



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

KOLEGIUM INFORMATYKI STOSOWANEJ

Kierunek: INFORMATYKA
Specjalność: Technologie IoT - Internetu
Rzeczy

Szymon Sutyła
Nr albumu studenta: w66012

Komunikacja człowiek-komputer

***Projektowanie i implementacja sieci przedsiębiorstwa z
wykorzystaniem narzędzia Packet Tracer***

Rzeszów 2024

Spis treści

1. Analiza istniejących rozwiązań	3
1.1. Cisco Network Solutions	3
1.2. Microsoft Azure	4
1.3. Fortinet	5
1.4. Elementy wspólne	6
1.5. Różnice	6
1.6. Wady i zalety przedstawionych rozwiązań	7
1.6.1. Cisco Network Solutions	7
1.6.2. Microsoft Azure	7
1.6.3. Fortinet	7
2. Wymagania funkcjonalne oraz нефункционалне	7
2.1. Zarys projektu	7
2.2. Zakres pracy	7
2.3. Założenia funkcjonalne i нефункционалне	8
2.3.1. Funkcjonalne	8
2.3.2. Нефункционалне	8
2.4. Opis wykorzystywanych technologii	8
2.4.1. Wybrane technologie	8
2.4.2. Zastosowanie Packet Tracer w projekcie	9
2.4.3. Korzyści z wykorzystania narzędzia Cisco Packet Tracer	10
3. Implementacja sieci	10
3.1. Projekt topologii sieci	10
3.2. Konfiguracja urządzeń sieciowych w Packet Tracerze	12
3.2.1. Konfiguracja routera Cisco ISR4321	12
3.2.2. Konfiguracja przełączników Cisco Catalyst 2960	15
3.2.3. Konfiguracja ruchu sieciowego	18
4. Testy	20
5. Podsumowanie	23
Spis literatury	24

1. Analiza istniejących rozwiązań

Do porównania istniejących rozwiązań wybrałem: Cisco Network Solutions, Microsoft Azure i Fortinet ze względu na ich renomę, szeroką gamę oferowanych produktów i usług oraz znaczącą pozycję na rynku technologii sieciowych i bezpieczeństwa. Każde z tych rozwiązań jest znane z zaawansowanych technologii i kompleksowego podejścia do rozwiązywania problemów sieciowych i zabezpieczeń, co sprawia, że są one idealnymi kandydatami do porównania.

1.1. Cisco Network Solutions

Cisco jest to renomowany dostawca rozwiązań sieciowych, oferujący szeroki zakres produktów. Do kluczowych obszarów, w których specjalizuje się Cisco zaliczyć możemy:

- Routery i przełączniki: Cisco dostarcza zaawansowane routery i przełączniki LAN i WAN, które umożliwiają efektywne zarządzanie ruchem sieciowym.
- Bezpieczeństwo: Cisco oferuje różnorodne produkty z zakresu bezpieczeństwa, takie jak firewalle, VPN, UTM, AAA (autoryzacja, uwierzytelnianie i rachunkowość) oraz NAC (Network Access Control). Te rozwiązania pomagają chronić sieci przed zagrożeniami i atakami.
- Telefonia IP: Cisco dostarcza systemy telefonii IP, które pozwalają na przesyłanie głosu w sieciach danych. To ważne dla firm, które chcą zintegrować komunikację głosową z danymi.
- Sieci bezprzewodowe: Cisco jest liderem w dziedzinie technologii Wi-Fi i oferuje produkty do budowy wydajnych i bezpiecznych sieci bezprzewodowych.
- Cisco DNA: To architektura sieciowa, która umożliwia automatyzację, analizę i zarządzanie siecią. Pozwala na tworzenie bardziej inteligentnych i elastycznych sieci.



Źródło:

https://www.cisco.com/c/pl_pl/index/jcr:content/homepagemaincontentparsys/full_9e22/Full/mosaic_row_wide_narr/mosaic_col_wide_parsys/mosaic_tile_wide_bf6.img.jpg/1707491883682.jpg dostęp 10.05.2024

1.2. Microsoft Azure

Microsoft Azure to platforma chmurowa, która oferuje różnorodne usługi sieciowe i obliczeniowe. Oto kilka kluczowych obszarów, w których Azure się specjalizuje:

- Azure Virtual Network (VNET): To usługa umożliwiająca tworzenie izolowanych, wirtualnych sieci w chmurze. Dzięki VNET możesz łączyć maszyny wirtualne, aplikacje i inne zasoby w jednym bezpiecznym środowisku. To idealne rozwiązanie dla organizacji, które potrzebują elastycznych i skalowalnych sieci.
- Azure Load Balancer: Jest to usługa równoważenia obciążenia, która automatycznie dystrybuje ruch między różnymi serwerami lub maszynami wirtualnymi. Dzięki temu można osiągnąć wyższą dostępność i wydajność aplikacji.
- Azure VPN Gateway: Usługa umożliwiająca bezpieczne połączenie między lokalnymi sieciami a siecią w chmurze. Pozwala na tworzenie wirtualnych sieci prywatnych (VPN) i zapewnia szyfrowaną komunikację.
- Azure App Service: To platforma do hostowania aplikacji internetowych, mobilnych i API. Pozwala na łatwe wdrażanie, skalowanie i zarządzanie aplikacjami w chmurze.



Źródło: https://media.licdn.com/dms/image/D4D12AOGUnhgqmwIvzQ/article-cover_image-shrink_720_1280/0/1658421811896?e=2147483647&v=beta&t=mqCHoKMvc-uU5PbGJJ8b-LcnuSTy8aSqUyO2p5F1QE
dostęp 10.05.2024

1.3. Fortinet

Fortinet to globalny lider w dziedzinie bezpieczeństwa sieciowego i rozwiązań cyberbezpieczeństwa. Oferuje szeroki zakres produktów i usług, które pomagają organizacjom chronić swoje sieci przed zagrożeniami. Oto kluczowe rozwiązania oferowane przez Fortinet:

- FortiGate: To seria urządzeń firewall, które łączą w sobie funkcje zapory sieciowej, VPN, wykrywania i eliminacji zagrożeń oraz kontroli treści. FortiGate jest znany ze swojej wydajności, skalowalności i zaawansowanych funkcji bezpieczeństwa.
- FortiAnalyzer: To narzędzie do analizy i raportowania ruchu sieciowego. Pomaga organizacjom monitorować i analizować dane z urządzeń FortiGate, aby zidentyfikować potencjalne zagrożenia.
- FortiManager: Jest to platforma do zarządzania urządzeniami Fortinet. Umożliwia zdalne konfigurowanie, monitorowanie i aktualizowanie urządzeń w sieci.
- FortiAP: To punkty dostępowe WiFi, które można zintegrować z urządzeniami FortiGate. Pozwalają na budowę bezpiecznych i wydajnych sieci bezprzewodowych.
- FortiWeb: To rozwiązanie do ochrony aplikacji internetowych przed atakami, takimi jak SQL injection, cross-site scripting (XSS) i inne.
- FortiSandbox: Jest to środowisko do analizy zachowania plików. Pozwala na wykrywanie zaawansowanych zagrożeń, takich jak złośliwe oprogramowanie i ransomware.

Rys. 3. Fortinet



Źródło: https://sieciowy.com.pl/hpeciai/4832a5f46043f30c243548e5e0270043/pol_pl_Firewall-Fortinet-FortiGate-90G-17307_1.jpg dostęp 10.05.2024

1.4. Elementy wspólne

Do elementów wspólnych wymienionych rozwiązań zaliczyć możemy:

- Bezpieczeństwo: Wszystkie trzy rozwiązania kładą duży nacisk na bezpieczeństwo sieci i oferują produkty do ochrony przed zagrożeniami.
- Sieci bezprzewodowe: Zarówno Cisco, jak i Fortinet oferują rozwiązania do budowy i zarządzania sieciami Wi-Fi.
- Zarządzanie siecią: Cisco DNA i FortiManager umożliwiają zaawansowane zarządzanie sieciami.

1.5. Różnice

Rozwiązania te różnią się od siebie w następujących aspektach:

- Zasięg usług: Microsoft Azure koncentruje się na usługach chmurowych, takich jak wirtualne sieci i równoważenie obciążenia, podczas gdy Cisco i Fortinet oferują bardziej tradycyjne rozwiązania sieciowe i bezpieczeństwa sprzętowego.
- Integracja komunikacji: Cisco wyróżnia się rozwiązaniami do telefonii IP, czego brakuje w ofercie Microsoft Azure i Fortinet.
- Specjalizacja: Fortinet jest silnie skoncentrowany na bezpieczeństwie, oferując szczegółowe narzędzia do analizy zagrożeń i zarządzania urządzeniami bezpieczeństwa, podczas gdy Cisco i Azure oferują bardziej wszechstronne rozwiązania.

1.6. Wady i zalety przedstawionych rozwiązań

1.6.1. Cisco Network Solutions

- Zalety: Wszechstronność, zaawansowane zarządzanie siecią, silne funkcje bezpieczeństwa.
- Wady: Może być kosztowne, skomplikowane do wdrożenia i zarządzania w mniejszych organizacjach

1.6.2. Microsoft Azure

- Zalety: Elastyczność chmury, łatwość skalowania, szeroki zakres usług chmurowych
- Wady: Może być zależne od połączenia internetowego, złożoność zarządzania dużymi infrastrukturami

1.6.3. Fortinet

- Zalety: Silne skupienie na bezpieczeństwie, zaawansowane narzędzia analizy i zarządzania
- Wady: Może być mniej wszechstronne niż rozwiązania oferujące pełne zarządzanie siecią i usługi chmurowe

2. Wymagania funkcjonalne oraz нефункционалне

2.1. Zarys projektu

Głównym celem pracy jest opracowanie kompleksowego projektu sieci komputerowej dla firmy, uwzględniającego zarówno aspekty funkcjonalne, jak i нефункционалне, z wykorzystaniem narzędzia Packet Tracer. Projekt ma za zadanie sprostać potrzebom różnych działów wewnątrz organizacji oraz zapewnić bezpieczny, wydajny i skalowalny dostęp do zasobów sieciowych.

2.2. Zakres pracy

W ramach projektu, zakres pracy obejmie analizę wymagań, wybór odpowiednich technologii oraz opracowanie w pełni funkcjonalnej sieci komputerowej dla przedsiębiorstwa. Koncentracja na tych kluczowych etapach umożliwi sprawną późniejszą implementację, testy funkcjonalności i dostarczy skutecznego oraz spersonalizowanego rozwiązania dla firmy.

1. Projektowanie topologii sieciowej dla firmy

Opracowanie planu topologii sieciowej uwzględniającej strukturę organizacyjną firmy oraz potrzeby poszczególnych działów.

2. Konfigurację urządzeń sieciowych w narzędziu Packet Tracer

Przeprowadzenie konfiguracji poszczególnych urządzeń sieciowych, takich jak serwery, przełączniki, routery oraz komputery, zgodnie z projektem topologii.

3. Implementację zabezpieczeń sieciowych w narzędziu Packet Tracer

Wdrożenie zabezpieczeń sieciowych, takich jak firewall, filtrowanie adresów MAC/IP oraz autoryzacja dostępu, przy użyciu funkcji dostępnych w narzędziu Packet Tracer.

4. Testowanie działania sieci w narzędziu Packet Tracer

Przeprowadzenie testów działania sieci w narzędziu Packet Tracer w celu sprawdzenia poprawności konfiguracji oraz funkcjonalności zaprojektowanej sieci.

5. Diagnozowanie ewentualnych problemów w narzędziu Packet Tracer

Identyfikacja i diagnozowanie ewentualnych problemów związanych z działaniem sieci w narzędziu Packet Tracer oraz proponowanie rozwiązań naprawczych.

2.3. Założenia funkcjonalne i нефункционалне

Oto przykładowe założenia funkcjonalne i нефункционалне dla sieci komputerowej dla firmy.

2.3.1. Funkcjonalne

- Możliwość komunikacji między wszystkimi działami firmy
- Zapewnienie bezpiecznego dostępu do zasobów sieciowych poprzez autoryzację i uwierzytelnienie
- Implementacja sieci VPN dla zdalnego dostępu pracowników spoza firmy

2.3.2. Niefunkcjonalne

- Wysoka dostępność sieci - minimalizacja przestojów i awarii.
- Optymalna przepustowość sieci, aby zapewnić płynną komunikację i przesyłanie danych
- Niskie opóźnienia sieciowe dla aplikacji wymagających szybkiej odpowiedzi, takich jak wideokonferencje czy transmisje strumieniowe

2.4. Opis wykorzystywanych technologii

W ramach tego punktu omówimy technologie i narzędzia, które zostaną wykorzystane w projekcie sieci komputerowej dla firmy, z uwzględnieniem ich implementacji w narzędziu Cisco Packet Tracer.

2.4.1. Wybrane technologie

- **Cisco Packet Tracer:** Cisco Packet Tracer jest potężnym narzędziem symulacyjnym stworzonym przez Cisco, które umożliwia

użytkownikom projektowanie, konfigurowanie i testowanie sieci komputerowych w wirtualnym środowisku. Narzędzie to jest szeroko stosowane w edukacji oraz przez profesjonalistów IT do ćwiczeń praktycznych, przygotowywania do certyfikacji oraz symulowania rzeczywistych scenariuszy sieciowych bez konieczności inwestowania w drogi sprzęt.

- **Router Cisco:** Router Cisco będzie stanowił główny punkt dostępu do sieci firmy. Zapewni on routowanie pakietów między różnymi podsieciami oraz dostęp do Internetu.
- **Switch Cisco:** W projekcie zostaną wykorzystane przełączniki Cisco do połączenia wszystkich komputerów i urządzeń wewnątrz sieci firmy. Switch umożliwi przesyłanie danych w obrębie lokalnej sieci LAN.
- **Komputery klienckie:** Komputery klienckie będą stanowić stanowiska pracy pracowników firmy. Będą one wyposażone w system operacyjny Windows i umożliwią użytkownikom dostęp do zasobów sieciowych.
- **Serwer DHCP:** Serwer DHCP (Dynamic Host Configuration Protocol) zostanie skonfigurowany w celu dynamicznego przydzielania adresów IP komputerom w sieci lokalnej. Umożliwi to automatyczne konfigurowanie adresów IP, bramek domyślnych i innych parametrów sieciowych.
- **Protokół VLAN:** W celu segmentacji sieci i zapewnienia większego bezpieczeństwa zostaną wykorzystane wirtualne sieci LAN (VLAN). Dzięki nim możliwe będzie logiczne dzielenie sieci na mniejsze, niezależne podsieci.

2.4.2. Zastosowanie Packet Tracer w projekcie

W kontekście projektu "Projektowanie i implementacja sieci przedsiębiorstwa z wykorzystaniem narzędzia Packet Tracer", narzędzie to będzie pełniło kilka kluczowych funkcji:

- **Projektowanie topologii sieci:** Packet Tracer umożliwia wizualne zaprojektowanie topologii sieci przedsiębiorstwa. Dzięki temu możemy w prosty sposób zrozumieć i przedstawić strukturę sieci, jak również zobaczyć, jak poszczególne urządzenia są ze sobą połączone.
- **Konfiguracja urządzeń sieciowych:** Narzędzie to pozwala na konfigurację różnorodnych urządzeń sieciowych, takich jak routery, przełączniki, komputery i serwery. W projekcie zostaną skonfigurowane urządzenia, takie jak router Cisco ISR4321, przełączniki Cisco Catalyst 2960.

- **Implementacja zabezpieczeń sieciowych:** Packet Tracer umożliwia wdrożenie i przetestowanie różnych mechanizmów zabezpieczeń sieciowych takich jak konfiguracja VLAN-ów.
- **Testowanie działania sieci:** Narzędzie pozwala na symulację ruchu sieciowego oraz testowanie funkcjonalności sieci. Możemy monitorować przepływ pakietów, diagnozować problemy i sprawdzać, czy sieć działa zgodnie z oczekiwaniami.

2.4.3. Korzyści z wykorzystania narzędzia Cisco Packet Tracer

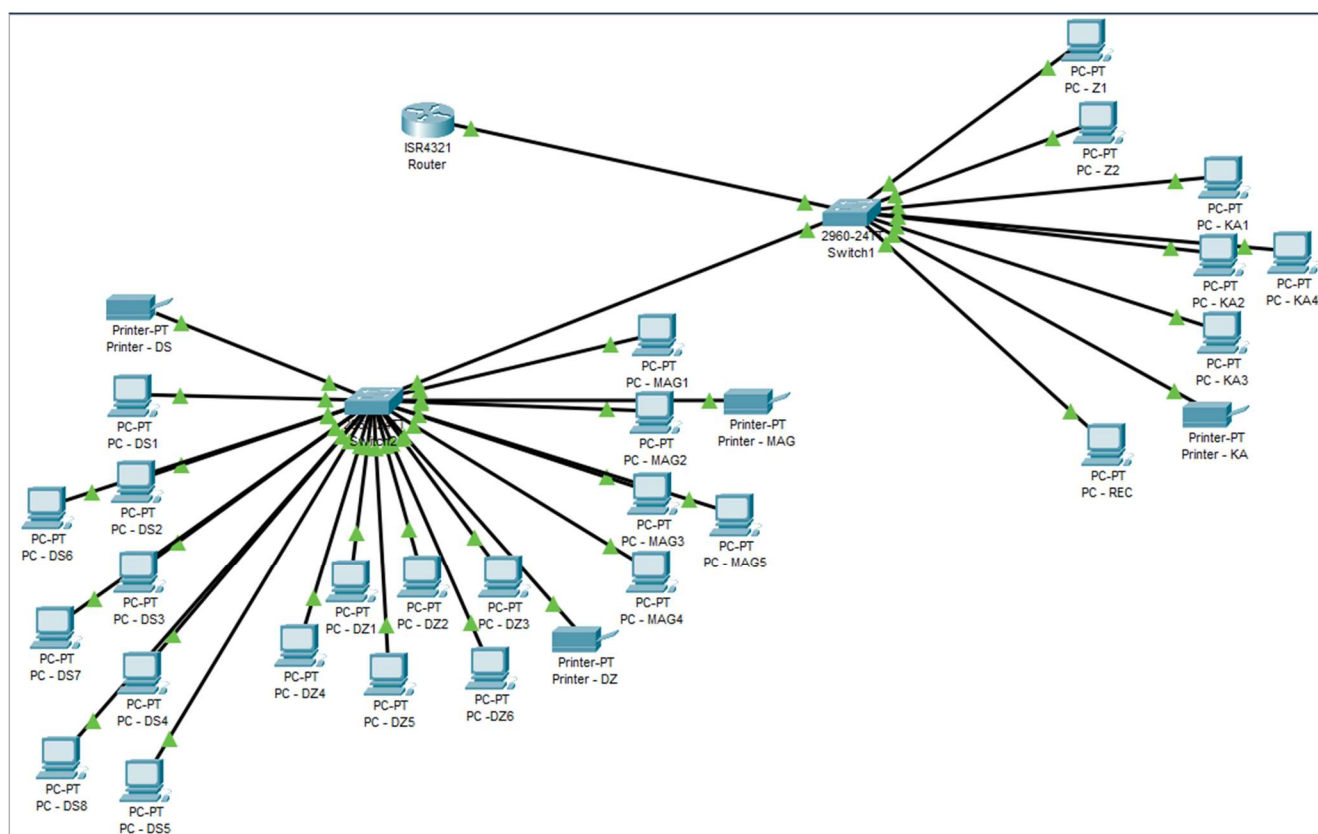
- **Oszczędność kosztów:** Brak konieczności zakupu drogiego sprzętu sieciowego do celów edukacyjnych i testowych.
- **Bezpieczeństwo:** Możliwość testowania różnych konfiguracji i scenariuszy bez ryzyka zakłócenia działania rzeczywistej sieci.
- **Elastyczność:** Łatwość w modyfikowaniu topologii i konfiguracji w celu dostosowania do zmieniających się wymagań i potrzeb projektu.
- **Praktyczne doświadczenie:** Użytkownicy mogą zdobyć cenne doświadczenie praktyczne, które jest trudne do uzyskania w czysto teoretycznych warunkach.

3. Implementacja sieci

3.1. Projekt topologii sieci

W tym punkcie przedstawię graficznie topologie sieci zaimplementowaną w narzędziu Packet Tracer oraz rozpisze podział komputerów, które należą do jakiego działu.

Rys. 4. Topologia sieci



Źródło: Opracowanie własne

Tab. 1. Urządzenia

Zarząd	Recepcja	Księgowość i Administracja	Dział sprzedaży
PC - Z1	PC - REC	PC - KA1	PC - DS1
PC - Z2		PC - KA2	PC - DS2
		PC - KA3	PC - DS3
		PC - KA4	PC - DS4
		PC - KA5	PC - DS5
Magazyn	Dział zakupów	Drukarki	PC - DS6
PC - MAG1	PC - DZ1	Printer - DS	PC - DS7
PC - MAG2	PC - DZ2	Printer - DZ	PC - DS8
PC - MAG3	PC - DZ3	Printer - KA	
PC - MAG4	PC - DZ4	Printer - MAG	
PC - MAG5	PC - DZ5		
	PC - DZ6		

Źródło: Opracowanie własne

Tab. 2. Rozpiska VLAN z adresacją

VLAN	NR	Nazwa	Switch	Adresacja	Porty
	VLAN10	Zarząd	Switch1	192.168.10.0	FE0/1 - FE0/5
	VLAN20	Księgowosc	Switch1	192.168.20.0	FE0/6 - FE0/14
	VLAN30	Recepcja	Switch1	192.168.30.0	FE0/15 - FE0/19
	VLAN40	Sprzedaz	Switch2	192.168.40.0	FE0/1 - FE0/9
	VLAN50	Zakupy	Switch2	192.168.50.0	FE0/11 - FE0/17
	VLAN60	Magazyn	Switch2	192.168.60.0	FE0/19 - FE0/23
	VLAN70	Drukarki	Switch1	192.168.70.0	FE0/20 - FE0/24
	VLAN70	Drukarki	Switch2	192.168.70.0	FE0/9, FE0/18, FE0/24

Źródło: Opracowanie własne

3.2. Konfiguracja urządzeń sieciowych w Packet Tracerze

3.2.1. Konfiguracja routera Cisco ISR4321

W tym kroku przedstawię konfigurację sieciową routera.

Rys. 5. Router Cisco ISR4321



Źródło: Opracowanie własne

- Konfigurujemy interfejs GigabitEthernet0/0/0 do którego będą podpięte pozostałe urządzenia sieciowe. Nadajemy mu adres sieciowy 192.168.1.1 i maskę podsieci 255.255.255.0.

Rys. 6. Konfiguracja interfejsu routera

The screenshot shows a web-based configuration interface for a router. The main window is titled "Router" and has tabs for "Physical", "Config", "CLI", and "Attributes". The "Config" tab is active, showing a tree view on the left with categories: GLOBAL (Settings, Algorithm Settings), ROUTING (Static, RIP), SWITCHING (VLAN Database), and INTERFACE (GigabitEthernet0/0/0, GigabitEthernet0/0/1). The "GigabitEthernet0/0/0" interface is selected, and its configuration is displayed on the right. The configuration includes: Port Status (On), Bandwidth (1000 Mbps), Duplex (Full Duplex), MAC Address (0001.6457.1201), IP Configuration (IPv4 Address: 192.168.1.1, Subnet Mask: 255.255.255.0), and Tx Ring Limit (10). Below the configuration fields, there is a section for "Equivalent IOS Commands" showing the following commands: Router(vlan)#, %SYS-5-CONFIG_I: Configured from console by console, Router(vlan)#exit, APPLY completed., Exiting..., Router#configure terminal, Enter configuration commands, one per line. End with CNTL/Z., Router(config)#interface GigabitEthernet0/0/1, Router(config-if)#, Router(config-if)#exit, Router(config)#interface GigabitEthernet0/0/0, and Router(config-if)#. At the bottom left, there is a "Top" button.

Router

Physical Config CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

SWITCHING

- VLAN Database

INTERFACE

- GigabitEthernet0/0/0
- GigabitEthernet0/0/1

GigabitEthernet0/0/0

Port Status ☒ On

Bandwidth ☒ 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0001.6457.1201

IP Configuration

IPv4 Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(vlan)#
%SYS-5-CONFIG_I: Configured from console by console

Router(vlan)#exit
APPLY completed.
Exiting....

Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

☐ Top

Źródło: Opracowanie własne

- Kolejnym krokiem będzie przypisanie interfejsów VLAN na routerze.

Rys. 7. Tworzenie interfejsów VLAN

```
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#description VLAN 10 Zarzad
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.20, changed state to up
encapsulation dot1Q 20
Router(config-subif)#
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#description VLAN 20 Ksiegowosc
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.30
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.30, changed state to up

Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#description VLAN 30 Recepcja
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.40
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.40, changed state to up

Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#description VLAN 40 Sprzedaz
Router(config-subif)#no shutdown
Router(config-subif)#exit

Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip address 192.168.50.1 255.255.255.0
Router(config-subif)#description VLAN 50 Zakupy
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.60
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.60, changed state to up

Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip address 192.168.60.1 255.255.255.0
Router(config-subif)#description VLAN 60 Magazyn
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface GigabitEthernet0/0/0.70
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0.70, changed state to up

Router(config-subif)#encapsulation dot1Q 70
Router(config-subif)#ip address 192.168.70.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#description VLAN 70 Drukarki
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

Źródło: Opracowanie własne

- Następnie skonfigurujemy serwer DHCP na routerze, który będzie nadawał odpowiednie adresy sieciowe dla każdego klienta podłączonego do odpowiedniego VLAN.

Rys. 8. Stworzenie serwera DHCP

```
Router>
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#exit
Router(config)#ip dhcp e
Router(config)#ip dhcp excluded-address 192.168.10.1
Router(config)#ip dhcp excluded-address 192.168.20.1
Router(config)#ip dhcp excluded-address 192.168.30.1
Router(config)#ip dhcp excluded-address 192.168.40.1
Router(config)#ip dhcp excluded-address 192.168.50.1
Router(config)#ip dhcp excluded-address 192.168.60.1
Router(config)#ip dhcp excluded-address 192.168.70.1
Router(config)#ip dhcp pool VLAN10_POOL
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#
```

Źródło: Opracowanie własne

Analogicznie tworzymy pule adresów dla pozostałych VLAN.

3.2.2. Konfiguracja przełączników Cisco Catalyst 2960

W tym projekcie do stworzenia sieci będą wymagane 2 switche Cisco, ze względu na ilość klientów w sieci. Na przełącznikach tych skonfigurowane zostaną VLAN, podzielone zostaną porty pod odpowiednie podsieci. Switche zostaną połączone w stack co zapewni wysoką przepustowość między nimi.

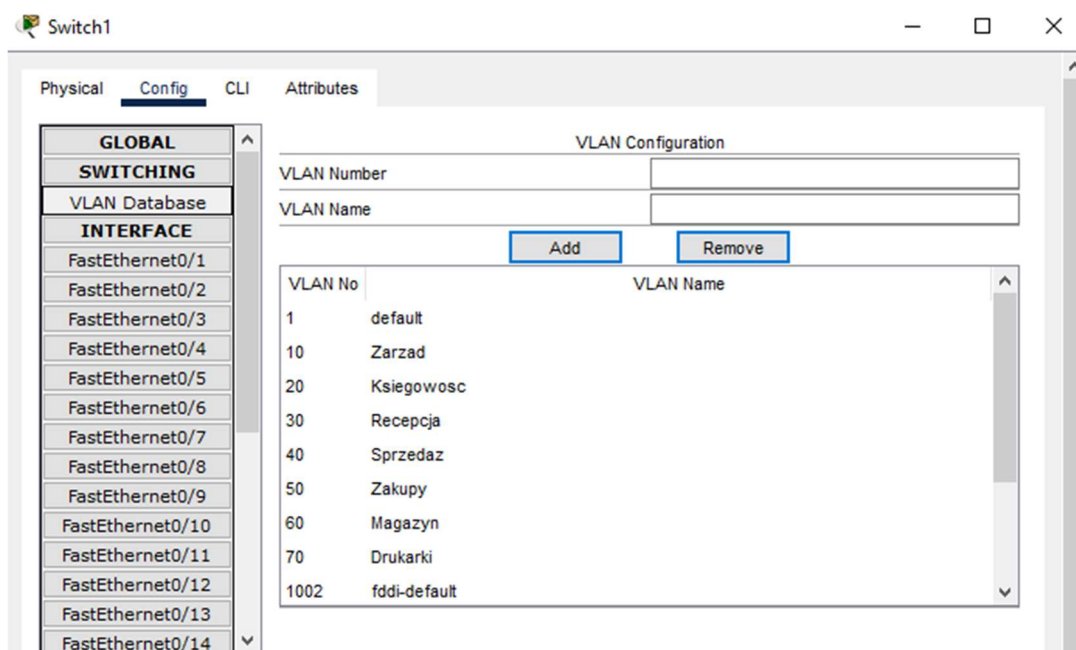
Rys. 9. Switch Cisco Catalyst 2960



Źródło: Opracowanie własne

- Na switchu nr 1 konfigurujemy VLAN i nadajemy im odpowiednie nazwy.

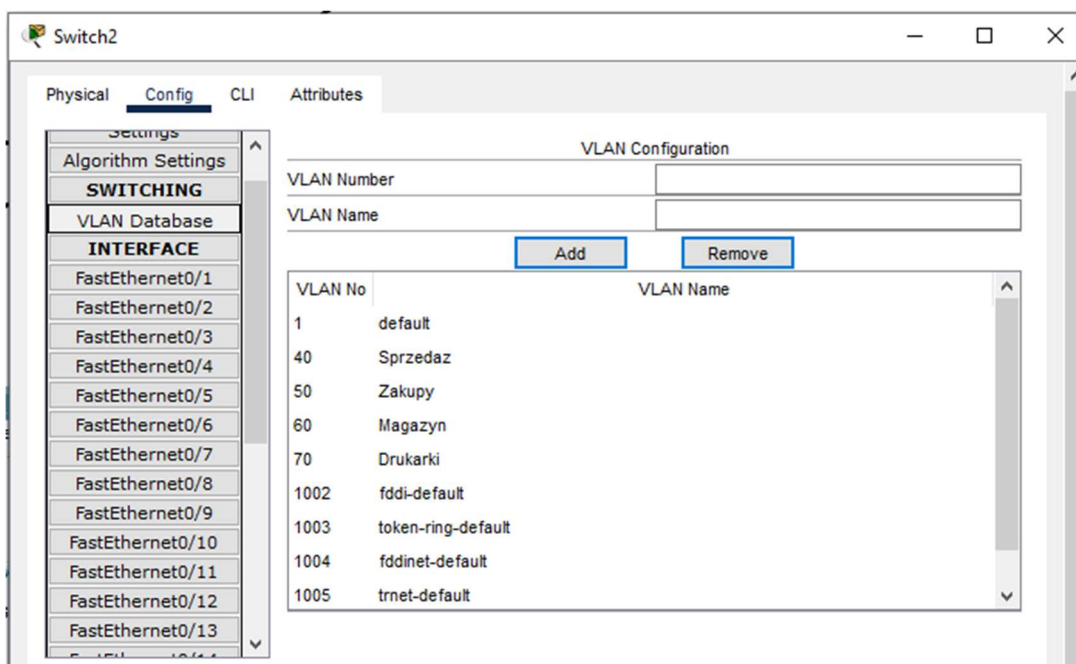
Rys. 10. VLAN switch1



Źródło: Opracowanie własne

- Analogicznie tworzymy VLAN na switchu nr 2 i nadajemy im odpowiednie nazwy. Na switchu nr 1 tworzymy wszystkie VLAN, ponieważ to on jest jako master w stacku i dzięki temu klienci podłączeni do switcha nr 2 dostaną odpowiednią adresację z serwera DHCP.

Rys. 11. VLAN switch2



Źródło: Opracowanie własne

- Kolejnym krokiem będzie przypisanie portów dla odpowiednich VLAN. Odpowiednie porty dla każdego VLAN zostały podane w tabeli Tab. 2. W tym

przypadku możemy zastosować polecenia w konsoli CLI, aby przypisać po kilka portów na raz.

Rys. 12. Przypisanie portów do odpowiednich VLAN na switch1

```
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/6-14
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/15-19
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/20-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 70
Switch(config-if-range)#exit
Switch(config)#
```

Źródło: Opracowanie własne

- Analogicznie wygląda to w przypadku switcha nr 2

Rys. 13. Przypisanie portów VLAN switch2

```
Switch2>enable
Switch2#conf term
Switch2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#interface range fastEthernet 0/1-9
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 40
Switch2(config-if-range)#exit
Switch2(config)#interface range fastEthernet 0/11-17
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 50
Switch2(config-if-range)#exit
Switch2(config)#interface range fastEthernet 0/19-23
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 60
Switch2(config-if-range)#exit
Switch2(config)#interface range fastEthernet 0/10, fastEthernet0/18, fastEthernet 0/24
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 70
Switch2(config-if-range)#exit
Switch2(config)#
```

Źródło: Opracowanie własne

- Celem zapisania konfiguracji stosujemy komendę: copy running-config startup-config.

Rys. 14. Zapisanie konfiguracji na przełączniku

```
Switch1>
Switch1>enable
Switch1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch1#
```

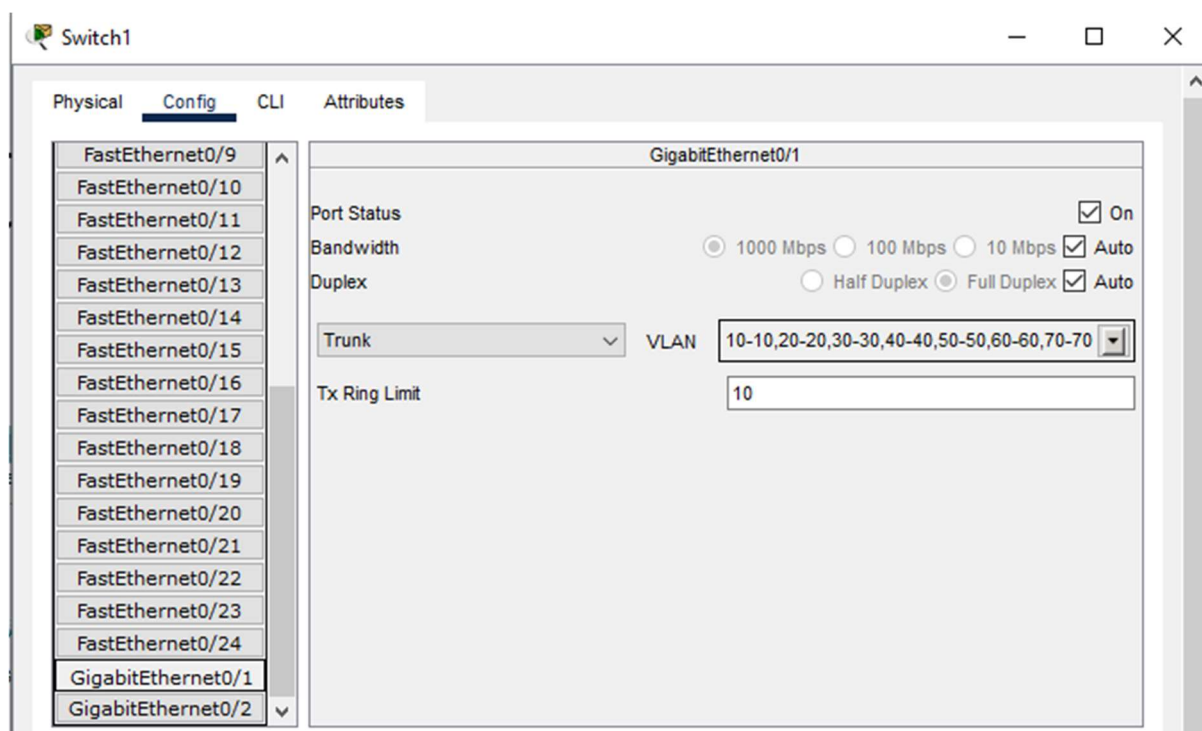
Źródło: Opracowanie własne

- Czynność tę powtarzamy na obu przełącznikach.

3.2.3. Konfiguracja ruchu sieciowego

Aby urządzenia podłączone do sieci dostały odpowiednie adresacje po podłączeniu się pod odpowiedni VLAN, musimy skonfigurować odpowiednio urządzenia. W tym celu musimy ustawić na przełącznikach protokół trunk. Aby to zrobić musimy przejść do konfiguracji switcha. Gdzie na odpowiednich interfejsach ustawiamy protokół trunk i odpowiadające mu VLAN.

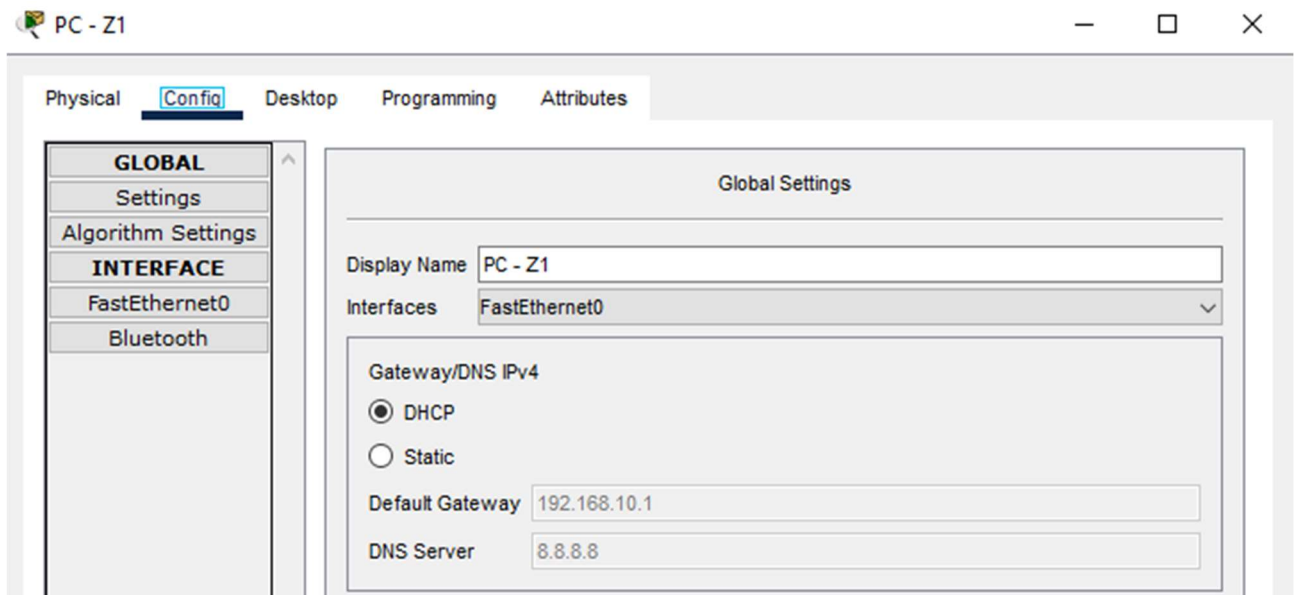
Rys. 15. Ustawienie protokołu trunk na switchu nr 1



Źródło: Opracowanie własne

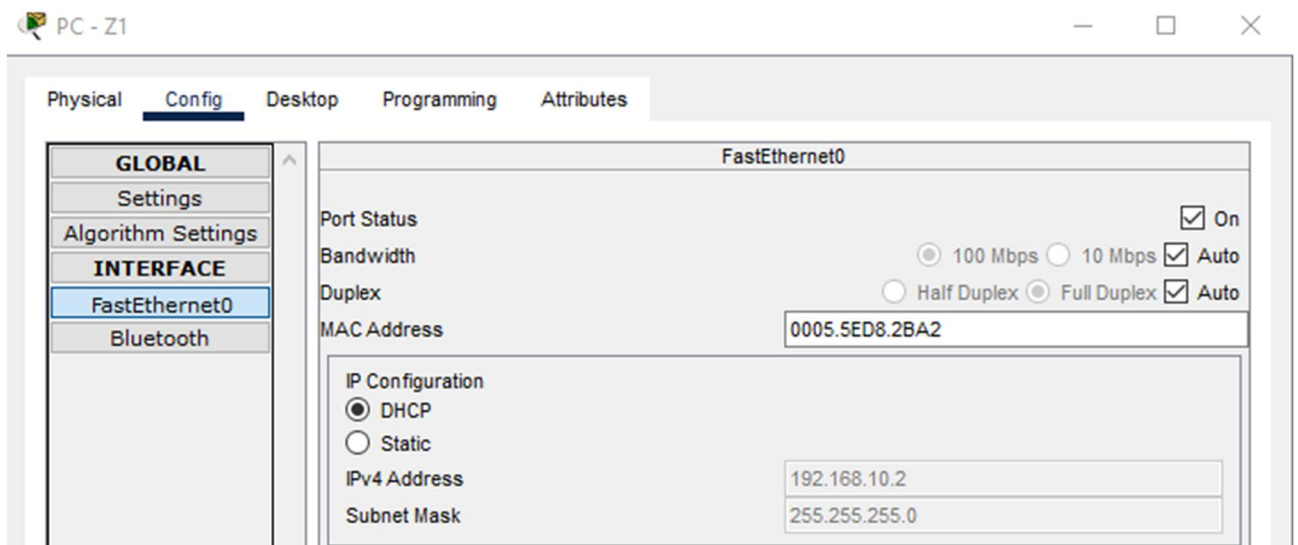
Analogicznie robimy to przypadku interfejsu do którego podłączony jest switch 2 i odpowiednio konfigurowujemy interfejs na switchu2. Po takim ustawieniu możemy zobaczyć, że urządzenia podpięte do sieci otrzymują odpowiednie adresacje odpowiadające danemu VLAN.

Rys. 16. Adresacja po DHCP dla PC - Z1



Źródło: Opracowanie własne

Rys. 17. Adresacja po DHCP dla PC -Z1



Źródło: Opracowanie własne

Niestety po tym zabiegu wszystkie VLAN są dla siebie widoczne, jesteśmy się w stanie dostać z jednej podsieci do drugiej. Aby temu zapobiec musimy na routerze skonfigurować Access Control List. Robimy to w następujący sposób.

Rys. 18. Konfiguracja ACL na routerze

```
Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g
Router(config)#ip
Router(config)#ip ac
Router(config)#ip access-list ex
Router(config)#ip access-list extended BL
Router(config)#ip access-list extended BLOCK_VLANS
Router(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
Router(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
```

Źródło: Opracowanie własne

Dodatkowo stosujemy ACL dla subinterfejsów VLAN na routerze.

Rys. 19. Konfiguracja ACL dla subinterfejsów routera

```
Router(config)#interface gigabitEthernet 0/0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#interface gigabitEthernet 0/0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#interface gigabitEthernet 0/0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#interface gigabitEthernet 0/0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#interface gigabitEthernet 0/0/0.50
Router(config-subif)#interface gigabitEthernet 0/0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#interface gigabitEthernet 0/0/0.50
Router(config-subif)#encapsulation dot1Q 50
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#interface gigabitEthernet 0/0/0.60
Router(config-subif)#encapsulation dot1Q 60
Router(config-subif)#ip access-group BLOCK_VLANS in
Router(config-subif)#
```

Źródło: Opracowanie własne

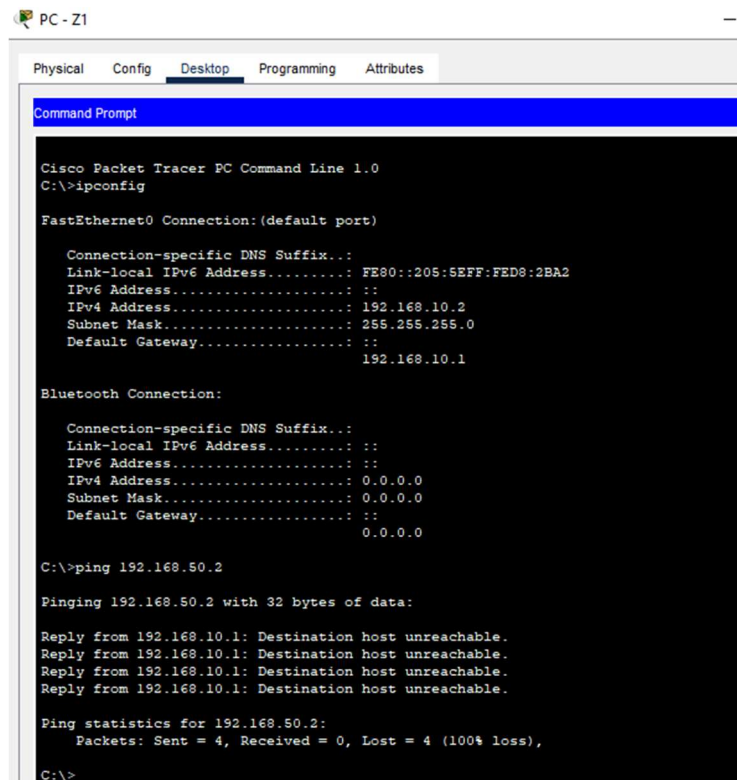
Kroki te powtarzamy dla każdej podsieci poza VLAN 70, ponieważ jest to VLAN przygotowany dla drukarek i każdy użytkownik sieci musi mieć dostęp do tych urządzeń.

4. Testy

Celem tej części projektu jest przeprowadzenie testów celem sprawdzenia czy nasza sieć działa w sposób taki jak byśmy tego oczekiwali. Testy przeprowadzę w sposób następujący:

- Urządzenia, które są podłączone np. do VLAN10 nie mogą się komunikować z urządzeniami podłączonymi do VLAN 50.

Rys. 20. Test z VLAN10 do VLAN50



```
PC - Z1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::205:5EFF:FED8:2BA2
IPv6 Address...: ::
IPv4 Address...: 192.168.10.2
Subnet Mask...: 255.255.255.0
Default Gateway...: 192.168.10.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address...: ::
IPv6 Address...: ::
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...: 0.0.0.0

C:\>ping 192.168.50.2

Pinging 192.168.50.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

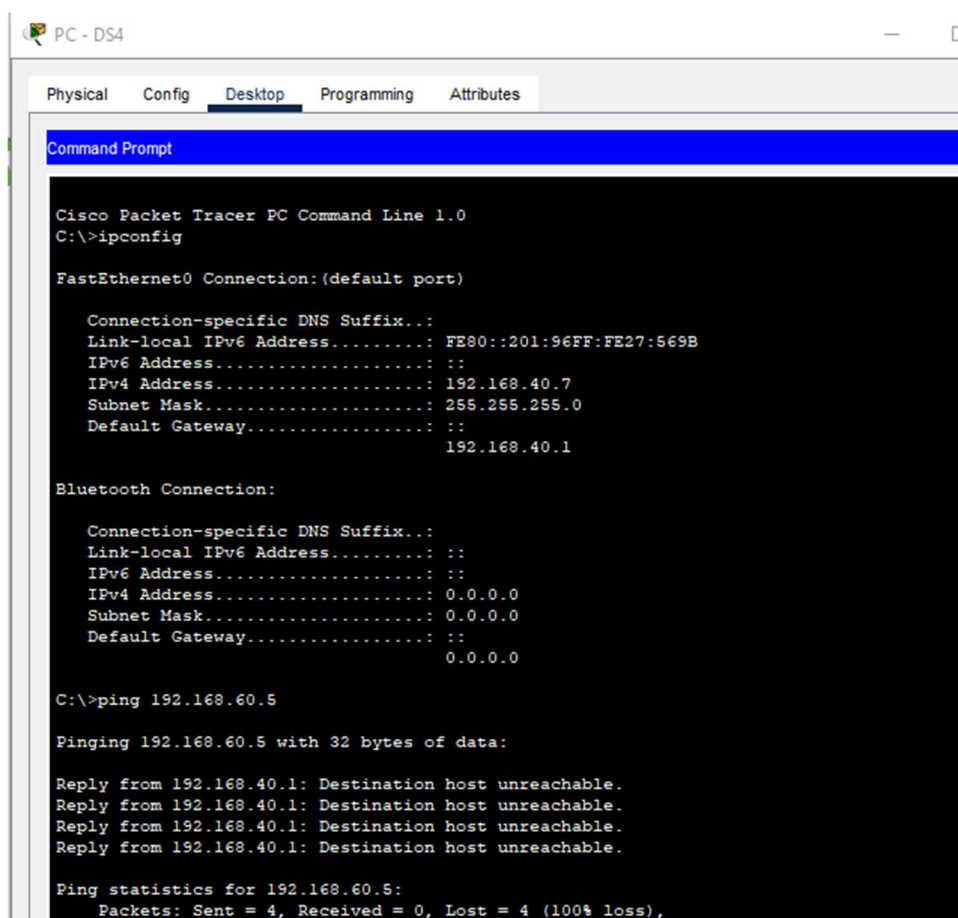
Ping statistics for 192.168.50.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

Źródło: Opracowanie własne

Jak możemy zauważyć urządzenia te nie komunikują się między sobą.

- Kolejnym testem będzie próba puszczenia pinga z urządzeń podłączonych do jednego switcha w tym wypadku będzie to switch nr 2. Spróbujemy puścić ping z VLAN40 do VLAN60.

Rys. 21. Test z VLAN40 do VLAN60



```
PC - DS4
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::201:96FF:FE27:569B
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.40.7
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.40.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 192.168.60.5

Pinging 192.168.60.5 with 32 bytes of data:

Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.
Reply from 192.168.40.1: Destination host unreachable.

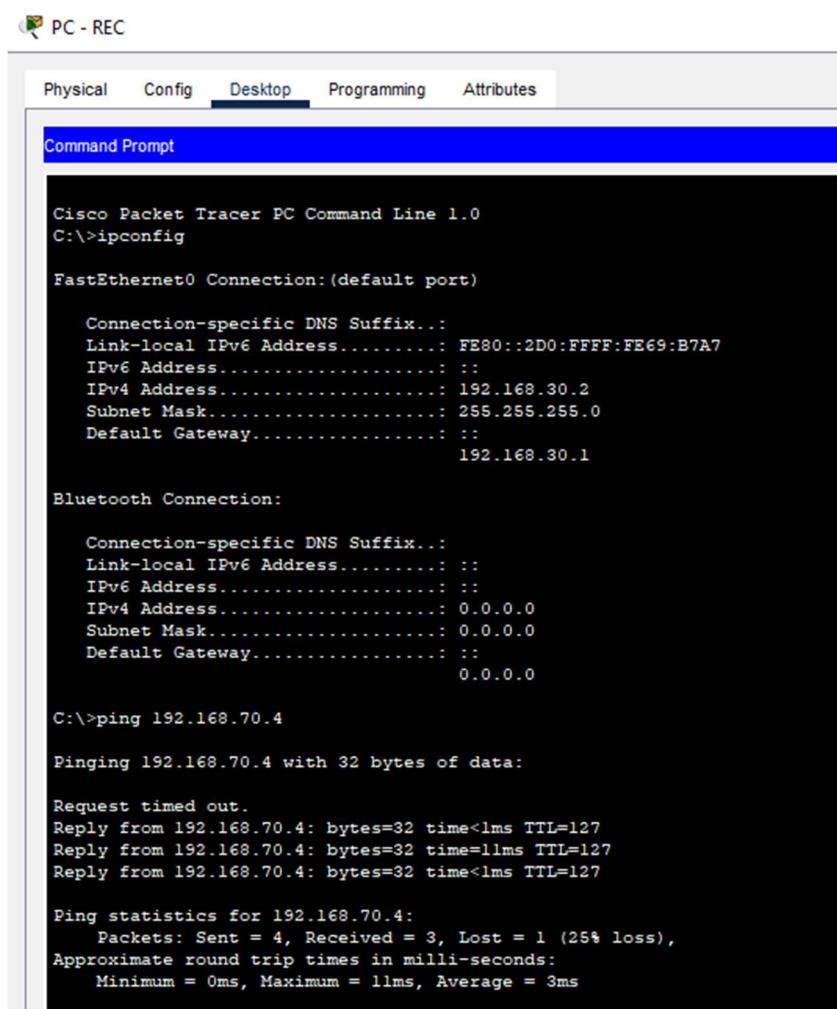
Ping statistics for 192.168.60.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Źródło: Opracowanie własne

W tym przypadku tak samo możemy zauważyć, że urządzenia się nie komunikują.

- Następnym testem będzie próba dostania się z VLAN 30 do VLAN 70. W tym przypadku urządzenia powinny się odnaleźć w sieci bo według założeń VLAN70 ma być ogólnie dostępny dla wszystkich urządzeń w sieci.

Rys. 22. Test VLAN30 do VLAN70



```
PC - REC

Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:FFFF:FE69:B7A7
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.30.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.168.30.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ping 192.168.70.4

Pinging 192.168.70.4 with 32 bytes of data:

Request timed out.
Reply from 192.168.70.4: bytes=32 time<1ms TTL=127
Reply from 192.168.70.4: bytes=32 time=11ms TTL=127
Reply from 192.168.70.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.70.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms
```

Źródło: Opracowanie własne

W tym przypadku widzimy, że próba puszczenia pingu się powiodła, więc zgodnie z założeniami sieć została skonfigurowana poprawnie.

5. Podsumowanie

Projektowanie i implementacja sieci przedsiębiorstwa z wykorzystaniem narzędzia Packet Tracer pozwala na dokładne zaplanowanie i symulację różnych rozwiązań sieciowych przed ich wdrożeniem w rzeczywistym środowisku. Przeanalizowane rozwiązania - Cisco Network Solutions, Microsoft Azure oraz Fortinet - dostarczają różnorodnych opcji, które różnią się pod względem funkcjonalności, kosztów i stopnia skomplikowania.

Cisco Network Solutions oferują kompleksowe i skalowalne rozwiązania, które są jednak kosztowne i wymagają zaawansowanej wiedzy technicznej. Microsoft Azure dostarcza elastycznych i skalowalnych rozwiązań chmurowych, które integrują się z istniejącymi systemami IT, ale mogą wiązać się z obawami dotyczącymi bezpieczeństwa i

zgodności. Fortinet skupia się na bezpieczeństwie sieci, oferując zintegrowane rozwiązania, które są efektywne kosztowo, lecz mogą wymagać dodatkowej konfiguracji.

Wymagania funkcjonalne i нефункционалне sieci przedsiębiorstwa obejmują nie tylko podstawowe potrzeby dotyczące łączności i dostępności, ale także zaawansowane wymagania bezpieczeństwa, zarządzania i skalowalności. Projektowanie sieci z wykorzystaniem Packet Tracer umożliwia uwzględnienie tych wymagań, a także przeprowadzenie symulacji różnych scenariuszy i konfiguracji, co pomaga w identyfikacji potencjalnych problemów i optymalizacji wydajności sieci.

Całościowo, implementacja sieci przedsiębiorstwa z wykorzystaniem narzędzia Packet Tracer stanowi istotny krok w kierunku stworzenia bezpiecznego, wydajnego i skalowalnego środowiska IT, które może sprostać współczesnym wymaganiom biznesowym.

Spis literatury

- [1] https://www.cisco.com/c/pl_pl/products/index.html#~products-by-technology, 10.05.2024.
- [2] <https://pl.linkedin.com/pulse/microsoft-azure-czy-i-kiedy-warto-skorzyst%C4%87-tomasz-wieczorkowski>, 10.05.2024.
- [3] <https://www.fortinet.com/>, 10.05.2024.
- [4] <https://tutorials.ptnetacad.net/>, 18.06.2024
- [5] <https://www.nastykusieci.pl/konfiguracja-vlanow/>, 20.06.2024