WYŻSZA SZKOŁA
HUMANISTYCZNO – EKONOMICZNA
W ŁODZI

WYDZIAŁ Informatyki, Zarządzania i Transportu

kierunek Informatyka

KAROL KUBICKI

53080

PROJEKT SIECI DLA ŚREDNIEJ WIELKOŚCI FIRMY

Przyjmuję pracę jako inżynierską

podpis promotora.....

data .....

Praca napisana pod kierunkiem
Dr inż. Jan Makuch

ŁÓDŹ 2009

Spis treści

1. Wstęp

1.1. Cel i zakres pracy

Celem niniejszej pracy jest projekt sieci zakładowej. Sieć przeznaczona jest dla firmy posiadającej dwie lokalizacje. Analiza potrzeb użytkownika wymaga stworzenia radiowego połączenia pomiędzy lokalizacjami, stworzenia sieci bezprzewodowej w sali konferencyjnej, przygotowania tak infrastruktury sieciowej aby była możliwość w przyszłości korzystania z usług VOIP, czy tez stworzenia kilku grup VLAN.

1.2. Uzasadnienie wyboru tematu

Praca nad projektem sieci lokalnej pozwoliła poznać mechanizmy tworzenia sieci komputerowych, normy okablowania oraz zapoznać się z trendami sprzętu sieciowego. Miałem możliwość wykorzystania ich w konkretnym projekcie a w przyszłości będę mógł zaobserwować ich działanie już na konkretnym wycinku rzeczywistości. Praca pozwoliła poznać metody zabezpieczania sieci, tworzenia planów i nanoszenia na nich okablowania, czy też przeliczania adresów IP podsieci. Jest to o tyle dla mnie istotne, że wiąże się to z moją przyszłością i wykonywanym rodzajem pracy zawodowej.

1.3. Układ pracy

- Praca składa się z trzech głównych rozdziałów. Pierwsze dwa dotyczą zagadnień czysto teoretycznych. Przedstawiono w nich między innymi:
- metody projektowania sieci lokalnych;
- media transmisyjne;
- rodzaje i topologie sieci;
- metody i zagadnienia dotyczące projektowania sieci;

Ostatni rozdział dotyczy tworzonego projektu sieci. Zawiera on analizę potrzeb przyszłych użytkowników. Przedstawia dobór urządzeń wykorzystanych w projekcie ich dane techniczne, metody konfiguracji i podłączenia. W rozdziale tym także zawarto

plany budynków, opis grup VLAN, adresowanie schematy sieci. Rozdział kończy się próbą stworzenia i przedstawienia polityki bezpieczeństwa dla pracowników firmy.

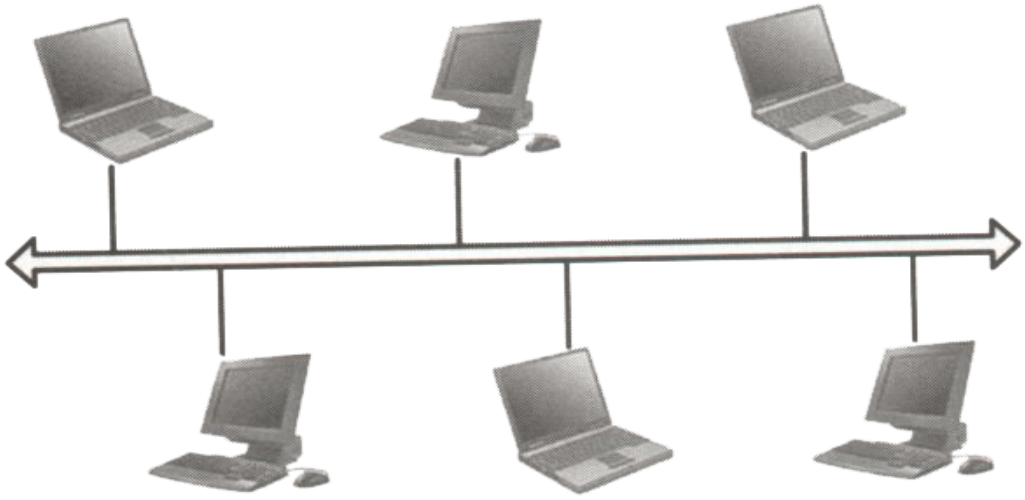
2. Urządzenia sieci LAN

2.1. Topologie sieci

Topologią sieci nazywamy fizyczny układ, geometryczne rozplanowanie najczęściej na planie kwadratu, koła lub trójkąta połączonych ze sobą komputerów. Prawidłowy dobór topologii sieci w procesie planowania i projektowania sieci decyduje o jej przyszłej niezawodności.

1. Topologia magistrali

Topologia magistrali (ang. *bus topology*) opiera się najczęściej na kablu koncentrycznym do którego przyłączone są komputery stanowiące sieć. Jakiś czas temu topologia magistrali była najczęściej spotykaną topologią sieci. Jest łatwa do zainstalowania i można w niej szybko wykryć usterki - to jej dwie decydujące zalety; jednakże ograniczone są w niej dopuszczalne odległości i liczba komputerów. W topologii tej najczęściej funkcję łącza pełni kabel koncentryczny, któremu IEEE nadała kategorię 802.3 10b2 (10 base 2). Sieci 10b2 zwykle przesyłają dane z przepustowością 4 Mb/s na odległości nie przekraczające 185 metrów. Do tego samego kabla przesyłającego dane podłączone są wszystkie komputery - stąd wzięło się pojęcie „magistrali". Sieć magistralowa posiada punkt początkowy i końcowy, zakończone opornikami o wartości 50 Ω [7].



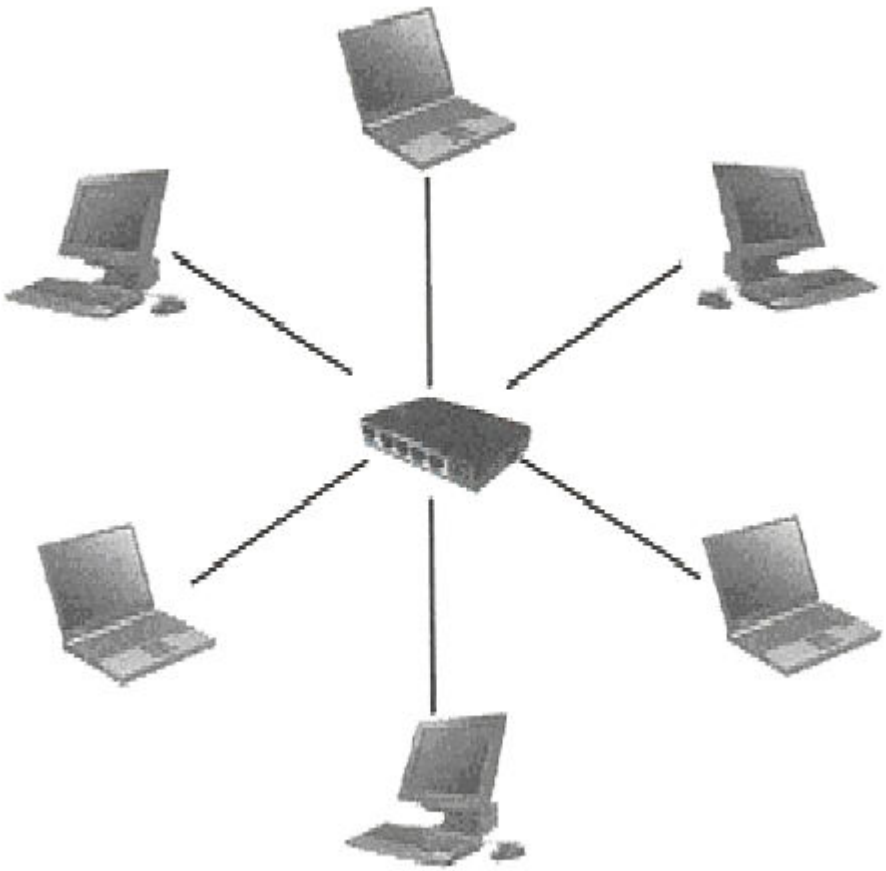
Rys.1. Topologia magistrali; źródło: [16]

Najważniejsze z cech topologii magistrali to:

- ograniczenia co do przepustowości i odległości,
- brak zdolności do komunikacji komputerów w przypadku przerwania kabla,
- łatwość w instalacji i znajdowaniu błędów,

2. Topologia gwiazdy

Wraz ze wzrostem zapotrzebowania na szybsze, bardziej wydajniejsze sieci o większej ilości komputerów opracowano topologie gwiazdy. W topologii tej wszystkie komputery podpięte są do centralnego urządzenia. Najczęściej urządzeniem tym jest przełącznik lub też koncentrator. Jego zadaniem jest przyjmowanie transmisji od nadawcy i w dalszej części przekierowanie danych do odpowiedniego odbiorcy.



Rys.2. Topologia gwiazdy; [16]

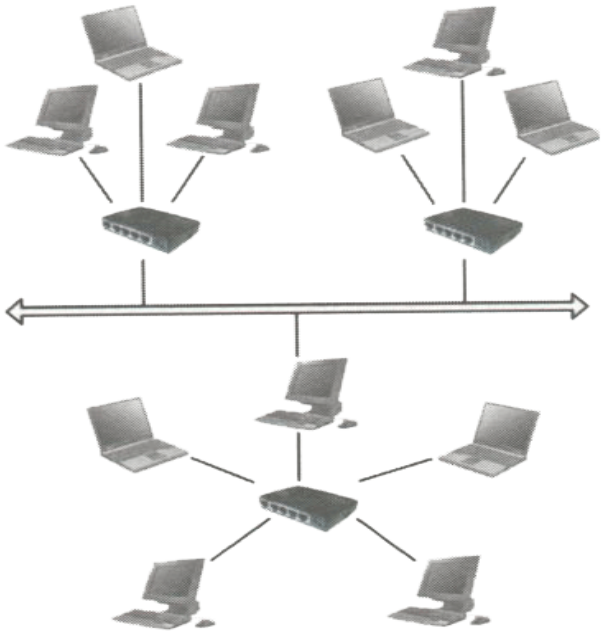
Maksymalna odległość pomiędzy komputerem a urządzeniem centralnym wynosi 100 metrów, jednakże może zostać zwiększona przy zastosowaniu regeneratorów. Sieć oparta o topologię gwiazdy daje możliwość przesyłania danych z prędkością do 1 Gb/s. IEEE sklasyfikował sieć opartą o topologię gwiazdy jako 802.3 10bT.

Topologia gwiazdy ma jedną podstawową przewagę nad innymi topologiami. Odłączenie jednego z komputerów nie wpływa na działanie sieci, która nadal działa bez zarzutów. Ponieważ jednak każdy komputer musi być indywidualnie podłączony do koncentratora, na sieć o topologii gwiazdy zużywa się więcej kabla.

3. Topologia drzewiasta

Topologia drzewiasta jest swego rodzaju odmianą topologii gwieździstej. Węzły połączone są z centralnym hubem, którego zadaniem jest kontrola ruchu w sieci. Jednakże nie zawsze komputer musi być podłączony do centralnego huba, kilka komputerów może być podpiętych do drugiego huba, który to z kolei jest wpięty do centralnego.

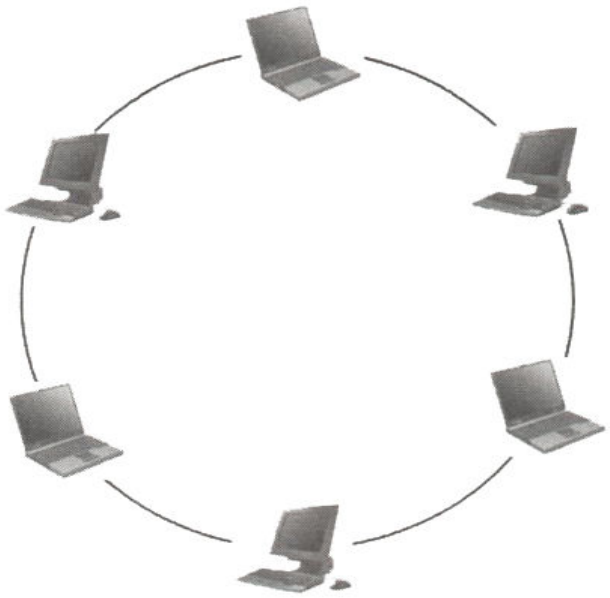
Centralny hub jest aktywny lub posiada repeter, który powtarza sygnał, a ten może wtedy pokonać znacznie większe odległości.



Rys.3. Topologia drzewiasta; źródło: [16]

4. Topologia pierścienia

Technologia Token Ring czyli pierścienia z przekazywaniem żetonu została opracowana przez IBM. Żeton przekazywany jest pomiędzy komputerami sieci i w danej chwili może nadawać lub odbierać ten komputer, który posiada żeton. W sieci dostępny jest tylko jeden żeton i przekazywany jest on w logicznym pierścieniu. Takie rozwiązanie naddawania i odbierania danych w chwili posiadania żetonu powoduje, że w sieci nie dochodzi do kolizji, utraty danych. Żeton może być przesłany 10 000 razy na sekundę w pierścieniu do długości 2 km. [7].



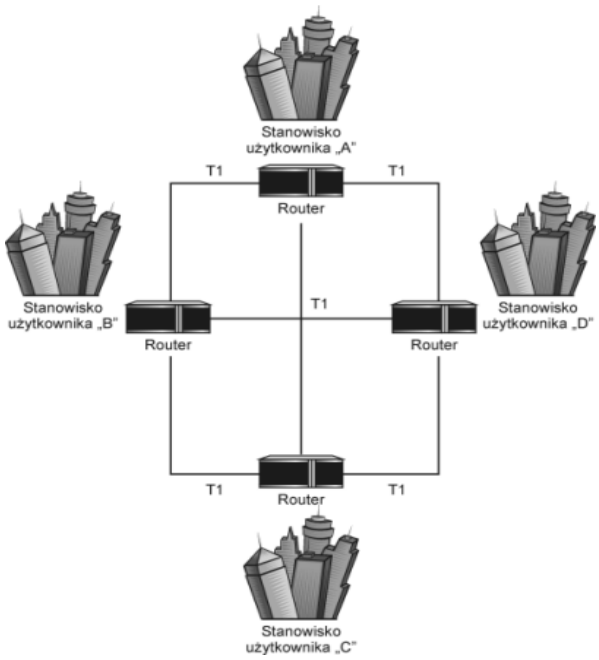
Rys.4. Topologia pierścienia; źródło: [16]

W większości dużych sieci w przypadku stosowania technologii tonek ring stosuje się struktury pierścienia odpornego na błędy. W sytuacji uszkodzenia pierścieni sieć nadal działa używając drugiego pierścienia.

W obecnej chwili, w czasach postępu dążenia do coraz szybszych transmisji danych, najczęściej spotykaną odmianą formą topologii pierścieniowej jest pierścień światłowodowy (ang. *Fiber-Optic Ring*)

5. Topologia oczkowa

Topologia oczkowa (ang. *Mesh*) jest strukturą sieci najbardziej odporną na wszelkiego rodzaju uszkodzenia i przerwy w transmisji. Z powodu dużych wymagań sprzętowych jest ona najczęściej stosowana w przypadku małych sieci. Brak jest w niej nadmiarowych transmisji lub są znikome.

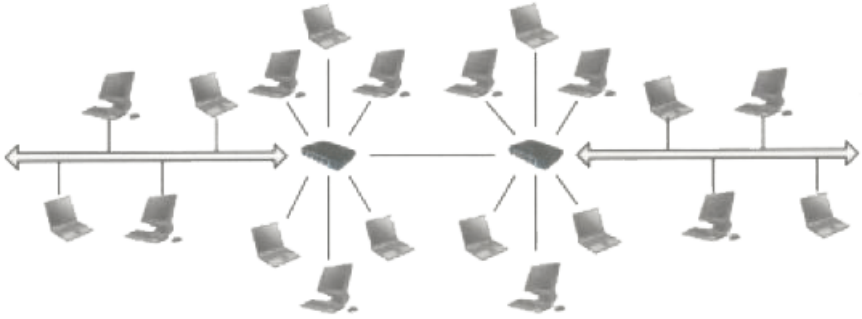


Rys.5. Topologia oczkowa; źródło: [17]

6. Topologie hybrydowe

Coraz częściej powstają sieci, oparte o kilka topologii. Są to sieci hybrydowe łączące w sobie kilka technologii, pozwalające na niezależne funkcjonowanie całych obszarów sieci.

Kilka sieci o topologii gwiazdy może zostać połączonych ze sobą magistralą w jedną spojoną całość, dając w wyniku topologię hybrydową gwiazda-magistrala. Chociaż nie daje ona odporności na uszkodzenia, nie posiada również pojedynczego punktu awarii.



Rys.6. Topologia hybrydowa; źródło: [16]

Uszkodzenie magistrali łączącej sieci o topologii gwiazdy spowoduje, że sieci te będą działać niezależnie. Natomiast w przypadku, kiedy uszkodzeniu ulegnie jeden z koncentratorów, druga sieć o topologii gwiazdy będzie funkcjonować dalej.

Sieci komputerowe można podzielić na kilka kategorii kierując się różnymi ich aspektami.

1. Ze względu na zasięg można wyróżnić następujące rodzaje sieci:
   - sieci lokalne (LAN - *local area network*)
   - sieci rozległe (WAN - *wide area network*)

   W skład sieci lokalnych i rozległych wchodzą jeszcze mniejsze i są to:
   - sieci osobiste PAN (ang. *personal area network*)
   - sieci miejskie MAN (ang. metropolitan area network)
   - sieci obejmujące ośrodki takie jak miasteczka akademickie (akademiki) CAN (ang. - *campus area network*).
2. Ze względu na medium transmisyjne:

a) sieci przewodowe
   - kabel koncentryczny;
   - skrętka;
   - światłowód;

b) sieci bezprzewodowe
   - radiowe (także satelitarne);
   - mikrofalowe;
   - podczerwone;

Idea powstania sieci lokalnych jest bardzo jasna do zrozumienia. Powstały one po to, aby ułatwić administratorom nadzorowanie i administrowanie nimi. Dużo prościej jest zarządzać mniejszymi zadaniami po podzieleniu dużej sieci na kawałki. Sieć LAN może składać się wielu segmentów, czyli części, które połączone są w jedną spójną całość za pomocą trwałego łącza fizycznego i urządzenia sieciowego – routera.

LAN nie zawiera połączeń korzystających z linii telefonicznych lub dzierżawionych. Wszystkie przewody sieci lokalnej należą do niej i nie przesyłają sygnałów niepochodzących od routerów lub komputerów tej sieci. Możemy wyobrazić sobie sieć, jako dziesięciopiętrowy budynek, w którym każde piętro odpowiada segmentowi sieci. Pomiędzy każdą parą sąsiednich pięter znajdują się routery zapewniające łączność pomiędzy piętrami. Routery połączone są przewodami należącymi do sieci, nie do zewnętrznej firmy zajmującej się łącznością. Aby się komunikować między sobą nie potrzebują korzystać z łącza dedykowanego lub dzierżawionego, ponieważ wszelka łączność odbywa się wewnątrz budynku. Sieć nie zawiera linii dzierżawionych, więc uznawana jest za sieć lokalną. Gdy łączność

pomiędzy dwoma obszarami sieci jest zależna od linii dzierżawionych, wówczas połączenie takie nazywane jest łączem sieci rozległej [7].

Poprzez łącza WAN odbywa się większość połączeń internetowych. Są one niezależnym nośnikiem nienależącym do sieci lokalnej. Oznacza to, że łączność wymaga wykupienia od operatora (tv kablowej, sieci telefonicznej) łącza szeregowego odpowiedniej przepustowości dostosowanej do własnych potrzeb. Obecnie na rynku istnieje szereg usługodawców oferujących łącza o rożnej przepustowości. Przepustowość jest to objętość, ilość danych, jakie można przesłać w określonej jednostce czasu. Typowe łącza są wielokrotnością 64 kb/s.

Istnieje zasadnicza różnica pomiędzy nośnikami sieci rozległych, a lokalnych. Łącza WAN są nietrwałe, oznacza to, że lokalny operator przy użyciu jednego kliknięcia może spowodować, iż łącze przestanie istnieć, a komunikacja zostanie ograniczona do łączności lokalnej. W wypadku sieci LAN utrata łączności może być spowodowana jedynie poprzez fizyczne uszkodzenie kabla lub brak w dostawie energii.

Sieci rozległe są zależne od lokalnego operatora, a z ich używaniem wiążą się comiesięczne opłaty. Brak opłaty na rzecz firmy zewnętrznej za łącze komunikacyjne powoduje, że łącze WAN przestaje funkcjonować i pozostaje jedynie łączność lokalna w odrębnych lokalizacjach.

3. Okablowanie strukturalne

3.1. Normy

Tworząc sieć komputerową dobierając okablowanie strukturalne należy pamiętać, aby spełniało ono odpowiednie normy tj. ISO/IEC 11801:2002 lub EN 50173-1:2002 w celu zapewnienia najlepszej, jakości łącza.

Zwiększająca się potrzeba przesyłania danych z coraz to większą prędkością na większe odległości wymusza na producentach okablowania podnoszenia, jakości samych systemów okablowania.

Kategoria 5 standardu ISO/IEC 11801 daje aplikacjom możliwość przenoszenia pasma do 100 MHz włącznie z Gigabitowym Ethernetem.

W czerwcu 2002 roku wprowadzono w USA standard 6 Kategorii, zaś we wrześniu tego samego roku został wprowadzony on w Europie. Według wymogów tego standardu, wydajność winna sięgać do 200/250 MHz dla wszystkich systemów opartych o okablowanie 6 kategorii.

Najbardziej rozpowszechnionym interfejsem 5 i 6 kategorii jest RJ45. Jest on tak zbudowany, że jest w stanie poprawnie działać dla systemów opartych o kategorie 7.

Wzrost znaczenia multimedialnych aplikacji wymusił powstanie nowego standardu kategorii 7 odpowiedniego dla kabli typu PiMF. Aplikacje multimedialne wymagają znacznie większego pasma przenoszenia, dlatego standard kategorii 7 opracowany przez ISO/IEC przeznaczony jest do obsługi aplikacji w paśmie do 600 MHz.

Normy dotyczące okablowania strukturalnego

1. PN-EN 50173-1:2004 oraz ISO/IEC 11801:2002 *„wymienione normy zawierają podstawowe zalecenia dotyczące instalowania okablowania ekranowanego i nieekranowanego. Dokładnie definiują parametry transmisyjne i fizyczne zainstalowanych torów miedzianych i światłowodowych w okablowaniu między budynkowym, pionowym i poziomym. Jako wyznacznik możliwości transmisyjnych torów miedzianych w okablowaniu poziomym wprowadzone jest pojęcie klasy toru, które definiuje rodzaje aplikacji. Zdefiniowane są również kategorie kabli*

światłowodowych OM1, OM2 i OM3, do których przypisane są odpowiednie aplikacje." [10].

2. PN-EN 50174-1:2002 *„Technika informatyczna. Instalacja okablowania. Część 1: Specyfikacja i zapewnienie jakości. Norma zawiera informacje, którymi należy się kierować, aby zapewnić prawidłowe funkcjonowanie sieci okablowania. Określa rodzaje kabli i złącz oraz miejsce ich stosowania dla zapewnienia najwyższej trwałości budowanej sieci. Wprowadza ona zalecenia odnośnie planowania i instalowania sieci, oznaczania testów oraz napraw eksploatacyjnych „[10]*.

3. PN-EN 50174-2:2002 *„Technika informatyczna. Instalacja okablowania. Część 2: Planowanie i wykonawstwo instalacji wewnątrz budynków. Norma zawiera szczegółowe opisy dotyczące planowania oraz instalacji ekranowego i nieekranowanego okablowania strukturalnego miedzianego oraz światłowodowego. Zaleca sposoby zapewnienia właściwych parametrów elektromagnetycznych sieci, prowadzenia uziemień oraz zabezpieczeń przepięciowych. Norma szczegółowo omawia sposoby zakańczania i prowadzenie kabli światłowodowych*" [10].

4. PN-EN 50174-3:2005 *„Technika informatyczna. Instalacja okablowania. Część 3. Planowanie i wykonawstwo instalacji na zewnątrz budynków – norma zawiera szczegółowe opisy dotyczące układania kabli na zewnątrz budynków"* [10].

5. PN-EN 50310:2002 *„Stosowanie połączeń wyrównawczych i uziemiających w budynkach z zainstalowanym sprzętem informatycznym norma definiuje sposoby budowy sieci zasilającej prądu stałego oraz zmiennego, budowy i prowadzenia instalacji uziemiającej oraz zapewnienia właściwego poziomu bezpieczeństwa elektromagnetycznego sieci. Całość zaleceń ma za zadanie zbudowanie sieci zapewniającej bezpieczeństwo pod kątem porażenia prądem elektrycznym"* [10].

6. PN-EN 50346:2002 *„Technika informatyczna. Instalacja okablowania. Badanie zainstalowanego okablowania norma opisuje sposoby testowania sieci okablowania strukturalnego"* [10].

W poniższej tabeli zostały zebrane normy oraz etap ich wykorzystania podczas budowy sieci okablowania strukturalnego w budynku:

Lp.	Etap powstawania sieci	Normy
1.	Projektowanie budynku pod kątem przyszłej sieci teleinformatycznej	PN-EN 50310:2002
2.	Wybór okablowania	PN-EN 50173-1:2004 i/lub ISO/IEC 11801:2002
3.	Planowanie instalacji	PN-EN 50174-1:2002, PN-EN 50174-2:2002, PN-EN 50310:2002
4.	Instalowanie okablowania	PN-EN 50174-1:2002, PN-EN 50174-2:2002, PN-EN 50310:2002, PN-EN 50346:2002
5.	Eksploatacja okablowania	PN-EN 50174-1:2002

Zaprojektowanie prawidłowo działającej sieci LAN wymaga dokładnej analizy potrzeb i możliwości użytkowników sieci oraz uwzględnienia szeregu uwarunkowań infrastruktury, w której sieć będzie działała. Sieć powinna być skalowalna, czyli umożliwiać łatwą rozbudowę. Do oszacowania potrzebnego w sieci pasma należy uwzględnić następujące problemy i zagadnienia:

- Prawo Moore'a zdefiniowane przez współzałożyciela firmy Intel mówiące, że liczba tranzystorów w układach elektronicznych zwiększa się dwukrotnie, co każde 24 miesiące. To powoduje wzrost mocy obliczeniowej komputerów, co pociąga wzrost ruchu w sieci.
- Rosnąca liczba użytkowników. W wielu przedsiębiorstwach oraz instytucjach nieustannie rośnie liczba użytkowników sieci wraz z informatyzacją kolejnych sfer działalności.
- Rozwój Internetu. Ogólny wzrost popularności Internetu powoduje większy ruchu w sieciach lokalnych oraz zmianę profilu ruchu. Zasada 80/20 mówiąca, że 80% ruchu w sieci ma charakter lokalny a tylko 20%

to ruchu związany z siecią WAN, uległa zmianie na 20/80, czyli 80% ruchu jest związana z użytkowaniem Internetu.

- Nowe aplikacje. Większa moc komputerów umożliwia rozwój aplikacji wymagających dużego pasma w sieci, np. multimedia, wideokonferencje.[9]

ETAPY PROJEKTOWANIA SIECI LOKALNYCH

Jakość funkcjonowania sieci lokalnych zależy od precyzyjnego planu projektowania i implementacji, uwzględniającego najważniejsze wykonywane czynności i procedury. [8]

1. Etap przygotowań wstępnych.

1.1. Zbieranie informacji o przedsiębiorstwie.

1.2. Zdefiniowanie problemu.

1.3. Poznanie wymagań użytkowników przyszłego systemu.

1.4. Rozpoznanie zasobów i ograniczeń.

1.5. Przygotowanie raportu dotyczącego zebranych informacji.

2. Etap doboru i projektowania.

2.1. Określenie wymaganego stopnia ochrony systemu.

2.2. Ustalenie sposobu zarządzania systemem.

2.3. Przeprowadzenie konsultacji z przyszłym użytkownikiem.

2.4. Zaprojektowanie diagramu obrazującego przepływ danych.

2.5. Wybranie optymalnej topologii i medium transmisyjnego.

2.6. Przeprowadzeni analizy dostępnego oprogramowania i sprzętu.

2.7. Zaprojektowanie sieci lokalnej.

2.8. Przygotowanie raportu podsumowującego bieżący etap.

3. Etap implementacji.

3.1. Zaplanowanie procesu implementacji.

3.2. Zaplanowanie oprogramowania.

3.3. Instalacja sprzętu.

3.4. Przetestowanie systemu i oprogramowania.

3.5. Opracowanie dokumentacji.

3.6. Przeprowadzenie szkolenia i przeprowadzenie spotkania podsumowującego.

4. **Etap wdrożenia**
    4.1. Przejście do nowego systemu.
    4.2. Czynności rutynowe.
    4.3. Ocena wydajności systemu.
    4.4. Wprowadzenie zmian w systemie. [8]

PRZYKŁADOWA ORGANIZACJA PROJEKTU SIECI LOKALNEJ

1. Inwentaryzacja sprzętu i infrastruktury dostępnej w przedsiębiorstwie.
2. Analiza potrzeb użytkowników.
3. Określenie wymagań projektowych.
4. Projekt logiczny sieci wraz z opisem koncepcji rozwiązania.
5. Projekt okablowania budynków.
6. Analiza niezawodnościowa sieci.
7. Zarządzanie siecią.
8. Kosztorys urządzeń, okablowania i robocizny.
9. Karty katalogowe proponowanych urządzeń. [8]

Bardzo szybko rozwijające się przemysł komputerowy wymusza częste zmiany i modernizacje w działających sieciach lokalnych. Główne powody potrzeby modernizacji sieci to:

- Niezadowoleni użytkownicy narzekający na zbyt wolno działającą sieć.
- Mierzony wzrost obciążenia sieci. Za pomocą specjalnych narzędzi (analizator protokołów, oprogramowanie zarządzające siecią) można monitorować sieć i wykryć przeciążenia sieci.

Wykrycie źródeł przeciążenia sieci wymaga dokładnej analizy architektury sieci oraz używanych technologii sieciowych.

W czasie modernizacji sieci może się pojawić tzw. efekt fali. Jest to związane z tym, że zwiększając pasmo dla grupy roboczej (części użytkowników sieci) możemy spowodować wzrost obciążenia w innym fragmencie sieci [8].

3.2. Elementy okablowania

Elementy systemu okablowania strukturalnego można podzielić na:

- Okablowanie poziome
- Gniazda abonenckie
- Punkty rozdzielcze
- Okablowanie pionowe

Okablowanie poziome stanowi część systemu od gniazda końcowego do punktu dystrybucyjnego. Punkty dystrybucyjne powinny być tak umiejscowione, aby maksymalna długość dowolnego segmentu okablowania poziomego ITP, UTP, nie przekraczała 90m. Zaleca się instalowanie kabla kategorii 5. Zapewni to zgodność z wytycznymi standardów EIA 568A oraz ISO 11801 i kompatybilność w przypadku szybkich zastosowań LAN. W prawidłowo zaprojektowanym systemie okablowania poziomego wszystkie gniazda robocze będą odwzorowane w odpowiednim punkcie dystrybucyjnym. [11]

Główny punkt dystrybucyjny (MDF) umożliwia krosowe przyłączenie kanałów poziomych do portów urządzeń pracujących w sieci, lub do kanału okablowania pionowego. Należy dokonać konwersji wszystkich portów urządzeń systemowych, w taki sposób, aby były dopasowane do urządzeń przyłączonych w punkcie rozdzielczym. W skład MDF wchodzą połączenia systemowe, telekomunikacyjne (głos) oraz LAN.

Pośredni punkt dystrybucyjny (IDF). Każdy punkt dystrybucyjny powinien być usytuowany w takim miejscu, aby długość okablowania poziomego była ograniczona do 90m w celu zagwarantowania kompatybilności z szybkimi aplikacjami LAN. Każdy segment kablowy powinien być jednorodny tzn. bez mostkowania złączy i koncentratorów [11].

Okablowane pionowe (BACKBONE) jest główną magistralą komunikacyjną w budynku. Może on mieć charakter osiedlowy, łącząc kilka budynków, może też być prowadzony pionowo pomiędzy piętrami łącząc kilka pośrednich punktów dystrybucyjnych (IDF) z punktem głównym MDF. Zaleca się stosowanie kabla światłowodowego, jakkolwiek zarówno UTP, jak i kombinacja obu tych mediów jest dopuszczalna. Do możliwych zastosowań zaliczyć można sieci lokalne

szerokopasmowe, sieci z transmisją w paśmie podstawowym, oraz sieci z multipleksowaniem kanałowym [11].

3.3. Media transmisyjne

Okablowanie jest nieodzownym elementem sieci. Winno ono spełniać odpowiednie normy i kategorie w zależności od przeznaczenia sieci, przepustowości oraz wykorzystanych urządzeń do budowy sieci. Wyróżnić można dwa rodzaje mediów w transmisji danych:

- bezprzewodowe media – przesyłanie sygnału przy użyciu fal, rozchodzących się w powietrzu lub kosmosie;
- przewodowe media – przesyłanie sygnału przy użyciu kabli miedzianych, światłowodowych;

W chwili obecnej najczęściej stosuje się kable miedziane zważywszy na ich cenę, chociaż coraz częściej w celu uzyskania większej przepustowości i prędkości transmisji danych stosuje się kable światłowodowe.

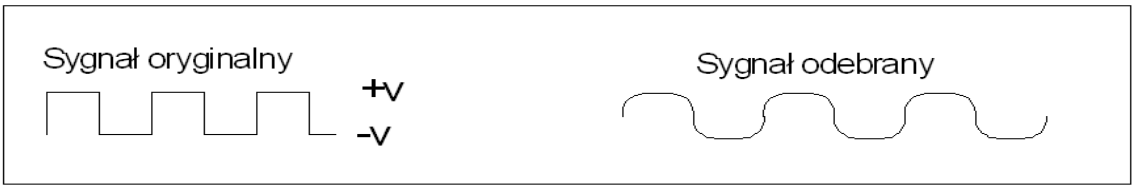
Właściwości kabli sieciowych.

Kable można podzielić na symetryczne i niesymetryczne.

- symetryczne – to takie, w których płynący prąd posiada taką samą wartość natężenia, składają się one z dwóch przewodów, w których prąd płynie w przeciwnych kierunkach, takie rozwiązanie pozwala na drastyczne zmniejszenie zakłóceń oraz szumów. Skrętka jest przykładem kabla symetrycznego;
- niesymetryczne – to takie medium, w którym poprzez przewód sygnałowy płynie prąd, zaś drugi przewód pełni funkcje uziemienia. Przykładem takiego rodzaju kabla może być kabel koncentryczny, w którym to siatka ekranującą pełni funkcje uziemienia; [12]

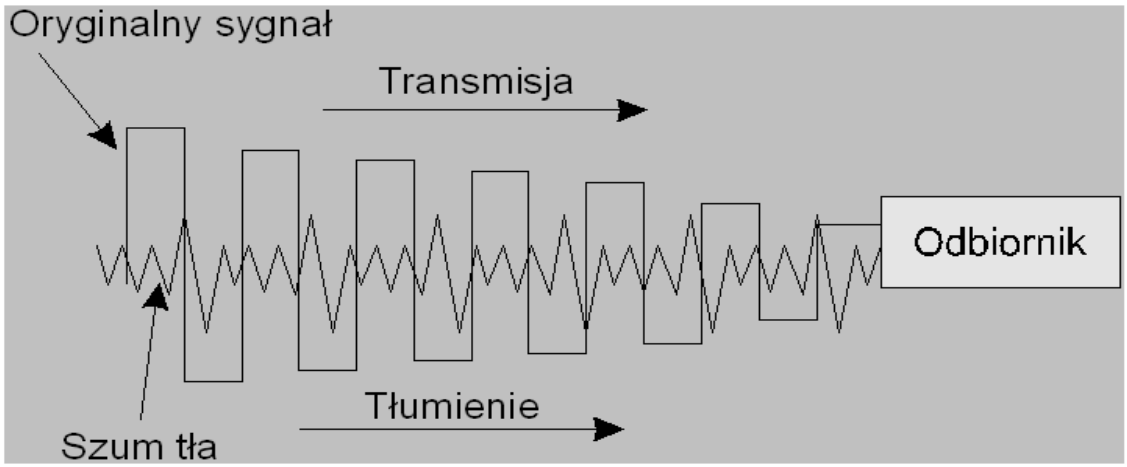
Do najważniejszych parametrów elektrycznych kabli zaliczyć można:

- tłumienie – określa spadek amplitudy sygnału, najczęściej jest to spowodowane, np. impedancją kabla. Efekt tłumienia decyduje o długości kabla, który może zostać wykorzystany do budowy sieci komputerowej. Jeśli długość kabla jest zbyt długa wpłynie to na osłabienie sygnału, a do stacji odbiorczej sygnał nie dotrze lub zostanie on zniekształcony;



Rys.7. Osłabienie sygnału na skutek tłumienia.[5]

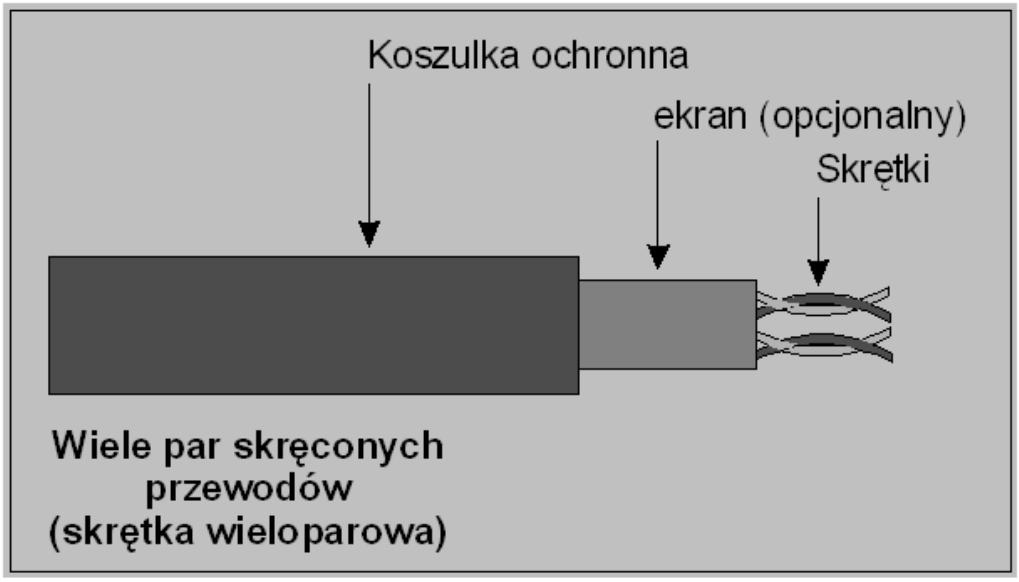
- pojemności pasożytnicze – określają zniekształcenia przesyłanego sygnału, na które ma wpływ grubość izolatora kabla oraz jego długość. Wartości pasożytnicze są tym większe im dłuższy kabel czy też grubszy izolator;
- zniekształcenia i impedancja opóźnieniowa – powoduje, że sygnał, który dociera do odbiornika, a konkretniej jego składniki częstotliwościowe są wzajemnie przesunięte. Na wielkość przesunięci ma wpływ częstotliwość sygnału, wraz z jej wzrostem wzrasta przesunięcie;
- szum tła – wiele urządzeń elektrycznych typu telefony, kuchenki mikrofalowe, bliska obecność innych kabli transmisyjnych powodują szum. W sytuacji, kiedy amplituda szumu jest nieznaczna w porównaniu z amplitudą właściwego sygnału, tłumienie może spowodować wyrównanie amplitudy szumu i sygnału.



Rys.8. Współczynnik sygnał-szum. [5]

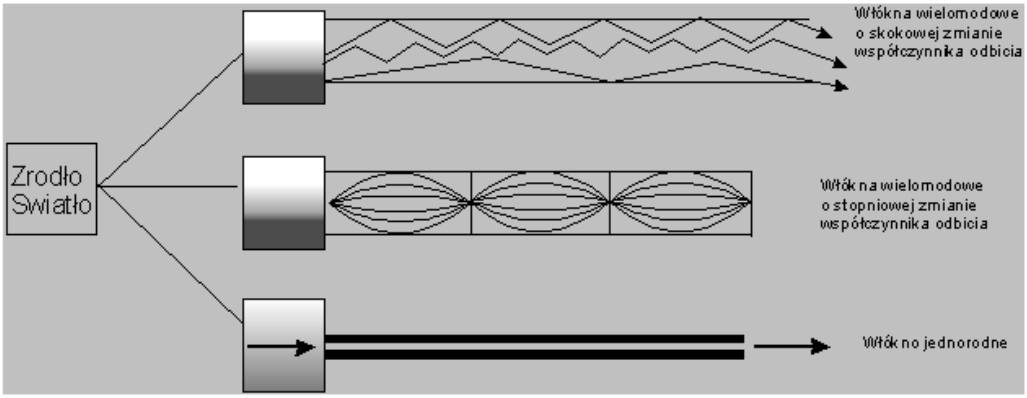
Rodzaje kabli sieciowych (miedzianych).

- kabel **prosty** (ang. *straight cable*) – nie jest stosowany do budowy sieci komputerowych, otoczony jest izolacją I składa się z kilku przewodów miedzianych. Najczęściej wykorzystywany jest do transmisji na niewielkie odległości w celu połączenia urządzeń peryferyjnych;
- **skrętka** (ang. *twisted pair cable*) – to dwa izolowane, splecione przewody. Kabel może być zbudowany z jednej pary takich splecionych przewodów lub z kilku. Do budowy sieci telefonicznych wykorzystuje się skrętkę UTP, czyli nieekranowaną. Standard EIA/TIA 586 określa specyfikację kabla typu skrętka i definiuje jego właściwości: [12]
  - **kategoria 1** - skrętka nieekranowana wykorzystywana do budowy linii telefonicznych, służy do przesyłania jedynie głosu, nie nadaje się do przesyłania danych;
  - **kategoria 2** - skrętka nieekranowana, dwa skręcone przewody służące do transmisji danych z prędkością do 4 Mbit/s;
  - **kategoria 3** - kabel tej kategorii to skrętka zbudowana z 4 par skręconych przewodów, służy do transmisji danych z prędkością do 10 Mbit/s;
  - **kategoria 4** - transmisja danych z prędkością 16 Mbit/s;
  - **kategoria 5** – transmisja danych z prędkością do 100 Mbit/s, kabel o rezystancji 100W, znikomy poziom szumów;



Rys.9. Skrętka [5]

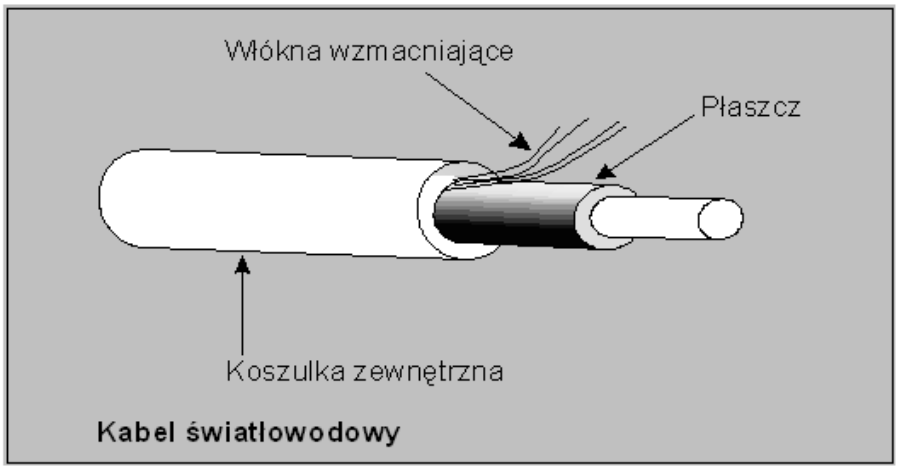
Światłowód jest dużo droższym medium transmisyjnym niż kable metalowe, jednakże nie posiada on tylu wad. W światłowodzie tłumienie jest bardzo małe, jest on odporny na zewnętrzne zakłócenia elektromagnetyczne oraz wokół siebie nie wytwarza pola elektromagnetycznego.



Rys.10. Dyspersja światła w światłowodzie [5]

Przesyłanie danych poprzez światłowód polega na wysyłaniu wiązki światła poprzez włókno szklane. Przechodzące światło przez światłowód odbija się wielokrotnie od powłoki rdzenia. Źródłem światła, nadajnikiem może być laser lub dioda, zaś odbiornikiem najczęściej jest fotodetektor. Załamujące się światło w światłowodzie powoduje, że światło dłużej dociera do drugiego końca przewodu. Jednakże opóźnienia te sięgają miliardowych części sekundy, w przeliczeniu na kilometr to tylko kilkanaście nanosekund. Światłowód daje możliwość transmisji danych z prędkościami sięgających Gbit/s.

Włókno szklane światłowodu wykonane jest z czystego szkła, zaś rdzeń optyczny z krzemu.



Rys.11. Budowa światłowód [5]

Rodzaje światłowodów:

a) plastikowy - tani, przesyła dane na krótkie odległości poniżej kilometra;

b) światłowód krzemiankowy powlekany plastikiem - minimalnie lepszy od plastikowego;

c) jednodomowe włókno – używane do transmisji na duże odległości, rdzeń zapewnia dużą przepustowość dzięki małej średnicy. Przewód ten jest drogi o jednej wiązce światła, jednakże daje możliwość przesyłania danych z dużymi prędkościami na duże odległości.

d) wielodomowe włókno o skokowej zmianie współczynnika światła – przewód o wielu wiązkach światła różnych częstotliwości, duża średnica rdzenia, dyspersja w granicach 15 – 30 nanosekund na kilometr;

e) wielodomowe włókno o stopniowej zmianie współczynnika odbicia – pozwala na przesyłanie danych na duże odległości, dyspersja w granicach 1 nanosekundy na kilometr, wykonany z kilku warstw szkła [13];

4. Projekt sieci

4.1. Założenia projektowe

- ✓ 2 lokalizacje w mieście „Rzeszów”
- ✓ 2 lokalizacje w mieście „Boguchwała”

Działalność firmy

- ✓ Firma komputerowa
- ✓ Magazyn
- ✓ Biurowiec
- ✓ Salon
- ✓ Nazwa „NEOTEK”
- ✓ Budynek 1 w „Rzeszów” – dyrekcja (budynek 2 piętrowy, posiadający centralny węzeł sieci, 11 punktów sieciowych, sala konferencyjna, łączność bezprzewodowa)
- ✓ Budynek 2 w „Rzeszów” – magazyn (budynek parterowy, posiadający 18 punktów sieciowych)
- ✓ Budynek 1 w „Boguchwała” – administracja (budynek parterowy, 40 punktów sieciowych)
- ✓ Budynek 2 w „Boguchwała” – biuro obsługi klienta (budynek 1 piętrowy, duży hall, 20-30 punktów sieciowych)
- ✓ Odległość pomiędzy budynkiem pierwszym i drugim w „Rzeszów” wynosi 3 km, widoczność optyczna
- ✓ Przepustowość połączenia między lokalizacjami budynków w „Rzeszów” wynosi 5 Mb/s, połączenie radiowe 5,8 GHz
- ✓ Przepustowość połączenia między pomiędzy piętrami w budynku 1 w „Rzeszów” wynosi 2 Mb/s
- ✓ Przepustowość połączenia między lokalizacjami budynku 1 i 2 w „Boguchwała” wynosi 2 Mb/s
- ✓ Odległość pomiędzy budynkami w „Boguchwała” wynosi ponad 4 km, brak widoczności optycznej
- ✓ Internet 2 Mb/s – tradycyjne (miedź) + backup radiowy (512 Kb/s)
- ✓ Strona WWW

- ✓ Handlowcy Mobilni (VPN)
- ✓ Serwer Pocztowy
- ✓ Serwer FTP
- ✓ Adresowanie
- ✓ Sieci, podsieci
- ✓ Protokół TCP/IP
- ✓ Systemy Operacyjne na Serwerach
- ✓ Nazwa Domenowa
- ✓ Okablowanie Poziome przepustowość 100 Mb/s
- ✓ Okablowanie Pionowe wynosi 1 Gb/s
- ✓ Okablowanie Poziome (miedź)
- ✓ Okablowanie Pionowe (światłowód)

„Rzeszów" - budynek 1

- ✓ Podział personalny
  - ➢ Dyrekcja (1 dyr.;2 z-c dyr.;2 sekretarki)
  - ➢ Księgowość (15 pkt)
  - ➢ Handlowcy (20 osób + sprzęt (skanery, drukarki) 40pkt)
  - ➢ Informatycy (2 osoby 6 pkt)
  - ➢ Technicy
  - ➢ Ochrona
  - ➢ Dział zamówień (10pkt)
- ✓ Dział projektowy 1 Gb/s
- ✓ Sala konferencyjna z łącznością bezprzewodową + wysokie wymagania ds. bezpieczeństwa
- ✓ Sprzęt
  - ➢ Router
  - ➢ DMZ
  - ➢ Serwer WWW i FTP (jedna maszyna, system wirtualny)
  - ➢ DMZ (Host Bastionowy) – IDS, serwer baz danych, serwer plików, VPN, centralny system antywirusowy, firewall centralny + firewalle na stacjach roboczych)
  - ➢ VLAN, Technicy jedna grupa VLAN

„Rzeszów” – budynek 2 (magazyn 18 pkt)

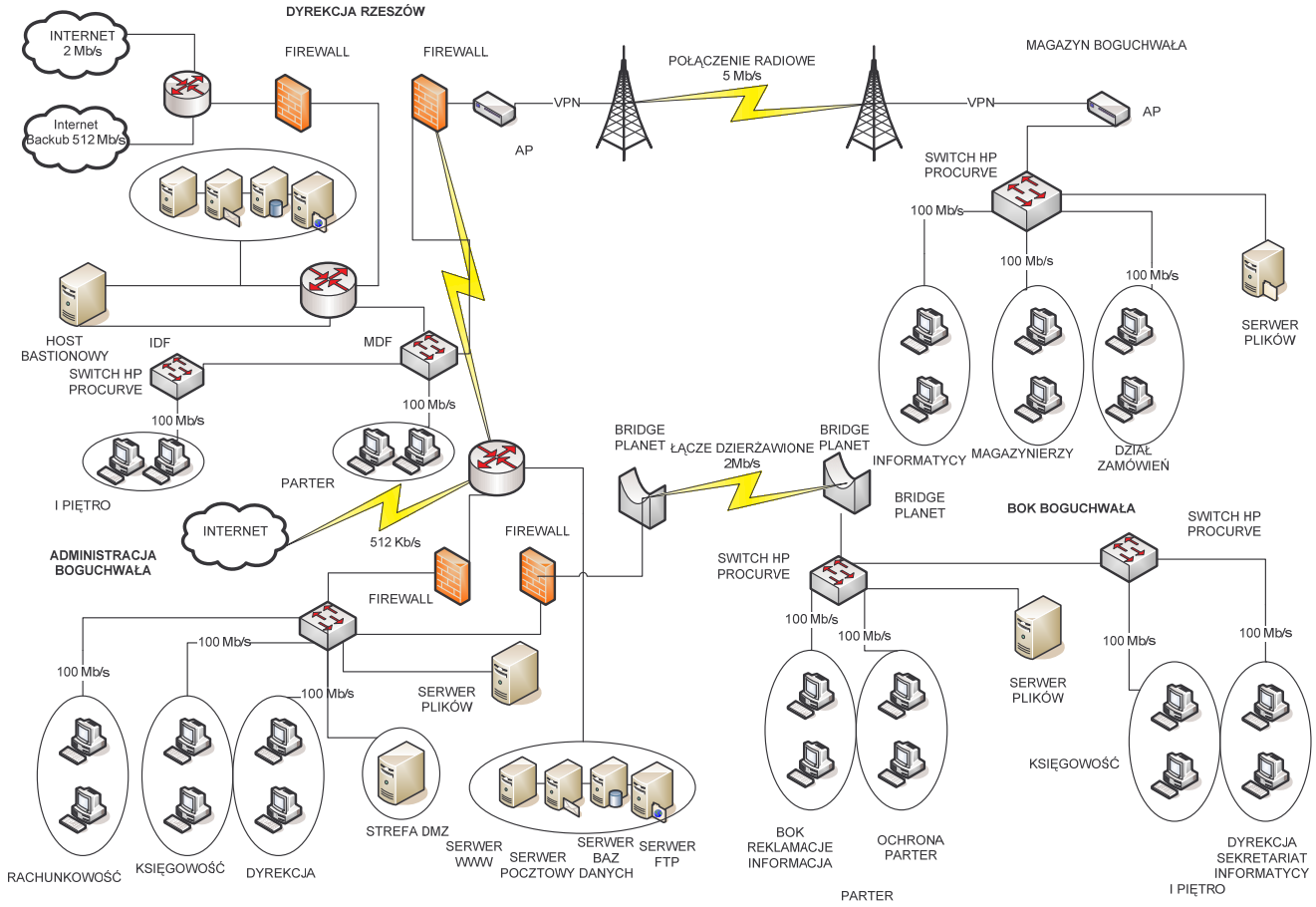
- ✓ Dział techniczny 6 pkt
- ✓ Przyjmowanie zamówień 6 pkt

„Boguchwała” (salon)

- ✓ Hotspot

4.2. Urządzenia aktywne

4.2.1. Ogólny schemat sieci



Rys.12. Ogólny schemat sieci

4.2.2. Opis sieci

Jest to sieć zakładowa, rozproszona na cztery lokalizacje. Provider dostarcza do głównego budynku w „Rzeszów" (budynku dyrekcji) łącze internetowe o przepustowości 2 Mb/s dodatkowo zapewnia backupowe łącze radiowe o przepustowości 512 Kb/s. Łącze to będzie wykorzystywane w razie jakiejś awarii głównego łącza. Ma to na celu zapewnienie ciągłości pracy firmy i nie pozbawienia jej łączności z siecią Internet. Dołączone są one do Routera Cisco 3825. Za routerem występuje firewall sprzętowy firmy Cisco, jest to model PIX 525. Wyodrębniono również strefę DMZ, w której umiejscowione będą serwer WWW, SFTP i serwer pocztowy. W strefie DMZ znajduje się również host bastionowy. Za strefą DMZ umieszczono kolejny router, który będzie bezpośrednio połączony ze switchem HP ProCurve Switch 5304xl-32G. Router ten łączy się również z firewallem. Będzie to główny switch w budynku, który tworzyć będzie główny punkt dystrybucyjny sieci (MDF). Do tego switcha wpięci zostaną handlowcy (grupa VLAN 5). Jako jedyni mają łącze o przepustowości 1 Gb/s, czyli gigabit Ethernet. Aby umożliwić taką przepustowość switch zostanie dodatkowo wyposażony w moduł 16 portowy 10/100/1000 do przełącznika ProCurve 5300XL, który umożliwia obsługę gigabit Ethernet. Wszystko to zostanie zrealizowane na zwykłych kablach miedzianych zakończonych RJ45.

Switch ten jest połączony z dwoma pozostałymi switchami w budynku kablami światłowodowymi, co stanowi szkielet okablowania pionowego. Te dwa switche tworzą dwa osobne IDF-y. Wymienione switche to HP ProCurve model 5304xl pracujący na I piętrze budynku i switch HP ProCurve 5304xl-32G umieszczony na II piętrze budynku. Łącze światłowodowe zakończone złączem LC. Wymusza to zastosowanie we wszystkich switchach modułów ProCurve switch XL mini-GBIC i Mini-GBIC do ProCurve Gigabit-LX-LC. Na obu piętrach użytkownicy mają łącze o przepustowości 100 Mb/s. Każde piętro to jedna grupa VLAN.

Z głównym switchem współpracują jeszcze dwa serwery, lokalny serwer plików i serwer baz danych.

Poprzez switch główny znajdujący się w MDF-ie budynek główny (dyrekcja) połączony jest z magazynem w „Rzeszów". Połączenie odbywa się poprzez sieć radiową. Przepustowość tej sieci wynosi 5 Mb/s. Połączenie to wykonane jest w technologii 5.8 GHz. Połączenie będzie odbywać się poprzez VPN (Virtual Private

Network - wirtualną sieć prywatną). Taką możliwość zapewnia zastosowanie firewalla PIX 525, który posiada wbudowaną obsługę VPN. W celu zwiększenia wydajności sieci, poprzez VPN firewall ten dodatkowo zostanie wyposażony w PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+) , kartę akceleracji szyfrowania. Po obu stronach sieci znajdować się będą urządzenia Access Point. Access Point znajdujący się w magazynie jest bezpośrednio łączony z switchem. W budynku znajduje się tylko jeden switch ProCurve Switch 5304xl z obsługą 16 portów 100 Mb/s. Do niego wpięci są wszyscy użytkownicy znajdujący się w tym budynku. Są podzieleni na 2 grupy VLAN. Informatycy grupa VLAN 2 i dział zamówień VLAN 4 Wewnątrz budynku sieć jest rozprowadzona poprzez tradycyjny kabel miedziany. W budynku dodatkowo znajduje się lokalny serwer plików wpięty bezpośrednio do switcha.

Z głównego budynku w „Rzeszów" (dyrekcja) będzie poprowadzone łącze dzierżawione do budynku firmy znajdującego się w „Boguchwała". Łącze to będzie posiadać przepustowość 2 Mb/s. Łącze to jest bezpośrednio wpięte do routera w „Boguchwała". Do tego samego urządzenia będzie doprowadzone łącze internetowe o przepustowości 512 Kb/s. Będzie to łącze dostarczone przez providera z „Boguchwała". W tym przypadku będzie to TP S.A a będzie to łącze DSL. Takie rozwiązanie zapewni swego rodzaju autonomię oddziału w „Boguchwała" w razie wystąpienia jakiejkolwiek awarii głównego łącza. Za routerem znajduje się firewall PIX 525 firmy Cisco a za nim switch ProCurve Switch 5304xl-32G dodatkowo wyposażony w 16 portów 100 Mb. Umożliwi to podłączenie 48 użytkowników.

W budynku tym będzie się mieścił tylko jeden punkt dystrybucyjny, do którego będą przyłączeni wszyscy użytkownicy. Do tego switcha przyłączone są serwer plików oraz pracownicy podzieleni na 3 grupy VLAN. Każda grupa VLAN ma dostęp do łącza o przepustowości 100 Mb/s. Serwery usługowe będą podłączone do routera. Będą to kopie danych znajdujących się na serwerach głównych pracujących w „Rzeszów". Pomiędzy serwerami w budynku dyrekcji w „Rzeszów" a tymi znajdującymi się w „Boguchwała" będzie przeprowadzana synchronizacja danych. Będzie zastosowany tzw mirroring. Pozwoli to w razie awarii łącza korzystać z danych umieszczonych na lokalnych serwerach w „Boguchwała". W przypadku odzyskania łączności dane będą automatycznie aktualizowane i synchronizowane.

Z tego switcha jest poprowadzone łącze do Biura obsługi klienta (BOK) w „Boguchwała". Dodatkowo za switchem umiejscowiono firewall PIX 525, który ma za zadanie filtrować pewne usługi. Biorąc pod uwagę, że sama linia dzierżawiona jest

łączem bezpiecznym, nie ma możliwości dostępu do niego z, zewnątrz więc nie jest wymagana jakaś skomplikowana ochrona tego łącza. Zastosowanie tutaj firewalla ma jedynie usprawnić działanie sieci i umożliwić cały czas prace z wysoką przepustowością. Połączenie to będzie miało przepustowość 2 Mb/s, odbywać się będzie poprzez linie dzierżawioną. Połączenie będzie zestawione poprzez wykorzystanie mostów (Bridges) firmy Planet. Będą to modele GRT-101. Umożliwiają one maksymalną przepustowość na poziomie 2,3 Mb/s na odległość do 6,7 km. W tym wypadku urządzenia te będą wystarczające. Następnie w BOK będą umiejscowione dwa switche, każdy na jedno piętro budynku. Połączenie pionowe będzie realizowane kablem światłowodowym o przepustowości 1 Gb/s i zakończone złączem LC. Na parterze znajdować się będzie switch HP ProCurve 5304xl wyposażony w 16 portowy moduł 100 Mb. Na I piętrze pracować będzie przełącznik ProCurve Switch 5304xl wyposażony w moduł 24 portów 10/100Base-T. Do obsługi światłowodu wymagane będą w obu przypadkach ProCurve switch XL mini-GBIC i Mini-GBIC do ProCurve Gigabit-LX-LC.

4.2.3. Adresowanie

Provider przydziela nam adresy z następującej klasy połączeniowej 212.51.192.0/30 Adres bramy będzie następujący 212.51.192.1/30 nasz adres zewnętrzny będzie to adres 212.51.192.5/30. Dodatkowo kolejna klasa połączeniowa będzie obejmować adresy dla połączenia backupowego. Będzie to klasa w postaci 80.200.50.0/30. Adres bramy będzie w postaci 80.200.50.1/30 a nasz adres zewnętrzny 80.200.50.5/30

Serwery usługowe typu WWW, serwer pocztowy i SFTP będą dostępne pod adresem publicznym

Provider w „Boguchwała” przydzieli adres z klasy połączeniowej 83.260.1.0/30 Adres bramy będzie następujący 83.260.1.1/30 Będzie to adres typowy dla usługi DSL. Adres zewnętrzny (publiczny) to 83.260.1.5/30

Cała sieć lokalna LAN (Local Area Network) zostanie podzielona na trzy podsieci:

Podsieć 1

Ta podsieć obejmie wszystkie komputery zlokalizowane w „Rzeszów" oraz serwery plików i serwer baz danych.

Wykorzystana pula adresów:	**192.168.1.0 – 192.168.1.127**
Maska:	**255.255.255.128**
Skrócony zapis adres/maska	**192.168.1.0 – 192.168.1.127/25**

Podsieć 2

Podsieć druga to wszystkie komputery pracujące w „Boguchwała" i serwery plików tam się znajdujące

Wykorzystane pule adresów:	**192.168.2.0 – 192.168.2.63**
	192.168.2.64 – 192.168.2.127
Maska:	**255.255.255..192**
Skrócony zapis adres/maska	**192.168.2.0 – 192.168.2.63/26**
	192.168.2.64 – 192.168.2.127/26

Podsieć 3

Podsieć trzecia przypadnie na urządzenia aktywne pracujące w sieci. Umieszczenie ich w osobnej podsieci umożliwi ich lepszą konfiguracje i zapobiegnie próbom konfiguracji przez osoby znajdujące się w innych podsieciach.

Na urządzenia przypadnie 18 adresów, więc pula zawierająca 32 adresy będzie wystarczająca. Umożliwi to nawet w przyszłości jakaś dalszą rozbudowę

Wykorzystana pula adresów:	**192.168.3.0 – 192.168.3.31**
Maska:	**255.255.255.224**
Skrócony zapis adres/maska	**192.168.3.0 – 192.168.3.31/27**

Podsieć 4

Dodatkowa czwarta podsieć będzie obejmować wszystkie telefony IP pracujące w sieci. Będzie ich 170, zostaną więc jeszcze wolne adresy w przypadku rozbudowy firmy.

Wykorzystane pule adresów:	**192.168.4.0 – 192.168.4.127**
	192.168.4.128 – 192.168.4.255
Maska:	**255.255.255.128**
Skrócony zapis adres/maska	**192.168.4.0 – 192.168.4.127/25**
	192.168.4.128 – 192.168.4.255/25

Router główny znajdujący się w „Rzeszów” będzie posiadał 3 interfejsy. Będą to trzy interfejsy Ethernetowi. Interfejs zewnętrzny, do którego będzie przyłączone stałe łącze internetowe dostarczone przez providera.

Adres na interfejsie zewnętrznym – 212.51.192.5 (stałe łącze internetowe)

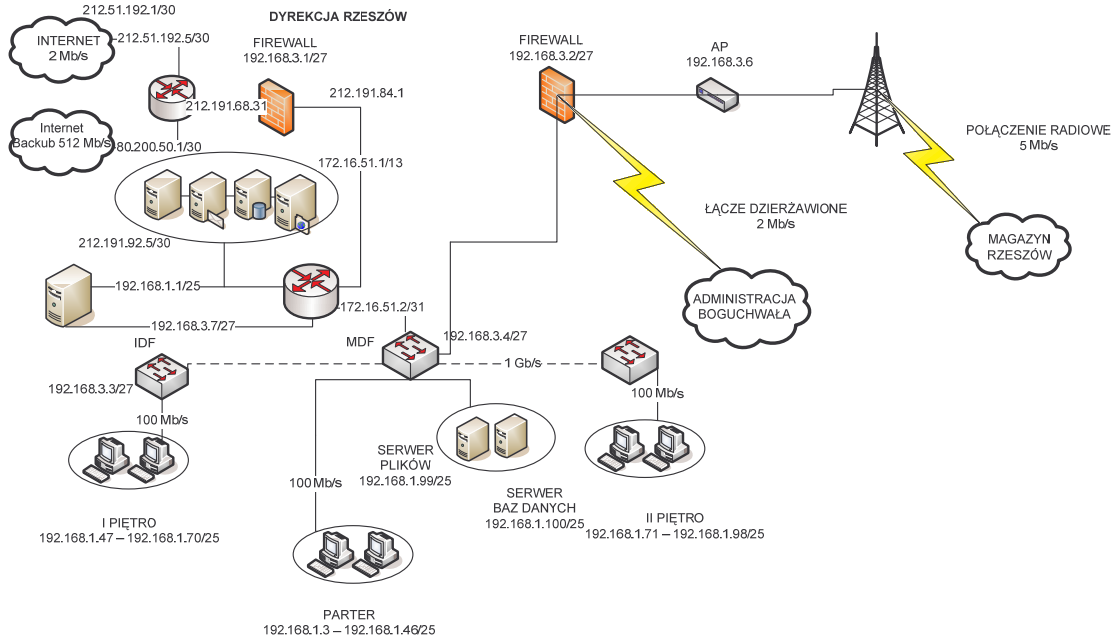
Adres na drugim interfejsie zewnętrznym – 80.200.50.5 (łącze backupowe)

Kolejny router umieszczony w „Rzeszów”, będzie również posiadał 3 interfejsy Ethernetowi. Router pracujący w „Boguchwała” będzie wymagał dodatkowego wyposażenia w kartę DSL do obsługi połączenia internetowego ADSL. Będzie to ADSL WAN INTERFACE CARD (WIC’s).

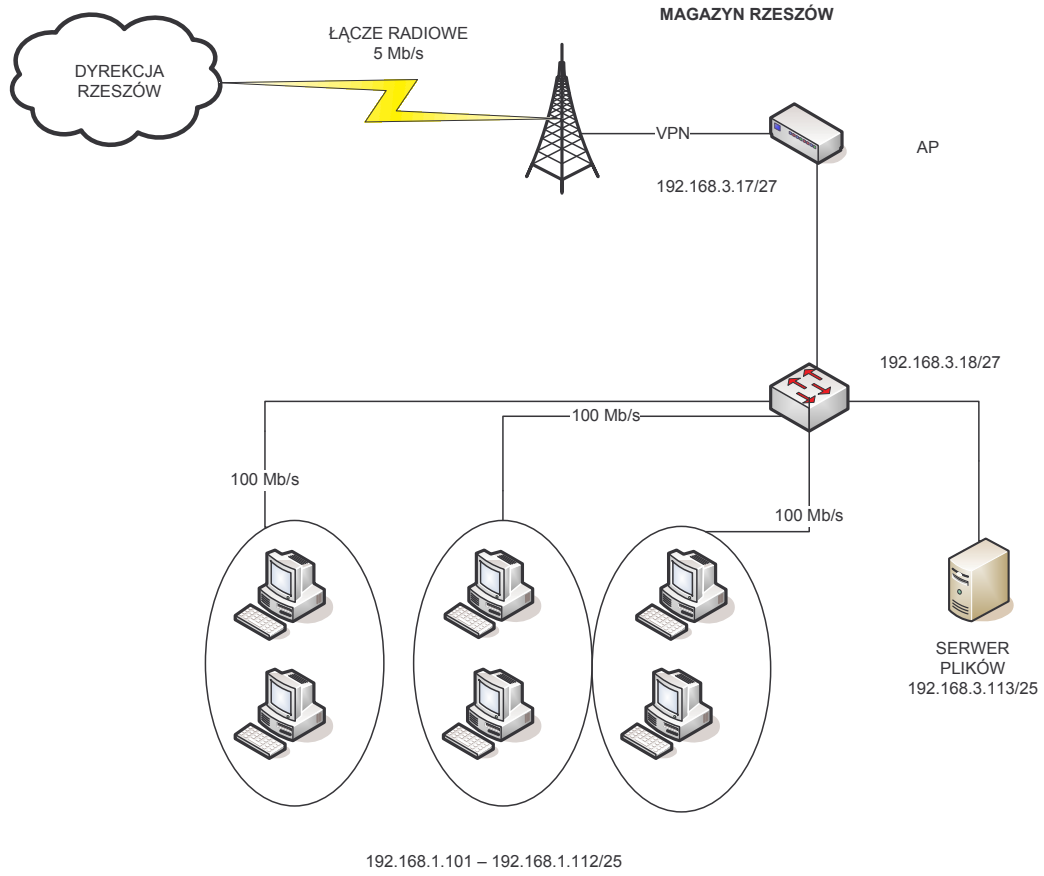
Pozostałe 3 interfejsy będą to interfejsy Ethernetowe.

Adres na interfejsie zewnętrznym – 83.260.240.180 (łącze internetowe ADSL)

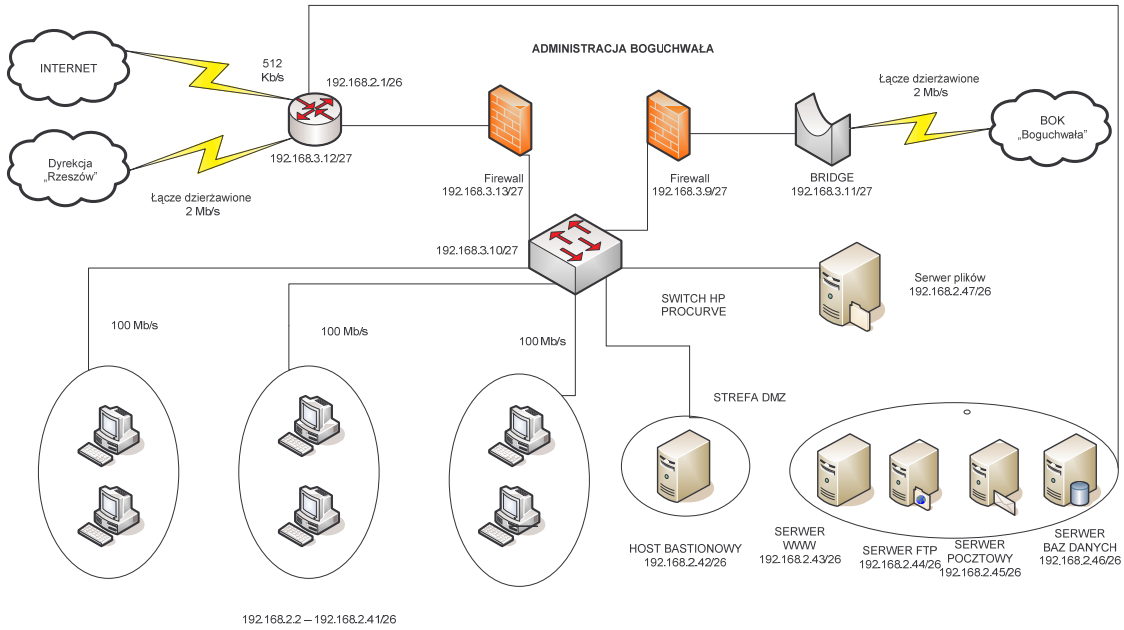
Adres na interfejsie wewnętrznym – 192.168.2.1



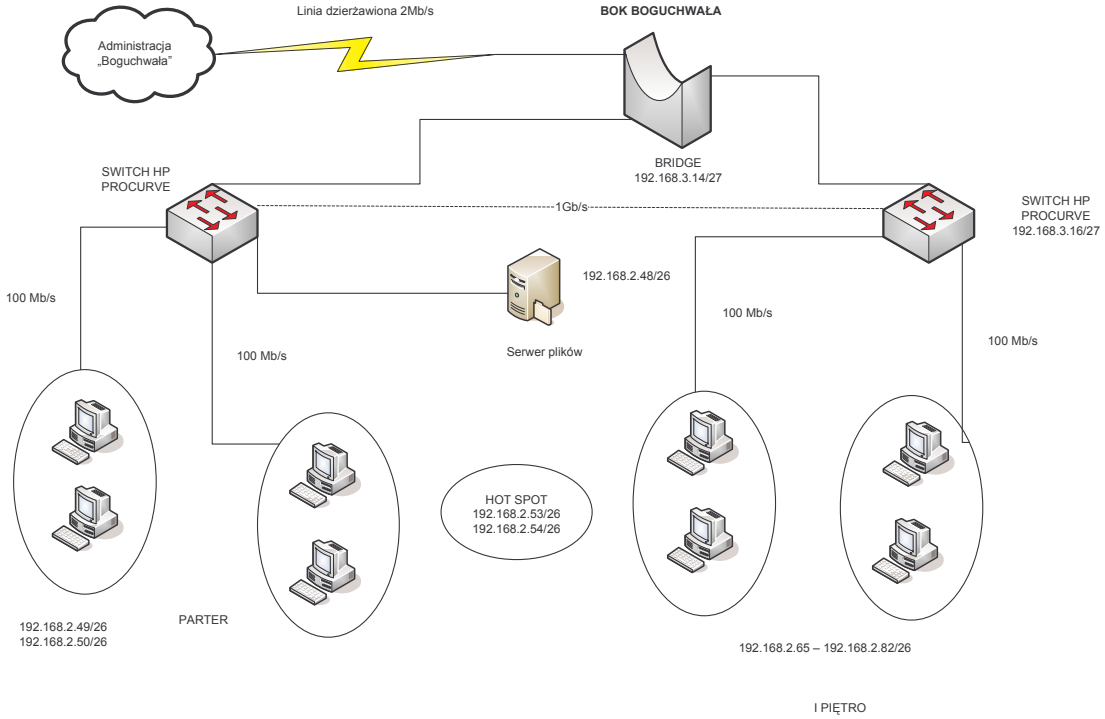
Rys.13. Adresowanie Dyrekcja „Rzeszów”



Rys.14. Adresowanie magazyn „Rzeszów”



Rys.15. Administracja „Boguchwała”



Rys.16. Adresowanie BOK „Boguchwała"

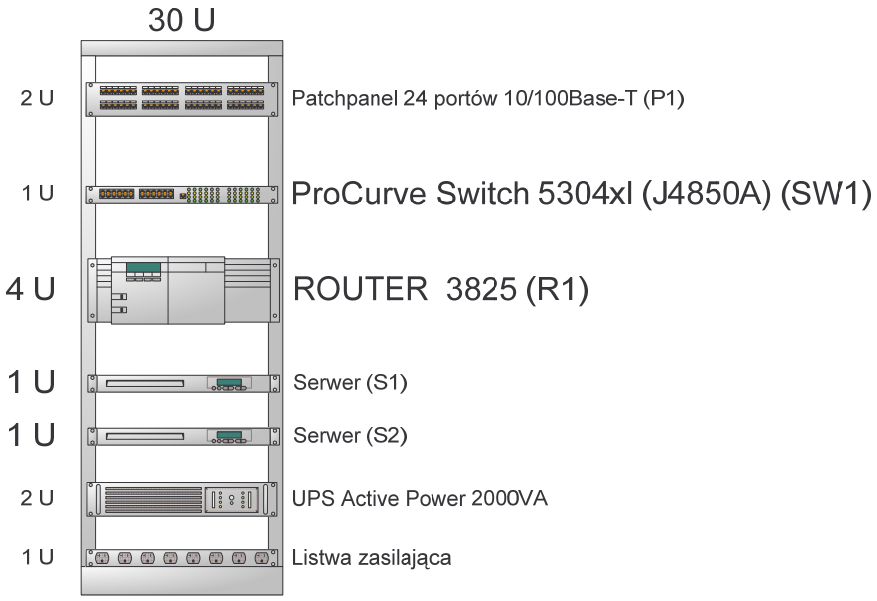
4.2.4. Plany budynków – rozmieszczenie urządzeń w szafach krosowniczych

Na potrzeby sieci zostaną zakupione trzy szafy krosownicze: dwie wiszące umieszczone na I i II piętrze oraz jedna stojąca umieszczona na parterze.

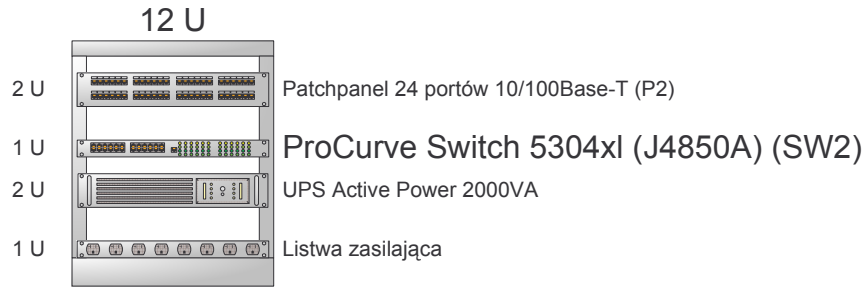
W szafie stojącej zostaną zamontowane:

- switch (SW1)
- router (R1)
- UPS

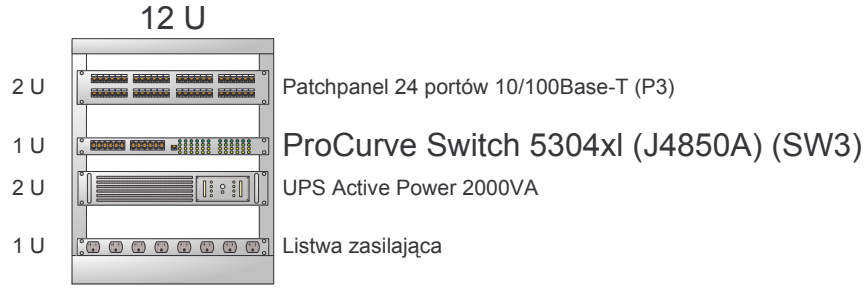
W szafie wiszącej na pierwszym piętrze zostanie zamontowany switch (SW2), a w szafie na piętrze drugim switch SW3. Zastosowane panele krosownicze zapewnią pełną funkcjonalność nowej sieci. Poniżej znajduje się schemat rozmieszczenia urządzeń w szafach na poszczególnych piretrach.



Rys.17. Szafa stojąca parter – rozmieszczenie urządzeń



Rys.18. Szafa wisząca piętro 1 – rozmieszczenie urządzeń



Rys.19. Szafa wisząca piętro II – rozmieszczenie urządzeń

Patchpanel P1											
1	2	3	4	5	6	7	8	9	10	11	12
A0-1-1,1	A0-1-2,1	A0-2-1,1	A0-3-1,1	A0-4-1,1	A0-5-1,1	A0-6-1,1	A0-7-1,1	-	-	-	-
13	14	15	16	17	18	19	20	21	22	23	24
-	-	-	-	-	-	-	-	-	-	-	
Patchpanel P2											
1	2	3	4	5	6	7	8	9	10	11	12
A1-1-2,1	A1-1-1,1	A1-2-1,1	A1-2-2,1	A1-3-1,1	A1-4-1,1	A1-5-1,1	A1-6-1,1	A1-7-1,1	-	-	-
13	14	15	16	17	18	19	20	21	22	23	24
-	-	-	-	-	-	-	-	-	-	-	
Patchpanel P3											
1	2	3	4	5	6	7	8	9	10	11	12
A2-1-1,1	A2-1-2,1	A2-2-1,1	A2-3-1,1	A2-4-1,1	A2-5-1,1	A2-6-1,1	A2-7-1,1	-	-	-	-
13	14	15	16	17	18	19	20	21	22	23	24
-	-	-	-	-	-	-	-	-	-	-	

Rys.20. Schemat połączeń wyprowadzonych z paneli krosowniczych

Oznaczenia i wyliczenia kabla prezentuje poniższa tabelka

PARTER		I PIĘTRO		II PIĘTRO	
OZNACZENIE	DŁUGOŚĆ	OZNACZENIE	DŁUGOŚĆ	OZNACZENIE	DŁUGOŚĆ
A0-1-1,1	7	A1-1-2,1	4	A2-1-1,1	7
A0-1-2,1	2	A1-1-1,1	7	A2-1-2,1	9
A0-2-1,1	12	A1-2-1,1	5	A2-2-1,1	15
A0-3-1,1	22	A1-2-2,1	9	A2-3-1,1	25
A0-4-1,1	32	A1-3-1,1	15	A2-4-1,1	35
A0-5-1,1	42	A1-4-1,1	32	A2-5-1,1	45
A0-6-1,1	72	A1-5-1,1	42	A2-6-1,1	72
A0-7-1,1	82	A1-6-1,1	72	A2-7-1,1	82
		A1-7-1,1	82		
Łącznie	271	Łącznie	268	Łącznie	290
Całkowita długość kabla 829 m					

Rys.21. Długości kabla pomiędzy gniazdami sieciowymi

4.2.5. VLAN

Z uwagi na duże rozproszenie firmy, ich poszczególnych działów, ważnym elementem budowy sieci będzie stworzenie kilku grup VLAN (Virtual Local Area Network).

Umożliwi to logiczne (wirtualne) pogrupowanie stacji roboczych niezależnie od tego, gdzie będą one fizycznie zainstalowane w sieci. Cała sieć fizyczna zostanie podzielona na elementy logiczne, nie zważając na to, w którym segmencie sieci są zainstalowane różne stanowiska pracy. Pozwali to na łatwe skalowanie sieci, skuteczne zarządzanie przepływnością poszczególnych jej odcinków i kontrolę przepływu informacji między wirtualnymi segmentami sieci.

Zakłada się stworzenie 5 grup VLAN. Założeniem jest pogrupowanie każdego newralgicznego działu firmy w jedną sieć wirtualną. Ułatwi to wymianę informacji pomiędzy danymi działami oraz zwiększy kontrolę nad przepływem informacji pomiędzy nimi.

Z tego względu działy księgowości, dyrekcji i sekretariatu rozmieszczone w budynkach w „Rzeszów", „Boguchwała" (administracja) i „Boguchwała" (BOK) będą tworzyć jedna grupę VLAN (VLAN 1). Cała grupa będzie obejmować ok. 50 punktów sieciowych. Dla tych działów ważnym elementem jest skuteczny zarządzanie przepływem informacji, stworzenie z nich wirtualnej grupy roboczej, znacznie ułatwi prace i oddzieli od reszty sieci, do której ich dostęp jest niepotrzebny. Księgowość w budynku w „Boguchwała" ma 6 punktów sieciowych, połączona jest z księgowością oraz z rachunkowością w „Boguchwała" (budynek Administracja) i z księgowością w BOK w „Boguchwała" (14 punktów abonenckich). Dyrektor, zastępcy dyrektora i sekretarki razem mają 13 punktów abonenckich. Połączeni są z dyrekcją w „Boguchwała" (Administracja), i z dyrekcja oraz sekretariatem BOK w „Boguchwała".

Kolejną grupę VLAN stanowić będzie dział handlowców VLAN 5. Z uwagi na to, że ten dział jest bardzo ważny dla całego funkcjonowania firmy ważne jest stworzenie dla nich optymalnych warunków pracy. Dlatego też w celu zwiększenia przepływu informacji i niezależności zakłada się stworzenie dla nich grupy VLAN (VLAN 5). Dział ten będzie często miedzy sobą wymieniał dużo informacji poprzez sieć, ma duże wymagania, dlatego tez takie rozwiązanie jest jak najbardziej wskazane.

Kolejna grupa VLAN będzie grupować pracowników ochrony i portierni ze wszystkich budynków. Ochrona w budynku dyrekcji w „Rzeszów" będzie połączona z ochrona i portierem w BOK w „Boguchwała", z administracją w „Boguchwała" i magazynem w „Rzeszów". Będzie to VLAN 3.

Dział informatyków wymaga również stworzenia grupy VLAN. Informatycy z budynku magazynu w „Rzeszów" połączeni zostaną z informatykami w budynku dyrekcji w „Rzeszów" oraz z informatykami w budynku w BOK („Boguchwała") i administracji (2 VLAN).

Dział zamówień („Rzeszów" dyrekcja) połączony będzie z działem bok/reklamacje/informacje w „Boguchwała" i z magazynem w „Rzeszów" to będzie 4 VLAN. Dział zamówień musi na bieżąco posiadać informacje z magazynu o ilości i rodzajach towaru, a także z działem BOK informacji/reklamacji, aby moc poinformować klienta o ewentualnym terminie odbioru reklamowanego produktu.

LP	VLAN	DZIAŁY	LOKALIZACJA
1	VLAN 1	Dyrekcja Księgowość Rachunkowość Sekretariat	Dyrekcja („Rzeszów"), BOK („Boguchwała") Dyrekcja („Rzeszów"), BOK („Boguchwała") Administracja („Boguchwała") Dyrekcja („Rzeszów"), BOK („Boguchwała")
2	VLAN 2	Informatycy	BOK („Boguchwała") Magazyn („Rzeszów") Dyrekcja („Rzeszów") Administracja („Boguchwała")
3	VLAN 3	Ochrona Portiernia	„Rzeszów" (Dyrekcja) BOK („Boguchwała")
4	VLAN 4	Zamówień Reklamacje / Informacje	„Rzeszów" (Dyrekcja) BOK („Boguchwała")
5	VLAN 5	Handlowy	„Rzeszów" (Dyrekcja)

4.2.6. Sprzęt zestawienie

W niniejszym podrozdziale przedstawiono dane techniczne najważniejszych urządzeń, które będą instalowane w poszczególnych budynkach. Zestawienie to nie stanowi faktycznego stanu ilościowego poszczególnych urządzeń. Tworząc należy wzorować się na schematach sieci i kosztorysie.

Dyrekcja w „Rzeszów"

Wyposażenie serwerowni (parter) główny punkt dystrybucyjny sieci (MDF)

URZĄDZENIE	**OPIS**			**WYSOKOŚĆ**	**ILOŚĆ**	**POBÓR MOCY**
Przełącznik ProCurve Switch 5304xl-32G	32 porty 10/100/1000			3U	1	630 W
	Moduł 16-portowy	16 portów 10/100/1000				
	moduł światłowodowy	ProCurve switch XL mini-GBIC	4 wolne gniazda mini-GBIC			
		Mini-GBIC do ProCurve Gigabit-LX-LC	z jednym portem 1000Base-LX			
Firewall PIX 525-UR-GE Bundle Chassis	oprogramowanie Unrestricted. SW, 2 GE+2 F)			2U	1	120W
	KARTA AKCELERACJI DO PIX 525 (PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+))					
	PIX 10/100 Fast Ethernet interface card, RJ45					
Firewall PIX 525-FO-GE Bundle	(Chassis, Failover SW,2				1	120W

	GE+2 F)					
Router CISCO 3825				2U	2	360 W

Wyposażenie reszty budynku (1 piętro) IDF

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl	moduł 24 portów 10/100Base-T			3U	1	630 W
	moduł światłowodowy	ProCurve switch XL mini-GBIC	4 wolne gniazda mini-GBIC			
		Mini-GBIC do ProCurve Gigabit-LX-LC	z jednym portem 1000Base-LX			

Wyposażenie reszty budynku (2 piętro) IDF

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl-32G	32 porty 10/100/10			3U	1	630 W
	moduł światłowodowy	ProCurve switch XL mini-GBIC	4 wolne gniazda mini-GBIC			
		Mini-GBIC do ProCurve Gigabit-LX-LC	z jednym portem 1000Base-LX			

Magazyn w „Rzeszów”

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl	16 portów 10/100/1000			3U	1	630 W

Administracja w „Boguchwała”

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl-32G	32 porty 10/100/100			3U	1	630 W
	16 portów 10/100/1000					
Firewall PIX 525-FO-GE Bundle	(Chassis, Failover SW,2 GE+2 F)			2U	2	120 W
Router CISCO 3825				2U	1	360 W
Bridge Planet	GRT-101				1	6 W

BOK w „Boguchwała”

IDF (parter)

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl	16 portów 10/100/10			3U	1	630 W
	moduł światłowodowy	ProCurve switch XL mini-GBIC	4 wolne gniazda mini-GBIC			
		Mini-GBIC do ProCurve Gigabit-LX-LC	z jednym portem 1000Base-LX			
Bridge Planet	GRT-101				1	6 W

IDF (I piętro)

URZĄDZENIE	OPIS			WYSOKOŚĆ	ILOŚĆ	POBÓR MOCY
Przełącznik ProCurve Switch 5304xl	24 portów 10/100Bas			3U	1	630 W
	moduł światłowodowy	ProCurve switch XL mini-GBIC	4 wolne gniazda mini-GBIC			
		Mini-GBIC do ProCurve Gigabit-LX-LC	z jednym portem 1000Base-LX			

4.2.7. Wybór elementów aktywnych

Za wyborem routerów oraz switchów firmy CISCO przemawiają następujące cechy tych urządzeń:

- niska cena
- niezawodność
- duży wybór dostępnych interfejsów
- prosta obsługa
- różnorodność realizowanych funkcji i protokołów
- bezpieczeństwo transmitowanych danych
- wysoka jakość obsługi transmisji

Routery te i switche przeznaczone są do budowy sieci korporacyjnych niewielkich firm, do łączenia niewielkich oddziałów do sieci korporacyjnych dużych przedsiębiorstw oraz realizacji dostępu do sieci Internet.

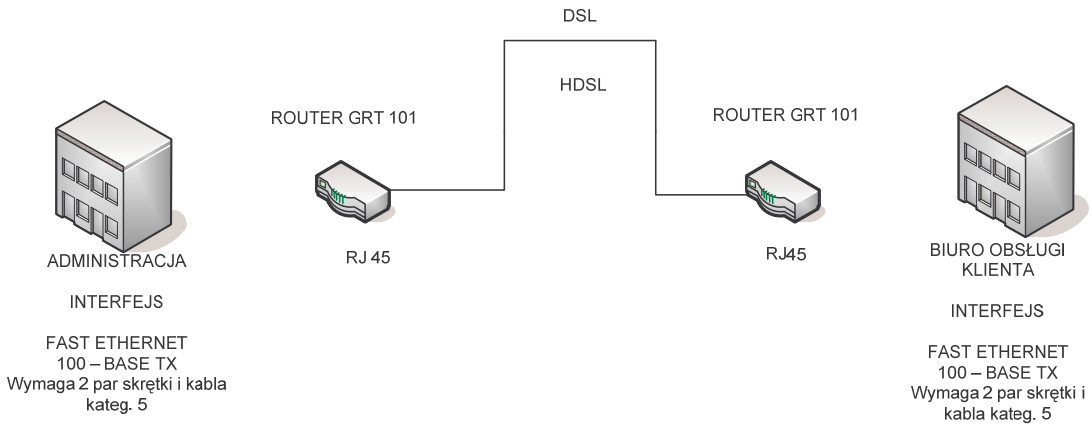
4.3. Sieć bezprzewodowa w sali konferencyjnej

4.3.1. Założenia projektowe

W głównym budynku w „Rzeszów" zakłada się stworzenie sieci bezprzewodowej w sali konferencyjnej. Sieć bezprzewodowa będzie musiała spełniać wysokie wymogi dotyczące bezpieczeństwa. Z uwagi na charakter działalności firmy, będzie posiadać wielu pracowników mobilnych, dla których będzie trzeba stworzyć VPN-y, czyli wirtualne sieci prywatne. Pracownik taki będzie miał dostęp do zasobów informatycznych firmy niezależnie od miejsca, w którym się znajduje. Połączenie takie będzie oczywiście szyfrowane.

4.4. Połączenia między lokalizacjami

4.4.1. Budowa sieci w „Boguchwała"



Rys.22. Połączenie między lokalizacjami w „Boguchwała"

Połączenie sieci pomiędzy budynkami uzyskany dzięki dzierżawie kanału analogowego od TPSA dla pasma 300-3400. Budynki położone są w odległości 4 km od siebie i brak jest widoczności optycznej.

Do połączenia tej sieci użyję Router Planet GRT 101:

PLANET G.SHDSL router GRT-101 pozwala na zwiększenie zasięgu pomiędzy sieciami Ethernet. Jest on odpowiednim rozwiązaniem dla połączenia LAN - LAN za

pomocą pojedynczej pary przewodów miedzianych AWG-26 RJ-11 (np. linia dzierżawiona), można z łatwością połączyć dwie oddalone (do 6.7 kilometra) sieci Ethernet. Maksymalna przepustowość wynosi 2,3Mbps (przy odległości 3,3km).

Dzięki zastosowaniu tego routera i dzierżawie kanału od telekomunikacji uzyskam przepustowość pomiędzy budynkami o szybkości 2 Mb/s.

4.4.2. Budowa sieci w „Rzeszów”

Rys.23. Połączenie pomiędzy lokalizacjami w „Rzeszów”

Do połączenia dwóch budynków mieszczących się w „Rzeszów” zastosowano technologie budowy sieci drogą radiową. Budynki położone są w odległości 3 km z widoczność optyczną. Do połączenia budynków zastosuję anteny:

- **Anten PARABOLA 24 dBi 5 GHz -** Model: BP-50PA-24

Rys.24. Antena PARABOLA 24 dBi 5 GHz

Parametry techniczne anteny:

Model	BP-50PA-24
Zysk energetyczny	24 dBi
Częstotliwość pracy anteny	5.15 - 5.875 GHz
Kąt promieniowania pionowo	10 stopni
Kąt promieniowania poziomo	11 stopni
Impedancja	50 Ohm
VSWR	1.5
Złącze	Wtyk typu N (męski)
Element promieniujący	zwarty stałoprądowo
Wymiary	średnica czaszy: 650 mm
Waga	2.5 kg
Polaryzacja	pionowa lub pozioma
Standard	Pełna zgodność ze standardem IEEE 802.11x
Zamocowanie	Uchwyt masztowy (cybant) na maszty od 3/4 do 7/4 cala (mocowanie pozwala na obrót o 360 stopni i korekcję azymutu).

Zastosowanie urządzenia **ACCES POINT RDAT – 81 firmy WISTRON** umożliwi budowę sieci o przepustowości **5.8 GHz.**

Obliczenie strat:

L=20log(x)+20log(f)+32,4

Gdzie: L straty w dB

x = 3 o odległość w km

f = 5,8GHz częstotliwość liczona w Mhz

L=20log(3)+20log(5800)+32,4

L=20*0,5+20*3,76+32,4

L=10+75,2+32,4

L=117,6dB

Strata na antenie przedstawionej powyżej i wynosi 117,6dB

Połączenie sieciowe uzyskam dzięki dzierżawie kanału cyfrowego z TP S.A. o przepustowości 2Mb/s

W ramach opłaty za uzyskanie abonamentu kanału cyfrowego TP S.A. zestawia, uruchamia i oddaje do użytku abonenta zamawiającego określonej, jakości kanał cyfrowy, doprowadzając go do punktów wskazanych przez abonenta.

Standardy jakościowe cyfrowych łączy dzierżawionych są zgodne z normami: PN-ETSI EN 300 247, 289, 418, 419, 288 (V1.2.1:2002U).

W przypadku usterki lub awarii, z wyjątkiem usterki lub awarii powstałej na skutek wystąpienia siły wyższej, maksymalny czas odtwarzania kanału cyfrowego klasy standardowej wynosi 24 godziny od momentu jego zgłoszenia.

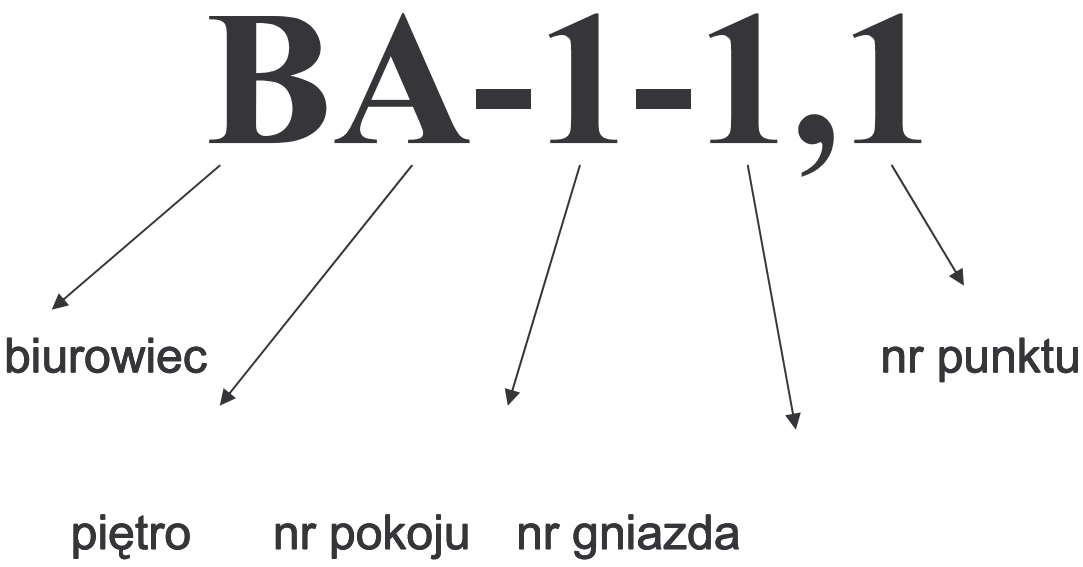
4.5. Elementy pasywne

W celu zapewnienia bezawaryjności i funkcjonalności przyszłej sieci jej budowę oparto na poniższych zasadach:

- wewnątrz budynku połączenia poziome sieci zostaną wykonane przy użyciu kabla – skrętki UTP, czteroparowej kategorii 5e. Wykorzystanie kabla kategorii 5e spowoduje, iż dane wewnątrz sieci będą mogły być przesyłane z prędkością 1000 Mbps

- kable zostaną zainstalowane w korytach w taki sposób, aby było łatwe do nich dojście w razie awarii lub przyszłej rozbudowy. Zostaną one oddalone minimum 3 mm od instalacji elektrycznych oraz od źródeł zakłóceń elektromagnetycznych
- w pomieszczeniach biurowych kable zostaną zamocowane na wysokości 1 metra od podłogi w korytkach elektroinstalatorskich PCV
- wszystkie zakończenia koryt zostaną wyposażone w zaślepki podobnie jak miejsca zgięć
- koryta zostaną przymocowane kołkami do ścian, co 0,5 metra począwszy od końca listwy
- szafa krosownica zostanie zamontowana w taki sposób, aby było do niej łatwe dojście z każdej strony jak i prosta i łatwa możliwość ściągania osłon bocznych
- kable zostaną oznaczone w czytelny sposób według schematu A–B–C–D gdzie:
    - A – piętro
    - B – pomieszczenie
    - C – nr gniazda
    - D – nr punktu
- nadmiarowe ilości kabla od strony liniowej zostaną umieszczone w prowadnicach w szafie taki sposób, aby promień ich zgięcia nie był zbyt duży (nie zaginać)
- kable wychodzące z pomieszczeń zostaną umieszczone w korytach PCV do przestrzeni między sufitowej korytarzy. Umocowane zostaną, co 1 metr do sufitu przy wykorzystaniu odpowiednich opasek

Oznaczenia gniazd sieciowych:



piętro nr pokoju nr gniazda

4.6. Kosztorys

Elementy pasywne				
L.P.	**Przedmiot zamowienia**	**ilość/j.m.**	**cena/j**	**cena zamówienia**
1	Szafa Molex MODBOX III, 19\\, 52U, 600x600	2	329,40 zł	658,80 zł
2	Szafa wisząca 12U 600x400x597	1	269,90 zł	269,90 zł
3	Panel-Patch panel 19", 2U, 48xRJ45, UTP	3	167,00 zł	501,00 zł
4	Zaciskarka RJ 45	1	208,00 zł	208,00 zł
5	Kabel UTP 4-pary Power CAT 5e PVC. 300m linka	3	475,00 zł	1 425,00 zł
6	Gniazda 2xRJ45 5 szt.	5	20,00 zł	100,00 zł
7	Kabel krosowy RJ45 2-parowy UTP linka, 2m	25	8,14 zł	203,50 zł
8	Koryto kablowe 75x75	220	8,90 zł	1 958,00 zł
9	Koryto Kablowe 50X50	15	10,90 zł	163,50 zł
10	Półka do szafy	1	90,00 zł	90,00 zł
11	UPS ACTIVE POWER 2000VA	3	994,48 zł	2 983,44 zł
		Cana końcowa		8 561,14 zł

Elementy aktywne				
L.P.	Przedmiot zamowienia	ilość/j.m.	cena/j	cena zamówienia
1	Przełącznik ProCurve Switch 5304xl-32G	4	18 363,98	73 455,92 zł
2	Router CISCO 3825	5	24 944,00	124 720,00 zł
3	Firewall PIX 525-FO-GE Bundle	2	16 164,00	32 328,00 zł
4	Firewall PIX 525-UR-GE Bundle	2	14 531,00	29 062,00 zł
5	Access Point Linksys WAP54G-EU 802.11g 54Mbps	2	295,00	590,00 zł
6	Bridge Planet GRT-101	2	154,12	308,24 zł
	Serwer Thecus N5200	4	3 458,00	13 832,00 zł
8	Serwer Netgear Readynas Duo RND2175	8	1 893,00	15 144,00 zł
9	Switch 3Com (3C16478) Baseline 2816 16x10/100/1000Mbps Rack 19' 1U	1	1 181,08	1 181,08 zł
10	Switch 3Com (3C17204) 4400 48x10/100Mbps, 2xSlot pod Moduł	3	4 094,93	12 284,79 zł
		Cena końcowa		302 906,03 zł

Elementy pasywne	**6 572,18 zł**
Elementy aktywne	**302 906,03 zł**
Cena ogółem	**309 478,21 zł**

4.7. Polityka bezpieczeństwa

1. Główny budynek w „Rzeszów" – zabezpieczenia sieci komputerowej:

Połączenie internetowe w tym budynku zapewnia provider. Łącze internetowe jest dołączone do Routera Cisco 3825. Provider dodatkowo zapewnia backupowe łącze radiowe o przepustowości 512 Kb/s wykorzystywane w razie awarii głównego łącza. Za routerem występuje Firewall sprzętowy firmy Cisco, jest to model PIX 525.

Następnie występuje strefa DMZ – strefa chroniona przez wyżej wymieniony firewall uniemożliwiający nawiązywanie połączeń do sieci wewnętrznych.

Jest to podsieć, która wydziela serwery dostępne na zewnątrz (serwer WWW, poczty, SFTP) od sieci wewnętrznej "zaufanej". W wypadku włamania na taki serwer, intruz nie będzie miał możliwości dostać się do sieci "zaufanej". DMZ działa, więc jako mała, odizolowana sieć pomiędzy siecią prywatną a Internetem. Zapora ogniowa powinna mieć tak skonstruowane reguły komunikacji, że ruch pomiędzy LAN a DMZ

posiada charakter jednostronny. Innymi słowy, połączenie powinno być dopuszczalne tylko wtedy, gdy ruch inicjujący wychodzi z sieci wewnętrznej. Całkowicie zabronione powinno być natomiast inicjowanie połączeń z serwera znajdującego się w strefie DMZ.

Działanie strefy DMZ polega na przechwytywaniu pakietów przesyłanych w sieci i analizowaniu ich zawartości pod kątem wykrywania znanych wzorców włamań. Po wykryciu niedozwolonych działań może natychmiast "zabić" połączenie, powiadomić administratora systemu poprzez E-Mail lub Pager, zarejestrować szczegóły przebiegu sesji, rekonfigurować politykę bezpieczeństwa systemu Firewall lub wykonać inne, zdefiniowane przez administratora czynności.

Konfiguracja DMZ po stronie routera polega na wpisaniu lokalnego adresu IP komputera, który ma zostać umieszczony w strefie. Należy zadbać o to, aby adres ten nie zmieniał się np. po odświeżeniu konfiguracji DHCP lub restarcie routera.

Zadania serwera WWW

- oczekuje na połączenie (zawierające żądania HTTP) na odpowiednim porcie TCP/IP i odpowiada na żądania, wysyłając do klientów strony HTML. Domyślnym portem serwera WWW jest port 80.
- Pozwala publikować informacje statyczne – informacje zawarte w plikach tekstowych w formacie HTML i graficznych w formatach GIF czy JPEG.
- Możliwość połączenia z bazami danych.
- Dynamiczna prezentacja danych.
- Wypełnianie formularzy.
- Wyszukiwanie informacji.
- Posiada pewne funkcje bezpieczeństwa:
    1. ograniczenie dostępu dla użytkowników, grup, określonych adresów IP, do określonych katalogów i plików.
    2. dostęp może być ograniczony w sposób niezauważalny dla użytkownika przez filtry lub z użyciem haseł i formularzy pozwalających dostać się do strzeżonych miejsc serwera.
    3. Do przesyłania haseł czy innych cennych danych służy bezpieczna transmisja z użyciem standardu SSL.

- Analiza działania serwera polegała na zapoznaniu się z jego logiem – plikiem znajdującym się na serwerze logującym, gdzie zapisywane są wszelkie transakcje przeprowadzane przez serwer.

Zadania serwera poczty

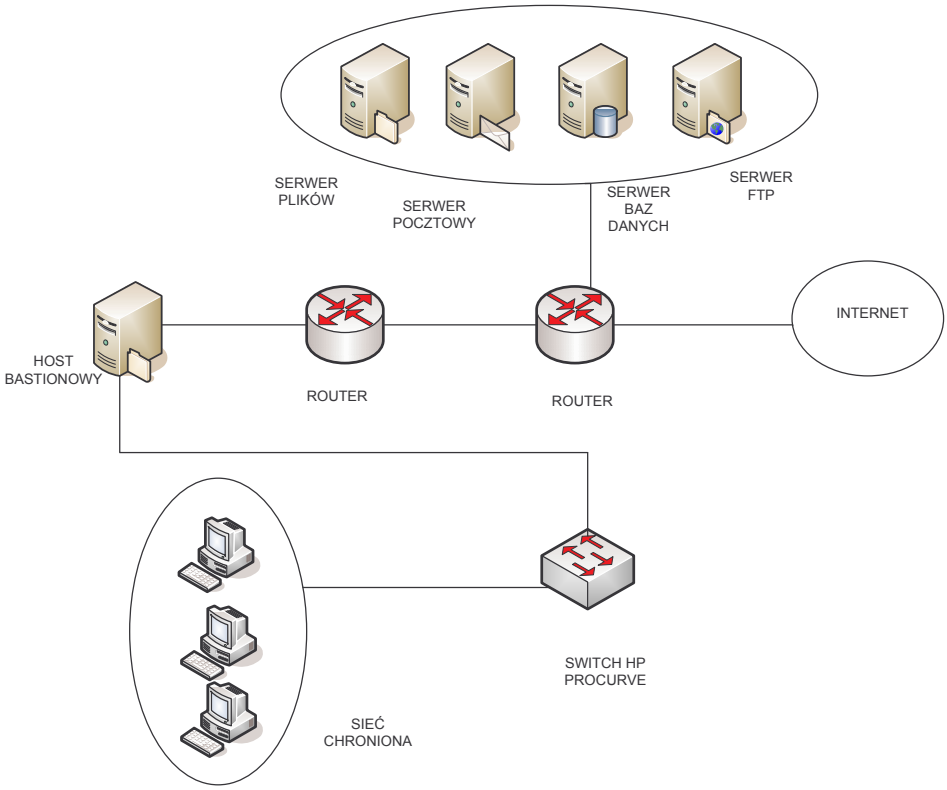
- Przechowywanie kont e-mail i zarządzanie nimi na serwerze poczty używając usługi POP3.
- Zezwolenie użytkownikom na dostęp do serwera poczty, aby mogli pobierać wiadomości e-mail z komputera lokalnego przy użyciu klienta poczty e-mail, który obsługuje protokół POP3, na przykład programu Microsoft Outlook.
- Sprawdzanie poprawności załączników.
- Szyfrowanie wiadomości.
- Zarządzanie poczta przychodzącą jak i wychodzącą.
- Ochrona przed spamami (wykrywanie ich na podstawie nagłówków wiadomości, blokowanie ich).
- Ochrona przed wirusami, robakami, koniami trojańskimi.
- Uwierzytelnianie kont.

Zadania serwera plików (SFTP)

- udostępnia zasoby dyskowe, dostęp do plików;
- służy do szyfrowanego przesyłania plików pomiędzy komputerami w sieci;
- stanowiąc centralny punkt sieci daję możliwość dostępu wielu użytkownikom do konkretnego pliku bez potrzeby rozsyłania go między komputerami;
- wprowadzona usługa indeksowania daje szybki dostęp do wyszukiwanych plików, jednakże może spowolnić sam serwer. Włączenie jej ma tylko sens wtedy gdy użytkownicy często korzystają z opcji wyszukiwania;
- posiada możliwość ograniczania miejsca na udostępnionym dysku poszczególnym użytkownikom lub grupom użytkowników;
- zaimplementowany proces uwierzytelniania poszczególnych użytkowników;

Poza strefą DMZ zastosowano kolejny host bastionowy będący dodatkowym zabezpieczeniem. Zapewnia on dostęp do serwerów usługowych jak również do

komputerów pracujących w sieci. Każdy system zewnętrzny próbujący uzyskać dostęp do wewnętrznych systemów lub usług musi się połączyć z tym hostem. Musi on być szczególnie dobrze zabezpieczony. Dzięki filtrowaniu pakietów host bastionowy może nawiązywać ze światem zewnętrznym dozwolone połączenia.



Rys.25. Strefa DMZ

Host ten będzie zabezpieczony przez firewall sprzętowy firmy Symantec – SGS-5400 pokazany na rysunku poniżej, który pozwala zachować lepsza ochronę przed zagrożeniami.

Do głównego switcha ProCurve 5300XL podłączone są dwa serwery: lokalny serwer plików, który ma za zadanie przechowywać i udostępniać pliki użytkownikom w sieci oraz serwer baz danych.

Zadania serwera baz danych:

- Możliwość dodawania nowych, modyfikacji i usuwania już stworzonych baz danych.
- Indywidualne ustanawianie praw dostępu dla poszczególnych użytkowników.
- Wykorzystywanie utworzonych baz danych w sieci Internet.
- Środki zapewniające spójność i bezpieczeństwo danych.

- Sprawny dostęp do danych (zwykle poprzez język zapytań, np. SQL).
- Środki programistyczne służące do aktualizacji lub przetwarzania danych (API dla popularnych języków programowania).
- Jednoczesny dostęp do danych dla wielu użytkowników (z reguły realizowany poprzez transakcje).
- Środki pozwalające na regulację dostępu do danych (autoryzację).
- Środki pozwalające na odtworzenie zawartości bazy danych po awarii.
- Zarządzanie katalogami, schematami i innymi metodami.
- Sprawuje kontrolę nad danymi.
- Udostępnia je innym programom.
- Optymalizacja zajętość pamięci oraz czasy dostępu (np. indeksy).
- Praca lub współdziałanie w środowiskach rozproszonych.
- Pakiety statyczne, pakiety dla przeprowadzania analiz (eksploracji danych).

Komputerach w sieci lokalnej zostaną zabezpieczone programem antywirusowy firmy Symantec - Norton AntiVirus 2008 w którym jest wbudowany firewall programowy, który umożliwia:

- aktualizację bazy wirusów;
- automatyczne usuwanie i wykrywanie szkodliwego oprogramowania;
- wyłapywanie podczas przeglądania stron WWW oprogramowania typu spyware i adware;
- skanowanie poczty pod względem spamu i niebezpiecznych załączników;

W budynku tym znajduje się sala konferencyjna, w której Internet będzie udostępniany droga radiową. Szyfrowanie danych pomiędzy punktami dostępowymi (zewnętrznymi) będzie odbywało się przy użyciu protokołu WPA (klucz 256-bitowy lub 128-bitowy (zależne od urządzenia), ponieważ AP są podłączone do szkieletu sieci, więc teoretycznie można się dostać do każdego komputera w firmie. Szyfrowanie danych pomiędzy laptopem a punktem dostępowym (wewnątrz budynków) odbywa się również z wykorzystaniem protokołu WPA, z kluczem 256-bitowym (lub 128 – 13 bitowym) automatycznie generowanym na podstawie podanego hasła. Ponieważ osoba znajdująca się w nie dalekiej odległości od budynku, może uzyskać dostęp do „tajnych” danych firmy.

Protokół WPA posiada mechanizm RADIUS, który wymusza uwierzytelniania nie tylko użytkowników, ale również punktów dostępowych. W ten sposób będziemy mieli pewność, że zalogowaliśmy się do właściwej sieci. Zdarzają się, bowiem przypadki podstawienia fałszywych sieci w celu wydobycia ważnych danych z komputera użytkownika.

W celu zaimplementowania tego mechanizmu, potrzebne będzie uruchomienie na serwerze usługi (oprogramowania), która stanowić będzie centralny punkt zarządzania wszystkimi hasłami i zasobami sieci.

Pomimo, że im dłuższy klucz szyfrujący (64/128/256 bit), tym transfer jest mniejszy, zastosujemy najbezpieczniejsze rozwiązanie - klucz 256-bitowy.

Zasięg sieci zostanie ograniczony do niezbędnego minimum, tak, aby sygnał radiowy nie wychodził poza budynek. Włączone zostanie również filtrowanie adresów MAC kart sieciowych, dzięki któremu ograniczymy dostęp do sieci (danych) tylko dla wybranych urządzeń (karty PCMCIA w laptopach).

Wyłączona zostanie również funkcja rozgłaszania SSID (ang. *Service Set Identifier*), dzięki której potencjalny intruz nie będzie widział nazwy naszej sieci.

2. Drugi budynek w „Rzeszów" (magazyn) – zabezpieczenia sieci komputerowej:

Magazyn w „Rzeszów" jest połączony poprzez switch główny ProCurve 5300XL znajdujący się w MDF-ie budynek główny (dyrekcja). Połączenie odbywa się poprzez sieć radiową zabezpieczoną jak w budynku Dyrekcji w „Rzeszów". Połączenie będzie odbywać się poprzez VPN (Virtual Private Network - wirtualną sieć prywatną) którą zapewnia zastosowanie firewalla PIX 525 posiadającego wbudowaną obsługę VPN. W celu zwiększenia wydajności sieci poprzez VPN firewall ten dodatkowo jest wyposażony w PIX 66-MHz DES/3DES/AES VPN Accelerator Card+ (VAC+) , kartę akceleracji szyfrowania.

Po obu stronach sieci znajdują się urządzenia Access Point. Access Point znajdujący się w magazynie jest bezpośrednio połączony ze switchem ProCurve Switch 5304xl z obsługą 16 portów 100 Mb/s do którego są wpięci wszyscy użytkownicy z tego budynku podzieleni na dwie grupy VLAN. Ich komputery są zabezpieczone programem antywirusowym firmy Symantec – Norton AntiVirus 2008 z wbudowanym firewallem. Switch ProCurve 5304xl połączony jest także z serwerem plików.

3. Budynek administracji w „Boguchwała”:

Do budynku Administracji poprowadzone jest łącze dzierżawione z głównego budynku w „Rzeszów” (dyrekcja). Łącze to jest bezpośrednio wpięte do routera w „Boguchwała”. Do tego samego urządzenia jest doprowadzone łącze internetowe o przepustowości 512 Kb/s. Jest ono dostarczone przez providera z „Boguchwała” – TP S.A. Zapewni to pracę oddziału w „Boguchwała” w razie wystąpienia awaria łącza głównego. Następnie znajduje się firewall PIX 525 firmy Cisco, który ma za zadanie filtrować pewne usługi a za nim switch ProCurve Switch 5304xl-32G do którego są przyłączone: serwer plików, pracownicy podzieleni na 3 grupy VLAN oraz strefa DMZ z hostem bastionowym i serwerem WWW. Serwery usługowe (serwer SFTP, pocztowy oraz baz danych) podłączone do routera zawierają kopie danych znajdujących się na serwerach głównych pracujących w „Rzeszów”. Pomiędzy serwerami w budynku dyrekcji w „Rzeszów” a tymi znajdującymi się w „Boguchwała” będzie przeprowadzana synchronizacja danych. Pozwoli to w razie awarii łącza korzystać z danych umieszczonych na lokalnych serwerach w „Boguchwała”. W przypadku odzyskania łączności dane będą automatycznie aktualizowane i synchronizowane.

Zadania serwerów będą takie same jak w przypadku serwerów w „Rzeszów”.

Podobnie z zabezpieczeniem komputerów w sieci lokalnej oraz bezpieczeństwem sieci bezprzewodowej.

4. Budynek Biura Obsługi Klienta w „Boguchwała”:

Za switchem ProCurve Switch 5304xl-32G umiejscowiono firewall PIX 525, który zapewnia wysokie bezpieczeństwo i niezawodność. Przy przepustowości 370 Mb/s jest on w stanie obsłużyć ponad 280 000 jednoczesnych połączeń. Pix 525 ma za zadanie jedynie usprawnić działanie sieci i filtrować pewne usługi. Chodzi przede wszystkim o:

- Zarządzanie ruchem w sieci - blokowanie niepożądanego ruchu. Ruch sieciowy z określonych adresów lub podsieci może być całkowicie blokowany lub przepuszczany bądź przekierowywany na inne adresy lub podsieci.
- Śledzi ruch przechodzący przez firewall - sniffer.

- Zapewnia ochronę poczty SMTP przed wirusami, nieprawidłowymi załącznikami oraz filtruje wiadomości w celu wykrycia SPAM-ów.
- Filtruje dostęp do stron internetowych indywidualnie dla poszczególnych użytkowników bądź ich grup.
- Pozwala na określenie odmowy dostępu do stron zawierających określone przez nas treści.
- Blokuje nieprawidłowe skrypty JavaScript, VBScript i ActveX oraz pliki cookies.
- Kontroluje ruchu wychodzący i przychodzący oraz blokuje lub przepuszcza połączenia w zależności od ustawionych reguł.
- Zapewnia ochronę przed atakami typu:

- DoS (denial of Service), której celem jest unieruchomienie wybranej usługi sieciowej.
- Ping of Heath - przesłanie pakietu przekraczającego maksymalna dozwolona długość.
- SYN Flood - "zalanie " komputera setkami żądań nawiązania połączenia.
- IP spoofing - przesyłanie pakietów ze sfałszowanym adresem nadawcy.

W przypadku ataku jego źródło jest automatycznie blokowane przez firewall a informacja o wykrytym zagrożeniu jest zapisywana do dziennika zdarzeń.

- identyfikuje i usuwa wirusy z sesji WWW, FTP, poczty.
- Wszystkie alerty są logowane do pliku, który podajemy w jego konfiguracji - dzienniku zdarzeń.

Na I piętrze, jak i na parterze jest zastosowany Switch HP ProCurve 5304xl. Switche te różnią się między sobą tylko ilością portów i modułem. Do jednego (parter) przyłączeni zostali pracownicy podzieleni na dwie grupy VLAN oraz serwer plików. Do drugiego (I piętro) natomiast dwie grupy VLAN. Komputery użytkowników są zabezpieczone programem antywirusowym firmy Symantec – Norton AntiVirus 2008.

5. Polityka bezpieczeństwa dla pracownika firmy oraz określenie zasad bezpiecznego logowania i używania haseł przez użytkownika:

1. Logowanie się użytkownika do systemu – użytkownik loguje się do systemu po uprzednim podaniu swojego loginu. Login będzie tworzony dla każdego

użytkownika z osobna na podstawie imienia i nazwiska, czyli przykładowo login może składać się z połączenia pierwszych liter imienia i nazwiska.

2. W sieci powinny być wydzielone grupy robocze w postaci wirtualnych sieci lokalnych (VLAN). Stwarza to możliwość istnienia w obrębie jednej sieci wielu niezależnych podsieci, które mogą komunikować się między sobą. Jest to możliwe dzięki przełącznikom, które umożliwiają utworzenie VLANów. Konfiguracja taka pozwala zwiększyć bezpieczeństwo w sieci, gdyż dane znajdujące się w każdej z wydzielonych podsieci są niedostępne (i niewidoczne) dla nieuprawnionych osób.

3. Polityka bezpieczeństwa dla pracowników firmy:

a) Użytkownik ma prawo otrzymać dostęp do wszystkich zasobów informatycznych, które są niezbędne do wykonywania obowiązków wynikających z zajmowanego stanowiska. O szczegółowym zakresie uprawnień użytkownika decyduje jego przełożony.

b) Użytkownik ma prawo zgłaszać wszelkie zauważone nieprawidłowości w pracy systemów informatycznych w następującej kolejności: do bezpośredniego przełożonego, do administratora systemu informatycznego.

c) Użytkownik ma prawo odmówić wykonania działań czy czynności w systemach informatycznych, jeśli stwierdzi, że działania te mogą doprowadzić do naruszenia bezpieczeństwa systemu informatycznego, a w szczególności do: utraty danych, ujawnienia informacji osobom do tego nieupoważnionym, naruszenia polityki bezpieczeństwa.

d) Użytkownik powinien odbierać dokumenty natychmiast po wykonaniu przez urządzenie typu drukarka sieciowa i kserokopiarka (bardzo często umieszczone na korytarzu) zleconego zadania. Nie powinny pozostawać dostępne ani dla obcych osób ani dla użytkowników nieposiadających stosownych uprawnień.

e) Użytkownik ma prawo do konfigurowania swojego informatycznego środowiska pracy w takim zakresie, na jaki pozwalają na to jego uprawnienia do tego środowiska i niewykraczającym poza przyjęte standardy.

f) Użytkownik ponosi odpowiedzialność za wszystkie skutki swoich działań w systemach informatycznych, w zakresie takim, jakie wynikają z normalnej pracy tych systemów.

g) Użytkownik powinien zdezaktualizowane dokumenty niszczyć za pomocą urządzeń typu niszczarka.

h) Użytkownik ma obowiązek pracować w systemach informatycznych wyłącznie na swoim koncie udostępnionym przez administratora. Wszelkie odstępstwa od tej zasady wymagają zgody dyrektora i administratora, jednoznacznie potwierdzonych i mogą mieć jedynie czasowy charakter.

i) Użytkownik ma obowiązek zgłaszać wszelkie zauważone nieprawidłowości w pracy systemów informatycznych, ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji polegających na niebezpieczeństwie utraty danych lub ujawnienia ich osobom nieupoważnionym. Zgłoszenia należy kierować w kolejności do: bezpośredniego przełożonego, administratora.

j) W szczególności zabronione jest:
   - udostępnianie swojego konta innym użytkownikom,
   - praca na innych kontach jak swoje, udostępnione przez administratora,
   - podszywanie się pod innych użytkowników w dowolny sposób,
   - ujawnianie swoich haseł do systemów informatycznych komukolwiek,
   - zapisywanie hasła i przechowywanie go w sposób mogący prowadzić do jego ujawnienia, udostępnianie innym jakichkolwiek informacji, które mogą doprowadzić do ujawnienia hasła,
   - próby łamania haseł przy użyciu dowolnych metod,
   - próby stosowania dowolnych metod w celu zdobycia dostępu do zasobów, do których nie zostały użytkownikowi nadane prawa przez administratora,
   - podejmowanie próby zmian w konfiguracjach użytkowanych zasobów informacyjnych, poza tymi, które wynikają z obowiązków użytkownika wobec danego zasobu informacyjnego oraz konfiguracji pulpitu użytkowanej przez siebie stacji roboczej,
   - instalowanie i próby uruchamiania jakiegokolwiek oprogramowania na zasobach informacyjnych (m.in. stacje robocze, serwery), niebędącym standardowym oprogramowaniem, chyba, że odbywa się to za zgodą właściciela zasobu i pod kontrolą Administratora systemu informatycznego, w skład, którego wchodzi w/w zasób,
   - kopiowanie i uruchamianie programów z sieci Internet,

- pozostawianie, w czasie przerw w pracy, niezabezpieczonej stacji roboczej i umożliwianie osobom nieupoważnionym dostępu do niej,
- wykorzystywanie udostępnionych zasobów, w tym sprzętu komputerowego, do prac niezwiązanych z obowiązkami użytkownika, jako pracownika,
- udostępnianie użytkowanych zasobów informacyjnych komukolwiek poza osobami upoważnionymi do tych zasobów. Za osoby upoważnione należy uważać te, które posiadają uprawnienia do w/w zasobów nadane przez administratora. Zakaz ten dotyczy wszelkiej formy udostępniania w tym wydruków komputerowych. Zakaz powyższy nie odnosi się do przypadku, gdy na udostępnienie użytkownik uzyskał jednoznaczna zgodę właściciela zasobu,
- tworzenie kopii zasobów informacyjnych (plików, katalogów itp.) i umieszczanie ich w innych miejscach jak do tego przeznaczone, a w szczególności na dyskach stacji roboczych (komputerów biurkowych),
- przechowywanie na dyskach stacji roboczych oraz udostępnionych dyskach serwerów plików niezwiązanych bezpośrednio z wykonywanymi obowiązkami, a w szczególności; plików dźwiękowych, zawierających obrazy, filmy, treści niezgodne z obowiązującym prawem,
- przechowywanie i uruchamianie gier komputerowych,
- kopiowanie danych i informacji oznaczonych, jako poufne i tajne na dyskietki i inne przenośne nośniki danych. Kopiowanie takie może być dozwolone po uzyskaniu zgody właściciela danych, dyrektora zarządzającego lub administratora,
- wykonywania zbędnej ilości wydruków oraz przechowywanie ich w sposób narażający na dostęp osób nieposiadających uprawnień do zasobów będących źródłem tych wydruków,
- nieuprawniona zmiana oznaczenia klasyfikacji stopnia poufności do zasobów informacyjnych,
- używanie programów szyfrujących bez zgody dyrektora zarządzającego,
- udostępnianie zasobów katalogowych innym użytkownikom, uprawniony do tej czynności jest wyłącznie administrator.

4. Hasła:
    - Cechy haseł – hasła muszą składać się z przynajmniej 7 znaków. Będą kombinacją wielkich i małych liter, muszą zawierać w sobie przynajmniej jedną liczbę i znak interpunkcyjny lub znak sterujący, czyli spację. Ale z drugiej strony musza być tak skonstruowane, żeby dały się łatwo wpisać w sposób uniemożliwiający ich podejrzenie przez ramię i były dość łatwe do zapamiętania bez konieczności ich zapisywania. Mogą być połączeniem wyrazów z liczbami i innymi znakami, np. roBot2_MY. Zmiana hasła będzie wymagana raz na 2 tygodnie.
    - Funkcjonowanie haseł i obowiązki użytkownika związane z hasłami administrator jest jedyną osobą, która będzie miała dostęp, wgląd do wszystkich haseł. Każdy użytkownik (pracownik) będzie posiadał swój własny login i hasło. Użytkownicy są zobowiązani do utrzymania swoich haseł w tajemnicy przed innymi użytkownikami. Nie wolno używać tego samego hasła do różnych programów, różnych celów. Zabrania się również przyklejania kartek z hasłem ma monitorach, pod klawiaturami, ani w żadnym innym miejscu w pobliżu komputera, na którym będzie używane to hasło. Nie wolno podawać swojego hasła innym osobom, ani nie wysyłać go pocztą elektroniczną, a jeśli zachodzi przymus przekazania swojego hasła osobie zaufanej – należy uczynić to w sposób niepozwalający na jego podsłuchanie przez osoby trzecie.
    - Komputery winny być zabezpieczone przed nieautoryzowanym ich uruchomieniem i wglądem do nich niepowołanych osób hasłem na BIOS (przy czym BIOS nie może być zabezpieczony uniwersalnym hasłem producenta), hasłem na system operacyjny (Windows), . hasłem na ważne dokumenty.
    - Hasła do urządzeń sieciowych muszą być pod szczególna ochrona i jedynie do wglądu administratora sieci komputerowej.
5. Tworzenie i przechowywanie wydruków i kopii bezpieczeństwa
    - Do obowiązków administratora będzie należało raz na 3 tygodnie tworzenie kopii zapasowych bezpieczeństwa systemu oraz raz na 3 dni kopii zapasowych wszystkich dokumentów, logów systemowych i innych plików mających jakąkolwiek wartość dla firmy. Kopie

awaryjne systemu będą tworzone raz na tydzień. Jeśli jest to możliwe, przed utworzeniem kopii pliki będą kompresowane.

- Kopie zapasowe będą przechowywane na dyskach komputerów, które będą znajdowały się w monitorowanym pomieszczeniu o szczególnych zabezpieczeniach, do którego będą miały dostęp tylko osoby upoważnione. Po zapełnieniu się jakiegoś z dysków, będzie dopinany nowy dysk, a stary odłączany i przechowywany w szafie pancernej do 6 miesięcy.
- Jakiekolwiek wydruki będą również przechowywane w monitorowanym pomieszczeniu z kontrolowanym wejściem, do którego będą miały dostęp tylko osoby upoważnione.
- Aby dodatkowo zabezpieczyć ważne dane, należy ustawić ich szyfrowanie za pomocą EFS (Encrypted File System). Pliki zaszyfrowane będą odszyfrowywane, gdy uprawniony użytkownik dokonuje ich odczytu i szyfrowane ponownie, gdy zostają zapisywane. Nie wymaga to działań ze strony użytkownika.
- Ochrona dokumentów - kopie bezpieczeństwa - nośniki zewnętrzne:

A) Bezpieczeństwo tworzonych przez siebie dokumentów spoczywa na samym użytkowniku. Odstępem od tej reguły stanowią użytkownicy systemów sieciowych, w których to za bezpieczeństwo dokumentów odpowiada administrator sieci;

B) Kopie bezpieczeństwa należy dokonywa przy użyciu legalnego oprogramowania na nośnikach zewnętrznych typu płyty CD, streamery, dyski zewnętrzne;

C) Wszyscy użytkownicy SA zobowiązanie do robienia kopi zapasowych własnych dokumentów w celu ochrony ich przed awaria sprzętowa lub systemowa;

D) Należy w jednoznaczny i ustalony sposób podpisywać nośniki kopi zapasowych, winna być to data kopi oraz zawartość;

E) Użytkownik sam winien decydować o częstotliwości wykonywania kopi zapasowych własnych dokumentów. Częstotliwość ta winna być uzależniona od ilości tworzonych dokumentów ich priorytetu, ale nie powinna być mniejsza niż raz w tygodniu.

F) Użytkownik winien posiadać umiejętności pozwalające na odzyskanie plików z kopi zapasowych;

6. Ochrona dokumentów przed zawirusowaniem:

a) Przez cały czas pracy komputera winien być włączony program antywirusowy, którego powinien być tak skonfigurowany, aby skanował każdy nowy plik

7. Tworzenie dokumentów elektronicznych:

a) Tworzenie dokumentów elektronicznych winno odbyć się tylko na legalnym, licencjonowanym oprogramowaniu.

- Licencje te będą posiadali pracownicy firmy oraz będą niezbędne do okazania upoważnionym do tego kontrolerom zewnętrznym sprawdzającym legalność używania danego programu

5. Wnioski końcowe

Podczas tworzenia projektu natrafiano na kilka problemów, które udało się rozwiązać. Chyba największym problemem był dobór urządzeń. Mam tutaj na myśli nie tylko cenę, ale i parametry. W chwili obecnej na rynku jest kilku wiodących producentów urządzeń sieciowych. Prześcigają się oni w swoich ofertach, jednakże oferują urządzenia o podobnych możliwościach, jednakże za różną cenę.

Obecnie stosowane sieci lokalne (LAN) oraz sieci intranetowe są potężnym narzędziem, aczkolwiek łatwym w użyciu dla użytkownika końcowego. Taka sieć zawiera jednak wiele skomplikowanych technologii, które muszą ze sobą współpracować. Projekt sieci powinien być tak zaprojektowany, aby spełniał oczekiwania wszystkich odbiorców. Budowanie sieci jest wybieraniem odpowiednich komponentów oraz łączenia ich razem.

5.1. Streszczenie

Niniejsza praca w całości została poświęcona zagadnieniom sieci LAN i projektowi takiej sieci. W części teoretycznej pracy podjęto próbę przybliżenia urządzeń wykorzystywanych do budowy sieci LAN i możliwych do zastosowania topologii. W dalszej części pracy przedstawiono media transmisyjne, rodzaje kabli oraz normy które winny one spełniać. Ostatnia część pracy, praktyczna poświęcona jest projektowi sieci LAN dla średniej wielkości firmy.

W projekcie zaproponowano konkretne rozwiązanie poparte odpowiednimi schematami i adresowaniem. Infrastruktura sieciowa została tak zaprojektowana aby jej rozbudowa lub w przyszłości wdrożenie chociażby usługi VOIP nie powodowało problemów. W projekcie przybliżono wykorzystane urządzenia aktywne i pasywne, dokonano odpowiednich obliczeń i przetestowano sieć. Zaproponowano także konkretne rozwiązania podnoszące bezpieczeństwo działania oraz użytkowania sieci.

W ostatnim podrozdziale podjęto próbę stworzenia polityki bezpieczeństwa dla pracowników firmy, jak i administratorów. Zaproponowano konkretne rozwiązania w celu doboru odpowiednich haseł, użytkowania sieci, przechowywania dokumentów, postępowania w razi awarii sieci.

Słowa kluczowe: sieć LAN, adresowanie, topologie sieciowe, polityka bezpieczeństwa, media transmisyjne, elementy aktywne, elementy pasywne, VLAN, okablowanie pionowe i poziome

Summary

The following thesis was dedicated to certain issues of Lan web as well as a project of the web. In the theoretical part, there was made an attempt to pesent some essential devices used to construct the web. In the following part of the thesis there were presented some transmissing media, different kinds of cable as well as certain norms which should by archived. The last part, practical part was dedicated to a project of the Lan web for an average size business. Moreover, in the project there were suggested concrete solution confirmed by appropriate schemes and addressing.

Web infrastucture was projected in the way that, in the future, its development or an implementation of Voip services should not cause any problems. Additionally, in the project, there was presented certain use of active and passive devices, as well as appropriate calculation. Moreover, the web was tested. Also, there were suggested some concrete solutions which increase security of working and using the web. In the last subchapter, there was an attempt made towards creating a kind of politics security for both employess and administrators. Furthermore, there suggested concrete solution in the field of a selection of appropriate passwords, using the web, saving data and certain action actions in case of a failure.

Key words: Lan web, adressing, web topologies, security politics, transmissing media, active elements, passive elements, vertical and horizontal wiring up

Spis ilustracji

Bibliografia

[1]. M. Świętalski, „Po prostu sieci," Helion, Gliwice 2004

[2]. J. F. Kurose, K. W. Ross, „Sieci komputerowe O ogółu do szczegółu z Internetem w tle", Helion, Gliwice 2006.

[3]. K. Krysiak, „Sieci komputerowe. Kompedium", Helion, Gliwice 2005.

[4]. J. Habraken, „ABC sieci komputerowych", Helion, Gliwice 2002.

[5]. Tomasz Rak „Tworzenie sieci komputerowej. Ćwiczenia praktyczne", Helion 2006

[6]. Scott Mueller, Terry W. Ogletree, "Rozbudowa i naprawa sieci. Kompendium", Helion 2004

[7]. Rob Scrimger, Paul LaSalle, Clay Leitzke, Mridula Parihar, Meeta Gupta, Tłumaczenie: Adam Jarczyk, „TCP/IP. Biblia", Helion 2002;

[8]. Wykład E. Walkowiak WWW.sieci.wshe.lodz.pl

[9]. http://www.cors.gov.pl/lan.html

[10]. http://www.ingenium.net.pl/index.php?option=com_content&task=view&id=41&Itemid=75

[11]. http://free.polbox.pl/c/cyfraa/okablowanie.htm

[12]. http://www.informawpigulce.ovh.org/sieciprzewody.php

[13]. K. Krysiak, „Sieci komputerowe. Kompedium", Helion, Gliwice 2005.

[14]. Sue Plumley, "Sieci komputerowe w domu i w biurze. Biblia", Helion 2001

[15]. Derflem Frank, Freed Les, *Okablowanie sieciowe w praktyce,* Helion 2000

[16]. http://erobnet.republika.pl/html/topologie_fizyczne.htm

[17]. http://studianet.pl/sieci/pliki/topologie_wan.htm

Karol Kubicki

Wydział Informatyki, Zarządzania i Transportu

Kierunek Informatyka

OŚWIADCZENIE

Świadomy/-a odpowiedzialności oświadczam, że przedkładana praca dyplomowa licencjacka/inżynierska/magisterska, przygotowana w ramach studiów odbywanych w WSHE w Łodzi, o tytule: **Projekt sieci dla średniej wielkości firmy** została napisana przeze mnie samodzielnie, w ramach toku studiów w WSHE. Jednocześnie oświadczam, że ww. praca nie narusza praw autorskich w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz. 83, z późn. zm.) oraz dóbr osobistych chronionych przepisami obowiązującego prawa. Ww. praca dyplomowa nie zawiera danych i informacji, które uzyskałem/-am w sposób niedozwolony.

Niniejsza praca dyplomowa nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadawaniem dyplomów wyższej uczelni lub tytułów zawodowych.

Oświadczam, iż przysługują mi wszelkie i nieograniczone czasowo i terytorialnie prawa autorskie do ww. pracy dyplomowej.

Zezwalam WSHE w Łodzi na nieodpłatne i bezterminowe korzystanie z przedmiotowej pracy dyplomowej na następujących polach eksploatacji:

a) utrwalenie (sporządzenie egzemplarza, który mógłby służyć publikacji utworu),
b) digitalizacja,
c) wygłoszenie,
d) zwielokrotnienie poprzez druk, nagranie na płycie kompaktowej, dyskietce,
e) wprowadzenie do pamięci komputera,
f) sporządzenie wydruku komputerowego,
g) wprowadzenie do obrotu,
h) wypożyczenie lub udostępnienie zwielokrotnionych egzemplarzy,
i) wprowadzanie w całości lub w części do sieci komputerowej Internet w sposób umożliwiający transmisję odbiorczą przez zainteresowanego użytkownika,
j) publikację i rozpowszechnianie w całości lub w części, w sieci Internet, łącznie z utrwalaniem materiałów w pamięci RAM.
k) utrwalenie technikami poligraficznymi, informatycznymi, fotograficznymi, cyfrowymi,
l) zwielokrotnienie technikami poligraficznymi, informatycznymi, fotograficznymi, cyfrowymi niezależnie od ilości egzemplarzy,
m) wykorzystanie w utworach audiowizualnych, multimedialnych,
n) rozpowszechnienie w ten sposób aby pojedyncze osoby miały dostęp do utworu w wybranym przez siebie miejscu i czasie,

o) rozpowszechnienie w programach telewizyjnych i utworach audiowizualnych nadawanych za pomocą wizji przewodowej i bezprzewodowej przez stacje naziemne oraz za pośrednictwem satelity, wyświetlanych w kinie, publiczne odtwarzanych,
p) rozpowszechnianie w programach telewizyjnych i utworach audiowizualnych nadawanych w sposób równoczesny i integralny z inną organizacją telewizyjną,
q) najem lub dzierżawa,
r) wydanie w wydawnictwach książkowych i innych wydawnictwach drukowanych (np. albumy, katalogi, leksykony, kalendarze), wydawnictwach multimedialnych, samodzielnie lub w wydaniach z utworami innych podmiotów,
s) rozpowszechnianie w całości lub w częściach w celu promocji i reklamy, w szczególności w formie plakatów, folderów reklamowych, niezależnie od ich rodzaju formatu, ogłoszeń, reklam w tym reklam audiowizualnych, audialnych, multimedialnych.

WSHE w Łodzi będzie uprawniona do udzielania licencji osobom trzecim na korzystanie z praw do pracy dyplomowej w zakresie wyżej wymienionych pól eksploatacji.

Oświadczam, że nie będzie przysługiwało mi żadne wynagrodzenie za korzystanie przez WSHE w Łodzi z pracy dyplomowej na którymkolwiek z wyżej wymienionych pół eksploatacji.

Łódź, 31.01.2009r. .....

podpis studenta