

SPRAWOZDANIE z ETAPU PROJEKTU
z przedmiotu „Projektowanie i obsługa sieci komputerowych I”

Data wykonania ćwiczenia:

11.01.2023

Rok studiów:

III

Semestr:

5.

Grupa studencka:

1b

Temat: **Dokumentacja projektu**

Osoby wykonujące ćwiczenia:

**Patrycja Kubica
Kamila Kmieciak
Oskar Walaszczyk
Dawid Waluszek
Artur Zelek**

Katedra Informatyki i Automatyki

1. Zrozumienie wymagań

TechMach to firma specjalizująca się w produkcji wysokiej jakości części mechanicznych o precyzyjnych parametrach, z zastosowaniem w różnych sektorach przemysłu, w tym w branżach motoryzacyjnej i lotniczej. W kontekście jej aktywności, istnieje konieczność stworzenia stabilnej i niezawodnej sieci LAN, która pozwoli na pełną kontrolę nad procesem produkcyjnym oraz skuteczne zarządzanie obszerną bazą danych produktów.

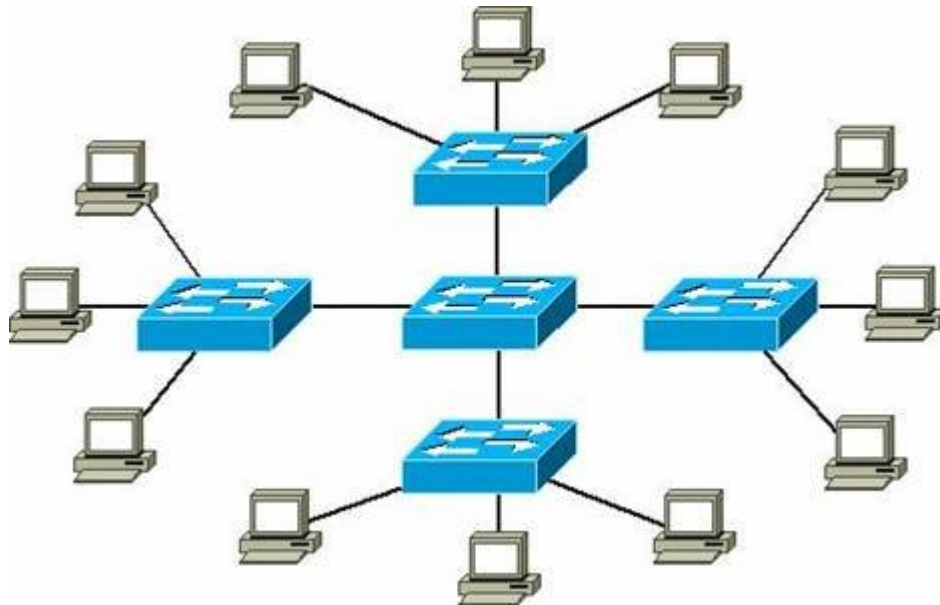
- A. Liczba pracowników wynosi 50 osób.
- B. Liczba urządzeń, które muszą być obsługiwane przez sieć, to 60 elementów, w tym:
 - a. Maszyny CNC: W firmie dostępne są co najmniej kilka maszyn CNC, które pełnią kluczową rolę w produkcji precyzyjnych komponentów mechanicznych. Sieć będzie integrować te maszyny, umożliwiając bieżący monitoring ich pracy, efektywne przesyłanie programów sterujących oraz zbieranie istotnych danych produkcyjnych.
 - b. Komputery biurowe: Niezbędne jest obsługiwane komputerów biurowych, które pracownicy wykorzystują do przetwarzania dokumentów, zarządzania bazą danych produktów, komunikacji e-mailowej oraz wykonywania innych rutynowych zadań biurowych.
- C. Rodzaje usług, jakie musi dostarczać sieć, obejmują:
 - a. Zabezpieczenia sieci: W związku z koniecznością ochrony danych produkcyjnych i informacji korporacyjnych, niezbędne jest zainwestowanie w odpowiednie środki zabezpieczające sieć przed dostępem nieuprawnionych osób.
 - b. Monitorowanie maszyn produkcyjnych: Sieć musi gwarantować ciągły dostęp do monitoringu pracy maszyn CNC w czasie rzeczywistym, zbieranie danych produkcyjnych, identyfikację potencjalnych problemów oraz zdalne zarządzanie nimi.
 - c. Zarządzanie bazą danych produktów: Firma potrzebuje sieci, która umożliwia efektywny dostęp do centralnej bazy danych produktów, zawierającej kompleksowe informacje na temat części mechanicznych, ich parametrów, historii produkcji, dostawców oraz innych kluczowych danych. Wartość dostępu do tej bazy danych musi być dostępna dla pracowników biurowych.
 - d. Komunikacja wewnętrzna: Sieć powinna być wyposażona w narzędzia ułatwiające komunikację wewnętrzną między pracownikami firmy, umożliwiając swobodną wymianę informacji, plików oraz komunikację e-mailową.

Firma "TechMach" potrzebuje zaawansowanej i niezawodnej sieci LAN, która sprosta wyzwaniom związanym z obsługą 50 pracowników i 60 urządzeń, w tym maszyn CNC i komputerów biurowych. Sieć musi umożliwiać ciągłe monitorowanie maszyn produkcyjnych, efektywne zarządzanie bazą danych produktów, skuteczną komunikację wewnętrzną oraz zapewniać najwyższe standardy zabezpieczeń danych.

2. Wybór topologii sieci

W kontekście przedsiębiorstwa "TechMach", które specjalizuje się w wytwarzaniu dokładnych komponentów mechanicznych, kluczowym krokiem w jego operacjach jest wybór właściwego układu sieci LAN. Ten wybór ma na celu sprostanie specyficznym wymaganiom firmy, takim jak pewność działania, zdolność do zapewnienia zduplikowanych rozwiązań oraz efektywność.

Wybrana topologia sieci: **ROZSZERZONA GWIAZDA**



Rys. 1. Przykładowy układ topologii rozszerzonej gwiazdy

Należy podkreślić, że "Rozszerzona Gwiazda" wprowadza znaczną redundancję, co jest najważniejsze w przypadku firmy produkcyjnej, gdzie każda chwila przestoju może oznaczać znaczące straty finansowe. Niemniej jednak, równie ważnym aspektem jest inwestycja w odpowiednie środki zabezpieczeń i monitorowania, które pomogą w minimalizacji ryzyka awarii i zagrożeń sieciowych. Dlatego wybór topologii "Rozszerzonej Gwiazdy" jest najlepszym rozwiązaniem dla firmy "TechMach."

W celu obiektywnego ocenienia prawidłowości dobranej topologii, przeprowadzono analizę wad i zalet proponowanego rozwiązania:

A. **Wydajność**

PLUS: Szybki i efektywny przepływ danych.

MINUS: Wymaga więcej kabli i zarządzania w porównaniu do topologii gwiazdy.

B. **Redundancja**

PLUS: Wysoka odporność na awarie.

MINUS: Wymaga dodatkowych centralnych punktów i zapasowych połączeń, co może zwiększyć koszty.

C. **Skalowalność**

PLUS: Łatwe rozszerzanie sieci w miarę rozwoju firmy.

MINUS: W przypadku znacznego rozwoju firmy, może wymagać zmian w infrastrukturze.

D. Ochrona danych

PLUS: Wysoki poziom bezpieczeństwa i kontroli dostępu.

MINUS: Wymaga inwestycji w odpowiednie środki zabezpieczeń.

E. Monitorowanie

PLUS: Możliwość ciągłego monitorowania w czasie rzeczywistym.

MINUS: Wymaga dedykowanego sprzętu i oprogramowania monitorującego.

F. Komunikacja wewnętrzna

PLUS: Ułatwiona komunikacja między pracownikami.

MINUS: Wymaga odpowiedniego zarządzania, aby uniknąć zagrożeń związanych z nadmierną komunikacją.

Podsumowanie rozważań zawarto w poniższej Tabeli.1.

Efektywność	Ta konfiguracja sieci łączy korzyści tradycyjnej topologii gwiazdy, gdzie każde urządzenie jest bezpośrednio skomunikowane z centralnym punktem zarządzania siecią . W ten sposób zachowany jest szybki i efektywny przepływ danych, co ma kluczowe znaczenie w produkcji części o tak szczególnych parametrach.
Skalowalność	Konfiguracja "Rozszerzonej Gwiazdy" jest elastyczna i pozwala na łatwe rozszerzanie sieci w miarę rozwoju firmy , bez konieczności znaczących zmian w infrastrukturze.
Zapewnienie ciągłości działania	Zdolność do obsługi sytuacji awaryjnych. Dzięki dodatkowym centralnym punktom lub alternatywnym połączeniom, firma może skutecznie minimalizować zakłócenia w pracy w przypadku uszkodzenia jednego z punktów centralnych.
Bezpieczeństwo danych	W obszarze produkcji mechanicznych komponentów, ochrona danych ma kluczowe znaczenie. Dzięki topologii "Rozszerzonej Gwiazdy," firma może skoncentrować się na zabezpieczeniach w głównym punkcie centralnym i jego zapasowych wersjach, co podnosi poziom ochrony danych korporacyjnych i produkcji.
Monitorowanie produkcji	Sieć w tej konfiguracji pozwala na ciągłe monitorowanie maszyn CNC w czasie rzeczywistym , co umożliwia dokładną kontrolę postępu produkcji, wczesne wykrywanie potencjalnych problemów oraz sprawną organizację procesów produkcyjnych.
Komunikacja w firmie	W kontekście tej topologii, komunikacja między pracownikami firmy jest ułatwiona oraz usprawniona, co sprzyja efektywnej wymianie informacji i skutecznej współpracy.

Tabela. 1. Rozważone aspekty podczas wyboru topologii

- A. **Wydajność:** Topologia "Rozszerzonej Gwiazdy" wyróżnia się nadzwyczajną efektywnością oraz **wydajnością**. Wszystkie urządzenia, w tym maszyny CNC oraz komputery biurowe, są bezpośrednio połączone z głównym punktem zarządzania siecią. Dzięki temu, przepływ danych jest ekspresowy, stabilny i niezakłócony.

W sektorze produkcji, gdzie czas często jest kluczowym aspektem, ta właściwość topologii "Rozszerzonej Gwiazdy" ma ogromne znaczenie, umożliwiając sprawną wymianę programów sterujących oraz zbieranie danych produkcyjnych w czasie rzeczywistym.

- B. **Redundancja:** Podobnie, jeśli chodzi o redundancję, "Rozszerzona Gwiazda" wyróżnia się zdolnością do obsługi awarii jako jednym z jej kluczowych atutów. Dodawanie zapasowych centralnych punktów lub połączeń pozwala firmie na kontynuowanie działalności w przypadku uszkodzenia jednego z punktów centralnych.

W dziedzinie produkcji, gdzie nawet krótka przerwa w pracy maszyn CNC może skutkować znacznymi stratami finansowymi, ta redundancja jest nieoceniona. Pomaga ona zminimalizować ryzyko przestojów i zapewnia ciągłość pracy, co jest niezmiernie istotne dla firmy "TechMach."

3. Wybór sprzętu sieciowego

- A. **Przełączniki (Switch):** Przełączniki sieciowe będą głównym urządzeniem zarządzającym ruchem w podsieciach LAN i komunikacją między nimi. Powinny one mieć odpowiednią liczbę portów, aby obsłużyć wszystkie urządzenia, w tym maszyny CNC i komputery biurowe. Przełączniki użyte w podsieciach z maszynami CNC, powinny obsługiwać ich zarządzanie i być w stanie zapewnić jakość usług (QoS), dla urządzeń które mogą wymagać priorytetowego przepływu danych.
- B. **Router/firewall:** Konieczne będzie urządzenie zapewniające dostęp do Internetu oraz zabezpieczenia sieci, takie jak zintegrowany router z funkcją firewalla. Warto również rozważyć urządzenie z możliwością wirtualnych sieci prywatnych (VPN) dla bezpiecznego zdalnego dostępu.
- C. **Serwer:** Serwer będzie potrzeby do stworzenia i zarządzania bazą danych produktów oraz uruchamiać oprogramowanie monitorujące maszyny produkcyjne.
- D. **Komputery wyposażone w karty sieciowe Ethernet:** Maszyny CNC i komputery biurowe powinny być wyposażone w odpowiednie karty sieciowe Ethernet lub przewody do podłączenia do przełącznika.

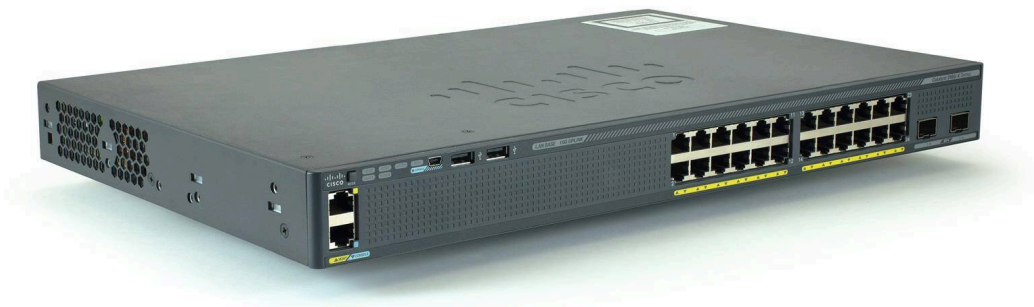
- E. **Zapaszowe zasilanie (UPS):** Aby zapewnić niezawodność sieci, warto zainstalować zasilanie bezprzerwowe (UPS), które zapewni zasilanie awaryjne w przypadku nagłego przerwania zasilania.
- F. **Zabezpieczenia sieciowe:** W zależności od funkcji komputera, powinien on mieć odpowiednie zabezpieczenia, takie jak zasady firewalla, oprogramowanie antywirusowe i inne środki bezpieczeństwa, aby chronić sieć przed zagrożeniami i blokować niepożądane osoby przed dostępem do informacji niejawnych.
- G. **Systemy kopii zapasowych:** Powinny być tworzone regularne kopie zapasowe danych firmowych i bazy danych produktów i przechowywane na odpowiednich urządzeniach lub w chmurze.
- H. **Okablowanie:** Kable muszą być wysokiej jakości, aby zapewnić szybką i niezawodną transmisję danych, a jednocześnie odporne na zakłócenia elektromagnetyczne.

Wybór modeli urządzeń do wykorzystania w firmie:

A. Switch - WS-C2960X-24PD-L

Do zrealizowania połączeń sieciowych w firmie będziemy potrzebować 3 switchy, które to pozwolą na rozdzielenie sieci między biurem, a halą produkcyjną. 2 z nich zostaną przeznaczone na urządzenia biurowe, a jeden na urządzenia hali produkcyjnej. Taka redundancja pozwoli uniknąć nam dużych awarii oraz szybko je naprawić.

Cena - 1 890 zł x 3 = 5 670 zł



Rys. 2. Switch WS-C2960X-24PD-L

<https://sklep.comel-it.com/pl/products/ws-c2960x-24td-l-switch-cisco-catalyst-2960x-10g-4417.html>

B. Router - ISR4451-X/K9

Dla tej firmy potrzeby jest router o wysokiej przepustowości oraz z wbudowanymi narzędziami ochrony sieci. Wysoko wydajny router z przepustowością nawet do 2Gbps jest potrzebny do stabilnego przesyłania i odbierania danych pracy urzędów.

Cena - 30000 zł



Rys. 3. Router ISR4451-X/K9

<https://www.router-switch.com/cisco-isr4451-x-k9-p-5293.html>

C. Serwer - HPE ProLiant DL380 Gen10 4214R 1P 32GB-R P408i-a NC 8SFF 800W PS Server

Cena - 15100 zł



Rys. 4. Serwer HPE ProLiant DL380

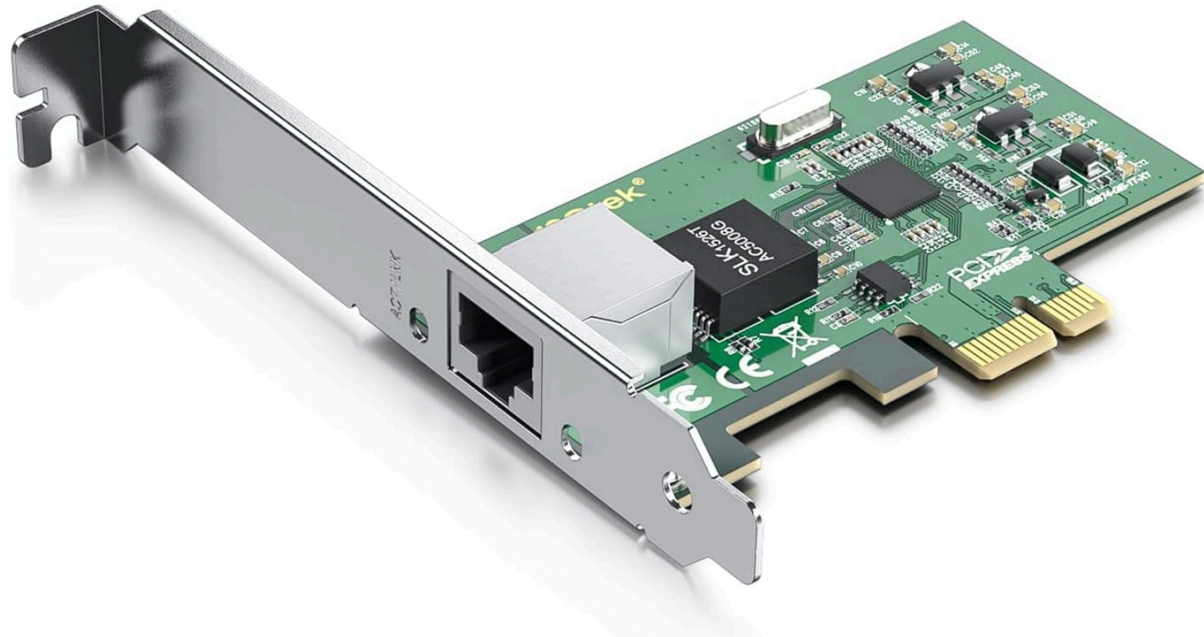
<https://buy.hpe.com/pl/en/compute/rack-servers/proliant-dl300-servers/proliant-dl380-server/hpe-proliant-dl380-gen10-4214r-1p-32gb-r-p408i-a-nc-8sff-800w-ps-server/p24842-b21>

D. Karty sieciowe - Intel Gigabit Ethernet Network Card

Możliwość podpięcia urządzenia będzie odbywała się za pomocą kabla typu skrętka, co powoduje, że każde takie urządzenie powinno mieć kartę sieciową z portem Ethernet.

Cena - 132 zł x 30 = 3960 zł

Wymagania - wolny port PCI w urządzeniu.



Rys. 5. Karta sieciowa Intel Gigabit Ethernet Network Card

<https://www.amazon.pl/1000Mbps-Gigabit-Ethernet-Converged-E1G42ET/dp/B01H6O7X0W?th=1>

E. Zasilacze UPS - APC Smart-UPS (1500VA/900W, 4x IEC, AVR, LCD, RACK)

Zasilacze zapasowe są kluczowe w utrzymaniu ciągłej pracy urządzeń sieciowych. Z powodu dużych wymagań wiatowych wybranych urządzeń będą nam potrzebne 2 UPSy.

Cena - 4780 zł x 2 = 9560 zł



Rys. 6. Zasilacz UPS APC Smart-UPS

<https://www.x-kom.pl/p/545949-zasilacz-awaryjny-ups-apc-smart-ups-1500va-900w-4x-iec-avr-lcd-rack.html>

F. ESET Protect Complete - Kompletna, wielowarstwowa ochrona stacji roboczych, aplikacji w chmurze i poczty e-mail - najważniejszego wektora zagrożeń



Rys. 7. Antywirus ESET Protect Complete

Antywirus w wykorzystaniu firmowym.

Cena - prosba o wycene dla danej firmy.

G. Okablowanie

W firmie glównym sposobem łaczenia urzadzén sieciowych będzie skrétka kategorii 7. Jest to skrétka bardzo odporna na zakłócenia oraz dzięki oplocie trudna do uszkodzania mechanicznego.

Cena - $4,23 \times 3000 \text{ mb} = 12690 \text{ zł}$

<https://www.speckable.pl/pl/product/60590,kabel-ftp-kat-7-s-ftp-4x2x0-57-b2ca-jasnoszary-l-soh-alantec> 3000mb

Inne kable - kable Console

Cena ok. 250zł

H. Inne

Szafa RACK - potrzebna do umieszczenia głównych urządzeń sieciowych

Cena - 1520 zł



Rys. 8. Szafa RACK stojąca

<https://szafyrack.pl/szafy-rack-stojace/1575-2111-sq6618-szafa-rack-19-szybkiego-montazu-600x600x18u.html#/311-kolor> [lista](#)
[punktowa-czarny/462-drzwi-szklane/465-wersja_lista_punktowa-szybki_montaz](#)

Akcesoria szafy RACK - suwnice, zaślepki itp.

Cena - ok. 1500 zł

I. Cena całkowita projektu

Lp.	Urządzenie	Ilość	Cena jednostkowa	Cena całkowita
1	Switch	3	1890	5670
2	Router	1	30000	30000
3	Serwer	1	15100	15100
4	Karta sieciowa	30	132	3960
5	UPS	2	4780	9560
6	Antywirus - licencja	1	1500	1500
7	Okablowanie	3000	4,23	12690
8	Okablowanie inne	1	250	250
9	Szafa RACK	1	1520	1520
10	Akcesoria szafy RACK	1	1500	1500
			SUMA:	81750

4. Projektowanie podsieci

A. Podsieć hali produkcyjnej

Lp.	Urządzenie	Interfejs	Adres IP	Maska podsieci	Switch
1	H-MaszynaCNC-1	karta sieciowa	192.168.10.10	255.255.255.0	Switch-1 (f/1)
2	H-MaszynaCNC-2	karta sieciowa	192.168.10.20	255.255.255.0	Switch-1 (f/2)
3	H-MaszynaCNC-3	karta sieciowa	192.168.10.30	255.255.255.0	Switch-1 (f/3)
4	H-MaszynaCNC-4	karta sieciowa	192.168.10.40	255.255.255.0	Switch-1 (f/4)
5	H-MaszynaCNC-5	karta sieciowa	192.168.10.50	255.255.255.0	Switch-1 (f/5)
6	H-MaszynaCNC-6	karta sieciowa	192.168.10.60	255.255.255.0	Switch-1 (f/6)
7	H-MaszynaCNC-7	karta sieciowa	192.168.10.70	255.255.255.0	Switch-1 (f/7)
8	H-MaszynaCNC-8	karta sieciowa	192.168.10.80	255.255.255.0	Switch-1 (f/8)
9	H-MaszynaCNC-9	karta sieciowa	192.168.10.90	255.255.255.0	Switch-1 (f/9)
10	H-MaszynaCNC-10	karta sieciowa	192.168.10.100	255.255.255.0	Switch-1 (f/10)
11	H-PC-1	karta sieciowa	192.168.10.11	255.255.255.0	Switch-1 (f/11)
12	H-PC-2	karta sieciowa	192.168.10.21	255.255.255.0	Switch-1 (f/12)
13	H-PC-3	karta sieciowa	192.168.10.31	255.255.255.0	Switch-1 (f/13)
14	H-PC-4	karta sieciowa	192.168.10.41	255.255.255.0	Switch-1 (f/14)
15	H-PC-5	karta sieciowa	192.168.10.51	255.255.255.0	Switch-1 (f/15)

16	H-PC-6	karta sieciowa	192.168.10.61	255.255.255.0	Switch-1 (f/16)
17	H-PC-7	karta sieciowa	192.168.10.71	255.255.255.0	Switch-1 (f/17)
18	H-PC-8	karta sieciowa	192.168.10.81	255.255.255.0	Switch-1 (f/18)
19	H-PC-9	karta sieciowa	192.168.10.91	255.255.255.0	Switch-1 (f/19)
20	H-PC-10	karta sieciowa	192.168.10.101	255.255.255.0	Switch-1 (f/20)
21	H-Laptop-1	karta sieciowa	DHCP	255.255.255.0	
22	H-Laptop-2	karta sieciowa	DHCP	255.255.255.0	
23	H-Laptop-3	karta sieciowa	DHCP	255.255.255.0	

Tabela 2. Tabela adresowania podsieci hali produkcyjnej

B. Podsieć biura

Lp.	Urządzenie	Interfejs	Adres IP	Maska podsieci	Switch(int)
1	B-Drukarka-1	karta sieciowa	192.168.20.11	255.255.255.0	Switch-3 (f/1)
2	B-Drukarka-2	karta sieciowa	192.168.20.12	255.255.255.0	Switch-3 (f/2)
3	B-Drukarka-3	karta sieciowa	192.168.20.13	255.255.255.0	Switch-3 (f/3)
4	B-Drukarka-4	karta sieciowa	192.168.20.14	255.255.255.0	Switch-3 (f/4)
5	B-PC-1	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/1)
6	B-PC-2	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/2)
7	B-PC-3	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/3)
8	B-PC-4	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/4)
9	B-PC-5	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/5)
10	B-PC-6	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/6)
11	B-PC-7	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/7)
12	B-PC-8	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/8)
13	B-PC-9	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/9)
14	B-PC-10	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/10)
15	B-PC-11	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/11)
16	B-PC-12	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/12)
17	B-PC-13	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/13)
18	B-PC-14	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/14)
19	B-PC-15	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/15)
20	B-PC-16	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/16)
21	B-PC-17	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/17)

22	B-PC-18	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/18)
23	B-PC-19	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/19)
24	B-PC-20	karta sieciowa	DHCP	255.255.255.0	Switch-2 (f/20)
25	B-Laptop-1	karta sieciowa	DHCP	255.255.255.0	
26	B-Laptop-2	karta sieciowa	DHCP	255.255.255.0	
27	B-Laptop-3	karta sieciowa	DHCP	255.255.255.0	

Tabela 3. Tabela adresowania podsieci biura

C. Podsieć szefostwa

Lp.	Urządzenie	Interfejs	Adres IP	Maska podsieci	Switch(int)
1	S-Drukarka-1	karta sieciowa	192.168.30.11	255.255.255.0	Switch-3 (f/7)
2	S-Drukarka-2	karta sieciowa	192.168.30.12	255.255.255.0	Switch-3 (f/8)
3	S-PC-1	karta sieciowa	DHCP	255.255.255.0	Switch-3 (f/11)
4	S-PC-2	karta sieciowa	DHCP	255.255.255.0	Switch-3 (f/12)
5	S-PC-3	karta sieciowa	DHCP	255.255.255.0	Switch-3 (f/13)
6	S-PC-4	karta sieciowa	DHCP	255.255.255.0	Switch-3 (f/14)
7	S-Laptop-1	karta sieciowa	DHCP	255.255.255.0	
8	S-Laptop-2	karta sieciowa	DHCP	255.255.255.0	
9	S-Laptop-3	karta sieciowa	DHCP	255.255.255.0	
10	S-Laptop-4	karta sieciowa	DHCP	255.255.255.0	
11	Serwer	karta sieciowa	192.168.30.50	255.255.255.0	Switch-3 (f/21)

Tabela 4. Tabela adresowania podsieci szefostwa

D. Urządzenia sieciowe

Lp.	Urządzenie	Interfejs	Adres IP	Maska podsieci	-
1	Router		192.168.1.1		
2	Switch-1 (g/1)	g/1	192.168.10.1	255.255.255.0	Router (g/1)
3	Switch-2 (g/1)	g/2	192.168.20.1	255.255.255.0	Router (g/2)
4	Switch-3 (g/1)	g/3	192.168.30.1	255.255.255.0	Router (g/3)
6	UPS	karta sieciowa	192.168.30.101	255.255.255.0	Switch-3 (f/20)
7	UPS	karta sieciowa	192.168.30.102	255.255.255.0	Switch-3 (f/21)

Tabela 5. Tabela adresowania urządzeń sieciowych

5. Wybór protokołów i zabezpieczeń

A. Zdecyduj, jakie protokoły będą używane w sieci (np. DHCP, DNS, VLAN).

a. DHCP (Dynamic Host Configuration Protocol):

- i. DHCP będzie używane do automatycznego przydzielania adresów IP dla komputerów, laptopów, i innych urządzeń w sieci. Dzięki temu, unikniemy konieczności ręcznego konfigurowania każdego urządzenia.

LP.	Podsieć	Dostępne adresy
1.	Podsieć hali produkcyjnej	192.168.10.121-192.168.10.220
2.	Podsieć biura	192.168.20.121-192.168.20.220
3.	Podsieć szefostwa	192.168.30.121-192.168.30.220
4.	Urządzenia sieciowe	Niewykorzystywany DHCP

Tabela.6. Dostępne adresy do DHCP w zależności od sieci

b. DNS (Domain Name System):

- i. DNS umożliwia konwersję nazw domenowych na adresy IP, co jest istotne dla komunikacji w sieci. Zabezpieczy on sieć przed atakami typu DNS spoofing.

B. Opracuj plan zabezpieczeń sieci (np. hasła, firewall, VPN)

a. Hasła:

- i. Wszystkie urządzenia, w tym routery, przełączniki, serwery, oraz urządzenia przechowujące dane, powinny być zabezpieczone silnymi hasłami. Hasła powinny być regularnie zmieniane, a dostęp do kluczowych urządzeń powinien być ograniczony do upoważnionych osób.
- ii. W komputerach firmowych będą zmieniane hasła co miesiąc. Hasła powinny być przynajmniej długości 10 znaków, posiadać przynajmniej jeden znak specjalny i dużą literę. Za dostarczenie nowych wygenerowanych haseł odpowiada administrator sieci. Jeśli pracownik źle wprowadzi hasło 4 razy z rzędu jego konto jest zablokowane na 30 minut lub dopóki nie odblokuje go administrator sieci.

b. Firewall:

- i. Wdrożenie firewalla na poziomie bramy sieciowej oraz na poszczególnych urządzeniach komputerowych zabezpieczy przed atakami z zewnątrz. Firewall powinien być skonfigurowany tak, aby blokować nieautoryzowany dostęp.
- ii. Korzystamy z licencji – [ESET PROTECT Complete](#)
Cena do negocjacji dla firm.

c. Regularne Audyty Bezpieczeństwa:

- i. Przeprowadzanie regularnych audytów bezpieczeństwa sieci, w tym skanowania pod kątem luk w zabezpieczeniach, pomoże w identyfikacji i naprawie potencjalnych zagrożeń.

d. Szyfrowanie Danych:

- i. Wszystkie dane przechodzące przez sieć powinny być szyfrowane, zwłaszcza dane osobiste pracowników, klientów i dostawców. Szyfrowanie chroni przed przechwyceniem i nieautoryzowanym dostępem.
- ii. Serwer oraz bazy danych firmy powinny być zabezpieczone protokołem SSL/TLS oraz dane powinny być szyfrowane algorytmem AES (Advanced Encryption Standard).

e. Regularne Szkolenia Bezpieczeństwa:

- i. Przeprowadzanie regularnych szkoleń dla pracowników na temat zagrożeń cybernetycznych i praktyk bezpieczeństwa pomaga zminimalizować ryzyko związane z błędami ludzkimi.

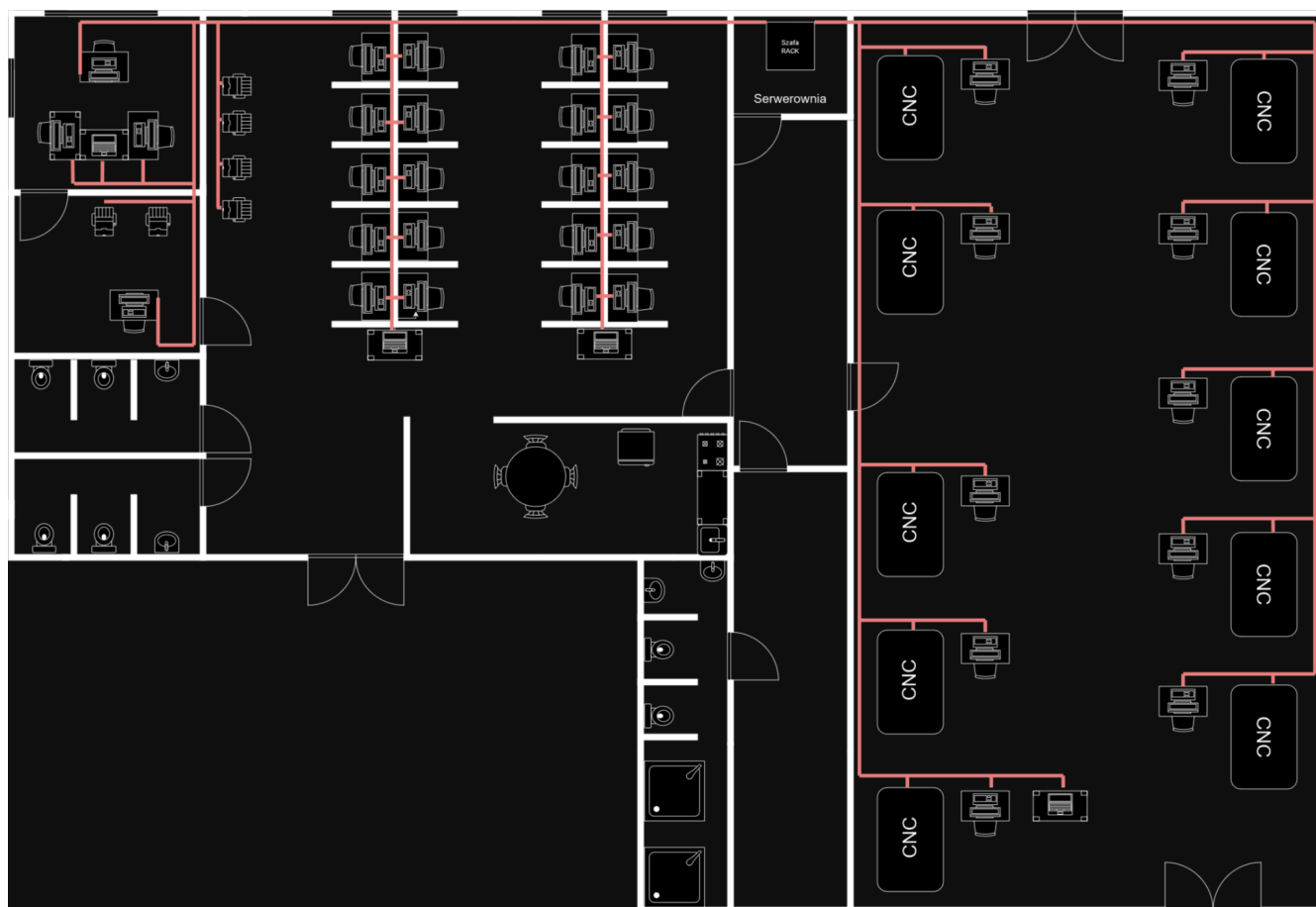
f. Monitorowanie Ruchu Sieciowego:

- i. System monitorujący ruch sieciowy pozwala szybko wykrywać potencjalne ataki lub nieautoryzowany dostęp. Automatyczne alerty będą wskazywały na podejrzaną aktywność.
- ii. [Microsoft Network Monitor](#) jest narzędziem stworzonym przez firmę Microsoft dla administratorów sieci. Umożliwia przechwytywanie oraz analizę ruchu sieciowego.

g. Backup i Przywracanie Danych:

- i. Regularne tworzenie kopii zapasowych danych i testowanie procedur przywracania danych pozwala zminimalizować skutki utraty danych spowodowanej awariami sprzętu, atakami ransomware czy błędami ludzkimi.
- ii. Backup bazy danych w zależności od wykorzystywanego oprogramowania – **MS SQL**.
- iii. Powinien być robiony pod koniec każdego dnia działania firmy. Na oddzielny nośnik do którego dostęp ma administrator sieci, lub podczas jego nieobecności jego zastępca.

6. Określenie lokalizacji urządzeń



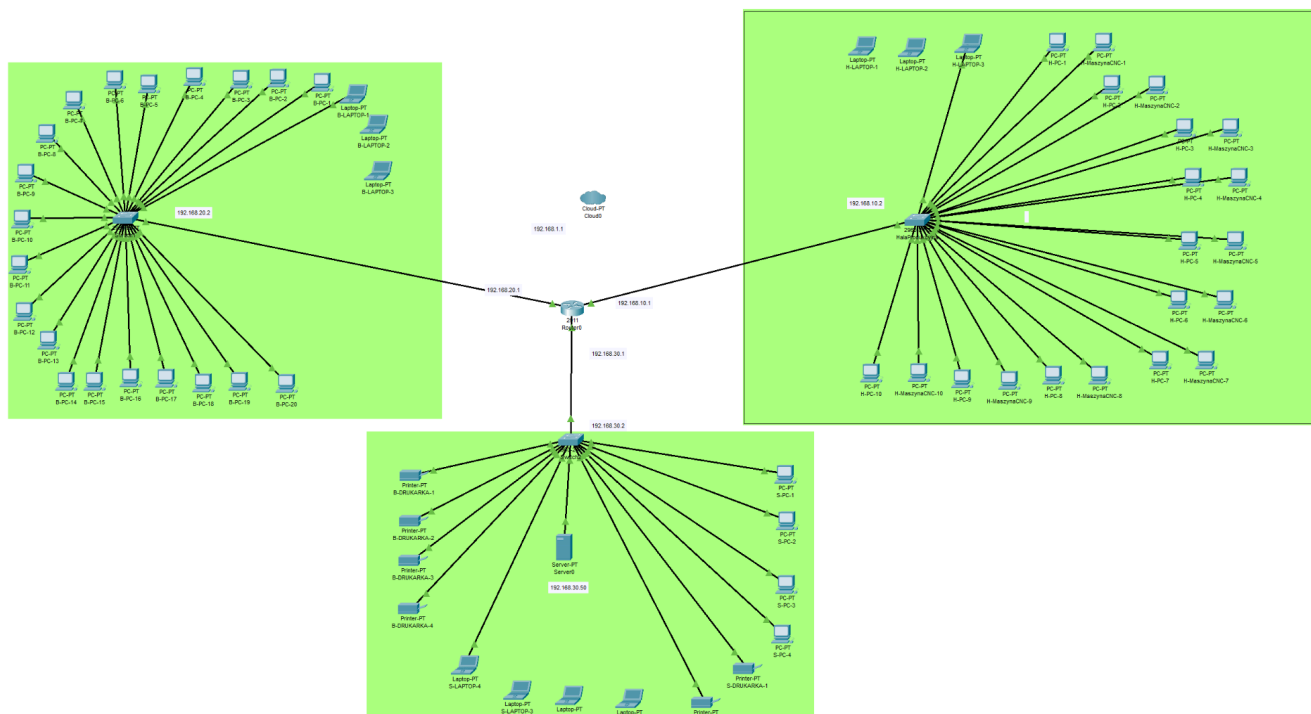
Rys.9. Określenie Lokalizacji Urządzeń na schemacie

Głębokość serwerowni powinna być wystarczająca, aby pomieścić szafy rackowe oraz zapewnić miejsce na instalację i dostęp do kabli. Standard TIA-942 może określać minimalną przestrzeń między rackami w celu zapewnienia wentylacji i łatwego dostępu do sprzętu. Wysokość pomieszczenia powinna uwzględniać miejsce na klimatyzację, wentylację oraz ewentualne systemy przeciwpożarowe.

Dostęp do serwerowni powinien być ograniczony, aby zapewnić bezpieczeństwo urządzeń oraz danych przechowywanych wewnątrz. Osoby, które mogą mieć dostęp do serwerowni:

- Administratorzy systemu,
- Personel obsługujący sprzęt,
- Personel zarządzający, tj. szefostwo.

7. Projekt topologii sieci



Rys.10. Topologia sieci – projekt