



**WYŻSZA SZKOŁA  
INFORMATYKI i ZARZĄDZANIA**  
z siedzibą w Rzeszowie

**Inżynieria oprogramowania**

*Projektowanie i wdrażanie sieci zarządzania hotelem przy użyciu*

*Packet Tracer*

Prowadzący:

mgr inż. Ewa Żesławska

Autor:

Piotr Kujda

w64874

Kierunek: 6 IIZ/2020, grupa GL04

Rzeszów r.a. 2022/2023

## Spis treści

<b>1. Opis świata rzeczywistego .....</b>	<b>3</b>
<b>1.1. Dane techniczne.....</b>	<b>3</b>
<b>1.2. Opis zasobów ludzkich .....</b>	<b>4</b>
<b>1.3. Wymagania funkcjonalne .....</b>	<b>5</b>
<b>1.4. Wymagania niefunkcjonalne .....</b>	<b>5</b>
<b>2. Diagramy UML .....</b>	<b>5</b>
<b>3. Diagramy aktywności.....</b>	<b>8</b>
<b>4. Diagram klas .....</b>	<b>10</b>
<b>5. Diagramy sekwencji .....</b>	<b>11</b>
<b>6. Diagram stanów .....</b>	<b>13</b>
<b>7. Harmonogram Prac Projektu .....</b>	<b>14</b>
<b>8. Koncepcja systemu oraz wybór środowiska programistycznego i rozwiązań .....</b>	<b>15</b>
<b>9. Testy jednostkowe .....</b>	<b>20</b>
<b>10. Repozytorium .....</b>	<b>53</b>
<b>11. Podsumowanie.....</b>	<b>53</b>
<b>12. Literatura .....</b>	<b>54</b>

## 1. Opis świata rzeczywistego

Celem projektu jest zaprojektowanie i wdrożeniu sieci dla Hotelu. Hotel składa się z trzech pięter, a na każdym piętrze znajdują się różne działy. Pierwsze piętro ma trzy działy (Recepcja, Magazyn i Logistyka), drugie piętro ma trzy działy (Finanse, HR oraz Sprzedaż/Marketing), a trzecie piętro to działy IT i Administracja. W związku z tym, podczas projektowania i wdrażania sieci należy wziąć pod uwagę następujące kwestie:

- Na każdym piętrze powinny znajdować się trzy routery (wszystkie umieszczone w pomieszczeniu serwerowym w dziale IT).
- Wszystkie routery powinny być ze sobą połączone kablem szeregowym DCE.
- Sieć między routerami powinna mieć adresację 10.10.10.0/30, 10.10.10.4/30 i 10.10.10.8/30.
- Każde piętro powinno mieć jeden switch (umieszczony na odpowiednim piętrze).
- Każde piętro powinno mieć sieci WIFI podłączone do laptopów i telefonów.
- Każdy dział powinien mieć drukarkę.
- Każdy dział powinien znajdować się w innej VLANie, z następującymi szczegółami.

### 1.1. Dane techniczne

Pierwsze piętro:

Recepcja - VLAN 80, sieć 192.168.8.0/24

Magazyn - VLAN 70, sieć 192.168.7.0/24

Logistyka - VLAN 60, sieć 192.168.6.0/24

Drugie piętro:

Finanse - VLAN 50, sieć 192.168.5.0/24

HR - VLAN 40, sieć 192.168.4.0/24

Sprzedaż - VLAN 30, sieć 192.168.3.0/24

Trzecie piętro:

Administracja - VLAN 20, sieć 192.168.2.0/24

IT - VLAN 10, sieć 192.168.1.0/24

Do przesyłania tras w sieci należy użyć protokołu routingu OSPF.

Wszystkie urządzenia w sieci powinny automatycznie uzyskiwać adresy IP od odpowiedniego routera skonfigurowanego jako serwer DHCP.

Wszystkie urządzenia w sieci powinny móc ze sobą komunikować się.

Na wszystkich routerach należy skonfigurować SSH do zdalnego logowania.

W dziale IT należy dodać komputer o nazwie Test-PC do portu fa0/1 i użyć go do testowania zdalnego logowania.

Na switchu działu IT należy skonfigurować zabezpieczenia portów, aby umożliwić dostęp tylko Test-PC do portu fa0/1. Aby to osiągnąć, należy wykorzystać metodę sticky, która umożliwia automatyczne uzyskanie adresu MAC urządzenia podłączonego do portu i zapamiętanie go w konfiguracji portu. W trybie naruszenia należy ustawić opcję shutdown, aby port został wyłączony w przypadku próby połączenia innego urządzenia z portem niż Test-PC.

## **1.2. Opis zasobów ludzkich**

Koordynator sieci w hotelu jest odpowiedzialny za zarządzanie siecią i zapewnienie, że urządzenia sieciowe są zawsze w pełni funkcjonalne. Koordynator sieci jest również odpowiedzialny za dostarczanie usług sieciowych, takich jak DHCP, SSH i port security. Do obowiązków koordynatora sieci należy również zarządzanie routerami i przełącznikami, tworzenie VLAN i podział sieci na podsieci. Ponadto, koordynator sieci musi zapewnić, że wszystkie urządzenia sieciowe są w pełni zgodne z wytycznymi bezpieczeństwa sieci i zapewnienia ochrony danych.

Pracownicy Recepcji, Magazynu, Logistyki, Finansów, HR, Sprzedaży/Marketingu, IT oraz Administracji są użytkownikami sieci i posiadają dostęp do Internetu, drukarek i innych urządzeń sieciowych. Klienci hotelu, którzy korzystają z sieci bezprzewodowej, muszą być również obsługiwani przez sieć hotelową i otrzymać adresy IP dynamicznie poprzez DHCP. Hotel korzysta z protokołu OSPF jako protokołu routingu, który umożliwia koordynatorowi sieci przekazywanie informacji o trasach pomiędzy routerami na różnych piętrach.

W każdym departamencie znajduje się drukarka, która jest używana przez pracowników do drukowania dokumentów. Każdy departament ma przypisaną własną sieć VLAN z unikalnym numerem VLAN i przypisaną adresacją IP dla podsieci.

Dodatkowo, w dziale IT znajduje się komputer Test-PC, który służy do testowania zdalnego logowania się do sieci. W celu zwiększenia bezpieczeństwa, port fa0/1 na przełączniku IT-dept został skonfigurowany z funkcją port security, która umożliwia tylko komputerowi Test-PC uzyskanie dostępu do portu.

### **1.3. Wymagania funkcjonalne**

Wymagania funkcjonalne:

- Administrowanie siecią
- Usuwanie usterek/błędów
- Zarządzanie sprzętem sieciowym
- Testowanie sieci
- Zarządzanie routerami i przełącznikami
- Użytkownicy sieci posiadają dostęp do Internetu, drukarek i innych urządzeń sieciowych.

### **1.4. Wymagania niefunkcjonalne**

Wymagania niefunkcjonalne:

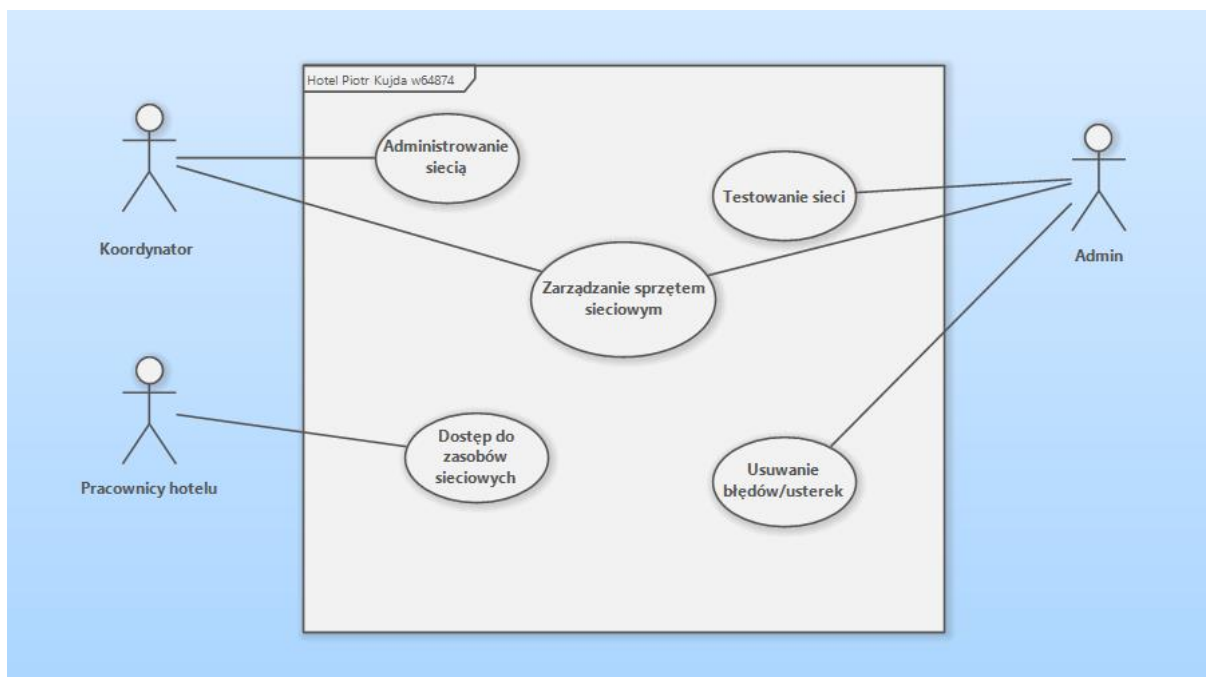
- Łatwy, bezinwazyjny dostęp do sieci
- Instalacja niezbędnych komponentów projektowanej sieci musi być wdrożona w sposób, który nie będzie uwidaczniał poszczególnych elementów oraz okablowania.

## **2. Diagramy UML**

Poniżej przedstawiamy diagram przypadków użycia dla sieci hotelowej. Diagram ten jest kluczowym elementem analizy systemowej i projektowania, który pomaga zrozumieć, jak różni użytkownicy lub "aktorzy" będą interaktować z proponowanym systemem sieciowym.

Diagram przypadków użycia jest graficznym przedstawieniem interakcji pomiędzy użytkownikami a systemem, które mają na celu osiągnięcie konkretnego celu. W kontekście sieci hotelowej, aktorami są różne role w hotelu, takie jak Koordynator, Pracownicy Hotelu i Admin, a przypadki użycia to różne zadania, które te role wykonują w ramach sieci, takie jak administrowanie siecią, zarządzanie sprzętem sieciowym, dostęp do zasobów sieciowych, testowanie sieci i usuwanie błędów/usterek.

Diagram przypadków użycia pomaga zrozumieć, jakie są główne funkcje systemu sieciowego i jakie są oczekiwania różnych użytkowników wobec systemu. Jest to niezbędne narzędzie do projektowania i wdrażania efektywnego i efektywnego systemu sieciowego, który spełnia wszystkie wymagania użytkowników.



Rysunek 1, Diagram przypadków użycia.

### Opis aktorów:

Aktor	Opis	Przypadki użycia
Koordynator	Koordynator jest odpowiedzialny za administrowanie siecią oraz zarządzanie sprzętem sieciowym. Administrowanie siecią obejmuje monitorowanie stanu sieci, konfigurację ustawień sieciowych, a także zarządzanie dostępem do sieci. Zarządzanie sprzętem sieciowym obejmuje monitorowanie stanu urządzeń sieciowych, takich jak routery, przełączniki i serwery, a także zarządzanie ich konfiguracją i utrzymaniem.	- PU Administrowanie siecią - PU Zarządzanie sprzętem sieciowym
Pracownicy hotelu	Pracownicy hotelu mają dostęp do zasobów sieciowych. Oznacza to, że mogą korzystać z usług sieciowych, takich jak dostęp do Internetu, drukowanie dokumentów za pomocą sieciowych drukarek, dostęp do sieciowych dysków twardych i innych zasobów.	- PU Dostęp do zasobów sieciowych
Admin	Admin ma trzy główne obowiązki: testowanie sieci, zarządzanie sprzętem sieciowym oraz usuwanie błędów/usterek. Testowanie sieci obejmuje przeprowadzanie regularnych testów wydajności i bezpieczeństwa sieci. Zarządzanie sprzętem sieciowym obejmuje monitorowanie i utrzymanie urządzeń sieciowych, takich jak routery, przełączniki i serwery. Usuwanie błędów/usterek obejmuje identyfikację i rozwiązywanie problemów z siecią i urządzeniami sieciowymi.	- PU Testowanie sieci - PU Zarządzanie sprzętem sieciowym - PU Usuwanie błędów/usterek

Tabela 1, Opis aktorów.

## **Przykłady scenariuszy definicji scenariuszy przypadków użycia gdzie:**

**PU – przypadek użycia, WS - warunki wstępne, WK - warunki końcowe.**

### **PU ADMINISTROWANIE SIECIĄ**

#### **OPIS**

**CEL:** ADMINISTROWANIE SIECIĄ

**WS:** może być wywołany przez Koordynatora lub Admina

**WK:** poprawne administrowanie siecią, w tym zarządzanie sprzętem sieciowym, konfiguracja sieci, zarządzanie ruterami i przełącznikami

#### **PRZEBIEG:**

Administrowanie siecią obejmuje zarządzanie sprzętem sieciowym, konfigurację sieci, zarządzanie ruterami i przełącznikami. Koordynator lub Admin musi mieć odpowiednie uprawnienia do wykonania tych zadań. Jeśli te zadania są wykonane poprawnie, sieć będzie działać prawidłowo.

### **PU DOSTĘP DO ZASOBÓW SIECIOWYCH**

#### **OPIS**

**CEL:** DOSTĘP DO ZASOBÓW SIECIOWYCH

**WS:** może być wywołany przez Pracowników Hotelu

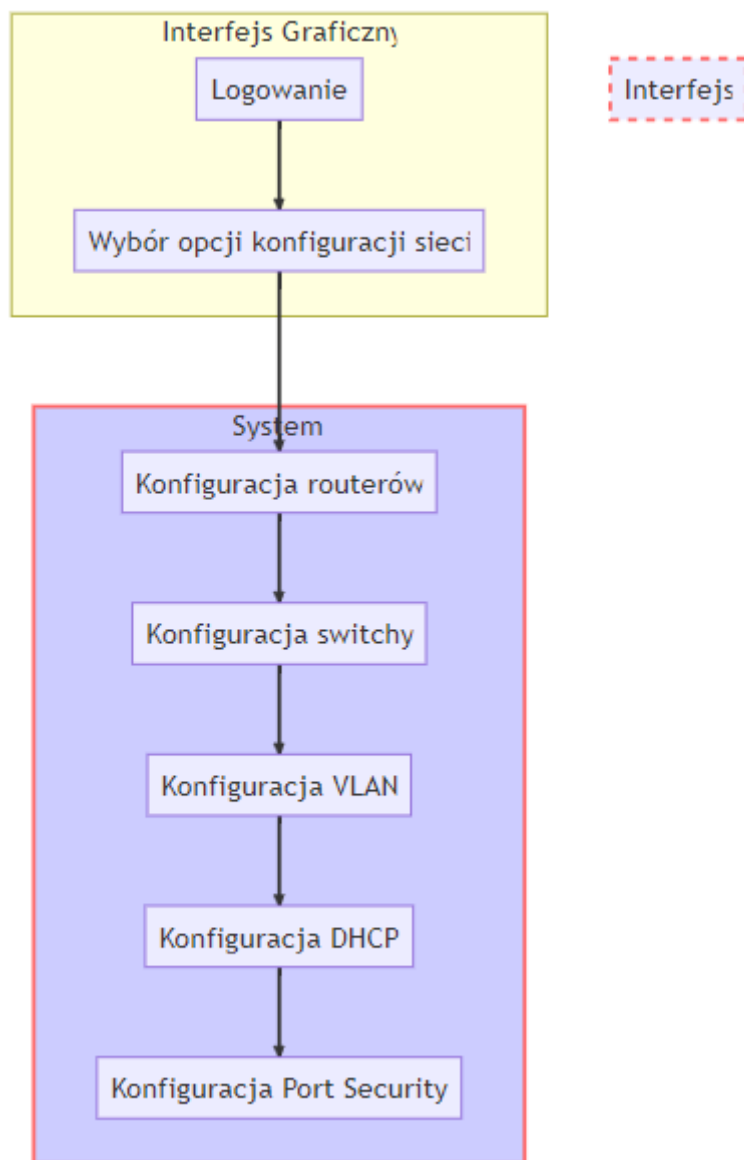
**WK:** poprawny dostęp do zasobów sieciowych, takich jak Internet, drukarki i inne urządzenia sieciowe

#### **PRZEBIEG:**

Dostęp do zasobów sieciowych obejmuje dostęp do Internetu, drukarek i innych urządzeń sieciowych. Pracownicy hotelu muszą mieć odpowiednie uprawnienia do korzystania z tych zasobów. Jeśli te zasoby są dostępne i działają prawidłowo, pracownicy będą mogli wykonywać swoje zadania efektywnie.

### 3. Diagramy aktywności

Poniżej znajduje się diagram aktywności, który ilustruje proces konfiguracji sieci w hotelu. Diagram jest podzielony na dwie części: Interfejs Graficzny i System.



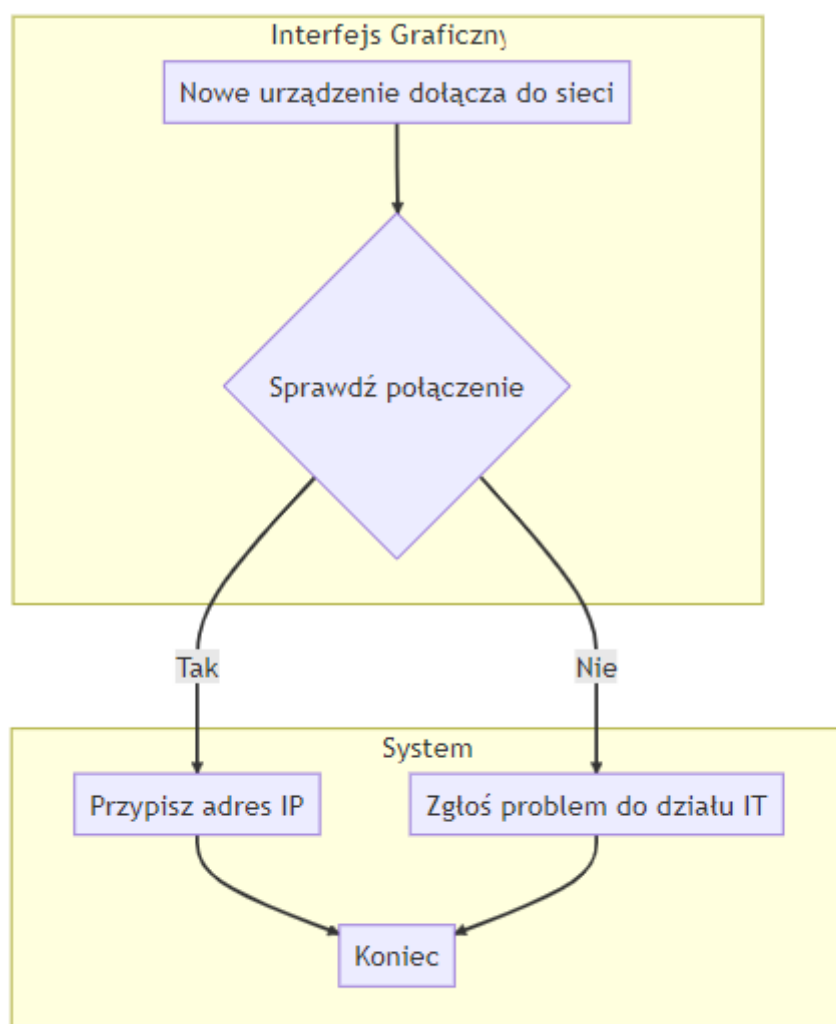
Rysunek 2, Proces konfiguracji sieci w hotelu.

Interfejs Graficzny obejmuje proces logowania i wyboru opcji konfiguracji sieci. Po zalogowaniu się, użytkownik ma możliwość wyboru opcji konfiguracji sieci.

System obejmuje szereg kroków konfiguracji sieci, takich jak konfiguracja routerów, konfiguracja switchy, konfiguracja VLAN, konfiguracja DHCP i konfiguracja Port Security. Każdy z tych kroków jest wykonywany po wyborze odpowiedniej opcji w interfejsie graficznym.



Poniżej znajduje się diagram aktywności, który ilustruje proces zarządzania siecią w hotelu. Diagram jest podzielony na dwie części: Interfejs Graficzny i System.

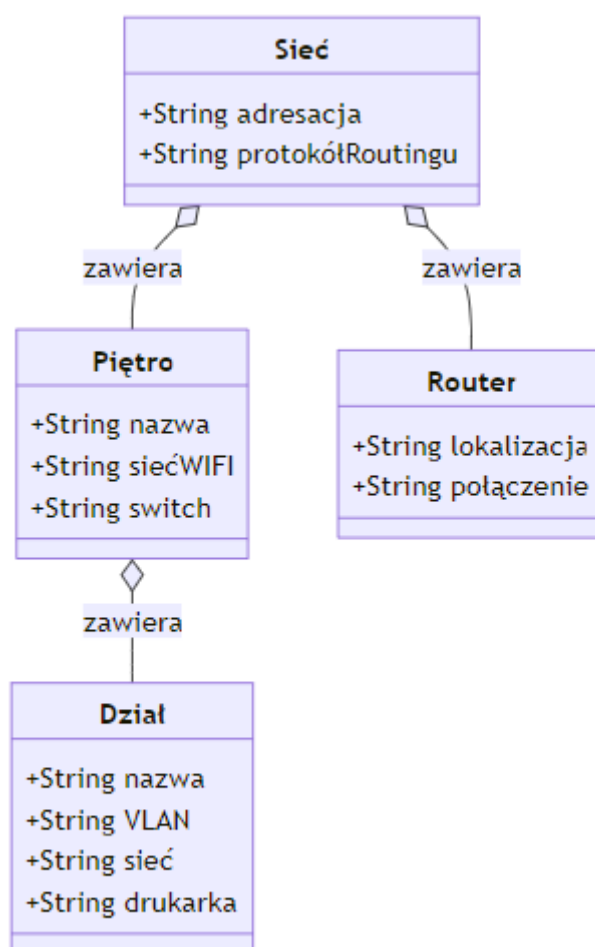


Rysunek 3, Proces zarządzania siecią w hotelu.

Diagram rozpoczyna się od momentu, gdy nowe urządzenie dołącza do sieci hotelowej. Następnie system sprawdza, czy połączenie z urządzeniem jest prawidłowe. Jeśli tak, system przypisuje urządzeniu adres IP, kończąc tym samym proces. Jeśli połączenie nie jest prawidłowe, system zgłasza problem do działu IT, który następnie podejmuje odpowiednie kroki w celu rozwiązania problemu.

#### 4. Diagram klas

Diagram klas przedstawia strukturę sieci hotelu.



Rysunek 4, Struktura sieci hotelu.

Klasa "Sieć" reprezentuje całą sieć hotelu, zawierającą informacje o adresacji sieci i używanym protokole routing. Sieć składa się z obiektów klas "Piętro" i "Router".

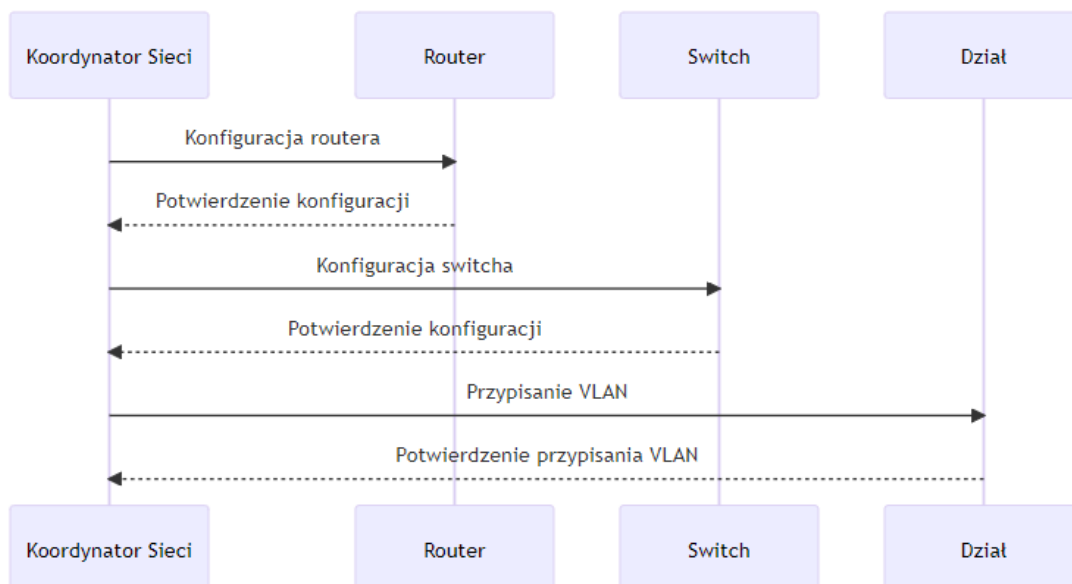
Klasa "Piętro" reprezentuje poszczególne piętra w hotelu, zawierając informacje o nazwie piętra, sieci WIFI i switchu na danym piętrze. Każde piętro składa się z obiektów klasy "Dział".

Klasa "Dział" reprezentuje poszczególne działy na danym piętrze, zawierając informacje o nazwie działu, VLAN, sieci i drukarce w danym dziale.

Klasa "Router" reprezentuje routery w sieci, zawierając informacje o lokalizacji routera i typie połączenia.

## 5. Diagramy sekwencji

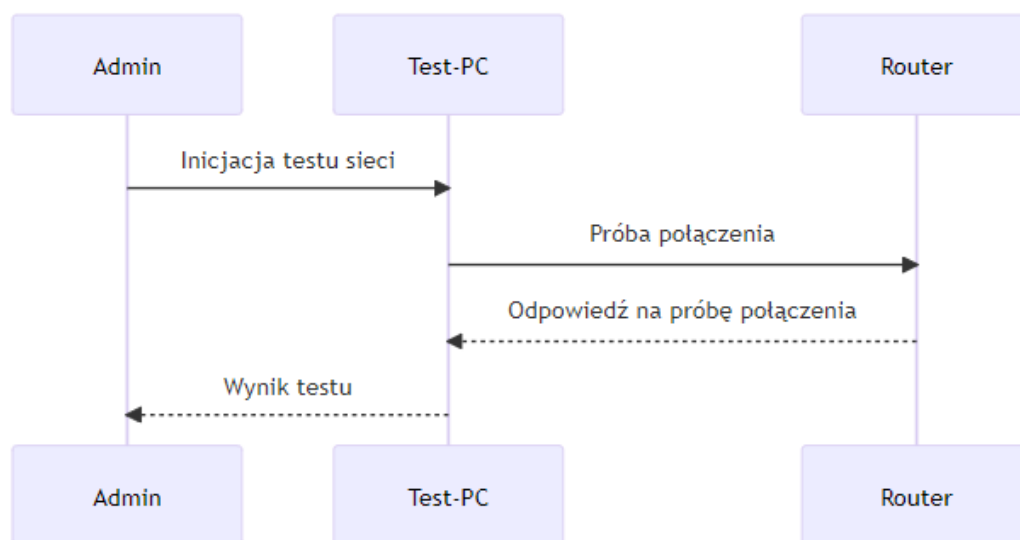
Pierwszy diagram sekwencji przedstawia proces konfiguracji sieci w hotelu. W tym procesie uczestniczą: Koordynator Sieci, Router, Switch oraz poszczególne Działy hotelu.



Rysunek 5, Proces konfiguracji sieci w hotelu.

Proces rozpoczyna się od konfiguracji routera przez Koordynatora Sieci. Po zakończeniu konfiguracji, Router wysyła potwierdzenie do Koordynatora. Następnie Koordynator przystępuje do konfiguracji switcha. Po zakończeniu konfiguracji, Switch wysyła potwierdzenie do Koordynatora. Na koniec, Koordynator przypisuje VLAN do poszczególnych Działów hotelu, które potwierdzają przypisanie VLAN.

Drugi diagram sekwencji przedstawia proces testowania sieci w hotelu. W tym procesie uczestniczą: Admin, Test-PC oraz Router.

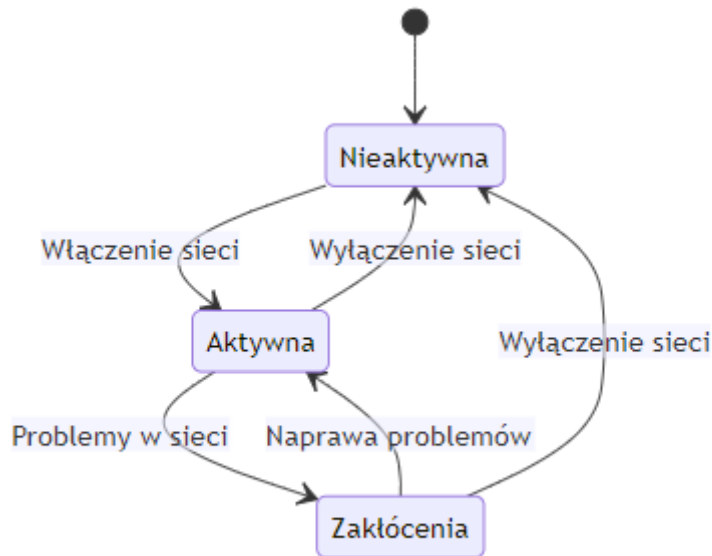


Rysunek 6, Proces testowania sieci w hotelu

Proces rozpoczyna się od inicjacji testu sieci przez Admina. Test-PC próbuje nawiązać połączenie z Routerem. Router odpowiada na próbę połączenia, a Test-PC przekazuje wynik testu do Admina.

## 6. Diagram stanów

Diagram stanów przedstawia różne stany, w których może znajdować się sieć hotelowa.



Rysunek 7, Stany sieci hotelowej.

Sieć może znajdować się w jednym z trzech stanów: Nieaktywna, Aktywna lub Zakłócenia.

- Stan "Nieaktywna" oznacza, że sieć jest wyłączona i nie jest dostępna dla użytkowników.
- Stan "Aktywna" oznacza, że sieć jest włączona i dostępna dla użytkowników.
- Stan "Zakłócenia" oznacza, że wystąpiły problemy w sieci, które wpływają na jej działanie.

Przejścia między stanami są następujące:

- Z stanu "Nieaktywna" do stanu "Aktywna" następuje, gdy sieć jest włączana.
- Z stanu "Aktywna" do stanu "Nieaktywna" następuje, gdy sieć jest wyłączana.
- Z stanu "Aktywna" do stanu "Zakłócenia" następuje, gdy wystąpią problemy w sieci.
- Z stanu "Zakłócenia" do stanu "Aktywna" następuje, gdy problemy w sieci zostaną naprawione.
- Z stanu "Zakłócenia" do stanu "Nieaktywna" następuje, gdy sieć jest wyłączana pomimo występujących problemów.

## **7. Harmonogram Prac Projektu**

### *1. Analiza Wymagań (2 tygodnie)*

- Zdefiniowanie wymagań funkcjonalnych i niefunkcjonalnych
- Zidentyfikowanie aktorów i przypadków użycia
- Analiza kosztów i dostępnych rozwiązań

### *2. Projekt Sieci (3 tygodnie)*

- Wybór i zakup odpowiednich urządzeń sieciowych (routery, przełączniki, access points)
- Określenie topologii sieci
- Przydzielanie adresów IP i konfiguracja podsieci
- Opracowanie planu bezpieczeństwa sieciowego

### *3. Konfiguracja Sprzętu Sieciowego (4 tygodnie)*

- Instalacja i konfiguracja routerów, przełączników i punktów dostępowych
- Utworzenie VLAN-ów i przypisanie portów do odpowiednich VLAN-ów
- Konfiguracja serwera DHCP i serwera DNS
- Wdrożenie zabezpieczeń, takich jak firewall i VPN

### *4. Testy i Optymalizacja (3 tygodnie)*

- Testowanie wydajności sieci
- Testy bezpieczeństwa sieciowego
- Optymalizacja konfiguracji sieciowej
- Rozwiązywanie ewentualnych problemów

### *5. Wdrożenie i Szkolenia (2 tygodnie)*

- Przeszkolenie personelu hotelu w zakresie korzystania z sieci
- Przeniesienie sieci do środowiska produkcyjnego
- Konfiguracja kopii zapasowych i monitorowanie sieci

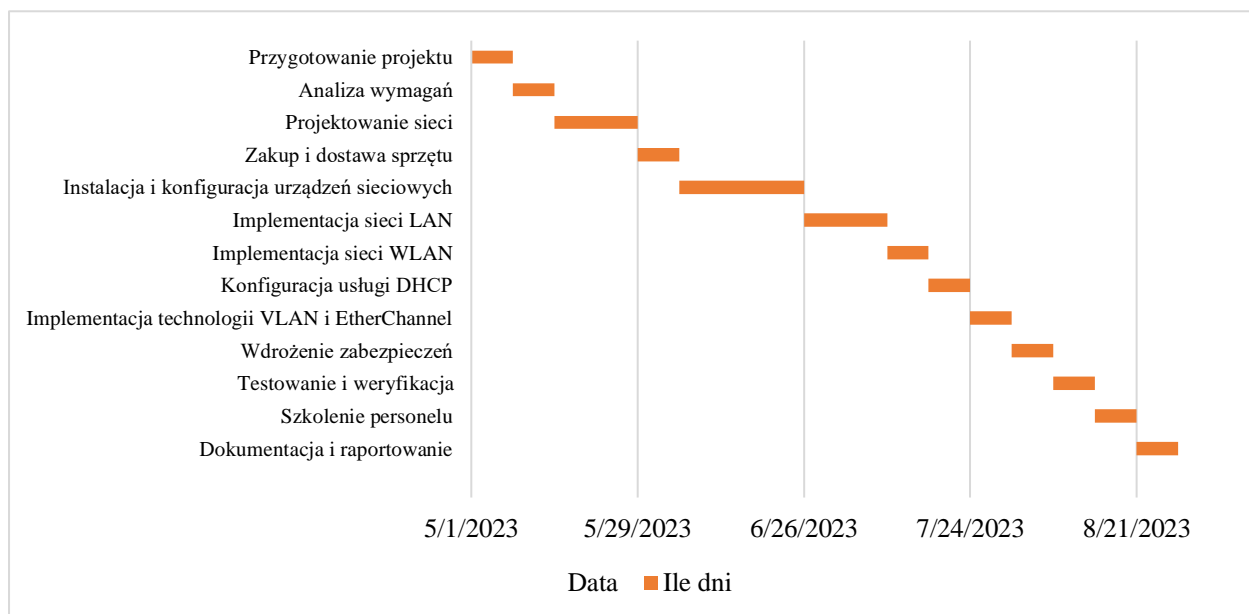
### *6. Monitorowanie i Utrzymanie (trwające przez cały okres eksploatacji)*

- Regularne monitorowanie sieci i urządzeń sieciowych
- Aktualizacje oprogramowania i zabezpieczeń
- Reagowanie na awarie i problemy
- Zapewnienie ciągłości działania i utrzymanie bezpieczeństwa sieci

### 7. Testy Użyteczności (1 tydzień, po wprowadzeniu do produkcji)

- Przeprowadzenie testów użyteczności z udziałem pracowników hotelu
- Zebranie opinii i informacji zwrotnych od użytkowników
- Dostosowanie systemu na podstawie wyników testów

Poniżej zamieszczono harmonogram realizacji projektu.



Rys. 1 Diagram Gantta

## 8. Koncepcja systemu oraz wybór środowiska programistycznego i rozwiązań

Koncepcja projektu sieci komputerowej opiera się na dostosowaniu rozwiązania do indywidualnych potrzeb hotelu, uwzględniając obecny stan zapotrzebowania oraz gotowość do przyszłego rozwoju infrastruktury sieciowej. W celu realizacji projektu wybrano starannie dostosowane narzędzia i rozwiązania, które zapewnią nie tylko niezawodność, ale także skalowalność i bezpieczeństwo sieci.

### 1. Wybór Środowiska Programistycznego:

- W celu symulacji i konfiguracji sieci komputerowej dla hotelu, zdecydowano się na wykorzystanie narzędzia "Cisco Packet Tracer". To zaawansowane oprogramowanie umożliwi dokładne modelowanie sieci, co pozwoli na przetestowanie i zoptymalizowanie konfiguracji przed wdrożeniem w rzeczywistym środowisku.

### 2. Wybór Rozwiązań Sieciowych:

- Wybór urządzeń sieciowych marki Cisco jest kluczowy, ponieważ zapewniają one wysoką jakość, niezawodność oraz możliwość rozbudowy sieci w przyszłości. W projekcie zakłada się wykorzystanie urządzeń takich jak routery, przełączniki i access pointy marki Cisco.

### *3. Konfiguracja Infrastruktury Sieciowej:*

- Sieć zostanie podzielona na wiele segmentów, w tym sieć LAN i WLAN, aby zaspokoić różnorodne potrzeby użytkowników w hotelu.
- Technologie takie jak VLAN, routing, EtherChannel i DHCP zostaną wdrożone, aby zapewnić elastyczność i efektywność sieci.
- Bezpieczeństwo sieci zostanie zapewnione poprzez odpowiednie konfiguracje VLAN, kontrolę dostępu do sieci oraz wyłączenie nieużywanych portów na przełącznikach.

### *4. Sieć Bezprzewodowa (WLAN):*

- Dla zapewnienia dostępu do Internetu i innych zasobów sieciowych z dowolnego miejsca w hotelu, zostanie zainstalowany access point, który umożliwi łączność urządzeń bezprzewodowych.
- Access point zostanie podłączony do odpowiedniego przełącznika w sieci, zapewniając dostęp do sieci WLAN.

### *5. Połączenie Między Budynkami:*

- W przypadku, gdy sieć obejmuje kilka budynków, zostanie zastosowany odpowiedni router główny, który umożliwi łączność między nimi.
- Segmentacja sieci VLAN pozwoli na dokładne zarządzanie dostępem do zasobów sieciowych w różnych częściach hotelu.

### *6. Bezpieczeństwo Sieci:*

- W celu zapewnienia bezpieczeństwa sieci zostaną wdrożone odpowiednie mechanizmy, takie jak kontrola dostępu, firewall oraz wyłączanie nieużywanych portów.
- Dla zwiększenia ochrony danych użytkowników oraz zapobiegania nieautoryzowanym dostępom, sieć zostanie dokładnie zabezpieczona.

### *7. Monitoring i Zarządzanie Siecią:*

- W ramach projektu zostanie wprowadzone narzędzie do monitorowania i zarządzania siecią, umożliwiające ciągłą kontrolę nad jej działaniem i wydajnością.

### *8. Automatyzacja Procesów:*

- W celu zwiększenia efektywności zarządzania siecią, zostaną wdrożone narzędzia do automatyzacji procesów, takie jak konfiguracja urządzeń sieciowych, wdrażanie aktualizacji oraz generowanie raportów.

Projekt zakłada dostarczenie kompleksowego rozwiązania sieciowego, które sprosta potrzebom hotelu, zarówno obecnie, jak i w przyszłości. Wdrożenie Cisco Packet Tracer oraz urządzeń sieciowych marki Cisco pozwoli na stworzenie wydajnej, niezawodnej i bezpiecznej infrastruktury sieciowej dla hotelu, zaspokajając potrzeby zarówno personelu hotelowego, jak i gości.



Tabela urządzeń dla piętra 1:

Urządzenie	Interfejs	IP	Maska podsieci	Brama
F1-Router	Serial0/2/0	10.10.10.5	255.255.255.252	-
F1-Router	Serial0/2/1	10.10.10.9	255.255.255.252	-
F1-Switch	-	-	-	-
Laptop1	Wireless	(DHCP) 192.168.6.6	255.255.255.0	192.168.6.1
Tablet PC1	Wireless	(DHCP) 192.168.6.4	255.255.255.0	192.168.6.1
Smartphone1	Wireless	(DHCP) 192.168.6.3	255.255.255.0	192.168.6.1
F1-Access-Point	-	-	-	-
PC2	FE	(DHCP) 192.168.8.2	255.255.255.0	192.168.8.1
Printer2	FE	(DHCP) 192.168.8.3	255.255.255.0	-
PC1	FE	(DHCP) 192.168.7.2	255.255.255.0	192.168.7.1
Printer1	FE	(DHCP) 192.168.7.3	255.255.255.0	-
PC0	FE	(DHCP) 192.168.6.2	255.255.255.0	192.168.6.1
Printer0	FE	(DHCP) 192.168.6.5	255.255.255.0	-

Tabela 2, Tabela urządzeń 1 piętro.

Tabela urządzeń dla piętra 2:

Urządzenie	Interfejs	IP	Maska podsieci	Brama
F2-Router	Serial0/1/0	10.10.10.1	255.255.255.252	-
F2-Router	Serial0/1/1	10.10.10.10	255.255.255.252	-
F2-Switch	-	-	-	-
Laptop0	Wireless	(DHCP) 192.168.3.6	255.255.255.0	192.168.3.1
Tablet PC0	Wireless	(DHCP) 192.168.3.5	255.255.255.0	192.168.3.1
Smartphone0	Wireless	(DHCP) 192.168.3.2	255.255.255.0	192.168.3.1
F2-Access-Point	-	-	-	-
PC5	FE	(DHCP) 192.168.3.4	255.255.255.0	192.168.3.1
Printer5	FE	(DHCP) 193.168.3.3	255.255.255.0	-
PC4	FE	(DHCP) 192.168.4.3	255.255.255.0	192.168.4.1
Printer4	FE	(DHCP) 192.168.4.2	255.255.255.0	-

PC3	FE	(DHCP) 192.168.5.3	255.255.255.0	192.168.5.1
Printer3	FE	(DHCP) 192.168.5.2	255.255.255.0	-

Tabela 3, Tabela urządzeń 2 piętro

Tabela urządzeń dla piętra 3:

Urządzenie	Interfejs	IP	Maska podsieci	Brama
F3-Router	Serial0/2/0	10.10.10.6	255.255.255.252	-
F3-Router	Serial0/2/1	10.10.10.2	255.255.255.252	-
F3-Switch	-	-	-	-
F3-Access-Point	-	-	-	-
TEST-PC	FE	(DHCP) 192.168.1.2	255.255.255.0	192.168.1.1
Printer6	FE	(DHCP) 192.168.1.3	255.255.255.0	-
PC7	FE	(DHCP) 192.168.2.2	255.255.255.0	192.168.2.1
Printer7	FE	(DHCP) 192.168.2.3	255.255.255.0	-

Tabela 4, Tabela urządzeń 3 piętro

Tabela VLAN dla piętra 1:

VLAN	Nazwa	Przypisane interfejsy
60 – Logistyka	VLAN0060	FE0/6-8
70 – Magazyn	VLAN0070	FE0/4-5
80 – Recepcja	VLAN0080	FE0/2-3

Tabela 5, Tabela VLAN 1 Piętro

Tabela VLAN dla piętra 2:

VLAN	Nazwa	Przypisane interfejsy
30 – Sprzedaż	VLAN0030	FE0/6-8
40 – HR	VLAN0040	FE0/4-5
50 – Finanse	VLAN0050	FE0/2-3

Tabela 6, Tabela VLAN 2 Piętro

Tabela VLAN dla piętra 3:

VLAN	Nazwa	Przypisane interfejsy
10 – IT	VLAN0010	FE0/2-3
20 – Administracja	VLAN0020	FE0/4-6

Tabela 7, Tabela VLAN 3 Piętro

Koncepcja projektu sieci hotelowej opiera się na stworzeniu rozwiązań dostosowanych do potrzeb hotelu, uwzględniając zarówno obecne zapotrzebowanie, jak i elastyczność dla przyszłego rozwoju infrastruktury sieciowej. Poniżej przedstawiamy wybrane technologie oraz narzędzia, które będą kluczowe dla projektu sieci hotelowej.

#### *1. VLAN (Virtual LAN):*

- W ramach projektu zostaną utworzone multiple Vlany, co pozwoli na stworzenie wielu oddzielnych sieci logicznych w ramach jednej sieci fizycznej.
- VLANy pozwalają na segregację ruchu i umożliwiają dostęp tylko do odpowiednich zasobów sieciowych dla różnych grup użytkowników, takich jak pracownicy hotelu, goście oraz administracja.

#### *2. EtherChannel:*

- Technologia EtherChannel pozwoli na efektywne wykorzystanie kilku łączy Ethernet do tworzenia jednego logicznego połączenia.
- Dzięki temu możliwe będzie równomierne rozłożenie obciążenia i zapewnienie niezawodności połączenia.

#### *3. DHCP (Dynamic Host Configuration Protocol):*

- Protokół DHCP zostanie wykorzystany do dynamicznego przydzielania adresów IP oraz innych ustawień, takich jak maska podsieci, brama domyślna i serwer DNS, dla urządzeń podłączonych do sieci hotelowej.
- To umożliwi gościom i pracownikom łatwe i automatyczne uzyskanie dostępu do sieci bez konieczności ręcznej konfiguracji.

#### *4. WLAN (Wireless Local Area Network):*

- Sieć bezprzewodowa WLAN zostanie stworzona w hotelu, co umożliwi urządzeniom z obsługą technologii Wi-Fi bezprzewodowe połączenie z siecią.
- Dla wygody gości, obszary z dostępem do sieci bezprzewodowej zostaną wyznaczone przez administratorów, umożliwiając korzystanie z urządzeń mobilnych w różnych częściach hotelu.

#### *5. Role Użytkowników:*

- W ramach projektu przewiduje się dwie główne role użytkowników: administratorów sieci oraz użytkowników i gości.
- Administratorzy sieci będą odpowiedzialni za zarządzanie siecią, jej bezpieczeństwo oraz rozwój infrastruktury sieciowej.
- Użytkownicy i goście będą mieli dostęp do sieci za pomocą połączenia przewodowego (kablem RJ45) oraz technologii Wi-Fi w wyznaczonych obszarach.

## 6. Segmentacja Sieci:

- Dzięki zastosowaniu technologii VLAN oraz routingu, możliwe będzie stworzenie bezpiecznej i skalowalnej sieci, gdzie użytkownicy i goście nie będą mieli dostępu do zasobów firmy, z wyjątkiem tych, do których zostali uprawnieni.

## 7. Bezpieczeństwo Sieci:

- W projekcie zostaną wprowadzone odpowiednie mechanizmy zabezpieczeń sieciowych, takie jak kontrola dostępu oraz zabezpieczenia przed nieautoryzowanymi dostęпами.
- Bezpieczeństwo sieci jest kluczowe, aby chronić dane gości oraz zapewnić stabilność sieci.

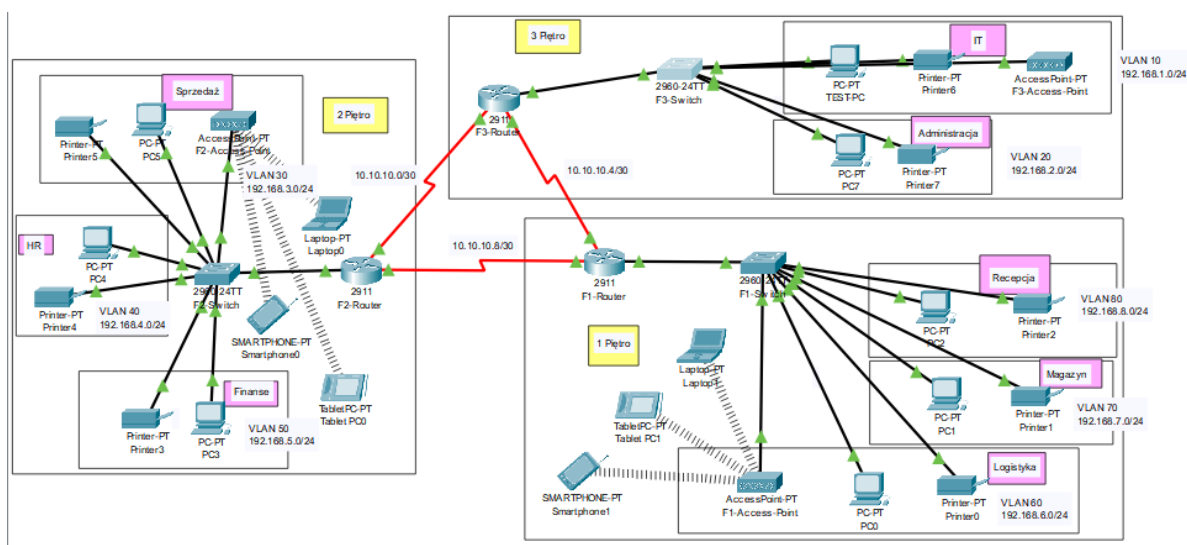
## 8. Narzędzie Symulacyjne:

- Do stworzenia, testowania i optymalizacji projektu sieci hotelowej zostanie wykorzystane narzędzie "Cisco Packet Tracer", które pozwoli na dokładną symulację rozwiązań i konfiguracji sieci przed wdrożeniem.

Projekt zakłada dostarczenie kompleksowego rozwiązania sieciowego, które sprostą potrzebom hotelu, zapewni gościom wygodny dostęp do sieci, a jednocześnie zabezpieczy sieć firmy oraz umożliwi jej rozwój w przyszłości. Wybór technologii i narzędzi, takich jak VLAN, EtherChannel, DHCP i WLAN, ma na celu stworzenie efektywnej i bezpiecznej infrastruktury sieciowej dostosowanej do specyficznych potrzeb hotelowej działalności.

## 9. Testy jednostkowe

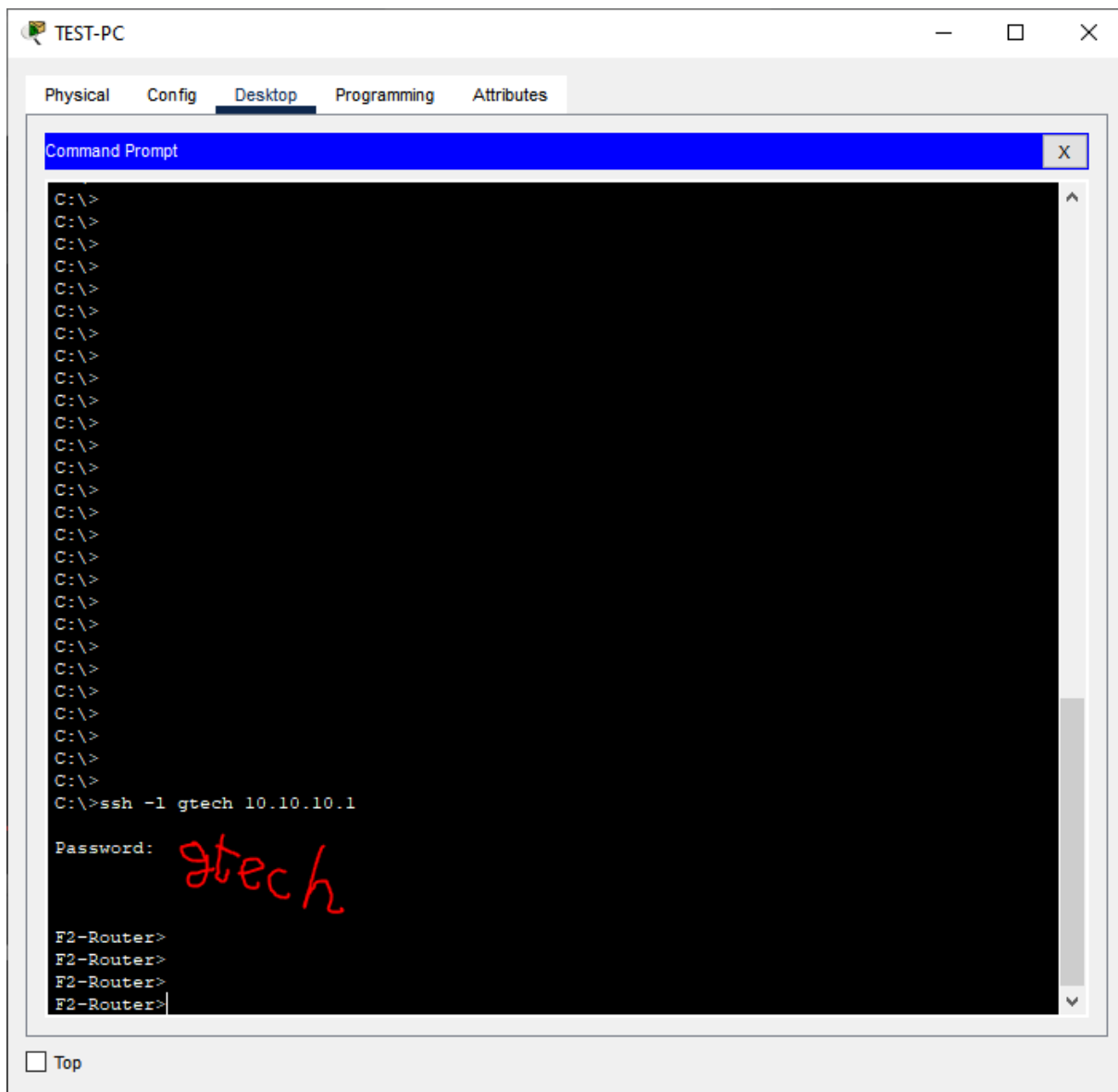
Testy jednostkowe są niezwykle ważnym aspektem projektów informatycznych, w tym projektów sieciowych. Pomagają one w weryfikacji poprawności działania poszczególnych komponentów i funkcji systemu.



Rysunek 8, Wizualizacja sieci komputerowej w programie Cisco Packet Tracer.

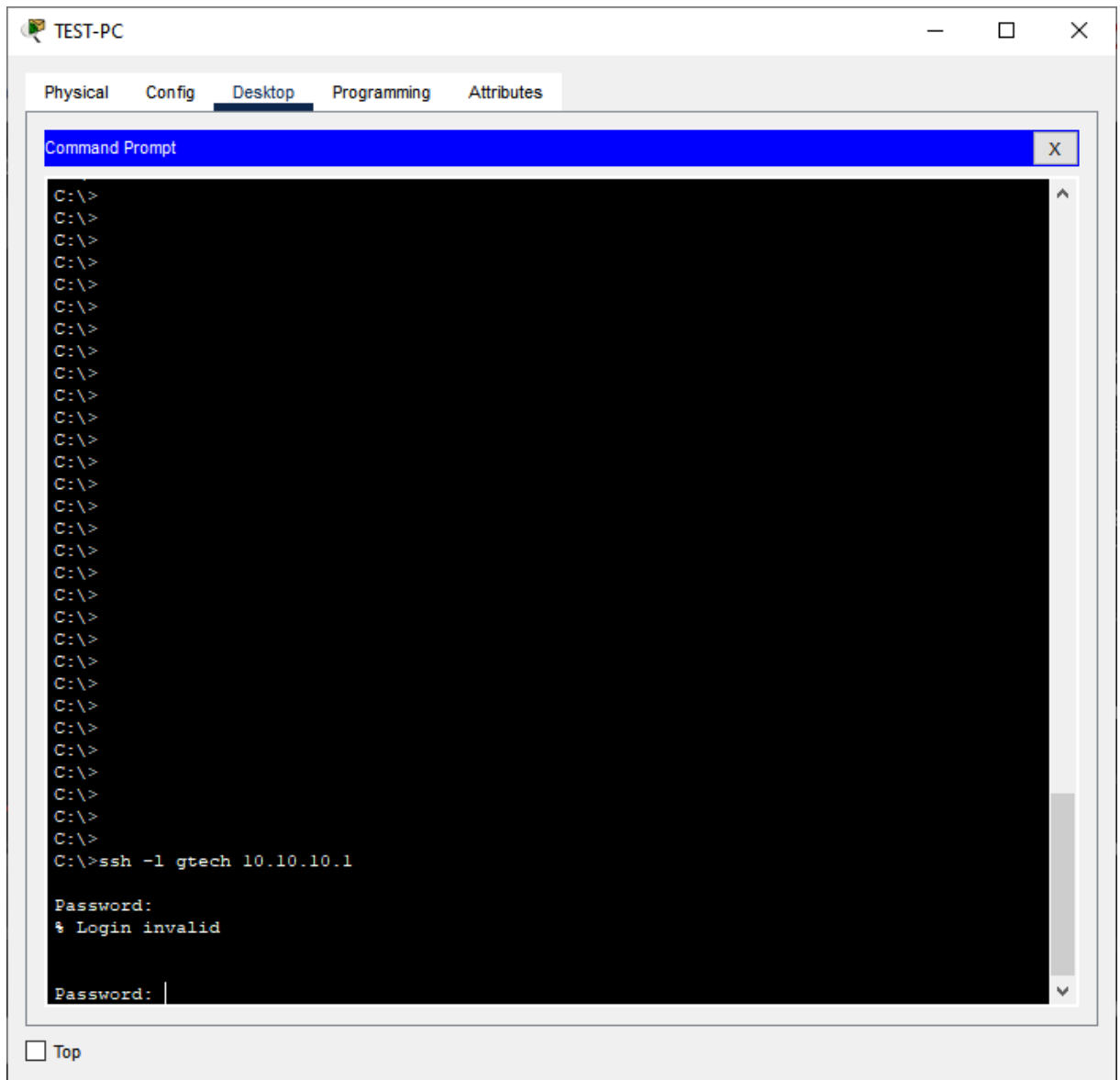
## Test jednostkowy 1: Weryfikacja logowania i autoryzacji użytkowników

- Cel: Upewnienie się, że proces logowania i autoryzacji użytkowników działa poprawnie.
- Krok 1: Test na poprawność logowania - Spróbuj zalogować się na konto użytkownika, podając poprawne dane uwierzytelniające. Upewnij się, że logowanie jest udane.



Rysunek 9, Test na poprawność logowania .

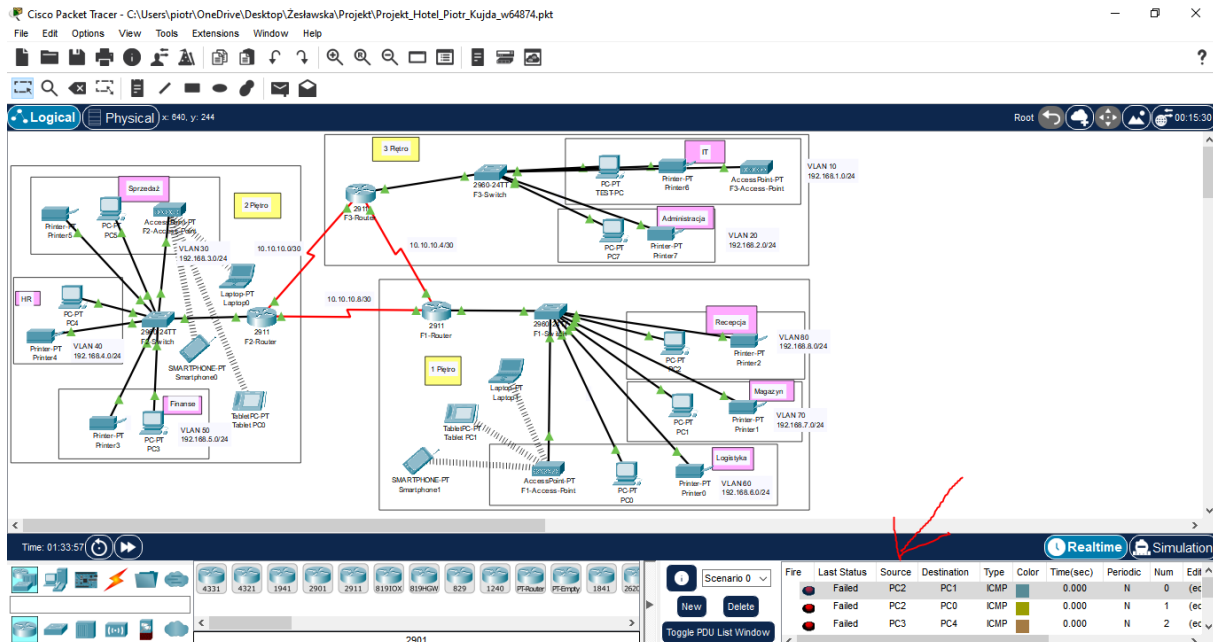
- Krok 2: Test na nieprawidłowe dane logowania - Spróbuj zalogować się na konto użytkownika, podając nieprawidłowe dane uwierzytelniające. Upewnij się, że system wyświetla odpowiedni komunikat o błędzie.



Rysunek 10, Test na nieprawidłowe dane logowania.

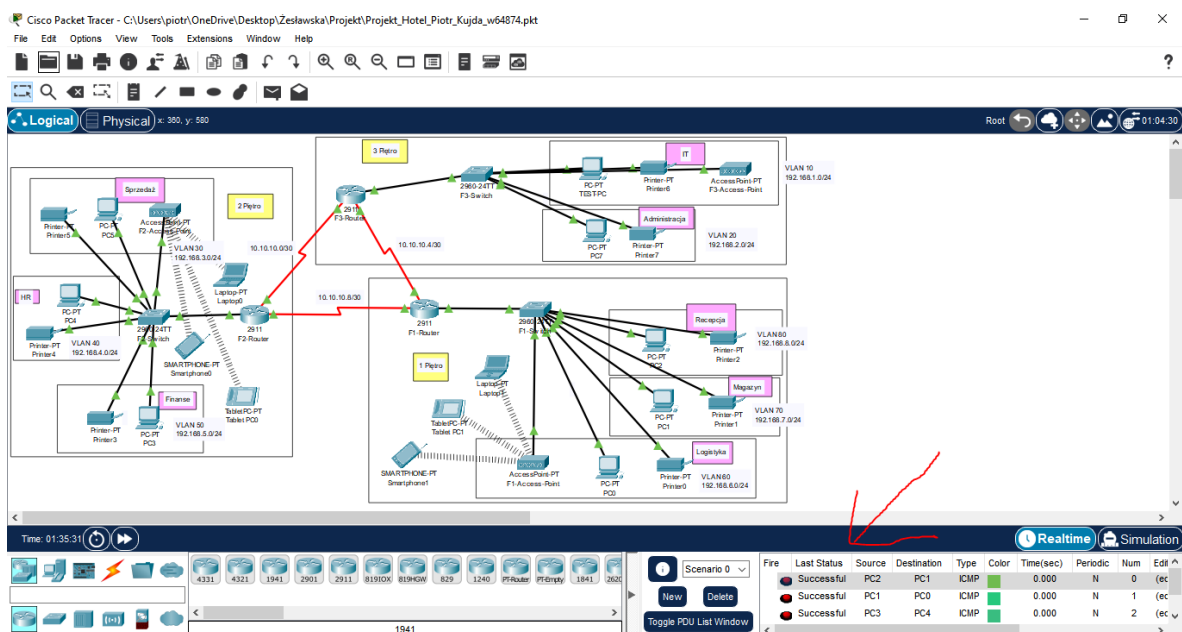
## Test jednostkowy 2: Weryfikacja konfiguracji VLAN

- Cel: Upewnienie się, że konfiguracja VLAN działa poprawnie.
- Krok 1: Test na izolację VLAN - Upewnij się, że urządzenia w jednym VLANie nie mogą komunikować się z urządzeniami w innym VLANie.



Rysunek 11, Test na izolację VLAN.

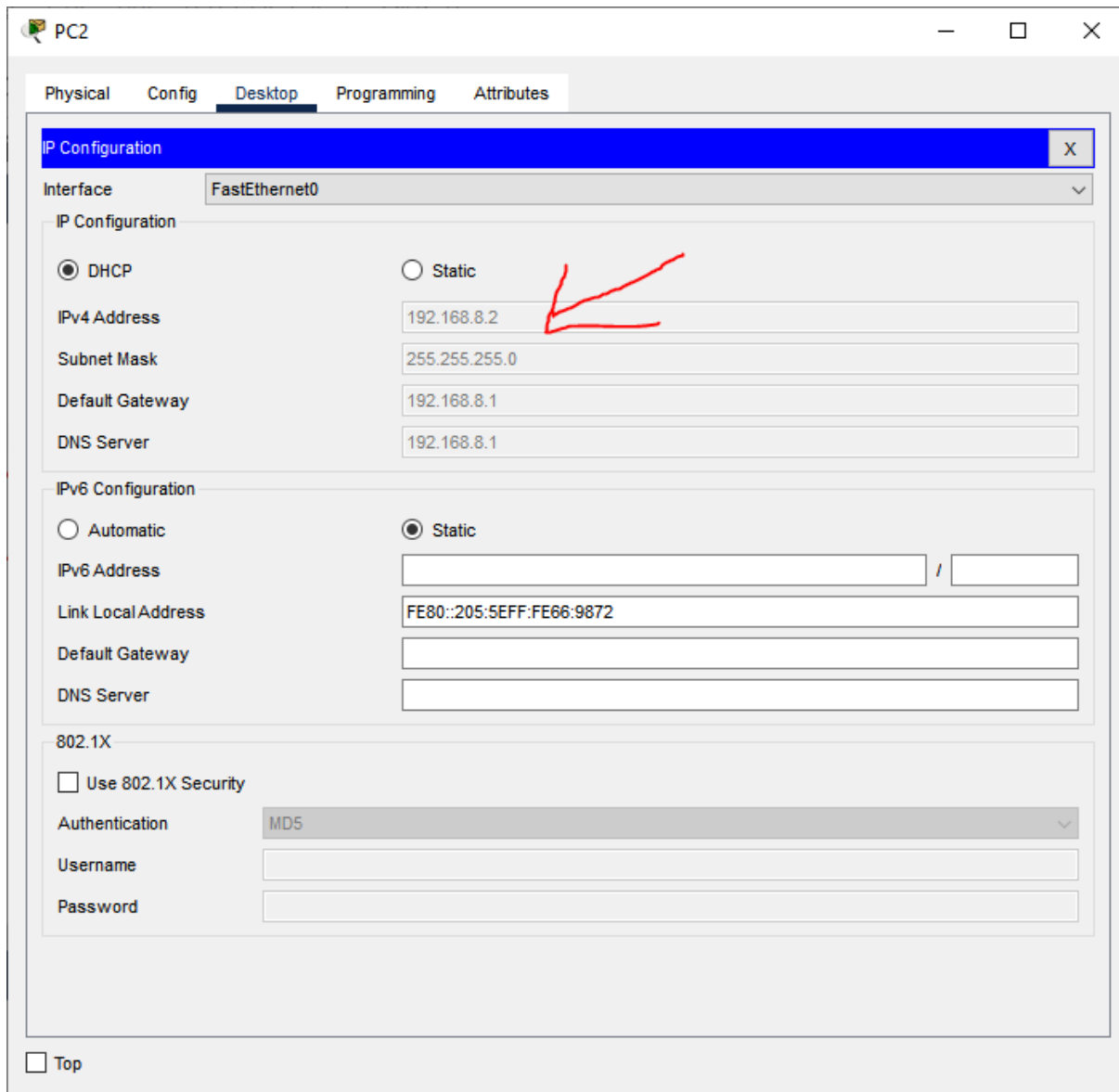
- Krok 2: Test na konfigurację routingu między VLANami - Sprawdź, czy routery pozwalają na komunikację między wybranymi VLANami.



Rysunek 12, Test na konfigurację routingu między VLANami.

### Test jednostkowy 3: Weryfikacja konfiguracji DHCP

- Cel: Upewnienie się, że serwer DHCP przypisuje poprawne adresy IP klientom.
- Krok 1: Test przydzielenia adresu IP - Podłącz nowe urządzenie do sieci i sprawdź, czy serwer DHCP przydzieli mu poprawny adres IP.



The screenshot shows the configuration window for PC2, specifically the 'Desktop' tab. The 'IP Configuration' section is active, showing settings for the 'FastEthernet0' interface. The 'DHCP' option is selected, and the 'Static' option is also visible. A red arrow points to the 'Static' option. The IPv4 Address is set to 192.168.8.2, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.8.1, and DNS Server is 192.168.8.1. The IPv6 Configuration section shows 'Static' selected, with IPv6 Address, Link Local Address (FE80::205:5EFF:FE66:9872), Default Gateway, and DNS Server fields. The 802.1X section shows 'Use 802.1X Security' unchecked, Authentication set to MD5, and Username and Password fields.

PC2

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 192.168.8.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.8.1

DNS Server 192.168.8.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::205:5EFF:FE66:9872

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

Password

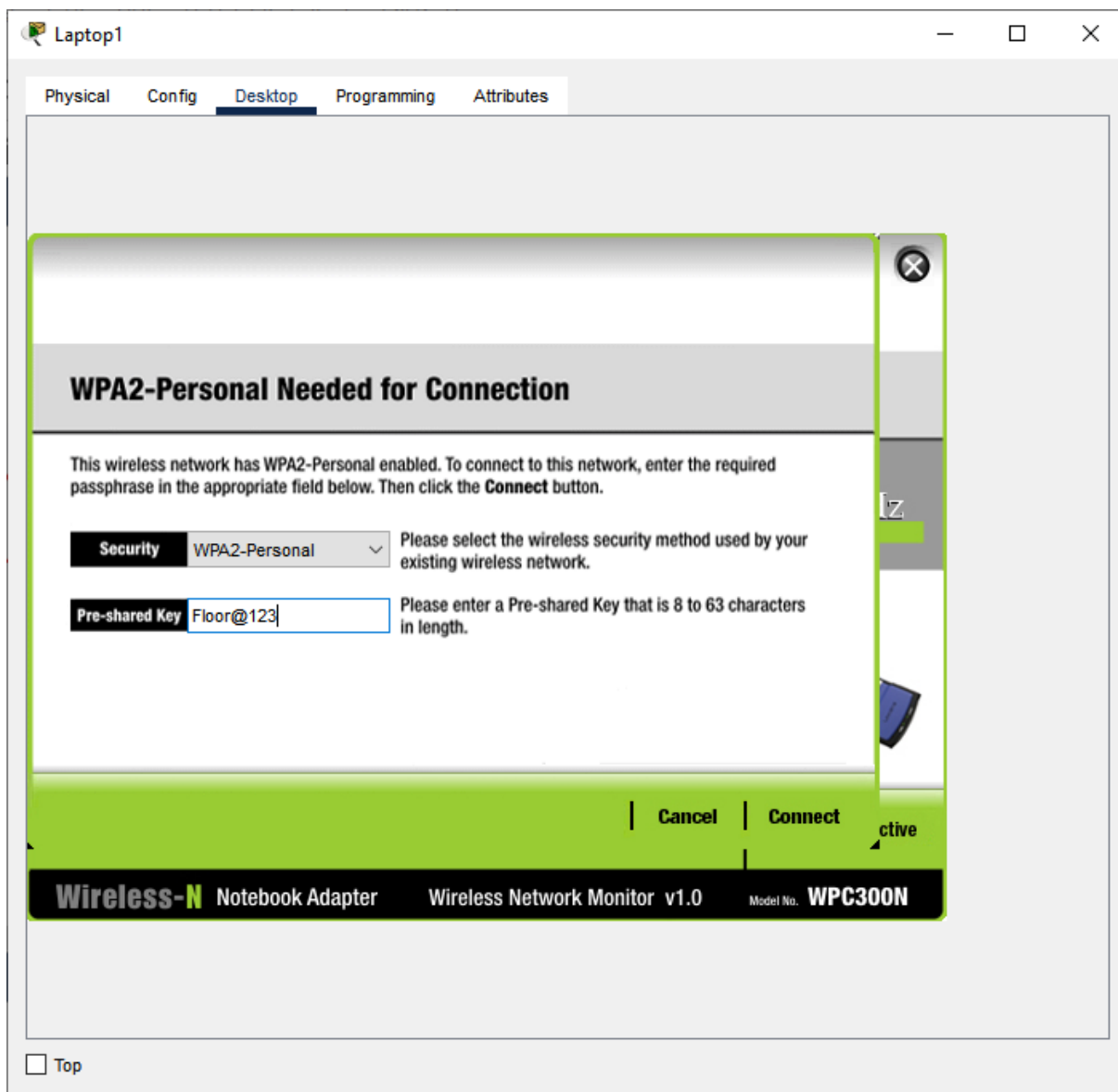
☐ Top

Rysunek 13, Test przydzielenia adresu IP.

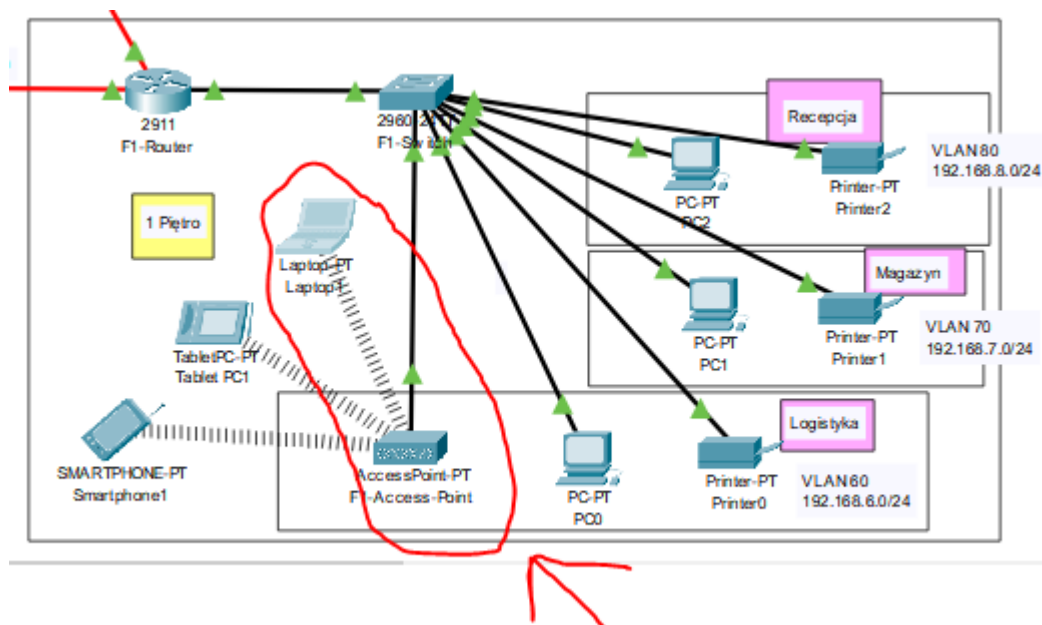


#### Test jednostkowy 4: Weryfikacja konfiguracji bezprzewodowej sieci LAN (WLAN)

- Cel: Upewnienie się, że sieć WLAN działa poprawnie i jest zabezpieczona.
- Krok 1: Test połączenia bezprzewodowego - Spróbuj połączyć się z siecią WLAN przy użyciu prawidłowego klucza dostępu.

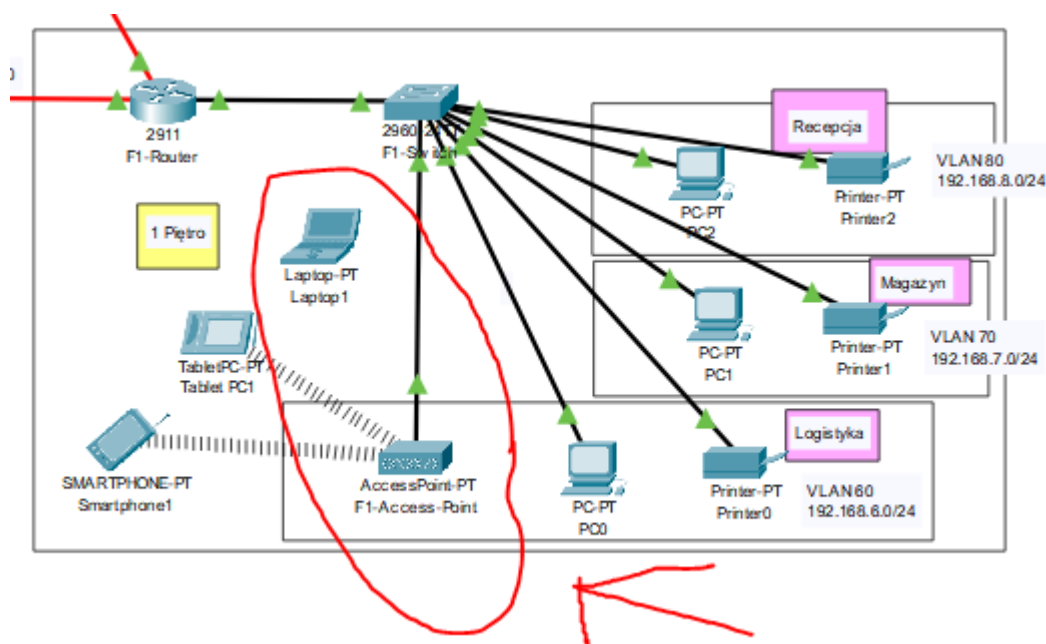


Rysunek 14, Test połączenia bezprzewodowego.



Rysunek 15, Test połączenia bezprzewodowego.

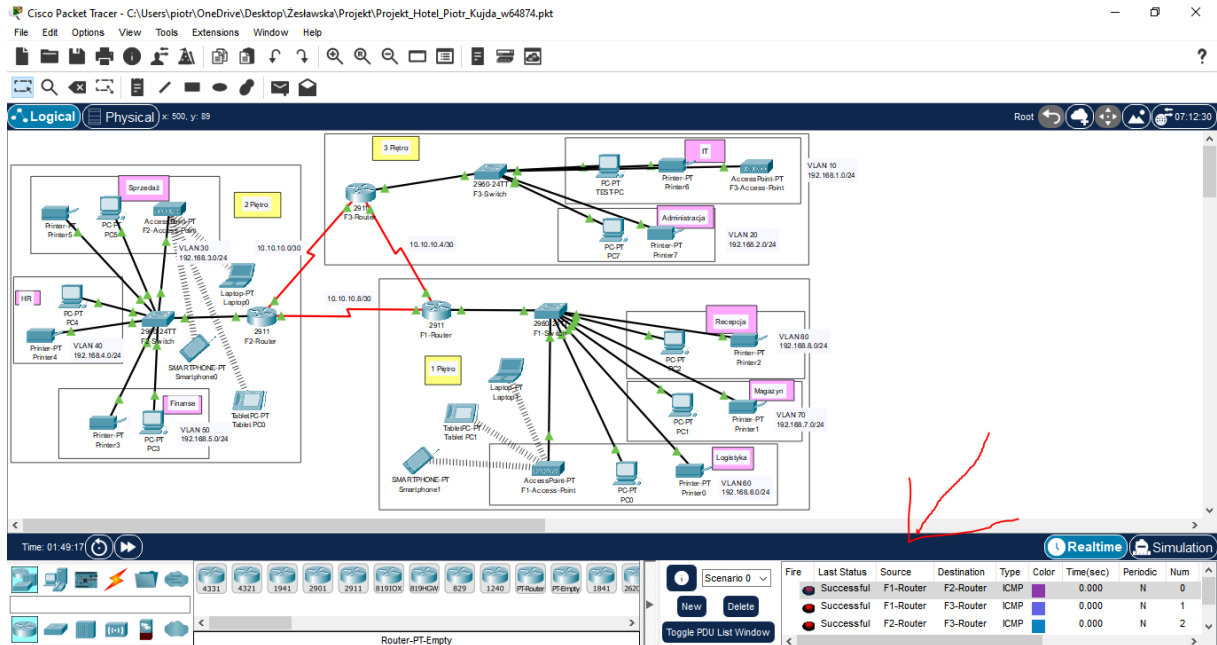
- Krok 2: Test nieautoryzowanego dostępu - Spróbuj uzyskać dostęp do sieci WLAN bez poprawnego klucza dostępu. Upewnij się, że dostęp jest zablokowany.



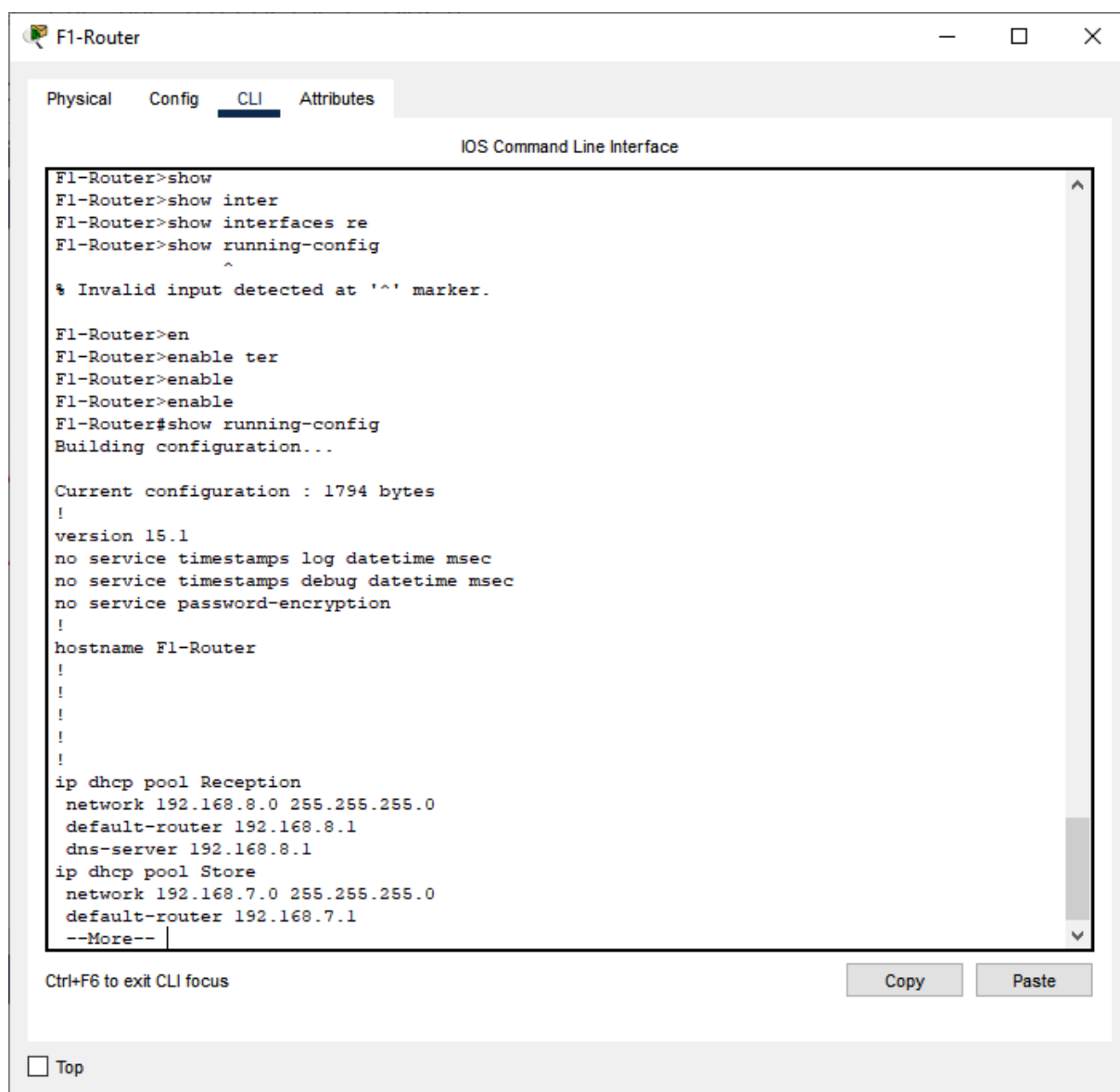
Rysunek 16, Test nieautoryzowanego dostępu.

## Test jednostkowy 5: Weryfikacja konfiguracji routingowej

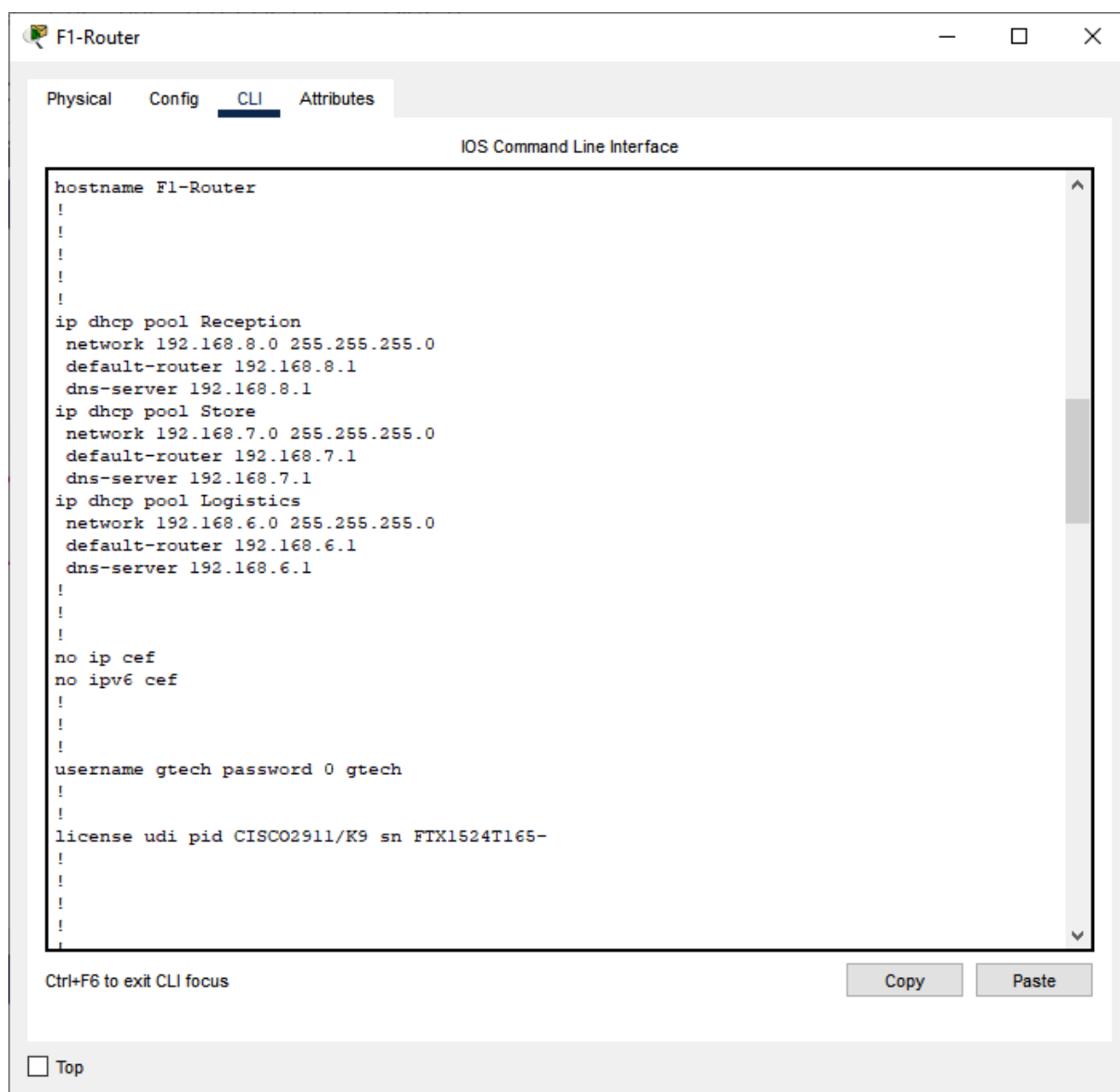
- Cel: Upewnienie się, że routing między różnymi podsieciami działa poprawnie.
- Krok 1: Test pinga między różnymi podsieciami - Spróbuj wysłać ping z jednej podsieci do urządzenia w innej podsieci. Upewnij się, że routing jest skonfigurowany poprawnie.



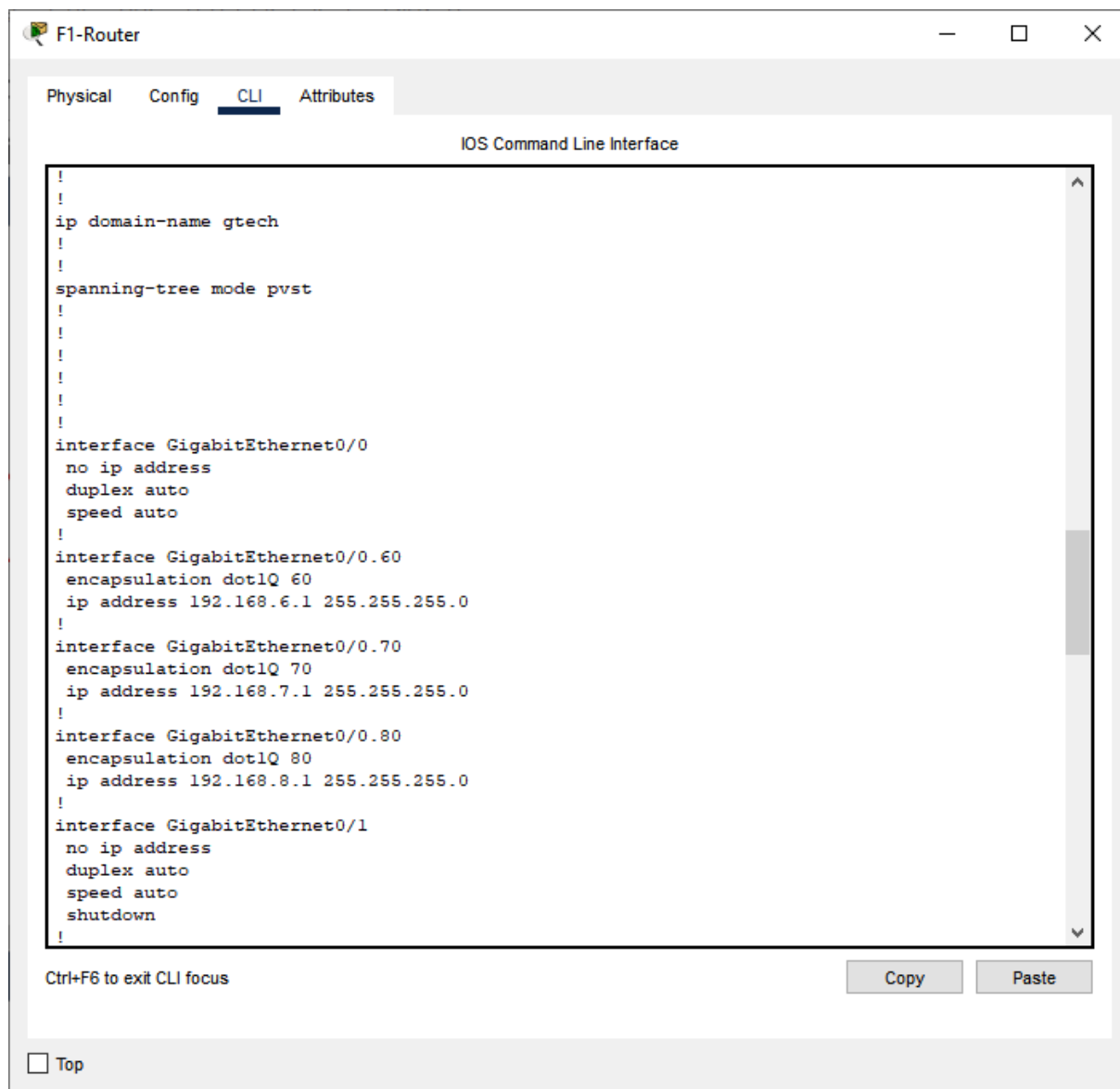
Rysunek 17, Test pinga między różnymi podsieciami.



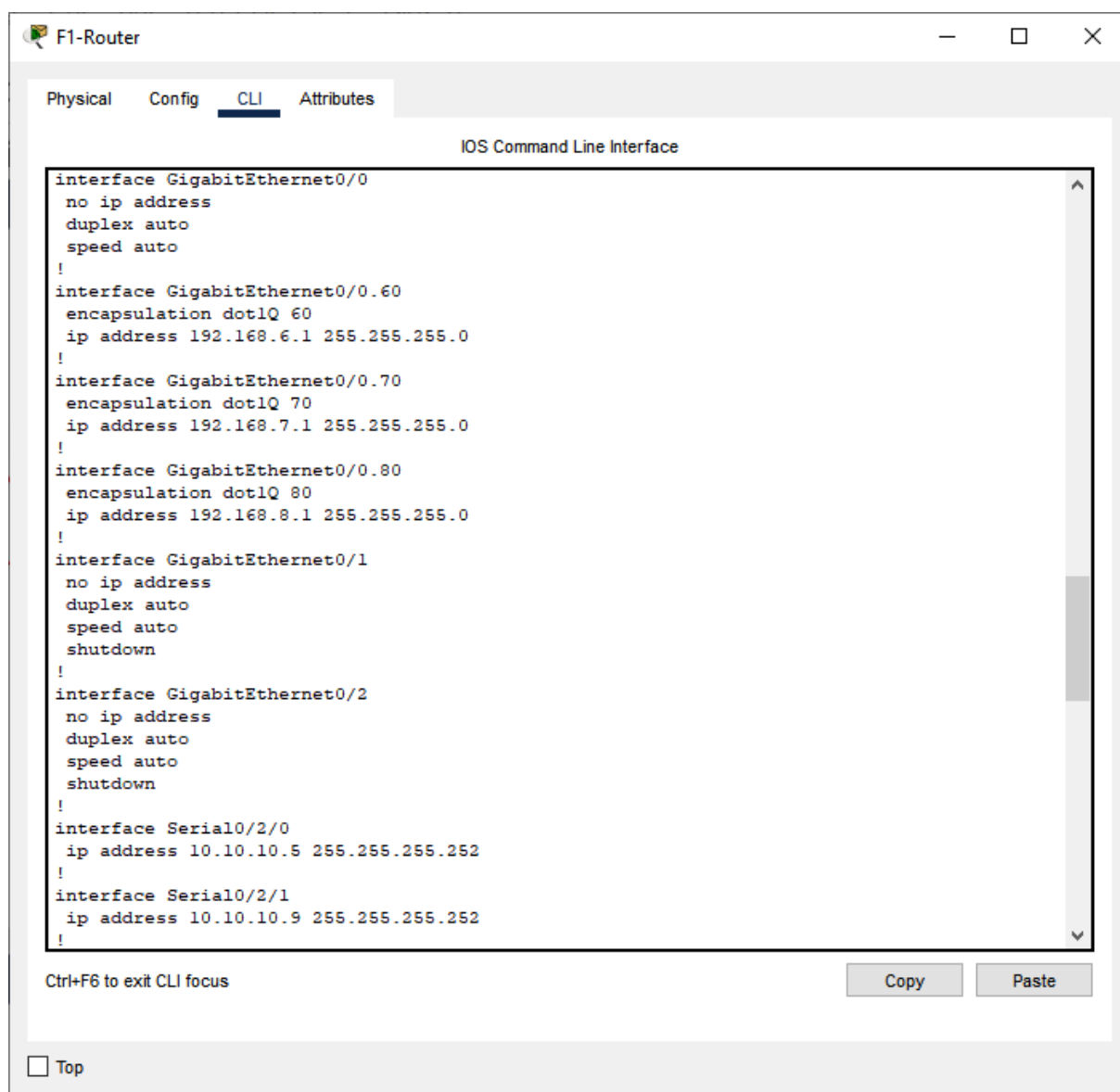
Rysunek 18, Konfiguracja urządzenia F1-Router.



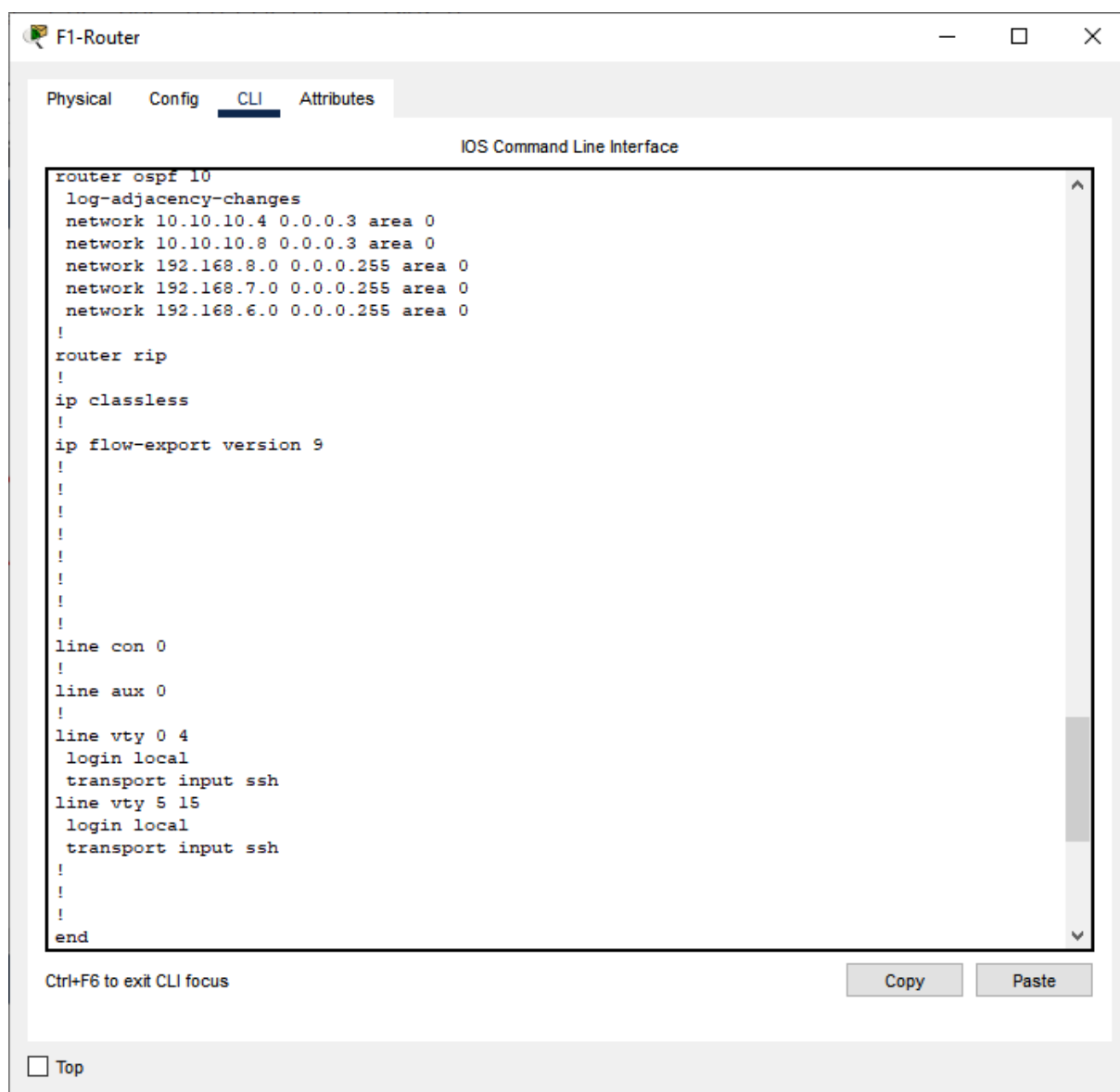
Rysunek 19, Konfiguracja urządzenia F1-Router.



Rysunek 20, Konfiguracja urządzenia F1-Router.

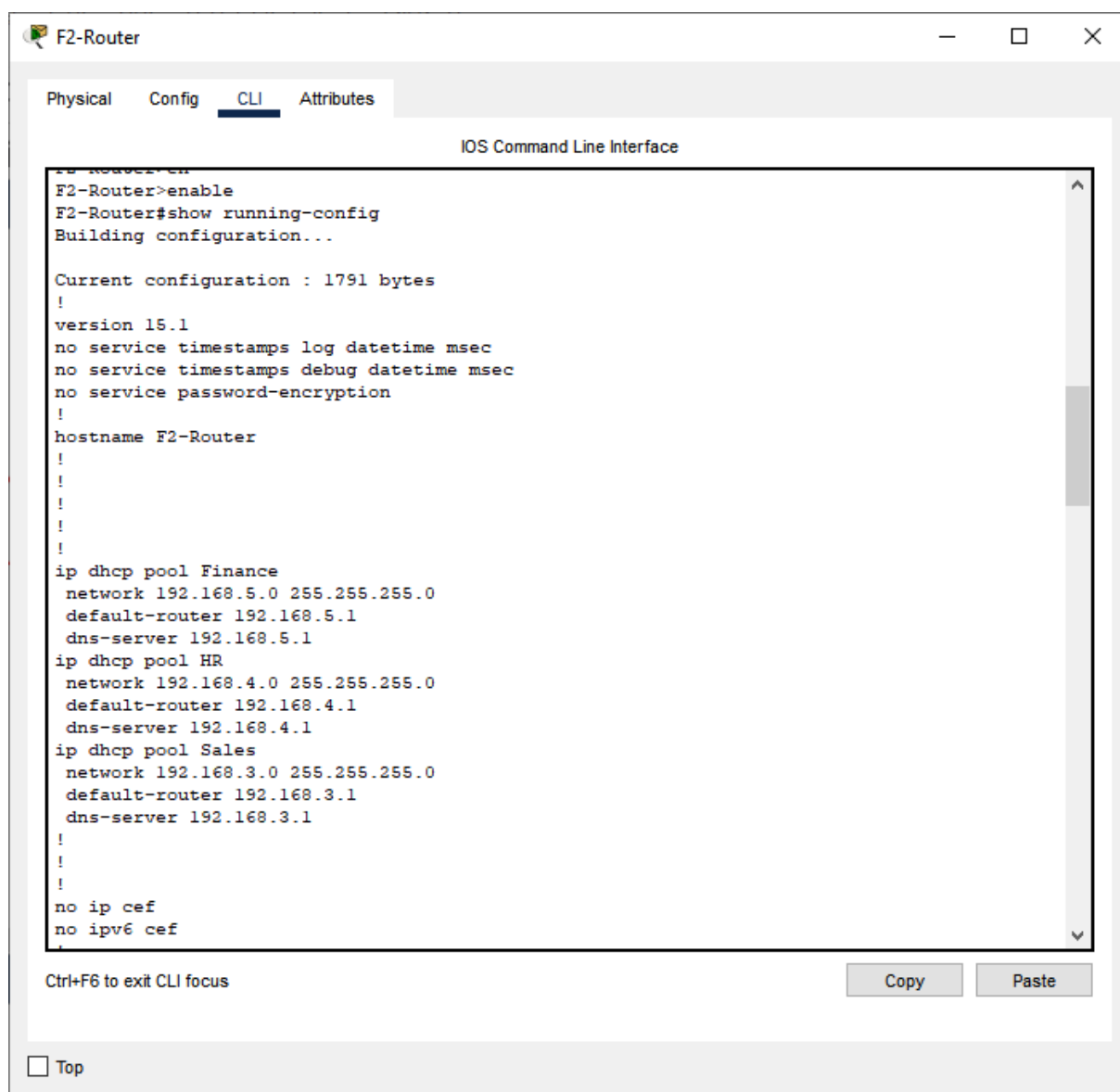


Rysunek 21, Konfiguracja urządzenia F1-Router.

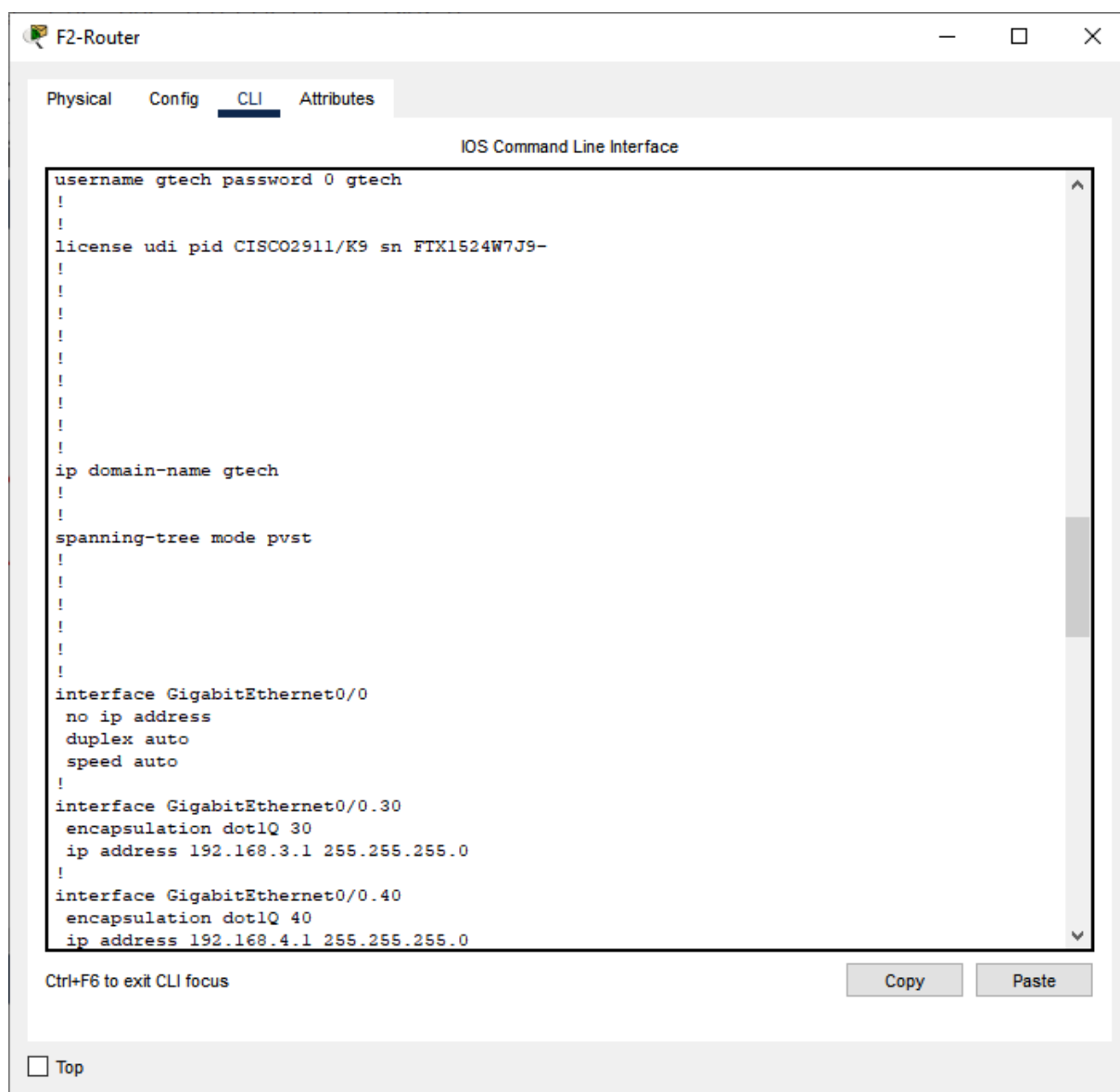


Rysunek 22, Konfiguracja urządzenia F1-Router.

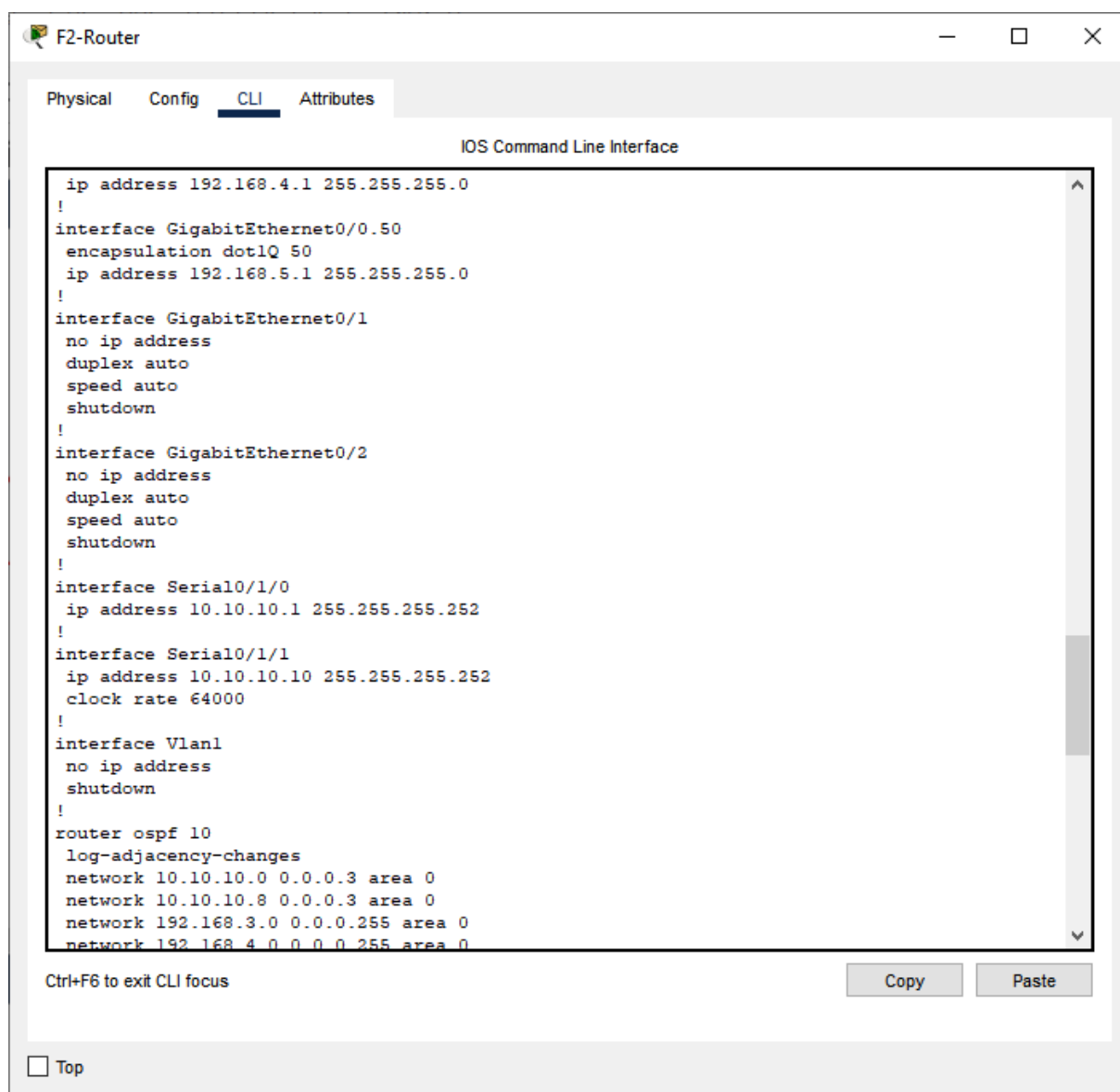




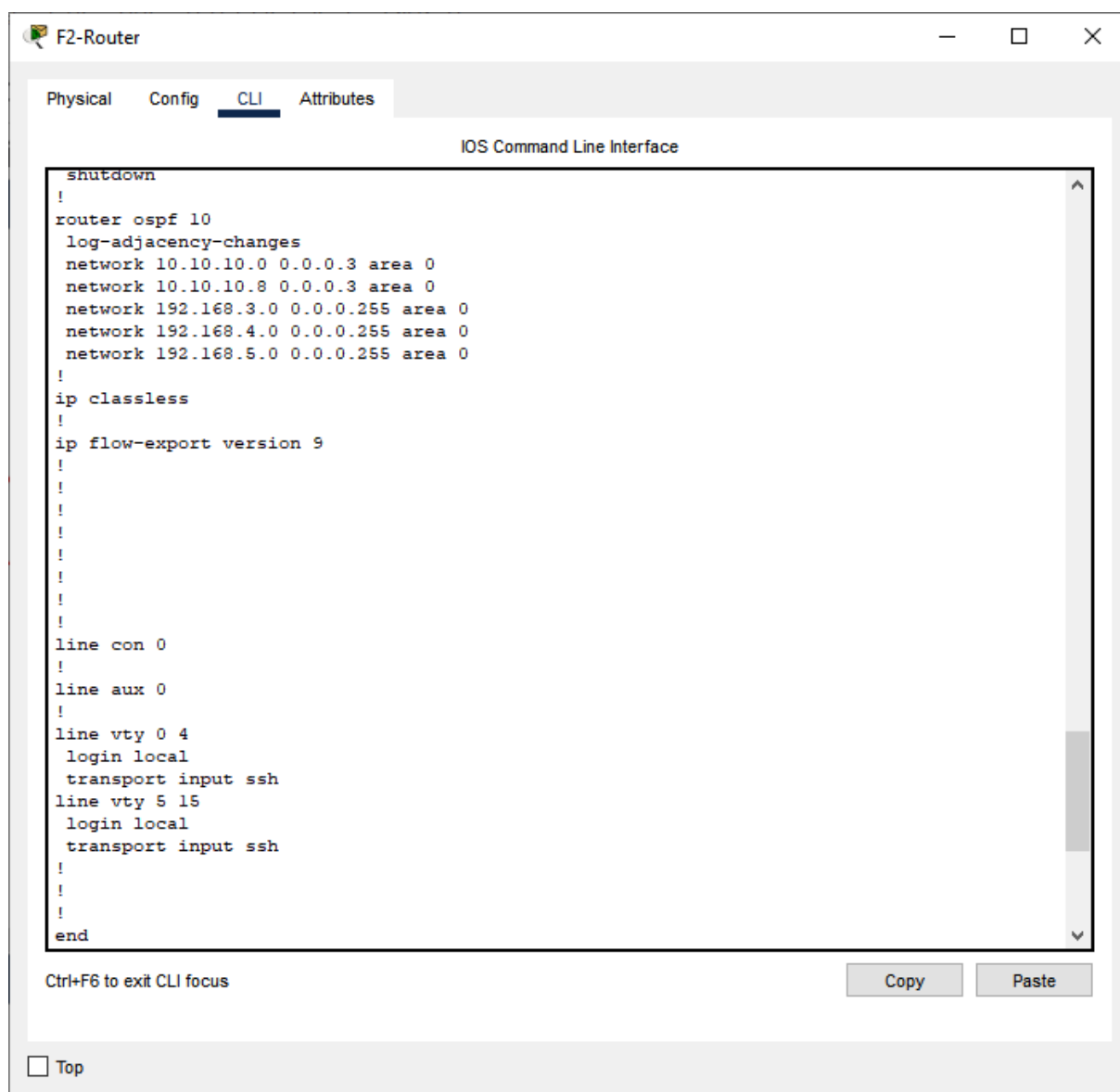
Rysunek 23, Konfiguracja urządzenia F2-Router.



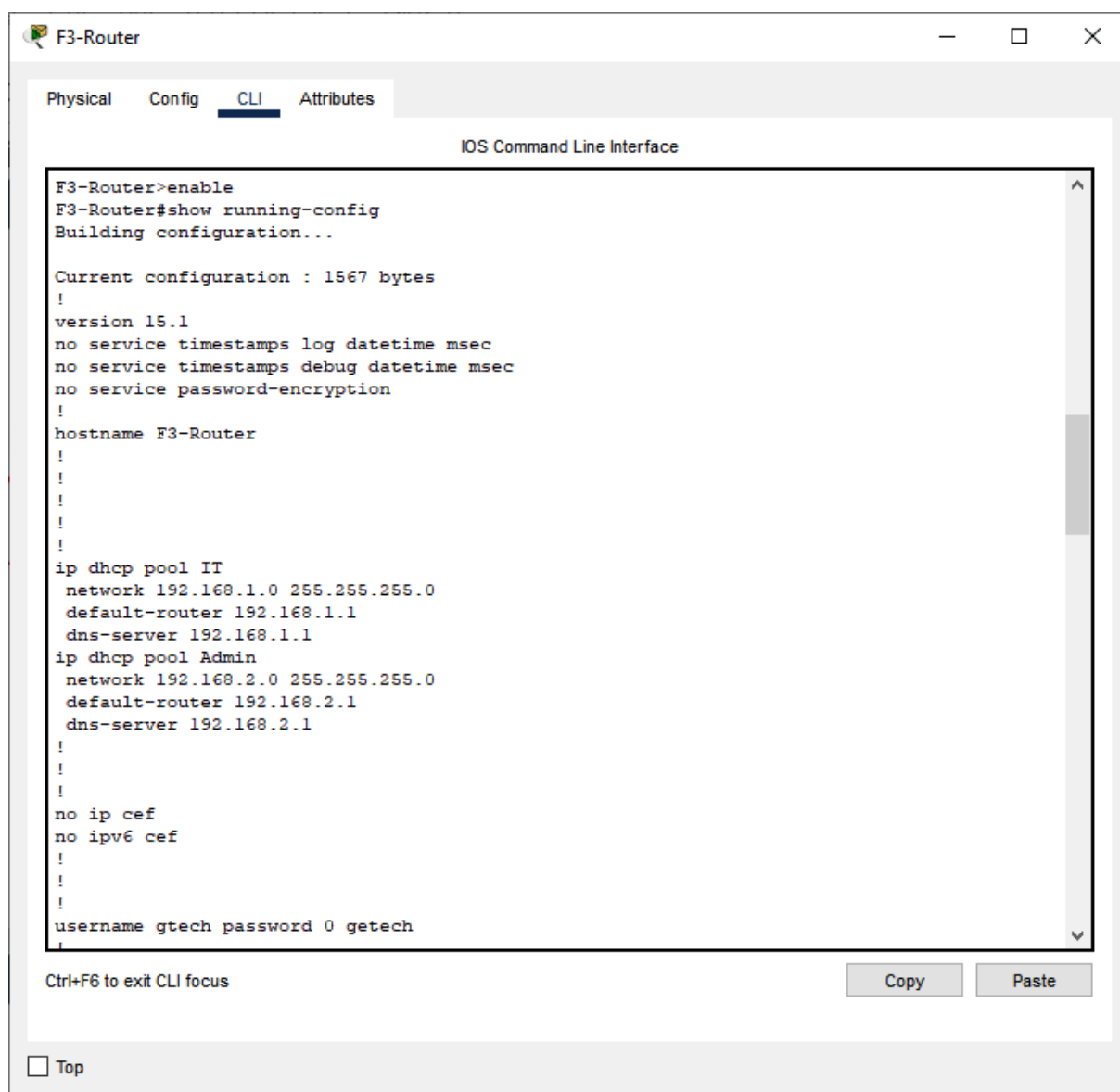
Rysunek 24, Konfiguracja urządzenia F2-Router.



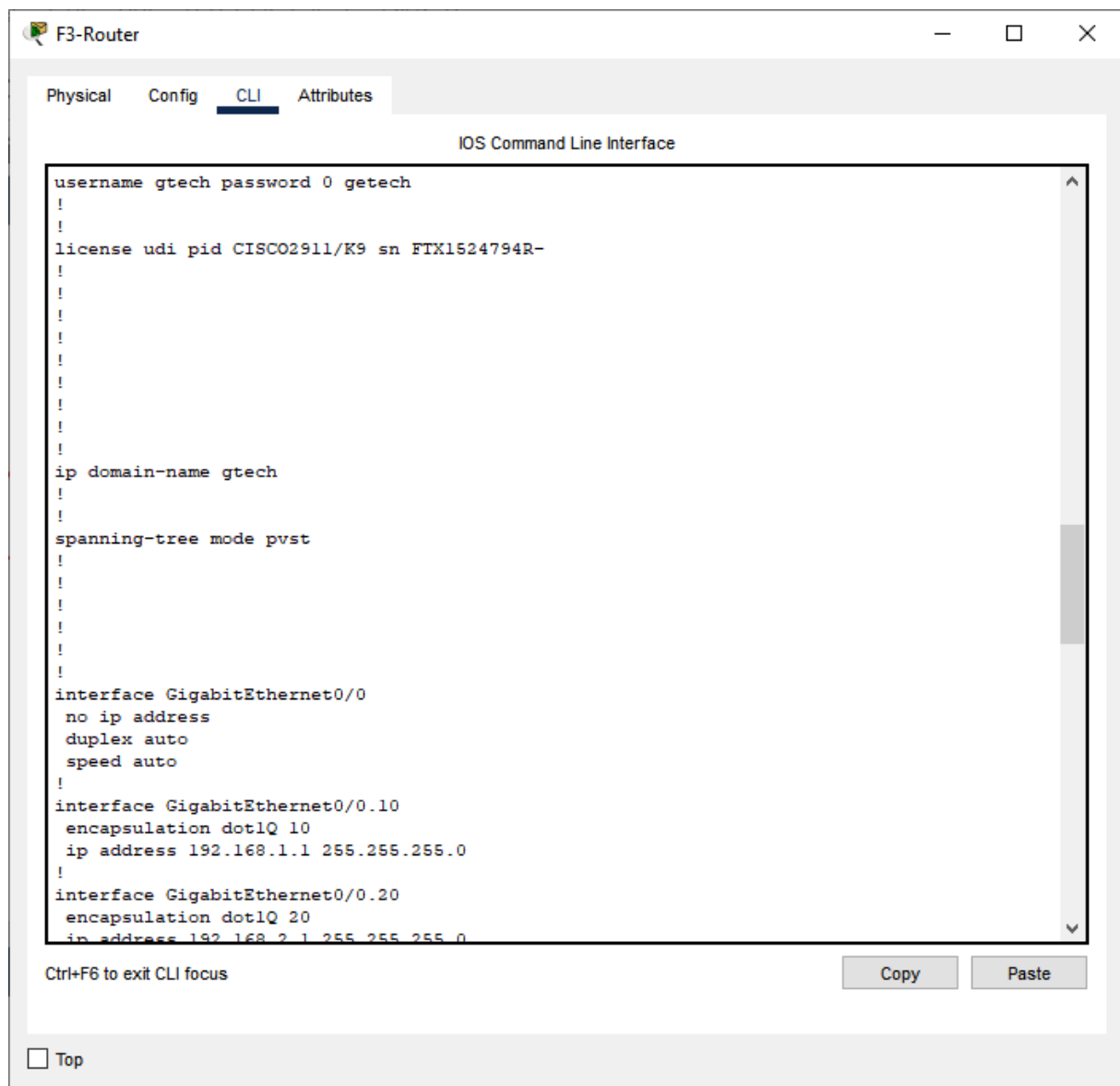
Rysunek 25, Konfiguracja urządzenia F2-Router.



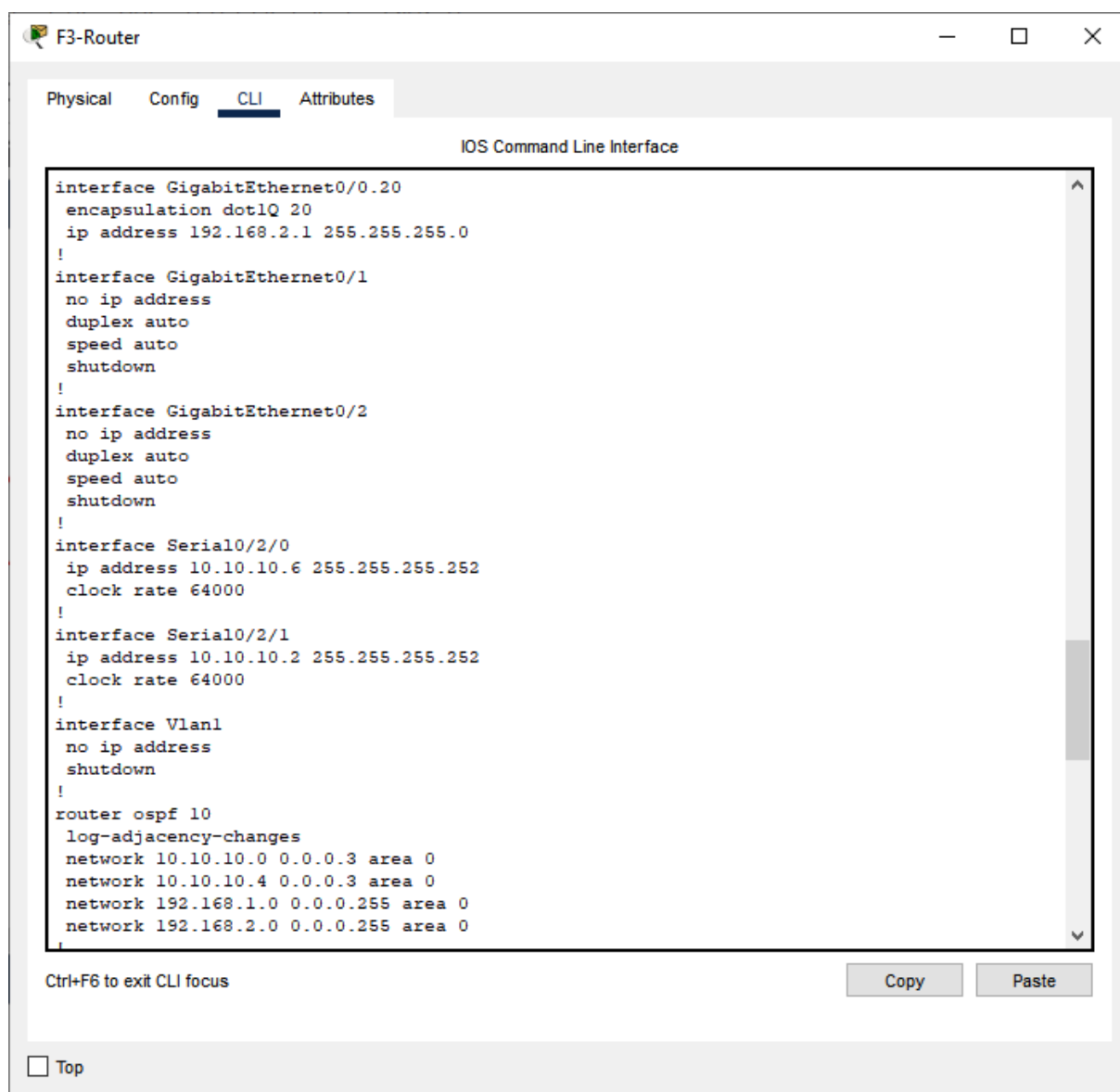
Rysunek 26, Konfiguracja urządzenia F2-Router.



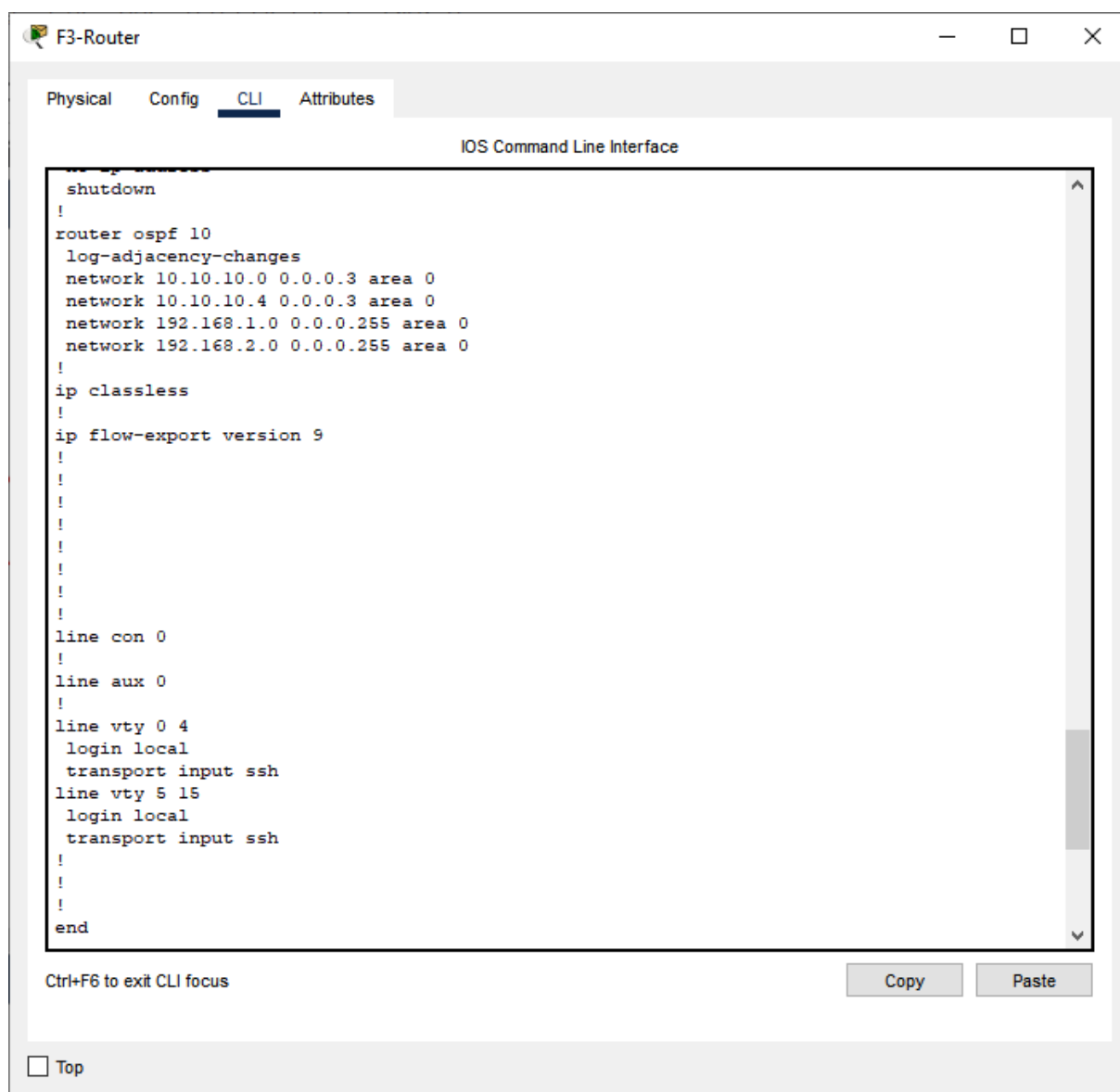
Rysunek 27, Konfiguracja urządzenia F3-Router.



Rysunek 28, Konfiguracja urządzenia F3-Router.

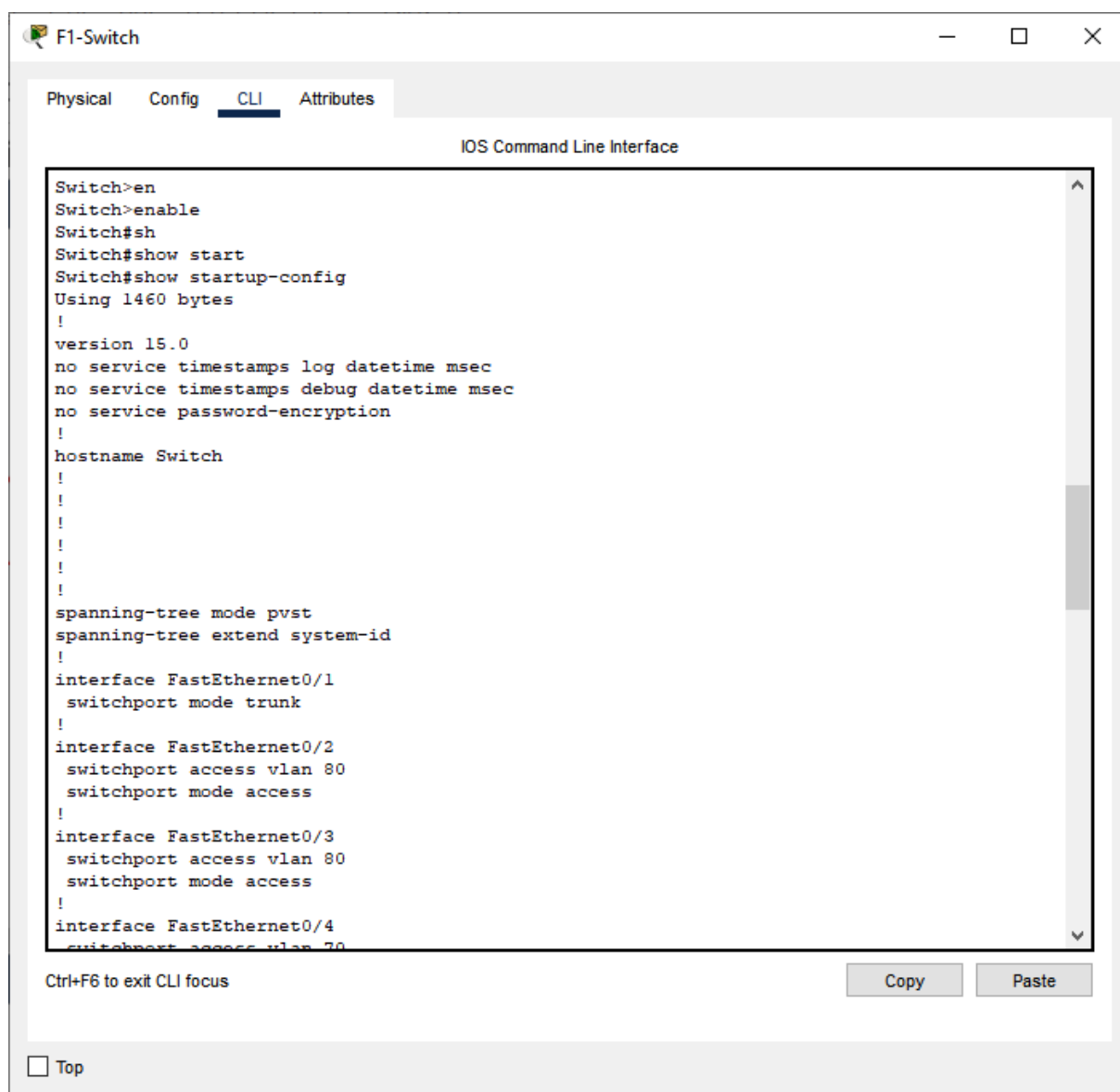


Rysunek 29, Konfiguracja urządzenia F3-Router.

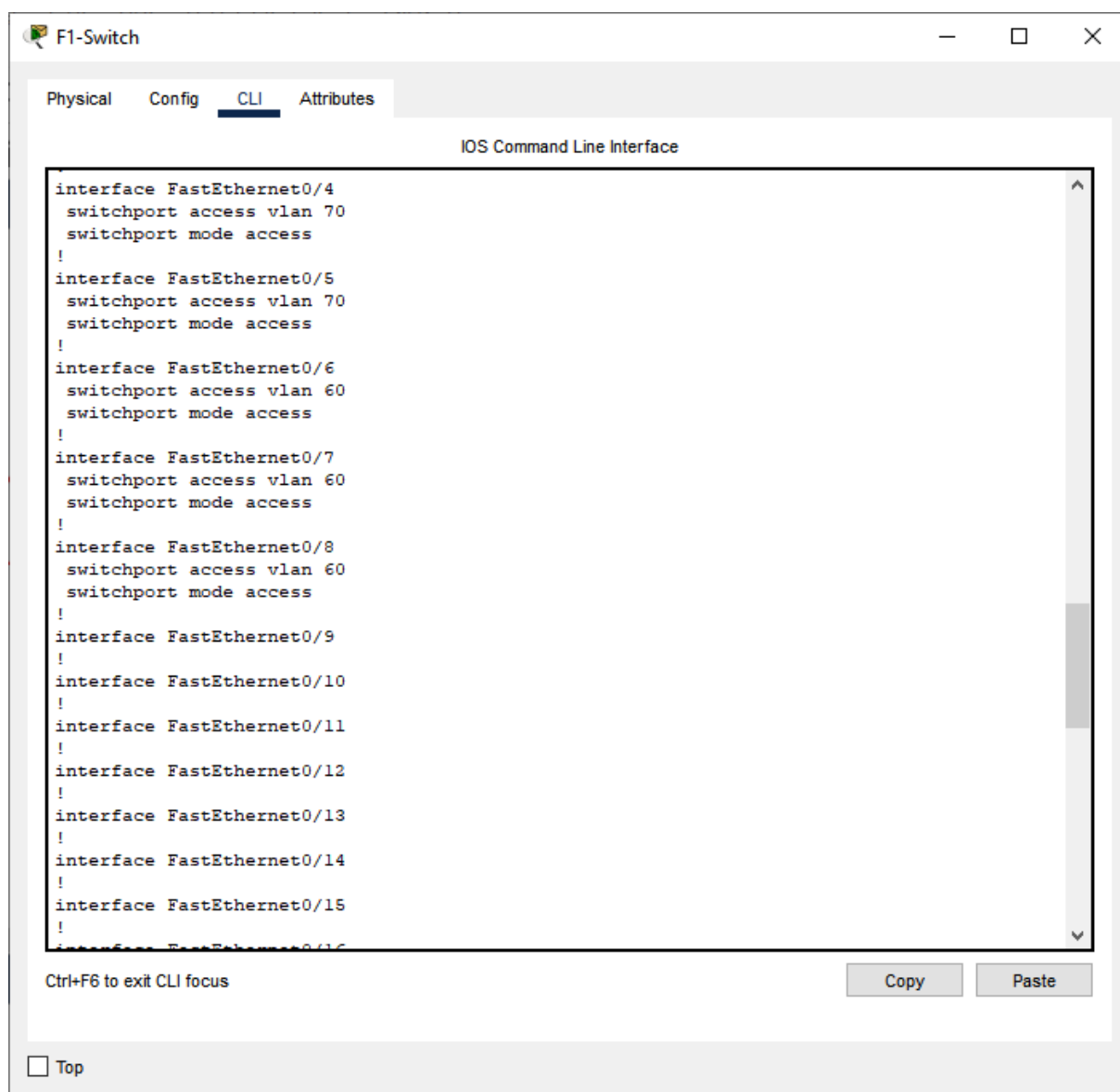


Rysunek 30, Konfiguracja urządzenia F3-Router.

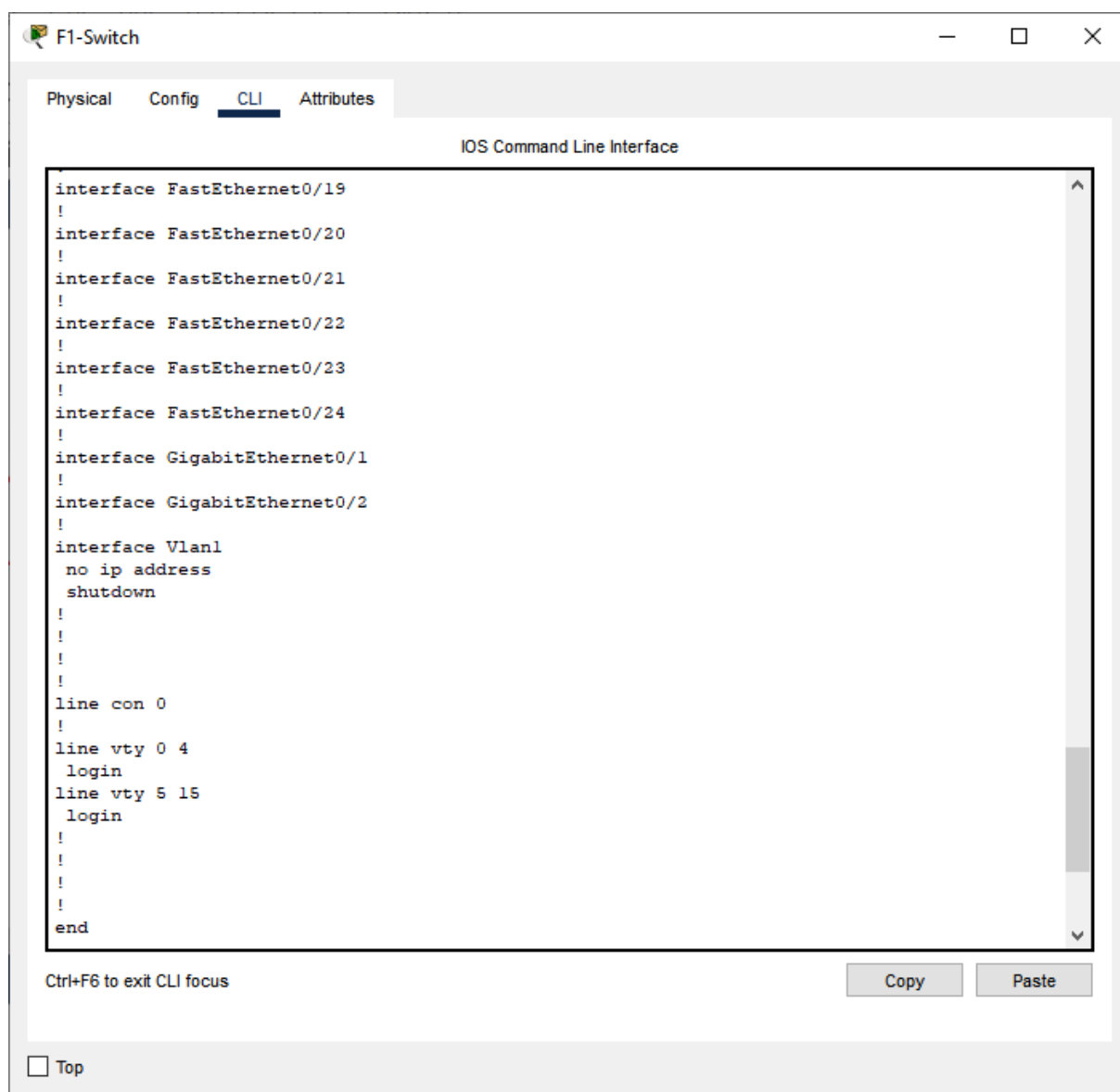




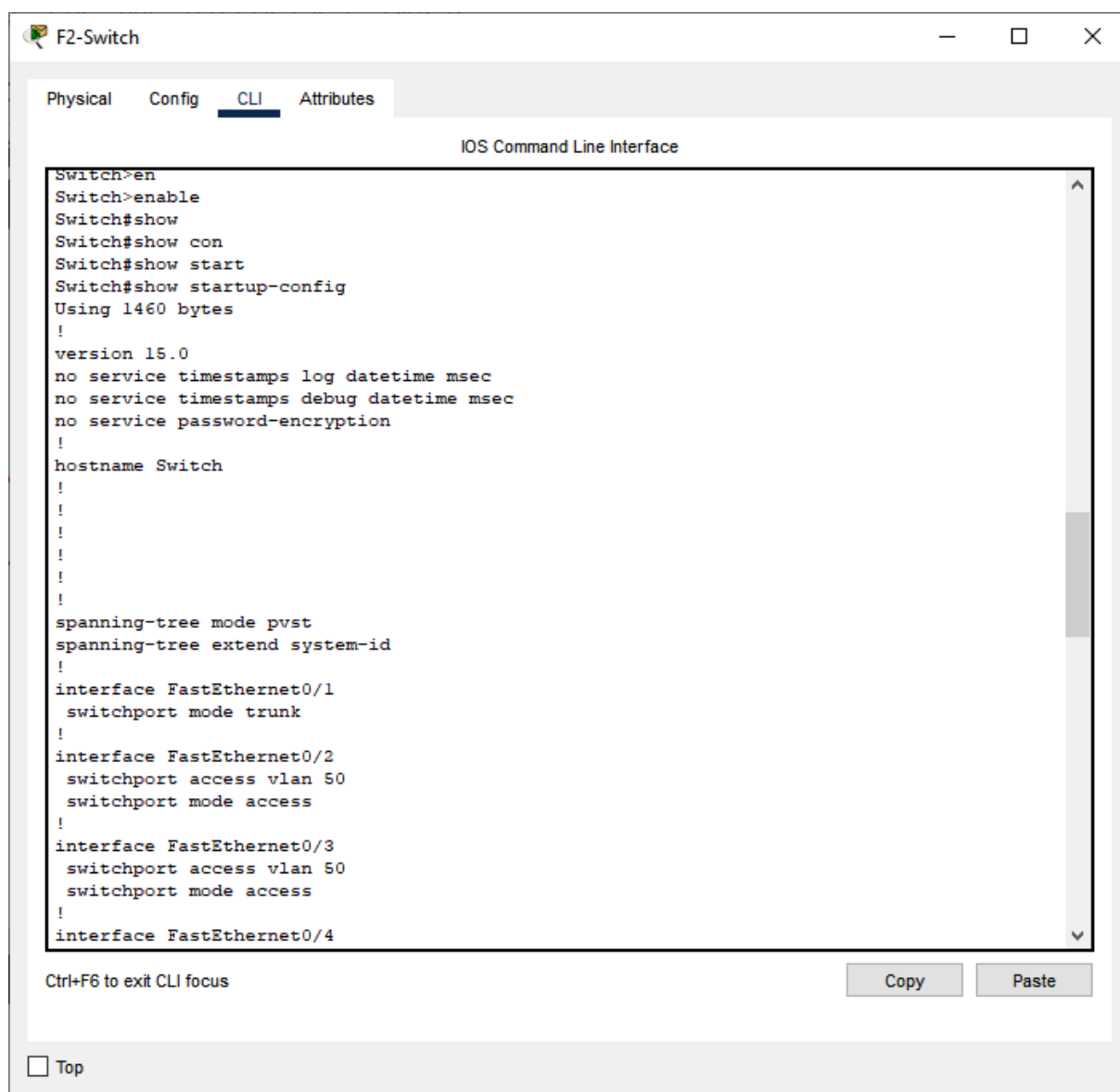
Rysunek 31, Konfiguracja urządzenia F1-Switch.



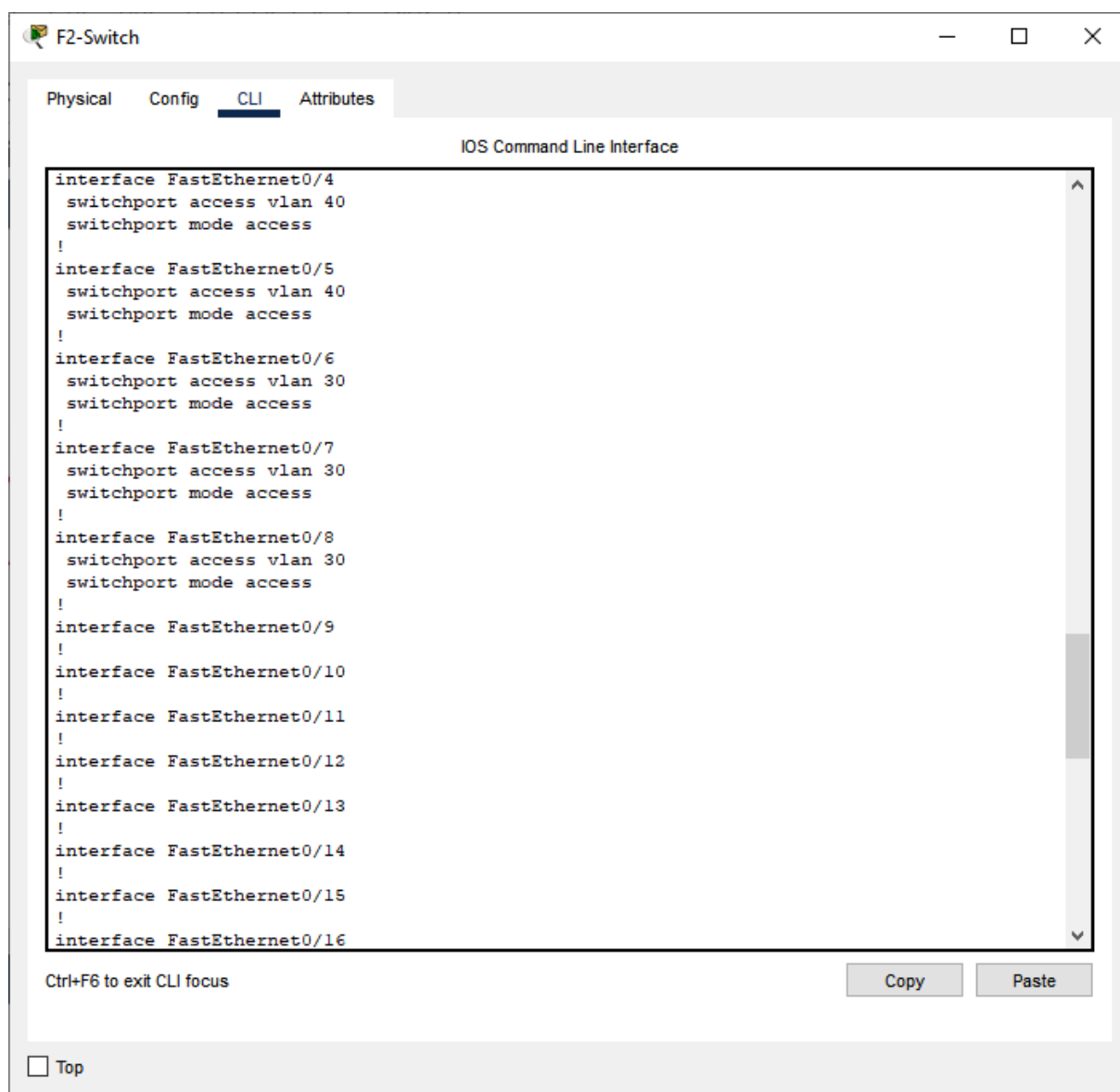
Rysunek 32, Konfiguracja urządzenia F1-Switch.



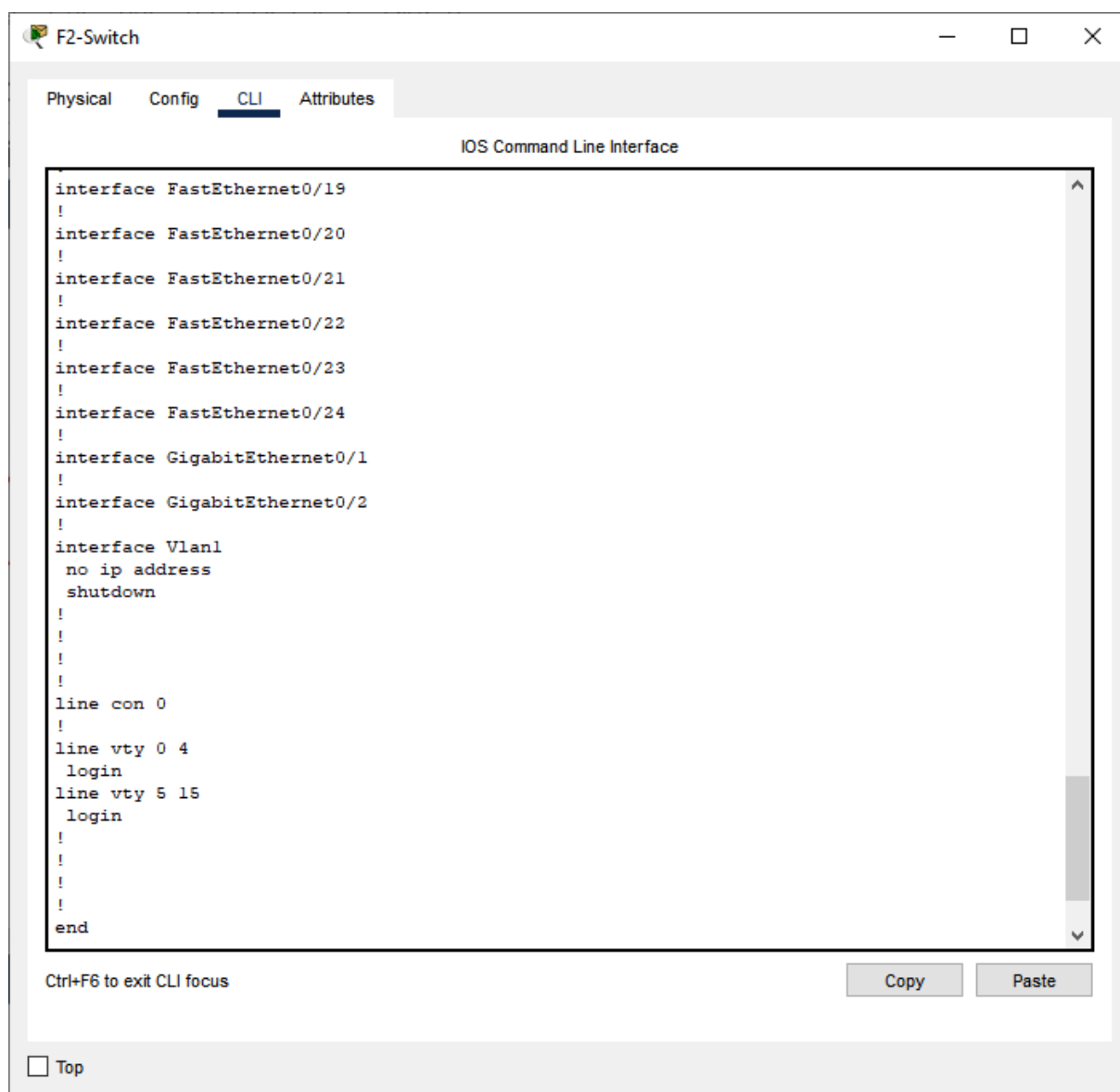
Rysunek 33, Konfiguracja urządzenia F1-Switch.



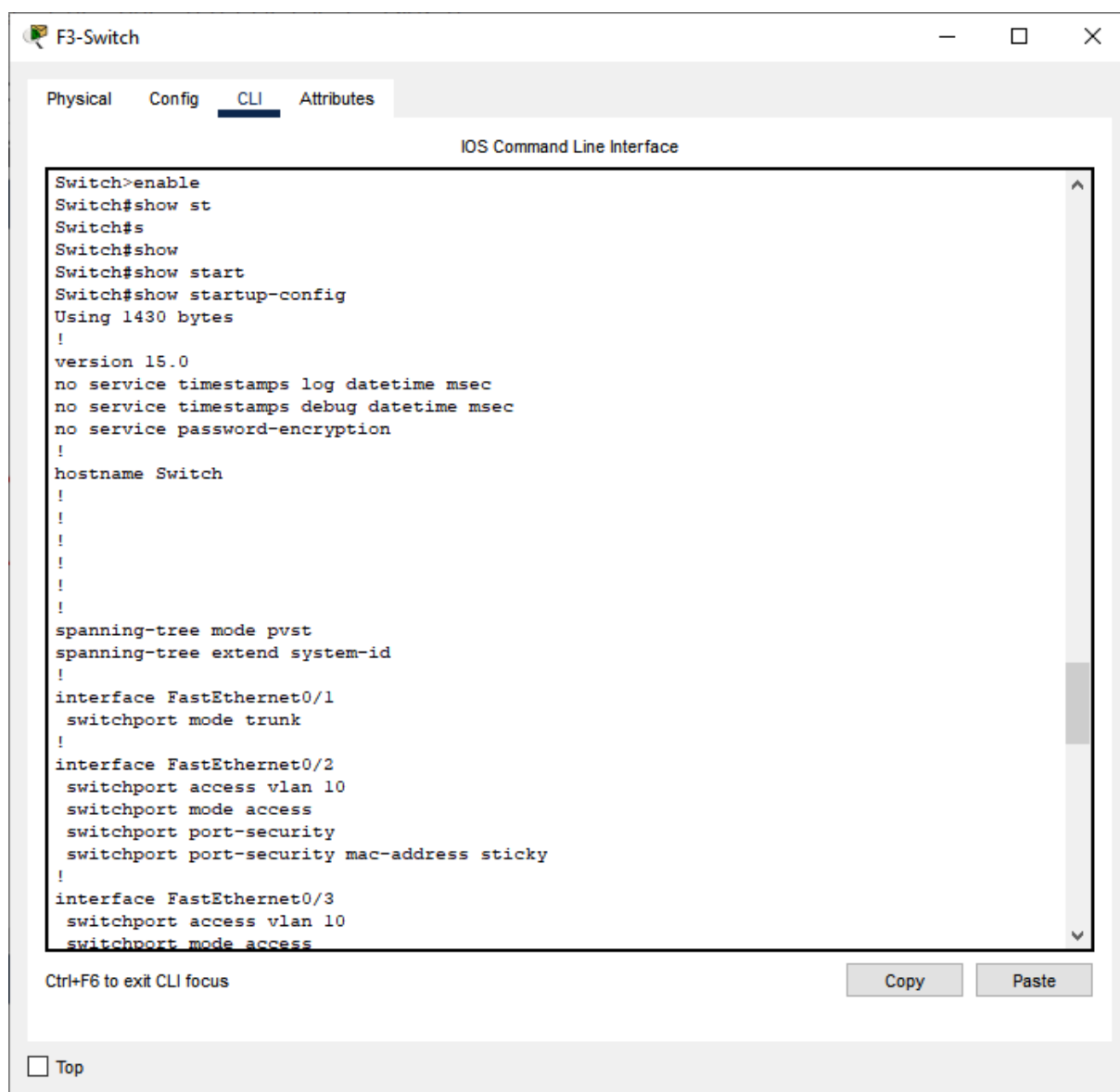
Rysunek 34, Konfiguracja urządzenia F2-Switch.



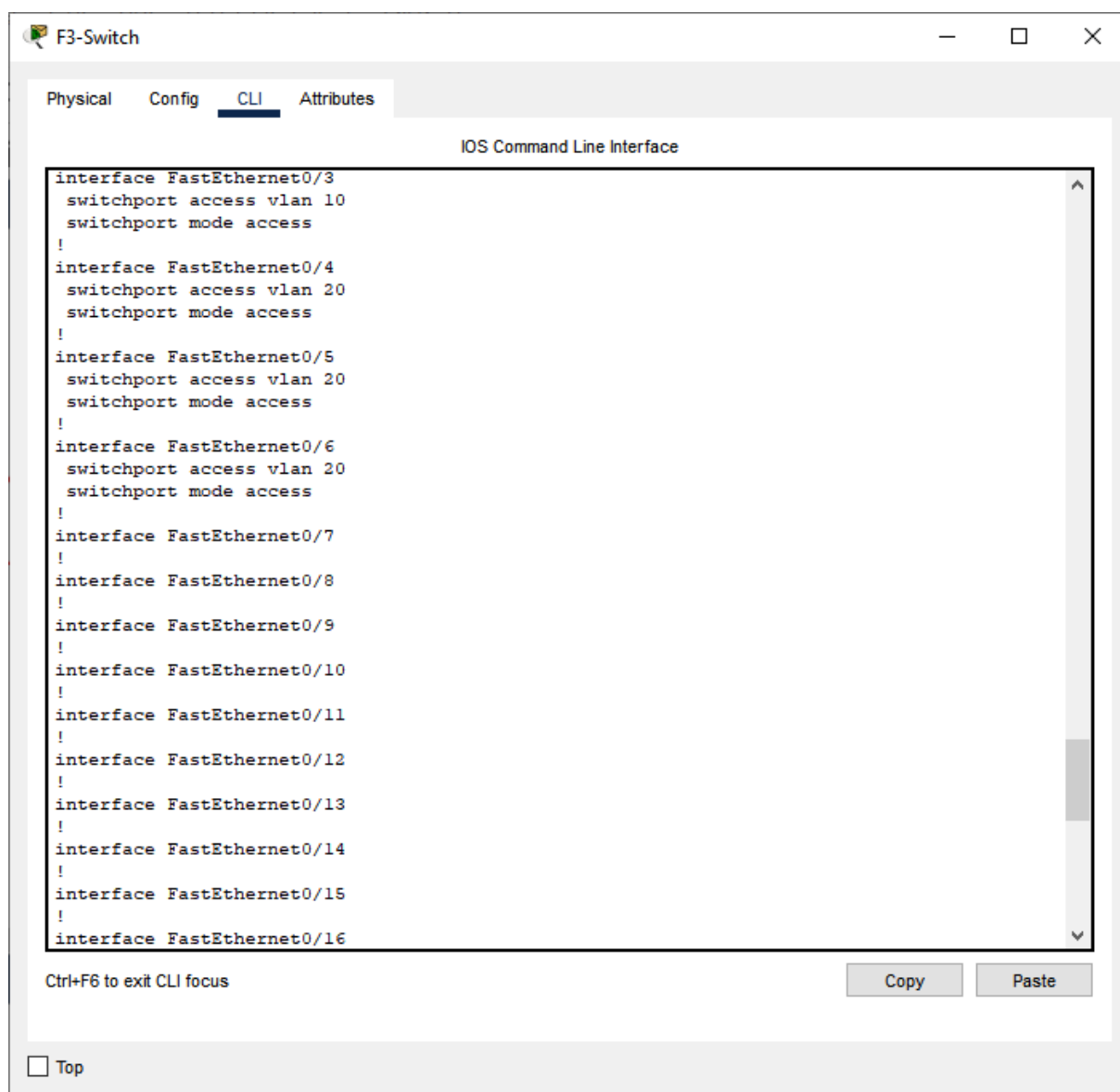
Rysunek 35, Konfiguracja urządzenia F2-Switch.



Rysunek 36, Konfiguracja urządzenia F2-Switch.

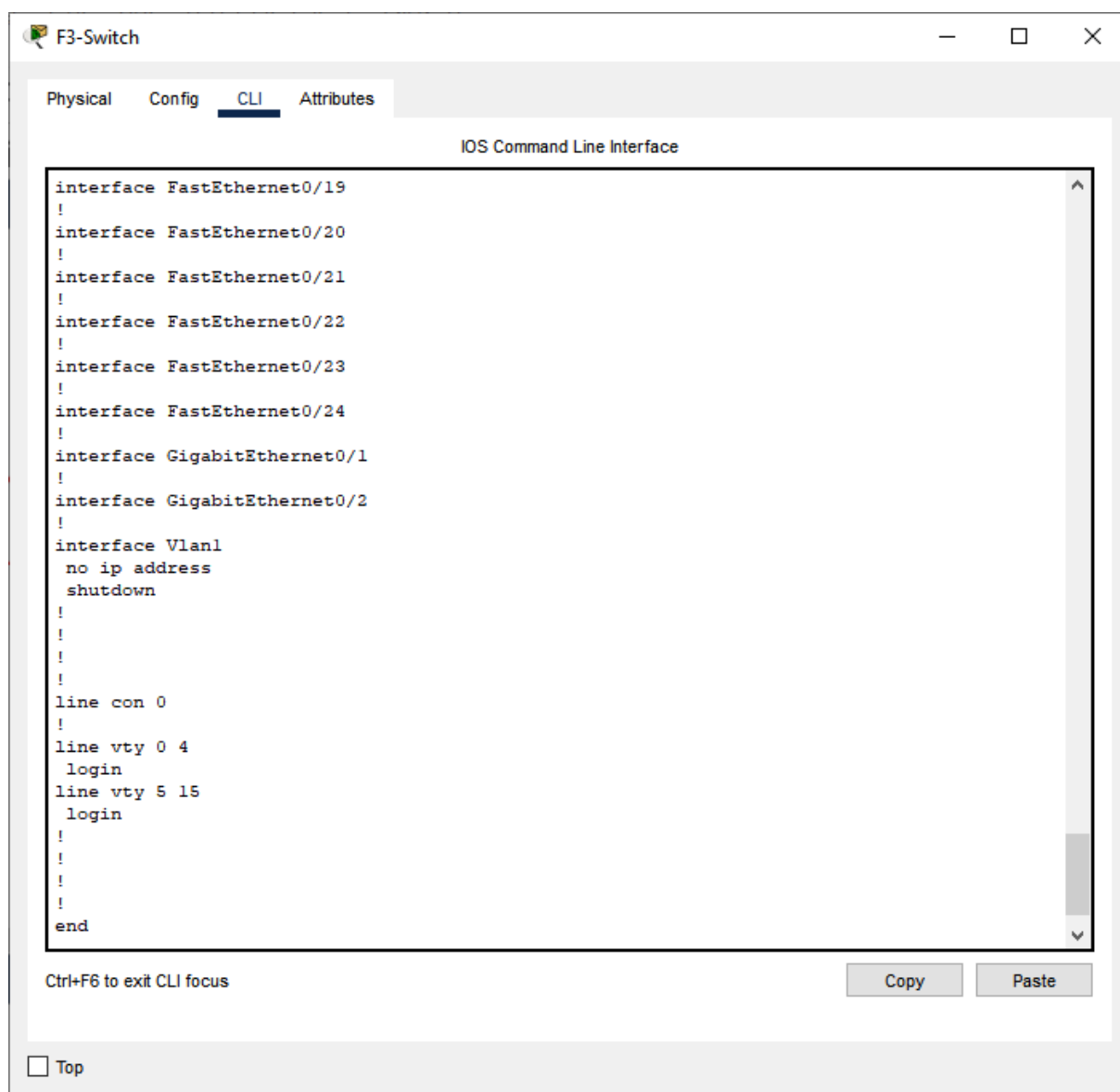


Rysunek 37, Konfiguracja urządzenia F3-Switch.



Rysunek 38, Konfiguracja urządzenia F3-Switch.





Rysunek 39, Konfiguracja urządzenia F3-Switch.

F1-Access-Point

Physical **Config** Attributes

**GLOBAL**

Settings

**INTERFACE**

Port 0

Port 1

Port 1

Port 1

Port Status ☒ On

SSID Floor1

2.4 GHz Channel 6

Coverage Range (meters) 140,00

Authentication

☐ Disabled ☐ WEP ☒ WPA2-PSK

WEP Key

PSK Pass Phrase Floor@123

User ID

Password

Encryption Type AES

☐ Top

Rysunek 40, Konfiguracja urządzenia F1-Access-Point.

F2-Access-Point

Physical
Config
Attributes

GLOBAL
Settings
INTERFACE
Port 0
Port 1

Port 1

Port 1

Port Status
☒ On

SSID
Floor2

2.4 GHz Channel
6

Coverage Range (meters)
140,00

Authentication

☐ Disabled
☐ WEP
☒ WPA2-PSK

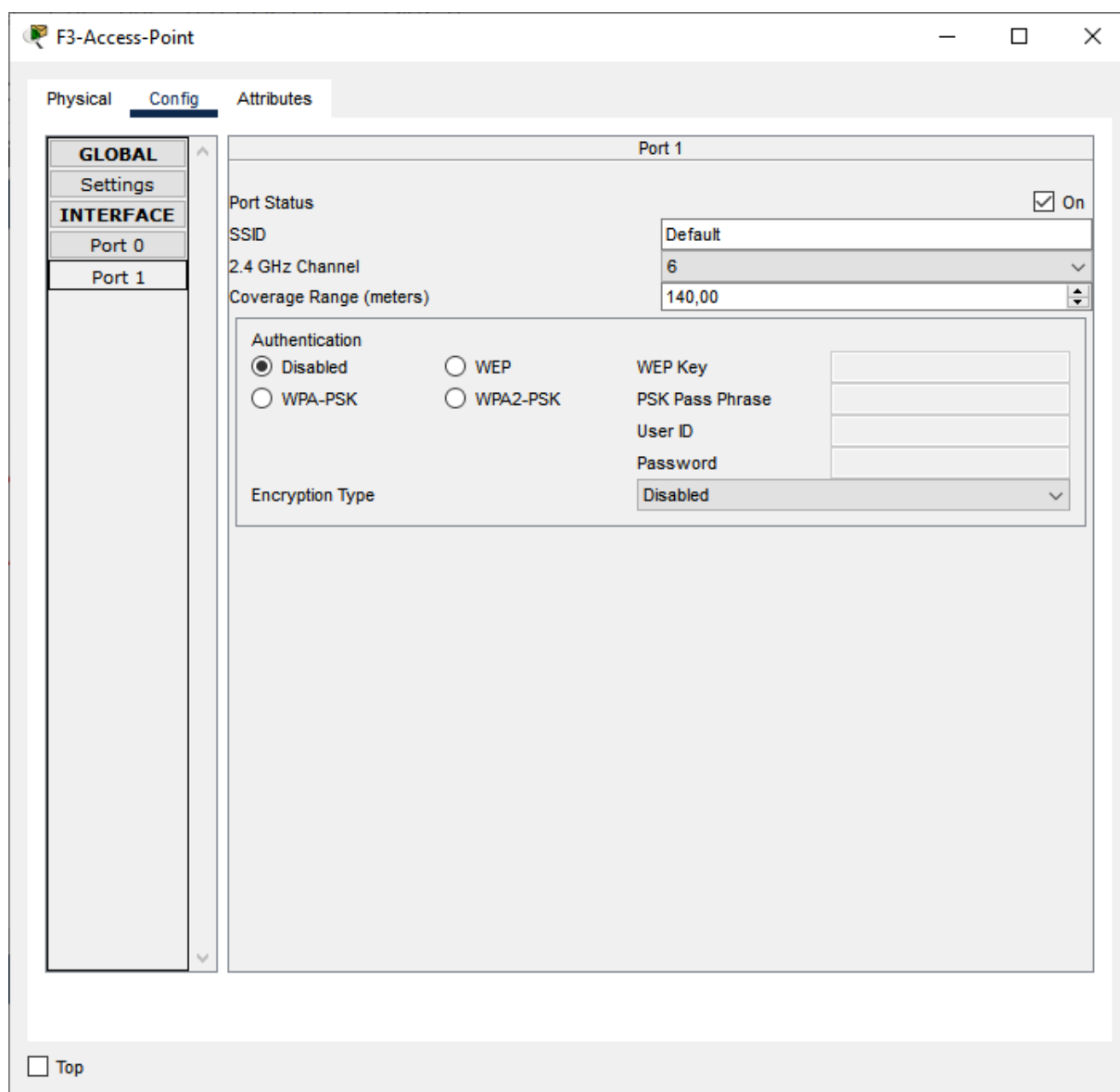
WEP Key
PSK Pass Phrase
User ID
Password

Floor@123

Encryption Type
AES

☐ Top

Rysunek 41, Konfiguracja urządzenia F2-Access-Point.



Rysunek 42, Konfiguracja urządzenia F3-Access-Point.

Testy jednostkowe te pomogą w identyfikacji ewentualnych problemów z konfiguracją i działaniem sieci, co pozwoli na ich szybkie rozwiązanie i zapewnienie, że sieć działa zgodnie z założeniami projektowymi.

Wyniki przeprowadzonych testów są zadowalające. Komunikacja między urządzeniami w różnych podsieciach została potwierdzona, a zastosowanie technologii EtherChannel przyczyniło się do płynniejszego i szybszego przesyłu danych w sieci.

Podsumowując wyniki testów, można stwierdzić, że konfiguracja sieci działa poprawnie i zgodnie z oczekiwaniami. Wszyscy użytkownicy uzyskali pozytywne wyniki, co świadczy o poprawnej konfiguracji sieci oraz jej płynnym działaniu.

Testowanie sieci komputerowej jest kluczowym etapem projektu, który pozwala na weryfikację, optymalizację i zabezpieczenie infrastruktury sieciowej. Dzięki identyfikacji błędów, wykrywaniu ograniczeń wydajnościowych, zapewnianiu bezpieczeństwa oraz

spełnianiu wymagań regulacyjnych, testowanie przyczynia się do utrzymania stabilności, wydajności i bezpieczeństwa sieci komputerowej.

Wszystkie przeprowadzone testy potwierdziły, że konfiguracja urządzeń jest zgodna z założeniami projektowymi, co oznacza, że nie są wymagane żadne korekty. Sieć jest gotowa do produkcji i spełni oczekiwania użytkowników w zakresie wydajności i bezpieczeństwa.

## 10. Repozytorium

[https://github.com/byczus69/PROJEKT-LAB\\_Inzynieria-oprogramowania/tree/main/Projekt\\_Repozytorium](https://github.com/byczus69/PROJEKT-LAB_Inzynieria-oprogramowania/tree/main/Projekt_Repozytorium)

## 11. Podsumowanie

Celem projektu było zaprojektowanie i wdrożenie kompleksowej sieci dla hotelu, która zapewniałaby niezawodne połączenie internetowe oraz dostęp do zasobów sieciowych dla pracowników i gości. Sieć musiała być skalowalna, łatwa w zarządzaniu i spełniać wysokie standardy bezpieczeństwa.

W ramach projektu zidentyfikowano trzy główne klasy aktorów: Koordynator, Pracownicy hotelu oraz Admin. Koordynator odpowiadał za zarządzanie siecią, administrowanie, zarządzanie sprzętem sieciowym oraz przypisywanie zasobów sprzętowych dla pracowników hotelu. Pracownicy hotelu korzystali z zasobów sieciowych, takich jak dostęp do Internetu, drukarek i innych urządzeń sieciowych. Admin zajmował się testowaniem sieci, zarządzaniem sprzętem oraz usuwaniem błędów/usterek.

Wymagania funkcjonalne projektu obejmowały administrowanie siecią, usuwanie usterek/błędów, zarządzanie sprzętem sieciowym, testowanie sieci, zarządzanie ruterami i przełącznikami oraz zapewnienie użytkownikom sieci dostępu do Internetu, drukarek i innych urządzeń sieciowych. Wymagania niefunkcjonalne obejmowały łatwy, bezinwazyjny dostęp do sieci oraz wdrożenie sieci w sposób niewidaczniający poszczególnych elementów i okablowania.

W projekcie zastosowano różne elementy sieciowe, takie jak routery, przełączniki, punkty dostępu WiFi oraz drukarki. Sieć była podzielona na VLANy, z każdym departamentem hotelowym mającym przypisaną odrębną sieć VLAN. Zastosowano protokół routingu OSPF do przesyłania tras w sieci, a serwer DHCP został skonfigurowany do automatycznego przydzielania adresów IP.

Diagramy używane w projekcie obejmowały diagram przypadków użycia, diagram aktywności oraz diagram stanów. Diagram przypadków użycia przedstawiał aktorów, takich jak Koordynator, Pracownicy hotelu i Admin, wraz z odpowiadającymi im przypadkami użycia. Diagram aktywności przedstawiał sekwencję działań w konkretnych procesach, takich jak dostęp do drukarek przez pracowników hotelu. Natomiast diagram stanów przedstawiał różne stany i przejścia w procesie łączenia się z siecią bezprzewodową.

Podsumowując, projekt "Projektowanie i wdrożenie sieci dla Hotelu" skoncentrował się na zapewnieniu niezawodnej sieci, umożliwiającej pracownikom i gościom dostęp do zasobów sieciowych. Zastosowane rozwiązania obejmowały odpowiednie zarządzanie sprzętem, testowanie sieci, obsługę błędów oraz konfigurację bezpieczeństwa. Projekt pomyślnie

zrealizowano, dostarczając funkcjonalną i bezpieczną sieć dla hotelu, spełniającą wszystkie wymagania i oczekiwania klienta.

## **12. Literatura**

Materiały źródłowe – wskazanie literatury i materiałów źródłowych wykorzystanych przy realizacji projektu.

1. Arduino dla początkujących. Podstawy i szkice - Simon Monk
2. <https://forbot.pl/blog/leksykon/esp8266> (12.04.2023)
3. <https://wolski.pro/diagramy-uml> (23.06.2023)