 784
 - RFC1918, 635
 - RFC2104, 731
 - RFC2409, 729
 - RFC3315, 653
 - RFC3410-3416, 784
 - RFC5340, 553
 - RFC5424, 779
 - RFC5996, 729
 - star topology, *Patrz:* sieć komputerowa topologia gwiazdy
 - STP, *Patrz:* skrętka ekranowana
 - Straight-Tip, *Patrz:* złącze ST
 - Subscribe Connector, *Patrz:* złącze SC
 - sumaryzacja, 421, 422, 423, 424, 472, 500, 547, 575, 576
 - automatyczna, 574
 - ręczna, 574, 577, 578
 - SuperPuTTY, 138, 174, 177, 194
 - zakładka, 174
 - nowa, 175
 - zmiana nazwy, 179

suplikant, 804
 switch, *Patrz:* przełącznik
 sygnał zagłuszania, 95
 symulator Cisco Packet Tracer, 135
 syslog, 779, 780
 system
 autonomiczny, 434, 563, 755
 binarny, 32, 229, 231, 235, 238, 240, 243, 453, 454
 operacyjny, 160, 165, 183
 obraz, 163
 routera, 815
 wirtualny, 141, 142, 147
 szesnastkowy, 41, 97, 453, 454
 szafa
 krosownicza, 49, 52, 53
 teleinformatyczna, *Patrz:* szafa krosownicza
 szum, 52
 szyfrowanie, 75, 725, 726, 730
 certyfikat, 749, 750, 752
 klucz
 prywatny, 728, 729
 publiczny, 728, 729
 symetryczny, 728
 metoda
 asymetryczna, 727, 728, 729
 symetryczna, 727, 728

Ś

średnica sieci, 364
 środowisko wirtualne VM
 VirtualBox, *Patrz:* VM
 VirtualBox
 światłowód, *Patrz też:* medium transmisyjne kabel światłowodowy, technologia światłowodowa
 budowa, 60
 jednomodowy, 61
 wielomodowy, 46, 53, 61

T

tablica
 ARP, 98, 99, 388
 FIB, 380, 412
 przylegania, 380, 412, 498
 routingu, 505, *Patrz:* routing tablica

sąsiadów, 565
 topologii, 565, 566, 572
 translacji, 636, 638, 639, 640
 technologia
 dial-up, 692
 DSL, *Patrz:* DSL
 EtherChannel, *Patrz:* EtherChannel
 Ethernet, *Patrz:* Ethernet
 ISDN, *Patrz:* ISDN
 światłowodowa, 46, 51, 61, *Patrz też:* światłowód, medium transmisyjne kabel światłowodowy
 telefonia
 komórkowa, 38
 VOIP, 811
 telewizja kablowa, 38
 TightVNC Viewer, 138
 tłumienie, 52
 topology table, *Patrz:* tablica topologii
 translacja
 dynamiczna, 640
 statyczna, 636
 z przeciążeniem, *Patrz:* PAT
 translation table, *Patrz:* tablica translacji
 transport layer, *Patrz:* warstwa transportu
 trasa, 85, 773
 domyślna, 424, 425, 426, 449, 471, 527, 584
 dystans administracyjny, 427
 filtrowanie, 601, 602
 koszt, 361, 432, 436, 517, 518, 519, 521, 522, 523
 nadrzędna pierwszego poziomu, 439
 najdłuższe dopasowanie, 426
 ostateczna, 438
 pierwszego poziomu, 439
 podrzędna drugiego poziomu, 439
 statyczna, 550
 wyszukiwanie rekurencyjne, 440
 trojan horse, *Patrz:* koń trojański
 tryb pracy
 client, 342
 global configuration, 187, 188

privileged executive, 187
 hasło, 201, 202
 server, 342, 343
 transparent, 342, 343
 user executive, 187
 tunelowanie, 725, 737
 GRE, 745, 746
 VPN SSL, 749

U

ultimate route, *Patrz:* trasa ostateczna
 unshielded twisted-pair, *Patrz:* skrętka nieekranowana urządzenie
 aktywne, 30, 49
 CPE, 696
 DCE, 386, 692, 697, 702, 703, 721
 dostępowe, 804
 DTE, 692, 697, 703
 monitorowanie, 766
 pasywne, 49
 pośredniczące, 804
 sieciowe, 26, 39
 bootstrap, 182
 komunikacja, *Patrz:* komunikacja
 monitorowanie, 174
 plik konfiguracyjny, 183, 187
 podłączanie, 175, 184
 POST, 181
 przewód konsolowy, 184
 rejestr konfiguracji, 182
 system operacyjny, *Patrz:* IOS
 tryb pracy, *Patrz:* tryb pracy
 uruchamianie, 181
 złącze, 61
 supplicant, *Patrz:* suplikant wirtualne, 175
 urządzenie DCE, 698
 usługa
 DHCP, 644, 646
 DNS, 84, 105, 109
 symetryczna, 776
 syslog, *Patrz:* syslog
 TFTP, 220
 UTP, *Patrz:* skrętka nieekranowana

uwierzytelnianie, 732, 737, 804
 MD5, 805, *Patrz też:*
 algorytm MD5
 MS-CHAP, 805
 PAP, 805
 podpis elektroniczny, 732
 pre-shared ke, 732
 PSK, 733
 RSA, 733

V

Virtual Private Network,
Patrz: VPN
 VirtualBox, 141, 142
 VirtualPC, 142
 virus, *Patrz:* wirus
 VM VirtualBox, 141
 VMware vSphere, 142
 VMware Workstation, 142
 VPCS, 138
 VPN, 724
 remote access, 725, 732,
 733, 749, 750, 752
 site-to-site, 732, 735, 744
 GRE, 745, 746
 konfiguracja, 735, 736,
 737, 738, 739, 742
 peer, 738, 741
 SSL, 749
 szyfrowanie, 725, 726

W

warstwa
 1., 74, 92, 692, 804
 2., 21, 70, 74, 89, 96, 115,
 692

adresacja, 315, 412
 LLC, 89
 MAC, 89, 412
 przełącznik, 334
 rozgłoszenie, 353, 354
 3., 21, 73, 74, 80, 377
 przełącznik, 334, 412
 rozgłoszenie, 354
 4., 74, 76, 77
 5., 74, 76
 6., 74, 75
 7., 74
 aplikacji, 72, 74
 OSI, *Patrz:* warstwa 7.
 dostępu do sieci, 72, 73
 fizyczna OSI, *Patrz:*
 warstwa 1.
 internetowa, 72, 73
 łącza danych OSI, *Patrz:*
 warstwa 2.
 prezentacji OSI, *Patrz:*
 warstwa 6.
 sesji OSI, *Patrz:* warstwa 5.
 sieci OSI, *Patrz:* warstwa 3.
 transportu, 72, 73, 115
 OSI, *Patrz:* warstwa 4.
 well-known port, *Patrz:* port
 dobrze znany
 WFQ, 812
 Wide Area Network, *Patrz:* sieć
 komputerowa WAN
 WIFI, 63
 wildcard mask, *Patrz:* maska
 podsieci odwrotna
 windowing, *Patrz:* metoda
 dynamiczne dostosowanie
 okien

WinPcap, 103, 138
 wireless, *Patrz:* sieć
 komputerowa bezprzewodowa
 Wireshark, 69, 103, 104, 123,
 136, 138, 222, 510, 801
 menu główne, 107, 108
 wirtualizacja, 141
 wirus, 66, 68
 workstation, *Patrz:* stacja
 robocza
 worm, *Patrz:* robak
 wtyk, *Patrz też:* gniazdo
 RJ45, 184
 RJ-45, 56

X

XE, 184
 XR, 184

Z

zaciskarka, 56
 zasilacz UPS, 49
 zegar BPDU, 364
 Zenmap, 69
 złącze, *Patrz też:* gniazdo, wtyk
 BNC, 59
 LC, 61, 62
 SC, 61
 ST, 61
 zombie, 69

Ż

żądanie echa, 116, 117

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA

 **Helion SA**

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 konkretnych, 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!**

sięgnij po **WIĘCEJ**



KOD KORZYSCI

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/nowości>

ISBN 978-83-283-3280-5



9 788328 332805

Informatyka w najlepszym wydaniu

cena: 199,00 zł