Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 9: Konfiguracja urządzeń sieciowych Cisco. Packet Tracer

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

04.2022

I. Wprowadzenie

Podstawowa konfiguracja urządzeń sieciowych obejmuje taką zmianę ich ustawień, aby urządzenie działało poprawnie (spełniało swoją rolę) i w sposób bezpieczny (tak, aby przykładowo nie można było się na nie włamać).

Na większości urządzeń działa jakiś system operacyjny, z którym administrator może komunikować się poprzez interfejs wiersza poleceń, łącząc się z urządzeniem zdalnie (przez telnet lub SSH) lub lokalnie (podłączając się do niego kablem konsolowym). W przypadku urządzeń firmy Cisco (jednego z wiodących producentów sprzętu sieciowego), system ten nazwa się *Cisco IOS*.

W przypadku urządzeń firmy Cisco, podstawowa konfiguracja obejmuje:

- ustawienie haseł:
  - dostępu do portu konsolowego (*line con 0* ⇒ *password*, *login*),
  - dostępu do połączeń zdalnych (linii witualnej — vty) (*line vty 0 4* ⇒ *password*, *login*),
  - trybu uprzywilejowanego (*enable secret/password*),
- zmianę nazwy urządzenia, tak, aby było rozpoznawalne przez administatora (*hostname*),
- ustawienie baneru *message-of-the-day* — informacji wyświetlanej podczas próby zalogowania na urządzenie, mającej na celu odstraszyć niepowołane osoby przed uzyskaniem nieautoryzowanego dostępu do urządzenia (*banner motd*),

- konfigurację interfejsów:
  - na routerze: ustawienie adresu IP (*ip address*) i włączenie portów (*no shutdown*),
  - na switchu: wyłączenie nieużywanych portów (*shutdown*), ustawienie adresu IP na interfejsie vlan1, aby móc się łączyć ze switchem przez telnet (*interface vlan1* ⇒ *ip address, no shutdown*),
- ewentualne uruchomienie na routerze serwera DHCP, aby automatycznie przydzielał adresy IP urządzeniom z danej sieci:
  - określenie adresów, które nie mają być przydzielane hostom (np. są już w użyciu przez router czy switch, ustawione statycznie przez administratora) (*ip dhcp excluded-address*),
  - stworzenie puli adresów przydzielanych hostom (*ip dhcp pool*),
  - określenie adresu bramy domyślnej (*default-router*), serwera DNS dla hostów z danej puli (czy też jeszcze innych danych).

Cisco Packet Tracer jest programem (stworzonym przez firmę Cisco), w którym możemy symulować sieci komputerowe — dodawać, łączyć i konfigurować różne urządzenia. To w tym programie przećwiczysz konfigurowanie urządzeń Cisco. Jeśli nie masz dostępu do Packet Tracera, zajrzyj na ⇒ stronę Cisco ⇐, dołącz do darmowego kursu z PT na ciscowej platformie edukacyjnej NetAcad i pobierz go za darmo.

II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest nabycie umiejętności konfiguracji urządzeń sieciowych (firmy Cisco):

- podstawowej konfiguracji (nazwa urządzenia, hasła do trybu uprzywilejowanego, na linię konsolową i vty, baner *message-of-the-day*),
- konfiguracji interfejsów (adres IP, włączenie interfejsu),
- konfiguracji trasy ostatniej szansy,
- konfiguracji serwera DHCP na routerze Cisco.

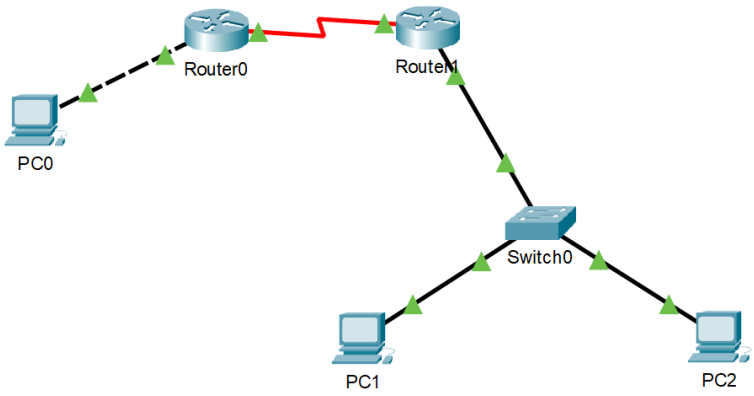
III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputera klasy PC z zainstalowanym programem Cisco Packet Tracer.

IV. Przebieg ćwiczenia

1 Projekt sieci w programie Cisco Packet Tracer

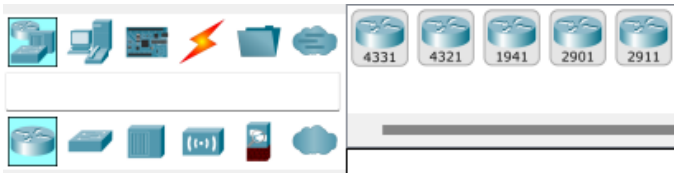
W tym ćwiczeniu w programie Cisco Packet Tracer stworzysz następującą sieć:



1.1 Dodaj w projekcie sieci właściwe urządzenia.

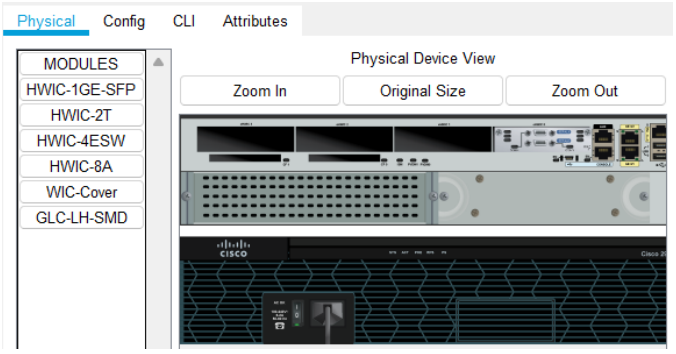
a) Uruchom program Cisco Packet Tracer.

b) Z dolnej części ekranu wybierz sekcję dotyczącą urządzeń pośredniczących (*Network Devices*) i routerów (*Routers*). Przeciągnij na białą część ekranu 2 routery (np. 2911).



c) Rozbuduj router o możliwość obsługi portów szeregowych.

- Kliknij raz lewym przyciskiem myszy na pierwszy router.
- W karcie *Physical* naciśnij wyłącznik routera, aby go wyłączyć.
- W wolne (ostatnie od prawej, oznaczone 0) pole przeciągnij kartę rozszerzeń HWIC-2T.
- Włącz router włącznikiem.
- To samo powtórz z drugim routerem.



d) Wybierz sekcję *Switches* i przeciągnij do projektu 1 switch (np. 2960).

e) Wybierz sekcję z urządzeniami końcowymi (*End Devices*) i przeciągnij do projektu 3 komputery PC.

1.2 Połącz urządzenia właściwymi kablami.

a) Przejdź do sekcji z okablowaniem (*Connections*).

b) Wybierz symbol połaczenia szeregowego (czerwona błyskawica, *serial DTE*). Kliknij w pierwszy router, wybierz port szeregowy Serial0/0/0, aby umieścić w nim jeden koniec kabla, a następnie klijnij w drugi router i umieść drugi koniec kabla w jego porcie Serial0/0/0.

c) Wybierz w sekcji *Connections* symbol skrętki bez przeplotu (czarna ciągła linia, *copper straight-through*) i połącz nim:

- router drugi ze switchem (np. w porty GigabitEthernet0/0),
- komputer PC1 do portu FastEthernet0/1 na switchu,
- komputer PC2 do portu FastEthernet0/2 na switchu.

d) Wybierz w sekcji *Connections* symbol skrętki z przeplotem (czarna przerywana linia, *copper cross-over*) i połącz nim komputer PC0 z portem GigabitEthernet0/0 na routerze pierwszym.

e) Po zakończeniu tego ćwiczenia wszystkie urządzenia powinny być już ze sobą podłączone. Połączenie switch-PC powinno być aktywne (wirtualne diody świecą się na zielono), a połączenia z routerami nie (czerwone diody), gdyż, jak pamiętamy, domyślnie porty na routerze są wyłączone.

2 Konfiguracja urządzeń sieciowych

Całą konfigurację wykonaj w zakładce CLI po kliknięciu na wybrane urządzenie (na początku wpisz *no*, aby wprowadzić konfigurację samodzielnie).

Wymagania:

- Podstawowa konfiguracja switcha i routerów:
  - Odpowiednie nazwy: SW, R1, R2
  - Hasło (szyfrowane) do trybu uprzywilejowanego: *cisco*
  - Hasło do linii konsolowej: *cisco*
  - Hasło do linii wirtualnych 0-4: *cisco*
  - Treść banera *message-of-the-day*: *Unauthorized access prohibited*
- Dostępność CLI urządzeń przez telnet z dowolnego miejsca w sieci (konieczność skonfigurowania tras ostatniej szansy na obu routerach oraz adresu IP na interfejsie vlan1 i bramy domyślnej na switchu)
- Adresy IP komputerów w sieci ze switchem nadawane automatycznie przez router (konieczność skonfigurowania serwera DHCP na routerze R2)
- Adresacja:
  - Sieć dołączona do interfejsu g0/0 routera R1: 10.10.10.0/30

Urządzenie	Interfejs	Adres IP
PC0	Fa0	10.10.10.6
R1	Gi0/0	10.10.10.5

  - Sieć łącząca routery R1 i R2: 10.10.10.4/30

Urządzenie	Interfejs	Adres IP
R1	s0/0/0	10.10.10.1
R2	s0/0/0	10.10.10.2

  - Sieć dołączona do interfejsu g0/0 routera R2: 192.168.0.0/24

Urządzenie	Interfejs	Adres IP
R2	Gi0/0	192.168.0.1
SW	vlan1	192.168.0.254
PC1	Fa0	DHCP
PC2	Fa0	DHCP

Pamiętaj o ustawieniu odpowiednich masek i adresów bramy domyślnej tam, gdzie jest to potrzebne

2.1 Skonfiguruj pierwszy router.

a) Ustaw nazwę urządzenia na R1:

```
Router>en
Router#conf t
Router(config)#hostname R1
```

b) Ustaw baner message-of-the-day o treści *Unauthorized access prohibited*:

```
R1(config)#banner motd $ Unauthorized access prohibited $
```

c) Ustaw szyfrowane hasło do trybu uprzywilejowanego *cisco*:

```
R1(config)#enable secret cisco
```

d) Ustaw hasło do linii konsolowej *cisco*:

```
R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
```

e) Ustaw hasło do linii wirtualnych 0-4 *cisco*:

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

f) Ustaw adres IP 10.10.10.5 z maską 255.255.255.252 na interfejsie g0/0 i włącz go:

```
R1(config)#interface g0/0
R1(config-if)#ip addr 10.10.10.5 255.255.255.252
R1(config-if)#no shutdown
```

g) Ustaw adres IP 10.10.10.1 z maską 255.255.255.252 na interfejsie s0/0/0 i włącz go:

```
R1(config-if)#interface s0/0/0
R1(config-if)#ip addr 10.10.10.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#exit
```

h) Stwórz statyczną trasę ostatniej szansy, prowadzącą do routera R2:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

2.2 Skonfiguruj drugi router.

a) Ustaw nazwę urządzenia na R2:

```
Router>en
Router#conf t
Router(config)#hostname R2
```

b) Ustaw baner message-of-the-day o treści *Unauthorized access prohibited*:

```
R2(config)#banner motd $ Unauthorized access prohibited $
```

c) Ustaw szyfrowane hasło do trybu uprzywilejowanego *cisco*:

```
R2(config)#enable secret cisco
```

d) Ustaw hasło do linii konsolowej *cisco*:

```
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
```

e) Ustaw hasło do linii wirtualnych 0-4 *cisco*:

```
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
```

f) Ustaw adres IP 192.168.0.1 z maską 255.255.255.0 na interfejsie g0/0 i włącz go:

```
R2(config)#interface g0/0
R2(config-if)#ip addr 192.168.0.1 255.255.255.0
R2(config-if)#no shutdown
```

g) Ustaw adres IP 10.10.10.2 z maską 255.255.255.252 na interfejsie s0/0/0 i włącz go:

```
R2(config-if)#interface s0/0/0
R2(config-if)#ip addr 10.10.10.2 255.255.255.252
R2(config-if)#no shutdown
R2(config-if)#exit
```

h) Stwórz statyczną trasę ostatniej szansy, prowadzącą do routera R1:

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

i) Skonfiguruj serwer DHCP, który będzie nadawał komputerom z sieci 192.168.0.0/24 adresy IP automatycznie:

- Wyklucz z puli DHCP adresy przydzielone switchowi SW i routerowi R2:

```
R2(config)#ip dhcp excluded-address 192.168.0.1
R2(config)#ip dhcp excluded-address 192.168.0.254
```

- Stwórz pulę z pozostałych adresów z sieci 192.168.0.0/24 i przekaż komputerom też adres bramy domyślnej (routera R2):

```
R2(config)#ip dhcp pool Pula
R2(dhcp-config)#network 192.168.0.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.0.1
```

2.3 Skonfiguruj switch.

a) Ustaw nazwę urządzenia na SW:

```
Switch>en
Switch#conf t
Switch(config)#hostname SW
```

b) Ustaw baner message-of-the-day o treści *Unauthorized access prohibited*:

```
SW(config)#banner motd $ Unauthorized access prohibited $
```

c) Ustaw szyfrowane hasło do trybu uprzywilejowanego *cisco*:

```
SW(config)#enable secret cisco
```

d) Ustaw hasło do linii konsolowej *cisco*:

```
SW(config)#line con 0
SW(config-line)#password cisco
SW(config-line)#login
```

e) Ustaw hasło do linii wirtualnych 0-4 *cisco*:

```
SW(config-line)#line vty 0 4
SW(config-line)#password cisco
SW(config-line)#login
SW(config-line)#exit
```

f) Ustaw adres IP 192.168.0.254 z maską 255.255.255.0 na interfejsie wirtualnym vlan1 i włącz go:

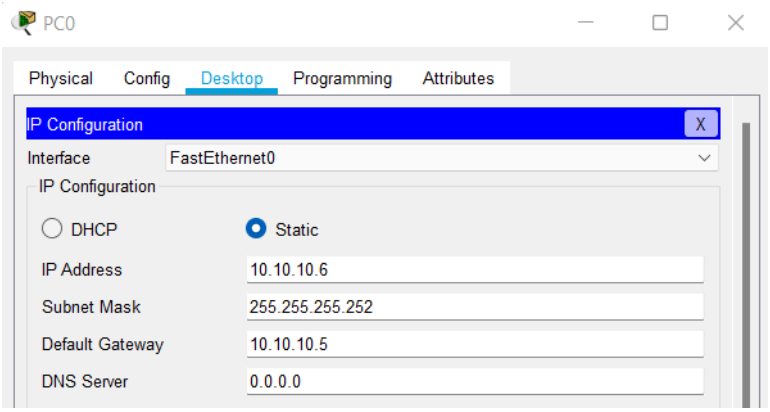
```
SW(config)#interface vlan1
SW(config-if)#ip addr 192.168.0.254 255.255.255.0
SW(config-if)#no shutdown
SW(config-if)#exit
```

g) Ustaw adres bramy domyślnej na switchu — jego bramą domyślną jest router R2:

```
SW(config)#ip default-gateway 192.168.0.1
```

2.4 Skonfiguruj komputery PC.

a) Kliknij w komputer PC0. Wybierz kartę *Desktop*, a następnie aplikację *IP Configuration*.



b) Upewnij, że wybrane jest nadawanie adresu IP statycznie, po czym nadaj komputerowi adres IP 10.10.10.6 z maską 255.255.255.252 i bramą domyślną 10.10.10.5.

c) Na komputerach PC1 i PC2 zmień ustawienia IP Configuration ze Static na DHCP i zobacz, czy kommputery dostały właściwe adresy od serwera DHCP.

3 Testowanie poprawności działania sieci

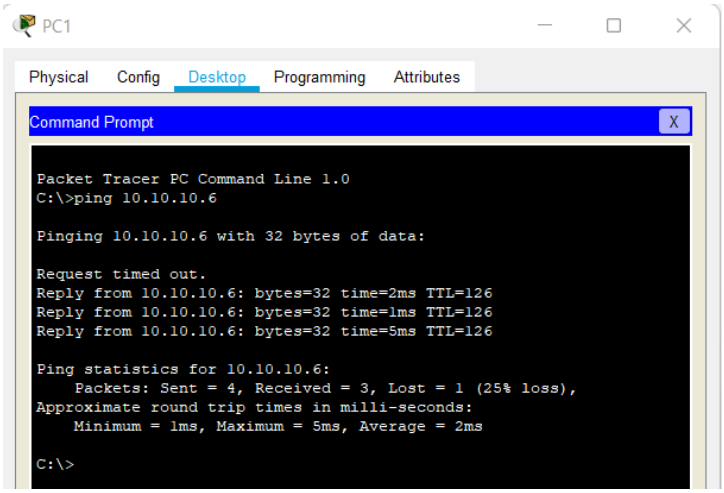
3.1 Sprawdź, czy istnieje komunikacja pomiędzy urządzeniami za pomocą komendy *ping*.

a) Na komputerze PC0 w zakładce *Desktop* wybierz *Command Prompt*. Z poziomu PC0 osiągalne powinny być wszystkie skonfigurowane interfejsy (g0/0 i s0/0/0 na R1, s0/0/0 i g0/0 na R2, vlan1 na SW, PC1 oraz PC2). Wykonaj więc polecenie ping na adresy IP: 10.10.10.5, 10.10.10.1, 10.10.10.2, 192.168.0.1, 192.168.0.254.

b) Powtórz to samo, wysyłając pingi z komputera PC1 oraz PC2 (w tym wypadku pinguj również adres IP komputera PC0, czyli 10.10.10.6).

3.2 Sprawdź, czy możesz połączyć się z urządzeniami sieciowymi poprzez telnet.

Z poziomu aplikacji *Command Prompt* w zakładce *Desktop* powinieneś móc wykonać telnet na wszystkie urządzenia sieciowe (R1 pod adresem 10.10.10.1,



R2 192.168.0.1, SW 192.168.0.254) ze wszystkich komputerów w sieci (PC0, PC1, PC2). Zaloguj się na każde z tych urządzeń, podając właściwe hasło.

W razie problemów sprawdź poprawność:

- adresacji IP (komendą *show ip int brief*),
- całości konfiguracji (komendą *show running-config*).

V. Pytania kontrolne

1. Wymień 3 rodzaje haseł, jakie można ustawić na routerze Cisco.
2. Jakie 2 podstawowe kroki należy podjąć, aby skonfigurować interfejs ethernetowy na routerze Cisco? Wymień odpowiadające im komendy.
3. Gdzie wyświetlany jest baner *message-of-the-day* i jaka jest jego rola?
4. Wymień etapy uruchamiania na routerze Cisco serwera DHCP.

Odpowiedzi:

Plik konfiguracyjny switcha SW:

```
SW#show runn
Building configuration...

Current configuration : 1259 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.0.254 255.255.255.0
!
ip default-gateway 192.168.0.1
!
banner motd ^C Unauthorized access prohibited ^C
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 login
!
!
!
!
```

Plik konfiguracyjny routera R1:

```
R1#show run
Building configuration...

Current configuration : 1008 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1524724V-
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.10.10.5 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.10.10.1 255.255.255.252
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.2
!
ip flow-export version 9
!
!
!
banner motd ^C Unauthorized access prohibited ^C
!
!
!
!
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
 password cisco
 login
!
!
!
end
```

Plik konfiguracyjny routera R2:

```
R2#show runn
Building configuration...

Current configuration : 1181 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R2
!
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.254
!
ip dhcp pool Pula
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX1524O6ZP-
!
!
!
!
spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 10.10.10.2 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.10.10.1
!
ip flow-export version 9
!
!
!
banner motd ^C Unauthorized access prohibited ^C
!
!
!
!
!
line con 0
 password cisco
 login
!
line aux 0
!
line vty 0 4
 password cisco
 login
!
!
!
end
```