



Politechnika Wrocławska

Wydział Informatyki i Telekomunikacji

kierunek studiów: **Informatyka techniczna**

nazwa kursu: **Technologie sieciowe**

Projekt

Lokalna sieć komputerowa dla Urzędu Miejskiego

Numer zestawu danych - 12

Autorzy:

Klaudia Melnyk 269189

Aleksander Nowacki 269194

Bartłomiej Muszyński 269196

Prowadzący:

Dr inż. Wojciech Kmiecik

17.01.2024 r.

Spis treści

<i>Spis treści</i>	2
1. Wstęp	3
1.1. Profil działania instytucji	3
1.2. Projekt logiczny sieci.....	3
1.3. Projekt VLAN.....	3
1.4. Wybór technologii sieciowej i urządzeń sieciowych.....	3
1.5. Podstawowa konfiguracja urządzeń.....	3
2. Inwentaryzacja zasobów: sprzętu, aplikacji, zasobów ludzkich	4
2.1. Zasoby sprzętowe	4
2.2. Zasoby aplikacyjne	4
2.3. Zasoby ludzkie.....	4
3. Analiza potrzeb użytkowników	5
3.1. Ruch z / do Internetu przez punkty dystrybucyjne	5
3.2. Ruch z/do Internetu dla serwerów WWW i FTP	5
3.3. Całkowity transfer do / z Internetu	6
3.4. Popyt na lokalny ruch użytkowników w poszczególnych punktach dystrybucyjnych.....	6
3.5. Transfer w łączach szkieletowych.....	7
3.6. Transfer do serwerów	7
4. Założenia projektowe	8
4.1. Rodzaj technologii i przepustowość w sieci LAN.....	8
4.2. Rodzaj i przepustowość łącza do Internetu	8
4.3. Zabezpieczenia sieci	8
4.4. Planowanie sieci.....	8
4.5. Kosztorys.....	8
4.6. Inwentaryzacja zasobów i analiza potrzeb	8
4.7. Analiza przepustowości sieci	8
5. Projekt sieci	9
5.1. Projekt logiczny sieci wraz z opisem koncepcji rozwiązania i uzasadnienie	9
5.2. Wybór urządzeń sieciowych	11
5.3. Projekt adresacji IP	11
5.4. Projekt konfiguracji urządzeń	12
5.5. Projekt podłączenia do Internetu	13
5.6. Analiza bezpieczeństwa i niezawodności sieci	13
5.7. Kosztorys.....	14
6. Karty katalogowe proponowanych urządzeń	15

1. Wstęp

1.1. Profil działania instytucji

Niniejszy dokument stanowi dokumentację projektu lokalnej sieci komputerowej dla Urzędu Miejskiego we Wrocławiu, zlokalizowanego przy placu Nowy Targ 1-2. Urząd ten odgrywa kluczową rolę w zarządzaniu miastem i świadczeniu usług publicznych. Projekt sieci komputerowej ma na celu wspieranie tych działań poprzez zapewnienie efektywnej komunikacji i dostępu do zasobów internetowych, co jest niezbędne dla skutecznego funkcjonowania urzędu w sferach planowania przestrzennego, zarządzania infrastrukturą komunalną, edukacji, kultury oraz bezpieczeństwa publicznego.

1.2. Projekt logiczny sieci

Kluczowym elementem projektu jest opracowanie logicznego schematu sieci. Celem jest stworzenie struktury, która w precyzyjny sposób określa, jak różne komponenty sieciowe, takie jak routery, przełączniki, i punkty końcowe, będą ze sobą współpracować. Projekt ten obejmuje projektowanie topologii sieciowej, plan adresacji IP, tworzenie podsieci, opracowanie strategii zapewnienia redundantnych ścieżek komunikacyjnych, a także integrację kluczowych usług sieciowych.

1.3. Projekt VLAN

Projekt VLAN ma na celu zwiększenie wydajności i bezpieczeństwa sieci, a także usprawnienie zarządzania ruchem sieciowym poprzez segmentację sieci na mniejsze, izolowane logicznie segmenty. Projekt ten uwzględnia przypisanie portów przełączników do różnych VLAN-ów, planowanie trasowania ruchu między nimi, ustalanie zasad bezpieczeństwa dla każdego VLAN-u oraz integrację VLAN-ów z istniejącymi usługami sieciowymi.

1.4. Wybór technologii sieciowej i urządzeń sieciowych

Wybór technologii i urządzeń sieciowych jest kierowany potrzebami Urzędu Miejskiego, przy uwzględnieniu przepustowości, skalowalności, bezpieczeństwa i niezawodności. Proces ten obejmuje analizę wymagań sieciowych, dobór odpowiednich urządzeń sieciowych, wybór technologii przesyłania danych oraz standardów sieciowych i protokołów komunikacyjnych, które najlepiej odpowiadają wymaganiom projektu.

1.5. Podstawowa konfiguracja urządzeń

Proces konfiguracji urządzeń sieciowych skupia się na zapewnieniu ich efektywnego i niezawodnego działania oraz bezpieczeństwa sieci. Obejmuje to ustawienie adresów IP, konfigurację firewalli, list kontrolnych dostępu, optymalizację wydajności poprzez regulację ustawień QoS, a także wdrożenie narzędzi do monitorowania i zarządzania siecią, co pozwala na bieżące śledzenie stanu sieci i szybką reakcję na ewentualne problemy.

2. Inwentaryzacja zasobów: sprzętu, aplikacji, zasobów ludzkich

Inwentaryzacja zasobów dla Urzędu Miejskiego obejmuje kompleksową analizę sprzętu komputerowego, oprogramowania oraz personelu w dwóch budynkach, podzielonych na różne grupy robocze.

2.1. Zasoby sprzętowe

W budynku 1 i 2 znajduje się łącznie 397 komputerów rozdzielonych między grupy robocze Nieruchomości, Podatki i Pojazdy. Liczba drukarek wynosi 8, a punktów dostępowych WiFi – 5, co wskazuje na skoncentrowane punkty dostępu do sieci. Łączna liczba urządzeń bezprzewodowych we wszystkich grupach wynosi 28, co może sygnalizować potrzebę szczególnej uwagi przy planowaniu pokrycia sieci WiFi. Punkty dystrybucyjne (MDF, IDF1, IDF2) służą podłączeniu urządzeń w różnych lokalizacjach, z kablowym połączeniem międzybudynkowym realizowanym optycznym kablem jednomodowym o długości 320 metrów.

2.2. Zasoby aplikacyjne

Urzednicy Urzędu Miejskiego korzystają z sześciu głównych rodzajów aplikacji, które generują znaczący ruch sieciowy:

- a. **Przeglądarki internetowe** - Generują 195 kb/s ruchu w górę oraz generują 30 kb/s ruchu w dół.
- b. **Aplikacje do videokonferencji** - Generują 80 kb/s ruchu zarówno w górę, jak i w dół na każdego użytkownika, co jest kluczowe dla zdalnych spotkań i komunikacji.
- c. **VoIP** - Dla komunikacji głosowej przez sieć również generuje po 40 kb/s w górę i w dół.
- d. **Klienty FTP** - Służą do transferu plików; ruch generowany przez te aplikacje to 127 kb/s na pobieranie i 32 kb/s na wysyłanie dla użytkowników.
- e. **Komunikatory** - Umożliwiają bieżącą wymianę wiadomości i informacji, generując 15 kb/s ruchu w górę i w dół na użytkownika, gdzie to dotyczy WiFi.
- f. **Aplikacje do pracy w chmurze** - Pozwalają na dostęp do zasobów i aplikacji hostowanych w internecie, generując 113 kb/s na pobieranie i 99 kb/s na wysyłanie danych.

Każdy rodzaj aplikacji wnosi do całkowitego obciążenia sieciowego specyficzny wkład, który musi być uwzględniony przy projektowaniu infrastruktury sieciowej. Ogólny ruch sieciowy dla serwerów internetowych, w tym serwera WWW i FTP, został określony na 300 kb/s na pobieranie i 120 kb/s na wysyłanie danych przy założeniu liczby jednoczesnych sesji odpowiednio 51 dla WWW i 14 dla FTP.

2.3. Zasoby ludzkie

W Urzędzie Miejskim pracuje łącznie 397 osób, podzielonych na grupy robocze według specjalizacji działów. Grupa robocza Nieruchomości liczy 132 osób, Podatki – 135 osób, a Pojazdy – 130 osób. Personel ten wymaga dostępu do różnych aplikacji i usług sieciowych, co wpływa na wymagania dotyczące przepustowości i bezpieczeństwa sieci.

3. Analiza potrzeb użytkowników

3.1. Ruch z / do Internetu przez punkty dystrybucyjne

Tabela 1 Ruch z / do Internetu przez punkty dystrybucyjne

	Down kb/s	Up kb/s
IDF1	21492	13441
IDF2	12667	7731
MDF	22451	11538

$$IDF1 \text{ up} = 55 * 85 + 34 * 46 + 4 * 100 + 26 * 85 + 22 * 46 + 28 * 100 + 12 * 65 = 13441 \frac{kb}{s}$$

$$IDF2 \text{ up} = 35 * 85 + 36 * 46 + 31 * 100 = 7731 \frac{kb}{s}$$

$$IDF1 \text{ down} = 55 * 80 + 34 * 132 + 4 * 165 + 26 * 80 + 22 * 132 + 28 * 165 + 12 * 195 = 21492 \frac{kb}{s}$$

$$IDF2 \text{ down} = 35 * 80 + 36 * 132 + 31 * 165 = 12667 \frac{kb}{s}$$

$$MDF \text{ up} = 21 * 46 + 60 * 100 + 16 * 85 + 32 * 46 + 7 * 100 + 16 * 65 = 11538 \frac{kb}{s}$$

$$MDF \text{ down} = 21 * 132 + 60 * 165 + 16 * 80 + 32 * 132 + 7 * 165 + 16 * 195 = 22451 \frac{kb}{s}$$

Ruch z/do internetu grupy/wifi na piętrze

= Ilość użytkowników na danym piętrze z danej grupy

* suma ruchu z/do wszystkich kategorii danej grupy

Ruch z/do internetu na piętrze

= ruchu z/do grupy nieruchomości na piętrze

+ ruchu z/do grupy podatki na piętrze

+ ruchu z/do grupy pojazdy na piętrze + **ruchu z/do wifi na piętrze**

MDF = ruchu z/do dla piętra pierwszego + ruchu z/do dla piętra drugiego

IDF1 = ruchu z/do dla piętra trzeciego + ruchu z/do dla piętra czwartego

IDF2 = ruchu z/do dla budynku drugiego

3.2. Ruch z/do Internetu dla serwerów WWW i FTP

Tabela 2 Ruch z/do Internetu dla serwerów WWW i FTP

	Down kb/s	Up kb/s
Serwer WWW	2040	4080
Serwer FTP	1120	3080
Suma	3160	7160

$$\text{Serwer WWW up} = 80 * 51 = 4080 \frac{kb}{s}$$

$$\text{Serwer WWW down} = 40 * 51 = 2040 \frac{kb}{s}$$

$$\text{Serwer FTP up} = 220 * 14 = 3080 \frac{kb}{s}$$

$$\text{Serwer FTP down} = 80 * 14 = 1120 \frac{kb}{s}$$

$$\text{Ruch internetowy} = \text{Liczba sesji} * \text{up/down}$$

3.3. Całkowity transfer do / z Internetu

Tabela 3 Całkowity transfer do / z Internetu

	Down kb/s	Up kb/s
Internet	59770	39870

$$\text{Suma down} = 21492 + 12667 + 22451 + 2040 + 1120 = 59770 \frac{kb}{s}$$

$$\text{Suma up} = 13441 + 7731 + 11538 + 4080 + 3080 = 39870 \frac{kb}{s}$$

Całkowity transfer

$$= \text{up/down IDF1} + \text{up/down IDF2} + \text{up/down MDF} + \text{up/down WWW} + \text{up/down FTP}$$

3.4. Popyt na lokalny ruch użytkowników w poszczególnych punktach dystrybucyjnych

Tabela 4 Zapotrzebowanie na ruch lokalny

	Down kb/s	Up kb/s
MDF	141020	190310
IDF1	168160	219040
IDF2	81270	111520

$$\text{MDF down} = 760 * 16 + 1410 * 53 + 710 * 67 + 410 * 16 = 141020 \frac{kb}{s}$$

$$\text{MDF up} = 960 * 16 + 1710 * 53 + 1060 * 67 + 500 * 16 = 190310 \frac{kb}{s}$$

$$\text{IDF1 down} = 760 * 81 + 1410 * 56 + 710 * 32 + 410 * 31 = 168160 \frac{kb}{s}$$

$$\text{IDF1 up} = 960 * 81 + 1710 * 56 + 1060 * 32 + 500 * 31 = 219040 \frac{kb}{s}$$

$$\text{IDF2 down} = 760 * 35 + 1410 * 26 + 710 * 31 = 81270 \frac{kb}{s}$$

$$\text{IDF2 up} = 960 * 35 + 1710 * 26 + 1060 * 31 = 111520 \frac{kb}{s}$$

Zapotrzebowanie na ruch lokalny

= Liczba użytkowników grupy punktu dystrybucyjnego
* suma down/up (z Serwera 1/2 oraz Drukarek)

3.5. Transfer w łączach szkieletowych

Tabela 5 Transfer w łączach szkieletowych

	z MDF kb/s	do MDF kb/s
IDF1	189652	232481
IDF2	93937	119251

$$IDF1 \text{ z MDF} = 21492 + 168160 = 189652 \frac{kb}{s}$$

$$IDF1 \text{ do MDF} = 13441 + 219040 = 232481 \frac{kb}{s}$$

$$IDF2 \text{ z MDF} = 12667 + 81270 = 93937 \frac{kb}{s}$$

$$IDF2 \text{ do MDF} = 7731 + 111520 = 119251 \frac{kb}{s}$$

Transfer w łączach szkieletowych

= Ruch lokalny do/z + ruch do/z do internetu przez punkty

3.6. Transfer do serwerów

Tabela 6 Transfer do serwerów

	Down kb/s	Up kb/s
S1	211650	210450
S2	178550	252850

$$S1 \text{ down} = 132 * 400 + 165 * 750 + 130 * 400 + 28 * 200 = 211650 \frac{kb}{s}$$

$$S1 \text{ up} = 132 * 250 + 165 * 850 + 130 * 450 + 28 * 150 = 210450 \frac{kb}{s}$$

$$S2 \text{ down} = 132 * 350 + 165 * 650 + 130 * 300 + 28 * 200 = 178550 \frac{kb}{s}$$

$$S2 \text{ up} = 132 * 550 + 165 * 850 + 130 * 450 + 28 * 250 = 252850 \frac{kb}{s}$$

Transfer do serwerów = Liczba użytkowników grupy * suma down/up Serwera 1/2

4. Założenia projektowe

4.1. Rodzaj technologii i przepustowość w sieci LAN

Technologia Ethernet: Wykorzystanie Ethernetu jako podstawowej technologii komunikacji. Zgodność z preferencjami firmy dotyczącymi rodziny technologii Ethernet.

Przepustowość Sieci LAN: Uwzględnienie wysokiej przepustowości zgodnie z analizowanymi obciążeniami związanymi z różnymi aplikacjami i urządzeniami. Należy zapewnić elastyczność w zakresie przepustowości, aby uniknąć zatorów i spowolnień, szczególnie podczas wzmożonego wykorzystania aplikacji do wideokonferencji, VoIP i przeglądania Internetu. Przepustowość powinna być dostosowana do średniego przewidywanego przepływu danych.

4.2. Rodzaj i przepustowość łącza do Internetu

Dwa łącza internetowe: Implementacja dwóch łączy internetowych - podstawowego i zapasowego, z przepustowością dostosowaną do potrzeb firmy. Podstawowe łącze powinno zapewniać minimalną gwarantowaną przepustowość wynoszącą 40% średniego przewidywanego przepływu (56 610 kb/s down, 32 710 kb/s up).

4.3. Zabezpieczenia sieci

Zaawansowane rozwiązania bezpieczeństwa: Wdrożenie firewalle, systemów wykrywania i zapobiegania włamaniom oraz szyfrowanie danych.

Separacja ruchu za pomocą VLAN: Wykorzystanie sieci VLAN do oddzielenia ruchu w ramach grup roboczych, zwiększając bezpieczeństwo i efektywność zarządzania siecią.

4.4. Planowanie sieci

Dodatkowe porty na przełącznikach: Zapewnienie 20% dodatkowych portów na przełącznikach dla przyszłego rozszerzenia sieci. W związku z przewidywanym wzrostem liczby pracowników.

Sieć bezprzewodowa: Instalacja sieci bezprzewodowej na każdym piętrze z odpowiednim pokryciem i przepustowością. Należy zapewnić dostępność sieci bezprzewodowej na każdym piętrze, zgodnie z wymaganiami firmy.

Kable Kategorii 6 i Okablowanie Optyczne: Używanie kabli kategorii 6 dla połączeń miedzianych oraz optycznego kabla jednomodowego o długości 320 metrów dla połączeń między budynkowych.

4.5. Kosztorys

Obejmowanie wszystkich urządzeń i połączeń internetowych: Uwzględnienie kosztów eksploatacji przez 2 lata.

4.6. Inwentaryzacja zasobów i analiza potrzeb

Zasoby Sprzętowe i Aplikacyjne: Analiza obecnych zasobów, takich jak liczba komputerów, drukarek, punktów dostępowych Wi-Fi oraz aplikacji generujących ruch sieciowy.

Analiza Potrzeb Użytkowników: Przeprowadzenie szczegółowej analizy potrzeb różnych grup roboczych, ich liczby i specjalizacji działów w kontekście przepustowości i bezpieczeństwa sieci.

4.7. Analiza przepustowości sieci

Sieć Szkieletowa i Łącza Internetowe: Określenie przepustowości dla różnych segmentów sieci, w tym połączeń między IDF a MDF oraz przepustowości łącza internetowego.

5. Projekt sieci

The diagram illustrates a multi-story office network architecture. It features three main building sections: Budynek 1, Budynek 2, and Budynek 3, all interconnected with a central cloud. Each building contains various network devices and user endpoints.

Legend:

- PCN - Komputery z danymi neurochirurgii
- PCP - Komputery z danymi pediatry
- PCPOU - Komputery z danymi polski
- D - Drukarka
- AP - punkt dostępu
- MP - Telefony komórkowe
- SZ - Switch maszynowy drugi
- SS - Switch maszynowy pierwszy

VLANs:

- Vlan 1: Neurochirurgia
- Vlan 2: Pediatria
- Vlan 3: Polski
- Vlan 4: Drukarka
- Vlan 5: WiFi
- Vlan 6: Serwery
- Vlan 7: Serwery internetowe
- Vlan 8: Serwery internetowe

Building Details:

- Budynek 1:** Includes PCN (1-35), PCP (1-26), PCPOU (1-31), SZ (28-34), D (8), SS (3), and various servers (Serwer WWW, Serwer FTP, DMS, Serwer BIP, Serwer BIP, Serwer BIP).
- Budynek 2:** Includes PCN (1-35), PCP (1-26), PCPOU (1-31), SZ (28-34), D (8), SS (3), and various servers (Serwer WWW, Serwer FTP, DMS, Serwer BIP, Serwer BIP, Serwer BIP).
- Budynek 3:** Includes PCN (1-35), PCP (1-26), PCPOU (1-31), SZ (28-34), D (8), SS (3), and various servers (Serwer WWW, Serwer FTP, DMS, Serwer BIP, Serwer BIP, Serwer BIP).

Rysunek 1 Schemat sieci komputerowej

Przedstawiony diagram sieciowy ilustruje projekt sieci w Urzędzie Miasta obejmujący dwa budynki. Zastosowano schemat oznaczania urządzeń z unikalnymi numerami inwentaryzacyjnymi, co pozwala na efektywne zarządzanie i identyfikację sprzętu w sieci. Komputery i inne urządzenia rozlokowane są według funkcji i lokalizacji, z wyraźnym podziałem na VLANy, co zwiększa bezpieczeństwo i efektywność sieci, a także umożliwia segregację ruchu sieciowego. Na przykład, PCN oznacza komputery działu nieruchomości, a PCPOJ komputery działu Pojazdy. Użycie kabli kategorii 6 gwarantuje odpowiednią przepustowość sieciową, a strategia połączeń przewodowych i bezprzewodowych odpowiada na różnorodne potrzeby użytkowników.

Struktura Sieci i Połączenia

Projekt sieci zaprojektowany został z myślą o modularności i efektywności, zapewniając optymalną organizację i łatwość zarządzania. Kluczowe elementy struktury sieci to:

- i. **Control Switch na każdym piętrze:** Każde piętro wyposażone jest w centralny przełącznik (control switch), do którego podłączone są wszystkie inne przełączniki na tym piętrze, odpowiadające za wszystkie urządzenia sieciowe.
- ii. **Połączenia między Control Switch a MDF/IDF:**
 - Control switch piętra pierwszego i drugiego łączy się bezpośrednio ze switchem MDF, który jest głównym węzłem sieciowym.
 - Control switch piętra trzeciego i czwartego łączy się ze switchem IDF1.
 - Control switch piętra 1 w budynku 2 łączy się ze switchem IDF2.
- iii. **Połączenia IDF z MDF:** Switch IDF1 oraz IDF2 są bezpośrednio połączone z MDF, co umożliwia im dostęp do sekcji serwerów oraz Internetu.

Zalety Projektu

Zaprojektowana struktura sieciowa zapewnia łatwość w rozbudowie i utrzymaniu. Modularność pozwala na elastyczne dostosowanie sieci do przyszłych wymagań, a także ułatwia zarządzanie i diagnostykę. Dzięki zastosowaniu 24-portowych switchy, maksymalna liczba urządzeń, która może zostać odłączona w przypadku awarii jednego switcha, jest ograniczona do 19. To minimalizuje ryzyko i wpływ potencjalnych przerw w działaniu sieci.

Wady

Wprowadzenie pełnej redundancji wiąże się ze stosunkowo wysokimi kosztami. Należy zważyć korzyści płynące z dodatkowej niezawodności w stosunku do inwestycji początkowej.

Redundancja

Na każdym piętrze przewidziano zapasowy control switch, co stanowi podstawowy element redundancji. Dodatkowo, zaplanowano zapasowe switchy IDF1, IDF2 oraz MDF, co zapewnia dodatkową warstwę bezpieczeństwa i niezawodności sieci, minimalizując ryzyko długotrwałych przerw w dostępie do sieci.

Podsumowanie

Ten projekt logiczny sieci skupia się na zrównoważeniu potrzeb efektywności operacyjnej, skalowalności i niezawodności, jednocześnie uwzględniając ograniczenia budżetowe. Modularna struktura, ograniczona redundancja i strategiczne rozmieszczenie switchy stanowią optymalne rozwiązanie, które spełnia wymagania instytucji, jednocześnie pozostawiając przestrzeń dla przyszłych rozbudów i ulepszeń.

5.2. Wybór urządzeń sieciowych

Przełącznik Sieciowy

Model: Cisco CBS220-24P-4G-EU Smart 24-port GE, PoE+ 195W, 4x1G SFP

Wybór: Wybór tego przełącznika był podyktowany koniecznością zapewnienia wysokiej wydajności oraz możliwością zasilania urządzeń końcowych przez PoE+, co jest istotne dla urządzeń takich jak kamery IP i telefony VoIP. Cena urządzenia jest atrakcyjna, zwłaszcza biorąc pod uwagę renomę i jakość produktów Cisco.

Router

Model: Cisco RV160W

Wybór: Router ten został wybrany z uwagi na jego zdolność obsługi do 50 użytkowników, co jest wystarczające dla naszej infrastruktury, a także ze względu na zaawansowane funkcje bezpieczeństwa i VPN. Brak mniejszych modeli dostosowanych do naszej skali działalności sprawia, że jest to optymalny wybór, który umożliwia przyszłą rozbudowę.

Punkt dostępowy

Model: Ubiquiti UniFi U6-Plus

Wybór: Wybór modelu Ubiquiti UniFi U6-Plus jako punktu dostępowego był podyktowany jego zaawansowanymi funkcjami i wydajnością. Jest to urządzenie klasy enterprise, które korzysta z najnowszej technologii Wi-Fi 6, zapewniając doskonałą przepustowość i stabilność połączenia, co jest kluczowe w środowiskach o dużej gęstości sieciowej. Urządzenie to oferuje port GbE RJ45 dla połączeń przewodowych, co zwiększa elastyczność w różnych scenariuszach instalacji. U6-Plus, dzięki swojej mocy i wsparciu dla zaawansowanych standardów bezpieczeństwa, jest idealny dla potrzeb małych i średnich przedsiębiorstw, które wymagają niezawodnego dostępu do sieci i wysokiej wydajności. Jego możliwość obsługi 300+ klientów jednocześnie oraz wsparcie dla funkcji takich jak VLAN i zaawansowane QoS czynią go świetnym rozwiązaniem dla organizacji, które pragną efektywnie zarządzać ruchem sieciowym i zapewnić bezpieczeństwo danych.

5.3. Projekt adresacji IP

Tabela 7 Projekt adresacji IP

VLAN	Grupa	Adres	Maska	Liczba urządzeń	Bramy
1	Nieruchomości	192.168.0.0	/24	132	192.168.0.1
2	Podatki	192.168.1.0	/24	135	192.168.1.1
3	Pojazdy	192.168.2.0	/24	132	192.168.2.1
4	Drukarki	192.168.3.0	/24	8	192.168.3.1
5	Wi-Fi	192.168.4.0	/24	5	192.168.4.1
6	Sterowanie	192.168.5.0	/24	40	192.168.5.1
7	Serwery wewnętrzne	192.168.6.0	/24	2	192.168.6.1
8	Serwery internetowe	192.168.7.0	/24	2	192.168.7.1

Ruter w naszej sieci jest skonfigurowany jako serwer DHCP, który efektywnie zarządza dynamicznym przydziałem adresów IP. Dzięki temu mechanizmowi, każde urządzenie podłączone do sieci automatycznie otrzymuje unikalny adres IP, co zapewnia płynną i efektywną komunikację w obrębie naszej infrastruktury sieciowej.

5.4. Projekt konfiguracji urządzeń

Zdalne logowanie

- Aktywacja zdalnego logowania przez protokół SSH w wersji drugiej.
- Wyłączenie serwera protokołu Telnet.

Bezpieczeństwo haseł

- Włączenie szyfrowania haseł w plikach konfiguracyjnych.
- Wymuszenie logowania przy użyciu danych przechowywanych w lokalnej bazie.

Konta użytkowników

- Utworzenie osobnego konta użytkownika dla każdego administratora.

Zapisywanie logów

- Aktywacja funkcji zapisywania logów.

Konfiguracja VLAN i portów dostępowych

- Przypisanie każdego używanego portu dostępowego do odpowiedniego VLAN'a.
- Dezaktywacja pozostałych portów.
- Ustawienie odpowiednich etykiet VLAN na wszystkich interfejsach.

Konfiguracja DHCP

- Ustawienie serwera DHCP dla automatycznego przydzielania adresów IP w poszczególnych VLAN-ach.

Switchy szkieletowe

- Ustawienie switchy MDF, IDF1 i IDF2 w trybie warstwy trzeciej.

Izolacja serwerów internetowych

- Umieszczenie serwerów internetowych w strefie DMZ.
- Ustawienie ściany ogniowej między siecią lokalną a DMZ.

Kontrola dostępu (ACL)

- Wykorzystanie listy kontroli dostępu (ACL) w celu zapobieżenia routingu pomiędzy strefą DMZ a pozostałymi urządzeniami.

Adresacja IP

- Przypisanie publicznych adresów IP do interfejsów sieciowych routera.
- Przekierowanie ruchu sieciowego do/z serwerów w strefie DMZ na adresy publiczne routera.

NAT i PAT

- Wdrożenie mechanizmu NAT Overload/PAT dla wszystkich podsieci prywatnych.
- Przypisanie publicznych adresów IP do interfejsów sieciowych routera.
- Przekierowanie ruchu sieciowego do/z serwerów w strefie DMZ na adresy publiczne routera.

Sieć Wi-Fi

- Skonfigurowanie punktów dostępowych Wi-Fi do rozgłaszania tej samej sieci o identycznym SSID.
- Zabezpieczenie sieci hasłem dostępowym z szyfrowaniem WPA2-PSK Enterprise.

5.5. Projekt podłączenia do Internetu

W ramach naszego projektu, szczególną uwagę poświęciliśmy zapewnieniu stabilnego i szybkiego dostępu do Internetu w urzędzie. Po dokładnej analizie różnych opcji, zdecydowaliśmy się na ofertę firmy Orange, która obecnie oferuje pakiet internetowy idealnie dostosowany do potrzeb naszej instytucji.

Zgodnie z informacjami uzyskanymi ze strony <https://panwybierak.pl/oferta/orange-internet-firmowy-pakiet-s-swiatlowod-do-600-mb-s-/24682>, Orange zapewnia pakiet internetowy, który oferuje prędkość pobierania danych na poziomie 600 Mb/s oraz prędkość wysyłania do 100 Mb/s. Taka prędkość pozwoli na płynną pracę wszystkich urzędników oraz zapewni szybką i efektywną obsługę mieszkańców.

Oferta Orange obejmuje umowę na okres 24 miesięcy. Jest to korzystne rozwiązanie, które zapewnia stabilność usług przez długi okres. Opłata jednorazowa wynosi 48,78 zł, co stanowi koszt inicjalny związany z aktywacją usługi. Opłata miesięczna za dostęp do Internetu wynosi 70,98 zł, co jest atrakcyjną stawką biorąc pod uwagę oferowaną prędkość i jakość usługi.

Kluczowym elementem oferty jest zapewnienie publicznego, statycznego adresu IP. Jest to istotne dla bezpieczeństwa i stabilności działania systemów informatycznych urzędu, umożliwiając m.in. zdalny dostęp do zasobów sieciowych, organizację zdalnych spotkań oraz bezpieczne korzystanie z aplikacji internetowych. Statyczny adres IP gwarantuje również łatwiejszą konfigurację oraz zarządzanie sieciami usługami, takimi jak serwery poczty elektronicznej, serwery FTP czy zdalne pulpity.

5.6. Analiza bezpieczeństwa i niezawodności sieci

W ramach zapewnienia bezpieczeństwa i niezawodności sieci w rozważanej firmie, przeprowadzono dogłębną analizę potencjalnych zagrożeń. Wśród nich wymienić należy awarie zasilania, ataki wirusowe oraz włamania przez Internet. W odpowiedzi na te wyzwania, zaimplementowano szereg mechanizmów zabezpieczających, dostosowanych do profilu działalności firmy, wymagań użytkowników oraz możliwości finansowych.

Zdalne logowanie

- Wprowadzono aktywację zdalnego logowania poprzez bezpieczny protokół SSH w wersji drugiej, co znacząco zwiększa bezpieczeństwo danych przesyłanych podczas zdalnej pracy.
- Wyłączono mniej bezpieczny serwer protokołu Telnet, co dodatkowo chroni sieć przed nieautoryzowanym dostępem.

Bezpieczeństwo haseł

- Włączono funkcję szyfrowania haseł w plikach konfiguracyjnych, co uniemożliwia ich łatwe odczytanie przez osoby niepowołane.
- Wprowadzono wymóg logowania przy użyciu danych przechowywanych w lokalnej bazie, co dodatkowo zabezpiecza przed nieautoryzowanym dostępem.

Architektura sieci

- Sieć została podzielona na VLAN-y, co pozwala na lepsze zarządzanie i izolację poszczególnych segmentów sieci, zwiększając tym samym bezpieczeństwo i efektywność pracy.
- Na każdym piętrze zainstalowano główny switch kontrolny (control switch), do którego podłączone są pozostałe switch'e, odpowiedzialne za wszystkie urządzenia na danym piętrze. Dzięki temu, możliwa jest centralna kontrola i zarządzanie siecią.

- Wprowadzono zapasowe switch'e kontrolne (spare control switches) na każdym piętrze, co minimalizuje ryzyko przestojów w pracy sieci w przypadku awarii.
- Zastosowano modularność w architekturze sieci, co ułatwia rozbudowę i utrzymanie systemu. Użycie 24-portowych switch'y zapewnia, że w przypadku awarii jednego switcha, zostanie odłączone maksymalnie 19 urządzeń, co ogranicza wpływ potencjalnych problemów na działalność firmy.

Zabezpieczenia przed wirusami i atakami zewnętrznymi

- Zainstalowano zaawansowane systemy firewall, które chronią sieć przed wirusami oraz nieautoryzowanym dostępem z zewnątrz. Firewall'e te są regularnie aktualizowane, aby zapewniać skuteczną ochronę przed najnowszymi zagrożeniami.
- Opracowano procedury reagowania na incydenty bezpieczeństwa, w tym plany szybkiego przywracania działania systemów po ewentualnych atakach.

Zapewnienie ciągłości działania

- Wdrożono systemy zapasowego zasilania, aby minimalizować ryzyko przerw w działaniu sieci spowodowanych awariami zasilania.
- Przyjęto strategię redundancji w kluczowych komponentach sieci, takich jak switch'e IDF1/IDF2/MDF, co zapewnia ciągłość pracy sieci nawet w przypadku awarii jednego z elementów.

5.7. Kosztorys

Access Pointy Ubiquiti UniFi U6+ (U6-PLUS)

Cena jednostkowa: 457 PLN

Ilość: 5 sztuk

Łączny koszt: 2,285 PLN

Router Cisco RV160W

Cena jednostkowa: 1,199.07 PLN

Ilość: 1 sztuka

Łączny koszt: 1,199.07 PLN

Przełączniki Cisco CBS220-24P-4G-EU Smart 24-port

Cena jednostkowa: 1,666.47 PLN

Ilość: 34 sztuki

Łączny koszt: 56,660.98 PLN

Usługa Internetowa od Orange

Opłata jednorazowa: 48,78 PLN

Opłata miesięczna: 70,98 PLN

Łączny koszt za 24 miesiące: 1,752.30 PLN.

Podsumowanie

Całkowity koszt zakupu sprzętu sieciowego i usługi internetowej wynosi:

- Access Pointy Ubiquiti UniFi U6+ (U6-PLUS): 2,285 PLN
- Router Cisco RV160W: 1,199.07 PLN
- Przełączniki Cisco CBS220-24P-4G-EU Smart 24-port: 56,660.98 PLN
- Usługa Internetowa od Orange (24 miesiące): 1,752.30 PLN

Łączny koszt: **61,897.35 PLN**

6. Karty katalogowe proponowanych urządzeń

Tabela 8 Ubiquiti UniFi U6 Plus

Ubiquiti UniFi U6 Plus	
Wymiary	Ø160 x 33 mm
Waga	Bez montażu: 338 g; Z montażem: 413 g
Interfejs sieciowy	1 port GbE RJ45
Metoda zasilania	PoE
Maksymalne zużycie energii	9W
Maksymalna moc TX	23 dBm (2.4 GHz i 5 GHz)
MIMO	2x2 (2.4 GHz i 5 GHz)
Przepustowość	573.5 Mbps (2.4 GHz), 2402 Mbps (5 GHz)
Wzmacniacz anteny:	3 dBi (2.4 GHz), 5.4 dBi (5 GHz)
Temperatura pracy	-30 do 60°C
Obsługa klientów jednocześnie	300+
Standardy WiFi	802.11a/b/g, WiFi 4/5/6
Bezpieczeństwo	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)

Punkt dostępowy Ubiquiti UniFi U6 Plus to nowoczesne urządzenie sieciowe zaprojektowane do obsługi standardów WiFi 802.11a/b/g oraz WiFi 4/5/6, zapewniające maksymalną przepustowość na poziomie 573.5 Mbps (2.4 GHz) oraz 2402 Mbps (5 GHz). Z kompaktowymi wymiarami Ø160 x 33 mm i wagą 338 g bez montażu (413 g z montażem) idealnie nadaje się do dyskretnego zamontowania w każdym środowisku. Posiada jeden port GbE RJ45 i jest zasilany metodą PoE (Power over Ethernet), co minimalizuje potrzebę prowadzenia dodatkowych kabli zasilających. Maksymalne zużycie energii wynosi zaledwie 9W, a maksymalna moc TX to 23 dBm dla obu pasm częstotliwości 2.4 GHz i 5 GHz. Zastosowanie technologii MIMO 2x2 znacząco poprawia wydajność i zasięg sieci Wi-Fi. Punkt dostępowy może obsługiwać ponad 300 klientów jednocześnie, a wbudowane wzmacniacze anten o mocy 3 dBi (2.4 GHz) i 5.4 dBi (5 GHz) zapewniają solidne połączenie. Urządzenie pracuje w temperaturach od -30 do 60°C, oferując niezawodność w różnorodnych warunkach. Funkcje bezpieczeństwa obejmują WPA-PSK, WPA-Enterprise z obsługą WPA/WPA2/WPA3.

Link do strony producenta:

<https://techspecs.ui.com/unifi/wifi/u6-plus>

Tabela 9 Cisco CBS220-24P-4G

Cisco CBS220-24P-4G	
Ilość portów	24 porty Gigabit Ethernet
Porty Uplink	4 porty Gigabit Ethernet SFP
Zasilanie PoE	Tak, budżet mocy PoE 195W
Wydajność przełączania	56 Gbps
Prędkość przekazywania	41.66 Mpps
Pojemność tabeli MAC	8192 adresy
VLANy	Wsparcie dla do 256 VLANów
QoS	Priorytetyzację ruchu, 8 kolejek sprzętowych na port
Bezpieczeństwo	ACL, IEEE 802.1X, port security, RADIUS, TACACS+
IPv6	Obsługa hosta IPv6
Zarządzanie	Cisco Business Dashboard, interfejs webowy, CLI, SNMP
Wymiary	440 x 257 x 44 mm
Waga	4.10 kg

Przełącznik Cisco CBS220-24P-4G to zaawansowane rozwiązanie sieciowe, oferujące 24 porty Gigabit Ethernet oraz 4 porty uplink Gigabit Ethernet SFP. Zasilanie PoE z budżetem mocy do 195W pozwala na efektywne zasilanie urządzeń końcowych. Urządzenie charakteryzuje się wydajnością przełączania na poziomie 56 Gbps oraz szybkością przekazywania 41.66 Mpps, co zapewnia płynne działanie sieci. Przełącznik obsługuje do 256 VLAN-ów, co umożliwia elastyczną segmentację sieci. Funkcje QoS z 8 kolejkami sprzętowymi na port zapewniają priorytetyzację ruchu sieciowego, a zabezpieczenia takie jak ACL, IEEE 802.1X, port security oraz integracja z RADIUS i TACACS+ wzmacniają bezpieczeństwo. Urządzenie wspiera także IPv6, a zarządzanie jest możliwe przez Cisco Business Dashboard, interfejs webowy, CLI oraz SNMP. Przełącznik ma wymiary 440 x 257 x 44 mm i waży 4.10 kg.

Link do strony producenta:

<https://www.cisco.com/c/en/us/products/collateral/switches/business-220-series-smart-switches/datasheet-c78-744915.html>

Tabela 10 Cisco RV160W

Cisco RV160W	
Typ	Router VPN z Wi-Fi Wireless-AC
Porty WAN	1 port RJ-45/SFP Gigabit Ethernet kombinacja
Porty LAN	4 porty RJ-45 Gigabit Ethernet
Port Konsolowy	1 port RJ-45
Wi-Fi	2x2 802.11ac
Bezpieczeństwo	SPI firewall, przekierowanie portów, kontrola dostępu
Zarządzanie	Web-based, SNMP, Bonjour, Universal Plug and Play (PnP)
Protokoły VPN	IPsec, PPTP, OpenVPN
QoS	Wsparcie dla 802.1p, 4 kolejki, wsparcie DSCP
Wymiary	200x150x30 mm
Waga	630 g

Router Cisco RV160W to nowoczesne urządzenie sieciowe klasy korporacyjnej, idealne dla małych firm i osób pracujących zdalnie. Posiada jedno uniwersalne gniazdo WAN RJ-45/SFP Gigabit Ethernet, które zapewnia elastyczność łączenia za pomocą kabla miedzianego lub światłowodowego. Dodatkowo, wyposażony jest w cztery porty LAN RJ-45 Gigabit Ethernet, co gwarantuje szybki i stabilny dostęp do lokalnej sieci.

Główną cechą tego routera jest jego zaawansowana funkcja VPN, która obsługuje protokoły IPsec, PPTP i OpenVPN. Dzięki temu zapewnia wyjątkowe bezpieczeństwo przesyłanych danych, co jest kluczowe dla firm. Wbudowany firewall SPI, funkcje przekierowania portów i kontrola dostępu dodatkowo wzmacniają bezpieczeństwo sieci.

Intuicyjne zarządzanie urządzeniem jest możliwe dzięki webowemu interfejsowi użytkownika, wsparciu dla SNMP oraz protokołów Bonjour i Universal Plug and Play (PnP). To ułatwia konfigurację i zarządzanie siecią. Technologia Wi-Fi 2x2 802.11ac zapewnia wysoką prędkość i stabilność połączenia bezprzewodowego. Funkcja QoS z wsparciem dla 802.1p i DSCP pozwala na efektywną priorytetyzację ruchu sieciowego, co jest niezbędne do płynnej pracy aplikacji biznesowych.

Router jest kompaktowy (200x150x30 mm) i lekki (630 g), co ułatwia jego umieszczanie w różnych środowiskach pracy. Model Cisco RV160W to idealne rozwiązanie dla tych, którzy szukają niezawodnego, bezpiecznego i łatwego w obsłudze routera VPN z funkcjami Wi-Fi.

Link do strony producenta:

<https://www.cisco.com/c/en/us/products/collateral/routers/rv160-vpn-router/datasheet-c78-741410.html>