

ADAM JÓZEFIOK

CCNA 200-301

ZOSTAŃ ADMINISTRATOREM
SIECI KOMPUTEROWYCH CISCO



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 Helion SA 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 Helion SA nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

Redaktor prowadzący: Małgorzata Kulik

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

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

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

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
<http://helion.pl/user/opinie/ccn301>
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-283-7168-2

Copyright © Helion 2020

Printed in Poland.

- Kup książkę
- Poleć książkę
- Oceń książkę

- Księgarnia internetowa
- Lubię to! » Nasza społeczność

Spis treści

Wprowadzenie	23
Rozdział 1. Certyfikacja i wiedza ogólna	25
Firma Cisco	25
Certyfikacja i egzamin	27
CCNA — tematyka i materiał	30
Rodzaje pytań na egzaminie	31
Sprzęt do nauki	32
Dokumenty RFC	34
Rozdział 2. Wstęp do sieci komputerowych	35
Podstawy sieci komputerowych	35
Przesyłanie danych w sieci	39
Pojęcie protokołu sieciowego	42
Liczby w sieciach komputerowych	43
Organizacje standaryzujące	44
Rodzaje sieci komputerowych	45
Model pracy klient – serwer	45
Sieć bezprzewodowa	46
Sieć SAN	47
Sieci lokalne i sieci rozległe	47
Reguły działania sieci (komunikacja)	49
Proces komunikacji i wykorzystanie protokołów sieciowych	51
Urządzenia sieciowe	51
Okablowanie sieci przedsiębiorstwa	57
Media transmisyjne (miedziane, światłowodowe, bezprzewodowe)	61
Topologie sieci	78
Rozmiary sieci i nowe trendy	80

Rozdział 3. Modele sieci i pojęcie sieci Ethernet	85
Model TCP/IP	85
Warstwa aplikacji	86
Warstwa transportu	87
Warstwa internetowa	87
Warstwa dostępu do sieci	87
Model OSI	88
Warstwa aplikacji	88
Warstwa prezentacji	91
Warstwa sesji	91
Warstwa transportu	91
Warstwa sieci	101
Warstwa łączy danych	111
Warstwa fizyczna	114
Podstawy sieci Ethernet	116
CSMA/CD	118
Szybkość pracy	120
Adresowanie w Ethernetie	120
Protokół ARP	121
Dodanie wpisu statycznego ARP	123
Komunikacja poza domyślną bramę	124
Rozdział 4. Zastosowanie programu Wireshark	127
Omówienie najważniejszych funkcji programu Wireshark	127
Menu główne	130
Działanie komunikacji DNS	132
Rozmiar okna TCP oraz three-way handshake	142
Działanie protokołu ARP	146
Komunikacja w sieci Ethernet — podsumowanie	149
Rozdział 5. Emulator GNS3 i symulator Cisco Packet Tracer	161
Informacje na temat programu GNS3	162
Pobieranie, instalacja i najważniejsze funkcje	163
Ważniejsze funkcje i opcje	166
Obszar roboczy GNS3	179
Przygotowanie serwera GNS3	182
Połączenie dwóch wirtualnych stacji w programie GNS3	184
Przygotowanie IOS	186
Podłączenie routerów i uruchomienie prostej sieci	196

Konfiguracja programu SuperPuTTY	199
Połączenie z urządzeniem wirtualnym	199
Wydanie polecenia wielu urządzeniom naraz	200
Zmiana nazwy zakładek	200
Symulator Cisco Packet Tracer	201
Instalacja programu Cisco Packet Tracer	203
Projekt w programie Cisco Packet Tracer	205
Środowisko rzeczywiste — lab domowy	207

Rozdział 6. Wprowadzenie do systemu operacyjnego IOS i podstawowa konfiguracja urządzeń Cisco209

Proces uruchamiania urządzenia	209
System operacyjny IOS	211
Podłączenie do urządzenia	212
Zarządzanie urządzeniem	214
Tryby pracy	215
System pomocy	216
Przeglądanie konfiguracji	219
Wstępna konfiguracja routera Cisco wraz z zabezpieczeniami	222
Konfiguracja interfejsu	226
Zarządzanie konfiguracją	227
Połączenie wirtualnego routera z siecią rzeczywistą za pomocą obiektu Cloud	231
Zarządzanie systemem IOS	248
Uruchomienie TFTP na routerze	251
Wykorzystanie programu Wireshark w GNS3	254

Rozdział 7. Adresacja IPv4257

Informacje wstępne o protokole IPv4	257
Pojęcia adresu sieci, adresu hosta i adresu rozgłoszeniowego	259
Ping na adres rozgłoszeniowy sieci	259
Typy adresów (prywatne i publiczne)	260
Binarna reprezentacja adresu IP	262
Zamiana liczb dziesiętnych na binarne	264
Zamiana liczb binarnych na dziesiętne	271
Podział sieci według liczby wymaganych podsieci	277
Podział klasy C	277
Podział klasy B	286
Podział klasy A	290

Podział sieci na podsieci — liczba hostów w każdej sieci	294
Podział klasy C	294
Podział klasy B	298
Podział klasy A	300
Podział sieci na podsieci — nierówna liczba hostów w podsieciach	301
Reverse engineering	310
Rozdział 8. Adresacja IPv6	315
Wstępne informacje na temat protokołu IPv6	315
Zamiana liczb	318
Rozdział 9. Przełączniki sieciowe — podstawy działania i konfiguracji	341
Model hierarchiczny	341
Przełącznik warstwy 2.	344
Tablica adresów MAC	346
Podłączanie urządzeń do przełącznika	353
Metody przełączania ramek	354
Podstawowa konfiguracja przełącznika	355
Konfiguracja adresu IP i domyślnej bramy	357
Zmiana parametrów interfejsów i wyłączenie nieużywanych	361
Zapisanie konfiguracji	362
Włączenie protokołu SSH	363
Emulowany przełącznik w GNS3	370
Wykorzystanie w GNS3 obiektu Ethernet switch	372
Przypisanie adresu IPv6 na interfejsie VLAN1 przełącznika	374
Przełączniki pracujące w stosie	375
Rozdział 10. Przełączniki sieciowe — Port Security	379
Przygotowanie konfiguracji i informacje wstępne	380
Konfiguracja Port Security	381
Konfiguracja czasu działania blokady	387
Wywołanie zdarzenia bezpieczeństwa	388
Uruchomienie interfejsu po zdarzeniu bezpieczeństwa	390
Funkcja autouruchamiania interfejsu	391
Zmiana adresu MAC karty sieciowej	392
Rozdział 11. Sieci VLAN	395
Działanie sieci VLAN	395
Konfiguracja sieci VLAN	398

Rodzaje sieci VLAN	402
Prywatne sieci VLAN	403
Połączenia typu trunk	403
Przykład znakowania na łączu trunk	407
Automatyczna konfiguracja trybów interfejsów	408
Protokół VTP	412
Ograniczenia VTP	417
Ustalanie hasła i innych parametrów	418
Usuwanie konfiguracji VLAN	420
VTP Pruning	421
Rozdział 12. Protokół STP i jego nowsze wersje	423
Algorytm działania STP	425
Rodzaje portów w STP	429
Koszty tras	431
Stany portów	434
Rozszerzenie protokołu STP, czyli protokół PVST	436
Konfiguracja PVST	439
Protokół RSTP	442
Konfiguracja RSTP	443
Rozdział 13. Wprowadzenie do routerów Cisco	447
Działanie routera i jego budowa	447
Budowa routera	452
Wstępna konfiguracja routera	454
Omówienie protokołu CDP	469
Protokół LLDP	472
Własne menu na routerze	473
Cisco IP SLA	474
Rozdział 14. Routing pomiędzy sieciami VLAN	477
Metoda klasyczna	478
Router-on-a-stick	482
Przełączanie w warstwie 3.	486
Rozdział 15. Routing statyczny	489
Wprowadzenie do routingu statycznego	489
Sumaryzacja tras statycznych	493

Default route	496
Najdłuższe dopasowanie	499
Floating Static Route	499
Rozdział 16. Routing dynamiczny i tablice routingu	505
Rodzaje protokołów routingu dynamicznego	506
Wymiana informacji i działanie protokołów	508
Protokoły distance vector	508
Protokoły link state	510
Tablica routingu routera	510
Proces przeszukiwania tablicy routingu	513
Tablica routingu stacji roboczej	521
Rozdział 17. Routing dynamiczny — protokół RIP	525
Charakterystyka i działanie protokołu RIPv1	525
Konfiguracja RIPv1	526
Charakterystyka i konfiguracja protokołu RIPv2	533
Konfiguracja RIPv2	534
Podstawy protokołu RIPng	538
Konfiguracja protokołu RIPng	538
Rozdział 18. Routing dynamiczny — protokół OSPF	545
Protokół OSPFv2	545
Pakiety hello	546
Konfiguracja protokołu OSPF	549
Alternatywna konfiguracja protokołu OSPF	554
Równoważenie obciążenia w OSPF	557
Zmiana identyfikatora routera	558
Stany interfejsów i relacje sąsiedzkie	561
Wymiana informacji pomiędzy routerami — obserwacja	562
Metryka w OSPF	568
Zmiana czasów	576
Konfiguracja passive-interface	578
Rozgłaszanie tras domyślnych	578
OSPF w sieciach wielodostępowych	579
Wybór routerów DR i BDR	580
Statusy po nawiązaniu relacji sąsiedztwa	586
Routery DR i BDR w połączeniu punkt – punkt	588
Uwierzytelnianie w OSPF	590

Wieloobszarowy OSPF	593
Typy przesyłanych pakietów LSA	595
Konfiguracja wieloobszarowego OSPF	595
Protokół OSPFv3	606
Konfiguracja OSPFv3	606
Rozdział 19. Listy ACL	613
Rodzaje list ACL	615
Konfiguracja standardowych list ACL	616
Przykład 1.	616
Przykład 2.	621
Przykład 3.	623
Przykład 4. (lista standardowa nazywana)	625
Konfiguracja rozszerzonych ACL	629
Przykład 5.	630
Przykład 6.	632
Przykład 7.	634
Przykład 8.	636
Przykład 9.	639
Listy ACL w IPv6	640
Przykład 10.	641
Przykład 11.	642
Przykład 12.	643
Przykład 13.	643
Rozdział 20. Network Address Translation (NAT)	
i Dynamic Host Configuration Protocol (DHCP)	645
Static NAT (translacja statyczna)	646
Dynamic NAT (translacja dynamiczna)	650
PAT	651
Konfiguracja routera R1 jako serwera DHCP	653
DHCP Snooping	654
Przykład	659
Konfiguracja routera R1 jako serwera DHCPv6 (SLAAC)	660
Konfiguracja routera jako bezstanowego serwera DHCPv6	662
Konfiguracja routera jako stanowego serwera DHCPv6	664
NAT dla IPv6	667

Rozdział 21. Redundancja w sieci i wykorzystanie nadmiarowości	669
Konfiguracja protokołu HSRP	671
Przygotowanie przykładowej sieci w programie GNS3	671
Konfiguracja HSRP	673
Konfiguracja VRRP	683
Konfiguracja GLBP	691
EtherChannel	695
Konfiguracja EtherChannel	697
Rozdział 22. Technologie sieci WAN i sieci VPN	701
Sieci WAN — ogólne informacje	701
Technologie sieci WAN	703
Frame Relay	703
ISDN	704
PPP	705
DSL	705
X.25	706
ATM	707
MPLS	707
Przykładowy model sieci WAN	708
Konfiguracja enkapsulacji w przykładowym modelu punkt – punkt	708
Technologia Frame Relay	714
Konfiguracja Frame Relay (hub-and-spoke)	717
Konfiguracja multipoint	719
Konfiguracja point-to-point	728
Samodzielna konfiguracja przełącznika Frame Relay	731
Technologia VPN	735
Szyfrowanie w VPN	737
Typy sieci VPN	745
Implementacja VPN site-to-site na routerze Cisco za pomocą CLI	747
Rozdział 23. Sieci wi-fi	767
Wprowadzenie do sieci bezprzewodowych	767
Działanie sieci bezprzewodowej	769
Standardy sieci wi-fi	773
Urządzenia bezprzewodowe	774
Format ramki	776
Mechanizm CSMA/CA	789
Sposób połączenia	789

Bezpieczeństwo sieci bezprzewodowych	797
Typowe ataki na sieci bezprzewodowe	798
Zastosowanie i projektowanie sieci bezprzewodowych	800
Konfiguracja kontrolera Cisco WLC i punktu dostępowego	801
Rozdział 24. Podstawy bezpieczeństwa w sieciach komputerowych	821
Bezpieczeństwo w sieci	821
Główne rodzaje niebezpieczeństw — pojęcia	824
Wybrane ataki warstwy 2. modelu OSI	830
Ataki na ARP	830
Ataki na STP	830
Ataki na VLAN	830
Ataki na DHCP	831
Ataki na tablicę ARP i MAC	831
Główne rodzaje niebezpieczeństw — przykładowe ataki	831
Denial of Service (DoS)	832
Denial of Service (DoS) — atak zwierciadlany	834
Ataki na ARP	834
Ataki na STP	837
Ataki STP na root bridge i wybór nowego roota	840
Ataki na VLAN	843
Ataki na DHCP	849
Ataki na tablicę MAC i ARP	856
Główne rodzaje niebezpieczeństw — obrona	859
System ochrony warstw wyższych	859
Model AAA	865
Rozwiązanie 802.1X	866
Szybkie bezpieczeństwo na urządzeniach Cisco	867
Rozdział 25. Quality of Service	871
Kolejkowanie w sieciach	871
Modele QoS	875
Wdrażanie QoS	875
Rozdział 26. Obsługa programu Cisco Configuration Professional	879
Program Cisco Configuration Professional	879
Instalacja programu CCP	880
Uruchomienie CCP Express na routerze w GNS3	880
Konfiguracja CCP na stacji roboczej i połączenie do routera uruchomionego w programie GNS3	883

Rozdział 27. Zarządzanie siecią	897
Niektóre problemy w sieci	897
Rozwiązywanie problemów z interfejsami	899
Narzędzie debugowania	900
Sprawdzanie komunikacji	902
Testowanie łącza z siecią internet	904
Testowanie połączenia w sieci lokalnej za pomocą narzędzia iperf	905
Logowanie zdarzeń i raportowanie	906
Obsługa logów systemowych syslog	908
Wykorzystanie SNMP	910
Wykorzystanie i działanie NetFlow	921
Konfiguracja funkcjonalności span port	925
 Rozdział 28. Projektowanie i automatyzacja sieci	 929
Projektowanie sieci	929
Działania wstępne	932
Dokumentacja sieci	939
Rozwiązywanie problemów z siecią	940
Wirtualizacja i automatyzacja sieci — wprowadzenie	943
Usługi chmury	943
Maszyny wirtualne	944
Sieci SDN	946
Automatyzacja sieci	949
API	952
Szablony	954
 Rozdział 29. Ćwiczenia praktyczne	 955
Ćwiczenie 1.	955
Odpowiedź do ćwiczenia	955
Ćwiczenie 2.	956
Odpowiedź do ćwiczenia	956
Ćwiczenie 3.	957
Odpowiedź do ćwiczenia	957
Ćwiczenie 4.	960
Odpowiedź do ćwiczenia	960
Ćwiczenie 5.	961
Odpowiedź do ćwiczenia	961
Ćwiczenie 6.	961
Odpowiedź do ćwiczenia	962

Ćwiczenie 7.	968
Odpowiedź do ćwiczenia	968
Ćwiczenie 8.	975
Odpowiedź do ćwiczenia	976
Ćwiczenie 9.	979
Odpowiedź do ćwiczenia	980
Ćwiczenie 10.	983
Odpowiedź do ćwiczenia	984
Ćwiczenie 11.	990
Odpowiedź do ćwiczenia	991
Rozdział 30. Słownik pojęć	999
Zakończenie	1025
Literatura	1027
Skorowidz	1029

Rozdział 14.

Routing pomiędzy sieciami VLAN

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

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

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

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

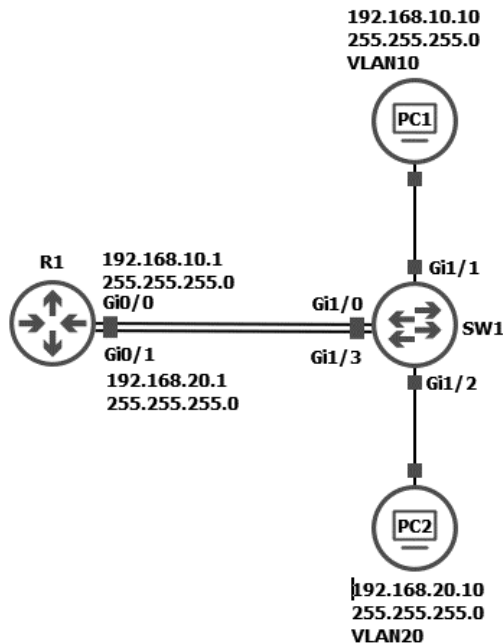
Każdą metodę postaram się wyjaśnić na podstawie projektów, które możesz wykonać samodzielnie w programie GNS3. Będzie Ci do tego potrzebny router Cisco 3745, o którym wspominałem w poprzednich rozdziałach.

Metoda klasyczna

Metoda klasyczna polega na skierowaniu ruchu z sieci VLAN do routera. Spójrz na rysunek 14.1. Przedstawia on dwie stacje robocze. Są to stacje VPC użyte w programie GNS3, ale możesz również użyć własnych wirtualnych maszyn. Stacja robocza H1 znajduje się w sieci VLAN10 i podsieci 192.168.10.0/24, a stacja H2 jest w sieci VLAN20 i podsieci 192.168.20.0/24. Jeśli w sieci nie będzie routera, te dwie stacje nie będą mogły się ze sobą komunikować. Stanie się tak, ponieważ znajdują się one w różnych podsieciach oraz, co najważniejsze, w różnych sieciach VLAN.

RYСУNEK 14.1.

Routing pomiędzy sieciami VLAN — model klasyczny



Aby te dwie stacje robocze mogły się ze sobą komunikować, użyjemy routera R1. Jest on wyposażony w dwa interfejsy: GigabitEthernet0/0 i GigabitEthernet0/1. W naszym przykładzie są konieczne właśnie dwa interfejsy. Metoda klasyczna wymaga, aby każdy interfejs routera należał do określonej sieci VLAN i był bramą domyślną dla wszystkich stacji w tej podsieci. Interfejs g0/0 ma więc adres IP 192.168.10.1 i jest domyślną bramą dla wszystkich urządzeń znajdujących się w sieci VLAN10.

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

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


W kolejnym kroku przypisz interfejs g1/1 do sieci VLAN10, a interfejs g1/2 do sieci VLAN20. Pamiętaj, aby określić przeznaczenie interfejsu, wykorzystując polecenie `switchport mode access`. Następnie poleceniem `switchport access vlan [symbol_sieci_vlan]` przypisz interfejs do określonej sieci VLAN.

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

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

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

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

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

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

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

Pamiętaj, że interfejsy routera będą domyślną bramą dla całego ruchu pochodzącego z określonej sieci VLAN. Przydziel odpowiednie adresy IP do interfejsów routera i uruchom interfejsy. Zauważ, że na

przykład interfejs g0/0 routera R1 ma adresację pochodzącą z tej samej podsiaci co stacja robocza H1, ponadto znajduje się w tej samej sieci VLAN. Na stacjach roboczych ustaw też adresy IP i adresy bram domyślnych. Stację VPCS skonfigurujesz za pomocą komendy `ip [adresIP] [maska] [adresIP_domyślnej_bramy]`, np. `ip 192.168.10.10 255.255.255.0 192.168.10.1`. Zajmijmy się teraz routerem R1.

```
R1(config)#int g0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#int g0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
```

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

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

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

Spójrz na pierwszy z nich, zawierający literę C, która oznacza źródło wpisu. Litera C pochodzi od słowa *connected*, co wskazuje na wpis z sieci bezpośrednio podłączonej. Następnie podana jest podsieć, której ów wpis dotyczy. W tym przypadku jest to 192.168.10.0/24. Za adresem sieci znajduje się fraza *is directly connected* (jest bezpośrednio podłączona). Natomiast identyfikator umieszczony na końcu oznacza interfejs, którym musi zostać przesłany pakiet, aby trafił właśnie do tej podsiaci. Litera L wskazuje na adres lokalnego interfejsu podłączonego do tej sieci. Jest to dodatkowa informacja, która pozwala odnaleźć się w gąszczu podsiaci.

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from Pfr
Gateway of last resort is not set
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
```

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

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

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

W takim przypadku stacja H1 musi uzyskać adres MAC stacji roboczej H2. Jest to niemożliwe, gdyż obie stacje znajdują się w różnych sieciach i różnych domenach rozgłoszeniowych. Stacja robocza H1 ma jednakże podaną w ustawieniach protokołu TCP/IP domyślną bramę, którą jest interfejs g0/0 routera R1. Wysyła więc rozgłoszenie ARP do sieci, podając jako docelowy adres IP domyślnej bramy. Ponieważ stacja robocza oraz interfejs routera znajdują się w tej samej sieci VLAN (tej samej domenie rozgłoszeniowej), ramka trafia do interfejsu routera i router przesyła adres MAC swojego interfejsu. Rozpoczyna się zatem komunikacja.

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

Ramka trafia do interfejsu routera R1. Router, dekapstułując ramkę, wyłania pakiet i sprawdza w nim, że adresem docelowym jest 192.168.20.10. Router bada więc tablicę routingu i dopasowuje adres docelowy do wpisów w tablicy. Okazuje się, że adres IP jest częścią podsieci 192.168.20.0/24, dlatego router odsyła pakiet przez interfejs g0/1, zgodnie z zapisem w tablicy routingu. Pakiet jest ponownie umieszczany w ramce i, po wcześniejszym przeprowadzeniu procesu ARP, wysyłany przez interfejs fizyczny. Ramka otrzymuje oznakowanie VLAN20 i trafia do stacji roboczej H2.

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

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

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

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

```

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

```

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

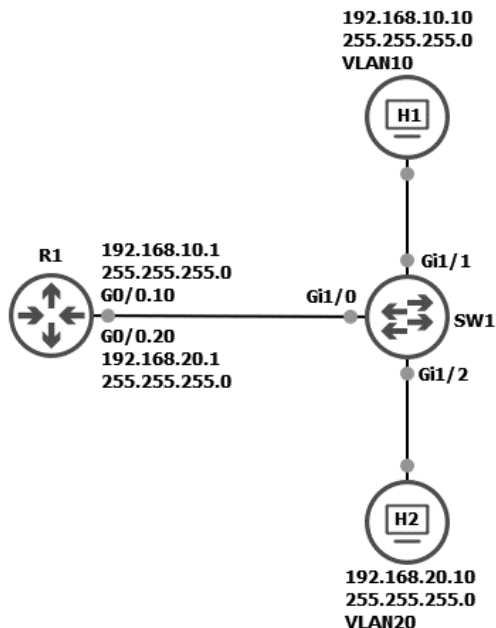
Router-on-a-stick

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

Na rysunku 14.2 pokazałem sieć komputerową, w której połączenie pomiędzy routerem a przełącznikiem realizowane jest za pomocą jednego przewodu. Przejdźmy więc do konfiguracji i szczegółowego omówienia działania prezentowanej tu metody. Możesz do tego ćwiczenia wykorzystać poprzednie, ale wymaż konfigurację routera i przełącznika, aby łatwiej Ci było dokonywać nowych ustawień.

RYSUNEK 14.2.

Metoda
router-on-a-stick



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

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

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

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

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

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

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



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

Jeśli więc mamy sieć VLAN10, komenda tworząca podinterfejs będzie wyglądała następująco: `interface g0/0.10`. Po utworzeniu podinterfejsu znajdziesz się w trybie jego konfiguracji. Zanim przypiszesz do niego adres IP, musisz wskazać enkapsulację oraz podać identyfikator sieci VLAN. Zrób to poleceniem `encapsulation dot1q [identyfikator_sieci_vlan]`. Teraz możesz już przypisać dowolny adres IP. Podanie enkapsulacji jest ważne, gdyż interfejs routera dzięki temu wie, jak obsłużyć oznakowane ramki, które będą do niego wysyłane. Ponadto musi on wiedzieć, jak znakować ramki, które sam będzie wysyłał do sieci.

Pamiętaj, że adres ten będzie adresem domyślnej bramy dla wszystkich stacji roboczych występujących w tej podsieci i znajdujących się w tej sieci VLAN. Przypisanie adresu IP odbywa się przy użyciu polecenia, które już znasz: `ip address [adres_ip] [maska_podsieci]`. Konfigurację obydwu podinterfejsów dla sieci VLAN10 i VLAN20 przedstawia poniższy listing. Na sam koniec przejdź do fizycznego interfejsu `g0/0` i uruchom go poleceniem `no shutdown`.

```

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

```

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

```

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

```

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

```

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

```

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

```

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

```

W kolejnym kroku przejdź do konfiguracji przełącznika i jeszcze raz przypisz interfejsy do odpowiednich sieci VLAN, jeśli wcześniej usunąłeś konfigurację. Dodatkowo interfejs `g1/0` należy jedynie ustawić do pracy jako trunk, korzystając z polecenia `switchport mode trunk`. Ustawienie interfejsu jako trunk sprawi, że będzie on przekazywał ruch płynący z różnych sieci VLAN. Nie można więc tego interfejsu ustawić do pracy w konkretnym VLAN-ie. Jeśli w trakcie zmiany interfejsu na tryb trunk pojawi się komunikat `Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk" mode`, należy zmienić enkapsulację na interfejsie z trybu automatycznego na tryb ustawiony manualnie.

```

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

```

```

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

```

Przejdź jeszcze na chwilę do konsoli routera i wyświetl tablicę routingu. Wyświetlenie tablicy routingu routera R1 pokazuje informacje podobne do tych, które pojawiły się w poprzedniej metodzie. Obie sieci w tablicy są oznaczone jako bezpośrednio połączone, zmieniły się jedynie interfejsy, przez które sieci są dostępne.

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is not set
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0.10
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L       192.168.20.1/32 is directly connected, GigabitEthernet0/0.20
R1#

```

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

```

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

```

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

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

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

Przełączanie w warstwie 3.

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

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

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

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

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

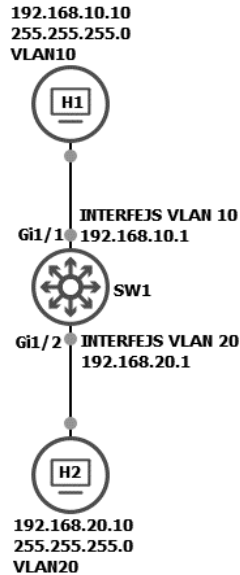
Adjacency table obejmuje wpisy dotyczące adresów warstwy 2., wykorzystywane m.in. w FIB i pomocne w trakcie przesyłania informacji dalej.

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

Opisywana metoda komunikowania się sieci VLAN między sobą oparta jest więc na przełącznikach warstwy 3. Na rysunku 14.3 został pokazany tylko przełącznik, nie ma tu już natomiast routera. Przełącznik, którego tu używam, to ten sam, którego używałem wcześniej, jednak dla zachowania przejrzystości schematu zmieniłem jego ikonę, tak aby kojarzył się z przełącznikiem warstwy 3.

RYSUNEK 14.3.

Komunikacja
pomiędzy sieciami
VLAN
z wykorzystaniem
przełącznika L3



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

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

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

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

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

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

```
SW1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
Gateway of last resort is not set
 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, Vlan10
L       192.168.10.1/32 is directly connected, Vlan10
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/24 is directly connected, Vlan20
L       192.168.20.1/32 is directly connected, Vlan20
SW1#
```

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

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

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

Skorowidz

3DES, Triple Data Encryption Standard, 740

A

- AAA, authentication,
 - authorization, accounting, 865
 - autoryzacja, 866
 - raportowanie, 866
 - uwierzytelnienie, 865
- ABR, Area Border Router, 594
- access point, 768
- ACK, acknowledgement frame, 142, 781
- ACL, Access Control List, 343, 613, 822
- AD, Administrative Distance, 500
 - wartości, 500
- adapter RS232-USB, 213
- adjacency table, tablica przynależności, 451, 486
- administrowanie bezpieczeństwem, 822
- adres
 - IP, Internet Protocol, 101, 106, 257
 - anycast, 320
 - automatyczne przypisanie, 109
 - docelowy, destination IP address, 101
 - domyślnej bramy, 106
 - global, globalny, 320
 - GUA, 661
 - helper, 994
 - hosta, 259
 - local-link, lokalnego łącza, 262, 320
 - loopback, lokalnej pętli, 320
 - multicast, grupowy, 320, 325
 - pętli zwrotnej, 262
 - przełącznika, 357, 359
 - reprezentacja binarna, 262
 - ręczne przypisanie, 106
 - rozgłoszeniowy, 259
 - sieci, 259
 - VIP, 670
 - źródłowy, source IP address, 101
 - IPv6, 315, 338
 - adres interfejsu przełącznika, 374
 - autokonfiguracja, 339
 - Global Routing Prefix, 338
 - konfiguracja interfejsu loopback, 330
 - konfiguracja tras statycznych, 334
 - konfiguracja trasy domyślnej, 334, 336
 - listy ACL, 640
 - nagłówek, 316
 - NAT, 667
 - Neighbor Solicitation, 327
 - podział sieci, 338
 - polecenia diagnostyczne, 340
 - protokół RIPng, 538
 - rodzaje adresów, 320
 - skracanie adresów, 319
 - subnet ID, 339
 - sumaryzacja tras, 337
 - Temporary IPv6, 328
 - Unspecified, nieokreślony, 320
 - MAC, 52, 138, 149, 155, 321, 346, 955
 - karty sieciowej, 392
 - wirtualny MAC, 674, 685, 691
 - adresowanie, 120
 - adresy
 - prywatne, 261
 - publiczne, 260
 - zdublowane, 323
 - adware, 821
 - AES, Advanced Encryption Standard, 739, 798
 - agent przekazujący, relay agent, 666
 - AH, Authentication Header, 739
 - AHP, 641
 - AIM, Advanced Integration Modules, 746
 - alarmy
 - falszywe, 864
 - prawdziwe, 864
 - algorytm
 - 3DES, 740
 - AES, 740, 798
 - DES, 740
 - DKE, 798
 - DSA, 745
 - ECDSA, 745
 - IDEA, 740, 741
 - MD5, 742
 - RC, 741
 - RSA, 745
 - SHA, 742
 - SPF, 545
 - STA, 425
 - TKIP, 797
 - algorytmy
 - haszujące, 742
 - szyfrowania, 738
 - alias, 464
 - alternate port, port alternatywny, 430, 443
 - AMP, Advanced Malware Protection, 860

- amplituda, 771
 analiza
 ruchu IPS, 863
 three-way handshake, 145
 analogowe połączenia telefoniczne, 706
 antena
 dookólna, omnidirectional antenna, 775
 kierunkowa, directional antenna, 776
 MIMO, 776
 API, 952
 ARP, Address Resolution Protocol, 121, 448, 460, 830, 831, 834, 856
 działanie protokołu, 146
 ramka rozgłoszeniowa, 151, 152
 wpisy statyczne, 123
 asocjacja, associate, 790
 atak
 buffer overflow attack, 827
 DoS, 799, 821, 827, 832
 DDoS, 827
 dostępu, 826
 DTP, 844
 flood attack, 829
 man-in-the-middle, 678, 744, 827
 passwords attack, 827
 poisoning, 125
 smurf attack, 828
 spoofing, 125, 828
 STP, 840
 trust exploitation attack, 828
 VLAN hopping, 843
 ataki
 lista ataków, 851
 modyfikowanie pola danych, 848
 ramki, 847
 na ARP, 828, 830, 834
 na DHCP, 831, 849
 na protokoły IPv4, 829
 na root bridge, 840
 na STP, 830, 837
 na tablicę ARP i MAC, 831, 856
 na VLAN, 828, 830, 843
 obserwacja, 851
 siłowe, 826
 z zewnątrz, 823
 zwierciadlane, 834
 ATM, Asynchronous Transfer Mode, 707
 autentykator, 866
 autoinstalacja, 215
 automatyczna konfiguracja trybów interfejsów, 408
 automatyczne wylogowywanie, 468
 zapisywanie konfiguracji, 246
 automatyzacja sieci, 943, 949
 Auto-MDIX, 353
 autosumaryzacja, 534, 536
 autouruchamianie interfejsu, 391
 AUX, auxiliary, 453
 AVF, Active Virtual Forwarders, 671, 691
 AVG, Active Virtual Gateway, 671, 691
 awaria interfejsu, 565
 awarie sieci, 897
- B**
- backbone area, 607
 backup port, port zapasowy, 443
 bajt, byte, 43
 banner MOTD, 226
 baza danych
 LSDB, 566
 OSPF, 566
 stanu łącza, 545
 BDR, Backup Designated Router, 548, 579
 bezpieczeństwo, 394
 autokonfiguracja urządzenia, 867
 autouruchamianie interfejsu, 391
 sieci bezprzewodowych, 797
 sieci komputerowej, 613
 w sieci, 821
 BGP, Border Gateway Protocol, 507
 BNC, Bayonet Neill-Conclemann, 37
 bootstrap, 210
 BPDU, Bridge Protocol Data Units, 425
 BPDU Guard, 446, 841
 brama domyślna
 żądanie ARP, 153
 żądanie ping, 153
 broadcast, 49, 50, 125, 421, 423
 broadcast storm, 424
 BSS, Basic Service Set, 768
 BSSID, BSS Identifier, 768
 BW, bandwidth, 570
 BYOD, 57
- C**
- CBWFQ, 874
 CCNA, 30
 Cisco, 25
 Configuration Professional, CCP, 879
 dodawanie użytkownika, 890
 instalacja programu, 880, 883
 Java Control Panel, 884
 konfiguracja interfejsów, 885
 konfiguracja na stacji roboczej, 883
 konfiguracja routera, 892
 konfiguracja routingu statycznego, 887
 syslog, 894
 monitorowanie routera, 892
 okno Add an Account, 891
 okno Deliver Configuration to Device, 888, 894
 okno Exception Site List, 884
 okno Logging, 895
 trasa statyczna, 889
 wyświetlanie powiadomień, 896
 zabezpieczenie routera, 890
 zarządzanie grupą urządzeń, 885
 Discovery Protocol, CDP, 469
 Expres, 881
 logowanie do routera, 882
 okno główne, 883
 Express Forwarding, CEF, 451, 486
 Feature Navigator, 249
 IP SLA, 474
 Packet Tracer, 161, 201
 Download Packet Tracer, 203
 instalacja programu, 203
 konfiguracja urządzenia sieciowego, 207
 okno główne, 204
 projekt, 205
 wybór wersji, 204
 zmiana nazwy zakładki, 202
 Prime NAM, 941

- certyfikat, 762
 CHAP, Challenge Handshake Authentication Protocol, 711
 chmura, 943
 prywatna, 944
 publiczna, 944
 CIR, Committed Information Rate, 704, 715
 CLI, 747
 Cloud, 231, 235
 coaxial cable, 71
 cold start, 508
 CoS, Class of Service, 876
 Cpulimit, 165
 crossover, 68
 CSMA/CA, 789
 CSMA/CD, 118
 CTS, clear to send, 780
 czas
 bezczynności routera, 467
 dead interval, 548
 dead time, 577
 działania blokady, 387
 flush, 583
 flushed, 529
 hello, 577, 677
 hello-interval, 576
 hold down, 529
 hold, 677
 interwał przesyłania pakietów, 548
 starzenia się, aging time, 387
 wzorcowy UTC, 462
 częstotliwości fal, 770
- D**
- DAD, Duplicate Address Detection, 323
 DAJ, Dynamic ARP Inspection, 857
 database description, 546
 DCE, Data Communications Equipment, 458, 704
 debugowanie, 817, 900
 komunikatów RIP, 530
 protokołu
 CDP, 902
 ICMP, 901
 default route, trasa domyślna, 496
 dekapulacja, 448
 deny, 613, 630
 DES, Data Encryption Standard, 739
 designated port, port desygnowany, 430, 443
 detekcja ruchu IPS, 863
 DFS, Dynamic Frequency Selection, 772
 DHCP, Dynamic Host Configuration Protocol, 42, 90, 333, 647, 654, 831, 849
 attack parameters, 853
 Consumption Attack, 831
 Snooping, 654, 853, 855, 857
 DHCPv6, 660–665
 dioda
 L, link, 453
 RPS, 345
 stanu portów, 345
 systemowa, 345
 trybu portów, 345
 distance vector, 508, 525
 DKE, Dragonfly Key Exchange, 798
 DLCI, Data-Link Connection Identifier, 704, 715
 DMVPN, Dynamic Multipoint VPN, 736
 DNS, Domain Name System, 90, 132
 działanie komunikacji, 132
 odpowiedź serwera, 141
 wyświetlanie tablicy, 133
 zapytanie, 139
 zasada działania, 137
 dokumentacja sieci, 939
 domena awarii, failure domain, 932
 DoS, Denial of Service, 821, 832, 834
 dostawca internetu, 36
 dostęp
 do sieci internetowej, 47
 do urządzeń sieciowych, 628
 dostępność, availability, 41
 DR, Designated Router, 548, 567, 579
 drother, 561, 582, 584, 597, 609
 drothery, 548
 DSL, Digital Subscriber Line, 48, 705
 rodzaje, 706
 DSSS, Direct-Sequence Spread Spectrum, 773
 DTE, Data Terminal Equipment, 458, 704
 DTLS, Datagram Transport Layer Security, 796
 DTP, Discovery Trunk Protocol, 381
 DTP, Dynamic Trunking Protocol, 408
 DWDM, Dense Wavelength Division Multiplexing, 702
 dynamic, 630
 dynamic NAT, 650
 Dynamips, 164
 dystans administracyjny, AD, 499
- E**
- EAP, Extensible Authentication Protocol, 867
 ECN, Extended Congestion Notification, 877
 edge port, port brzegowy, 446
 EIGRP, Enhanced IGRP, 506, 554
 EIR, Excess Information Rate, 704
 EMI, Enhanced Multilayer Software, 33
 emulator GNS3, 161
 enkapsulacja, 155, 159, 449, 708
 HDLC, 708, 712
 PPP, 708, 710
 ESCON, Enterprise Systems Connection, 74
 ESP, ESP, Encapsulating Security Payload, 641, 739
 EtherChannel, 424, 695
 konfiguracja, 697
 Ethernet, 116, 149
 adresowanie, 120
 switch, 372
- F**
- fala radiowa, 769
 FHSS, Frequency Hopping Spread Spectrum, 773
 FIB, Forwarding Information Base, 451, 486
 FIFO, first in, first out, 873
 filtrowanie
 adresów URL, 860
 pakietów przychodzących, 859
 ramek ARP, 148
 firewall, 822, 859, 861
 flash, 453
 Floating Static Route, 499, 503
 fluktuacje, jitter, 873

formaty danych, 950
 Frame Relay, 703, 714
 konfiguracja, 717
 konfiguracja przełącznika, 720, 732
 FromDS, From Distribution System, 781
 FTP, File Transfer Protocol, 90
 funkcja Desg, 433
 funkcjonalność
 Auto-MDIX, 353
 BPDU Guard, 841
 buffering, 144
 DAI, 857
 DHCP Snooping, 857
 EtherChannel, 696
 flow control, 143
 helper-address, 656, 658
 LAG, 802
 load balancing, 671
 passive interface, 533, 578
 podłączanie wirtualnego routera, 231
 Port Security, 342, 384
 PortFast, 436
 Preemption, 675, 676, 692
 Pruning Mode, 415
 QoS, 872
 relay agent, 666
 rsh-enable, 469
 segmentacja, 144
 SLAAC, 661
 span port, 925
 subinterfaces, 483
 sumaryzacja, 493
 track, 681

G

GBIC, Gigabit Interface Converter, 353
 GE, Gigabit Ethernet, 453
 generowanie klucza, 367, 740
 symetrycznego, 741
 GLBP, Gateway Load Balancing Protocol, 671, 691
 konfiguracja, 691
 maksymalna liczba urządzeń, 691
 równoważenie obciążenia, 692
 tryb pracy
 AVF, 691
 AVG, 691

gniazdo abonenckie, 58
 GNS3, Graphical Network Simulator, 161
 Adapters, 195
 Add a note, 196
 APPLIANCES, 188
 Ask for settings profile at application startup, 167
 Automatically check for update, 167
 Base MAC, 195
 Browse configuration directory, 167
 Browse end devices, 184
 Configuration file, 167
 Configure custom adapters, 195
 Configure template, 184
 dodanie dodatkowego opisu, 186
 Enable experimental features, 167
 funkcje, 166
 General preferences, 166, 167
 implementowanie maszyny wirtualnej, 179
 urządzenia L2, 194
 Import appliance, 188
 importowanie obrazu przełącznika, 194
 instalacja, 163
 IOS, 186
 karty sieciowe, 232
 konfiguracja wirtualnego serwera, 183
 konsola routera, 193
 menu funkcji, 181
 Network, 195, 197
 obiekt

 Cloud, 233, 235
 Ethernet switch, 372
 obszar roboczy, 179

okno

 główne, 165
 importu plików, 191
 importu VMware, 183
 Node properties, 195, 233, 237
 Packet capture, 255
 Qemu settings, 190
 Topology Summary, 196, 198
 Usage, 192

opcje, 166
 Open project, 179

podłączenie
 routerów, 196
 wirtualnego przewodu, 185
 dwóch wirtualnych stacji, 184
 routera z siecią rzeczywistą, 231
 program Wireshark, 254
 przełączniki, 370
 przygotowanie serwera, 182
 Send anonymous crash reports, 167
 Send anonymous usage statistics, 167
 Servers Summary, 182
 Show special Ethernet interfaces, 237
 Show/Hide interface labels, 196
 sieć
 Frame Relay, 721, 728
 VLAN site-to-site, 748
 test ping, 188
 uruchomienie
 maszyny wirtualnej, 178
 sieci, 196
 ustawienia wirtualnego routera, 195
 VMware Virtual Machine, 179
 wybór
 maszyny wirtualnej, 180
 wzorca urządzenia, 189
 GRE, Generic Routing Encapsulation, 758
 GUA, Global Unicast Address, 661

H

haker, 823
 hash, 679
 hash value, 591
 hasło, 222
 do linii konsolowej, 225
 do trybu uprzywilejowanego, 229
 przechwytywanie, 591
 haszowanie, 742
 HDLC, High-Level Data Link Control, 708
 helper-address, 656, 658
 HIPS, host-based IPS, 862
 historia poleceń, 219
 HMAC, Hashed Message Authentication Code, 744

- HSRP, Hot Standby Router Protocol, 670
- konfiguracja
 - czasów, 677
 - protokołu, 671
 - priorytety, 676
 - uwierzytelnianie, 678
 - weryfikacja konfiguracji, 675
- HSWIC, High-Speed WIC, 454
- HTML, Hypertext Markup Language, 950
- HTTP, Hypertext Transfer Protocol, 89, 637
- I**
- IaaS, Infrastructure as a Service, 944
- IBSS, Independent Basic Service Set, 768
- ICMP, Internet Control Message Protocol, 109, 141, 151, 160, 257, 641
- IDEA, International Data Encryption Algorithm, 741
- identyfikator
 - area ID, 547
 - bridge ID, 427, 441
 - BSSID, 768
 - DLCI, 704
 - Extended System ID, 439
 - obszaru, 550, 598
 - root ID, 425, 441
 - router ID, 546, 558, 607
 - SSID, 768, 775
- IDS, Intrusion Detection Systems, 861
- IGRP, Interior Gateway Routing Protocol, 506
- IKE, Internet Key Exchange, 741
 - Phase 1, 747, 751
- implementacja VPN site-to-site, 747
- infrastruktura jako usługa, IaaS, 944
- initial exchange, 508
- instalacja programu CCP, 880
- integralność, integrity, 82
 - danych, 742
- interfejs, 37
 - BNC, 37
 - Console, 453
 - dynamic auto, 410
 - dynamic desirable, 410
 - GBIC, 353
 - GE, 453
 - konfiguracja, 226
 - LC, 76
 - loopback, 233, 236, 240, 330
 - opis, 226
 - pasywny, 532
 - Serial, 458
 - SFP, 354
 - stan
 - blocking, 434
 - forwarding, 434
 - learning, 434
 - listening, 434
 - status Desg, 438
 - trunk, 408, 410
 - tryb pracy
 - full duplex, 899
 - half duplex, 899
 - tunelowy, 761
 - w CCP, 885
 - wpis statyczny MAC, 385
- interfejsy
 - rozwiązywanie problemów, 899
- internet, 47, 56
- IOS, Internetwork Operating System, 187, 211
 - system pomocy, 216
 - zarządzanie systemem, 248
- IP SLA, 474
- IP, Internet Protocol, 101, 106, 257
- iperf, 905
- IPS, Intrusion Prevention System, 822, 860–862
 - analiza ruchu, 863
 - detekcja ruchu, 863
 - metoda
 - anomaly-based, 863
 - honeypot detection, 863
 - Policy-based, 863
 - signature-based, 863
- IPv4, *Patrz* adres IP
- IPv6, *Patrz* adres IPv6
- ISDN, Integrated Services Digital Network, 704
- IS-IS, Intermediate System to Intermediate System, 507
- J**
- język
 - HTML, 950
 - Jinja, 954
- K**
- kabel
 - koncentryczny, 71
 - konsolowy, 212
 - miedziany, copper cable, 61
 - światłowodowy, fiber-optic cable, 61
- karta
 - HSWIC, 454
 - loopback, 237
 - NME, 453
 - sieciowa, NIC, 38, 39, 52, 232, 233
 - adres MAC, 955
 - tryb pracy, 955
 - zmiana adresu MAC, 392
 - WAAS NME, 454
 - WIC, 453, 708
- keylogger, 826
- Kiwi Syslog, 911
 - ustawienia programu, 911
- klasy adresów, 645
 - A, 290
 - B, 286
 - C, 277
 - prywatnych, 261
- klient
 - DHCP, 991
 - iperf, 907
 - RADIUS, 867
 - serwer, 45
- kodowanie, encoding, 51
- kolejkowanie, 871, 872
- kolektor NetFlow, 921
- komenda, *Patrz* polecenie
- komunikacja, 49
 - bezprowadowa, wireless, 77
 - broadcast, 50
 - multicast, 50
 - rozgłoszeniowa, broadcast, 125
 - unicast, 49
 - w sieci Ethernet, 149

- komunikat
- Active router is local, 676
 - Bad secrets, 229
 - Change Cipher Spec, 763
 - Destination host unreachable, 481
 - DHCP Acknowledgment, 655
 - DHCP Discover, 655
 - DHCP Offer, 655, 853
 - DHCP Request, 655
 - ICMP packet debugging is on, 901
 - is directly connected, 511
 - MORE--, 217
 - nd-na, 641
 - Neighbor Solicitation, 327
 - Number of existing VLANs, 415
 - Preemption disabled, 675
 - RA, 334, 661
 - Redistributing: rip, 530
 - Request timed out, 236
 - Routing for Networks, 530
 - Routing Information Sources, 530
 - sending v2, 536
 - solicit, 662
 - Spanning tree enabled protocol
 - rstp, 443
 - startup-config is not present, 227
 - State is Active, 675
 - State is Master, 685
 - This bridge is the root, 428, 440
 - VTP Operating Mode, 415
- komunikaty
- debugowania, 901
 - ICMPv6, 322
 - protokołu OSPF, 562
 - typu 4, 564
- koncentrator, hub, 55, 341
- konfiguracja, 219
- adresu IP, 357
 - alternatywna OSPF, 554
 - automatyczne zapisywanie, 246
 - CCP, 883
 - czasów, 677, 686
 - czasu działania blokady, 387
 - domyślnej bramy, 357
 - enkapsulacji, 708
 - EtherChannel, 697
 - Frame Relay, 717
 - funkcjonalności span port, 925
 - GLBP, 691
 - HSRP, 671
- IKE Phase 1, 751
- interfejsów, 226
- loopback, 330
 - punkt – punkt, point-to-point, 717
 - routera, 318
 - wielopunkt, multipoint, 717
- kolektora NetFlow, 923
- kontrolera WLC, 801
- kopiowanie, 227
- do serwera TFTP, 241
 - z serwera TFTP, 244
 - z USB, 228
- MD5, 680
- multipoint, 719
- NAT na routerze, 647
- oprogramowania PRTG, 916
- OSPF wieloobszarowego, 595
- OSPF, 549, 984
- OSPFv3, 606
- passive-interface, 578, 596
- point-to-point, 728
- połączenia VPN GRE, 758
- Port Security, 381
- PPP, 712
- przełącznika, 355
- punktu dostępowego, 793, 801, 817
- PVST, 439
- RIP, 988
- RIPng, 332, 538
- RIPv1, 526
- RIPv2, 533
- routera, 222, 454
- routingu statycznego, 887
- rozszerzonych ACL, 629
- RSTP, 443
- running-config, 452
- serwera
- DHCP, 653
 - TFTP, 242
- sieci VLAN, 398
- SNMP, 910, 912
- SNMPv2c, 911
- SNMPv3, 914
- SSH, 368
- standardowych list ACL, 616
- startowa, 229
- syslog w CCP, 894
- track, 688
- tras statycznych, 334
- trasy domyślnej, 334, 336
- trybów interfejsów, 408
- urządzeń, 209
- usuwanie, 229
- VPN site-to-site, 749
- VRRP, 683
- vWLC, 804, 808
- kontrola przepływu, flow control, 143
- kontroler
- LAP, 775
 - SDN, 948
 - WLC, 775, 801
- koń trojański, 821, 825
- kopiowanie konfiguracji, 227
- do serwera, 241
 - z serwera TFTP, 244
 - z USB, 228
- koszt przesłania pakietów
- ustalenie ręczne, 573
 - zmiana wartości referencyjnej, 575
- koszty tras, 431
- kreator dodawania sprzętu, 236
- L**
- LACP, Link Aggregation Control Protocol, 696
- LAG, Link Aggregation Group, 802
- LAN, Local Area Network, 47
- LAP, Lightweight Access Point, 775
- LAR, Local Access Rate, 715
- LCP, Link Control Protocol, 708, 710
- liczby
- binarne, 264
 - szesnastkowe, 317
- linia
- dzierżawiona, 701
 - komend, command line, 53
 - konsolowa, 223
- link state, 510
- lista
- aktywnych ataków, 851
 - sąsiadów, 549
- listy ACL, 343, 613, 822
- komentarze, 621
 - nazywane, 616
 - reflective ACL, 616
 - rozszerzone, 616, 996
 - konfiguracja, 629

standardowe, 615
 adresy prywatne, 651
 konfiguracja, 616
 nazywane, 626
 ograniczanie dostępu, 628
 w IPv6, 640
 LLC, Logical Link Control, 111
 LLDP, Link Layer Discovery
 Protocol, 472
 LMI, Local Management Interface,
 715
 load balancing, 671
 logi systemowe, 908
 logowanie zdarzeń, 906
 lokalna sieć komputerowa, LAN, 47
 LSA, Link State Advertisement,
 546, 584
 typy pakietów, 595
 LSAck, Link State
 Acknowledgment, 546
 LSDB, Link State Database, 566
 LSP, Link State Packet, 545
 LSU, Link State Update, 546
 LWAPP, Lightweight Access Point
 Protocol, 775

Ł

ładunek, payload, 257

M

MAC, Media Access Control, 52,
 101, 111, 856
 malware, 826
 maska
 odwrotna, 550, 631
 podsieci, 263
 maszyna wirtualna, 168, 944
 ustawienia, 177
 vWLC, 802, 804
 w GNS3, 178
 MD5, 592, 679, 739
 konfiguracja, 680
 mechanizm
 CSMA/CA, 780, 789
 CSMA/CD, 780
 DFS, 772
 MIC, 797
 TPC, 773

medium
 bezprzewodowe, wireless, 61
 transmisyjne, 38, 61
 menedżer urządzeń, 213
 metody przekazywania informacji
 in-band, 908
 out-of-band, 908
 metryka, 575
 w OSPF, 568
 mGRE, Multipoint Generic
 Routing Encapsulation, 737
 MIB, Management Information
 Base, 910
 MIC, Message Integrity Check, 797
 Microsoft Network Monitor, 785
 okno
 główne, 787
 Network Interface
 Configuration, 787
 WiFi Scanning Options, 787
 przechwycone ramki, 788
 MIMO, Multiple Input Multiple
 Output, 776
 MITM, man-in-the-middle attack,
 799
 model
 AAA, 865
 best-effort, 875
 hierarchiczny, 342
 klient – serwer, 953
 OSI, 88
 punkt – punkt, 708
 sieci WAN, 708
 TCP/IP, 85
 zintegrowanych usług, 875
 zróżnicowanych usług, 875
 modele QoS, 875
 modem, 706
 modulacje sygnału, 773
 moduł SFP, 354
 modyfikowanie
 pola danych, 848
 ramki, 847
 monitorowanie routera, 892, 893
 MOTD, Message Of The Day, 226
 MPLS, Multi-Protocol Label
 Switching, 707
 MPO, Multi-fiber Push On, 74
 MT-RJ, Mechanical Transfer
 Registered Jack, 75

multicast, 49, 50
 multipoint, 717
 konfiguracja, 719

N

nadmiarowość, 423
 nagłówek, header, 257
 IPv6, 316
 pakietu IP, 258
 ramki wi-fi, 776, 792
 narzędzie uderzeniowe, 60
 NAT, Network Address
 Translation, 261, 645
 dla IPv6, 667
 dynamiczny, 650
 statyczny, 646
 z przeciążeniem, 651
 NAT64, 317
 NBAR, Network Based Application
 Recognition, 876
 NCP, Network Control Protocol, 710
 Neighbor Solicitation, 327
 NetFlow
 działanie, 921
 konfiguracja
 kolektora, 923
 na routerze, 921
 parametry pracy, 924
 wybór sensora, 924
 NGFW, Next Generation Firewall, 860
 NGIPS, Next-Generation Intrusion
 Prevention System, 860
 NHRP, Next Hop Resolution
 Protocol, 737
 NIC, Network Interface Controller, 52
 NME, Network Module, 453
 Non-designated port, port
 niededykowany, 430
 Npcap, 164
 NTP, Network Time Protocol, 462
 NVRAM, Non-Volatile Random
 Access Memory, 452

O

obiekt
 Cloud, 231, 235
 Ethernet switch, 372
 obszar zerowy, backbone area, 607

- odkodowanie, decoding, 51
 - odkrywanie, discover, 789
 - OFDM, Orthogonal Frequency Division Multiplexing, 773
 - okablowanie, 57
 - poziome, horizontal cabling, 63
 - szkieletowe, building backbone cabling, 63
 - okno
 - Choose protocol attack, 851
 - Połączenia sieciowe, 393
 - TCP, 146
 - opis interfejsu, 226
 - opóźnienie, delay, 40, 873
 - oprogramowanie
 - jako usługa, SaaS, 943
 - szpiegujące, 821
 - organizacje standaryzujące, 44
 - OSI
 - warstwa
 - aplikacji, 88
 - fizyczna, 114
 - łącza danych, 111
 - prezentacji, 91
 - sesji, 91
 - sieci, 101
 - transportu, 91
 - OSPF, Open Shortest Path First, 507, 549, 727
 - baza danych, 566
 - konfiguracja
 - alternatywna, 554
 - passive-interface, 578
 - protokołu, 549, 984
 - metryka, 568
 - polecenia weryfikujące, 603
 - polecenie area 0 authentication, 590
 - przepustowość, 569
 - relacje sąsiedztwa, 561
 - rozgłaszanie tras domyślnych, 578
 - równoważenie obciążenia, 557
 - sieć broadcast multiaccess, 579
 - stany interfejsów, 561
 - uwierzytelnianie, 590
 - wielooobszarowy, 593
 - konfiguracja, 595
 - rozgłaszanie tras domyślnych, 600
 - właściwości interfejsów, 567
 - OSPFv2, 545
 - pakiety hello, 546
 - OSPFv3, 606
 - konfiguracja, 606
 - overloaded NAT, 651
- P**
- PaaS, Platform as a Service, 944
 - PAGP, Port Aggregation Protocol, 696
 - pakiet
 - database description, 546
 - hello, 546, 562, 564
 - Backup Designated Router, 548
 - Designated Router, 548
 - ID obszaru, 547
 - identyfikator routera, 546
 - intervals, czasy, 547
 - List of Neighbors, 549
 - network mask, 548
 - router priority, 548
 - typ komunikatu, 546
 - IP, 257
 - LSA, 546, 584, 595
 - LSAck, 546
 - LSP, 545
 - LSR, 546
 - LSU, 546
 - SYN, 762
 - SYN/ACK, 762
 - pamięć
 - flash, 210, 211, 453
 - NVRAM, 210, 452
 - RAM, 221, 452
 - panel krosowniczy, patch panel, 59
 - PAP, Password Authentication Protocol, 711
 - pasmo, band, 39, 572
 - passive-interface, 533, 578, 592
 - PAT, Port Address Translation, 651
 - patchcord, 353
 - PCP, Payload Compression Protocol, 641
 - peer, 751, 755
 - permit, 613, 630, 638
 - pełta, 423
 - zwrotna, 236
 - phishing, 829
 - głosowy, 829
 - SMS, 829
 - platforma jako usługa, PaaS, 944
 - plik
 - konfiguracyjny, 210
 - z konfiguracją routera, 244
 - PMF, 798
 - podinterfejsy, subinterfaces, 483, 718
 - podłączenie do urządzenia, 212
 - podpis elektroniczny, 745
 - podsieci, 277, 294, 338
 - podział sieci, 277
 - klasa A, 290
 - klasa B, 286
 - klasa C, 277
 - liczba hostów
 - klasy A, 300
 - klasy B, 298
 - klasy C, 294
 - nierówna liczba hostów, 301
 - w IPv6, 338
 - PoE, Power over Ethernet, 342
 - point-to-point, 717
 - konfiguracja, 728
 - pola ramki wi-fi, 777, 793
 - polecenia
 - diagnostyczne, 340
 - niepoprawne, 218
 - testujące, 460
 - weryfikujące OSPF, 603
 - polecenie
 - accept-lifetime, 680
 - access-list ?, 617
 - access-list 1 permit any, 620
 - access-list 1 permit, 651
 - access-list 2 deny ?, 622
 - access-list 2 permit any, 623
 - alias exec, 464
 - alias, 253
 - arp -a, 349, 694
 - arp -d, 694
 - authentication, 749
 - auto secure, 867
 - auto-cost reference-bandwidth, 575
 - bandwidth, 569, 993
 - banner motd, 958
 - boot system flash:, 251
 - channel-group [] mode, 697
 - clear ip dhcp binding *, 656
 - clear ip ospf process, 559, 560, 604
 - clear mac-address-table dynamic, 351

- clock rate, 458, 733
- clock timezone, 462
- config-register 0x2102, 230
- config-register, 210
- configure terminal, 355
- confreg 0x2142, 230
- confreg, 210
- copy running-config startup-config, 228, 231, 362, 959
- copy running-config tftp, 243
- copy startup-config tftp, 960
- copy startup-config running-config, 230
- copy tftp flash:, 250, 252
- copy tftp running-config, 246
- copy tftp: flash:, 880
- crypto isakmp enable, 749
- crypto isakmp identity address, 751
- crypto isakmp key 0, 751
- crypto isakmp policy, 749
- crypto key generate rsa, 367, 459, 958
- crypto map [] ipsec-isakmp, 752
- debug capwap console cli, 817
- debug ip icmp, 901
- debug ip ospf adj, 604
- debug ip ospf packet, 562
- debug ip rip, 530, 535
- debug ipv6 rip, 543
- debug kron all, 248
- debug matm all, 351
- default-information originate, 531, 579, 601
- delete vlan.dat, 420
- deny ip host, 635
- deny ipv6 any any, 640
- deny, 627
- description, 959
- dir flash:, 251, 253
- dns-server, 653, 663
- do show access-list, 627
- do show clock, 357
- do show interface, 390
- do show mac address-table, 386
- duplex, 362
- enable secret, 222, 355, 455
- enable, 355
- encapsulation frame-relay, 728
- encapsulation dot1q, 483
- encapsulation frame-relay, 732
- encapsulation ppp, 713
- encryption, 749
- errdisable recovery cause psecure-violation, 391
- errdisable recovery interval, 391, 843
- exec-timeout 0 0, 455, 468
- extended ping, 902
- foreach address, 461
- frame-relay interface-dlci, 729
- frame-relay intf-type dce, 733
- frame-relay map [] broadcast, 723
- frame-relay route, 733
- frame-relay switching, 732
- group 5, 750
- hash, 750
- hostname SSH_TEST, 366
- hostname, 222, 355, 969
- interface [] point-to-point, 728
- interface fa0/0, 456
- interface loopback, 493
- interface range, 361
- interface vlan 1, 969
- interface, 227, 483, 487
- ip access-group 1 ?, 618
- ip access-group 1 out, 619
- ip access-list ?, 635
- ip access-list extended, 639, 659
- ip access-list standard 1, 625
- ip access-list standard LAN_NAT, 652
- ip access-list standard, 627
- ip address dhcp, 647, 959
- ip address, 227, 456, 817
- ip arp inspection, 857
- ip dhcp pool, 653
- ip dhcp snooping trust, 854
- ip dhcp snooping vlan 1, 853
- ip dhcp snooping, 854
- ip domain-lookup, 465
- ip domain-name, 366, 459, 958
- ip flow egress, 921
- ip flow ingress, 921
- ip flow-export version, 922
- ip helper-address, 658, 659
- ip http authentication local, 881
- ip http server, 636, 881
- ip nat inside source [] pool, 651
- ip nat outside, 647
- ip nat, 647
- ip ofsp dead-interval, 548
- ip ospf authentication-key, 590
- ip ospf cost, 573
- ip ospf hello-interval, 548
- ip ospf message-digest-key [] md5, 592
- ip ospf network point-to-point, 589
- ip ospf priority, 549
- ip ospf, 555
- ip rcmd remote-host, 469
- ip rcmd rsh-enable, 469
- ip route, 672
- ip sla, 474
- ip ssh version 2, 467, 958
- ipconfig /all, 53, 955
- ipconfig /displaydns, 133
- ipconfig /flushdns, 134
- ipconfig /renew, 657
- ipconfig -all, 392
- ipv6 access-list, 642, 643
- ipv6 address dhcp, 374
- ipv6 address, 329
- ipv6 dhcp pool, 665
- ipv6 dhcp relay destination, 667
- ipv6 enable, 322
- ipv6 nd other-config-flag, 663, 664
- ipv6 rip [] enable, 332, 608
- ipv6 route, 334
- ipv6 router ospf 1, 609
- ipv6 router rip, 609
- ipv6 traffic-filter [] in, 642
- ipv6 unicast-routing, 333, 661, 665
- key, 680
- key-string, 680
- kron policy-list, 247
- lifetime 86400, 750
- line console 0, 455
- line console, 223
- line vty 0 15, 356
- line vty, 223
- lldp transmit i lldp receive, 472
- logging synchronous level, 909
- logging synchronous, 455
- login local, 367, 460, 959
- matm all, 351
- monitor session [] source, 927
- netsh interface ipv6 show neighbors, 328
- netstat, 99
- network, 528, 653, 984
- no access-list 1, 625

- polecenie
 no auto-summary, 536
 no cdp advertise-v2, 471
 no cdp enable, 472
 no debug ip icmp, 901
 no debug matm all, 351
 no ip address, 483
 no ip dhcp snooping
 information option, 858
 no ip domain-lookup, 464
 no ipv6 nd managed-config-
 flag, 661
 no passive-interface, 578
 no service dhcp, 654
 no service timestamps, 909
 no setup express, 346
 no shutdown, 390, 899
 no spanning-tree cost, 432
 no vlan, 402
 no access-list 100, 632
 nslookup, 137
 ntp authenticate, 464
 ntp server, 462, 463
 ntp trusted-key, 464
 occurrence, 247
 passive-interface default, 578
 passive-interface, 533
 password, 223, 455
 permit any any, 643
 permit any, 627
 permit ipv6, 644
 permit tcp, 996
 ping ?, 902
 ping, 260, 340
 ppp authentication chap, 714
 redistribute ospf, 989
 redistribute rip, 609
 redistribute static subnets
 metric 1, 602
 reload cancel, 231
 reload in, 231
 reload, 230
 router ospf 1, 726
 router ospf, 550
 router rip, 528, 980
 router-id, 559, 607, 991
 service dhcp, 654
 service password-encryption,
 224, 958
 set transform, 752
 show access-lists, 618, 619
 show cdp entry, 471
 show cdp interface, 471
 show cdp neighbors detail, 470
 show cdp neighbors, 470, 606, 975
 show clock, 246, 357, 462
 show controllers serial, 459
 show controllers, 710
 show crypto ipsec sa, 753
 show crypto isakmp peers, 754,
 756
 show crypto isakmp policy, 750
 show crypto isakmp sa, 753
 show crypto map, 753
 show etherchannel summary, 697
 show etherchannel summary, 698
 show flash, 420
 show frame-relay lmi, 725
 show frame-relay map, 734
 show glbp brief, 693
 show glbp, 692
 show interface brief | json, 951
 show interface brief | xml, 951
 show interface trunk, 405, 407
 show interface, 390, 406, 900
 show ip interface brief, 458
 show ip arp inspection, 858
 show ip cache flow, 922
 show ip dhcp binding, 654, 657,
 849
 show ip dhcp conflict, 658
 show ip dhcp pool, 654
 show ip dhcp snooping, 854
 show ip flow export, 923
 show ip interface brief, 226, 359,
 361, 473, 480, 493, 698, 761
 show ip interface, 620
 show ip nat translations, 652
 show ip ospf database, 566
 show ip ospf interface brief, 567,
 603, 986
 show ip ospf interface, 567
 show ip ospf neighbor, 555, 561,
 587, 597
 show ip protocols, 537, 551, 603
 show ip route connected, 511
 show ip route ospf, 553, 572, 734
 show ip route static, 494
 show ip route, 154, 480, 491,
 726, 760, 976
 show ip sla statistics, 475
 show ip ssh, 370, 467
 show ipv6 dhcp pool, 664, 665
 show ipv6 int brief, 330
 show ipv6 int, 324
 show ipv6 ospf interface brief,
 608, 609
 show ipv6 interface, 332, 374
 show ipv6 ospf neighbor, 609
 show ipv6 protocols, 539, 540
 show ipv6 rip database, 543
 show ipv6 route rip, 540, 542
 show ipv6 route static, 337
 show ipv6 route, 335, 539
 show kron schedule, 247
 show mac address-table, 349
 show mac-address-table
 interface, 352
 show mac-address-table |
 include, 352
 show ntp association, 463
 show port-security interface,
 383, 384
 show port-security, 380, 386,
 389, 967
 show post, 211
 show processes cpu monitor, 838
 show processes, 351
 show run | section crypto, 750
 show running | incl access, 621
 show running | section include
 con|vty, 224
 show running-config | begin
 line vty, 356
 show running-config | incl
 access-list 1, 624
 show running-config | section
 line, 468
 show running-config interface,
 457
 show running-config, 223
 show session, 460
 show snmp community, 914
 show snmp user, 915
 show snmp, 913, 916
 show spanning-tree summary,
 841
 show spanning-tree, 426–429,
 437, 695, 838
 show standby, 675, 682
 show startup-config, 228
 show switch, 377
 show users, 465, 628

- show version, 210, 219
- show vlan brief, 401, 418, 479, 963
- show vlan, 358, 398
- show vrrp, 685, 690
- show vtp password, 418
- show vtp status, 414, 416, 422
- show VTP status, 415
- shutdown, 682
- snmp-server community [] ro, 912
- snmp-server contact, 912
- snmp-server group, 915
- snmp-server host, 912
- snmp-server location, 912
- snmp-server view, 914
- spanning-tree [] root primary, 440
- spanning-tree bpduguard
 - enable, 842
- spanning-tree cost, 432
- spanning-tree mode rapid-pvst, 443
- spanning-tree portfast
 - bpduguard default, 841
- spanning-tree portfast, 436, 842, 964
- spanning-tree vlan [] root
 - primary, 966
- standby [] authentication ?, 678
- standby [] authentication md5
 - key-chain, 681
- standby [] preempt, 676
- standby 1 timers ?, 677
- static, 388
- sudo apt install dsniff, 836
- sudo ifconfig, 836
- sudo ip route, 836
- sudo netdiscover -r, 836
- switchport access vlan, 401, 479, 969
- switchport mode access, 381, 401, 410, 479, 969
- switchport mode dynamic
 - desirable, 410
- switchport mode trunk native
 - vlan 999, 407
- switchport mode trunk, 405, 410, 484
- switchport nonegotiate, 410
- switchport port-security
 - mac-address ?, 382
- switchport port-security
 - mac-address sticky, 382
- switchport port-security max 1, 967
- switchport port-security
 - maximum 1, 383
- switchport port-security
 - violation shutdown, 967
- switchport port-security
 - violation shutdown, 967
- switchport trunk allowed vlan, 407
- switchport trunk encapsulation
 - dot1q, 405, 970
- tclquit, 462
- tclsh, 461
- telnet, 465
- tftp-server flash:, 253
- trace, 481
- traceroute, 340, 460
- tracert, 554
- track [] line-protocol, 689
- transport input ssh, 367, 459, 465, 959
- transport input telnet ssh, 465
- tunnel destination, 759
- tunnel source, 759
- tunnel mode gre ip, 759
- Type, 388
- undebg all, 351, 544, 901
- undebg, 531
- username [] autocommand
 - menu, 473
- username [] password, 713
- username [] privilege [] secret, 881
- version 2, 534
- vlan, 400, 963
- vrrp [] ip, 683
- vrrp [] timers advertise msec, 686
- vtp domain, 416, 962
- vtp mode client, 415, 962
- vtp password, 418, 962
- vtp pruning, 422
- write memory, 247
- yersinia -G, 838
- połączenie
 - ad hoc, 781
 - optyczne, optical fiber, 708
 - punkt – punkt, 588
 - site-to-site, 735
 - SSL/TLS, 762
 - trunk, 381, 396, 403, 407, 844
- VPN GRE, 758
- VPN remote access, 761
- wi-fi
 - asocjacja, associate, 790
 - odkrywanie, discover, 789
 - tryb aktywny, 790
 - tryb pasywny, 791
 - uwierzytelnianie,
 - authenticate, 789
- wirtualne
 - przełączane, SVC, 704
 - stałe, PVC, 704
- zdalny dostęp, remote access, 735
- pomoc, 216
- POP3, Post Office Protocol, 90
- port, 98
 - alternatywny, 430, 443
 - AUX, 453
 - brzegowy, 446
 - designated, 433
 - desygnowany, 430, 443
 - dystrybucyjny, distribution
 - system port, 802
 - główny, 430, 443
 - konsolowy, console port, 802
 - niedesygnowany, 430
 - Port Security, 379
 - konfiguracja, 381
 - typu trunk, 402
 - zapasowy, 443
- PortFast, 435, 436, 446
- potwierdzenie LSack, 586
- poufność, confidentiality, 82
- Power-on Self Test, 209
- PPP, Point-to-Point Protocol, 705, 710
 - konfiguracja, 712
 - uwierzytelnianie, 713
- prędkość, 43
- problemy z interfejsami, 899
- proces
 - EUI-64, 320
 - wymiany kluczy, 366
- program
 - antywirusowy, 861
 - CCP, 879
 - CCP Express, 881
 - Cisco Feature Navigator, 249
 - Cisco Prime NAM, 941
 - Cpulimit, 165

- program
 - Dynamips, 164
 - GNS3, 161
 - iperf, 905
 - Kiwi Syslog, 911
 - Microsoft Network Monitor, 785
 - NetFlow, 921
 - Npcap, 164
 - PRTG, 916
 - QEMU, 164
 - Solar Winds Response, 164
 - SuperPutty, 165
 - Tftpd64, 242
 - TightVNC Viewer, 165
 - VMware Workstation, 167
 - VPCS, 165
 - VirtualBox, 167
 - vWLC, 802
 - Wireshark, 127
 - Yersinia, 845
- projektowanie sieci, 929
 - bezpieczeństwo, 935
 - dokumentacja, 939
 - harmonogram, 934
 - określenie wymagań, 935
 - projekt
 - fizyczny, 933
 - logiczny, 933
 - schemat Cisco PPDIIO, 933
- protokoły
 - bezklasowe, 545
 - distance vector, 508
 - hashujące, 739
 - IPsec, 739
 - klasowe, 525
 - komunikacji sieciowej, 42
 - link state, 510
 - negocjacyjne, 739
 - ochrony procesu wymiany
 - kluczy, 739
 - redundancji, 670
 - routingu, 42
 - routingu dynamicznego, 506, 507
 - symetrycznego szyfrowania, 739
 - szyfrowania, 739
 - wykrywania usług, 42
- protokół 802.1.x, 866
 - AHP, 641
 - ARP, 121, 146, 448
 - BGP, 507
 - CAPWAP, 795
 - CCMP, 798
 - CDP, 469, 606
 - CHAP, 711
 - DHCP, 647
 - Diffiego-Hellmana, 739
 - distance vector, 526
 - DTLS, 796
 - DTP, 381, 408
 - EAP, 867
 - EIGRP, 506, 554
 - enkapsulacji, encapsulation
 - protocol, 736
 - ESP, 641
 - GLBP, 671, 691
 - HSRP, 670
 - HTTP, 638
 - ICMP, 109, 141, 160, 257, 641
 - IGRP, 506
 - IKE, 741
 - IPv4, 106, 257
 - IPv6, 315
 - IS-IS, 507
 - LACP, 696
 - LCP, 708, 710
 - LLDP, 472
 - LWAPP, 775
 - mGRE, 737
 - MPLS, 707
 - NCP, 710
 - NHRP, 737
 - NTP, 462
 - operatora, provider protocol, 736
 - OSPF, 507
 - OSPFv2, 545
 - OSPFv3, 606
 - PAGP, 696
 - PAP, 711
 - PCP, 641
 - PPP, 705, 710
 - przenoszenia, transfer protocol,
 - 736
 - PVST, 436
 - RIP, 506, 512, 516
 - RIPng, 332, 538
 - RIPv1, 525
 - RIPv2, 506, 533
 - RSTP, 442
 - SDEE, 863
 - sieciowy, 42
 - SNMP, 910
 - SSH, 363
 - SSL, 365, 761
 - SSL/TLS, 762
 - STP, 423, 695
 - TCP, 92, 142
 - telnet, 363
 - TLS, 762
 - UDP, 95, 139
 - VRRP, 671
 - VTP, 412
 - X.25, 706
- PRTG, 916
 - konfiguracja, 916
 - okno główne, 917
 - okno ustawień urzędzenia, 918
- przechwytywanie pakietów, 131
- przeciążenie, congestion, 873
- przekierowywanie portów, 826
- przełączanie
 - obwodów, 701
 - pakietów, 702
 - procesów, process switching, 450
 - szybkie, CEF, 451
 - szybkie, fast switching, 451
- przełącznik, switch, 33, 54, 341, 775
 - adres IP, 357
 - age time, 347
 - autouruchamianie interfejsu, 391
 - cut-through, 354
 - dioda
 - RPS, 345
 - stanu portów, 345
 - systemowa, 345
 - trybu portów, 345
 - dotatkowe interfejsy, 353
 - emulowany w GNS3, 370
 - fast-forward switching, 354
 - fragment-free switching, 354
 - Frame Relay, 720, 732
 - interfejsy
 - FastEthernet, 357
 - GigabitEthernet, 357
 - jednomodułowy, 344
 - komunikat ostrzegający, 357
 - konfiguracja
 - bramy domyślnej, 357
 - Port Security, 381
 - metody buforowania, 355
 - modułarny, 344
 - negocjacja typu połączenia, 411
 - obiekt Ethernet switch, 372
 - podłączanie urządzeń, 353

- przełącznik, switch
- podstawowa konfiguracja, 355
 - Port Security, 379
 - pracujący w stosie, 375
 - protokół
 - PVST, 436
 - RSTP, 442
 - STP, 423
 - VTP, 413
 - przełączanie ramek, 354
 - przycisk MODE, 346
 - przypisanie adresu IPv6, 374
 - root bridge, 431, 433, 439
 - schemat współpracy, 947
 - sprawdzanie ramki, 355
 - stack master, 376
 - stany portów, 434
 - status SSH, 370
 - statusy STP, 434
 - statyczne dodanie wpisu, 352
 - store-and-forward, 354
 - tablica
 - adresów MAC, 346
 - przylegania, 486
 - tryb pracy
 - client, 413
 - transparent, 413
 - server, 413
 - VTP Pruning, 421
 - warstwy 2., 344
 - warstwy 3., 486, 946
 - warstwy dostępu, 343
 - warstwy dystrybucji, 343
 - warstwy rdzenia, 343
 - włączenie protokołu SSH, 363
 - wyłączanie interfejsów, 361
 - zapisanie konfiguracji, 362
 - zdarzenie bezpieczeństwa, 388, 390
 - zmiana
 - parametrów interfejsów, 361
 - szybkości interfejsów, 362
- przepływność
- gwarantowana minimalna, 704
 - niegwarantowana maksymalna, 704
- przepustowość, bandwidth, 40, 569, 873
- przepuszczenie, permit, 613
- przeszukiwanie tablicy routingu, 513
- przewód
- DB60-DB60, 709
 - miedziany, 64
 - światłowodowy, 71
- przydzielanie adresu IPv4, 655
- PSK, Pre-Shared Key, 746
- punkt dostępowy, access point, 768, 775, 784
- adres MAC, 782
 - etapy połączenia, 789
 - komunikacja z WLC, 812
 - konfiguracja, 793, 801, 817
 - tryb pracy
 - autonomous, 775
 - controller-based, 775
 - w vWLC, 811
- PVC, Permanent Virtual Circuits, 704, 716
- PVRST, Per-VLAN Rapid Spanning Tree, 436
- PVST, Per-VLAN Spanning Tree, 427, 436
- konfiguracja, 439
- ## Q
- QEMU, 164
- QoS, Quality of Service, 82, 398, 871
- modele, 875
 - wdrażanie, 875
- Quiet Mode, 755
- ## R
- RA, Router Advertisement, 661
- RADIUS, 866
- RAM, Random Access Memory, 452
- ramka wi-fi, 776
- ACK, 780, 781
 - association request, 778
 - association response, 779
 - beacon, 779, 791
 - CSMA/CA, 780
 - CTS, 780
 - deauthentication, 780
 - disassociation, 780
 - FromDS, 781
 - podtypy, 779
 - pola adresów, 781
- pole
- Adres 1, 778
 - Czas trwania, 777
 - Dane, 785
 - ECN, 877
 - DSCP, 878
 - Frame Body, 791
 - IPP, 877
 - kontrolne ramki, 777
 - nagłówka, 792
 - Podtyp ramki, 778
 - Powtórz, 785
 - Sekwencja sterująca, 778
 - Wersja protokołu, 778
 - Więcej danych, 785
 - Wi-Fi Traffic Identifier, 876
 - Zabezpieczenia, 785
 - Zarezerwowane, 785
 - Zarządzanie energią, 785
- probe request, 779
- probe response, 782, 790
- reassociation request, 779
- reassociation response, 779
- RTS, 780
- Source address, 782
- ToDS, 781
- Transmitter address, 782
- typ ramki, 778
- ramki
- BPDU, 425
 - DTP, 411
 - ethernetowe, 112, 116, 396
 - rozgłoszeniowe, broadcast, 421, 423
 - ARP, 147, 151, 152
 - ransomware, 826
 - raportowanie, 906
 - RC, Rives Cipher, 741
 - redundancja, 343, 669
 - redystrybucja, 988
 - OSPF, 609
 - RIP, redistribute rip, 609
 - RIPng, 610
 - tras, 609
 - domyślnych, 600
 - statycznych, 602
 - rejestr konfiguracji, configuration register, 209
 - rekonesans, 825
 - relacje sąsiedztwa, 551, 561
 - statusy urządzeń, 586

- remark, 630
- resetowanie hasła, 229
- restart routera, 230
- RESTful API, 953
- reverse engineering, 310
- RFC, 34
- RIP, Routing Information Protocol,
 - 506, 512, 516
 - konfiguracja protokołu, 988
 - wymiana komunikatów, 530
- RIPng, 332, 538
 - konfiguracja protokołu, 538
- RIPv1
 - działanie protokołu, 525
 - konfiguracja protokołu, 526
- RIPv2
 - konfiguracja protokołu, 533
- robak, 821, 825
- rollover, 69
- root bridge, 840
- root port, port główny, 430, 443
- rootkit, 827
- router, 55, 33
 - ABR, 594
 - sumaryzacja tras, 599
 - BDR, backup designated,
 - zapasowy desygnowany, 580, 609
 - Cisco 1941, 453
 - Cisco 3745, 477
 - Cisco 7200, 527
 - Cisco IP SLA, 474
 - DR, designated, desygnowany,
 - 580, 609
 - połączenie punkt – punkt, 588
 - wybór, 580
 - zmiana, 582
 - drother, 609
 - router-on-a-stick, 398, 482
 - z serii 2800, 212
- routery
 - automatyczne zapisywanie
 - konfiguracji, 246
 - budowa, 452
 - czas bezczynności, 467
 - distance vector, 509
 - działanie, 447
 - informacja
 - o interfejsach, 471
 - o sąsiedzie, 471
 - interfejs Serial, 458
 - jako agent przekazujący, 666
 - jako serwer DHCP, 653
 - jako serwer DHCPv6, 660
 - bezstanowy, 662
 - stanowy, 664
 - konfiguracja
 - interfejsu, 318, 717
 - NAT, 647
 - link state, 510
 - mechanizmy przełączania, 450
 - najdłuższe dopasowanie, 499
 - obliczanie trasy, 506
 - odwzorowanie nazw
 - domenowych, 464
 - pakiety hello, 546
 - polecenia testujące, 460
 - podłączanie
 - obiektu Cloud, 239
 - w GNS3, 196
 - połączenie
 - site-to-site, 735
 - z siecią rzeczywistą, 231
 - proces otrzymywania ramki, 154
 - protokół
 - ARP, 460
 - CDP, 469
 - LLDP, 472
 - NTP, 462
 - OSPFv2, 545
 - OSPFv3, 606
 - RIP, 525, 533
 - RIPng, 538
 - RIPv1, 526
 - SSH, 459
 - przechwycona ramka, 156
 - przesyłanie ramki, 158
 - restart, 230
 - rodzaje pakietów, 545
 - serwer NTP, 463
 - tablica routingu, 447, 510
 - wpisy, 449
 - tworzenie aliasu, 464
 - uruchomienie TFTP, 251
 - w CCP, 890
 - wartości AD, 500
 - własne menu, 473
 - wstępna konfiguracja, 222, 454
 - wybór trasy, 496, 499
 - wyłączenie protokołu CDP, 472
 - wymiana
 - informacji, 562
 - pakietów LSA, 584
 - wysyłanie komunikatów, 466
 - wyświetlanie listy
 - użytkowników, 465
 - zdalne zarządzanie, 469
 - zmiana identyfikatora, 558
- routing, *Patrz także* trasy
 - metoda klasyczna, 478
 - pomiędzy sieciami VLAN, 477
 - router-on-a-stick, 482
 - dynamiczny, 505, 525
 - protokoły, 506, 507
 - OSPFv2, 545
 - OSPFv3, 606
 - RIPng, 538
 - RIPv1, 526
 - RIPv2, 533
 - statyczny, 489
- rozgłaszanie tras domyślnych, 531, 578
- rozległa sieć komputerowa, WAN, 47
- rozwiązywanie problemów
 - adresacja IP, 942
 - analizatory protokołów, 941
 - błędna konfiguracja ACL, 942
 - błędy okablowania, 942
 - Cisco Prime NAM, 941
 - dziel i zwyciężaj, 940
 - od ogółu do szczegółu, 940
 - od szczegółu do ogółu, 940
 - podstawienie innego
 - urządzenia, 941
 - utrata połączenia, 942
 - wąskie gardło, 942
 - równoważenie obciążenia, load balancing, 557
 - RPS, Redundant Power Supply, 345
 - RSA, 746
 - RSTP, Rapid Spanning Tree Protocol, 442
 - konfiguracja, 443
 - porty, 443
 - stan blocking, 442
 - stan discarding, odrzucanie, 442
 - RTS, request to send, 780
 - ruch
 - HTTP, 637
 - inbound, przychodzący, 618
 - outbound, wychodzący, 618

S

- SaaS, Software as a Service, 943
- SAN, 47
- SDEE, Security Device Event Exchange, 863
- SDH, Synchronous Digital Hierarchy, 702
- SDN controller, 948
- SDN, Software-Defined Network, 946
- segmentacja, 144
- sekwencyjne przesyłanie danych, 144
- serwer, server, 54
 - bezstanowy DHCPv6, 662, 664 czasu, 463
 - DHCP, 333, 647, 653, 850
 - DHCPv6, 660
 - DNS, 137
 - autorytatywne, 142
 - lokalne, 142
 - iperf, 906
 - NAS, 765
 - NHRP, 737
 - RADIUS, 818
 - stanowy DHCPv6, 664, 665
 - syslog, 892
 - TFTP, 241
 - TLD, 142
 - VPN, 746
- serwery domeny głównej, 142
- SFP, Small Form Factor Plugable, 353
- SHA, Secure Hash Algorithm, 739, 742
- sieci
 - automatyzacja, 943, 949
 - bezpośrednio podłączone, include-connected, 609
 - bezczynowe, 46, 77, 767
 - ad hoc, 781
 - ataki DoS, 799
 - ataki MITM, 799
 - bezpieczeństwo, 797
 - częstotliwości, 772
 - format ramki, 776
 - identyfikator SSID, 775, 792
 - kanały, 772
 - mechanizm CSMA/CA, 789
 - mechanizm TPC, 773
 - modulacje sygnału, 773
 - pasma, 771
 - połączenie, 789
 - projektowanie, 800
 - przechwytywanie ramek, 785
 - punkt dostępowy, 775, 784
 - sposób działania, 769
 - standardy, 773
 - szyfrowanie, 796
 - tryby pracy, 768
 - ustawienie nazwy, 794
 - ustawienie trybu działania, 794
 - uwierzytelnianie, 795
 - VLAN, 768
 - WDS, 784
 - WLAN, 767
 - WPAN, 767
 - WWAN, 767
 - zastosowanie, 800
- dokumentacja projektowa, 939
- konwergentne, 81
- model
 - dwuwarstwowy, 929
 - trójwarstwowy, 931
- niekonwergentne, 81
- projekt
 - fizyczny, 933
 - logiczny, 933
- projektowanie, 929
- rozwiązywanie problemów, 940
- wielodostępowe
 - protokół OSPF, 579
- wi-fi, 767
- wirtualizacja, 943
- sieć
 - BSS, 768
 - Ethernet, 116
 - Frame Relay, 714
 - internet, 47, 56, 904
 - IPv6, 641
 - komputerowa, 35
 - domowa, 36, 80
 - NBAR, 876
 - OSPF wieloobszarowa, 594
 - OSPFv3, 606
 - punkt – punkt, point-to-point, 579, 587, 709
 - SAN, 47
 - SDN, 946
 - typu broadcast multiaccess, 579
 - VLAN, 357, 395
 - VPN, 735
 - WAN, 701
 - signature matching, 863
 - site-to-site
 - tunel GRE, 758
 - skalowalność, scalability, 83
 - skrętka
 - ekranowana, 66
 - nieekranowana, 65
 - skrótów klawiaturowe, 218
 - SLAAC, Stateless Address Autoconfiguration, 333, , 660 661
 - SMTP, Simple Mail Transport Protocol, 90, 910
 - działanie, 910
 - konfiguracja, 910, 912
 - ustawienia dla urządzenia, 919
 - SNMP Object Navigator, 915
 - SNMPv2c
 - konfiguracja, 911
 - SNMPv3
 - konfiguracja, 914
 - SOHO, small office and home office networks, 80
 - Solar Winds Response, 164
 - SONET, Synchronous Optical Networking, 702
 - span port
 - konfiguracja funkcjonalności, 925
 - SPF, Shortest Path First, 545
 - sprawdzanie komunikacji, 902
 - spyware, 821, 826
 - SSH, secure shell, 363, 459
 - SSID, Service Set Identifier, 768
 - SSL, Secure Sockets Layer, 90, 761
 - Change Cipher, 762
 - handshake, 762
 - stacja robocza, workstation, 52
 - stan
 - Active, 682
 - discarding, odrzucanie, 442
 - drother, 582
 - forwarding, 434
 - learning, 434
 - Standby, 682
 - standardy sieci wi-fi, 773
 - stany portów, 434
 - static NAT, 646
 - status
 - 2-WAY/DROTHER, 587
 - backup, 691
 - FULL/DR, 587

- status
 - interfejsu OSPF
 - 2WAY, 561
 - Down, 561
 - Exchange, 561
 - ExStart, 561
 - Init, 561
 - Loading, 561
 - Master, 690
 - połączenia VPN, 765
 - statystyki IP SLA, 475
 - stos, stack, 375
 - STP, Spanning Tree Protocol, 423, 695, 830, 837
 - algorytm działania, 425
 - działanie protokołu, 425
 - PortFast, 435
 - rodzaje portów, 429
 - rozszerzenie PVST, 436
 - STP status
 - blocking, blokowanie, 434
 - forwarding, przekazywanie, 434
 - learning, uczenie się, 434
 - listening, nasłuchiwanie, 434
 - sumaryzacja
 - sieci, 337
 - tras, 599
 - tras statycznych, 493
 - trzech podsieci, 495
 - SuperPutty, 165, 199
 - Commands, 200
 - Host, 214
 - konfiguracja programu, 199
 - okno główne, 199, 214
 - połączenie z urządzeniem, 199
 - Protocol, 214
 - Rename Tab, 201
 - Serial, 214
 - wydanie polecenia wielu urządzeniom, 200
 - zmiana nazwy zakładek, 200
 - suplikant, 866
 - SVC, Switched Virtual Circuits, 704
 - symulator Cisco Packet Tracer, 161, 201
 - SYN, 142
 - SYN-ACK, 142
 - syslog, 908
 - system
 - binarny, 43
 - firewall, 861
 - IDS, 861
 - IPS, 860–862
 - NGIPS, 860
 - operacyjny IOS, 211
 - pomocy, 216
 - szablony, 954
 - szybkość pobierania, 905
 - szyfrowanie danych, encryption, 82, 225, 798
 - metoda
 - asymetryczna, 741
 - symetryczna, 740
 - w VPN, 738
- Ś**
- światłowód
 - jednomodowy, single-mode fiber, 71
 - wielomodowy, multi-mode fiber, 71
- T**
- tablica
 - ARP, 149, 155, 856
 - DNS, 133
 - FIB, 946
 - MAC, 346, 856
 - czyszczenie, 351
 - obserwacja czynności, 351
 - statyczne dodanie wpisu, 352
 - wyświetlanie, 349
 - wyświetlenie, 386
 - przynależności, 451
 - RIB, 946
 - routingu, routing table, 154, 157, 333, 447
 - cold start, 508
 - initial exchange, 508
 - level 1 parent route, 512
 - level 1 route, 512
 - najdłuższe dopasowanie, 499
 - odtworzenie topologii sieci, 513, 519
 - proces przeszukiwania, 513
 - relacje sąsiedztwa, 551
 - routera, 510
 - stacji roboczej, 521
 - ultimate routes, trasy ostateczne, 512
 - wpis connected,
 - bezpośrednio podłączone, 449, 511
 - wpis default route, 496
 - wpis dynamic, dynamiczny, 449
 - wpis L, local, 511
 - wpis O*E2, 601
 - wpis R, RIP, 511
 - wpis static, statyczny, 449, 491
 - translacji, 652
 - TCP, Transmission Control Protocol, 92
 - kontrola przepływu, 143
 - uzgodnienie trójstopniowe, 142
 - TCP/IP
 - warstwa
 - aplikacji, 86
 - dostępu do sieci, 87
 - internetowa, 87
 - transportu, 87
 - technologia
 - ATM, 707
 - DSL, 705
 - DMVPN, 737
 - DWDM, 702
 - Frame Relay, 703, 714
 - GRE, 758
 - ISDN, 704
 - linia dzierżawiona, 701
 - przełączania
 - obwodów, 701
 - pakietów, 702
 - SDH, 702
 - SONET, 702
 - VPN, 735
 - WDS, 784
 - X.25, 706
 - telnet, 363
 - teredo, 317
 - test POST, 209
 - testowanie
 - łącza internetowego, 904
 - połączenia w sieci lokalnej, 905
 - tethering, 776
 - TFTP, 241
 - konfiguracja serwera, 242
 - kopiowanie konfiguracji, 241, 244
 - uruchamianie na routerze, 251
 - Tftpd64, 241

- three-way handshake, 142
 - analiza, 145
 - TightVNC Viewer, 165
 - TKIP, Temporal Key Integrity Protocol, 797
 - TLD, Top Level Domain servers, 142
 - TLS, Transport Layer Security, 762
 - ToDS, To Distribution System, 781
 - topologia
 - dual-homed, 703
 - fizyczna, physical topology, 78
 - full mesh, 716
 - fully meshed topology, 703
 - gwiazdy, 78
 - hub-and-spoke, 702, 716, 718
 - magistrali, 79
 - partial mesh, 717
 - partially meshed topology, 703
 - pierścienia, 79
 - point-to-point, 702
 - PVC, 716
 - rozszerzonej gwiazdy, 79
 - TPC, Transmit Power Control, 773
 - track, 681
 - transfer, transfer, 40
 - translacja
 - adresów IPv4, *Patrz* NAT
 - dynamiczna, 650
 - stacyczna, 646
 - z przeciążeniem, 651
 - transmisja bezprzewodowa, 77
 - transmitery sieciowe, network transmitter, 83
 - trasa Floating Static Route, 499, 503
 - trasy, *Patrz także* routing
 - bezpośrednio podłączone, 511
 - koszty połączeń, 431
 - domyślne, 334, 336, 496
 - rozgłaszanie, 531, 578, 600
 - dynamiczne, 505
 - external, 610
 - nadrzędne pierwszego poziomu, 512
 - ostateczne, 512
 - pierwszego poziomu, 512
 - prezentujące najdłuższe dopasowanie, 499
 - redundantne, 573
 - stacyczne, 334, 489
 - redystrybucja, 602
 - sumaryzacja, 493, 599
 - trunk, 396, 402, 403, 407, 408
 - tryb
 - Bridge, 232
 - Bridged, 232
 - desirable, 697
 - global configuration, 215
 - passive, 697
 - pracy
 - IBSS, 768
 - punkt dostępowy, access point, 768
 - privileged executive, 215
 - user executive, 215
 - TTL, Time To Live, 157
 - tunel
 - CAPWAP, 796
 - GRE w site-to-site, 758
 - VPN SSL, 761
 - VPN, 736
 - tunelowanie, tunneling, 317, 736
 - tworzenie
 - aliasu, 464
 - konta użytkownika, 459
 - maszyny wirtualnej, 168
 - sieci WLAN, 809
 - szablonów, 954
 - typy
 - anten, 775
 - pakietów LSA, 595
 - sieci VPN, 745
 - szyfrowania, 225
- U**
- UDP, User Datagram Protocol, 95, 139
 - unicast, 49
 - URI, Uniform Resource Identifier, 953
 - URL, Uniform Resource Locator, 953
 - URL filtering, 860
 - URN, Uniform Resource Name, 953
 - uruchamianie urządzenia, 209
 - urządzenia
 - beziprzewodowe, 774
 - inteligentne, smart device, 83
 - konfiguracja, 209
 - nadawcze, transmitter, 767
 - odbiorcze, receiver, 767
 - tyby pracy, 215
 - uruchamianie, 209
 - zarządzanie, 214
 - USB, 228
 - usługa, 38
 - DHCP, 654, 655
 - SLAAC, 660
 - syslog, 908
 - usługi
 - bezzstanowe, stateless services, 661
 - chmury, 943
 - stanowe, statefull services, 661
 - ustawienia maszyny wirtualnej, 177
 - usuwanie konfiguracji
 - startowej, 229
 - VLAN, 420
 - UTC, Universal Time Clock, 462
 - uwierzelnianie, authenticate, 745, 755, 789, 797, 865
 - CHAP, 711
 - PAP, 711
 - poprzez serwer RADIUS, 818
 - HSRP, 678
 - MD5, 592
 - proste, 590
 - VRRP, 687
 - w OSPF, 590
 - w PPP, 713
 - uzgodnienie trójstopniowe, *Patrz* three-way handshake
- V**
- VF45, Volition Fiber, 75
 - VIP, Virtual IP, 670
 - VirtualBox, 167
 - VLAN, Virtual LAN, 357, 395, 769, 830
 - danych, 402
 - domyślny, 403
 - działanie sieci, 395
 - interfejsy przełącznika, 396
 - konfiguracja sieci, 398
 - natywny, 402, 407
 - nieoznakowany, 402
 - połączenia typu trunk, 403
 - protokół VTP, 412
 - rodzaje sieci, 402
 - router, 398
 - routing, 477
 - metoda router-on-a-stick, 482
 - model klasyczny, 478

- VLAN, Virtual LAN
 sieci prywatne, 403
 stacje robocze, 397, 400
 tryby interfejsów, 408
 usuwanie konfiguracji, 420
 VTP Pruning, 421
 zarządzania, 403
- VLAN hopping, 830, 843
- VLSM, Variable Length Subnet Masking, 261
- VMware Workstation, 167
- VMware Workstation Pro, 168
 Advanced local settings, 175
 Customize Hardware, 171
 instalacja systemu operacyjnego, 171
 Managed VMnet interfaces, 175
 Menu podręczne, 177
 nazwa wirtualnej maszyny, 172
 Network Adapter, 174
 Network connection, 174
 New virtual machine wizard, 176
 okno
 główne, 169
 Hardware, 174
 parametry wirtualnej maszyny, 173
 Power Off, 178
 rozmiar pliku maszyny wirtualnej, 173
 Run in Background, 178
 Specify Disk Capacity, 171
 Split virtual disk into multiple files, 171
 Suspend, 178
 tworzenie maszyny wirtualnej, 168
 ustawienia
 interfejsu sieciowego, 175
 maszyny wirtualnej, 177
 Virtual machine name, 171
 zarządzanie wirtualnymi interfejsami, 176
- VPCS, 165
- VPN, Virtual Private Network, 38, 735
 algorytmy szyfrowania, 738
 bezpieczna komunikacja, 746
 dostęp
 poprzez przeglądarkę, 763
 przez klienta, 765
 funkcjonalność serwera, 746
 IKE Phase 1, 747
 integralność danych, data integrity, 738
 logowanie do sieci, 764
 remote access, 745
 site-to-site, 745
 status połączenia, 765
 szyfrowaniem, encryption, 738
 uwierzytelnianie, authentication, 738
 zachowanie poufności, confidentiality, 738
- VRRP, Virtual Router Redundancy Protocol, 671
 konfiguracja, 683
 czasów, 686
 track, 688
 uwierzytelniania, 687
 przeglądanie rozgłoszeń, 686
- VTP, VLAN Trunking Protocol, 413
 client, 420
 ograniczenia, 417
 Pruning, 421
 server, 418
 ustalanie hasła, 418
- vWLC, 802
 aktywacja, 810
 AP mode, 812, 814
 DHCP Bridging, 805
 konfiguracja
 adresów IP, 817
 interfejsów, 819
 konsola, 807
 logowanie, 808
 podłączenie punktu dostępowego, 811
 serwer RADIUS, 818
 testowanie komunikacji, 807
 tworzenie sieci WLAN, 809
 uruchamianie procesów, 804
 ustawienia
 maszyny wirtualnej, 804
 wstępne, 805
- VLAN Identifier, 805
 zapisywanie ustawień, 806
 zmiana adresu IP, 818
- warstwa
 aplikacji, 86, 88
 control plane, 946
 dostępu, access, 341
 dostępu do sieci, 87
 dystrybucji, distribution, 341
 fizyczna, 114
 forwarding plane, 946
 internetowa, 87
 łącza danych, 111
 prezentacji, 91
 rdzenia, core, 341
 sesji, 91
 sieci, 101
 transportu, 87, 91
- wartość
 AD, 500
 BW, 570
 pasma, 572
- warunek
 allow, 859
 deny, 630, 638, 859
 deny any, 638, 660
 dynamic, 630
 permit, 630
 permit any any, 638
 permit ip any any, 996
 permit tcp any any eq domain, 660
 remark, 630
- wąskie gardło, bottleneck, 873
- WDS, Wireless Distribution System, 784
- weak reversible algorithm, 225
- wektor inicjalizujący, initialization vector, 797
- WEP, Wired Equivalent Privacy, 794, 797
- wiadomość SYN, 143
- WIC, WAN Interface Card, 454, 708
- wi-fi, 77, 767
- WinPCAP, Windows Packet Capture, 164
- Wireshark, 127, 164
 analiza three-way handshake, 145
 Destination, 129, 140
 Domain Name System, query, 139
 Domain Name System, response, 140
 działanie DNS, 137
 filtrowanie ramek, 148

W

- WAAS NME, Wide Area Application Services, 454
- WAN, Wide Area Network, 47, 701

- interfejsy przechwytywania, 129
 logowanie do banku, 763
 menu główne, 130
 opcje przechwytywania, 128
 protokół
 ARP, 146
 TCP, 142
 przechwytywanie, 128
 hasła, 591
 pakietów HSRP, 679
 ramek wi-fi, 785
 Queries, 139
 Restartuj aktualne
 przechwytywanie, 131
 Save file as, 131
 segmentacja, 144
 Sender IP address, 147
 Source, 129
 Strumień TCP, 363
 Śledź strumień TCP, 363, 365
 Target IP address, 147
 Uruchom przechwytywanie
 pakietów, 131
 w GNS3, 254
 Zapisz przed kontynuowaniem,
 131
 Zastosuj filtr wyświetlania, 138
 Zatrzymaj przechwytywanie
 pakietów, 131
 wirtualizacja, 168, 945
 sieci, 943
 wirtualna sieć prywatna, VPN, 735
 wirus, 821, 824
 WLAN, Wireless LAN, 767
 w vWLC, 809
 WLC, WLAN Controller, 775, 802
 właściwości interfejsów OSPF, 567
 WPA, Wi-Fi Protected Access, 794,
 797
 WPA2, 793, 798
 WPA3, 798
 WPAN, Wireless Personal Area
 Network, 767
 wstrzymywanie potwierżeń,
 buffering, 144
 wtyk RJ-45, 67
 WWAN, Wireless Wide Area
 Networks, 767
 wybór karty sieciowej, 233
 wyłączenie
 autosumaryzacji, 536
 rozwłaszania, 532
 wyłudzenia informacji, 829
 wymiana pakietów LSA, 584
- X**
- X.25, 706
- Y**
- Yersinia, 845
- Z**
- zabezpieczenie BPDU guard, 446
 zablokowanie, deny, 613
 zaciskanie wtyków, 68
 zamiana liczb
 binarnych, 271
 dziesiętnych, 264
 szesnastkowych, 318
 zapisywanie konfiguracji
 przełącznika, 362
 zapora, firewall, 822, 859
 zapytanie
 ARP, 148, 153
 DNS, 137
 zarządzanie
 konfiguracją, 227
 siecią, 897
 systemem IOS, 248
 urządzeniem, 214
 zbieżność sieci, convergence, 41, 506
 zdalne zarządzanie routerem, 469
 zdarzenie bezpieczeństwa
 uruchomienie interfejsu, 390
 wywołanie, 388
 złącze
 LC, Lucent Connector, 73
 MT-RJ, 75
 SC, Subscribe Connector, 73
 ST, Straight-Tip, 73
 VF45, 75
 złośliwe oprogramowanie, 826
 zmiana
 adresu MAC, 392
 czasów, 576
 identyfikatora routera, 558
 mostu głównego, 439
 parametrów
 interfejsów, 361
 obliczania kosztu, 575
 szybkości interfejsów, 362
 znak
 ?, 217, 511
 ^, 218
 }, 461
 myślnika, 693
 zrównoważenie obciążenia, load
 balancing, 692

PROGRAM PARTNERSKI

— GRUPY 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
Helion

ZOSTAŃ PROFESJONALNYM ADMINISTRATOREM SIECI CISCO

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

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

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

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

ŚMIAŁO WKROCZ NA ŚCIEŻKĘ CERTYFIKACJI CCNA!

DR ADAM JÓZEFIOK ukończył studia doktoranckie na Politechnice Śląskiej w Gliwicach, na Wydziale Automatyki, Elektroniki i Informatyki. Specjalizuje się w tematyce sieci komputerowych (przełączanie, routing, bezpieczeństwo i projektowanie), jest autorem polskich oraz zagranicznych publikacji z tej dziedziny. Brał udział w konferencjach naukowych (krajowych oraz międzynarodowych) dotyczących sieci komputerowych. Posiada certyfikaty: CCNA Security, CCNP Routing and Switching, Cisco CCDP, CCNAV oraz certyfikat instruktorski Cisco CCAI, jak również certyfikaty ITIL i PRINCE2. Jego pasją jest pisanie książek, praca ze studentami i szeroko rozumiana dydaktyka.

Helion



helion.pl



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

Sprawdź nasze szkolenia!



AKADEMIA IT & BUSINESS

HELIONSZKOLENIA.PL

KOD KORZYŚCI
Sięgnij po więcej! ▶



ISBN 978-83-283-7168-2



9 788328 371682

INFORMATYKA W NAJLEPSZYM WYDANIU

Cena: 249,00 zł