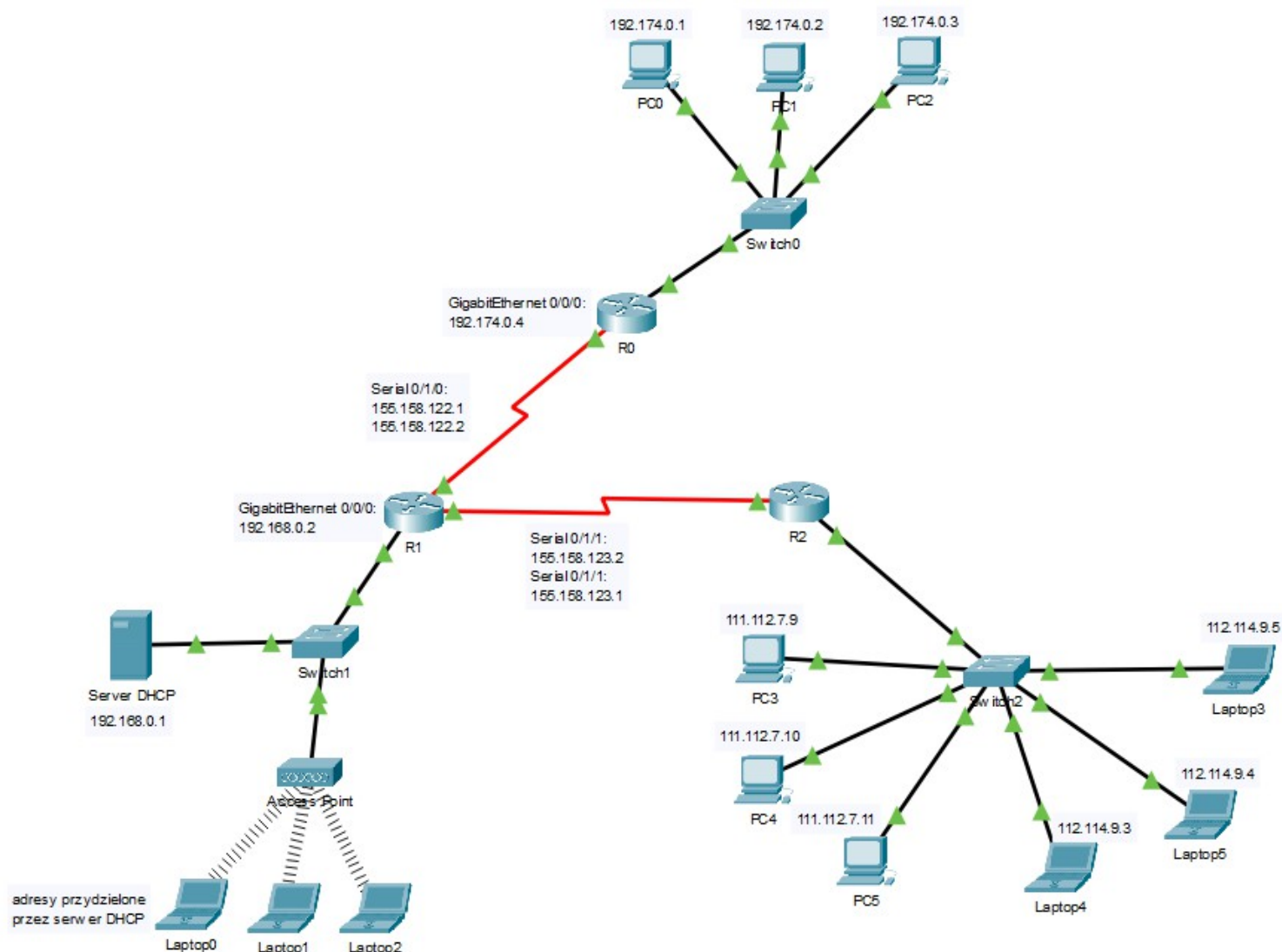


## Sprawozdanie – projekt zaliczeniowy

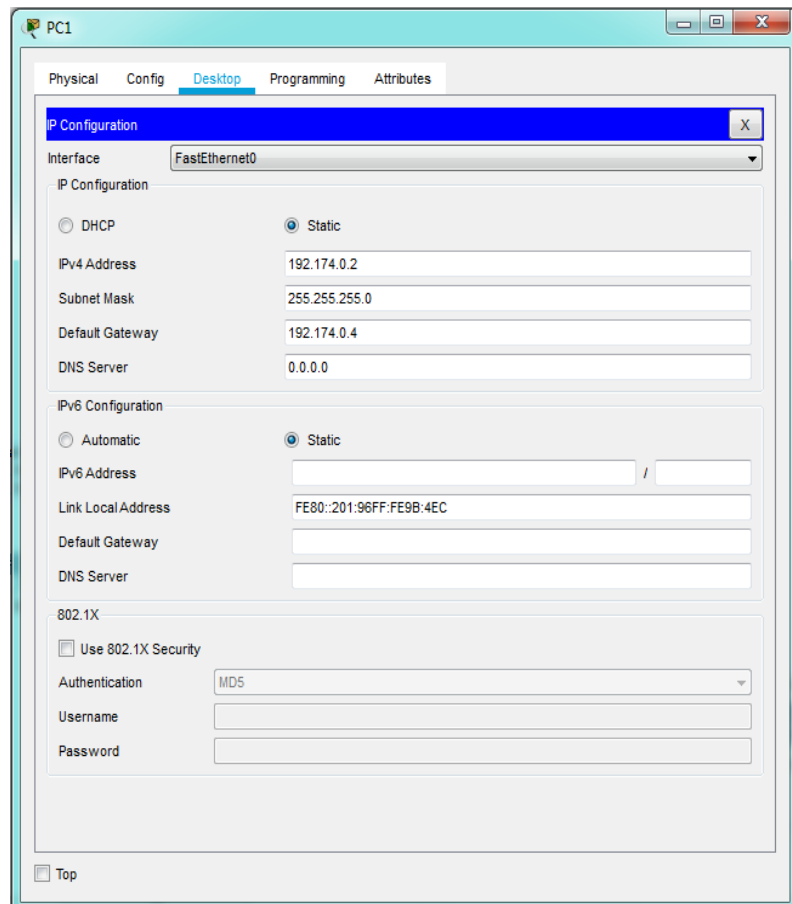
Ewa Namysł



Celem projektu była podstawowa konfiguracja, dopuszczenie możliwości komunikacji komputerów z różnych sieci oraz poprzez SSH (wyłączając przy tym Telnet). Ponadto sieć na skrajnym lewym krańcu (zielona) powinna umożliwiać łączność bezprzewodową (poprzez wireless router albo punkt dostępu), a adresy przydzielane są przez serwer DHCP. Natomiast sieć na prawo (szara) powinna być skonfigurowana jako router on a stick, umożliwiając dwie adresacje na jednym routerze. Jeśli chodzi o sieć na samej górze (niebieska), jest to standardowa sieć Ethernet z adresami przydzielonymi ręcznie.

Pierwszym etapem pracy było podłączenie do przełączników sieciowych wymagających tego urządzeń końcowych. Wykorzystano do tego kabel prosty (copper straight-through), łącząc komputer do wybranego wejścia FastEthernet.

W przypadku niebieskiej sieci, na tym etapie można już skonfigurować adresy IP, a po podłączeniu switcha do routera także bramę.



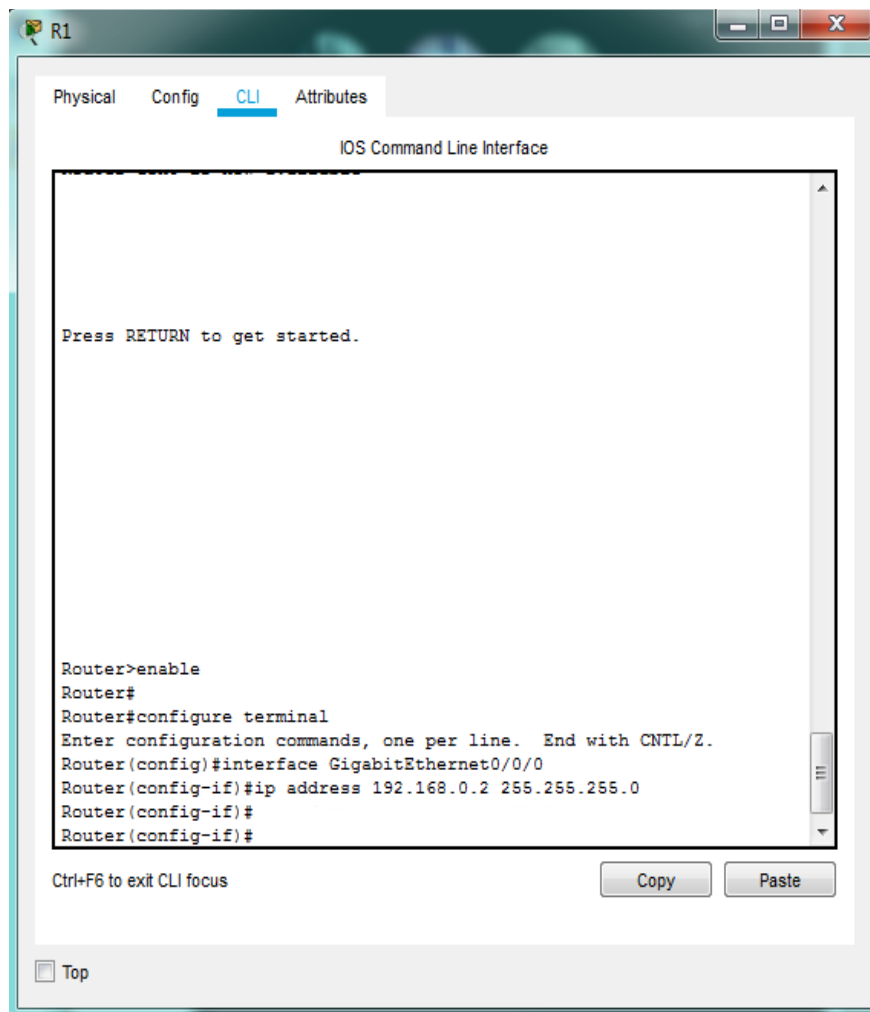
Aby skonfigurować router, należy w konsoli routera zmodyfikować jego adres i maskę na podłączonym FastEthernetie, wchodząc w tryb pracy privileged mode poprzez komendę enable, a następnie wpisując:

```
Router# config terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 192.174.0.4 255.255.255.0
```

Wybrany przez nas adres IP dla routera, wpisujemy w urządzeniach końcowych z tej sieci jako Default Gateway, co umożliwi w późniejszym etapie przesyłanie pakietów do innych sieci.

Aby sprawdzić, czy sieć została prawidłowo skonfigurowana można wykorzystać komendę **ping** w terminalu wybranego komputera wraz z adresem IP hosta docelowego.

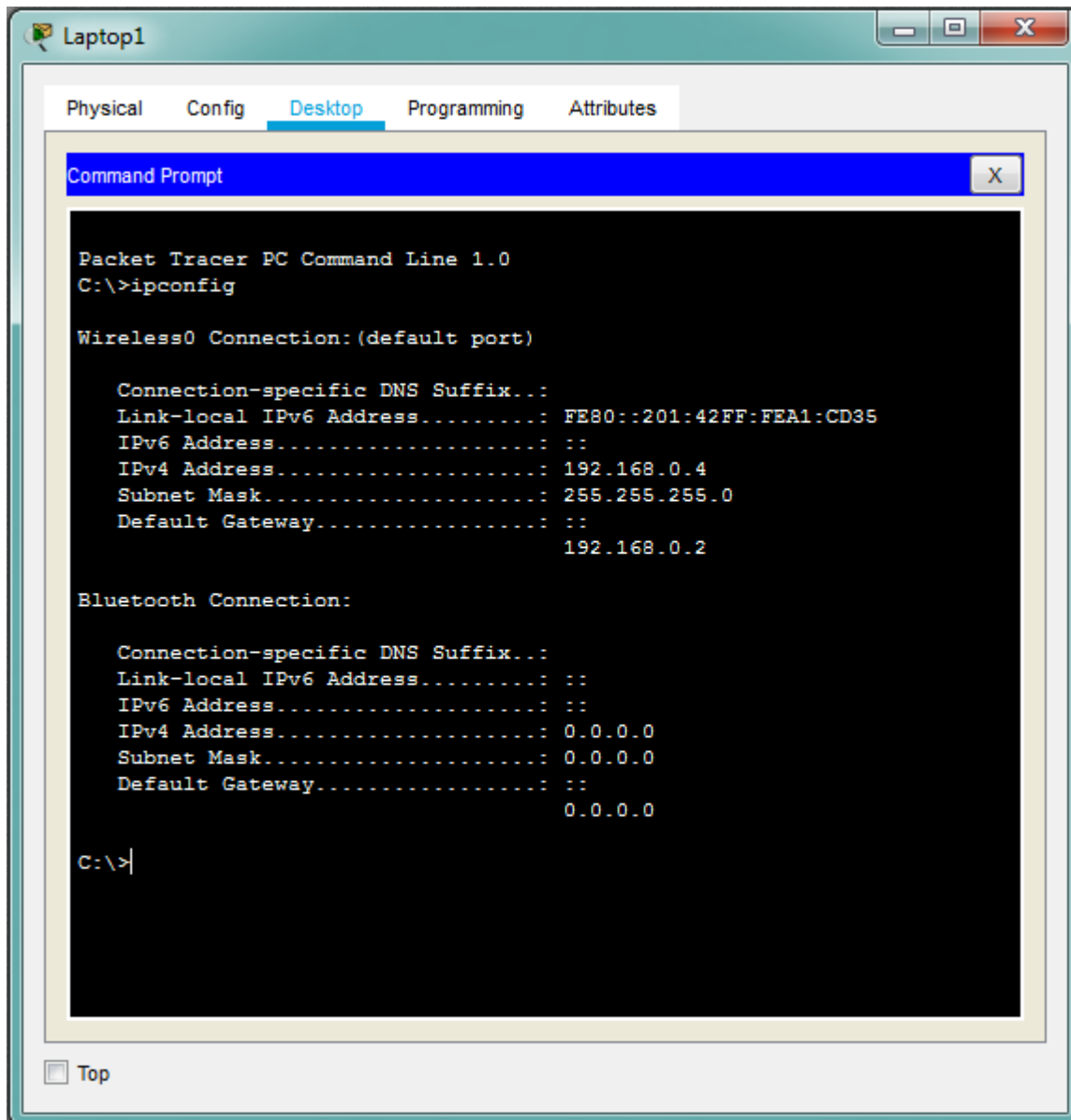
Aby w zielonej sieci umożliwić dostęp do sieci bezprzewodowej, można wykorzystać access point, który pozwoli hostom na łączenie się z siecią bez użycia kabla. Punkt dostępu łączymy kablem prostym ze switchem, a następnie switch z serwerem oraz routerem (którego konfigurujemy w podobny sposób, co poprzednio).



Ponadto, aby laptopy mogły korzystać z bezprzewodowego łącza, należy wyposażyć je w moduł WPC300N. Aby adresy były przydzielane im automatycznie, przełączamy również w każdym IP Configuration statyczne IP na DHCP.

Jeśli chodzi o serwer DHCP, to należy wprowadzić adres IP od którego ma zacząć przydzielanie adresów hostom (w tym przypadku 192.168.0.0) wraz z maską. Konieczne jest także zdefiniowanie bramy na adres routera dla usługi DHCP (jak i dla samego serwera), aby możliwe było przesyłanie pakietów z urządzeń końcowych do innych sieci.

Można sprawdzić przydzielone IP laptopów komendą **ipconfig**:



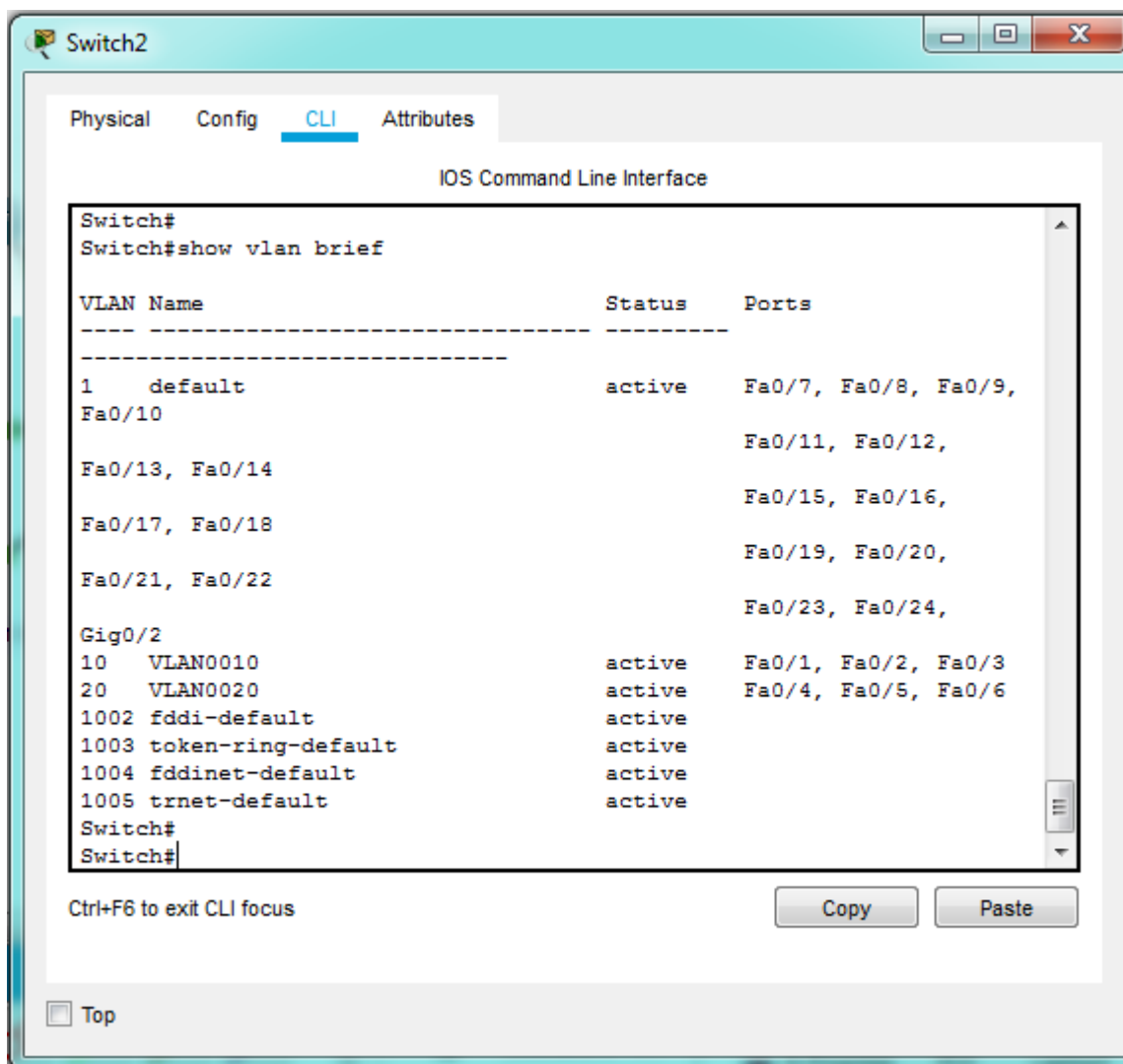
W przypadku szarej sieci, należy umożliwić komunikację między hostami z dwóch różnych sieci, które działają jako VLAN.

Po podłączeniu urządzeń końcowych ze switchem i routerem oraz przypisaniu urządzeniom IP, należy przejść do konfiguracji VLANów na switchu, tworząc dwa i przypisując do każdego po 3 komputery na odpowiadającym im portom:

```
Switch(config)# vlan 10
Switch(config-vlan)# vlan 20
Switch(config) # interface f0/1
```

```
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 10
```

W celu sprawdzenia czy VLANy zostały poprawnie skonfigurowane,  
użyta jest komenda **show vlan brief**:



Po podstawowej konfiguracji routera, przechodzimy do enkapsulacji dla VLANu 10 i 20:

```
Router(config)# interface g0/0/0  
Router(config-subif)# encapsulation dot1Q 10  
Router(config-subif)# ip address 111.112.7.8 255.255.255.000  
Router(config-subif)# encapsulation dot1Q 20  
Router(config-subif)# ip address 112.114.9.2 255.255.255.000  
Router(config-subif)# exit  
Router(config)# interface g0/0/0  
Router(config-if)# no shutdown
```

Po czym należy aktywować trunking na switchu, ponieważ router został skonfigurowany z sześcioma subinterfejsami przypisanymi do dwóch różnych VLANów. Dzięki trunkowi komunikacja może zachodzić poprzez jeden kanał fizyczny, podzielony na wiele kanałów

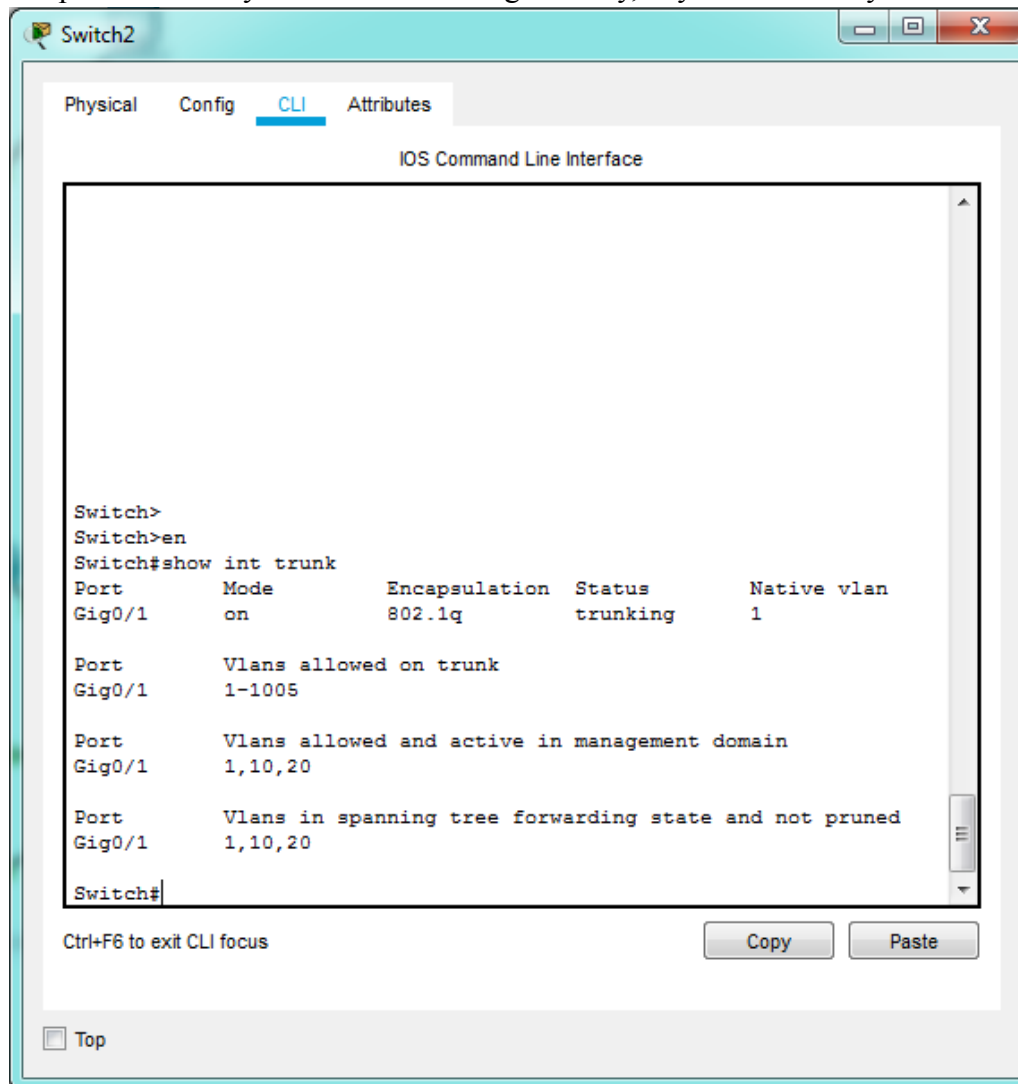
logicznych.

```
Switch(config)# int g0/1
```

```
Switch(config-if)# switchport mode trunk
```

Komunikacja między laptopami i komputerami powinna być już możliwa.

W celu sprawdzenia czy trunk został skonfigurowany, używam komendy **show int trunk**:



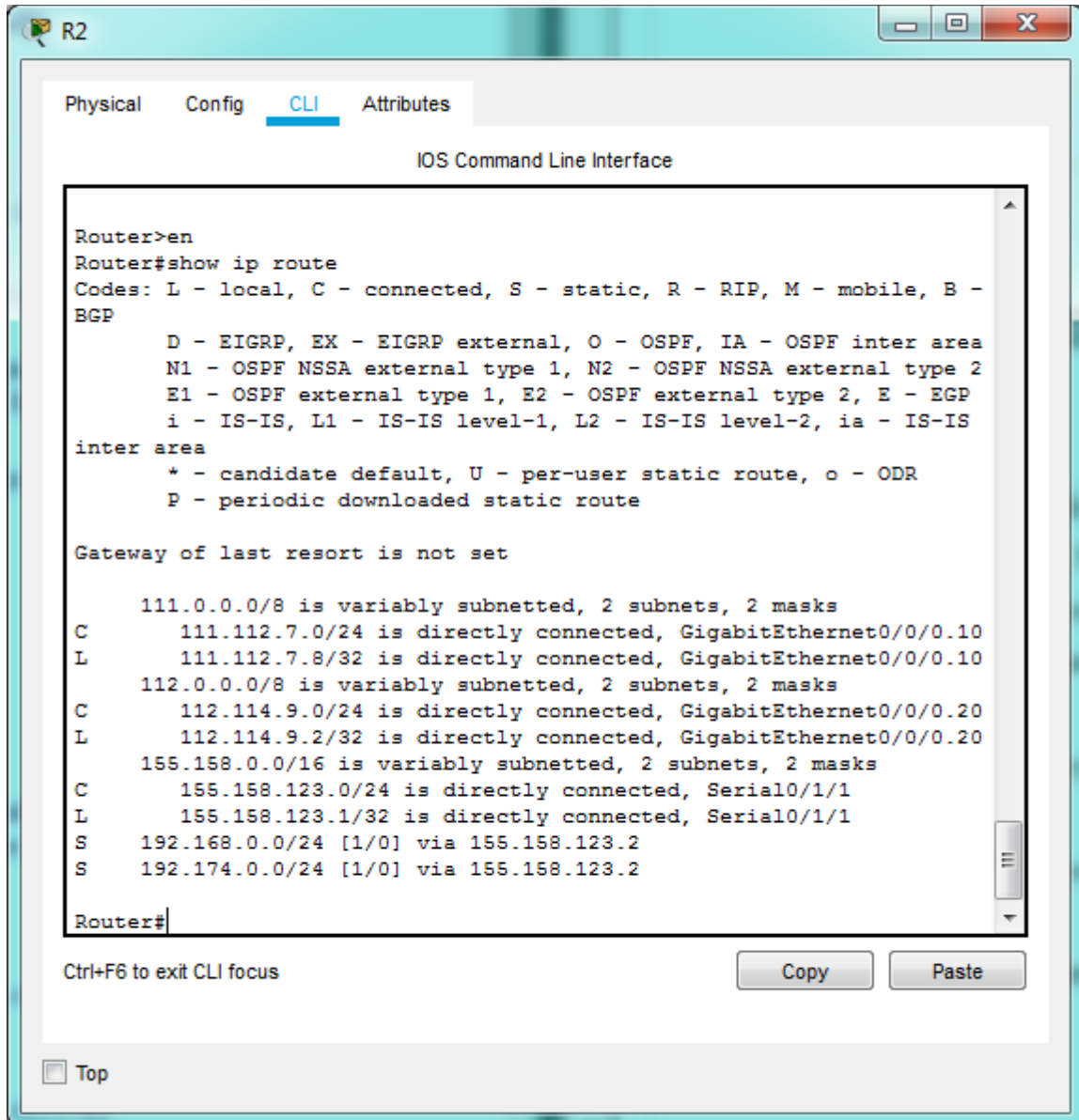
Aby umożliwić komunikację między odrębnymi sieciami, należy dodać każdemu routerowi moduł NIM-2T, połączyć kablem Serial, a w końcu aktywować routing statyczny. Pozwoli to na wybór ścieżki dla pakietów po której muszą się poruszać, aby dotrzeć od nadawcy do adresata. Na każdym routerze musimy wyznaczyć ścieżki, które będą łączyć router z innym.

Przykładowo dla routera R2, aby wyznaczyć drogę do routera R1, wpisujemy:

```
Router(config)# iproute 192.168.0.0 255.255.255.0 155.158.122.2
```

gdzie najpierw podajemy IP routera docelowego, jego maskę, a następnie IP na Serial0/1/1.

Aktualny stan tablic routingu (komenda **show ip route** na R2):



```
Router>en
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
      BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

    111.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       111.112.7.0/24 is directly connected, GigabitEthernet0/0/0.10
L       111.112.7.8/32 is directly connected, GigabitEthernet0/0/0.10
    112.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       112.114.9.0/24 is directly connected, GigabitEthernet0/0/0.20
L       112.114.9.2/32 is directly connected, GigabitEthernet0/0/0.20
    155.158.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       155.158.123.0/24 is directly connected, Serial0/1/1
L       155.158.123.1/32 is directly connected, Serial0/1/1
S       192.168.0.0/24 [1/0] via 155.158.123.2
S       192.174.0.0/24 [1/0] via 155.158.123.2

Router#
```

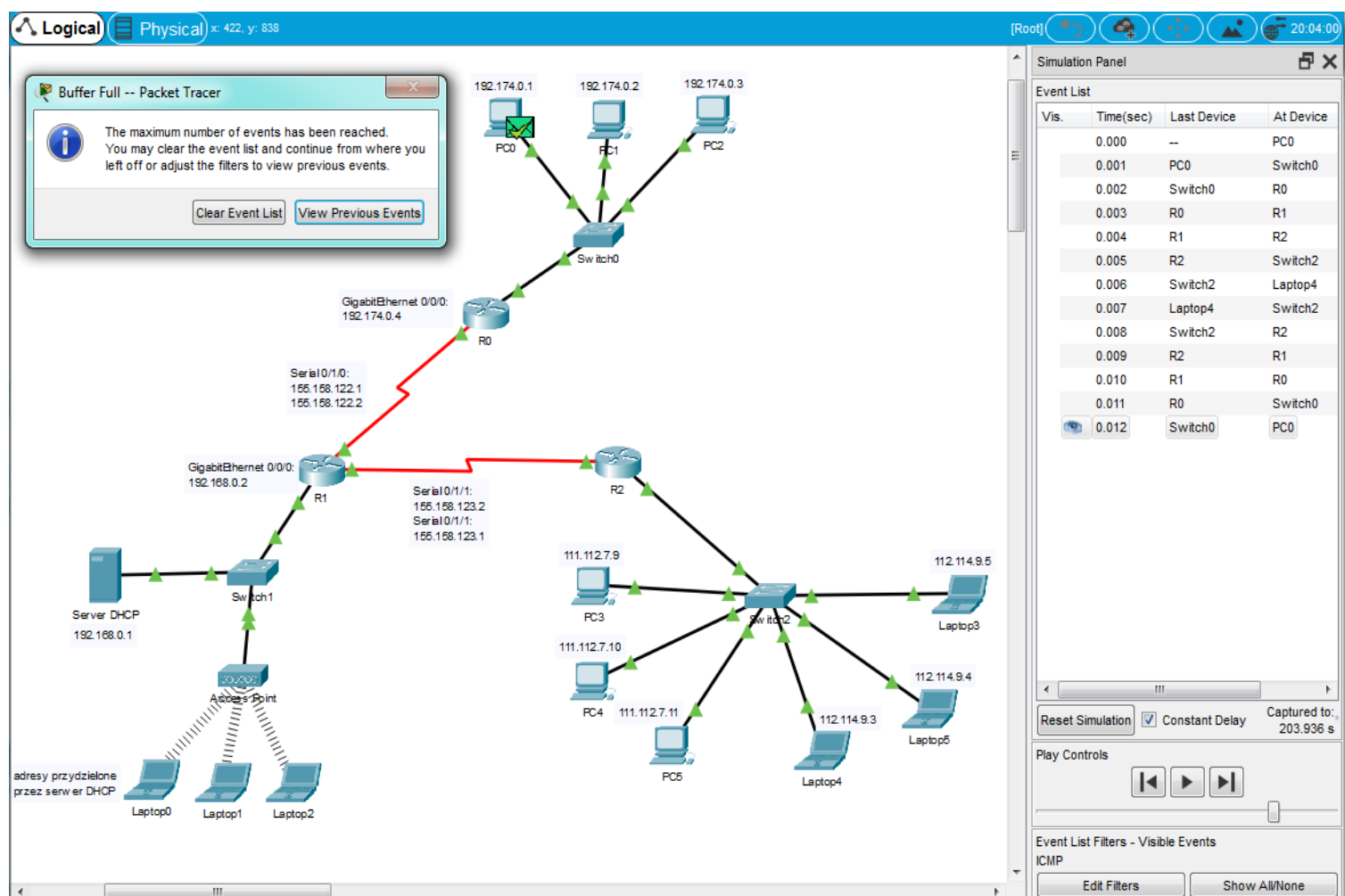
Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

## ICMP wysłany z PC0 do Laptop4

(protokół ICMP wykorzystywany jest w poleceniach terminala ping i traceroute):



Zarówno Telnet, jak i SSH pozwalają na dostęp zdalny do terminala. Jednak Telnet, w przeciwieństwie do SSH, nie szyfruje w żaden sposób danych.

Aby wyłączyć Telnet na urządzeniach sieciowych - na przykładzie routera:

```
Router# config t
Router(config)# line vty 0 4
Router(config-line) transport input ssh
```

Aby włączyć SSH i szyfrowanie haseł należy przejść do trybu konfiguracyjnego:

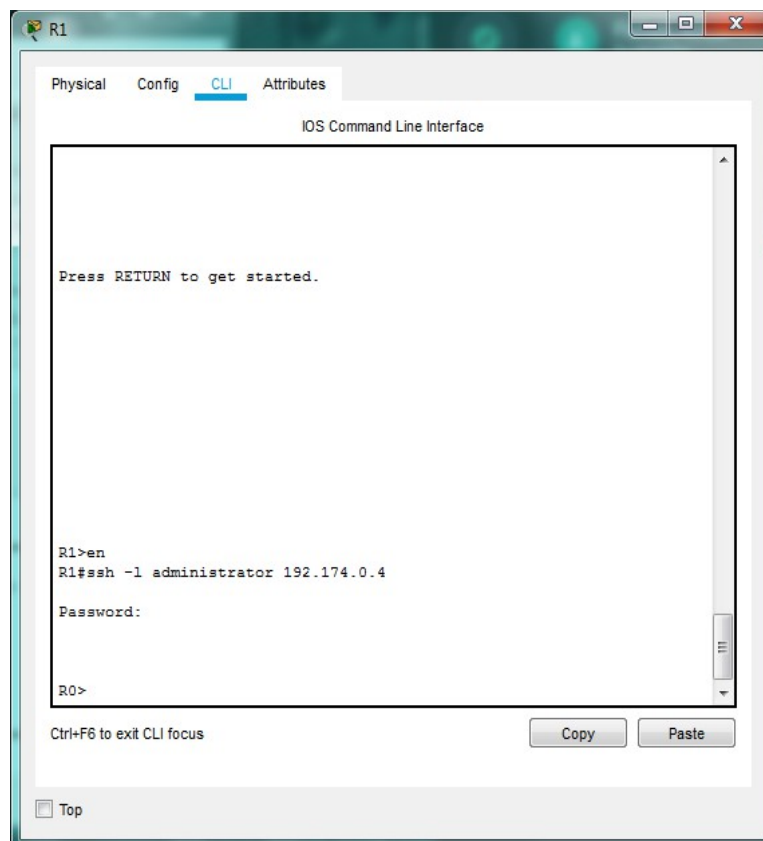
```
Router(config)# service password-encryption
Router(config)# ip domain-name Router0
Router(config)# hostname Router0
Router0(config)# crypto key generate rsa ← następnie wybór długości klucza
Router0(config)# username administrator secret haslo1234
```



```
Router0(config)# line vty 0 15
Router0(config-line)# transport input ssh
Router0(config-line)# login local
```

W podobny sposób należy skonfigurować każde urządzenie sieciowe, na których chcemy mieć możliwość zdalnego łączenia się poprzez SSH.

#### Połączenie SSH Router1 → Router0:



#### Odrzucone połączenie Telnet Router0 → Router1:

