

Adam Józefiok

CCNA

200-301

Zostań administratorem
sieci komputerowych Cisco

Wydanie II



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

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn

Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.

ul. Kościuszki 1c, 44-100 Gliwice

tel. 32 230 98 63

e-mail: helion@helion.pl

WWW: helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

helion.pl/user/opinie/cc3012

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-2283-9

Copyright © Helion S.A. 2025

Printed in Poland.

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

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

Spis treści

Wprowadzenie	17
ROZDZIAŁ 1. Certyfikacja i wiedza ogólna	20
Firma Cisco	20
Certyfikacja i egzamin	22
CCNA — tematyka i materiał	25
Rodzaje pytań na egzaminie	26
Sprzęt do nauki	27
Dokumenty RFC	29
ROZDZIAŁ 2. Wstęp do sieci komputerowych	30
Podstawy sieci komputerowych	30
Przesyłanie danych w sieci	33
Pojęcie protokołu sieciowego	36
Liczby w sieciach komputerowych	37
Organizacje standaryzujące	39
Rodzaje sieci komputerowych	39
Model pracy klient – serwer	40
Sieć bezprzewodowa	41
Sieć SAN	41
Sieci lokalne i sieci rozległe	41
Reguły działania sieci (komunikacja)	43
Proces komunikacji i wykorzystanie protokołów sieciowych	45
Urządzenia sieciowe	46
Okablowanie sieci przedsiębiorstwa	53
Media transmisyjne (miedziane, światłowodowe, bezprzewodowe)	58
Topologie sieci	74
Rozmiary sieci i nowe trendy	76
Pytania kontrolne	83
Odpowiedzi	84
ROZDZIAŁ 3. Modele sieci i pojęcie sieci Ethernet	85
Model TCP/IP	85
Warstwa aplikacji	86
Warstwa transportu	86
Warstwa internetowa	87
Warstwa dostępu do sieci	87
Model OSI	87
Warstwa aplikacji	88
Warstwa prezentacji	91

Warstwa sesji	91
Warstwa transportu	92
Warstwa sieci	100
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	126
Omówienie najważniejszych funkcji programu Wireshark	126
Menu główne	129
Działanie komunikacji DNS	131
Rozmiar okna TCP oraz three-way handshake	141
Działanie protokołu ARP	145
Komunikacja w sieci Ethernet — podsumowanie	148
Pytania kontrolne	158
Odpowiedzi	159
ROZDZIAŁ 5. Emulator GNS3 i symulator Cisco Packet Tracer	160
Informacje na temat programu GNS3	160
Pobieranie, instalacja i najważniejsze funkcje	162
Ważniejsze funkcje i opcje	164
Obszar roboczy GNS3	178
Przygotowanie serwera GNS3	180
Połączenie dwóch wirtualnych stacji w programie GNS3	181
Przygotowanie IOS	185
Podłączenie routerów i uruchomienie prostej sieci	193
Konfiguracja programu SuperPuTTY	195
Połączenie z urządzeniem wirtualnym	195
Wydanie polecenia wielu urządzeniom naraz	197
Zmiana nazwy zakładek	197
Symulator Cisco Packet Tracer	198
Instalacja programu Cisco Packet Tracer	199
Projekt w programie Cisco Packet Tracer	201
Środowisko rzeczywiste — lab domowy	202
ROZDZIAŁ 6. Wprowadzenie do systemu operacyjnego IOS i podstawowa konfiguracja urządzeń Cisco	204
Proces uruchamiania urządzenia	204
System operacyjny IOS	206
Podłączenie do urządzenia	206

Zarządzanie urządzeniem	209
Tryby pracy	210
System pomocy	211
Przeglądanie konfiguracji	214
Wstępna konfiguracja routera Cisco wraz z zabezpieczeniami	216
Konfiguracja interfejsu	220
Zarządzanie konfiguracją	221
Połączenie wirtualnego routera z siecią rzeczywistą za pomocą obiektu Cloud	225
Zarządzanie systemem IOS	241
Uruchomienie TFTP na routerze	244
Wykorzystanie programu Wireshark w GNS3	247
ROZDZIAŁ 7. Adresacja IPv4	250
Informacje wstępne o protokole IPv4	250
Pojęcia adresu sieci, adresu hosta i adresu rozgłoszeniowego	252
Ping na adres rozgłoszeniowy sieci	252
Typy adresów (prywatne i publiczne)	253
Binarna reprezentacja adresu IP	255
Zamiana liczb dziesiętnych na binarne	257
Zamiana liczb binarnych na dziesiętne	263
Podział sieci według liczby wymaganych podsieci	268
Podział klasy C	269
Podział klasy B	277
Podział klasy A	280
Podział sieci na podsieci — liczba hostów w każdej sieci	284
Podział klasy C	284
Podział klasy B	288
Podział klasy A	289
Podział sieci na podsieci — nierówna liczba hostów w podsieciach	290
Reverse engineering	300
ROZDZIAŁ 8. Adresacja IPv6	303
Wstępne informacje na temat protokołu IPv6	303
Zamiana liczb	306
Pytania kontrolne	329
Odpowiedzi	330
ROZDZIAŁ 9. Przełączniki sieciowe — podstawy działania i konfiguracji	331
Model hierarchiczny	331
Przełącznik warstwy 2.	334
Tablica adresów MAC	336
Podłączanie urządzeń do przełącznika	342
Metody przełączania ramek	344
Podstawowa konfiguracja przełącznika	345
Konfiguracja adresu IP i domyślnej bramy	347
Zmiana parametrów interfejsów i wyłączenie nieużywanych	351

Zapisanie konfiguracji	352
Włączenie protokołu SSH	352
Emulowany przełącznik w GNS3	359
Wykorzystanie w GNS3 obiektu Ethernet switch	362
Przypisanie adresu IPv6 na interfejsie VLAN1 przełącznika	362
Przełączniki pracujące w stosie	363
ROZDZIAŁ 10. Przełączniki sieciowe — Port Security	367
Przygotowanie konfiguracji i informacje wstępne	367
Konfiguracja Port Security	369
Konfiguracja czasu działania blokady	375
Wywołanie zdarzenia bezpieczeństwa	376
Uruchomienie interfejsu po zdarzeniu bezpieczeństwa	378
Funkcja autouruchamiania interfejsu	379
Zmiana adresu MAC karty sieciowej	379
ROZDZIAŁ 11. Sieci VLAN	382
Działanie sieci VLAN	382
Konfiguracja sieci VLAN	385
Rodzaje sieci VLAN	389
Prywatne sieci VLAN	389
Połączenia typu trunk	390
Przykład znakowania na łączu trunk	394
Automatyczna konfiguracja trybów interfejsów	395
Protokół VTP	399
Ograniczenia VTP	403
Ustalanie hasła i innych parametrów	404
Usuwanie konfiguracji VLAN	406
VTP Pruning	407
ROZDZIAŁ 12. Protokół STP i jego nowsze wersje	409
Algorytm działania STP	411
Rodzaje portów w STP	415
Koszty tras	417
Stany portów	419
Rozszerzenie protokołu STP, czyli protokół PVST	422
Konfiguracja PVST	425
Protokół RSTP	427
Konfiguracja RSTP	428
Pytania kontrolne	431
Odpowiedzi	432
ROZDZIAŁ 13. Wprowadzenie do routerów Cisco	433
Działanie routera i jego budowa	433
Budowa routera	438
Wstępna konfiguracja routera	440
Omówienie protokołu CDP	455

Protokół LLDP	458
Własne menu na routerze	458
Cisco IP SLA	459
Pytania kontrolne	461
Odpowiedzi	461
ROZDZIAŁ 14. Routing pomiędzy sieciami VLAN	462
Metoda klasyczna	462
Router-on-a-stick	467
Przełączanie w warstwie 3.	470
ROZDZIAŁ 15. Routing statyczny	474
Wprowadzenie do routingu statycznego	474
Sumaryzacja tras statycznych	478
Default route	481
Najdłuższe dopasowanie	483
Floating Static Route	484
ROZDZIAŁ 16. Routing dynamiczny i tablice routingu	488
Rodzaje protokołów routingu dynamicznego	489
Wymiana informacji i działanie protokołów	491
Protokoły distance vector	491
Protokoły link state	492
Tablica routingu routera	493
Proces przeszukiwania tablicy routingu	496
Tablica routingu stacji roboczej	504
ROZDZIAŁ 17. Routing dynamiczny — protokół RIP	506
Charakterystyka i działanie protokołu RIPv1	506
Konfiguracja RIPv1	507
Charakterystyka i konfiguracja protokołu RIPv2	514
Konfiguracja RIPv2	514
Podstawy protokołu RIPng	518
Konfiguracja protokołu RIPng	519
ROZDZIAŁ 18. Routing dynamiczny — protokół OSPF	525
Protokół OSPFv2	525
Pakiety hello	526
Konfiguracja protokołu OSPF	529
Alternatywna konfiguracja protokołu OSPF	534
Równoważenie obciążenia w OSPF	537
Zmiana identyfikatora routera	538
Stany interfejsów i relacje sąsiedzkie	540
Wymiana informacji pomiędzy routerami — obserwacja	541
Metryka w OSPF	547
Zmiana czasów	554
Konfiguracja passive-interface	556
Rozgłaszanie tras domyślnych	557

OSPF w sieciach wielodostępowych	557
Wybór routerów DR i BDR	558
Statusy po nawiązaniu relacji sąsiedztwa	565
Routery DR i BDR w połączeniu punkt – punkt	566
Uwierzytelnianie w OSPF	568
Wieloobszarowy OSPF	571
Typy przesyłanych pakietów LSA	573
Konfiguracja wieloobszarowego OSPF	573
Protokół OSPFv3	583
Konfiguracja OSPFv3	583
Pytania kontrolne	589
Odpowiedzi	589
ROZDZIAŁ 19. Listy ACL	590
Rodzaje list ACL	592
Konfiguracja standardowych list ACL	593
Przykład 1.	593
Przykład 2.	598
Przykład 3.	600
Przykład 4. (lista standardowa nazywana)	602
Konfiguracja rozszerzonych ACL	606
Przykład 5.	606
Przykład 6.	609
Przykład 7.	611
Przykład 8.	613
Przykład 9.	616
Listy ACL w IPv6	616
Przykład 10.	618
Przykład 11.	619
Przykład 12.	620
Przykład 13.	620
ROZDZIAŁ 20. Network Address Translation (NAT) i Dynamic Host	
 Configuration Protocol (DHCP)	622
Static NAT (translacja statyczna)	623
Dynamic NAT (translacja dynamiczna)	626
PAT	628
Konfiguracja routera R1 jako serwera DHCP	629
DHCP Snooping	631
Przykład	635
Konfiguracja routera R1 jako serwera DHCPv6 (SLAAC)	637
Konfiguracja routera jako bezstanowego serwera DHCPv6	638
Konfiguracja routera jako stanowego serwera DHCPv6	641
NAT dla IPv6	643
Pytania kontrolne	644
Odpowiedzi	645

ROZDZIAŁ 21. Redundancja w sieci i wykorzystanie nadmiarowości	646
Konfiguracja protokołu HSRP	648
Przygotowanie przykładowej sieci w programie GNS3	648
Konfiguracja HSRP	650
Konfiguracja VRRP	660
Konfiguracja GLBP	668
EtherChannel	671
Konfiguracja EtherChannel	673
Pytania kontrolne	675
Odpowiedzi	677
ROZDZIAŁ 22. Technologie sieci WAN i sieci VPN	678
Sieci WAN — ogólne informacje	678
Technologie sieci WAN	680
Frame Relay	680
ISDN	681
PPP	682
DSL	682
X.25	683
ATM	684
MPLS	684
Przykładowy model sieci WAN	684
Konfiguracja enkapsulacji w przykładowym modelu punkt – punkt	685
Technologia Frame Relay	690
Konfiguracja Frame Relay (hub-and-spoke)	694
Konfiguracja multipoint	695
Konfiguracja point-to-point	703
Samodzielna konfiguracja przełącznika Frame Relay	707
Technologia VPN	711
Szyfrowanie w VPN	713
Typy sieci VPN	721
Implementacja VPN site-to-site na routerze Cisco za pomocą CLI	723
ROZDZIAŁ 23. Sieci wi-fi	741
Wprowadzenie do sieci bezprzewodowych	741
Działanie sieci bezprzewodowej	743
Standardy sieci wi-fi	748
Urządzenia bezprzewodowe	749
Format ramki	752
Mechanizm CSMA/CA	765
Sposób połączenia	765
Bezpieczeństwo sieci bezprzewodowych	772
Typowe ataki na sieci bezprzewodowe	774
Zastosowanie i projektowanie sieci bezprzewodowych	775
Konfiguracja kontrolera Cisco WLC i punktu dostępowego	777
Pytania kontrolne	795
Odpowiedzi	796

ROZDZIAŁ 24. Podstawy bezpieczeństwa w sieciach komputerowych	797
Bezpieczeństwo w sieci	797
Główne rodzaje niebezpieczeństw — pojęcia	800
Wybrane ataki warstwy 2. modelu OSI	806
Ataki na ARP	806
Ataki na STP	806
Ataki na VLAN	806
Ataki na DHCP	807
Ataki na tablicę ARP i MAC	807
Główne rodzaje niebezpieczeństw — przykładowe ataki	808
Denial of Service (DoS)	808
Denial of Service (DoS) — atak zwierciadlany	810
Ataki na ARP	811
Ataki na STP	813
Ataki STP na root bridge i wybór nowego roota	815
Ataki na VLAN	818
Ataki na DHCP	824
Ataki na tablicę MAC i ARP	831
Główne rodzaje niebezpieczeństw — obrona	834
System ochrony warstw wyższych	835
Model AAA	840
Rozwiązanie 802.1X	841
Szybkie bezpieczeństwo na urządzeniach Cisco	843
ROZDZIAŁ 25. Quality of Service	847
Kolejkowanie w sieciach	847
Modele QoS	851
Wdrażanie QoS	851
Kształtowanie ruchu w QoS	854
Pytania kontrolne	859
Odpowiedzi	859
ROZDZIAŁ 26. Konfiguracja urządzeń Cisco za pomocą interfejsu GUI	860
Wprowadzenie	860
Środowisko testowe	861
Konfiguracja urządzenia za pomocą Web UI	862
Menu monitorowania	865
Menu konfigurowania	867
Menu administrowania	871
Menu rozwiązywania problemów	872
ROZDZIAŁ 27. Zarządzanie siecią	874
Niektóre problemy w sieci	874
Rozwiązywanie problemów z interfejsami	876
Narzędzie debugowania	877
Sprawdzanie komunikacji	879

Testowanie łącza z siecią internet	881
Testowanie połączenia w sieci lokalnej za pomocą narzędzia iperf	882
Logowanie zdarzeń i raportowanie	884
Obsługa logów systemowych syslog	885
Wykorzystanie SNMP	886
Wykorzystanie i działanie NetFlow	896
Konfiguracja funkcjonalności span port	900
ROZDZIAŁ 28. Projektowanie i automatyzacja sieci	905
Projektowanie sieci	905
Działania wstępne	908
Dokumentacja sieci	915
Rozwiązywanie problemów z siecią	916
Wirtualizacja i automatyzacja sieci — wprowadzenie	918
Usługi chmury	919
Maszyny wirtualne	920
Sieci SDN	922
Automatyzacja sieci	924
API	928
Szablony	929
Zastosowanie sztucznej inteligencji i uczenia maszynowego	
w operacjach sieciowych	930
Sztuczna inteligencja i uczenie maszynowe	930
Jak się uczy sztuczna inteligencja?	932
Sztuczna inteligencja w sieciach komputerowych	932
Pytania kontrolne	934
Odpowiedzi	936
ROZDZIAŁ 29. Ćwiczenia praktyczne	937
Ćwiczenie 1.	937
Odpowiedź do ćwiczenia	937
Ćwiczenie 2.	938
Odpowiedź do ćwiczenia	938
Ćwiczenie 3.	939
Odpowiedź do ćwiczenia	940
Ćwiczenie 4.	942
Odpowiedź do ćwiczenia	942
Ćwiczenie 5.	942
Odpowiedź do ćwiczenia	943
Ćwiczenie 6.	943
Odpowiedź do ćwiczenia	944
Ćwiczenie 7.	949
Odpowiedź do ćwiczenia	950
Ćwiczenie 8.	956
Odpowiedź do ćwiczenia	956
Ćwiczenie 9.	960
Odpowiedź do ćwiczenia	960

Ćwiczenie 10.	963
Odpowiedź do ćwiczenia	964
Ćwiczenie 11.	970
Odpowiedź do ćwiczenia	971
ROZDZIAŁ 30. Słownik pojęć	977
Zakończenie	1003
Literatura	1004
Skorowidz	1005

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.

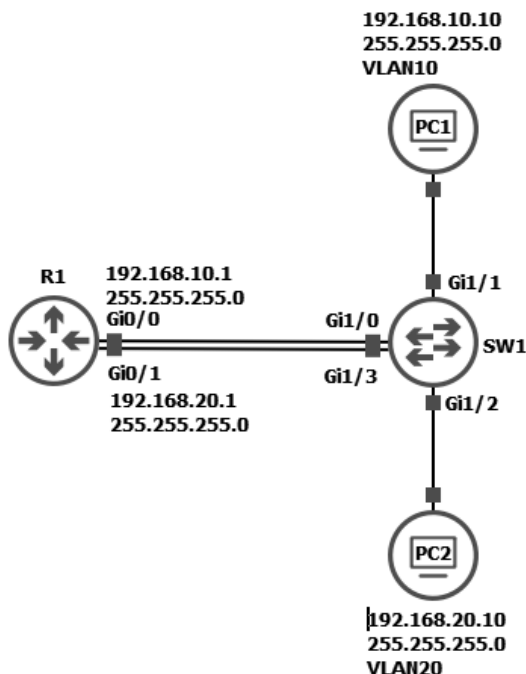
Każdą metodę postaram się wyjaśnić na podstawie projektów, które możesz wykonać samodzielnie w programie GNS3. Będzie Ci do tego potrzebny router Cisco 3745, o którym wspominałem w poprzednich rozdziałach.

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

RYSUNEK 14.1.

Routing pomiędzy sieciami VLAN — model klasyczny



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.

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 podsieci co stacja robocza H1, ponadto znajduje się w tej samej sieci VLAN. Na stacjach roboczych ustaw też adresy IP i adresy bram domyślnych. Stację VPCS skonfigurujesz za pomocą komendy `ip [adresIP] [maska] [adresIP_domyślnej_bramy]`, np. `ip 192.168.10.10 255.255.255.0 192.168.10.1`. Zajmij się teraz routerem R1.

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

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

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

```
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1	192.168.20.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down

```
R1#
```

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

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

```
R1#show ip route
```

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

```
Gateway of last resort is not set
```

```
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.20.0/24 is directly connected, GigabitEthernet0/1
L    192.168.20.1/32 is directly connected, GigabitEthernet0/1
R1#
```

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

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

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

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

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

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

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

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

```
PC1> trace 192.168.20.10
trace to 192.168.20.10, 8 hops max, press Ctrl+C to stop
 1  192.168.10.1  14.031 ms  13.028 ms  10.330 ms
 2  192.168.20.10  18.993 ms
PC1>
```

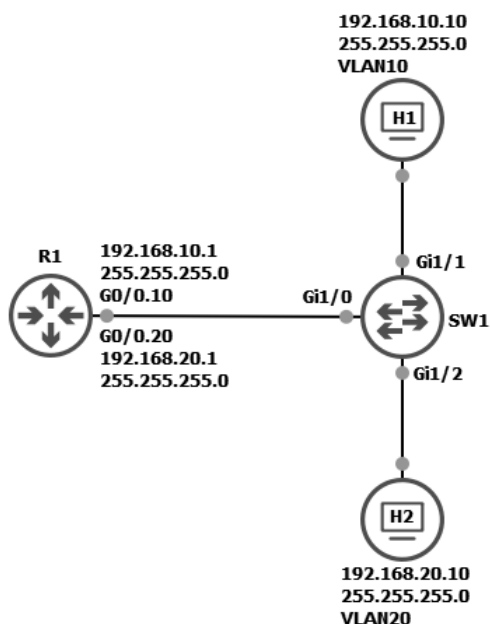
Pora na podsumowanie informacji dotyczących metody klasycznej. Jak zauważyłeś, w przypadku dwóch sieci VLAN właściwie nie ma przeszkód, aby zastosować tę metodę. Jednak każda kolejna sieć VLAN wymaga odrębnego interfejsu na routerze i przełączniku. Oznacza to, że przy 20 sieciach VLAN trudno będzie w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

Router-on-a-stick

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

Na rysunku 14.2 pokazałem sieć komputerową, w której połączenie pomiędzy routerem a przełącznikiem realizowane jest za pomocą jednego przewodu. Przejdźmy więc do konfiguracji i szczegółowego omówienia działania prezentowanej tu metody. Możesz do tego ćwiczenia wykorzystać poprzednie, ale wymaga 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 podłączone, zmieniły się jedynie interfejsy, przez które sieci są dostępne.

R1#show ip route

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

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

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

H1> ping 192.168.20.10

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

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

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

H1> trace 192.168.20.10

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

Przełączanie w warstwie 3.

Przełączanie w warstwie 3. wygląda nieco inaczej niż w warstwie 2., gdzie odbywało się wyłącznie na podstawie adresów MAC. Wszystkie inne czynności dostosowywane były właśnie do tych identyfikatorów. W warstwie 3. przełączanie następuje na podstawie adresów IP, czyli warstwy 3. Ze względu na to, że praca odbywa się w warstwie 3., przełączniki

mają również wiele innych funkcjonalności routerów. Mogą więc z powodzeniem przejmować część ruchu sieciowego, tak by routery nie musiały być angażowane.

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

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

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

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

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

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

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

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

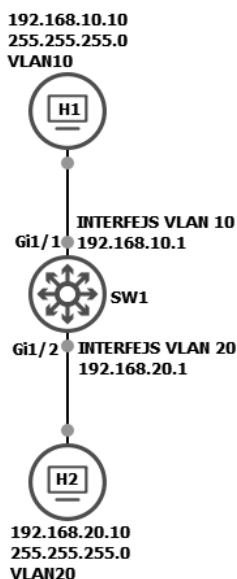
```
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#ip routing
SW1(config)#
```

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

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

RYSUNEK 14.3.

Komunikacja pomiędzy sieciami VLAN z wykorzystaniem przełącznika L3



```

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 wątplenia 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, 716

A

AAA, authentication,
authorization, accounting, 840
autoryzacja, 841
raportowanie, 841
uwierzytelnienie, 840

ABR, Area Border Router, 572

access point, *Patrz* punkt
dostępowy

ACL, Access Control List, 333,
590, 798

AD, Administrative Distance, 484
adapter RS232-USB, 207

administrowanie

bezpieczeństwem, 798

adres

domyślnej bramy, 106

GUA, Global Unicast Address,
637

hosta, 252

IPv4, Internet Protocol, 101

automatyczne

przypisanie, 109

docelowy, destination IP

address, 101

przełącznika, 347, 348

przydzielanie, 631

reprezentacja binarna, 255

ręczne przypisanie, 106

źródłowy, source IP

address, 101

IPv6, 326

anycast, 308

global, globalny, 308

local-link, lokalnego

łącza, 254, 308

loopback, pętli zwrotnej,
254, 308

multicast, grupowy, 308,
313

Temporary IPv6, 315
unspecified,

nieokreślony, 308

MAC, 47, 120, 138, 309, 336

karty sieciowej, 379

wirtualny, 651, 661

zmiana, 379

rozgłoszeniowy sieci,

broadcast, 252

sieci, 252

VIP, Virtual IP, 647

adresacja

IPv4, 102, 250

IPv6, 303

adresy

prywatne, 253

publiczne, 253

zapasowe, 973

zdublowane, 311

adware, 797

AES, Advanced Encryption

Standard, 716, 774

agent przekazujący, relay agent,
642

AHP, Authentication Header

Protocol, 617

alarmy

falszywe, 839

prawdziwe, 839

algorytm

3DES, 716

AES, 716, 774

DES, 716

DKE, 775

DSA, 720

ECDSA, 720

IDEA, 716

MD5, 718

RC, 716

RSA, 720

SHA, 718

SPF, 525

STA, 411

TKIP, 774

algorytmy

haszujące, 718

szyfrowania, 714

alias, 450

AMP, Advanced Malware
Protection, 51, 835

analiza

ruchu IPS, 838

three-way handshake, 143

analogowe połączenia

telefoniczne, 683

antena

dookólna, omnidirectional

antenna, 752

kierunkowa, directional

antenna, 752

MIMO, 752

API, 928

architektura sieci

dwuwarstwowa, 83, 905

spine-and-leaf, 81

trójwarstwowa, 82, 907

ARP, Address Resolution

Protocol, 121, 434, 446

ataki, 806, 811, 831

działanie protokołu, 145

ramka rozgłoszeniowa, 149,
150

wpisy statyczne, 123

atak

DDoS, 803

DoS, 776, 797, 803, 808

DTP, 820

typu

access attack, dostępu, 802

brute-force attack,

siłowy, 802

buffer overflow attack,
803

flood attack, zalewanie,
806

man-in-the-middle attack,
655, 719, 776, 803

passwords attack, 803

poisoning, 125

reflection attack,

zwierciadlany, 810

smurf attack, 804

spoofing, 125, 804

trust exploitation attack,
804

VLAN hopping, 818

ataki
 modyfikowanie
 pola danych, 823
 ramki, 822
 na DHCP, 807, 824
 na protokoły IPv4, 806
 na root bridge, 815
 na STP, 806, 813, 815
 na tablicę ARP, 806, 811, 831
 na tablicę MAC, 807, 831
 na VLAN, 804, 806, 818
 z zewnątrz, 799
 ATM, Asynchronous Transfer Mode, 684
 autentykator, authenticator, 842
 autoinstalacja, 209
 automatyczna konfiguracja trybów interfejsów, 395
 automatyczne
 wylogowywanie, 453
 zapisywanie konfiguracji, 239
 automatyzacja sieci, 924
 Auto-MDIX, 342
 autosumaryzacja, 515
 wyłączanie, 517
 autouruchamianie interfejsu, 379
 AVF, Active Virtual Forwarders, 648
 AVG, Active Virtual Gateway, 648
 awaria interfejsu, 544
 awarie sieci, 874

B

bajt, byte, 38
 banner MOTD, 219
 baza danych
 LSDB, 525, 545
 OSPF, 545
 BDR, Backup Designated Router, 528
 bezpieczeństwo, 367,
Patrz także Port Security
 autokonfiguracja urządzenia, 843
 autouruchamianie interfejsu, 379
 dostępność, availability, 79
 integralność, integrity, 79, 718
 poufność, confidentiality, 79
 sieci
 bezprzewodowej, 773
 komputerowej, 590
 wi-fi, 771

szyfrowanie, encryption, 79, 219, 774
 w sieci, 797
 BGP, Border Gateway Protocol, 490
 BNC, Bayonet Neill-Conclemann, 32
 bootstrap, 205
 BPDU Guard, 431, 817
 BPDU, Bridge Protocol Data Units, 411
 brama domyślna, 151
 broadcast, 43, 45, 125, 407
 storm, 409
 BSA, Basic Service Area, 742
 BSS, Basic Service Set, 742
 BSSID, BSS Identifier, 742
 BYOD, *Bring Your Own Device*, 53

C

CCNA, 25
 CDP, Cisco Discovery Protocol, 455, 583, 878
 informacje o interfejsach, 457
 informacje o sąsiedzie, 456
 CEF, Cisco Express Forwarding, 437, 471
 certyfikat, 737
 CHAP, Challenge Handshake Authentication Protocol, 688
 chmura, cloud, 919
 prywatna, private cloud, 920
 publiczna, public cloud, 920
 CIR, Committed Information Rate, 681, 691
 Cisco, 20
 AI Network Analytics, 860
 Digital Network Architecture, DNA
 narzędzia automatyzacji, 860
 zabezpieczanie sieci, 860
 Feature Navigator, 242
 Firepower, 51
 ISE, Identity Services Engine, 50
 Packet Tracer, 160, 198
 instalacja programu, 199
 okno główne, 200
 okno konfiguracji, 203
 tworzenie projektu, 201
 wybór wersji, 200
 Prime NAM, 917
 SecureX, 51
 Threat Grid, 51
 Umbrella, 51

Cpulimit, 163
 CSMA/CA, 765
 CSMA/CD, 118, 756
 czas
 bezczynności routera, 453
 dead interval, 527
 dead time, 541, 556
 działania blokady, 375
 flush, 561
 flushed, 510
 hello, 556, 654
 hello-interval, 554
 hold, 654
 hold down, 510
 interwał przesyłania pakietów, 527
 starzenia się, aging time, 338, 375
 TTL, 154
 wzorcowy UTC, 448

D

DAD, Duplicate Address Detection, 311
 DAI, Dynamic ARP Inspection, 832
 DCE, Data Communications Equipment, 444, 681
 DDoS, Distributed Denial of Service, 803
 debugowanie, 877
 komunikatów RIP, 511
 protokołu CDP, 878
 protokołu ICMP, 878
 dekapsulacja, 434
 DES, Data Encryption Standard, 716
 detekcja ruchu IPS, 838
 DFS, Dynamic Frequency Selection, 747
 DHCP, Dynamic Host Configuration Protocol, 37, 90, 321, 631, 807, 824
 attack parameters, 828
 Consumption Attack, 807
 komunikaty, 631
 przydzielanie adresu IP, 631
 Snooping, 631, 829–832
 DHCPv6 serwer, 637
 bezstanowy, 638
 stanowy, 641
 diody
 routera, 439
 przełącznika, 335
 DKE, Dragonfly Key Exchange, 775

DLCI, Data Link Connection Identifier, 681, 691
 DMVPN, Dynamic Multipoint VPN, 712, 713
 DNS, Domain Name System, 90, 131
 działanie komunikacji, 131
 odpowiedź serwera, 138
 w IPv6, 328
 wyświetlanie tablicy, 132
 zapytanie, 137
 zasada działania, 136
 dokumentacja sieci, 915
 domena awarii, failure domain, 908
 DoS, Denial of Service, 797, 803, 808
 dostawca internetu, 31
 dostęp
 do sieci internetowej, 42
 do urządzeń sieciowych, 604
 dostępność, availability, 35
 DR, Designated Router, 528
 drother, 528, 541, 560, 562, 575, 586
 DSL, Digital Subscriber Line, 42
 rodzaje, 682
 DSSS, Direct-Sequence Spread Spectrum, 748
 DTE, Data Terminal Equipment, 444, 681
 DTLS, Datagram Transport Layer Security, 773
 DTP, Discovery Trunk Protocol, 368
 DTP, Dynamic Trunking Protocol, 395
 DWDM, Dense Wavelength Division Multiplexing, 679
 dynamic NAT, 626
 Dynamips, 163
 dystans administracyjny, AD, 484

E

EAP, Extensible Authentication Protocol, 842
 EIGRP, Enhanced IGRP, 489, 534
 EIR, Excess Information Rate, 681
 EMI, Enhanced Multilayer Software, 28
 emulator GNS3, 160
 enkapsulacja, 153–156, 435
 HDLC, 685, 689
 konfiguracja, 685
 PPP, 685, 687

ESP, Encapsulating Security Payload, 617, 714
 ESS, Extended Service Set, 742
 EtherChannel, 410, 671
 konfiguracja, 673
 Ethernet, 116, 148
 adresowanie, 120
 switch, 362
 extranet, 77

F

fala radiowa, 743
 amplituda, 744
 częstotliwość, 744
 FHSS, Frequency Hopping Spread Spectrum, 748
 FIB, Forwarding Information Base, 437, 471
 FIFO, first in, first out, 849
 filtrowanie
 adresów URL, 835
 pakietów, packet filtering, 591, 835
 ramek ARP, 146
 firewall, 798, *Patrz także* Cisco Firepower, 51, NGFW, 50, 835
 formaty danych, 925
 Frame Relay, 680, 690
 CIR, 691
 DLCI, 691
 konfiguracja
 multipoint, 695
 point-to-point, 703
 samodzielna
 przełącznika, 707
 w hub-and-spoke, 694
 LAR, 691
 LMI, 691
 topologie PVC, 692
 FTP, File Transfer Protocol, 91
 funkcjonalność
 Auto-MDIX, 342
 BPDU Guard, 431, 816
 buffering, 142
 Cisco IP SLA, 459
 DAI, 833
 DHCP Snooping, 631, 829–832
 EtherChannel, 410, 671–673
 flow control, 142
 helper-address, 633, 634
 LAG, 779
 load balancing, 648
 passive interface, 514, 556, 570
 podłączanie wirtualnego routera, 225

Port Security, 332, 367, 372
 PortFast, 420, 421, 431
 Preemption, 652, 653
 Pruning Mode, 401
 QoS, 79, 384, 847
 relay agent, 642
 rsh-enable, 454
 segmentacja, 142
 SLAAC, 321, 637
 span port, 900
 subinterfaces, 468
 sumaryzacja, 325, 478, 480, 577
 track, 658, 665
 VTP Pruning, 407

G

GBIC, Gigabit Interface Converter, 343
 GE, Gigabit Ethernet, 439
 generowanie klucza, 356
 GLBP, Gateway Load Balancing Protocol, 648
 konfiguracja, 668
 maksymalna liczba urządzeń, 668
 równoważenie obciążenia, 669
 tryb pracy AVF, 668
 tryb pracy AVG, 668
 gniazdo abonentkie, 55
 GNS3, Graphical Network Simulator, 160, 161
 implementowanie
 maszyny wirtualnej, 176
 przełącznika L2, 191
 serwera GNS3, 180
 import obrazu
 IOSv, 188
 IOSvL2, 191
 instalacja, 162
 karty sieciowe, 226
 konfiguracja
 obiektu Cloud, 228
 routingu statycznego
 IPv6, 321
 wirtualnego routera, 192
 wirtualnego serwera, 181
 konsola routera, 190
 obiekt
 Cloud, 226
 Ethernet switch, 362
 obszar roboczy
 ikony urządzeń, 179
 menu funkcji, 178

- GNS3, Graphical Network Simulator
 - okno
 - General preferences, 165
 - główne, 164
 - importu, 187
 - Node properties, 192, 228, 233
 - Packet capture, 248
 - Project, 164
 - Qemu settings, 187
 - Required files, 188
 - Server, 187
 - Servers Summary, 180
 - Topology Summary, 195
 - Usage, 189
 - podłączanie
 - obiektu Cloud, 228, 232
 - dwóch stacji, 181
 - trzech routerów, 193
 - program Wireshark, 247
 - projekt sieci
 - dla span port, 901
 - dla IP SLA, 459
 - dla Port Security, 368
 - Frame Relay, 697, 704, 708
 - lokalnych i sieci internet, 733
 - OSPFv2, 534
 - router z przełącznikiem, 309
 - router z siecią
 - rzeczywistą, 225
 - VLAN site-to-site, 723
 - z protokołem HSRP, 648
 - z protokołem RIPng, 519
 - z protokołem RIPv1, 508
 - z dostępem do internetu, 623
 - z połączeniem trunk, 394
 - z SNMP, 888
 - przełączniki, 359
 - system operacyjny IOS, 185
 - testowanie środowiska GUI, 861
 - ustawienia domyślne, 166
 - ważniejsze funkcje i opcje, 164
 - wybór wzorca urządzenia, 186
 - wyświetlanie
 - opisu interfejsów, 194
 - identyfikatorów interfejsów, 194
 - zarządzanie wirtualnymi interfejsami, 174
- GRE, Generic Routing Encapsulation, 713, 732
- GUI
 - konfiguracja urządzeń, 860
 - Web UI, 862
- H**
- haker, 799
- hash, 656
 - value, 569
- hasło, 217
 - przechwycenie, 569
 - resetowanie, 223
 - do linii konsolowej, 220
 - do trybu uprzywilejowanego, 223
- haszowanie, 718
- HDLC, High-Level Data Link Control, 685
- HIPS, host-based IPS, 838
- HMAC, Hashed Message Authentication Code, 719
- HSRP, Hot Standby Router Protocol, 647
 - funkcjonalność track, 658
 - konfiguracja czasów, 654
 - konfiguracja protokołu, 650
 - parametr Preempt, 653
 - priorytety, 653
 - uwierzytelnianie, 655
 - weryfikacja konfiguracji, 652
- HTML, Hypertext Markup Language, 925
- HTTP, Hypertext Transfer Protocol, 89
- I**
- IaaS, Infrastructure as a Service, 919
- IBSS, Independent Basic Service Set, 742
- ICMP, Internet Control Message Protocol, 109, 140, 250, 617
- IDEA, International Data Encryption Algorithm, 716
- identyfikator
 - Area ID, 527, 576
 - Bridge ID, 413, 425, 426
 - BSSID, 742
 - DLCI, 681, 692
 - Extended System ID, 424
 - Root ID, 411, 426
 - router ID, 526, 538, 584
 - SSID, 742, 750, 768, 769
- IDS, Intrusion Detection Systems, 836
- IGRP, Interior Gateway Routing Protocol, 489
- IKE, Internet Key Exchange, 717
- infrastruktura jako usługa, IaaS, 919
- interfejs, 32
 - BNC, 32
 - Console, 439
 - GBIC, 343
 - GE, 439
 - konfiguracja, 220
 - LC, 72
 - loopback, 227, 229, 232, 234, 317
 - pasywny, 512
 - Serial, 444
 - SFP, 344
 - stan
 - blocking, 419
 - forwarding, 419
 - listening, 419
 - status Desig, 418, 423
 - tunelowy, 735
 - wpis statyczny MAC, 373
- interfejsy
 - tryb pracy
 - dynamic auto, 397
 - dynamic desirable, 396
 - full duplex, 876
 - half duplex, 876
 - trunk, 395, 396
 - rozwiązywanie problemów, 876
- internet, 42, 52
- IOS, Internetwork Operating System, 185, 206
 - system pomocy, 211
 - zarządzanie systemem, 241
- IP SLA, 459
- IP, Internet Protocol, 250
- iperf, 882
- IPS, Intrusion Prevention System, 51, 798, 835–837
 - analiza ruchu, 838
 - detekcja ruchu, 838
 - metoda
 - anomaly-based, 839
 - honeypot detection, 839
 - policy-based, 838
 - signature-based, 838
- IPv6, 303
 - autokonfiguracja, 325
 - działanie DNS, 327
 - komunikacja multicast, 313
 - komunikat Neighbor Solicitation, 314
 - konfiguracja
 - list dostępu ACL, 616
 - tras statycznych, 321
 - trasy domyślnej, 323

nagłówek, 304
 NAT, 643
 podział sieci, 325
 polecenia diagnostyczne, 327
 przypisanie do interfejsu, 317, 362
 rodzaje adresów, 308
 skracanie adresu, 307
 sumaryzacja tras, 324
 ISDN, Integrated Services Digital Network, 681
 IS-IS, Intermediate System to Intermediate System, 489

J

język
 HTML, 925
 Jinja, 929

K

kabel, *Patrz* przewód
 karta
 rozszerzeń
 HSWIC, High-Speed WIC, 439
 NME, Network Module, 439
 WAAS NME, 439
 WIC, Wan Interface Card, 438, 439, 684
 loopback, 230, 231
 sieciowa, network card, NIC, 32, 46, 226
 bezprzewodowa, 761
 tryb monitorowania, 761
 tryb pracy, 937
 zmiana adresu MAC, 379
 keylogger, 802
 Kiwi Syslog, 887
 ustawienia programu, 888
 klasa
 A, 254, 280, 289
 B, 254, 277, 288
 C, 254, 269, 284
 D, 254
 E, 254
 klasy adresów
 publicznych, 254
 prywatnych, 254, 622
 klient
 DHCP, 971
 iperf, 883
 RADIUS, 842
 klient-serwer, 40

klucz PSK, 721
 kodowanie, encoding, 45
 kolejkowanie, 847
 CBWFQ, 850
 działanie systemu, 848
 LLQ, 850
 metoda FIFO, 849
 WFQ, 850
 kolektor NetFlow, 896
 komenda, *Patrz* polecenie
 komunikacja, 43
 bezprzewodowa, wireless, 73
 broadcast, rozgłoszeniowa, 45, 125
 multicast, 44
 unicast, 43
 w sieci Ethernet, 148
 komunikat
 Active router is local, 652
 Bad secrets, 223
 Change Cipher Spec, 737
 Destination host unreachable, 466
 ICMP packet debugging is off, 878
 ICMP packet debugging is on, 878
 is directly connected, 491
 --MORE--, 212
 Neighbor Solicitation, 314
 Number of existing VLANs, 401
 Preemption disabled, 652
 RA, Router Advertisement, 321, 637
 Redistributing: rip, 510
 Request timed out, 229
 Routing for Networks:, 510
 Routing Information Sources, 510
 RS, Router Solicitation, 321
 sending v2, 516
 Spanning tree enabled protocol rstp, 428
 State is Active, 652
 State is Master, 661
 This bridge is the root, 412, 413, 425
 VTP Operating Mode, 401
 komunikaty
 debugowania, 878
 DHCP, 631, 829
 ICMPv6, 310
 protokołu OSPF, 541
 typu 4, 543
 koncentrator, hub, 49, 331

konfiguracja
 adresu IP, 347
 czasów, 654, 664
 czasu działania blokady, 375
 domyślnej bramy, 347
 enkapsulacji, 685
 EtherChannel, 673
 Frame Relay, 694, 695, 703
 funkcjonalności span port, 900
 IKE Phase 1, 726
 interfejsu loopback, 317
 kolektora NetFlow, 899
 kontrolera WLC, 778
 list ACL
 rozszerzonych, 606
 standardowych, 593
 maszyny wirtualnej, 174
 MD5, 656, 657
 multipoint, 695
 NAT na routerze, 624
 obiektu Cloud, 228
 oprogramowania PRTG, 892
 passive-interface, 556, 570, 574
 point-to-point, 703
 połączenia VPN GRE, 733
 Port Security, 369
 protokołu
 GLBP, 668
 HSRP, 648
 OSPF alternatywna, 534
 OSPF wieloobszarowego, 573
 OSPF, 529, 964
 OSPFv3, 583
 PPP, 689
 PVST, 425
 RIP, 968
 RIPng, 320, 519
 RIPv1, 507
 RIPv2, 514
 RSTP, 428
 SNMP, 887, 888
 SNMPv2c, 887
 SNMPv3, 890
 SSH, 357
 VRRP, 660
 przełącznika, 335
 Frame Relay, 697, 707
 punktu dostępowego, 769, 771, 778, 794
 routera
 automatyczne zapisywanie, 239
 interfejs, 220, 307, 694
 kopiowanie, 221
 kopiowanie z USB, 222

konfiguracja
 routera
 usuwanie, 223
 wirtualnego, 192
 wstępna, 216, 440
 za pomocą Web UI, 862
 running-config, 438
 serwera DHCP, 629
 serwera TFTP, 235
 kopiowanie do serwera, 234
 kopiowanie z serwera, 238
 sieci VLAN, 385
 tras statycznych, 321
 trasy domyślnej, 323
 trybów interfejsów, 395
 urządzeń, 204
 przeglądanie, 214
 VPN site-to-site, 724
 vWLC, 785
 kontrola przepływu, flow control, 142
 kontroler
 Cisco WLC, 778
 LAP, 750
 SDN, 923
 WLC, 750
 koń trojański, 797, 801
 kopiowanie konfiguracji, 221, 222, 234, 238
 koszt przesłania pakietów, 547, 553
 koszty tras, 417
 kreator dodawania sprzętu, 230

L

LACP, Link Aggregation Control Protocol, 673
 LAG, Link Aggregation Group, 779
 LAN, Local Area Network, 41
 LAP, Lightweight Access Point, 750
 LAR, Local Access Rate, 691
 LCP, Link Control Protocol, 682
 liczby
 binarne, 257
 zamiana na dziesiętne, 263
 dziesiętne, 263
 zamiana na binarne, 257
 szesnastkowe, 305
 linia
 dzierżawiona, leased line, 678
 komend, command line, 47
 konsolowa, 217

lista sąsiadów, 529
 listy ACL, 333, 590, 798
 filtrowanie pakietów, 591
 nazywane, named, 593, 602
 reflective ACL, 593
 rozszerzone, extended ACL, 592, 975
 konfiguracja, 606
 standardowe, 592
 adresy prywatne, 627
 edytowanie, 601
 konfiguracja, 593
 ograniczanie dostępu, 604
 usuwanie, 601
 w IPv6, 616
 warunek
 deny any, 636
 deny, zablokowanie, 590, 607, 614
 dynamic, 607
 nd-na, 617
 nd-sn, 617
 permit ip any any, 975
 permit tcp any any eq domain, 636
 permit, przepuszczenie, 590, 607, 614
 remark, 607
 wstawianie komentarzy, 597

LLC, Logical Link Control, 111
 LLDP, Link Layer Discovery Protocol, 458
 LMI, Local Management Interface, 691
 logi systemowe, 885
 logowanie zdarzeń, 884
 LSA, Link State Advertisement, 526, 562
 typy pakietów, 573
 LSack, Link State Acknowledgment, 526
 LSDB, Link State Database, 525, 545
 LSP, Link State Packet, 525
 LSU, Link State Update, 526
 LWAPP, Lightweight Access Point Protocol, 750

M

MAC, Media Access Control, 47, 101, 111, 831
 malware, 802
 maska
 odwrotna, 530, 608
 podsieci, 256

maszyna wirtualna, 920
 tworzenie, 167
 ustawienia, 174, 781
 w GNS3, 176
 z serwerem GNS3, 180, 182
 z vWLC, 780
 MD5, 569, 656, 714, 718
 konfiguracja, 656, 657
 media transmisyjne, 32
 bezprzewodowe, wireless, 58
 menedżer urządzeń, 208
 metody przekazywania informacji
 in-band, 885
 out-of-band, 884
 metryka w OSPF, 547
 mGRE, Multipoint Generic Routing Encapsulation, 713
 MIB, Management Information Base, 886
 MIC, Message Integrity Check, 774
 Microsoft Network Monitor
 konfiguracja programu, 762, 764, 765
 przechwytywanie ramek wi-fi, 761
 MIMO, Multiple Input Multiple Output, 752
 model
 AAA, 840
 hierarchiczny, 331
 klient – serwer, 928
 OSI, 87
 sieci WAN, 684
 TCP/IP, 85
 modele QoS, 851
 modem, 683
 moduł SFP, 343
 MPLS, Multi-Protocol Label Switching, 684
 multicast, 43, 44
 multipoint
 konfiguracja, 695

N

nadmiarowość, 409
 nagłówek
 IP, 251
 IPv6, 304
 TCP, 94
 UDP, 96
 narzędzie uderzeniowe, 56
 NAT, Network Address Translation, 253, 622
 dla IPv6, 643
 dynamiczny, 626

statyczny, 623
 z przeciążeniem, overloaded NAT, 627
 NAT64, 305
 NBAR, Network Based Application Recognition, 852
 NCP, Network Control Protocol, 682
 Neighbor Solicitation, 314
 NetFlow
 działanie protokołu, 896
 konfiguracja kolektora, 899
 konfiguracja na routerze, 898
 parametry pracy, 901
 wybór sensora, 900
 NGFW, Next Generation Firewall, 50, 835
 NGIPS, Next-Generation Intrusion Prevention System, 835
 NHRP, Next Hop Resolution Protocol, 713
 NIC, Network Interface Controller, 46
 Npcap, 163
 NTP, Network Time Protocol, 448
 NVRAM, Non-Volatile Random Access Memory, 438

O

obiekt
 Cloud, 225, 228
 Ethernet switch, 362
 obszar zerowy, backbone area, 585
 odekodowanie, decoding, 45
 OFDM, Orthogonal Frequency Division Multiplexing, 748
 okablowanie, 53
 poziome, horizontal cabling, 60
 szkieletowe, building backbone cabling, 60
 opóźnienie, delay, 35
 oprogramowanie
 jako usługa, SaaS, 919
 szpiegujące, 797
 organizacje standaryzujące, 39
 OSI
 warstwa
 aplikacji, 88
 fizyczna, 114
 łącza danych, 111
 prezentacji, 91
 sesji, 91

sieci, 100
 transportu, 92
 OSPF, Open Shortest Path First, 489, 529
 baza danych, 545
 konfiguracja, 529, 702, 964
 alternatywna, 534
 passive-interface, 556
 metryka, 547
 przepustowość, 548
 ręczne ustalanie kosztu, 552
 zmiana parametrów, 553
 polecenia weryfikujące, 580
 redystrybucja do sieci
 RIPng, 587
 relacje sąsiedztwa, 540
 rozgłaszanie tras
 domyślnych, 557
 równoważenie obciążenia, 537
 status interfejsu, 540
 2WAY, 541
 Down, 540
 Exchange, 541
 ExStart, 541
 Init, 541
 Loading, 541
 uwierzytelnianie, 568
 w sieciach
 wielodostępowych, 557
 wieloobszarowy, 571
 konfiguracja, 573
 redystrybucja tras
 domyślnych, 578
 redystrybucja tras
 statycznych, 579
 właściwości interfejsów, 546
 wybór routerów DR i BDR, 528, 558
 OSPFv2, 525
 pakiety hello, 526
 OSPFv3, 583
 konfiguracja, 583

P

PaaS, Platform as a Service, 919
 PAGP, Port Aggregation Protocol, 673
 pakiet
 database description, 526
 hello, 526, 543
 ID obszaru, 527
 identyfikator routera, 526
 intervals, czasy, 527

List of Neighbors, 529
 network mask, 528
 router priority, 528
 typ komunikatu, 526
 IP
 ładunek, payload, 250
 nagłówki, header, 250
 LSA, 526, 562, 573
 LSack, 526
 LSP, 525
 LSR, 526
 LSU, 526
 SYN, 141, 736
 SYN/ACK, 141, 736
 pamięć
 flash, 204, 206, 438
 NVRAM, 204, 438
 RAM, 215, 438
 panel krosowniczy, patch panel, 56
 PAP, Password Authentication Protocol, 688
 pasmo, band, 34, 550
 passive-interface, 514, 570
 PAT, Port Address Translation, 628
 PCP, Payload Compression Protocol, 617
 peer, 726, 730
 pętla, 409, 410
 zwrotna, loopback, 254
 phishing
 głosowy, 805
 SMS, 805
 piaskownica, sandbox, 51
 platforma jako usługa, PaaS, 919
 plik z konfiguracją routera, 205, 237
 pliki .ova, 180, 780
 PMF, Protected Management Frames, 775
 podinterfejsy, subinterfaces, 468, 694
 połączenie
 przewodu konsolowego, 206
 wirtualnego routera, 225
 podpis elektroniczny, digital signature, 720
 podsieci, 268, 325
 podział sieci, 268
 klasa A, 254, 280, 289
 klasa B, 254, 277, 288
 klasa C, 254, 269, 284
 liczba hostów, 284, 288–290
 w IPv6, 325
 PoE, Power over Ethernet, 332
 point-to-point
 konfiguracja, 703

polecenia

- diagnostyczne w IPv6, 327
- niepoprawne, 213
- przeglądanie historii, 213
- testujące, 446
- weryfikujące OSPF, 580

polecenie

- accept-lifetime, 657
- access-list ?, 594
- access-list 1 permit, 627
- access-list 1 permit any, 596
- access-list 100 ?, 607
- access-list 2 deny ?, 599
- access-list 2 permit any, 599
- alias exec, 450
- alias, 246
- area 0 authentication, 568
- arp -a, 338, 670
- arp -d, 671
- authentication [], 724
- auto secure, 843
- auto-cost reference-bandwidth, 547, 553
- bandwidth, 548, 973
- banner motd, 219, 940
- boot system flash:, 244
- channel-group [] mode, 673
- clear ip dhcp binding *, 633
- clear ip ospf process, 527, 539, 581
- clear mac-address-table dynamic, 340
- clock rate, 444, 708
- clock timezone, 448
- config-register, 205, 224
- configure terminal, 345
- confreg 0x2142, 223
- confreg, 205
- copy running-config startup-config, 222, 225, 352, 443, 941
- copy running-config tftp, 236
- copy startup-config tftp, 941
- copy startup-config running-config, 224
- copy tftp flash:, 243, 245
- copy tftp running-config, 238
- crypto isakmp enable, 724
- crypto isakmp identity address, 726
- crypto isakmp key 0, 726
- crypto isakmp policy, 724
- crypto key generate rsa, 356, 445, 940
- crypto map [] ipsec-isakmp, 727
- debug capwap console cli, 794
- debug ip icmp, 878

- debug ip ospf adj, 581
- debug ip ospf packet, 541
- debug ip rip, 511, 516
- debug ipv6 rip, 523
- debug kron all, 241
- debug matm all, 341
- default-information originate, 512, 557, 579
- delete vlan.dat, 406
- deny icmp [] echo-request, 620
- deny ip host, 612
- deny ipv6 any any, 617
- deny, 603
- description, 941
- dir flash:, 244, 247
- dns-server [], 640
- dns-server, 630
- do show access-list, 604
- do show clock, 346
- do show interface, 378
- do show mac address-table, 374
- domain-name [], 640
- duplex, 352
- enable secret, 217, 218, 345, 441
- enable, 345
- encapsulation frame-relay, 704
- encapsulation dot1q, 468
- encapsulation frame-relay, 696, 708
- encapsulation ppp, 689
- encryption [], 724
- errdisable recovery cause psecure-violation, 379
- errdisable recovery interval, 379, 818
- exec-timeout 0 0, 441, 453
- exec-timeout, 453
- extended ping, 879
- foreach address, 447
- frame-relay interface-dlci, 704
- frame-relay intf-type dce, 708
- frame-relay map [] broadcast, 699
- frame-relay route [], 708
- frame-relay switching, 708
- hash, 725
- hostname SSH_TEST, 356
- hostname, 216, 345, 950
- interface [] point-to-point, 704
- interface fa0/0, 441
- interface loopback, 478
- interface range, 351

- interface vlan, 349, 950
- interface, 221, 468, 471
- ip access-group 1 ?, 595
- ip access-group 1 out, 595
- ip access-list ?, 611
- ip access-list extended, 611, 635, 975
- ip access-list standard [], 602, 603
- ip access-list standard LAN_NAT, 628
- ip address dhcp, 229, 623, 941
- ip address, 221, 441, 478, 794
- ip arp inspection, 833
- ip dhcp pool, 629
- ip dhcp snooping, 829
- ip dhcp snooping trust, 829
- ip dhcp snooping vlan 1, 829
- ip domain-lookup, 450
- ip domain-name, 356, 445, 940
- ip flow egress, 898
- ip flow ingress, 898
- ip flow-export version, 898
- ip helper-address [], 634, 635
- ip http server, 613
- ip nat inside source [] pool, 627
- ip nat outside, 624
- ip nat pool [] netmask [], 627
- ip nat, 624
- ip ofsp dead-interval, 528
- ip ospf authentication-key, 568
- ip ospf cost, 552
- ip ospf hello-interval, 528
- ip ospf message-digest-key [] md5, 569, 570
- ip ospf network point-to-point, 567
- ip ospf priority, 529
- ip ospf, 534
- ip rcmd remote-host, 454
- ip rcmd rsh-enable, 454
- ip route, 649
- ip sla, 459
- ip ssh version 2, 453, 940
- ipconfig /all, 47, 937
- ipconfig /displaydns, 132
- ipconfig /flushdns, 132
- ipconfig /renew, 633
- ipconfig -all, 380
- ipv6 access-list [], 618
- ipv6 address dhcp, 363
- ipv6 address, 317
- ipv6 dhcp pool [], 639, 641

- ipv6 dhcp relay destination, 643
- ipv6 dhcp server [], 641
- ipv6 enable, 310
- ipv6 nd other-config-flag, 638, 639
- ipv6 rip [] enable, 319, 585
- ipv6 route, 322
- ipv6 router ospf 1, 584
- ipv6 router rip, 587
- ipv6 traffic-filter [] in, 618
- ipv6 unicast-routing, 317, 321, 637
- key, 657
- key-string, 657
- kron policy-list, 240
- line console 0, 217, 441
- line vty 0 15, 217, 346
- lldp receive, 458
- lldp transmit, 458
- logging synchronous, 441
- logging synchronous level, 886
- login local, 357, 445, 941
- matm all, 341
- monitor session []
 - destination interface [], 903
- monitor session [] source [], 903
- netsh interface ipv6 show neighbors, 315
- netstat, 100
- network, 509, 576, 629, 964
- no access-list 1, 601
- no auto-summary, 517
- no cdp advertise-v2, 456
- no cdp enable, 457
- no debug ip icmp, 878
- no debug matm all, 341
- no ip address, 467
- no ip dhcp snooping
 - information option, 833
- no ip domain-lookup, 450
- no ipv6 nd managed-config-flag, 638
- no passive-interface, 556
- no service dhcp, 631
- no service timestamps, 886
- no setup express, 336
- no shutdown, 378, 876
- no spanning-tree cost, 417
- no vlan, 388
- no access-list 100, 609
- nslookup, 136
- ntp authenticate, 449
- ntp server, 448, 449
- ntp trusted-key, 449
- occurrence, 240
- passive-interface default, 556
- passive-interface, 513
- password, 217, 441
- permit any any, 619
- permit any, 603
- permit ipv6, 620
- permit tcp [] host [] eq 80, 614
- permit tcp, 975
- ping ?, 879
- ping, 252, 327
- ppp authentication chap, 690
- redistribute ospf 1 include-connected metric, 587
- redistribute ospf, 969
- redistribute rip [] metric []
 - include-connected, 586
- redistribute static subnets metric 1, 580
- reload cancel, 225
- reload in, 224
- reload, 224
- router ospf 1, 529, 702
- router rip, 509, 961
- router-id, 538, 971
- send, 451
- service dhcp, 631
- service password-encryption, 215, 940
- set peer [], 727
- set transform [], 727
- show access-lists, 595, 596, 600
- show cdp entry, 456
- show cdp interface, 457
- show cdp neighbors, 455, 583, 955
- show cdp neighbors detail, 455
- show clock, 239, 346, 448
- show controllers [], 687
- show controllers serial, 444
- show crypto ipsec sa, 728
- show crypto isakmp peers, 729, 731
- show crypto isakmp policy, 725
- show crypto isakmp sa, 726, 730
- show crypto map, 728
- show etherchannel summary, 674
- show flash, 406
- show frame-relay lmi, 701
- show frame-relay map, 710
- show glbp brief, 670
- show glbp, 668
- show interface brief | json, 926
- show interface brief | xml, 927
- show interface trunk, 392, 393
- show interface, 378, 877
- show interfaces trunk, 820
- show interfaces, 390
- show ip arp inspection, 833
- show ip cache flow, 898
- show ip dhcp binding, 630, 825
- show ip dhcp conflict, 635
- show ip dhcp pool, 630
- show ip dhcp snooping, 830
- show ip flow export, 899
- show ip interface brief, 220, 349, 458, 674, 735
- show ip interface, 597
- show ip nat translations, 625, 629
- show ip ospf database, 545
- show ip ospf interface, 535
- show ip ospf interface brief, 546, 580, 967
- show ip ospf neighbor, 535, 540, 575
- show ip protocols, 510, 515, 531, 580
- show ip route, 152, 465, 476, 702, 957
- show ip route connected, 494
- show ip route ospf, 533, 710
- show ip route static, 479
- show ip sla statistics, 460
- show ip ssh, 359, 452
- show ip interface brief, 444
- show ipv6 dhcp pool, 640, 642
- show ipv6 int, 312
- show ipv6 int brief, 311, 317
- show ipv6 interface, 307, 318, 362
- show ipv6 ospf interface brief, 585
- show ipv6 ospf neighbor, 586
- show ipv6 protocols, 519, 521
- show ipv6 rip database, 523
- show ipv6 route, 322, 519
- show ipv6 route rip, 521, 522
- show ipv6 route static, 324
- show kron schedule, 240
- show mac address-table, 339, 373

polecenie

show mac-address-table |
include, 342
show mac-address-table
interface, 342
show ntp association, 449
show port-security, 368,
374, 377, 948
show port-security
interface, 371–74, 377
show post, 206
show processes, 341
show processes cpu
monitor, 814
show run | section crypto,
726
show running | incl access,
597
show running | section
include con|vty, 218
show running-config | begin
line vty, 346
show running-config | incl
access-list 1, 601
show running-config |
section line, 454
show running-config
interface, 443
show running-config, 215,
218
show session, 446
show snmp, 890, 892
show snmp community, 890
show snmp user, 892
show spanning-tree
summary, 817
show spanning-tree, 411, 413,
415, 422, 672, 675, 814
show standby, 652, 659
show startup-config, 221
show switch, 364
show users, 451, 605
show version, 204, 214
show vlan, 348, 385
show vlan brief, 386, 387,
404, 464, 945
show vrrp, 661, 662
show vtp password, 404
show vtp status, 400–402
shutdown, 659
snmp-server community []
ro, 888
snmp-server contact, 889
snmp-server group, 891
snmp-server host, 889
snmp-server location, 889
snmp-server view, 891

spanning-tree [] root
primary, 425
spanning-tree bpduguard
enable, 818
spanning-tree cost, 417
spanning-tree mode rapid-
pvst, 428
spanning-tree portfast, 421,
817, 946
spanning-tree vlan [] root
primary, 947
standby [] authentication ?,
655
standby [] authentication
md5 key-chain, 658
standby [] preempt, 653
standby 1 timers ?, 654
standby 1 track, 658
startup-config is not present,
222
static, 376
sudo apt install dsniff, 812
sudo ifconfig, 812
sudo ip route, 812
sudo netdiscover -r, 812
switchport access vlan, 388,
463, 950
switchport mode access,
369, 388, 463, 950
switchport mode dynamic
desirable, 396
switchport mode trunk, 391,
396, 469
switchport mode trunk
native vlan 999, 393
switchport nonegotiate, 395
switchport port-security
mac-address ?, 370
switchport port-security
mac-address sticky, 370
switchport port-security
max 1, 948
switchport port-security
maximum 1, 371
switchport port-security
violation ?, 371
switchport port-security
violation shutdown, 948
switchport port-security,
368
switchport trunk allowed
vlan, 393
switchport trunk
encapsulation dot1q, 392,
951
tclquit, 448
tclsh, 447
telnet, 451

tftp-server flash:, 246
trace, 466
traceroute, 327, 446
tracert, 533
track [] line-protocol, 666
transport input ssh, 357,
445, 451, 941
transport input telnet ssh, 451
tunnel destination [], 733
tunnel source [], 733
tunnel mode gre ip, 733
type, 376
undebg all, 341, 511, 524,
878
undebg, 511
username [] autocommand
menu, 458
username [] password [],
690
username [] secret [], 356
version 2, 515
vlan, 387, 945
vrrp [] ip, 660
vrrp [] timers advertise
msec, 664
vtp domain, 402, 944
vtp mode client, 401, 944
vtp password, 404, 944
vtp pruning, 407
write memory, 240
yersinia -G, 814, 825

połączenia
optyczne, optical fiber, 684
point-to-point, punkt-punkt,
566
site-to-site, 711
SSL/TLS, 736
typu trunk, 368, 383, 389,
394, 819
VPN GRE, 733

wi-fi
asocjacja, 766
odkrywanie, 765
tryb aktywny, 766
tryb pasywny, 767
uwierzytelnianie, 766

wirtualne
przełączane, SVC, 681
stałe, PVC, 681

pomoc, 211
POP3, Post Office Protocol, 90
port, 99
alternatywny, alternate port,
415, 428
AUX, auxiliary, 439
brzegowy, edge port, 431
desygnowany, designated
port, 415, 419, 428

- dystrybucyjny, distribution system port, 779
- główny, root port, 415, 428
- konsolowy, console port, 779
- niedesygnowany, non-designated port, 415
- typu trunk, 389
- zapasowy, backup port, 428
- Port Security, 332, 372
 - konfiguracja, 369
 - zmiana adresu MAC, 379
- PortFast, 420, 421, 431
- potwierdzenie LSack, 564
- PPP, Point-to-Point Protocol, 682
 - konfiguracja, 689
 - uwierzytelnianie, 690
- Preemption, 652, 653
- prędkość, 37
 - pobierania, 881
- problemy z interfejsami, 876
- proces
 - EUI-64, 308
 - wymiany kluczy, 355
- program
 - antywirusowy, 836
 - Cisco Feature Navigator, 242
 - Cisco Prime NAM, 917
 - Cpulimit, 163
 - Dynamips, 163
 - GNS3, 160
 - iperf, 882
 - Kiwi Syslog, 887
 - Microsoft Network Monitor, 762
 - Npcap, 163
 - PRTG, 892
 - QEMU, 163
 - Solar Winds Response, 163
 - SuperPutty, 164, 195
 - Tftpd64, 235
 - TightVNC Viewer, 164
 - VirtualBox, 166
 - VMware Workstation Pro, 166
 - VPCS, 163
 - vWLC, 780
 - Wireshark, 126, 163, 761
 - Yersinia, 821
- projektowanie sieci, 905
 - bezpieczeństwo, 911
 - dokumentacja, 915
 - harmonogram, 910
 - określenie wymagań, 911
 - projekt fizyczny, 908
 - projekt logiczny, 908
 - schemat Cisco PPDI00, 909
- protokoły
 - bezklasowe, 525
 - bezpieczeństwa sieci, 37
 - bezpółłączeniowe, connectionless, 250
 - distance vector, 491
 - IPsec hashujące
 - MD5, 714
 - SHA, 714
 - IPsec negocjacyjne
 - AH, Authentication Header, 714
 - ESP, 617, 714
 - IPsec ochrony procesu wymiany kluczy
 - Diffiego-Hellmana, 715
 - IPsec szyfrowania
 - 3DES, 714
 - AES, 714
 - DES, 714
 - SEAL, 714
 - klasowe, classful, 506
 - komunikacji sieciowej, 37
 - link state, 492
 - redundancji, 647
 - routingu, 37
 - routingu dynamicznego, 489, 490
 - sieciowe, 36
 - wykrywania usług, 37
- protokół
 - 802.1.x, 841
 - AHP, 617
 - ARP, 121, 145, 434, 446
 - BGP, 490
 - BPDU, 411
 - CAPWAP, 772
 - CCMP, 774
 - CDP, 455, 583, 878
 - CHAP, 688
 - DHCP, 90, 623
 - distance vector, 491, 492, 507
 - DTLS, 773
 - DTP, 368, 395
 - EAP, 842
 - EIGRP, 489, 534
 - ESP, 617, 714
 - FTP, 91
 - GLBP, 648, 668
 - HSRP, 647
 - HTTP, 89, 614
 - ICMP, 109, 140, 157, 250, 617
 - IGRP, 489
 - IKE, 717
 - IPv4, 250
 - IPv6, 303
 - IS-IS, 489
 - LACP, 673
 - LCP, 685, 687
 - link state, 492
 - LLDP, 458
 - LWAPP, 750
 - mGRE, 713
 - MPLS, 684
 - NCP, 687
 - NetFlow, 896
 - NHRP, 713
 - NTP, 448
 - OSPF, 489
 - OSPFv2, 525
 - OSPFv3, 583
 - PAGP, 673
 - PAP, 688
 - PCP, 617
 - POP3, 90
 - PPP, 682, 687
 - PVST, 422
 - RIP, 489, 494, 499, 506, 514
 - RIPng, 320, 518
 - RIPv1, 506
 - RIPv2, 489, 514
 - RSTP, 427
 - SAE, 774
 - SDEE, 838
 - SMTP, 90
 - SNMP, 886
 - SSH, 352, 445
 - SSL, 90, 355, 736
 - SSL/TLS, 736
 - STP, 409
 - TCP, 93, 141
 - telnet, 352
 - TLS, 736
 - UDP, 96, 138
 - VRRP, 648
 - VTP, 399
 - X.25, 683
- PRTG
 - dodawanie urządzenia, 894
 - konfiguracja, 892
 - okno główne, 893
 - ustawienia SNMP dla urządzenia, 895
 - ustawienia urządzenia, 894
- przechwytywanie pakietów, 129
- przekierowywanie portów, 802
- przełączanie
 - obwodów, circuit switched, 678
 - pakietów, packet switched, 679
 - przełączanie procesów, process switching, 436

przełączanie
 pakietów, packet switched,
 przełączanie szybkie, fast
 switching, 436
 metoda CEF, 438
 przełącznik, switch, 28, 49, 331,
 750
 Ethernet switch, 362
 Frame Relay, 691, 695
 root bridge, 416, 418, 425
 stack master, 364
 warstwy 2., 334
 jednomodułowy, 334
 modularny, 334
 warstwy 3., 470
 control plane, 922
 forwarding plane, 922
 metoda CEF, 471
 tablica FIB, 922
 tablica przynależności,
 471
 tablica RIB, 922
 przełączniki
 autouruchamianie
 interfejsu, 379
 buforowanie
 port-based memory
 buffering, 344
 shared memory
 buffering, 344
 diody, 335
 dodatkowe interfejsy, 343
 emulowane w GNS3, 359
 funkcjonalność VTP Pruning,
 407
 interfejsy
 FastEthernet, 347
 GigabitEthernet, 347
 wyłączenie, 351
 zmiana parametrów, 351
 zmiana szybkości, 351
 konfiguracja
 adresu IP, 347
 adresu IPv6, 362
 bramy domyślnej, 347
 komunikatu
 ostrzegającego, 347
 podstawowa, 345
 Port Security, 367, 369
 zapisywanie, 352
 zerowanie, 336
 naruszenie bezpieczeństwa,
 376, 378
 negocjacja typu połączenia,
 397
 podłączanie urządzeń, 342
 pracujące w stosie, 363

protokół
 PVST, 422
 RSTP, 427
 STP, 409
 VTP, 399
 przełączanie ramek
 cut-through, 344
 fast-forward switching,
 344
 fragment-free switching,
 344
 store-and-forward, 344
 schemat współpracy, 923
 stany portów, 419
 statusy STP, 419
 tablica adresów MAC, 336
 czas starzenia się, age
 time, 338
 statyczne dodanie wpisu,
 342
 tryby pracy
 client, 399
 transparent, 400
 server, 399
 warstwy
 dostępu, 332
 dystrybucji, 333
 rdzenia, 333
 włączenie protokołu SSH,
 352
 przepływność
 gwarantowana minimalna,
 681
 niegwarantowana
 maksymalna, 681
 przepustowość, bandwidth, 34,
 548
 przewód
 DB60-DB60, 686
 koncentryczny, coaxial
 cable, 67
 konsolowy, 207
 miedziany, copper cable, 58,
 61
 światłowodowy, fiber-optic
 cable, 58, 67
 z przeplotem, crossover
 cable, 64
 PSK, Pre-Shared Keys, 720
 punkt dostępowy, access point,
 742, 750, 760
 adres MAC, 742
 identyfikator SSID, 768
 komunikacja z WLC, 789
 konfiguracja, 769, 771, 778,
 794

tryb pracy
 autonomous, 750
 controller-based, 750
 w vWLC, 788
 PVC, Permanent Virtual
 Circuits, 681, 692
 PVRST, Per-VLAN Rapid
 Spanning Tree, 422
 PVST, Per-VLAN Spanning Tree,
 412, 422
 konfiguracja, 425

Q

QEMU, 163
 QoS, Quality of Service, 79, 384,
 847
 fluktuacje, jitter, 849
 kolejkovanie, 847
 kształtowanie ruchu, 854
 model
 best-effort, 851
 differentiated services,
 DiffServ, 851
 integrated services,
 IntServ, 851
 opóźnienie, delay, 849
 parametr CIR, 856
 priorytetyzacja ramek, 848
 przeciążenie, congestion,
 849
 przepustowość, bandwidth,
 849
 wąskie gardło, bottleneck,
 849
 wdrażanie, 851
 znakowanie pakietów
 pole CoS, 852
 pole DSCP, 852
 pole ECN, 853, 854
 pole IPP, 852, 853
 pole PRI, 852
 pole TID, 852
 pole Traffic Class., 853
 pole Type of Service, 853

R

RADIUS, 842
 RAM, Random Access Memory,
 438
 ramka beacon
 nagłówków, 767, 768
 BSS Id, 767
 Destination address, 767
 Receiver address, 767
 Source address, 767
 Transmitter address, 767

- pola w Wireshark, 769
- pole
 - Channel, 767
 - Frame Body, 767
 - Frequency, 767
 - Signal strength, 767
 - Timestamp, 767
- ramka wi-fi
 - Dane, 761
 - FSC, suma kontrolna, 761
 - nagłówki, 752
 - Adres 1, 754, 757–759
 - Adres 2, 757–759
 - Adres 3, 757–759
 - Adres 4, 757, 759
 - Czas trwania, 754
 - Pole kontrolne ramki, 753, 754
 - Sekwencja sterująca, 754
- Podtyp ramki
 - ACK, 757
 - association request, 755
 - association response, 755
 - authentication, 756
 - beacon, 756, 767
 - CTS, 756, 757, 765
 - deauthentication, 756
 - disassociation, 756
 - probe request, 755, 766
 - probe response, 755, 766
 - reassociation request, 755
 - reassociation response, 755
 - RTS, 756, 757, 765
- Pole kontrolne ramki
 - FromDS, 757–760
 - Podtyp ramki, 754–757
 - Powtór, 761
 - ToDS, 757–760
 - Typ ramki, 754
 - Wersja protokołu, 754
 - Więcej danych, 761
 - Zabezpieczenia, 761
 - Zarezerwowane, 761
 - Zarządzanie energią, 761
- ramki
 - BPDU, 411
 - DTP, 398
 - ethernetowe, 112, 116, 118, 383
 - ICMP, 157, 249
 - priorytetyzacja, 848
 - rozgłoszeniowe ARP, 146, 149, 150
 - rozgłoszeniowe, broadcast, 407, 409
 - SSH, 358
- ransomware, 802
- raportowanie, 884
- RC, Rives Cipher, 716
- redundancja, 333, 646
- redystrybucja, 969
 - OSPF, 587
 - RIP, 586
 - RIPng, 587
 - tras
 - domyślnych, 578
 - statycznych, 579
- rekonesans, 801
- relacje sąsiedztwa, 531, 540
 - status urządzeń, 565
- resetowanie hasła, 223
- RESTful API, 928
- reverse engineering, 300
- RFC, 29
- RIP, Routing Information Protocol, 489, 494, 499
 - konfiguracja protokołu, 968
 - wymiana komunikatów, 511
- RIPng, 320, 518
 - konfiguracja protokołu, 519
- RIPv1
 - działanie protokołu, 506
 - konfiguracja protokołu, 507
- RIPv2
 - konfiguracja protokołu, 514
- robak, 797, 801
- rollover, 65
- root bridge, 815
- rootkit, 803
- router, 28, 49
 - ABR, 572
 - sumaryzacja tras, 577
 - ASBR, 572
 - BDR i DR, 528
 - połączenie punkt – punkt, 566
 - wybieranie, 528, 558
 - zmienianie, 560
- Cisco
 - 1941, 439
 - 2800, 207
 - 3745, 462
 - 7200, 508
 - CSR1000V, 863
- router-on-a-stick, 467
- routery
 - budowa, 438
 - działanie, 433
 - funkcjonalność Cisco IP SLA, 459
 - jako
 - agent przekazujący, 642
 - klient NTP, 448
 - przełącznik, 360
- serwer DHCP, 629
- serwer DHCPv6, 637
- komunikacja w sieci Ethernet, 148–157
- konfiguracja
 - automatyczne
 - zapisywanie, 239
 - interfejsów, 220, 307, 694
 - NAT, 624
 - wstępna, 216, 440
 - za pomocą Web UI, 862
 - zarządzanie, 221–223
 - zarządzanie zdalne, 454
- pakiety
 - enkapsulacja, 153–156, 435
 - filtrowanie, 591
 - przełączanie, 438, 679
 - rodzaje, 525
- podłączanie
 - w GNS3, 193
 - przez interfejs Serial, 444
- protokoły
 - distance vector, 491, 492, 506
 - link state, 492
- protokół
 - CDP, 455, 583, 878
 - LLDP, 458
- restartowanie, 224
- status
 - 2-WAY/DROTHER, 565
 - Active, 659
 - backup, 667
 - FULL/DR, 565
 - Master, 667
 - Standby, 659
- tablica
 - ARP, 153
 - routingu, 152, 433, 493
- uruchamianie usługi TFTP, 244
- wartość AD, 484
- wirtualny
 - konfiguracja, 192
 - połączenie z siecią rzeczywistą, 225
- wstępna konfiguracja, 216, 440
 - czas bezczynności, 453
 - odwzorowanie nazw domenowych, 450
 - polecenia testujące, 446
 - protokół ARP, 446
 - protokół SSH, 445
 - tworzenie aliasu, 450

routery
 wstępna konfiguracja
 wysyłanie komunikatów, 451
 wyświetlanie listy użytkowników, 450
 własne menu, 458
 wybór trasy, 481–484
 wymiana informacji, 491, 541
 zmiana identyfikatora, 538

routing
 dynamiczny, 488
 protokoły, 489–492
 protokół OSPFv2, 525
 protokół OSPFv3, 583
 protokół RIP, 506
 protokół RIPv2, 518
 protokół RIPv1, 507
 protokół RIPv2, 514
 metoda
 klasyczna, 462
 router-on-a-stick, 467
 pomiędzy sieciami VLAN, 462
 statyczny, 474

rozgłaszanie
 wyłączanie, 512
 trasy domyślnej, 512, 557

rozwiązywanie problemów
 adresacja IP, 918
 analizatory protokołów, 917
 błędna konfiguracja ACL, 918
 błędy okablowania, 918
 Cisco Prime NAM, 917
 dziel i zwyciężaj, 916
 od ogółu do szczegółu, 907
 od szczegółu do ogółu, 916
 podstawienie innego urządzenia, 916
 utrata połączenia, 917
 wąskie gardło, 849, 917
 równoważenie obciążenia, load balancing, 537
 RSTP, Rapid Spanning Tree Protocol, 427
 konfiguracja, 428
 porty, 428
 stany, 427

S

SaaS, Software as a Service, 919
 SAE, Simultaneous Authentication of Equals, 774
 SDEE, Security Device Event Exchange, 838
 SDH, Synchronous Digital Hierarchy, 679

SDN, Software-Defined Network, 922
 segmentacja, 142
 sekwencyjne przesyłanie danych, 143
 serwer, server, 48
 czasu, 449
 DHCP, 321, 623, 629, 825
 DHCPv6, 637
 bezstanowy, 638
 stanowy, 641
 DNS, 135
 autorytatywny, 140
 domeny głównej, 140
 lokalny, 140
 TLD, 140
 GNS3, 180, 181
 iperf, 883
 NAS, 739
 NHRP, 713
 RADIUS, 795
 TFTP, 234
 VPN, 721
 SFP, Small Form Factor Plugable, 343
 SHA, Secure Hash Algorithm, 718
 sieć bezprzewodowa, 41, 73, 741
 ataki, 775
 bezpieczeństwo, 773
 częstotliwości i kanały, 746, 747
 działanie sieci, 743
 format ramki, 752
 identyfikator SSID, 750, 769
 mechanizm
 CSMA/CA, 756, 765
 CSMA/CD, 756
 DFS, 747
 MIC, 774
 TPC, 747
 parametr SNR, 752
 podłączanie klienta, 765
 projektowanie, 776
 punkt dostępowy, 760
 system WDS, 760
 szyfrowanie, 773
 technika
 DSSS, 748
 FHSS, 748
 OFDM, 748
 tethering, 752
 tryb pracy
 access point, 742
 ad hoc, 742, 757
 unikanie kolizji, 756, 765
 urządzenia bezprzewodowe, 749

ustawienie
 nazwy sieci, 770
 trybu działania, 771
 uwierzytelnianie, 771
 VLAN, 742
 WLAN, 741
 WPAN, 741
 WWAN, 741
 zastosowanie, 776

sieci
 architektury, 81
 automatyzacja, 924
 awarie, 874
 bezpośrednio podłączone, include-connected, 586
 domowe, 76
 Ethernet, 116
 Frame Relay, 691
 internet, 42, 52, 881
 komputerowe, 30
 konwergentne, 78
 LAN, 41
 NBAR, 852
 niekonwergentne, 78
 OSPF wielobszarowe, 572
 OSPFv3, 584
 projektowanie, 905–915
 rozwiązywanie problemów, 916
 SAN, 41
 SDN, 922
 kontroler SDN, 923
 sprawdzanie komunikacji, 879
 testowanie
 łącza internetowego, 881
 połączeń, 882
 topologie, 74
 typu
 broadcast multiaccess, 557
 point-to-point, 557, 565, 679, 686, 703
 VLAN, 347, 382, 742, 806
 VPN, 32, 711
 WAN, 42, 678
 wielodostępowe, 557
 wi-fi, 741
 wirtualizacja, 918
 zastosowanie
 sztucznej inteligencji, 930
 uczenia maszynowego, 930
 zbieżność, convergence, 36, 488
 signature matching, 838
 skalowalność, scalability, 79

skrętka
 ekranowana, 62
 nieekranowana, 62
 skróty klawiaturowe, 212
 SLAAC, Stateless Address
 Autoconfiguration, 321, 637
 SMTP, Simple Mail Transport
 Protocol, 90
 SNMP, Simple Network
 Management Protocol, 886
 działanie protokołu, 886
 konfiguracja, 887, 888
 Object Navigator, 891
 SNMPv2c
 konfiguracja, 887
 SNMPv3
 konfiguracja, 890
 SOHO, small office and home
 office networks, 76
 Solar Winds Response, 163
 SONET, Synchronous Optical
 Networking, 679
 span port
 konfiguracja, 900
 SPF, Shortest Path First, 525
 spyware, 797, 802
 SSH, secure shell, 352, 353, 445
 SSID, Service Set Identifier, 742
 SSL, Secure Sockets Layer, 90,
 736
 Change Cipher, 736
 handshake, 736
 stacja robocza, workstation, 46
 standardy sieci wi-fi, 748
 static NAT, 623
 statystyki IP SLA, 460
 stos, stack, 363
 STP, Spanning Tree Protocol,
 409
 ataki, 806, 813, 815
 działanie protokołu, 410,
 411
 PortFast, 420
 rodzaje portów, 415
 rozszerzenie PVST, 422
 status
 blocking, blokowanie,
 419
 forwarding,
 przekazywanie, 419
 learning, uczenie się, 419
 listening, nasłuchiwanie,
 419
 sumaryzacja
 sieci, 325
 tras, 577
 tras statycznych, 478
 trzech podsieci, 480

SuperPutty, 164, 195
 Commands, 197
 Host, 208
 konfiguracja programu, 195
 okno główne, 196, 209
 połączenie z urządzeniem,
 195
 Protocol, 208
 Rename Tab, 197
 Serial, 208
 suplikant, supplicant, 842
 SVC, Switched Virtual Circuits,
 681
 symulator Cisco Packet Tracer,
 160, 198
 syslog, 885
 system
 binarny, 37
 IDS, 836
 IPS, 835–837
 NGIPS, 835
 operacyjny IOS, 185, 206
 pomocy, 211
 szablony, 929
 szafa krosownicza, 54
 sztuczna inteligencja, AI, 930
 szyfrowanie danych,
 encryption, 79, 774
 metoda asymetryczna, 717
 metoda symetryczna, 716
 typ, 219
 w VPN, 713

Ś

światłowód
 jednomodowy, single-mode
 fiber, 68
 wielomodowy, multi-mode
 fiber, 68

T

tablica
 ARP, 147, 153, 671, 831
 DNS, 132
 FIB, 922
 MAC, 336, 831
 czyszczenie, 340
 obserwacja czynności, 341
 statyczne dodanie wpisu,
 342
 wyświetlanie, 339, 374
 przynależności, adjacency
 table, 437, 471
 RIB, 922

routingu, routing table, 152,
 433, 493
 cold start, 491
 initial exchange, 491
 level 1 parent route, 495
 level 1 route, 495
 najdłuższe dopasowanie,
 483
 odtwarzanie topologii
 sieci, 496, 502
 przeszukiwanie, 496
 relacje sąsiedztwa, 531
 stacji roboczej, 504
 ultimate route, 495
 wpis connected,
 bezpośrednio
 połączone, 435, 494
 wpis default route, 481
 wpis dynamic,
 dynamiczny, 435
 wpis L, local, 494
 wpis O*E2, 557, 579
 wpis R, RIP, 494
 wpis static, statyczny,
 435, 476
 wyświetlanie, 152, 155,
 320
 translacji, 629
 TCP, Transmission Control
 Protocol, 93
 kontrola przepływu, 142
 maksymalny rozmiar
 segmentu, 144
 uzgodnienie three-way
 handshake, 141
 TCP/IP
 warstwa
 aplikacji, 86
 dostępu do sieci, 87
 internetowa, 87
 transportu, 86
 technologia
 ATM, 684
 DMVPN, 713
 DSL, 682
 DWDM, 679
 Frame Relay, 680, 690
 GRE, 732
 ISDN, 681
 SDH, 679
 SONET, 679
 VPN, 711
 WDS, 760
 X.25, 683
 telnet, 352
 teredo, 305

- testowanie
 - łącza internetowego, 881
 - połączenia w sieci lokalnej, 882
 - TFTP, 234
 - konfiguracja serwera, 235
 - kopiowanie konfiguracji, 234, 238
 - uruchamianie na routerze, 244
 - Tftpd64, 235
 - three-way handshake, 141
 - analiza, 143
 - TightVNC Viewer, 164
 - TKIP, Temporal Key Integrity Protocol, 774
 - TLS, Transport Layer Security, 736
 - topologia
 - dual-homed, 680
 - fizyczna, physical topology, 74
 - full mesh, 693
 - fully meshed topology, 680
 - gwiazdy, 75
 - hub-and-spoke, 679, 692, 694
 - logiczna, logical topology, 76
 - magistrali, 75
 - partial mesh, 693
 - partially meshed topology, 680
 - pierścienia, 76
 - point-to-point, 679
 - rozszerzonej gwiazdy, 75
 - TPC, Transmit Power Control, 747
 - transfer, 35
 - translacja adresów, *Patrz* NAT
 - transmisja bezprzewodowa, 73
 - transmitery sieciowe, network transmitter, 80
 - trasa
 - domyślna, default route, 323, 481
 - redystrybucja, 578
 - rozgłaszanie, 512, 557
 - Floating Static Route, 484, 487
 - nadrzędna pierwszego poziomu, 495
 - ostateczna, ultimate routes, 495
 - pierwszego poziomu, 495
 - prezentująca najdłuższe dopasowanie, 483
 - trasy
 - dynamiczne, 488, 489
 - external, 587
 - inter area, 587
 - koszty połączeń, 417
 - obliczanie, 489
 - redundantne, 552
 - sumaryzacja, 577
 - statyczne, 321, 474
 - redystrybucja, 579
 - sumaryzacja, 478
 - trunk, 368, 383, 389–394, 819
 - tryb pracy urządzenia
 - Bridged karty, 225
 - global configuration, 210
 - privileged executive, 210
 - user executive, 210
 - TTL, Time To Live, 154
 - tunel
 - CAPWAP, 772
 - GRE, 732
 - VPN, 711
 - VPN SSL, 736
 - tunelowanie, tunneling, 305, 712
 - tworzenie
 - aliasu, 450
 - konta użytkownika, 445
 - maszyny wirtualnej, 167
 - szablonów, 929
 - typy
 - anten, 751
 - pakietów LSA, 573
 - sieci VPN, 721
- ## U
- uczenie maszynowe, ML, 930
 - UDP, User Datagram Protocol, 96, 138
 - unicast, 43
 - URI, Uniform Resource Identifier, 928
 - URL, Uniform Resource Locator, 929
 - filtering, 835
 - URN, Uniform Resource Name, 929
 - uruchamianie urządzeń
 - etap Power-on Self Test, 204
 - sprawdzenie rejestru konfiguracji, 204
 - urządzenia
 - autokonfiguracja, 843
 - bezprzewodowe, 746, 749
 - anteny, 751
 - karty sieciowe, 749
 - kontrolery, 750
 - punkty dostępowe, 750
 - routerzy bezprzewodowe, 750
 - inteligentne, smart devices, 80
 - interfejs loopback, 229
 - konfiguracja, 204
 - konfiguracja za pomocą Web UI, 862
 - nadawcze, transmitter, 741
 - odbiorcze, receiver, 741
 - podłączenie przewodu, 206
 - tryby pracy, 210
 - uruchamianie, 204
 - zarządzanie, 209
 - usługa
 - DHCP, 631
 - SLAAC, 637
 - syslog, 885
 - usługi, 32
 - bezstanowe, stateless services, 637
 - chmury, 919
 - stanowe, statefull services, 637
 - usuwanie konfiguracji
 - startowej, 223
 - VLAN, 406
 - UTC, Universal Time Clock, 448
 - uwierzytelnianie, authenticate, 773
 - HSRP, 655
 - MD5, 570
 - model AAA, 840
 - poprzez serwer RADIUS, 795
 - proste, 568
 - RRRP, 664
 - w metodzie Quiet Mode, 730
 - w OSPF, 568
 - w PPP, 690
 - CHAP, 688
 - PAP, 688
 - w sieci bezprzewodowej, 766, 771
 - w VPN, 720
- ## V
- VirtualBox, 166
 - VLAN, Virtual LAN, 347, 382
 - ataki, 806, 818
 - działanie sieci, 382
 - funkcjonalność VTP Pruning, 407
 - konfiguracja sieci, 385
 - parametr private, 389
 - połączenia typu trunk, 390
 - protokół VTP, 399
 - rodzaje sieci
 - danych, data VLAN, 389
 - domyślny, default VLAN, 389

- natywny, 389, 393
 - nieoznakowany, 389
 - zarządzania, management
 - VLAN, 389
 - routing, 462
 - metoda router-on-a-stick, 467
 - model klasyczny, 463
 - tryby interfejsów, 395
 - usuwanie konfiguracji, 406
 - zastosowanie routera, 385
 - VLSM, Variable Length Subnet Masking, 254
 - Workstation Pro, 166
 - import wirtualnej maszyny, 180, 780
 - instalacja systemu
 - operacyjnego, 169, 175
 - menu podręczne, 175
 - okno główne, 168
 - tworzenie maszyny
 - wirtualnej, 168
 - Customize Hardware, 171
 - Finish, 173
 - Hardware, 172
 - Specify Disk Capacity, 171
 - Virtual machine name, 170
 - VMnet2 (Host-only), 172
 - ustawienia
 - interfejsu sieciowego, 172–174
 - maszyny wirtualnej, 174
 - wyłączanie, 175
 - VPCS, 163
 - VPN, Virtual Private Network, 32, 711
 - algorytmy szyfrowania, 714
 - bezpieczna komunikacja, 717
 - dostęp
 - poprzez przeglądarkę, 738
 - przez klienta, 739
 - integralność danych, data integrity, 713
 - protokół
 - enkapsulacji, encapsulation protocol, 712
 - operatora, provider protocol, 712
 - przenoszenia, transfer protocol, 712
 - remote access, 721, 736
 - tunel VPN SSL, 736
 - site-to-site, 721
 - implementacja, 723
 - konfiguracja, 724
 - tunel GRE, 732, 733
 - utworzenie tunelu, 731
 - szyfrowanie, encryption, 714
 - uwierzytelnianie, authentication, 713
 - zachowanie poufności, confidentiality, 713
 - VRRP, Virtual Router Redundancy Protocol, 648
 - konfiguracja, 660
 - czasów, 664
 - track, 665
 - uwierzytelniania, 664
 - przeglądanie rozgłoszeń, 663
 - VTP, VLAN Trunking Protocol, 399
 - ograniczenia, 403
 - Pruning, 407
 - zabezpieczanie hasłem, 404
 - vWLC, 780
 - aktywacja, 786
 - AP Mode, 790
 - DHCP Bridging, 783
 - konfiguracja, 783, 785
 - adresów IP, 794
 - interfejsów, 796
 - wstępna, 782
 - konsola, 784
 - logowanie, 785
 - serwer RADIUS, 795
 - strona główna, 786
 - testowanie komunikacji, 785
 - tworzenie sieci WLAN, 786
 - uruchamianie procesów, 782
 - ustawienia punktu
 - dostępowego, 788–791
 - VLAN Identifier, 782
 - zakładka Security, 787
 - zapisywanie ustawień, 784
- ## W
- WAN, Wide Area Network, 42, 678
 - linia dzierżawiona, 678
 - przełączanie obwodów, 678
 - przełączanie pakietów, 679
 - warstwa
 - TCP/IP
 - aplikacji, 86
 - dostępu do sieci, 87
 - internetowa, 87
 - transportu, 86
 - OSI
 - aplikacji, 88
 - fizyczna, 114
 - łącza danych, 111
 - prezentacji, 91
 - sesji, 91
 - sieci, 100
 - transportu, 92
 - przełączników
 - dostępu, access, 331
 - dystrybucji, distribution, 331
 - rdzenia, core, 331
 - wartość
 - AD, Administrative Distance, 484
 - BW, bandwidth, 548
 - pasma, 550
 - warunek
 - allow, przepuszczanie, 835
 - deny, blokowanie, 835
 - wąskie gardło, 849, 917, *Patrz także* rozwiązywanie problemów
 - WDS, Wireless Distribution System, 760
 - Web UI, Web User Interface, 861
 - konfiguracja routera, 862
 - menu Administration, 871
 - menu Configuration, 867
 - menu Monitoring, 865
 - menu Troubleshooting, 872
 - panel Dashboard, 862
 - wektor inicjalizujący, initialization vector, 774
 - WEP, Wired Equivalent Privacy, 773
 - WIC, WAN Interface Card, 684
 - wiersz poleceń, CLI, 723, 860
 - wi-fi, 73, 741, *Patrz sieć*
 - beziprzewodowa
 - standardy, 748
 - Windows
 - okno Połączenia sieciowe, 380
 - przypisanie adresu IPv4, 106, 109
 - WinPCAP, Windows Packet Capture, 163
 - Wireshark, 126, 163
 - analiza
 - three-way handshake, 141, 143
 - działania ARP, 145
 - działania DNS, 136
 - Domain Name System (query), 138
 - Domain Name System (response), 139
 - filtrowanie ramek, 137, 146

- Wireshark
 - funkcje programu, 126–129
 - Menu główne, 129
 - przechwytywanie
 - hasła, 569
 - pakietów HSRP, 656
 - pakietów LSA, 562
 - ramek wi-fi, 761
 - sesji logowania, 738
 - segmentacja, 142
 - śledzenie strumienia TCP, 353, 354
 - tryb monitorowania, 762
 - w GNS3, 247
 - wirtualizacja, 166, 920
 - sieci, 918
 - wirtualna sieć prywatna, VPN, 32, 711
 - wirus, 797, 800
 - WLAN, Wireless LAN, 741
 - w vWLC, 785
 - WLC, Wireless LAN Controller, 750, 780
 - WPA, WiFi Protected Access, 774
 - WPA2, 774
 - WPA3, 774, 775
 - WPAN, Wireless Personal Area Network, 741
 - wstrzymywanie potwierdzeń, buffering, 142
 - wytyk RJ-45, 64, *Patrz także*
 - złącze
 - WWAN, Wireless Wide Area Networks, 741
 - wybór karty sieciowej, 227
 - wyłączenie
 - autosumaryzacji, 517
 - rozgłaszania, 512
 - wyłudzenia informacji, 805
- Y**
- Yersinia, 814, 821
 - fałszywy serwer DHCP, 828
 - lista aktywnych ataków, 827
 - okno wyboru ataku, 815
 - przeprowadzanie ataku, 816, 825, 828
- Z**
- zabezpieczenie BPDU guard, 431
 - zaciskanie wtyków, 64
 - zamiana liczb
 - binarnych, 263
 - dziesiętnych, 257
 - szesnastkowych, 306
 - zapisywanie konfiguracji przełącznika, 352
 - zapora, *Patrz także* Cisco Firepower, 51
 - NGFW, 50, 835
 - sieciowa, firewall, 798
 - zapytanie
 - ARP, 147, 151
 - DNS, 135
 - zarządzanie
 - konfiguracją, 221
 - siecią, 874
 - systemem IOS, 241
 - urządzeniem, 209
 - zbieżność sieci, convergence, 36, 488
 - zdalne zarządzanie routerem, 454
 - zdalny dostęp, remote access, 712
 - zdarzenie bezpieczeństwa, 376, 378
 - złącze
 - ESCON, Enterprise Systems Connection, 71
 - FC, Fiber Connector, 70
 - LC, Lucent Connector, 69
 - MPO, Multi-fiber Push On, 70
 - MT-RJ, Mechanical Transfer Registered Jack, 71
 - SC, Subscribe Connector, 69
 - ST, Straight-Tip, 69
 - VF45, Volition Fiber, 71
 - złośliwe oprogramowanie, 802
 - zmiana
 - adresu MAC, 379
 - czasów, 554
 - identyfikatora routera, 538
 - mostu głównego, 425
 - parametrów interfejsów, 351
 - szybkości interfejsów, 351
 - znak
 - ?, 211, 494, 640
 - ^, 213
 - |, 307
 - myślnika, 670
 - zachęty, 447
 - zrównoważenie obciążenia, load balancing, 669

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 

Poznaj sieci komputerowe Cisco i przygotuj się do egzaminu certyfikującego

Sieci komputerowe są niezwykle istotną częścią ekosystemu cyfrowego świata, w którym żyjemy. Ułatwiają nam komunikację, pozwalają sprawniej zarządzać firmą czy organizacją. Dzięki nim mamy dostęp do ogromu informacji, wyników badań, statystyk i innych materiałów, możemy wymieniać się pomysłami i pracować wspólnie na jednym pliku. Bez sieci komputerowych mielibyśmy zdecydowanie mniejsze możliwości.

Ta książka przybliży Ci wiedzę o sieciach komputerowych w zakresie umożliwiającym administrowanie nimi i zdanie egzaminu certyfikującego. Wprowadzi Cię w tematykę od strony zarówno teoretycznej, jak i — przede wszystkim — praktycznej, ucząc tworzenia i konfigurowania sieci, a także wskazując coraz bardziej skomplikowane i ciekawsze kwestie dotyczące zarządzania siecią.

Dzięki tej książce opanujesz takie zagadnienia jak:

- 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

Drugie wydanie **CCNA 200-301. Zostań administratorem sieci komputerowych Cisco** zostało zaktualizowane i uzupełnione. Wiele miejsca poświęcono w nim sprawom związanym z rolą AI w rozwoju sieci komputerowych.

**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 publikacji polskich i zagranicznych z tej dziedziny. Brał udział w konferencjach naukowych (krajowych i międzynarodowych) dotyczących sieci komputerowych. Jest pracownikiem naukowym Katedry Sieci i Systemów Komputerowych Politechniki Śląskiej. Na co dzień administruje również bezpieczeństwem urządzeń sieciowych, konfiguruje między innymi urządzenia sieciowe (Cisco, HP), utrzymuje sieci WAN. Przez siedem lat kierował komórką realizacji wsparcia usług IT. Ma wieloletnie doświadczenie w pracy jako administrator sieci i projektant sieci komputerowych. Przez lata projektował serwerownie i tworzył projekty okablowania. Opracowywał procedury i dokumentację projektowe. Na koncie ma wiele zrealizowanych projektów w zakresie zakupu sprzętu IT wraz z prowadzeniem procedur przetargowych, wdrożeniem, wykonaniem dokumentacji i testami. Posiada certyfikaty: CCNA Security, CCNP Routing and Switching, Cisco CCDP, CCNAV, jak również certyfikat instruktorski Cisco CCAI, certyfikaty ITIL i PRINCE2. Jego pasją jest pisanie książek, praca ze studentami i szeroko rozumiana dydaktyka.

Helion



helion.pl



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

KOD KORZYŚCI
Sięgnij po więcej! ▶



ISBN 978-83-289-2283-9



9 788328 922839

Cena: 249,00 zł