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

Helion

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

Printed in Poland.

Spis treści

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

Międzysieciowy 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 runts, 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 `inteface 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.

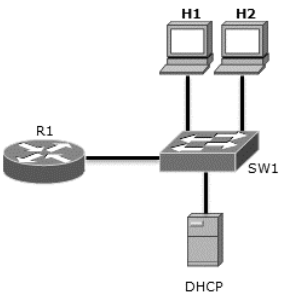
Rysunek 5.2.
Założenia do 2. laboratorium

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



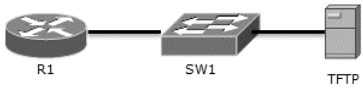
2. Nazwij wszystkie urządzenia, tak jak pokazano na rysunku.
3. Ustaw komunikat informacyjny na routerze oraz przełączniku.

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. Wydaj 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)#
```

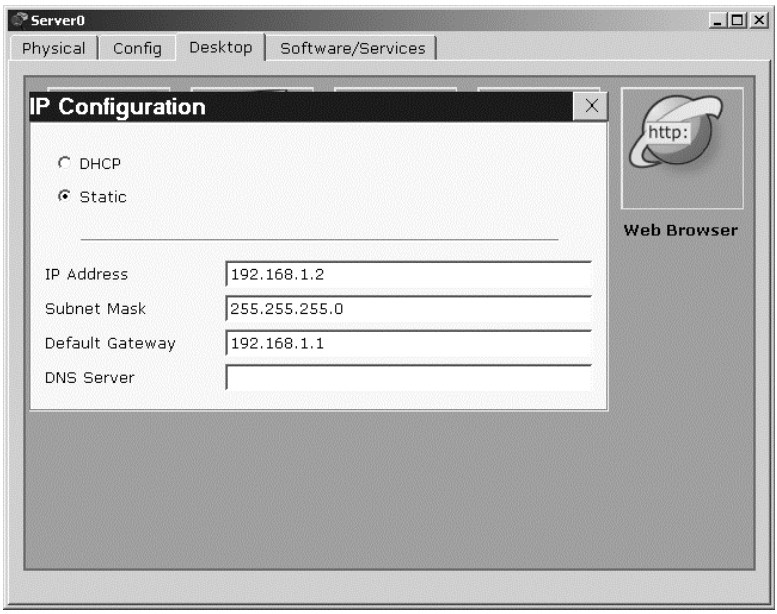
W ostatnim kroku konfiguracji routera R1 należy przydzielić adres IP do interfejsu *FastEthernet0/0*. W tym przypadku możesz przydzielić dowolny adres IP. Poniżej przedstawiono konfigurację interfejsu routera R1:

```
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)#
```

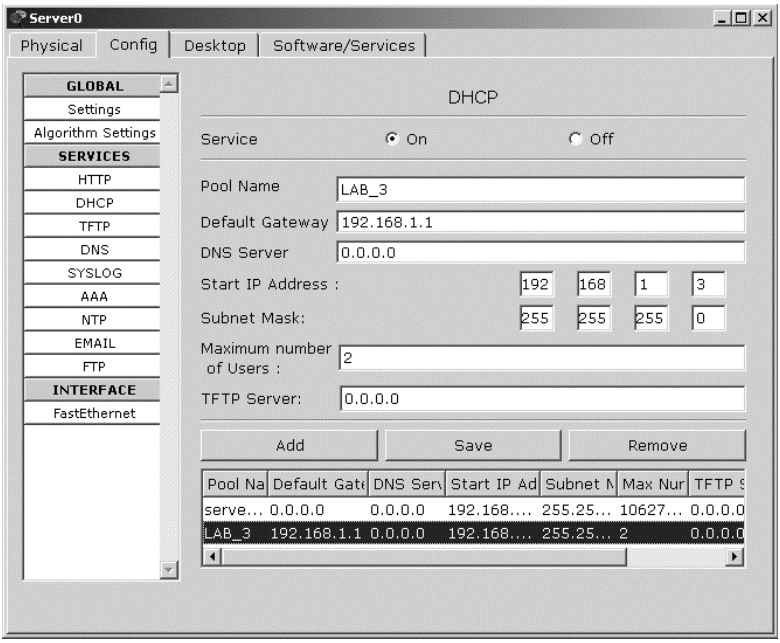
W ostatnim punkcie powyższego laboratorium należy skonfigurować serwer DHCP. W tym celu kliknij go dwukrotnie i przejdź do zakładki *Desktop*. Następnie kliknij pozycję *IP Configuration*. Podaj adres IP, jaki będzie przypisany do serwera (rysunek 5.6). Pamiętaj, że adres musi znajdować się w tej samej 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 informację 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-confg]? 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 runnig-config startup-config`. Spójrz na listing poniżej:

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

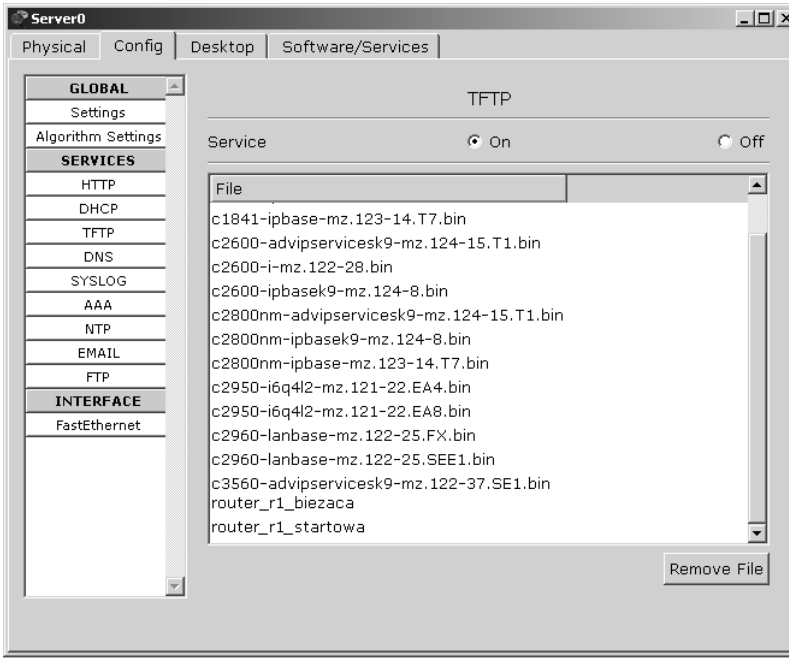
Teraz skopiuj zapisaną konfigurację startową na serwer, wykorzystaj polecenie `copy startup-config tftp`. Oto przykład:

```
R1#copy startup-config tftp
Address or name of remote host []? 192.168.1.2
Destination filename [R1-confg]? 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*. Przejedź 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.

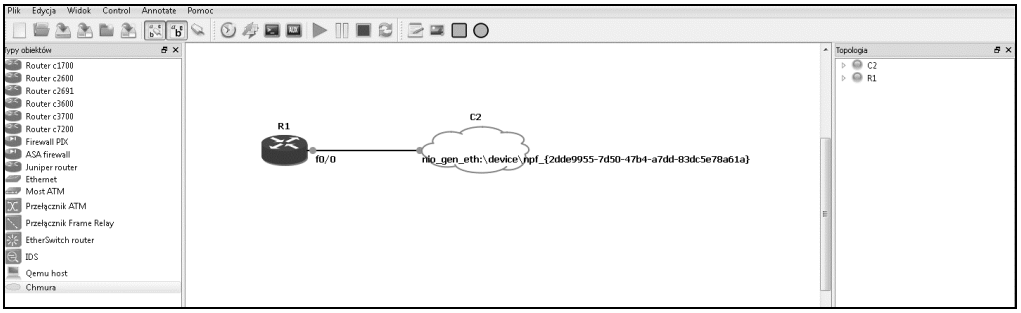
Wszystkie zarchiwizowane konfiguracje pozostaw na serwerze tak długo, jak to możliwe. Pliki te nie zajmują wiele przestrzeni dyskowej, a czasami zdarzają się sytuacje, które wymagają cofnięcia się.

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. Zacznijmy od przygotowania środowiska GNS3 i połączenia go z rzeczywistą siecią.

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



Rysunek 5.9. *Połączenie routera do sieci lokalnej*

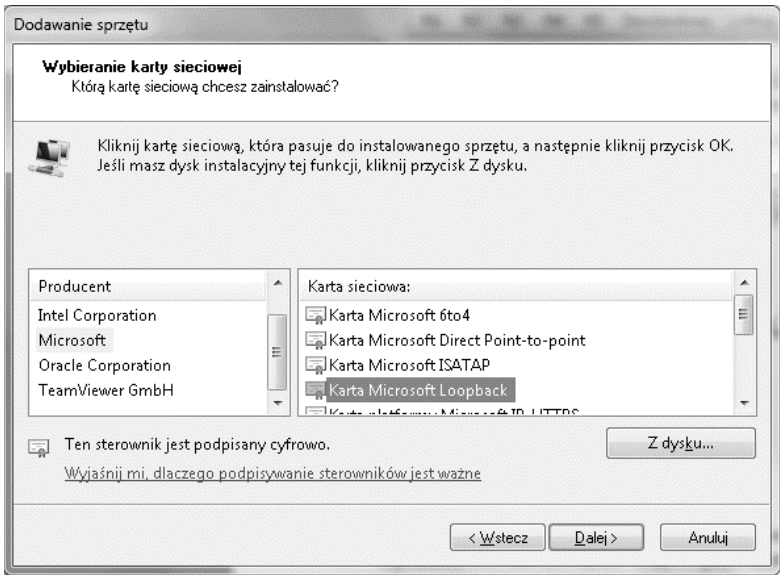
Założeniem jest, aby router mógł komunikować się z internetem, ponadto ma otrzymać dowolny adres IP z podsieci 192.168.137.X/24. Więc w pierwszym kroku utworzymy w systemie operacyjnym interfejs wirtualny *LOOPBACK*. Przedstawiona konfiguracja została opisana na podstawie systemu Windows 7.

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 zapełnienie 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 ustawiania 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).

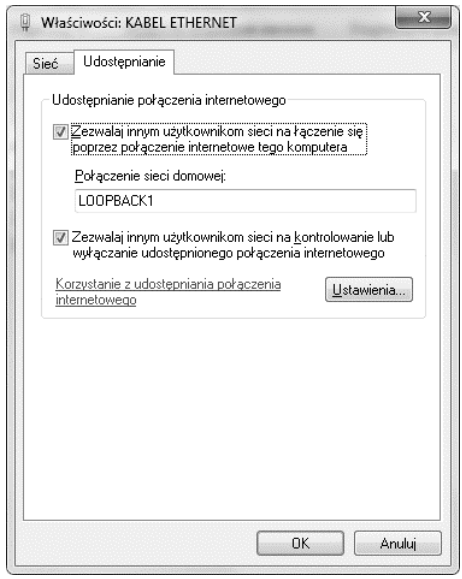
Teraz kliknij prawym przyciskiem myszy kartę *LOOPBACK* i wybierz *Właściwości*. Z listy na karcie *Sieć* wybierz pozycję *Protokół internetowy w wersji 4 (TCP/IPv4)* i kliknij *Właściwości*. W polu *Adres IP* możesz podać dowolny zakres, jaki ma być przydzielany (rysunek 5.12).

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

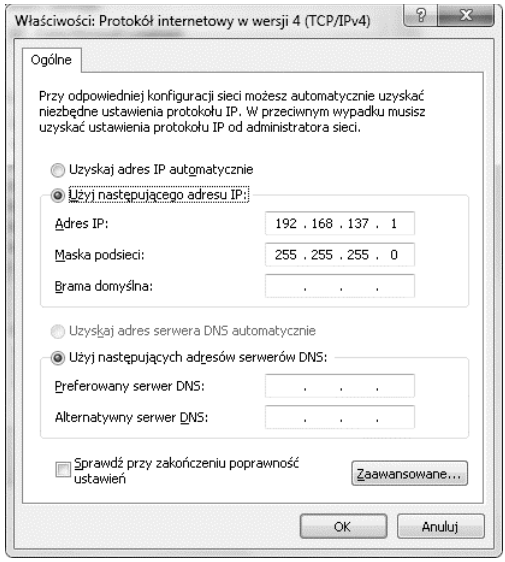
W oknie *Konfigurator urządzenia* przejdź na zakładkę *NIO Ethernet*. Z listy rozwijalnej wybierz kartę *LOOPBACK*, następnie kliknij przycisk *Dodaj*. Kliknij *Zastosuj* i *OK*, aby zapisać ustawienia. Zamknij okno i połącz router z chmurą, następnie przejdź do konfiguracji routera R1.

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`:

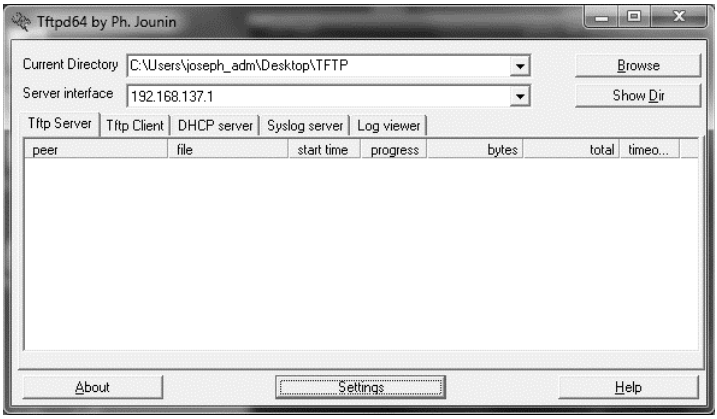
```
R1#show interface fa0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is c400.10e4.0000 (bia c400.10e4.0000)
  Internet address is 192.168.137.235/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, 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).

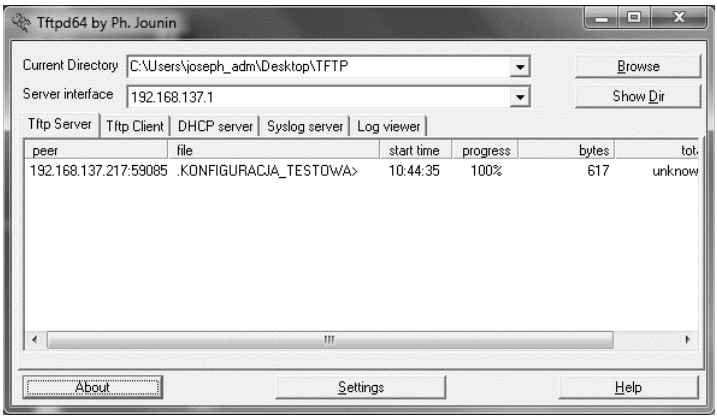


Rysunek 5.13. *Konfiguracja serwera TFTP*

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-confg]? 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

E

F

G

H

I

K

L

Ł

M

N

O

P

Q

R

S

T

U

V

W

Z

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 przesyłać dokumenty. Bez żadnej przesady można nazwać je krwiobiegiem każdego przedsiębiorstwa, warunkującym jego normalne funkcjonowanie. Ekspertom w tej dziedzinie na pewno nigdy nie zabraknie pracy!

Dwie pierwsze części cyklu „W drodze do CCNA" dały przyszłym profesjonalistom w zakresie sieci komputerowych doskonałe 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. Przyjrzysz 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!

ISBN: 978-83-246-3319-7

9 788324 633197

Cena: 69,00 zł