

W drodze do CCNA

Zadania przygotowujące do egzaminu

Adam Józefiok

Zostań specjalistą — CCNA masz w zasięgu ręki!



Podstawy sieci komputerowych

Routing w sieciach komputerowych

Przełączanie w sieciach LAN

Technologie WAN i bezpieczeństwo sieci

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

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

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

Redaktor prowadzący: Ewelina Burska

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Materiały graficzne na okładce zostały wykorzystane za zgodą iStockPhoto Inc.

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

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

ISBN: 978-83-246-3319-7

Copyright © Helion 2012

Printed in Poland.

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

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

Spis treści

Wprowadzenie	9
Część I Podstawy sieci komputerowych	11
Rozdział 1. Wprowadzenie do sieci komputerowych	13
Rozdział 2. Symulatory i emulatory sieci	17
Wprowadzenie	17
Symulator sieci Cisco Packet Tracer	17
Poruszanie się w programie PT	18
Emulator GNS3	31
Wstępna konfiguracja	32
Rozdział 3. Komunikacja w sieciach LAN	35
Wprowadzenie	35
Podział sieci	35
Modele sieciowe	36
Model ISO/OSI	36
Model TCP/IP	39
Media sieciowe	40
Laboratorium 1.	42
Laboratorium 2.	42
Laboratorium 3.	43
Laboratorium 4.	43
Wskazówki do laboratoriów	43
Rozdział 4. Adresowanie w sieciach komputerowych	53
Wprowadzenie	53
Adresacja w sieciach komputerowych	54
Klasy adresów IP	54
Standardowe maski podsieci	56
Adresy prywatne i publiczne	56
Podział na podsieci — idea	56
System binarny (dwójkowy)	58
Przekształcanie liczby dziesiętnej na binarną	58
Adresacja w sieciach komputerowych	61
Tworzenie podsieci w klasie C — wymagane 31 podsieci	62
Tworzenie podsieci w klasie B — 296 podsieci	63
Tworzenie podsieci w klasie A — 3000 podsieci	64

Dzielenie sieci na podsieci na podstawie wymaganej ilości hostów	66
Tworzenie podsieci na podstawie ilości wymaganych hostów	
— klasa C (30 hostów)	66
Laboratorium 1.	69
Laboratorium 2.	70
Laboratorium 3.	70
Wskazówki do laboratoriów	71
Test sprawdzający	76
Odpowiedzi	81
Rozdział 5. Podstawowa konfiguracja urządzeń Cisco	83
Wprowadzenie	83
Podstawy IOS	83
Polecenia show	84
Wstępna konfiguracja urządzenia	87
Zapisywanie konfiguracji	87
Zabezpieczanie dostępu do urządzenia	88
Laboratorium 1.	88
Laboratorium 2.	89
Laboratorium 3.	89
Laboratorium 4.	90
Laboratorium 5.	90
Wskazówki do laboratoriów	90
Test sprawdzający	102
Odpowiedzi	104
Rozdział 6. Laboratoria podsumowujące	105
Wprowadzenie	105
Laboratorium 1.	105
Laboratorium 2.	105
Wskazówki do laboratoriów	107
Część II Routing w sieciach komputerowych	115
Rozdział 7. Działanie routera i routing statyczny	117
Istota działania routera i praca interfejsów	117
Laboratorium 1.	118
Laboratorium 2.	118
Laboratorium 3.	119
Laboratorium 4.	119
Protokół CDP	119
Laboratorium 5.	119
Laboratorium 6.	121
Laboratorium 7.	121
Routing statyczny	124
Laboratorium 8.	124
Laboratorium 9.	125
Laboratorium 10.	125
Wskazówki do laboratoriów	125
Rozdział 8. Routing dynamiczny i tworzenie podsieci	139
Laboratorium 1.	140
Laboratorium 2.	141
Laboratorium 3.	143
Laboratorium 4.	144

Laboratorium 5.	145
Wskazówki do laboratoriów	146
Test sprawdzający	154
Odpowiedzi	156
Rozdział 9. Dynamiczne protokoły routingu. RIPv1	157
Laboratorium 1.	158
Laboratorium 2.	159
Laboratorium 3.	159
Laboratorium 4.	160
Laboratorium 5.	160
Laboratorium 6.	160
Wskazówki do laboratoriów	161
Test sprawdzający	178
Odpowiedzi	180
Rozdział 10. Dynamiczne protokoły routingu. RIPv2	181
Laboratorium 1.	182
Laboratorium 2.	183
Laboratorium 3.	183
Laboratorium 4.	184
Laboratorium 5.	184
Laboratorium 6.	184
Wskazówki do laboratoriów	186
Test sprawdzający	197
Odpowiedzi	198
Rozdział 11. Dynamiczne protokoły routingu. EIGRP	199
Laboratorium 1.	201
Laboratorium 2.	201
Laboratorium 3.	202
Laboratorium 4.	202
Laboratorium 5.	203
Laboratorium 6.	203
Wskazówki do laboratoriów	204
Test sprawdzający	221
Odpowiedzi	223
Rozdział 12. Dynamiczne protokoły routingu. OSPF	225
Laboratorium 1.	227
Laboratorium 2.	228
Laboratorium 3.	228
Laboratorium 4.	228
Laboratorium 5.	230
Laboratorium 6.	230
Wskazówki do laboratoriów	231
Test sprawdzający	247
Odpowiedzi	249
Część III Przełączanie w sieciach LAN	251
Rozdział 13. Podstawy przełączania i sieci VLAN	253
Laboratorium 1.	254
Laboratorium 2.	254
Laboratorium 3.	254

Laboratorium 4.	255
Laboratorium 5.	255
Laboratorium 6.	255
Laboratorium 7.	256
Laboratorium 8.	256
Laboratorium 9.	256
Laboratorium 10.	257
Wskazówki do laboratoriów	257
Test sprawdzający	272
Odpowiedzi	273
Rozdział 14. Protokół VTP	275
Laboratorium 1.	275
Laboratorium 2.	276
Laboratorium 3.	276
Laboratorium 4.	277
Wskazówki do laboratoriów	277
Test sprawdzający	284
Odpowiedzi	284
Rozdział 15. Routing pomiędzy sieciami VLAN	285
Laboratorium 1.	285
Laboratorium 2.	286
Laboratorium 3.	286
Laboratorium 4.	287
Wskazówki do laboratoriów	288
Test sprawdzający	295
Odpowiedzi	296
Rozdział 16. Protokół STP	297
Laboratorium 1.	299
Laboratorium 2.	300
Laboratorium 3.	301
Laboratorium 4.	301
Laboratorium 5.	302
Laboratorium 6.	302
Wskazówki do laboratoriów	303
Test sprawdzający	319
Odpowiedzi	320
Część IV Technologie WAN i bezpieczeństwo sieci	321
Rozdział 17. Sieci WAN	323
Laboratorium 1.	324
Laboratorium 2.	324
Laboratorium 3.	324
Laboratorium 4.	325
Wskazówki do laboratoriów	325
Test sprawdzający	329
Odpowiedzi	331
Rozdział 18. Frame Relay	333
Laboratorium 1.	334
Laboratorium 2.	334
Laboratorium 3.	334

Laboratorium 4.	336
Wskazówki do laboratoriów	336
Test sprawdzający	348
Odpowiedzi	349
Rozdział 19. Listy ACL	351
Laboratorium 1.	352
Laboratorium 2.	352
Laboratorium 3.	352
Laboratorium 4.	352
Wskazówki do laboratoriów	353
Test sprawdzający	356
Odpowiedzi	357
Rozdział 20. Serwer DHCP i technologia NAT	359
Laboratorium 1.	360
Laboratorium 2.	360
Laboratorium 3.	360
Laboratorium 4.	361
Laboratorium 5.	361
Laboratorium 6.	362
Wskazówki do laboratoriów	363
Test sprawdzający	370
Odpowiedzi	372
Skorowidz	373

Rozdział 5.

Podstawowa konfiguracja urządzeń Cisco

Wprowadzenie

Jak już zapewne wiesz, system IOS to nic innego jak system operacyjny zainstalowany na sprzęcie firmy Cisco. Oczywiście, nie każde urządzenie posiada IOS, lecz każde wyposażone jest w system operacyjny. Niektóre urządzenia Cisco mają zainstalowane specjalnie przygotowane wersje systemu **Linux**, a niektóre — wersję systemu **CatOS** (szczególnie starsze modele).

Generalnie system operacyjny daje użytkownikowi możliwość zarządzania urządzeniem. To za jego pomocą wykonasz wszystkie konfiguracje.

Podstawy IOS

Międzynieciowy System Operacyjny, czyli IOS (ang. *Internetwork Operating System*), to system operacyjny umożliwiający konfigurację urządzeń Cisco. Obsługiwany jest przez użytkownika za pomocą interfejsu **CLI** (ang. *Command Line Interface*).

Pamiętaj, że podczas pierwszej konfiguracji urządzenia Cisco możesz podłączyć się do niego jedynie przez dostępny z tyłu port oznaczony jako **CONSOLE**. W większości przypadków jest to wejście żeńskie RJ45. Połączenie realizowane jest przez specjalnie przygotowany do tego kabel konsolowy, z jednej strony zakończony wtykiem RJ45 (męskim), natomiast z drugiej wtykiem DB-9 popularnie zwanym COM.

Przed podłączeniem należy odpowiednio skonfigurować emulator terminalu, taki jak np. HyperTerminal lub Putty, wpisując poniższe parametry:

- ♦ bity na sekundę — 9600;
- ♦ bity danych — 8;
- ♦ parzystość — brak;
- ♦ bity stopu — 1;
- ♦ sterowanie przepływem — brak.

W systemie IOS występują trzy tryby pracy. Pierwszy tryb to **tryb użytkownika** (ang. *User Exec Mode*). Przeznaczony jest wyłącznie do przeglądania parametrów lub bieżącej konfiguracji. Nie jest możliwe, aby w tym trybie w jakikolwiek sposób wpływać na konfigurację urządzenia. Tryb użytkownika posiada znak zachęty w postaci matematycznego znaku większości (>). Znak jest poprzedzony nazwą, np.: switch>.

Drugim trybem pracy jest **tryb uprzywilejowany** (ang. *Privileged Exec Mode*). W trybie uprzywilejowanym możliwa jest konfiguracja urządzenia oraz wszystkich jego parametrów. Dostęp do niego można zabezpieczyć hasłem. Znakiem zachęty dla trybu uprzywilejowanego jest tzw. hash (#), który również jest poprzedzony nazwą urządzenia, np. switch#. Aby przejść z trybu użytkownika do trybu uprzywilejowanego, po podłączeniu do urządzenia wpisz polecenie enable i naciśnij przycisk Enter, np.:

```
switch>enable  
switch#
```

Jeśli chcesz ponownie przejść do trybu użytkownika, możesz to wykonać, wpisując polecenie disable.

Trzecim trybem jest **tryb konfiguracji globalnej** (ang. *global configuration mode*), służący do konfiguracji interfejsów, ich szybkości itd. W tym trybie możesz wprowadzić zmiany wyświetlanej nazwy oraz wielu innych parametrów, o których będzie mowa w dalszej części.

Do trybu konfiguracyjnego można wejść tylko z trybu uprzywilejowanego; służy do tego polecenie configure terminal, np.:

```
switch>enable  
switch#configure terminal  
switch(config)#
```

System IOS wyposażony jest w bardzo rozbudowany system pomocy. Możesz skorzystać z niego, wpisując znak ?. Jeśli wpiszesz znak ? w trybie uprzywilejowanym, otrzymasz całą dostępną w tym trybie listę poleceń.

Polecenia show

Polecenia rozpoczynające się od słowa show służą do przeglądania różnych elementów konfiguracji. Często przydają się do rozwiązywania problemów z konfiguracją. Ponadto pomagają w przeglądaniu bieżących parametrów pracy urządzeń.

show clock

Polecenie `show clock` dostarcza informacje na temat daty oraz czasu dostępnego na urządzeniu. Ustawienie poprawnej daty oraz godziny jest bardzo istotną sprawą w wielu przypadkach, np. podczas analizy logów systemowych.

```
Switch#show clock
03:37:09.231 UTC Tue May 05 2011
Switch#
```

show interfaces

Stan wszystkich dostępnych na urządzeniu interfejsów można sprawdzić przy użyciu polecenia `show interfaces`. Po jego wydaniu pojawi się informacja na ich temat, zawierająca również szereg ważnych informacji, które zostaną wyjaśnione w dalszych częściach książki.

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 3cdf.1e75.7c81 (bia 3cdf.1e75.7c81)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    236 packets input, 27440 bytes, 0 no buffer
    Received 236 broadcasts (77 multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 77 multicast, 0 pause input
    0 input packets with dribble condition detected
    215 packets output, 16620 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 PAUSE output
    0 output buffer failures, 0 output buffers swapped out
Switch#
```

show running-config oraz show startup-config

Polecenia `show running-config` oraz `show startup-config` są bardzo istotne. Dzięki nim masz możliwość sprawdzenia całej konfiguracji urządzeń. Polecenie `running-config` umożliwia przeglądanie konfiguracji bieżącej, natomiast `startup-config` pokazuje konfigurację startową.

```
Switch#show running-config
Building configuration...

Current configuration : 1264 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
<POMINIĘTO>
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
line vty 5 15
!
end

Switch#
```

show version

Polecenie `show version` wyświetla m.in. informacje na temat wersji systemu IOS, pliku źródłowego z IOS oraz ilości interfejsów urządzenia. Na końcu listingu znajdują się numery seryjne poszczególnych części, modułów oraz innych kart rozszerzeń, jeśli dane urządzenie je posiada.

Wstępna konfiguracja urządzenia

Aby przypisać nową nazwę dla urządzenia oraz nadać interfejsowi odpowiedni adres IP, najpierw przejdź z trybu nieuprzywilejowanego do trybu uprzywilejowanego. Służy do tego polecenie `enable`. Następnie za pomocą polecenia `configure terminal` przejdź do trybu konfiguracji globalnej. Kolejnym wydanym poleceniem powinno być `hostname`, które umożliwi Ci zmianę nazwy urządzenia.

W trybie konfiguracji globalnej wydaj polecenie `interface fastethernet0/0`, aby przejść do konfiguracji interfejsu. W tym trybie wydaj polecenie `ip address [adres_IP]`, aby przypisać odpowiedni adres IP. Na koniec wpisz `no shutdown`, aby uruchomić interfejs. Spójrz na poniższy listing przedstawiający całą konfigurację:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname TEST_1
TEST_1(config)#interface fastethernet0/0
TEST_1(config-if)#ip address 192.168.1.1 255.255.255.0
TEST_1(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
TEST_1(config-if)#
```

Zapisywanie konfiguracji

Istotnym elementem jest zapisywanie konfiguracji. Pamiętaj, że wszystkie wprowadzane zmiany są zapisywane w konfiguracji bieżącej, czyli pamięci RAM. W przypadku nagłego wyłączenia urządzenia są więc bezpowrotnie tracone. Ważne jest, aby zawsze, kiedy konfiguracja bieżąca jest prawidłowa, zapisać ją w **pamięci nieulotnej**, czyli **NVRAM** (ang. *non voltage RAM*). W ten sposób uchronisz się przed jej utratą. Konfiguracja zapisana w pamięci nieulotnej nazywana jest **konfiguracją startową** (ang. *startup-config*).

Ważne jest również, aby niektóre pliki konfiguracyjne znalazły się na zewnętrznym nośniku, np. na dysku serwera. Możesz do tego celu użyć serwera TFTP.

Komendą, która spowoduje zapisanie konfiguracji bieżącej jako startowej, jest polecenie `copy running-config startup-config`. Aby zapisać konfigurację startową na serwer TFTP, użyj polecenia `copy startup-config tftp`. Oczywiście, wcześniej musisz zapewnić komunikację z serwerem.

Zabezpieczanie dostępu do urządzenia

Pamiętaj, że bardzo ważną rzeczą jest odpowiednie zabezpieczenie urządzenia przed dostępem osób niepowołanych. Oznacza to nie tylko zamknięcie urządzeń w specjalnych szafach LAN, ale przede wszystkim zapewnienie ochrony przed zalogowaniem się na nie.

Pamiętaj, że jeśli urządzenie pracuje w sieci i posiada adres IP, każdy użytkownik będzie mógł się na nie zalogować (oczywiście, jeśli nie zostało odpowiednio zabezpieczone). Zanim urządzenie zostanie podłączone do sieci, należy je zabezpieczyć przynajmniej w podstawowym zakresie.

Na początek zabezpiecz dostęp do trybu uprzywilejowanego. Możesz to wykonać przy użyciu polecenia `enable secret` wydanego w trybie konfiguracji globalnej. Następnie zabezpiecz hasłem dostęp do linii wirtualnych oraz portu konsoli. W tym celu należy przejść do trybu konfiguracji linii i wydać polecenie `password`, a następnie `login`, np. tak:

```
R1(config)#line vty 0 4
R1(config-line)#password adam_vty
R1(config-line)#login
```

Dość istotnym poleceniem jest również `service password-encryption`, które szyfruje wszystkie hasła widoczne jako jawny tekst w pliku konfiguracji urządzenia.

Inną praktyką raczej prewencyjną niż zabezpieczającą jest ustawienie komunikatów informujących potencjalnych włamywaczy.

Aby ustawić odpowiedni baner, należy w trybie konfiguracji globalnej posłużyć się poleceniem `banner`. Po wybraniu polecenia `banner` oraz rodzaju banera trzeba wstawić dowolny znak, np. `#`, który oznacza początek komunikatu. Znak `#` wstaw również na końcu wpisanego komunikatu. Najbardziej popularny jest baner MOTD.

Laboratorium 1.

Uruchom program GNS3 i przeciągnij na obszar roboczy jeden z routerów, do którego posiadasz obraz IOS. Przejdź do trybu uprzywilejowanego i wykorzystując listę poniższych poleceń, uzupełnij tabelę (rysunek 5.1).

- ♦ `show running-config;`
- ♦ `show clock;`
- ♦ `show interfaces;`
- ♦ `show ip interface brief;`
- ♦ `show version;`
- ♦ `show history;`
- ♦ `show flash.`

Rysunek 5.1.
Tabela poleceń

POLECENIE	ODPOWIEDŹ
Podaj wielkość pliku konfiguracyjnego	
Nazwa routera	
Liczba dostępnych linii wirtualnych	
Aktualna godzina i data na routerze	
Wersja systemu IOS	
Liczba interfejsów i ich rodzaj	
Nazwa wersji IOS	
Liczba dostępnej pamięci flash	
Adres MAC dowolnego interfejsu FastEthernet	
Tryb pracy i szybkość interfejsu FastEthernet	

Laboratorium 2.

W programie Cisco Packet Tracer przeciągnij na obszar roboczy trzy routery. Następnie przy użyciu linii poleceń przydziel im odpowiednie adresy IP zgodnie z poniższym rysunkiem (rysunek 5.2). Nadaj również odpowiednie nazwy routerom.

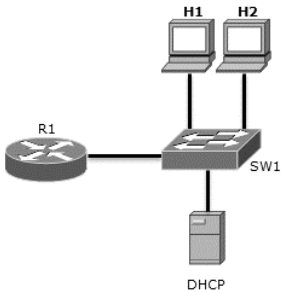
Rysunek 5.2.
*Założenia
do 2. laboratorium*

NAZWA ROUTERA	INTERFEJS	ADRES IP	MASKA
R1	FA0/0	192.168.1.1	255.255.255.0
	FA0/1	192.168.2.1	255.255.255.0
R2	FA0/0	192.168.1.2	255.255.255.0
	FA0/1	192.168.3.1	255.255.255.0
R3	FA0/1	192.168.2.2	255.255.255.0
	FA0/0	192.168.3.2	255.255.255.0

Laboratorium 3.

- 1. Utwórz w programie Cisco Packet Tracer model sieci podany na poniższym rysunku (rysunek 5.3).

Rysunek 5.3.
*Schemat sieci
do wykonania
w programie
Cisco Packet Tracer*



- 2. Nazwij wszystkie urządzenia, tak jak pokazano na rysunku.
- 3. Ustaw komunikat informacyjny na routerze oraz przełączniku.

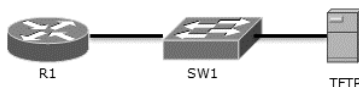
4. Zabezpiecz dostęp do wszystkich linii wirtualnych na urządzeniach aktywnych.
5. Dokonaj konfiguracji interfejsu *FastEthernet0/0* routera R1. Przypisz mu dowolny adres IP.
6. Skonfiguruj serwer DHCP tak, aby stacje robocze mogły komunikować się ze sobą. Ustaw takie parametry serwera, aby otrzymywały one adres domyślnej bramy (interfejsu routera).

Laboratorium 4.

1. Wykonaj poniższy schemat w PT (rysunek 5.4).

Rysunek 5.4.

Schemat sieci
z serwerem TFTP



2. Ustal dowolną adresację i przydziel adresy IP do urządzeń.
3. Skopiuj konfigurację bieżącą routera R1 na serwer TFTP.
4. Skopiuj konfigurację startową routera R1 na serwer TFTP.
5. Skopiuj zapisaną konfigurację bieżącą z serwera TFTP do konfiguracji startowej routera R1.

Laboratorium 5.

1. W programie GNS3 połącz wirtualny router z Twoim komputerem tak, aby można było wykonać test ping z routera do sieci internet.
2. Na interfejsie routera uruchom klienta DHCP. Router ma otrzymać adres 192.168.137.X.
3. Utwórz na pulpicie komputera lokalnego folder o nazwie *TFTP* i skopiuj do niego konfigurację bieżącą routera R1.

Wskazówki do laboratoriów

Laboratorium 1.

Wynik, który otrzymałeś, może nieco różnić się od poniższego, w zależności od tego, na jakim routerze zostały wydane podane polecenia.

Aby otrzymać wielkość pliku konfiguracyjnego, nazwę routera oraz liczbę wirtualnych linii, wydaj polecenie `show running-config`. Spójrz na poniższy listing:

```
R1#show running-config
Building configuration...
```



```
Current configuration : 625 bytes

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
ip cef
!
no ip domain lookup
<POMINIĘTO>
line con 0
  exec-timeout 0 0
  logging synchronous
line aux 0
line vty 0 4
end
R1#
```

Pozycja `Current configuration` pokazuje aktualną wielkość pliku konfiguracyjnego. Pozycja `hostname` to nazwa routera, a pozycja `line vty` wskazuje ilość linii wirtualnych od 0 do 4.

Aby wyświetlić aktualną datę i godzinę, wydaj na routerze polecenie `show clock`. Oto przykład:

```
R1#show clock
*00:02:47.051 UTC Fri Mar 1 2002
R1#
```

Jeśli chcesz uzyskać informację na temat zainstalowanego systemu IOS, wydaj polecenie `show version`. W pierwszej linii znajdziesz potrzebne informacje, np.:

```
R1#show version
Cisco IOS Software, 3700 Software (C3745-ADVENTERPRISEK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Fri 17-Nov-06 15:09 by prod_rel_team

<POMINIĘTO>
```

Kolejną informacją jest ilość dostępnej pamięci FLASH. Te informacje możesz uzyskać, wydając polecenie `show flash`. Spójrz na poniższy listing.

```
R1#show flash
System CompactFlash directory:
No files in System CompactFlash
```

```
[0 bytes used, 16777212 available, 16777212 total]
16384K bytes of ATA System CompactFlash (Read/Write)
R1#
```

Ostatnimi informacjami, jakie należy wyświetlić w tym laboratorium, są dane na temat adresu MAC oraz trybu pracy dowolnego interfejsu. Taką informację możesz uzyskać, wydając polecenie `show interface FastEthernet0/0`. Oto przykład:

```
R1#show interface fastethernet0/0
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is Gt96k FE, address is c400.10a0.0000 (bia c400.10a0.0000)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
<POMINIĘTO>
```

W drugiej linii listingu znajduje się informacja na temat adresu MAC, natomiast niżej w siódmej jest informacja na temat trybu pracy interfejsu. W tym przypadku interfejs pracuje z szybkością 100 Mb/s w trybie Full-duplex.

Na poniższym rysunku znajduje się podsumowanie wszystkich otrzymanych danych (rysunek 5.5).

Rysunek 5.5.
Wypełniona tabela

POLECENIE	ODPOWIEDŹ
Podaj wielkość pliku konfiguracyjnego	625 bajtów
Nazwa routera	R1
Liczba dostępnych linii wirtualnych	5
Aktualna godzina i data na routerze	00:04:42 Fri Mar 1 2002
Wersja systemu IOS	12.4(12)
Liczba interfejsów i ich rodzaj	2, FastEthernet
Nazwa wersji IOS	C3745-ADVENTERPRISEK9-M
Liczba dostępnej pamięci flash	16777212 bajtów
Adres MAC dowolnego interfejsu FastEthernet	C402.10c0.0000
Tryb pracy i szybkość interfejsu FastEthernet	100Mb/s, Full Duplex

Laboratorium 2.

W tym laboratorium wykorzystaj polecenia `hostname` — do zmiany nazwy routera, `ip address` — do nadania adresu IP interfejsów oraz `no shutdown` — do włączenia interfejsu. Poniżej znajdują się trzy listingi prezentujące konfigurację każdego z trzech routerów.

```
R1:
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
```

```
R1(config-if)#  
R1(config-if)#exit  
R1(config)#int fa0/1  
R1(config-if)#ip address 192.168.2.1 255.255.255.0  
R1(config-if)#no shut  
R1(config-if)#
```

R2:

```
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#hostname R2  
R2(config)#int fa0/0  
R2(config-if)#ip address 192.168.1.2 255.255.255.0  
R2(config-if)#no shut  
R2(config-if)#exit  
R2(config)#int fa0/1  
R2(config-if)#ip address 192.168.3.1 255.255.255.0  
R2(config-if)#no shut  
R2(config-if)#
```

R3:

```
Router#conf t  
Router(config)#hostname R3  
R3(config)#int fa0/1  
R3(config-if)#ip address 192.168.2.2 255.255.255.0  
R3(config-if)#no shut  
R3(config-if)#exit  
R3(config)#int fa0/0  
R3(config-if)#ip address 192.168.3.2 255.255.255.0  
R3(config-if)#no shut  
R3(config-if)#
```



Wskazówka

Zauważ, że w listingach pojawiły się skrócone formy poleceń. Jak mogłeś przeczytać w ósmym rozdziale książki „W drodze do CCNA. Część I”, system IOS umożliwia skracanie wszystkich poleceń. Aby przejść do trybu konfiguracji globalnej, nie trzeba więc wydawać pełnego polecenia `configure terminal`, a wystarczy podać `conf t`.

Laboratorium 3.

Po wykonaniu modelu sieci w programie PT nadaj urządzeniom odpowiednie nazwy. W kolejnym kroku ustaw hasło trybu uprzywilejowanego oraz ustal komunikat powitalny. Na poniższym listingu przedstawiono konfigurację routera, tę samą czynność wykonaj również dla przełącznika.

```
R1#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
R1(config)#enable secret test  
R1(config)#  
R1(config)#banner motd @ KOMUNIKAT TRESC @  
R1(config)#
```

Kolejny punkt to zabezpieczenie dostępu do urządzeń aktywnych poprzez linie wirtualne oraz konsolę. Wydadź polecenie `show running-config`, aby sprawdzić, ile linii wirtualnych posiada Twoje urządzenie.

```
<POMINIĘTO>
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
end
<POMINIĘTO>
```

W powyższym przypadku zakres linii wirtualnych wynosi od 0 do 15. Należy zabezpieczyć wszystkie. Pamiętaj, że pozostał interfejs konsoli. Oto przykład:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#line con 0
R1(config-line)#password test
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password test
R1(config-line)#login
R1(config-line)#
```

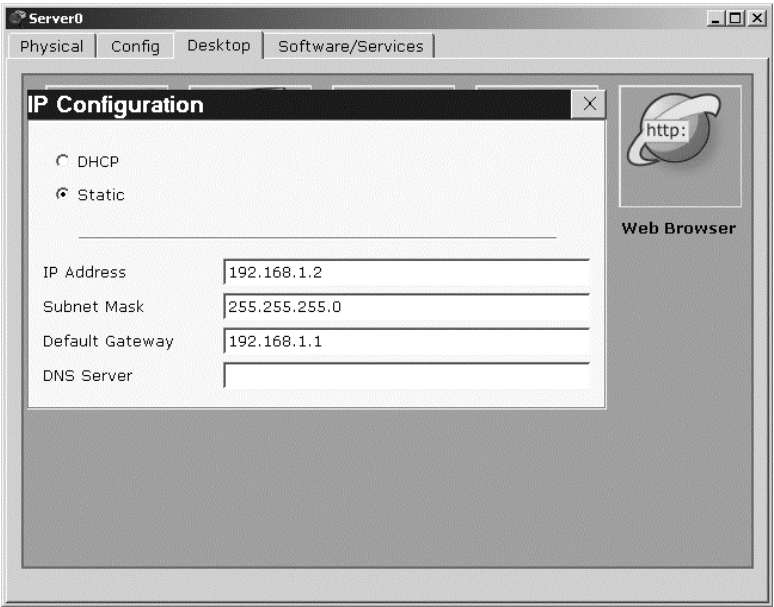
W ostatnim kroku konfiguracji routera R1 należy przydzielić adres IP do interfejsu *FastEthernet0/0*. W tym przypadku możesz przydzielić dowolny adres IP. Poniżej przedstawiono konfigurację interfejsu routera R1:

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
```

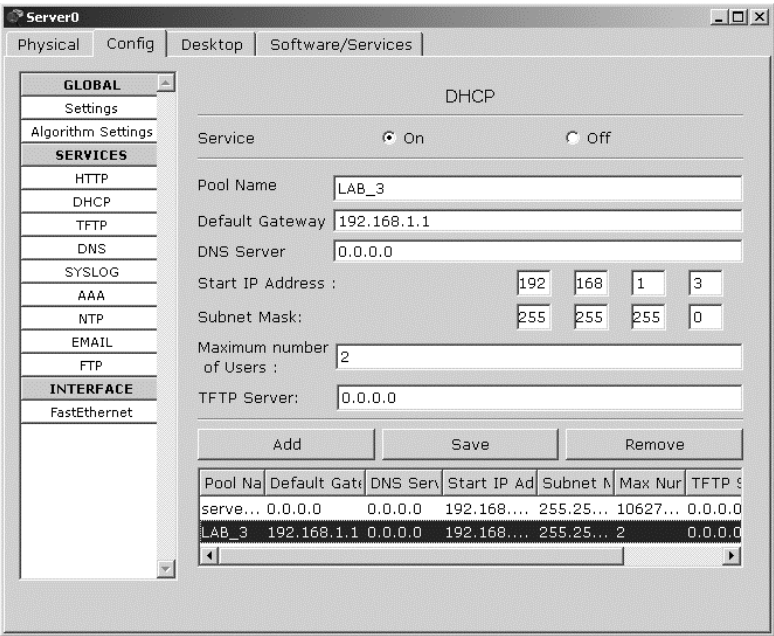
W ostatnim punkcie powyższego laboratorium należy skonfigurować serwer DHCP. W tym celu kliknij go dwukrotnie i przejdź do zakładki *Desktop*. Następnie kliknij pozycję *IP Configuration*. Podaj adres IP, jaki będzie przypisany do serwera (rysunek 5.6). Pamiętaj, że adres musi znajdować się w tej samej podsieci, co adres przypisany do interfejsu routera.

Przejdź na zakładkę *Config* i kliknij przycisk *DHCP*. W polu *PoolName* podaj dowolną nazwę, np. *LAB_3*. Jeśli chcesz, aby adres domyślnej bramy był przesyłany w uaktualnieniach DHCP, podaj jego adres w polu *Default Gateway*. Następnie w polu *Start IP Address* wpisz początkowy adres IP, od którego serwer będzie przypisywać adresy dla hostów. Kliknij przycisk *Add*, aby zapisać konfigurację (rysunek 5.7).

Rysunek 5.6.
Przypisanie adresu IP



Rysunek 5.7.
Konfiguracja serwera DHCP



Po kilku sekundach możesz sprawdzić, czy stacje robocze otrzymały adresy IP.

Laboratorium 4.

W tym laboratorium zadanie polega na skopiowaniu konfiguracji do serwera TFTP i na odwrót z serwera TFTP do routera.

Pamiętaj, że w rzeczywistych warunkach aktualna konfiguracja startowa musi być tworzona na każdym z urządzeń sieciowych. W przypadku ich wyłączenia będzie możliwość wczytania wszystkich danych od nowa. Pliki z konfiguracją i obraz systemu IOS powinny być przechowywane w innym miejscu (serwerze TFTP). Podczas archiwizacji serwera TFTP można dodatkowo kopiować na nośniki elektroniczne konfiguracje routerów. W ten sposób kopie konfiguracji będą dodatkowo zabezpieczone.

Po utworzeniu schematu sieci oraz wybraniu odpowiedniej adresacji przypisz wybrane adresy do urządzeń — routera oraz serwera TFTP. W pierwszej kolejności skopiuj konfigurację bieżącą na serwer. W tym celu użyj polecenia `copy running-config tftp`. Zostaniesz poproszony o podanie adresu serwera oraz nazwy dla pliku z konfiguracją. Zalecam, aby w rzeczywistych warunkach nazwy były tworzone w następujący sposób, np. `router_2800_R1_biezaca_2011_04_11_12_34_AJ`. Nazwa pliku zawiera informacje na temat rodzaju routera, jego nazwy oraz daty i godziny utworzenia konfiguracji, na końcu są inicjały administratora, który wykonał kopię. Spójrz na poniższy listing.

```
R1#copy running-config tftp
Address or name of remote host []? 192.168.1.2
Destination filename [Router-config]? router_r1_biezaca
Writing running-config....!!
[OK - 463 bytes]
463 bytes copied in 3.135 secs (0 bytes/sec)
```

Zauważ, że w przedostatniej linii pojawiła się informacja `[OK - 463 bytes]`; oznacza to, że kopia została utworzona na serwerze. Za chwilę sprawdzisz, czy na pewno się tam znajduje.

Wykonaj teraz kopię konfiguracji startowej na serwer TFTP. Zanim to uczynisz, skopiuj konfigurację bieżącą do konfiguracji startowej. W tym celu wydaj polecenie `copy running-config startup-config`. Spójrz na listing poniżej:

```
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Teraz skopiuj zapisaną konfigurację startową na serwer, wykorzystaj polecenie `copy startup-config tftp`. Oto przykład:

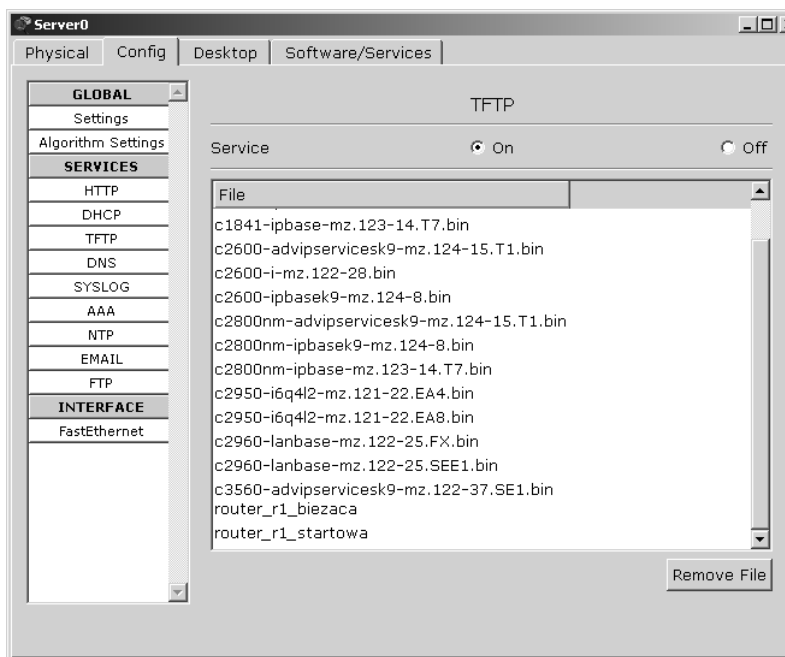
```
R1#copy startup-config tftp
Address or name of remote host []? 192.168.1.2
Destination filename [R1-config]? router_r1_startowa
Writing startup-config....!!
[OK - 463 bytes]
463 bytes copied in 0.125 secs (3000 bytes/sec)
R1#
```

W programie Cisco Packet Tracer można bardzo łatwo sprawdzić, czy wszystkie konfiguracje zostały poprawnie zapisane. W tym celu kliknij dwukrotnie serwer i przejdź do zakładki *Config* (rysunek 5.8).

Następnie w menu po lewej stronie kliknij pozycję *TFTP*. Przejdź paskiem przewijania w dół i sprawdź, czy na liście znajdują się zapisane konfiguracje.

Rysunek 5.8.

Dostęp do zapisanych konfiguracji



Teraz możesz skopiować konfigurację startową z serwera na router. W tym celu na routerze wydaj polecenie `copy tftp startup-config`, np.:

```
R1#
R1#copy tftp startup-config
Address or name of remote host []? 192.168.1.2
Source filename []? router_r1_biezaca
Destination filename [startup-config]?

Accessing tftp://192.168.1.2/router_r1_biezaca...
Loading router_r1_biezaca from 192.168.1.2: !
[OK - 463 bytes]
463 bytes copied in 0.047 secs (9851 bytes/sec)
R1#
```

Pamiętaj, aby wszystkie kopie były tworzone na bieżąco. Zasada jest prosta: jeśli wprowadzisz zmiany w konfiguracji routera, w pierwszej kolejności wykonaj kopię konfiguracji bieżącej, dopiero potem wprowadź zmiany. Po wprowadzeniu zmian w konfiguracji bieżącej nie zapisuj ich od razu do konfiguracji startowej, lecz sprawdź, jak zareagowała sieć. Przeanalizuj, czy wszystko działa poprawnie, tak jak założyłeś. Jeśli wszystko jest tak, jak zaplanowałeś, skopiuj dotychczasową konfigurację startową na serwer, dopiero potem skopiuj konfigurację bieżącą do startowej. Dokonaj archiwizacji wszystkich konfiguracji. Dzięki wprowadzeniu w nazwie konfiguracji daty i godziny będziesz mógł bardzo szybko odnaleźć i przywrócić poprzednią konfigurację, jeśli okaże się, że sieć działa nieprawidłowo.

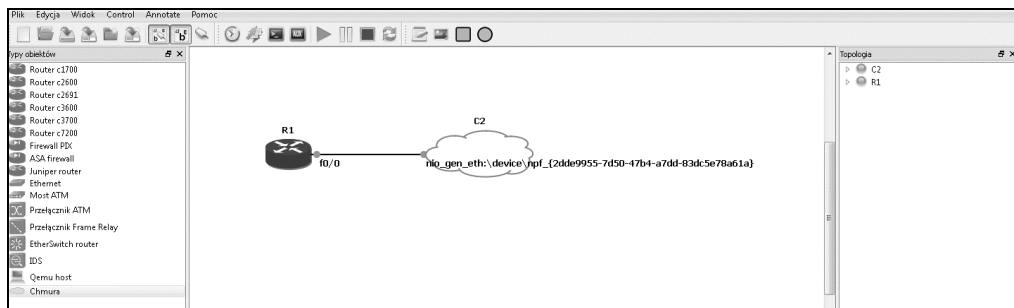
Wszystkie zarchiwizowane konfiguracje pozostaw na serwerze tak długo, jak to możliwe. Pliki te nie zajmują wiele przestrzeni dyskowej, a czasami zdarzają się sytuacje, które wymagają cofnięcia się.

Zaleca się, aby regularnie sprawdzać, czy kopia bezpieczeństwa może zostać użyta. Nie zalecam przywracania kopii na urządzeniach pracujących w sieci produkcyjnej. Najlepiej zrobić to na urządzeniach znajdujących się w środowisku przedprodukcyjnym lub sprzęcie wolno stojącym. Jeśli sprawa dotyczy routerów, można w programie GNS3 wykonać wirtualną kopię całej sieci przedsiębiorstwa i tam testować wszystkie kopie. Oczywiście, jeśli sieć nie jest bardzo dużych rozmiarów.

Laboratorium 5.

To laboratorium wymaga kilku dodatkowych czynności, takich jak utworzenie wirtualnego interfejsu, konfiguracji DHCP oraz instalacji i konfiguracji prostego serwera TFTP. Zaczniemy od przygotowania środowiska GNS3 i połączenia go z rzeczywistą siecią.

W programie GNS3 przeciągnij na obszar roboczy dowolny router z interfejsem *Fast-Ethernet* oraz chmurę symbolizującą sieć (rysunek 5.9).



Rysunek 5.9. Połączenie routera do sieci lokalnej

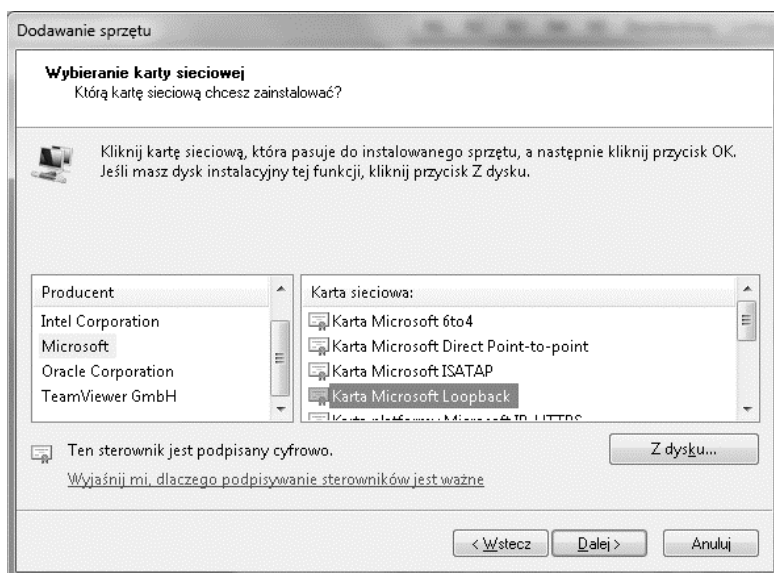
Założeniem jest, aby router mógł komunikować się z internetem, ponadto ma otrzymać dowolny adres IP z podsieci 192.168.137.X/24. Więc w pierwszym kroku utworzymy w systemie operacyjnym interfejs wirtualny *LOOPBACK*. Przedstawiona konfiguracja została opisana na podstawie systemu Windows 7.

W rzeczywistości interfejs *LOOPBACK* nie istnieje. Można jednak wykorzystać go do połączenia środowiska wirtualnego GNS3 i rzeczywistej sieci.

Kliknij *Start* i polu wyszukiwania wpisz *hdwwiz*, naciśnij *Enter*. Pojawi się kreator dodawania sprzętu. Kliknij *Dalej*.

W kolejnym kroku zaznacz pole wyboru *Zainstaluj sprzęt, który wybiorę ręcznie z listy (zaawansowane)* i kliknij przycisk *Dalej*. Z listy wybierz pozycję *Karty sieciowe*, kliknij *Dalej* i poczekaj na wypełnienie listy. Następnie z okna *Producent* wybierz *Microsoft*, a w oknie *Karta sieciowa*: kliknij pozycję *Karta Microsoft Loopback* (rysunek 5.10). Kliknij *Dalej*. Nowa wirtualna karta sieciowa *LOOPBACK* zostanie zainstalowana.

Rysunek 5.10.
Instalowanie karty
LOOPBACK



Zanim podłączysz emulowany router do środowiska rzeczywistej sieci, musisz w systemie Windows udostępnić swoje połączenie z internetem, w ten sposób uruchomisz również prosty serwer DHCP i będziesz mógł wpisać dowolną podsieć, z zakresu której router otrzyma adres IP. W tym celu przejdź do *Centrum sieci i udostępniania* w systemie Windows.

W menu po lewej stronie wybierz pozycję *Zmień ustawienia karty sieciowej*. Kliknij prawym przyciskiem myszy połączenie, które realizuje komunikację z siecią internet i wybierz *Właściwości*.

Kliknij zakładkę *Udostępnianie* i zaznacz pole wyboru *Zezwalaj innym użytkownikom sieci na łączenie się poprzez połączenie internetowe tego komputera*, następnie z listy wybierz połączenie *LOOPBACK* (w Twoim systemie to połączenie może posiadać inną nazwę — sprawdź to, zanim wybierzesz). Kliknij *OK* (rysunek 5.11).

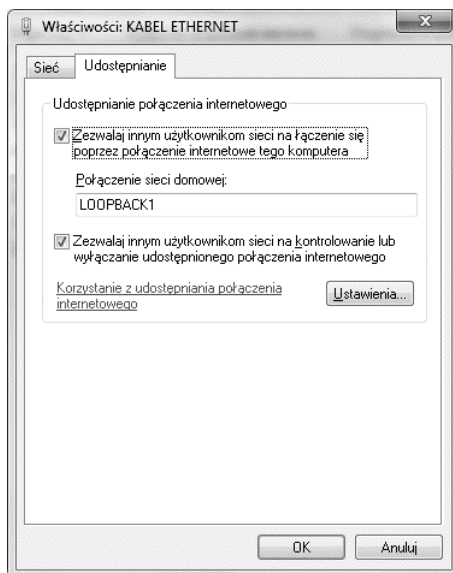
Teraz kliknij prawym przyciskiem myszy kartę *LOOPBACK* i wybierz *Właściwości*. Z listy na karcie *Sieć* wybierz pozycję *Protokół internetowy w wersji 4 (TCP/IPv4)* i kliknij *Właściwości*. W polu *Adres IP* możesz podać dowolny zakres, jaki ma być przydzielany (rysunek 5.12).

Przejdź do programu GNS3, kliknij prawym przyciskiem myszy ikonę chmury i wybierz *Konfiguruj*.

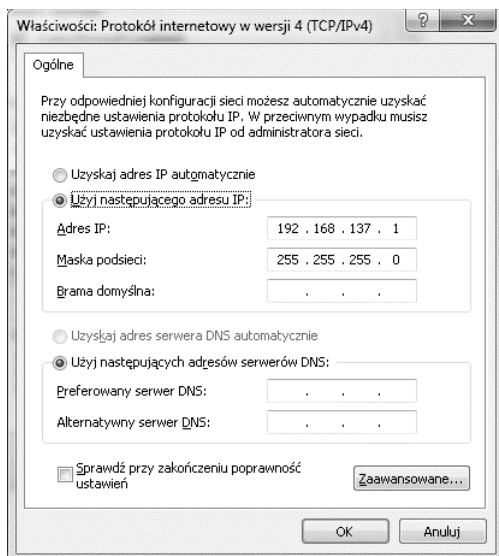
W oknie *Konfigurator urządzenia* przejdź na zakładkę *NIO Ethernet*. Z listy rozwijalnej wybierz kartę *LOOPBACK*, następnie kliknij przycisk *Dodaj*. Kliknij *Zastosuj* i *OK*, aby zapisać ustawienia. Zamknij okno i połącz router z chmurą, następnie przejdź do konfiguracji routera R1.

Skonfiguruj interfejs, do którego podłączona została chmura, najprawdopodobniej jest to *FastEthernet0/0*. Na początek ustaw interfejs w trybie klienta DHCP, np. tak:

Rysunek 5.11.
*Udostępnianie
 połączenia
 internetowego*



Rysunek 5.12.
*Konfiguracja
 adresacji IP*



```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int fa0/0
R1(config-if)#ip address dhcp
R1(config-if)#no shut
R1(config-if)#
```

Po kilku sekundach sprawdź, jaki adres otrzymał interfejs *FastEthernet* z serwera DHCP. W tym celu wyjdź z trybu konfiguracji interfejsu i w trybie konfiguracji globalnej wydaj komendę `show interface fastEthernet 0/0`; teraz spójrz na pozycję `Internet address is`:

```

R1#show interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c400.10e4.0000 (bia c400.10e4.0000)
    Internet address is 192.168.137.235/24
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)

```

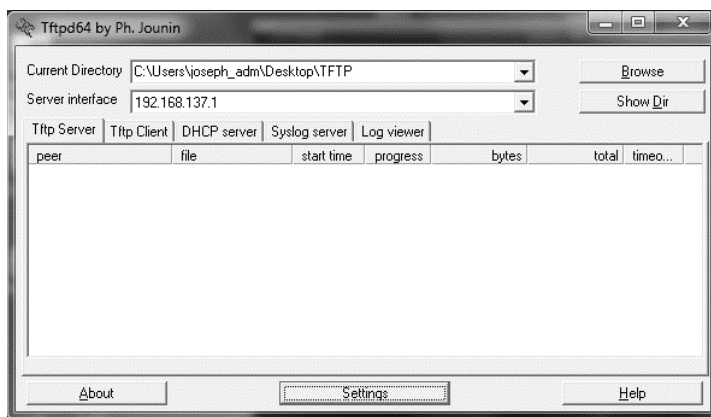
W celu przetestowania komunikacji wydaj ping na adres 192.168.137.1. Jeśli stacja robocza odpowiada, możesz przejść do dalszej konfiguracji. Jeśli nie odpowiada, spróbuj najpierw wyłączyć systemowy firewall. W większości przypadków problem zostanie rozwiązany. Powinieneś mieć również możliwość wykonania testu ping na dowolny zewnętrzny adres IP np. 212.77.100.101 (*wp.pl*).

W ostatnim kroku skonfigurujesz serwer TFTP.

Utwórz na pulpicie folder *TFTP*, następnie pobierz z internetu darmowy program *tftpd64* (jeśli posiadasz system 32-bitowy, pobierz *tftpd32*). Zainstaluj program i uruchom go.

W oknie głównym kliknij przycisk *Browse* i odszukaj folder *TFTP*, następnie wybierz z listy rozwijalnej adres IP interfejsu, do którego podłączony jest router (rysunek 5.13).

Rysunek 5.13.
Konfiguracja
serwera TFTP



W zasadzie konfiguracja serwera TFTP jest zakończona. Przejdź do konsoli routera i wydaj polecenie `copy running-config tftp` i podaj adres serwera TFTP, tak jak podano na poniższym listingu:

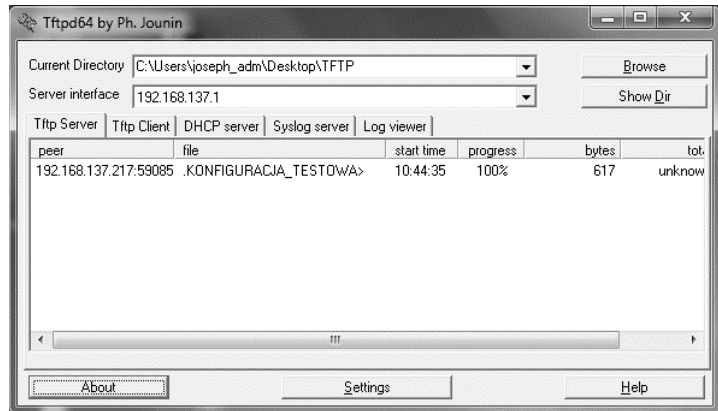
```

R1#copy running-config tftp
Address or name of remote host []? 192.168.137.1
Destination filename [r1-config]? KONFIGURACJA_TESTOWA
!!
617 bytes copied in 1.096 secs (563 bytes/sec)
R1#

```

Po kilku sekundach konfiguracja zostanie zapisana w utworzonym folderze (rysunek 5.14).

Rysunek 5.14.
*Zapisana
konfiguracja
na serwerze TFTP*



Test sprawdzający

1. Jaki port służy do konfiguracji routera, jeśli ten nie posiada przypisanego adresu IP?
 - a) vty 0;
 - b) console;
 - c) vty 0 4;
 - d) telnet.
2. Jakie polecenie pozwala na opuszczenie trybu uprzywilejowanego?
 - a) enable;
 - b) conf t;
 - c) disable;
 - d) exit.
3. Dlaczego podczas konfiguracji interfejsu *FA0/1* pojawił się komunikat:
% 192.168.1.0 overlaps with FastEthernet0/0?
 - a) interfejs *FA0/0* jest wyłączony;
 - b) interfejs *FA0/0* nie istnieje na tym routerze;
 - c) adres IP jest w tej samej podsieci, co adres na interfejsie *FA0/0*;
 - d) podany adres IP jest błędny.
4. Które polecenie szyfruje hasła w pliku konfiguracji?
 - a) service password-encryption;
 - b) encrypt;

- c) no service password-encryption;
 - d) nie można szyfrować haseł w pliku konfiguracji.
5. Administrator wydał na routerze polecenie `show int S0/0`, aby poznać adres MAC interfejsu. Dlaczego adres MAC nie został wyświetlony?
- a) należy dodać ten adres ręcznie;
 - b) interfejs jest wyłączony i należy go włączyć;
 - c) w interfejsach szeregowych nie ma adresów MAC;
 - d) podany interfejs jest uszkodzony.
6. Jak nazywa się pamięć nieulotna na routerze, w której trzymana jest konfiguracja startowa?
- a) FLASH;
 - b) NVRAM;
 - c) RAM;
 - d) ROM.
7. Jakie polecenie uruchamia interfejs?
- a) shutdown;
 - b) no shut;
 - c) shut;
 - d) no shutdown.
8. Jakie polecenie służy do kopiowania konfiguracji startowej do serwera TFTP?
- a) copy running-config tftp;
 - b) copy tftp startup-config;
 - c) copy tftp running-config;
 - d) copy startup-config tftp.
9. Jakie polecenie umożliwia wyświetlenie na routerze przyznanych mu adresów IP?
- a) show ip dhcp;
 - b) show dhcp lease;
 - c) show dhcp ip;
 - d) żadne z powyższych.
10. Jakie polecenie służy do wyświetlania wersji systemu IOS?
- a) show running-config;
 - b) show startup-config;
 - c) show version;
 - d) żadne z powyższych.

Odpowiedzi

1. B;
2. C, D;
3. C;
4. A;
5. C;
6. B;
7. B, D;
8. D;
9. B;
10. A, B, C.

Skorowidz

100 Base-TX, 128
2WAY, 227

A

active, 265
Adapters, 289
Add link, 289
adres
 docelowy, 351
 domyślnej bramy, 108
 grupowy 224.0.0.5, 225–226
 identyfikujący przełącznik, 258
 IP, 118
 IP interfejsu, 118
 IP urządzenia, 87
 MAC, 118, 261
 multicast protokołu RIPv2, 191
 podinterfejsu, 289
 publiczny (public address), 56
 rozgłoszeniowy, 165
 źródłowy, 351
adresacja w sieciach, 61
algorytm DUAL, 200
analiza routingu, 168
Aterm, 175
automatyczne pobieranie adresów IP, 360
automatyczne podsumowywanie sieci
 klasowych, 158
autosumaryzacja tras, 215, 182

B

baner MOTD, 88
bezklasowy routing, 181
bezpieczna transmisja SSH, 260

blokowanie
 dostępu do sieci, 353
 dostępu do strony, 352
 ICMP, 352
 obsługi ping, 352
 portów, 354
 protokołu TCP, 355
 dostępu do NAT, 366
Bridge ID, 305
burza rozgłoszeniowa, 297

C

CCNA, 17
CHAP, 323 *Patrz także* uwierzytelnianie
chmura, 15
CIDR, 181
Cisco Network Academy, 18
Cisco Packet Tracer, 17
Command Prompt, 24, 261
CONSOLE, 28, 83
Current configuration, 93
czas Dead, 241
czas Hello, 241
czas starzenia się (age time), 253
czasy protokołu OSPF, 241

D

DCE, Data Circuit-Termination Equipment, 323
DHCP, Dynamic Host Configuration Protocol,
 24, 39
dialog konfiguracyjny, 127
diody LED, 41
długość maski, 181

DNS, Domain Name System, 39, 245
Dodaj połączenie, 34
domena VTP, 279
dopuszczalna odległość, 200
dopuszczalny sukcesor, 200
DROther, 226
DTE, Data Terminal Equipment, 323
DUAL, Diffusing update Algorithm, 200
Dynamips, 32

E

emulator GNS3, 31
enable password, 127
enable secret, 127
End devices, 19
enkapsulacja, 326
enkapsulacja Cisco ISL, 291
enkapsulacja HDLC (High-level Data Link Control), 323
Ethernet, 53
Event list, 22

F

FastEthernet, 19
feasible distance, 211
filtrowanie pakietów, 351
FLASH, 94
folder TFTP, 103
format binarny adresu, 211
Frame Relay (FR), 321, 333
 Committed Information Rate (CIR), 333
 Data Link Connection Identifier (DLCI), 333
 Excess Information Rate (EIR), 333
 Local Access Rate (LAR), 333
 Local Management Interface (LMI), 333
 Permanent Virtual Circuit (PVC), 334
FTP, File Transfer Protocol, 39
full-duplex, 128
funkcja Add Simple PDU, 45, 47
funkcja Manual., 289
funkcja PortFast, 299
funkcja skrótu (hash), 182
FWD, 305

G

Generic, 19, 27
GNS3, 174

H

hasło dostępu, 258
hasło linii wirtualnej, 118
hasło trybu uprzywilejowanego, 118
HDLC, High-level Data Link Control, 323
hello, 199
hostname, 93
HTTP, Hyper Text Transfer Protocol, 39
hub, 14
HyperTerminal, 29, 83

I

identyfikator
 DLCI, 336
 RID, 246
 routera, 226, 231
 SSID, 108
ikony Cisco, 14
informacja o sieci, 158
instalowanie karty LOOPBACK, 101
instrukcje blokujące (deny), 351
instrukcje zezwalające (permit), 351
interfejs
 CLI (Command Line Interface), 83
 COM, 29
 FastEthernet, 19, 48, 52, 118, 215
 GigabitEthernet, 19
 LOOPBACK, 100, 188
 Null0, 215
 Port 1, 108
 PORT0, 113
 Serial0/0, 215
 szeregowy (serial), 118
 trunk, 293
 VLAN99, 282
 wirtualny, 100, 188
 wyjściowy, 171
internet, 13
IOS, Internetwork Operating System, 31, 83, 118
IP Address, 24
IP Configuration, 24, 108, 282
ISO/OSI, 22

K

kabel bez przeplotu, 19
kabel koncentryczny, 41
kabel światłowodowy, 41
karta rozszerzeń, 286
karta rozszerzeń NM-16ESW, 289
karta sieciowa, 13

- key, 182
- key chain, 182
- key-string, 182
- klasa A, 54, 64
- klasa B, 54, 63
- klasa C, 54, 62
- klasy adresów IP, 54
- klucz WPA2-PSK, 108
- komenda
 - broadcast, 343
 - default-information originate, 171
 - ifconfig eth0, 369
 - interface Loopback, 188
 - ip address dhcp, 50
 - login local, 260
 - no shutdown, 50
 - root primary, 301
 - service password-encryption, 245
 - show interface fa0/0, 50
 - unpack.exe, 32
 - vtp mode client, 279
- kompresowanie danych, 323
- komunikacja bezprzewodowa (wireless), 42
- koncentrator, 14
- konfiguracja
 - routingu statycznego, 111
 - serwera DHCP, 45
 - serwera TFTP, 103
 - adresacji IP, 102, 282
 - adresu IP hosta, 176
 - bazy danych VLAN, 341
 - bieżąca routera (running-config), 117
 - chmury, 318
 - EIGRP, 200
 - emulatora, 32
 - enkapsulacji, 290
 - klienta, 34
 - linii konsolowej, 260
 - linii wirtualnych, 260
 - listy dostępu, 355
 - parametrów wirtualnego terminalu, 30
 - protokołu OSPF, 232, 242
 - protokołu RIPv2, 182
 - protokołu routingu RIP, 169, 173
 - protokołu TCP/P, 44
 - protokołu VTP, 283, 315
 - przełącznika Frame Relay, 337
 - przełącznika poprzez dialog
 - konfiguracyjny, 254
 - routera, 29, 153
 - routera na patyku, 285
 - routingu, 243
 - routingu EIGRP, 346
 - routingu statycznego, 110

- sieci bezprzewodowej, 109
- sieci WAN, 323
- stacji QEMU, 174
- startowa (startup-config), 87, 117
- trasy domyślnej, 171
- urządzenia, 87
- urządzenia SW1, 315
- ustawień TCP/IP, 26
- konfiguracja uwierzytelnienia, 182, 191
 - ip rip authentication key-chain, 182
 - ip rip authentication mode md5, 182
 - key, 182
 - key chain, 182
 - key-string, 182
 - zegara synchronizacji, 118
- Konsola, 34
- kopia bezpieczeństwa, 100
- koszt dotarcia do mostu głównego, 297
- koszt przesłania pakietu, 237
- koszt trasy, 210

L

- LAN, Local Area Network, 35
- Layer 2 switch, 14
- Layer 3 switch, 14
- liczba binarna, 58
- licznik
 - oczyszczania (flush timer), 157, 168
 - uznania trasy za nieistniejącą (invalid timer), 157
 - wstrzymania (hold down timer), 157
- line vty, 93
- linie VTY, 258
- listy dostępu ACL, 321
- listy kontroli dostępu, 351
- listy rozszerzone, 351
- LOOPBACK, 100

Ł

- łączenie przełączników, 269
- łączenie trunk, 254

M

- mapa sieci, 146
- mapowanie statyczne, 343
- maska odwrotna (wildcard mask), 200
- maska podsieci, 56
- maska podsieci w formie odwróconej, 225
- MD5, 182 *Patrz także* uwierzytelnianie
- media optyczne (optical media), 41

medium transmisyjne, 13
 metryka: dopuszczalna odległość, 200
 metoda point-to-multipoint, 336
 metoda punkt-punkt, 338
 miedź (copper), 40
 Międzysieciowy System Operacyjny
Patrz IOS, 83
 minimalizowanie ruchu rozgłoszeniowego, 285
 minimalizowanie tablicy routingu, 214
 model ISO/OSI, 22, 36
 aplikacji (warstwa siódma), 36
 prezentacji (warstwa szósta), 36
 sesji (warstwa piąta), 36
 transportu (warstwa czwarta), 36
 sieci (warstwa trzecia), 36
 łącza danych (warstwa druga), 36
 fizyczna (warstwa pierwsza), 36
 model TCP/IP, 39
 warstwa aplikacji, 39
 warstwa transportu, 39
 warstwa internetowa, 39
 warstwa dostępu do sieci, 39
 modem, 15
 moduł NM-1FE-TX, 131
 moduł NM-4T, 131
 most główny (root bridge), 297, 309
 MPLS, 333

N

nadmiarowość, 15
 NAT, Network Address Translation, 56, 321, 359
 translacja dynamiczna, 359
 translacja statyczna, 359
 translacja z przeciążaniem, 359
 nazwa domeny VTP, 278
 nazwa routera, 118
 Neighbor ID, 246
 niezawodność, 201
 NIO Ethernet, 101
 NM-16ESW, 289
 numer korekty konfiguracji, 275
 numer systemu autonomicznego, 200
 NVRAM, non voltage RAM, 87

O

obciążenie, 201
 obliczanie ilości hostów, 67
 obliczanie ilości sieci, 67
 obliczanie metryki, 200
 obniżanie pasma, 237
 ochrona interfejsów, 254

ogłoszenia VTP, 275
 okno
 Captures, 195
 Event list, 22
 IP Configuration, 24
 konfiguracji interfejsów, 28
 konfiguracji Qemu, 175
 konfiguracji urządzenia z linii komend, 28
 Network, 175
 PDU Information, 22
 preferencje, 33
 programu Wireshark, 194
 symulatora Cisco Packet Tracer, 18
 wiersza poleceń, 26
 właściwości programu GNS3, 193
 właściwości przełącznika, 27
 wyboru połączeń, 20
 wyboru urządzeń, 19
 zarządzania obrazami IOS, 34
 opóźnienie, 201
 OSPF
 czas Dead, 241
 czas Hello, 241

P

Packet Tracer, 17
 pakiet hello, 199, 225
 pakiet LSA, 226
 pamięć
 FLASH, 118
 NVRAM, 87, 117
 nieulotna, 87, 117
 RAM, 117
 ROM, 117
 PAP, 323 *Patrz także* uwierzytelnianie
 parametr
 eq, 355
 gt, 355
 lt, 355
 neq, 355
 parametr TTL, 297
 pełna relacja sąsiedzka (FULL), 227
 pętla routingu, 157
 pętla zwrotna, 188
 ping, 22
 plik konfiguracyjny, 32, 93
 podgląd ramki, 22
 podinterfejs, 288, 343
 podsieci, 56
 podsieci w klasie A, 64
 podsieci w klasie B, 63
 podsieci w klasie C, 62

- podwarstwa LLC, 38
- podwarstwa MAC, 38
- podział sieci, 194
- pole
 - Authentication, 108
 - Hostname, 27, 108
 - Image directory, 32
 - Image file, 33
 - IP Address, 24, 50, 175
 - Katalog projektów, 32
 - Modules, 27
 - PoolName, 96
 - Port Status, 108, 109
 - Static, 24
 - Subnet Mask, 24, 108
 - WPA2-PSK, 108
- polecenia konfiguracyjne, 27
- polecenie
 - access-list, 353, 354, 364
 - bandwidth, 201, 226
 - banner, 88
 - banner motd, 112
 - clear ip ospf process, 226, 235
 - client-identifier, 369
 - client-name, 369
 - clock rate, 134
 - conf t, 50
 - configure terminal, 84, 87
 - copy running-config startup-config, 87, 264
 - copy running-config tftp, 98, 318
 - copy startup-config tftp, 87, 113, 264
 - crypto key generate rsa, 260
 - debug ip rip, 165
 - default router, 367
 - default-information originate, 190
 - default-router, 368
 - delay, 201
 - delete flash vlan.dat, 268
 - description, 161, 165, 304
 - dir flash, 268
 - do sh ip int brief, 162
 - do show vlan, 263
 - duplex, 264
 - enable, 50, 87
 - enable secret, 88, 112, 259
 - encapsulation dot1q, 285, 292, 343
 - encapsulation frame-relay, 336, 338, 343
 - encapsulation ppp, 326, 329
 - exit, 265
 - frame-relay interface-dlci, 339
 - frame-relay map ip, 343
 - hostname, 94, 263
 - interface fa0/0, 50
 - interface fastethernet0/0, 87
 - interface point-to-point, 339
 - interface FastEthernet, 285
 - interface loopback0, 232
 - interface range, 263
 - interface serial 0/0.101 multipoint, 347
 - ip access-group 10 out, 353
 - ip access-list extended, 355
 - ip address, 87, 94, 188
 - ip address dhcp, 190
 - ip bandwidth-percent eigrp, 216
 - ip debug rip, 190
 - ip dhcp excluded-address, 367
 - ip dhcp pool, 367, 368
 - ip dhcp pool test, 368
 - ip domain-name, 260
 - ip hello-interval eigrp 1 30, 216
 - ip host, 246
 - ip nat inside, 364
 - ip nat inside source list 1 pool, 364
 - ip nat outside, 363, 364
 - ip nat pool netmask, 364
 - ip ospf cost, 226
 - ip ospf message-digest-key md5, 244
 - ip ospf name-lookup, 246
 - ip ospf priority, 227
 - ip rip authentication key-chain, 182
 - ip rip authentication mode md5, 182, 191
 - ip route, 124, 133, 171
 - ip ssh version 2, 260
 - ipconfig /all, 51, 261
 - lease, 368
 - line vty 0 4, 112
 - log-adjacency-changes, 245
 - log-adjacency-changes detail, 245
 - login, 88, 112
 - name, 267
 - network, 158, 188, 226
 - no, 268
 - no auto-summary, 189
 - no ip split-horizon., 336
 - no shutdown, 87, 161, 363
 - option 15 ascii, 368
 - option 3 ip, 368
 - option 6 ip, 368
 - passive-interface, 169
 - password, 88, 112
 - ppp authentication chap, 329
 - ppp pap sent-username password, 328
 - router eigrp, 120, 200, 344
 - router ospf, 225, 232
 - router rip, 158, 162
 - router-id, 226, 232, 234
 - service dhcp, 367
 - service password-encryption, 88

polecenie

- setup, 126, 258
- show access-lists, 353
- show cdp neighbors, 132
- show cdp neighbors detail, 131
- show clock, 85, 88
- show flash, 88
- show history, 88
- show interface description, 304, 314
- show interface fastEthernet 0/0, 102
- show interfaces, 85, 88
- show interfaces description, 265
- show ip access-lists, 366
- show ip eigrp neighbors, 207
- show ip eigrp topology, 200, 209
- show ip int brief, 344
- show ip interface brief, 88, 162, 196
- show ip nat translation, 365, 366
- show ip ospf interface, 244
- show ip ospf neighbors, 239, 244
- show ip protocols, 163, 166, 168, 232, 233, 234
- show ip rip database, 168
- show ip route, 134, 168, 170, 207, 236, 292
- show port-security, 262
- show running-config, 85, 88, 93, 96, 112, 168
- show spanning-tree, 307
- show spanning-tree blockedports, 306
- show spanning-tree brief, 304
- show spanning-tree root, 306
- show startup-config, 85
- show version, 87, 88, 125
- show vlan, 265
- show vlan brief, 266, 268, 269, 280
- show vlan name, 266
- show vlan-switch, 290, 291, 316
- shutdown, 154
- spanning-tree mode pvst, 311
- spanning-tree mode rapid-pvst, 299, 313
- spanning-tree portfast, 298
- spanning-tree vlan, 312
- spanning-tree vlan root primary, 308, 318
- switchport access, 253, 317
- switchport access vlan, 266
- switchport mode access, 261, 266, 317
- switchport mode trunk, 254, 270, 317, 346
- switchport port-security, 261
- switchport port-security violation shutdown, 261
- switchport trunk allowed vlan, 270
- terminal monitor, 165
- timers basic, 168
- traceroute, 209
- transport input ssh, 260
- username password, 260
- vlan, 253, 265
- vlan database, 341
- vtp client, 293
- vtp domain, 279
- vtp mode transparent, 279

połączenie

- Ethernet, 15, 136
- konsolowe, 19
- routera do sieci lokalnej, 100
- trunk, 285

POP3, Post Office Protocol, 39

port

- brzegowy, 299
- CONSOLE, 28, 83
- desygnowany, 298
- konsolowy (console), 28, 257
- przełącznika, 253
- port szeregowy, 29
- port trunk, 254

priorytet 32768, 297, 306

proces routingu OSPF, 233

program

- GNS, 194
- SETUP, 118, 257
- Wireshark., 192, 324

projekt sieci, 106

protokoły routingu, 139

protokół

- BGP, 139
- CDP, Cisco Discovery Protocol, 119, 132, 142
- CHAP, 324
- DHCP, 367
- EIGRP, 157, 199
- LCP, 323
- NCP, 323
- OSPF, 225
- PPP, Point-to-Point Protocol, 323
- PVST, 251
- PVST+, 299
- RIP, 148, 157
- RIPv1, 181
- RIPv2, 181
- routingu, 110
- RSTP, 251, 299
- RTP, Reliable Transport Protocol, 199
- STP, 251, 297
- TCP, 40
- UDP, User Datagram Protocol, 37, 40
- VTP, 251, 275

przechwytywanie pakietów, 193

przełącznik, 19, 251, 253
3560, 259
L2, 14
L3, 14

przycisk
Apply, 175
Auto Capture/Play, 22
Network, 175
Testuj, 32

przydzielanie identyfikatorów, 226
PT, 17
PT-REPEATER-NM-1CFE, 43
punkt dostępowy, 110
Putty, 83

Q

QEMU, 174

R

ramka, 22
ramki BPDU, 298
redundancy, 15
reguła podzielonego horyzontu, 158
relacja sąsiedzka 2WAY, 227
relacja sąsiedztwa, 207, 242
reported distance, 211
RJ45, 29
rodzaj połączenia
FastEthernet, 19
role portów w protokole RSTP
port alternatywny, 299
port desygnowany, 299
port główny, 299
port zapasowy, 299
role portów w protokole STP
port desygnowany, 298
port główny, 298
port niedesygnowany, 298
Root ID, 305
router, 14, 117
1841, 19
BDR, 227, 229
desygnowany, 239
desygnowany DR, 226, 229
Router ID, 232
router na patyku, router-on-a-stick, 251, 285, 343
routing
bezklasowy, 139
dynamiczny, 117, 139
klasowy, 139
pomiędzy sieciami VLAN, 285
statyczny, 124, 136

Routing for Network, 163
Routing Information Sources, 233
rozgłaszanie
sieci, 188
tablic, 196
tras, 173
.bin, 32
.bin.unpacked, 33
rozszerzone listy ACL (extended ACL), 351
RS232, 19
ruch wchodzący (inbound), 351
ruch wychodzący (outbound), 351

S

samoczynny wybór połączenia, 20
scalability, 15
schemat sieci z adresami IP interfejsów, 150
Security Violation Count, 262
SecurityViolation, 262
serwer, 15
DHCP, 43, 101, 360
DNS, 246
TFTP, 97, 255
sieć
bezklasowa, 62
domyślna VLAN1, 254
EIGRP, 151
klasowa, 61
komputerowa, 13
połączeniowa, 70
PUNKT-PUNKT, 237
VLAN, 251, 253
WAN, 321, 323
wirtualna, 253
Simulation Mode, 22
skalowalność, 15
skrętka ekranowana, 41
skrętka nieekranowana, 41
SMTP, Simple Mail Transport Protocol, 39
SNMP, 127
Spanning tree enabled protocol rstp, 313
SSH, 259
stacja robocza, 15
stan
blokowania, 298
nasłuchiwanie, 298
przekazywanie, 298
uczenia się, 298
standardowe listy ACL (standard ACL), 351
State, 244
sukcesor, 200
sumaryzacja sieci, 137
symulator sieci, 17

system binarny, 54
system CatOS, 83
system operacyjny IOS, 31, 83, 118
szerokość pasma, 201

T

tabela poleceń, 89
tablica
 adresów MAC, 253
 przełączania, 253
 routingu, 117, 140, 143, 187
 topologii, 211
 translacji, 366
tablice sąsiadów EIGRP, 207
TCP, Transmission Control Protocol, 37
TCP/IP
 konfiguracja ustawień, 26
TCP/IPv4, 101
technologia
 CIDR, 181
 Frame Relay (FR), 321, 333
 NAT, Network Address Translation, 321, 359
 VLSM, 155, 181
telefon IP, 14
Terminal, 29
TEST, 278
test ping, 364
TLS, Transport Layer Security, 39
topologia częściowej siatki, 334
topologia gwiazdy, 334
topologia hub-and-spoke, 334
topologia pełnej siatki, 334
translacja adresów, 359 *Patrz także* NAT
transmisja rozgłoszeniowa (broadcast), 56
trasa
 domyślna, 124
 statyczna, 124, 139
 zapasowa, 211
trójstopniowe uzgodnienie, 40
tryb
 100 Base-TX, 128
 dostępowy, 341
 dostępowy interfejsu, 261
 full-duplex, 128
 konfiguracji globalnej, 84, 205, 265
 konfiguracji interfejsów, 216, 263
 przekazywania, 311
 symulacji, 22, 46
 transparentny, 275
 uprzywilejowany (Privileged Exec Mode), 84, 126
 użytkownika (User Exec Mode), 84

tryb pracy
 access, 294
 klient, 275
 serwer, 275, 293
 trunk, 294
 przełącznika w protokole VTP, 275
tworzenie podsieci, 152
tworzenie sieci VLAN, 265
tworzenie zbioru kluczy, 191
Type, 370

U

udostępnianie połączenia internetowego, 102
urządzenia końcowe
 komputer stacjonarny, 19
 laptop, 19
 serwer, 19
 telefon IP, 19
 telewizor, 19
urządzenia sieciowe, 26
urządzenie
 DCE, Data Circuit-Termination Equipment, 323
 DTE, Data Terminal Equipment, 323
usługa CDP, 132
ustawienia domyślne przełącznika, 257
usuwanie pliku konfiguracyjnego, 268
usuwanie sieci VLAN, 268
uwierzelnianie
 CHAP, 323
 MD5, 182
 PAP, 323
 plain text, 182

V

vlan natywny, 254
VLSM, 155, 181
VOIP, 37

W

WAN, Wide Area Network, 36
warstwa
 aplikacji, 36, 39
 fizyczna, 38, 40
 internetowa, 40
 łącza danych, 38
 prezentacji, 37
 sesji, 37
 sieci, 38
 transportu, 37, 39

- warstwy modelu ISO/OSI, 36
- warunek dopuszczalności, 211
- wektor odległości, 158
- Wireshark, 192
- WPA2-PSK, 108
- wtyk
 - DB-9, 83
 - RJ45, 83
- wybór
 - interfejsu, 19
 - najlepszej ścieżki, 200
 - rodzaju połączenia, 19
- wykluczenia adresów, 61
- wyznaczanie maski podsieci, 73

Z

- zakładka Config routera, 129
- zakładka emulatora
 - Dynamips, 32
 - General Settings, 32
 - Obrazy IOS, 33
 - Preferences, 192
 - Simulation mode, 45

- zakładka symulatora, 24, 27
 - Config, 22, 24, 27, 108
 - Desktop, 22, 24, 29, 107
 - Physical, 22, 24, 109
 - Slots, 289
 - Software/Services, 22
- zakresy adresów, 63, 64, 65
- zapasowy router desygnowany, 239
- zapisana konfiguracja, 96, 99, 114
- zawartość
 - przesłanej ramki, 23
 - ramki Cisco HDLC, 326
 - zakładki Config, 25
 - zakładki Desktop, 25
 - zakładki Physical, 24
- zegar DCE, 154
- znak ?, 84
- zsumaryzowana sieć
 - 172.16.0.0/21, 212
 - 192.168.0.0/20, 212

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



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

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

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

GRUPA WYDAWNICZA

 **Helion SA**

W drodze do CCNA

Uzyskanie certyfikatu CCNA to ważny krok na drodze do kompleksowego opanowania wszelkich zagadnień związanych z działaniem sieci komputerowych. Wiedza na temat tego, co dzieje się w rzeczywistej, działającej sieci, pozwala nie tylko rozwiązywać bieżące problemy, lecz także przewidywać nadciągające katastrofy. I często okazuje się bezcenna, zarówno w małym biurze, jak i ogromnej firmie. W dzisiejszym świecie połączenia między komputerami zapewniają obieg informacji, pozwalają szybko się porozumiewać i przysyłać dokumenty. Bez żadnej przesady można nazwać je krwioobiegiem każdego przedsiębiorstwa, warunkującym jego normalne funkcjonowanie. Ekspertem w tej dziedzinie na pewno nigdy nie zabraknie pracy!

Dwie pierwsze części cyklu „W drodze do CCNA” dały przyszłym profesjonalistom w zakresie sieci komputerowych doskonale przygotowanie teoretyczne, natomiast część trzecia zapewni świetne przygotowanie praktyczne. Twoim celem będzie rozwiązanie jak największej liczby zamieszczonych tu zadań o bardzo różnym charakterze oraz udzielenie odpowiedzi na setki pytań testowych. Przyjrzyj się skomplikowanym problemom, zdarzającym się w realnie działających sieciach, i postarasz się zaproponować sensowne rozwiązania, a potem porównasz je z podanymi odpowiedziami. Książka podzielona jest na cztery części odpowiadające czterem najważniejszym obszarom tematycznym.

- Wprowadzenie do sieci komputerowych, symulatory i emulatory sieci
- Komunikacja w sieciach LAN i adresowanie w sieciach komputerowych
- Podstawowa konfiguracja urządzeń Cisco
- Działanie routera i routing statyczny
- Routing dynamiczny i tworzenie podsieci
- Dynamiczne protokoły routingu — RIPv1, RIPv2, EIGRP, OSPF
- Podstawy przełączania i routing pomiędzy sieciami VLAN
- Protokoły VTP i STP
- Sieci WAN, Frame Relay i listy ACL
- Serwer DHCP i technologia NAT

Bądź pewniakiem — zdobądź bez trudu certyfikat CCNA!

helion.pl
księgarnia
internetowa

Nr katalogowy: 6896

Księgarnia internetowa:
<http://helion.pl>

Zamówienia telefoniczne:
0 801 339900
0 601 339900



Helion

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

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

sięgnij po **WIĘCEJ**



KOD KORZYŚCI

ISBN: 978-83-246-3319-7



Cena: 69,00 zł

Informatyka w najlepszym wydaniu