

Technologie sieciowe 2 - projekt

Autor:

Tymon Tobolski (181037)

Jacek Wieczorek (181043)

Prowadzący:

Dr inż. Marcin Markowski

Wydział Elektroniki

III rok

Śr 13.15 - 15.00

4 stycznia 2012

Spis treści

1	Wstęp	3
2	Inwentaryzacja sprzętu i infrastruktury dostępnej w przedsiębiorstwie	3
2.1	Budynki	3
2.1.1	Budynek 1	3
2.1.2	Budynek 2	4
2.2	Wypożyczenie	12
3	Analiza potrzeb użytkownika	13
3.1	Główne wymagania jakie stawiane są wobec tworzonej sieci . .	13
3.2	Bezpieczeństwo sieci	13
3.3	Tele i wideokonferencje	14
3.4	Sieć bezprzewodowa	14
3.5	Program antywirusowy	14
3.6	VLAN	14
3.7	VPN	15
3.8	Jakość usług sieciowych	15
3.9	Minimalna wymagana przepustowość	15
3.10	Okablowanie	16
4	Założenia projektowe	17
5	Projekt sieci	19
5.1	Projekt logiczny sieci	19
5.2	Konfiguracja adresacji <i>IP</i>	23
5.3	Projekt fizyczny	24
5.3.1	Projekt okablowania	24
5.3.2	Umieszczenie urządzeń w szafach	32
5.3.3	Tabela połączeń	34
5.4	Połączenie pionowe	42
5.5	Podłączenie do internetu	43
5.6	Bezpieczeństwo	43
5.7	Kosztorys	44
5.8	Koszt okablowania, szaf, etc...	45
5.9	Koszt urządzeń	46
5.10	Całkowity koszt	46

6	Karty katalogowe	47
6.1	Przełącznik warstwy 3	47
6.2	Przełącznik warstwy 2	48
6.3	Router	49
6.4	Access Point	50
6.5	Firewall	51
6.6	Serwer	52

1 Wstęp

Celem przedsięwzięcia jest stworzenie projektu sieci komputerowej dla firmy informatycznej świadczącej usługi programistyczne. Firma mieści się w dwóch budynkach zlokalizowanych niedaleko siebie, oddalonych o ok. 50m. Głównym celem firmy jest tworzenie aplikacji internetowych, a także oprogramowania na urządzenia przenośne.

Firma zatrudnia ok. 180 pracowników podzielonych na 6 zespołów zajmujących po jednym piętrze budynku. Jedna kondygnacja przeznaczona jest na serwerownię, pomieszczenia administracyjne oraz biura członków zarządu. Na każdym piętrze znajduje się sala konferencyjna.

Ze względów bezpieczeństwa dostęp do niektórych zasobów sieci jest dostępny tylko dla wybranych grup użytkowników.

Projektowana sieć musi cechować się jakością, niezawodnością oraz skalowalnością w przypadku potrzeby zwiększenia ilości pracowników w firmie. Ważnym czynnikiem jest również estetyczna jakość wykonania instalacji.

2 Inwentaryzacja sprzętu i infrastruktury dostępnej w przedsiębiorstwie

2.1 Budynki

Firma ma swoją siedzibę w dwóch budynkach oddalonych od siebie o około 50m. Pierwsza z budowli składa się z czterech pieter, natomiast druga z trzech. Pięć kondygnacji jest zaadaptowanych jako pomieszczenia dla programistów. Dwie kondygnacje przeznaczone są na serwerownię, pomieszczenia administracyjne i pomieszczenia członków zarządu. Na każdym piętrze zlokalizowana będzie sala konferencyjna, oraz kuchnia i pomieszczenia sanitarne. Kondygnacje mają wysokość około 2,5 metra.

2.1.1 Budynek 1

Na parterze mieści się serwerownia i pomieszczenia pracowników administracyjnych. Kolejne dwie kondygnacje zajmują programiści aplikacji webo-

wych, a na ostatnim piętrze mają swoją siedzibę programiści aplikacji na systemy mobilne.

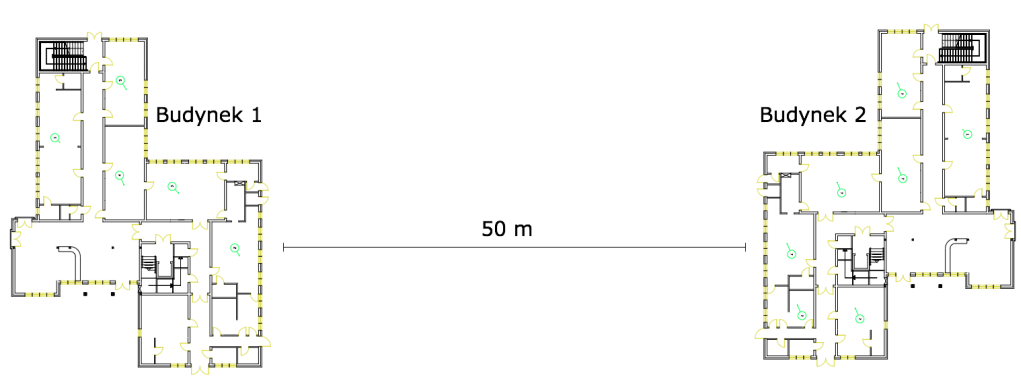
2.1.2 Budynek 2

Parter oraz pierwsze piętro zajmują sale konferencyjne oraz pomieszczenia dla programistów. Na ostatnim piętrze znajdują się biura członków zarządu.

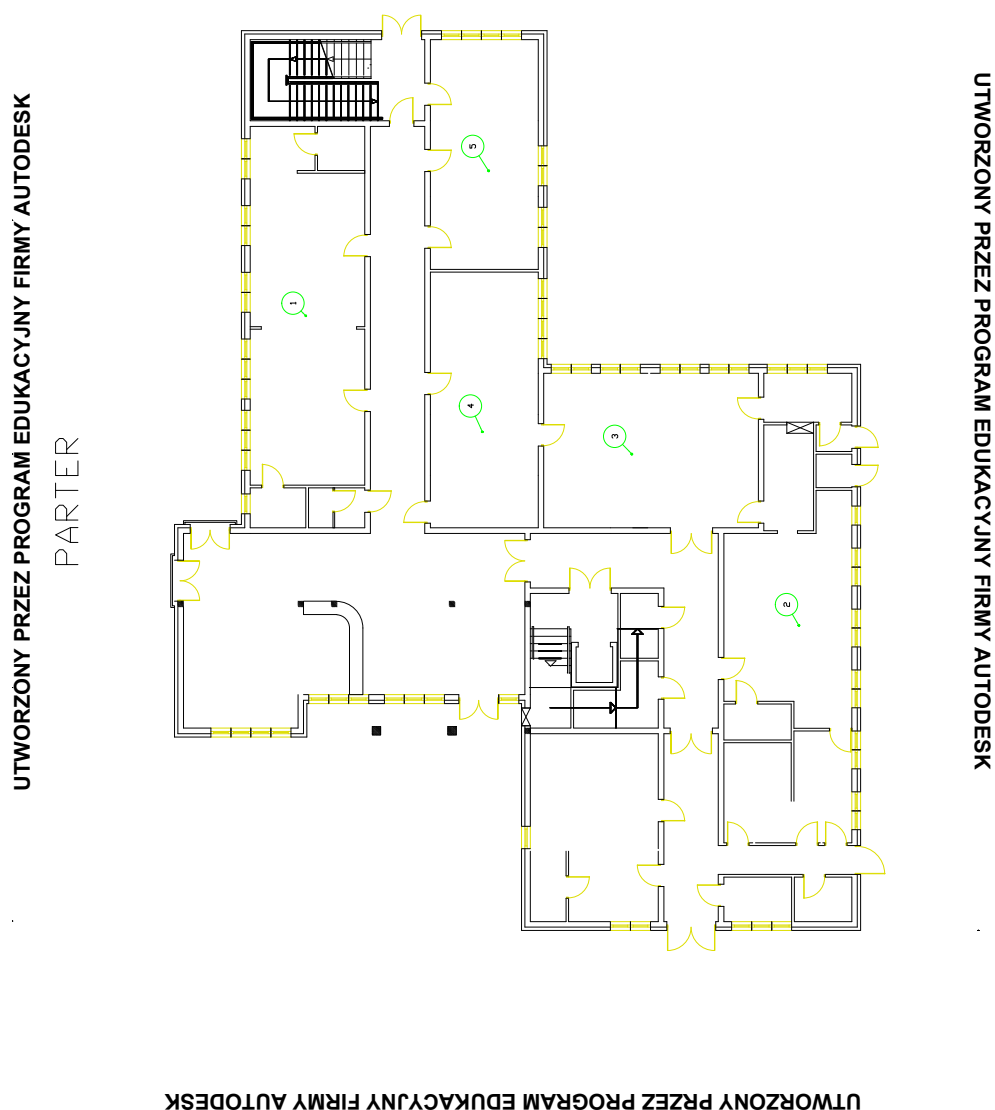
Poniżej znajdują się plany obu budynków w skali 1 : 265 oraz ich wzajemne położenie.

1	Sala konferencyjna
2	Serwerownia
3,4,5	Pomieszczenia administracyjne
7	Pomieszczenia programistów
11	Pomieszczenia członków zarządu

Tabela 1: Oznaczenia pomieszczeń



Rysunek 1: Wzajemne położenie budynków

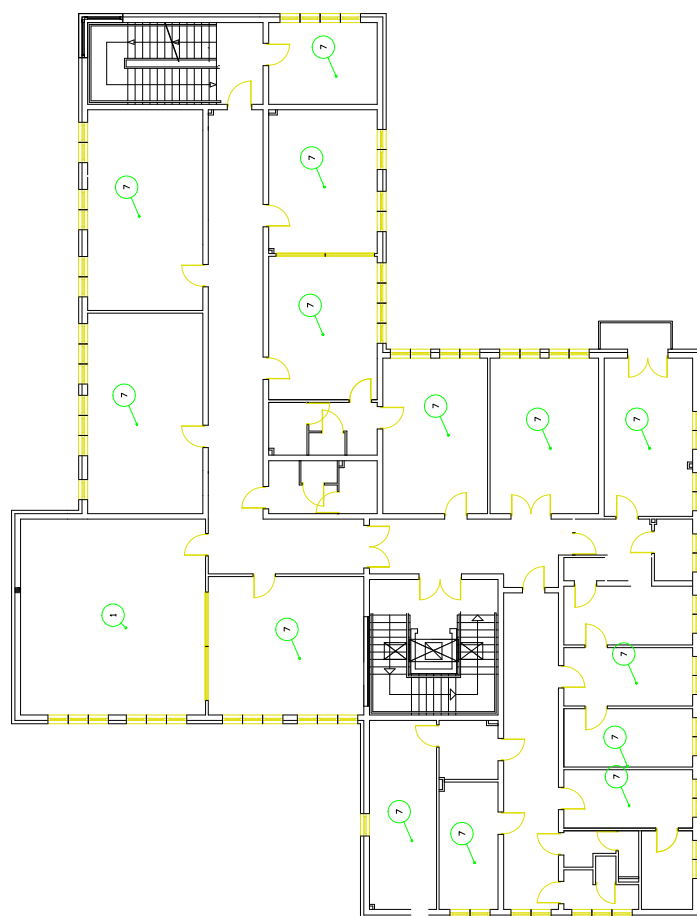


Rysunek 2: Budynek 1 - Parter

UTWORZONY PRZEZ PROGRAM EDUKACYJNY FIRMY AUTODESK

UTWORZONY PRZEZ PROGRAM EDUKACYJNY FIRMY AUTODESK

PIĘTRO I



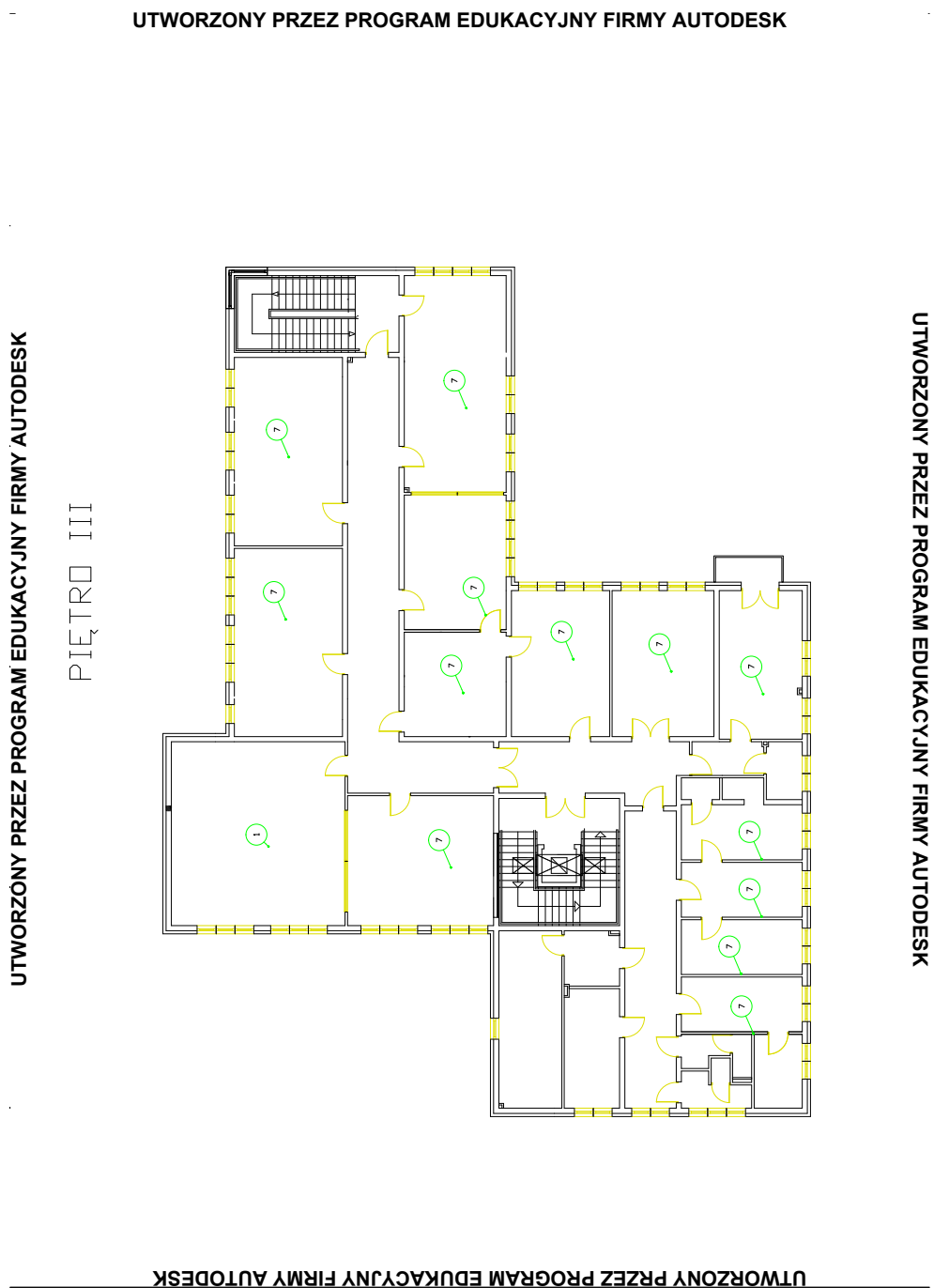
UTWORZONY PRZEZ PROGRAM EDUKACYJNY FIRMY AUTODESK

UTWORZONY PRZEZ PROGRAM EDUKACYJNY FIRMY AUTODESK

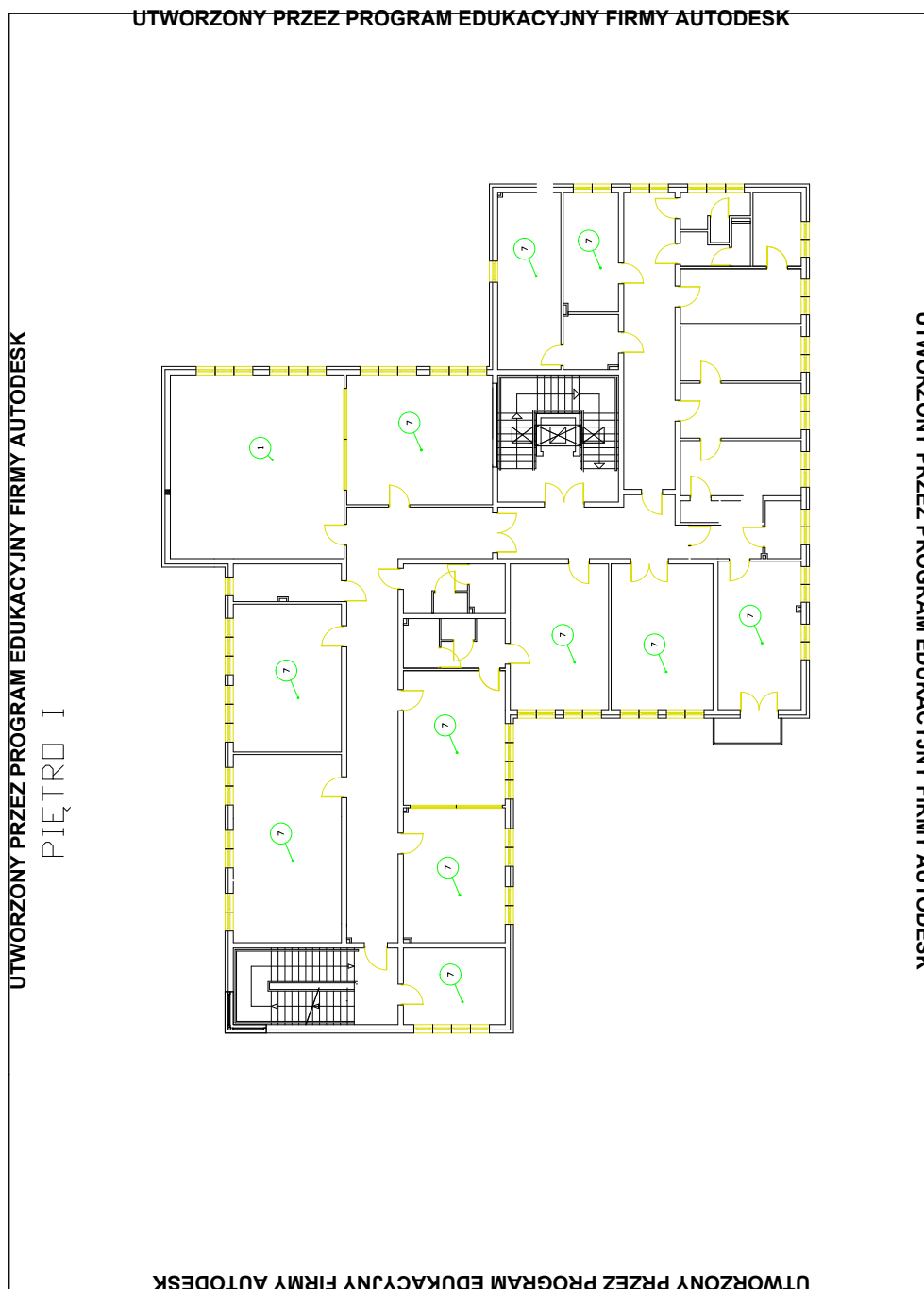
Rysunek 3: Budynek 1 - Piętro I



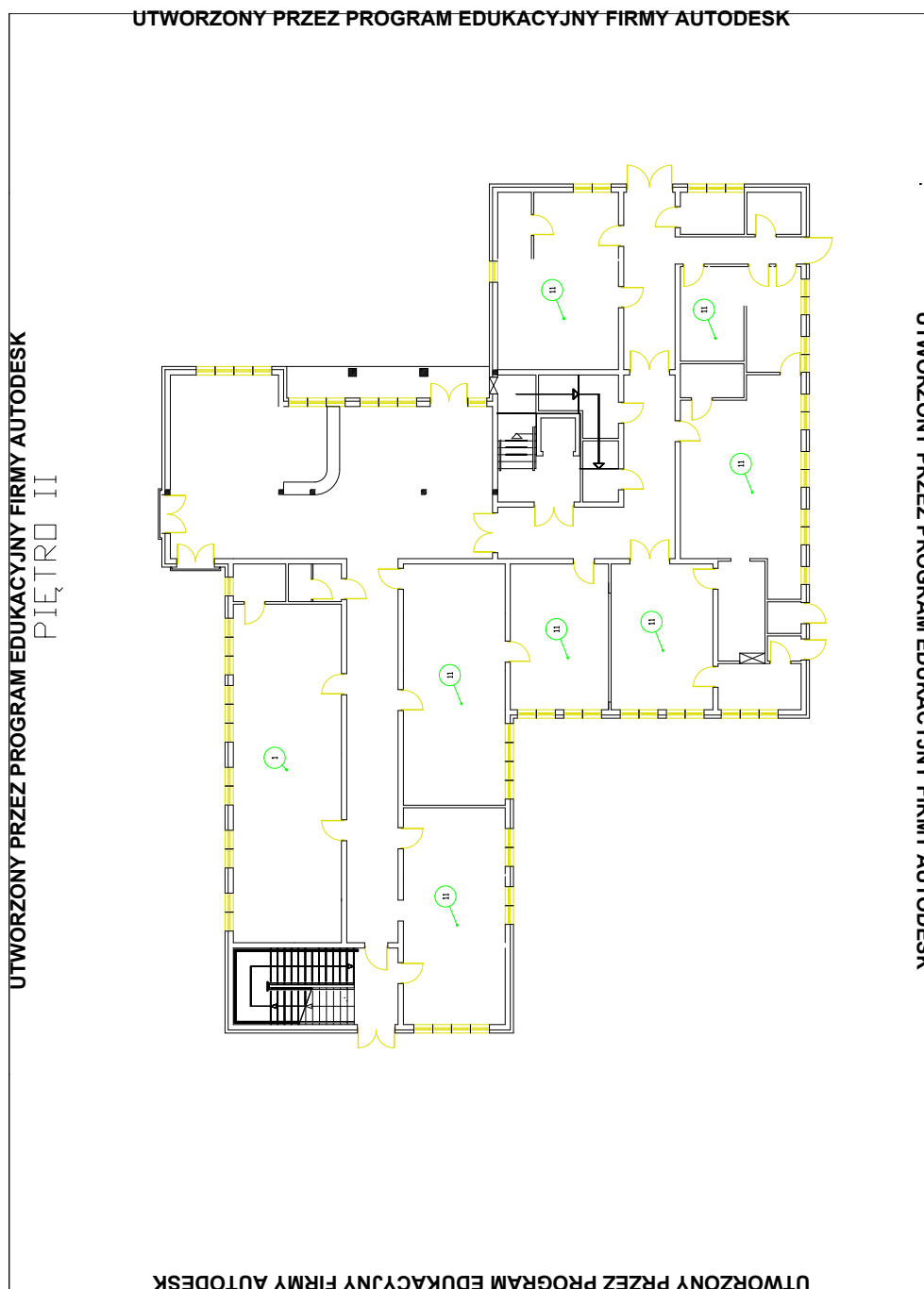
Rysunek 4: Budynek 1 - Piętro II



Rysunek 5: Budynek 1 - Piętro III



Rysunek 7: Budynek 2 - Piętro I



Rysunek 8: Budynek 2 - Piętro II

2.2 Wyposażenie

Wyposażeniem każdego pracownika jest stacjonarny zestaw komputerowy, w skład którego wchodzi: jednostka centralna, mysz, klawiatura, monitor, kamera internetowa, słuchawki z mikrofonem. Na każdym piętrze znajduje się sieciowe urządzenie wielofunkcyjne, podłączone i skonfigurowane w sposób zapewniający dostęp wszystkim pracownikom z danego piętra.

Każda z sal konferencyjnych została wyposażona w rzutnik multimedialny, a także komputer stacjonarny umożliwiający prowadzenie tele i wideokonferencji. Ponadto w każdej z sal konferencyjnych umieszczony jest punkt dostępowy sieci bezprzewodowej.

Część parteru jednego z budynków została zaadaptowana jako serwerownia, w której umieszczono kilka serwerów. Serwery te pozwalają na przechowywanie repozytoriów kodu źródłowego, przeprowadzanie testów oprogramowania, składowanie i wymianę plików między pracownikami, kopie zapasowe danych, a także dostęp do baz danych wykorzystywanych do administracji oraz przy pracy nad projektami.

Systemy operacyjne dostępne dla pracowników:

- Windows 7
- Ubuntu 11
- Mac OS X Lion 10.7

Oprogramowanie wykorzystywane przez pracowników:

- Komunikator internetowy (protokół XMPP)
- Program do tele i wideokonferencji Skype
- Program pocztowy (dowolny)
- System kontroli wersji (svn, git)
- Oprogramowanie umożliwiające współdzielenie plików Samba
- Narzędzia służące do wytwarzania oprogramowania :

- Windows : Microsoft Visual Studio 2010, Eclipse
 - Linux : Eclipse
 - Mac OS X : XCode
- Program do pracy zdalnej TeamViewer
- Pakiet Office

3 Analiza potrzeb użytkownika

Przy projektowaniu sieci lokalnej dla tak dużej firmy informatycznej należy wziąć pod uwagę bardzo wiele czynników, ale przede wszystkim zapewnić ciągły dostęp do zasobów, a także jak największą predkość łącza.

3.1 Główne wymagania jakie stawiane są wobec tworzonej sieci

1. Możliwość przeprowadzania tele i wideokonferencji przy minimalizacji zakłóceń przy transmisji zadań
2. Ciągła możliwość połączenia z serwerem
3. Bez problemowy *download* i *upload* kodu z serwera
4. Przeglądanie witryn internetowych
5. Współdzielenie plików między komputerami, serwerami. Bez problemowa wymiana plików między stacjami używającymi systemów operacyjnych Linux i Mac OS, a stacjami używającymi Windows.
6. Backup danych składowanych na serwerach
7. Możliwość pracy zdalnej za pomocą Remote Desktop i ssh.

3.2 Bezpieczeństwo sieci

1. Konfiguracja Firewall
2. Oprogramowanie antywirusowe

3.3 Tele i wideokonferencje

Z racji świadczonych usług dla klientów międzynarodowych niezbędne jest zapewnienie odpowiedniej przepustowości sieci do prowadzenia tele oraz wideokonferencji. Zalecana przez producenta oprogramowania (Skype) minimalna przepustowość łącza pozwalająca na prowadzenie telekonferencji wynosi 30/30 kb/s, jednak w przypadku większej ilości osób rozmawiających jednocześnie wymagane jest szybsze łącze, ok. 200/100 kb/s. Wideokonferencje wymagają znacznie szybszego połączenia. Minimalna prędkość podana przez producenta to 128/128 kb/s, jednak podobnie jak w przypadku telekonferencji większa ilość osób uczestniczących w wideokonferencji zwiększa wymagania łącza internetowego do ok 4/1 Mb/s.

3.4 Sieć bezprzewodowa

W każdej sali konferencyjnej znajduje się punkt dostępowy sieci bezprzewodowej oferujący jedynie dostęp do Internetu i innych komputerów w obrębie tej sali. Ma to na celu zwiększenie bezpieczeństwa i zablokowanie dostępu do sieci wewnętrznej firmy osobom postronnym. Sieć bezprzewodowa wykończona będzie w standardzie 802.11n, będącym całkowicie zgodnym z poprzednim standardem 802.11g. Uwierzytelnienie użytkowników podłączających się do sieci odbywać się będzie za pomocą szyfrowania *WPA2 – PSK*.

Ze względu na charakter i wymagania pracy osób zajmujących się produkcją oprogramowania dla urządzeń mobilnych, zachodzi potrzeba utworzenia bezpiecznej sieci bezprzewodowej z dostępem do sieci wewnętrznej firmy. Sieć ta o ograniczonym zasięgu, dostępna będzie dla wybranych urządzeń o zautoryzowanych adresach *MAC*.

3.5 Program antywirusowy

W celu zabezpieczenia stacji roboczych przed złośliwym oprogramowaniem, użyty zostanie program antywirusowy ESET Nod32. Jest to oprogramowanie zapewniające duży poziom bezpieczeństwa, jednocześnie nie obciążając zbytnio systemu komputerowego. Kolejną zaletą jest możliwość instalacji go na systemach Linux.

3.6 VLAN

Biorąc pod uwagę specyfikę działania firmy i dynamiczne przydzielanie zadań poszczególnym pracownikom, najlepszym rozwiązaniem będzie odse-

parowanie logicznej struktury sieci od struktury fizycznej za pomocą wirtualnych sieci LAN. Serwery i stacje robocze używane przez konkretną grupę korzystają z tej samej sieci VLAN. Pozwoli to na współpracę wielu osób w ramach jednej grupy niezależnie od ich położenia. Wirtualne sieci LAN znacznie ułatwiają przenoszenie stacji roboczych między podsieciami oraz dodawanie nowych stacji roboczych do istniejących już sieci. Usprawniają też nadzorowanie ruchu w sieci, a także poprawiają bezpieczeństwo.

3.7 VPN

Ze względu na możliwość pracy zdalnej, pracownicy muszą mieć dostęp do serwerów znajdujących się w siedzibie firmy. Mając na uwadze bezpieczeństwo danych sieć firmowa musi udostępniać usługę VPN. Daje to możliwość monitoringu i logowania dostępu do zasobów w bezpieczny sposób, niezależnie od fizycznej lokalizacji pracownika.

3.8 Jakość usług sieciowych

W celu zapewnienia jak najlepszej jakości usług sieciowych, odpowiednich przepustowości łącza, a także eliminacji przeciążenia infrastruktury sieciowej w firmie, zastosowane zostanie urządzenie służące do limitowania ruchu sieciowego (limiter). Pozwoli ono ustalić priorytety połączeń (tele i wideokonferencje - najwyższy, przeglądanie internetu najniższy), ustawić *QoS* oraz pozwoli na filtrowanie ruchu sieciowego, blokowanie niebezpiecznych stron internetowych, czy ograniczyć ściąganie nielegalnych plików.

3.9 Minimalna wymagana przepustowość

Szacując ruch sieciowy w firmie należy rozdzielić ruch wewnątrz sieci lokalnej oraz ruch do sieci zewnętrznej (Internet). W przypadku analizy wymaganej przepustowości na zewnątrz sieci trzeba uwzględnić wymagania, które stawia wykorzystywane oprogramowanie.

Szacowany dzienny przepływ danych w sieci wewnętrznej dla jednego pracownika wynosi ok. 200 Mb. Biorąc pod uwagę fakt, iż serwerownia mieści się w budynku pierwszym, a w budynku drugim będzie pracować ok. 75 osób, można przyjąć założenie, że dzienny transfer pomiędzy budynkami wyniesie 15 Gb. Ruch sieciowy nie jest stały w ciągu dnia, ze względu na sytuacje losowe wymagające wysokiej przepustowości sieci (np. reinstalacja systemu, aktualizacja oprogramowania, tworzenie kopii zapasowych, pobieranie nowego

oprogramowania). Z tego względu budynki powinny zostać połączone światłowodem.

Poniższa tabela przedstawia zalecane przez producenta oprogramowania parametry przepustowości łącza dla pojedynczego użytkownika. W najgorszym hipotetycznym przypadku potrzebuje on przepustowości rzędu 11/7 Mb/s. Takie zapotrzebowanie na łącze jest jednak bardzo mało prawdopodobne. Mimo tego, należy wziąć pod uwagę możliwość prowadzenia kilku wideokonferencji w tym samym czasie bez znacznego ograniczania dostępu do Internetu reszcie pracowników.

	Download [Mb/s]	Upload [Mb/s]
Komunikator internetowy	0,1	0,1
Telekonferencje	0,2	0,1
Wideokonferencje	4	1
Program pocztowy	1	0,5
Zdalny pulpit (TeamViewer, RD)	5	5
Przeglądanie internetu	1	0,5
SUMA	11,3	7,2

Podsumowując wymagania dotyczące przepustowości sieci zalecane łącze internetowe powinno posiadać następujące parametry :

- Download : 20 Mb/s
- Upload : 10 Mb/s

W celu zapewnienia ciągłości połączenia z siecią Internet zalecane jest wydzierżawienie łącza zapasowego o przepustowości 10/5 Mb/s.

W celu zapewnienia skalowalności sieci, w przypadku zwiększenia zatrudnionej liczby pracowników, umowa powinna być zawarta na czas nieokreślony. Daje to możliwość w każdej chwili zwiększenia przepustowości łącza do wymaganej, lub w przypadku redukcji kosztów na zmniejszenie.

3.10 Okablowanie

- Zważając na fakt, iż dwie siedziby firmy znajdują się w pewnej odległości od siebie, a niezbędny jest stały i szybki dostęp do serwerów znajdujących się w jednym z budynków połączenie między dwoma budynkami

firmy będzie zrealizowane za pomocą światłowodu 10 Gb/s (przewidywany jest wzrost ruchu sieciowego związany z wytwarzaniem coraz bardziej skomplikowanego oprogramowania i zatrudnieniem większej liczby osób)

- Ze względu na fakt, iż główny ruch w sieci odbywa się między użytkownikiem, a serwerem, gdzie przechowywany jest kod i aplikacje testowe, połączenia pionowe powinny zapewniać większą przepustowość, niż połączenia poziome. Ten typ połączeń wykonany zostanie za pomocą okablowania typu 1000Base-T Gigabit Ethernet, skrętka ekranowana kategorii 6.
- Okablowanie poziome zostanie zrealizowane w technologii 100Base-T Fast Ethernet, skrętka ekranowana UTP kategorii 6. Decydujemy się na ten typ okablowania, ponieważ pojedynczy użytkownicy sieci, nie będą potrzebowali większej przepustowości niż oferowana przez ten typ połączenia

4 Założenia projektowe

Projekt zakłada stworzenie sieci dla firmy zatrudniającej 180 pracowników, mającej siedzibę w dwóch budynkach oddalonych od siebie o ok. 50 m. Sieć będzie nowoczesna i łatwa do rozbudowy w przyszłości.

W każdym budynku będą znajdować się dwa przełączniki warsty trzeciej połączone funkcją EtherChannel w celu równomiernego rozłożenia obciążenia sieci. Aby zapewnić ciągłość dostępu do Internetu wykonane zostaną dwa przyłącza - główne oraz zapasowe. W celu obsługi podłączenia z Internetem wykorzystane zostaną dwa routery (po jednym na przyłączy) wspierające protokół *VRRP* zapewniający niezawodność połączenia.

Budżet przeznaczony na inwestycję wynosi 150 000 PLN.

Główne założenia projektowe :

1. Okablowanie szkieletowe za pomocą technologii 1000Base-T Gigabit Ethernet, poziome - 100Base-T Fast Ethernet, połączenie między budynkami - światłowód.
2. Wykorzystanie technologii VLAN w celu ograniczenia ilości burz broadcastowych, ułatwienia prac członkom zespołów programistycznych,

zwiększenia bezpieczeństwa sieci. 7 sieci VLAN, ok. 25 pracowników w każdej.

3. Zapewnienie odpowiedniej konfiguracji sieci bezprzewodowej i kontroli dostępu - sieć zabezpieczona hasłem z szyfrowaniem WPA-PSK, z ograniczonym dostępem do zasobów wewnętrznych firmy.
4. W celu zapewnienia niezawodności połączenia z internetem, dzierżawa dwóch łączy od niezależnych operatorów.
5. Umożliwienie bezpiecznej i bezproblemowej pracy zdalnej za pomocą Remote Desktop. W tym celu wykorzystana zostanie technologia VPN.
6. Bezproblemowe korzystanie z usług w sieci wewnętrznej : upload i download kodu, testowanie aplikacji, dostęp do bazy danych.
7. Odpowiednia priorytetyzacja łączy : tele i wideokonferencje - wysoki priorytet, przeglądanie stron www - niski - zastosowanie menadżera pasma.
8. Estetyka wykonania instalacji - ukrycie kabli w podwieszanym suficie i podłodze lub w korytkach.
9. Zapewnienie maksymalnego bezpieczeństwa sieci : ochrona przed atakami z zewnątrz, a także odporność na fizyczne uszkodzenia - ograniczenie dostępu do sieci, zastosowanie oprogramowania antywirusowego NOD32, automatyczna aktualizacja oprogramowania (łatwy bezpieczeństwa), zastosowanie plastikowych osłon przewodów.

5 Projekt sieci

Kolejnym etapem naszego projektu jest projekt logiczny sieci. Na Rysunku 1 przedstawiony zostało wzajemne położenie względem siebie budynków, które dla ułatwienia oznaczeń nazywać i opisu nazywać będziemy *B1* i *B2*.

5.1 Projekt logiczny sieci

Ze względu na charakterystykę działania firmy i potrzeby odbiorcy, sieć podzielona została na sieci *VLANy*, odpowiadające każdemu zespołowi programistów. Pozwoli to na łatwe dołączanie osób do różnych zespołów (np. testerów oprogramowania), bez konieczności fizycznego przenoszenia komputera do pomieszczenia danego zespołu.

Na każdym piętrze dostępna będzie drukarka sieciowa, posiadająca adres z puli odpowiedniego *VLANu*.
















W celu zapewnienia płynnego ruchu sieciowego na każdym piętrze znajdować się będzie switch warstwy 2, podpięty do dwóch przełączników warstwy trzeciej znajdujących się na parterze każdego z budynków. Pomiędzy przełącznikami warstwy trzeciej skonfigurowane zostanie funkcja EtherChannel, pozwalający na połączeniu kilku ethernetowych łączy fizycznych w jedno logiczne. Dzięki temu, przełączniki mogą równomiernie rozkładać obciążenie na łączy, zapewniając wysokowydajnościowe połączenie pomiędzy urządzeniami sieciowymi.

Przełączniki warstwy trzeciej połączone ze sobą zostaną światłowodem w połączeniu każdy z każdym, by zapewnić niezawodność połączenia i zminimalizować ryzyko braku połączenia do internetu lub serwerowni *B2* w wyniku awarii switch'a.

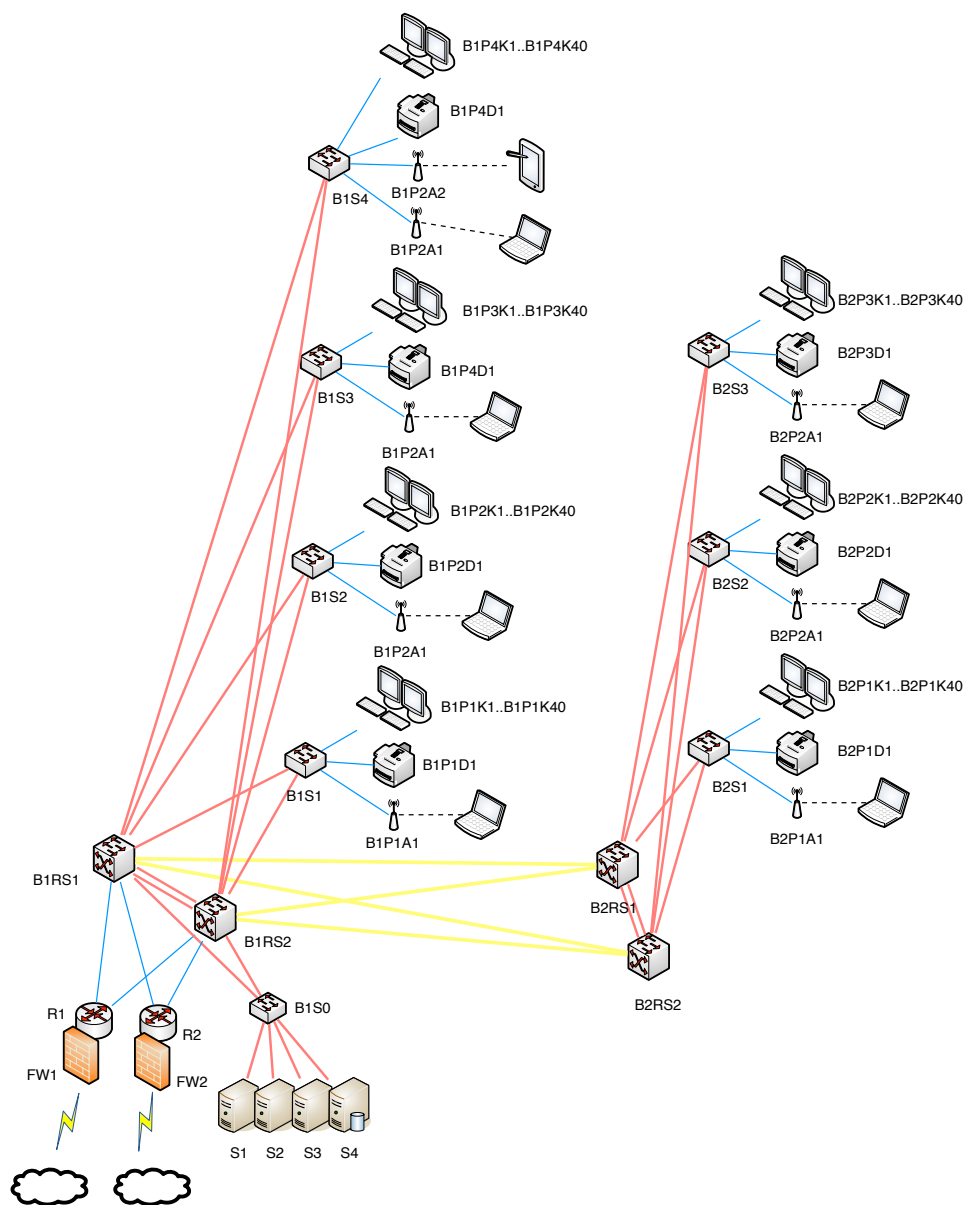
Dwa routery znajdujące się w *B1* odpowiedzialne będą za zapewnienie niezawodnego połączenia z internetem. Pomiędzy routerami zastosowany zostanie protokół VRRP, pozwalający na stworzenie klastra dostępowego, określanego jako wirtualny router. Przysieszy to ruch sieciowy, oraz zwiększy bezpieczeństwo i niezawodność połączenia z internetem.

Oznaczenia :

- $B\{X\}S\{Y\}$ - Switch warstwy 2, gdzie $\{X\}$ - numer budynku, $\{Y\}$ - numer piętra
- $B\{X\}RS\{Y\}$ - Switch warstwy 3, gdzie $\{X\}$ - numer budynku, $\{Y\}$ - numer urządzenia
- $R\{X\}$ - Router, gdzie $\{X\}$ - numer urządzenia
- $S\{X\}$ - Serwer, gdzie $\{X\}$ - numer urządzenia
- $B\{X\}P\{Y\}A\{Z\}$ - Access Point, gdzie $\{X\}$ - numer budynku, $\{Y\}$ - numer piętra, $\{Z\}$ - numer urządzenie
- $B\{X\}P\{Y\}K\{Z\}$ - Stacja robocza, gdzie $\{X\}$ - numer budynku, $\{Y\}$ - numer piętra, $\{Z\}$ - numer urządzenie
- $B\{X\}P\{Y\}D\{Z\}$ - Drukarka sieciowa, gdzie $\{X\}$ - numer budynku, $\{Y\}$ - numer piętra, $\{Z\}$ - numer urządzenie
- $FW\{X\}$ - Firewall sprzętowy, gdzie $\{X\}$ - numer urządzenia
- UPS - UPS

	Światłowód
	GigabitEthernet
	FastEthernet
	Router
	Przełącznik warstwy 3
	Przełącznik
	Stacje robocze
	Punkt dostępowy
	Urządzenie podłączone do sieci bezprzewodowej
	Urządzenia mobilne
	Serwer
	Serwer bazy danych
	Firewall
	Internet
	Połączenie z internetem

Rysunek 9: Schemat logiczny - legenda



Rysunek 10: Schemat logiczny

Podział na Vlany :

- Vlan WiFi - grupujący użytkowników zewnętrznych (np. klientów), niemających dostępu do zasobów wewnętrznych sieci
- Vlan ZarzadIAministracja - grupujący pracowników z działu Administracyjnego, HR oraz zarząd firmy
- Vlan Team{X} - ({X} numer zespołu) grupujący członków danego zespołu
- Vlan UrzadzeniaMobilne - grupujący urządzenia mobilne, wykorzystywane przez programistów aplikacji na przenośne aparaty
- Vlan Serwerownia - grupujący serwery

5.2 Konfiguracja adresacji IP

W celu zapewnienia odpowiedniej puli adresów, zapewniającej możliwość skalowalności i robudowy sieci (np o nowe switchy na poszczególnych piętrach) zdecydowaliśmy się na pulę adresów prywatnych klasy A, zaczynając od adresu sieci *10.1.1.0*.








Poniżej przedstawiono pule adresowe dla poszczególnych *Vlanów* :

- Vlan WiFi : 10.1.1.0 - 10.1.1.255, Adres sieci : 10.1.1.0, Broadcast : 10.1.1.255, Maska : 255.255.255.0
- Vlan ZarzadIAministracja : 10.1.2.0 - 10.1.2.255, Adres sieci : 10.1.2.0, Broadcast : 10.1.2.255, Maska : 255.255.255.0
- Vlan Team1 10.1.3.0 - 10.1.3.255, Adres sieci : 10.1.3.0, Broadcast : 10.1.3.255, Maska : 255.255.255.0
- Vlan Team2 10.1.4.0 - 10.1.4.255, Adres sieci : 10.1.4.0, Broadcast : 10.1.4.255, Maska : 255.255.255.0
- Vlan Team3 10.1.5.0 - 10.1.5.255, Adres sieci : 10.1.5.0, Broadcast : 10.1.5.255, Maska : 255.255.255.0
- Vlan Team4 10.1.6.0 - 10.1.6.255, Adres sieci : 10.1.6.0, Broadcast : 10.1.6.255, Maska : 255.255.255.0
- Vlan Team5(Testerzy) 10.1.7.0 - 10.1.7.255, Adres sieci : 10.1.7.0, Broadcast : 10.1.7.255, Maska : 255.255.255.0

- Vlan Urządzenia Mobilne 10.1.8.0 - 10.1.8.255, Adres sieci : 10.1.8.0, Broadcast : 10.1.8.255, Maska : 255.255.255.0
- Vlan Serwerownia 10.1.9.0 - 10.1.9.255, Adres sieci : 10.1.9.0, Broadcast : 10.1.9.255, Maska : 255.255.255.0

5.3 Projekt fizyczny

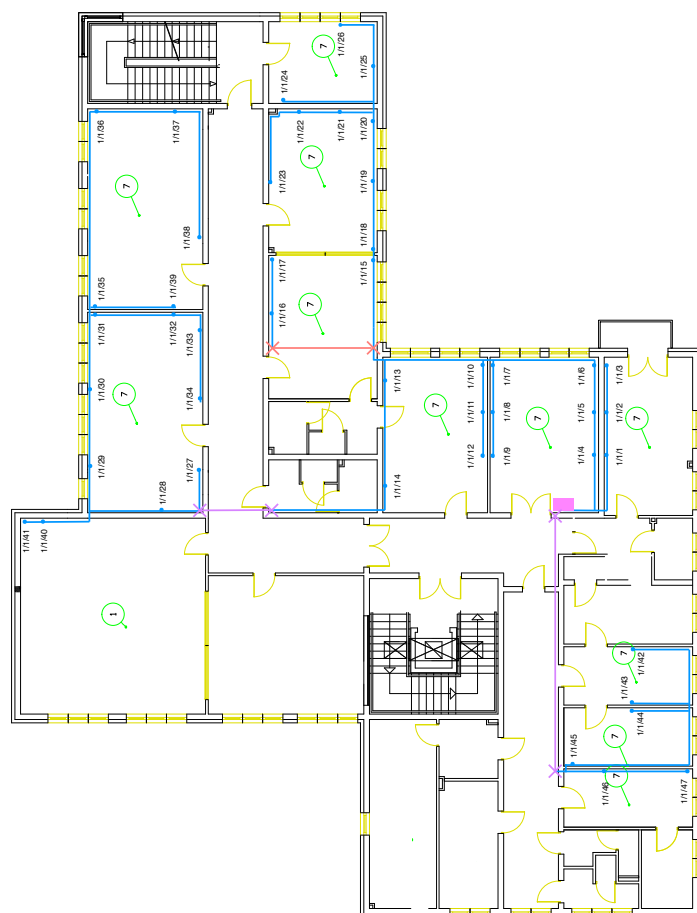
5.3.1 Projekt okablowania

	okablowanie w korytkach PCV
	gniazdo sieciowe
	okablowanie pod sufitem w korycie metalowym
	zejście z sufitu do ściany
	okablowanie w listwie podłogowej
	zejście ze ściany do podłogi
	szafka wisząca

Rysunek 11: Schemat okablowania - legenda

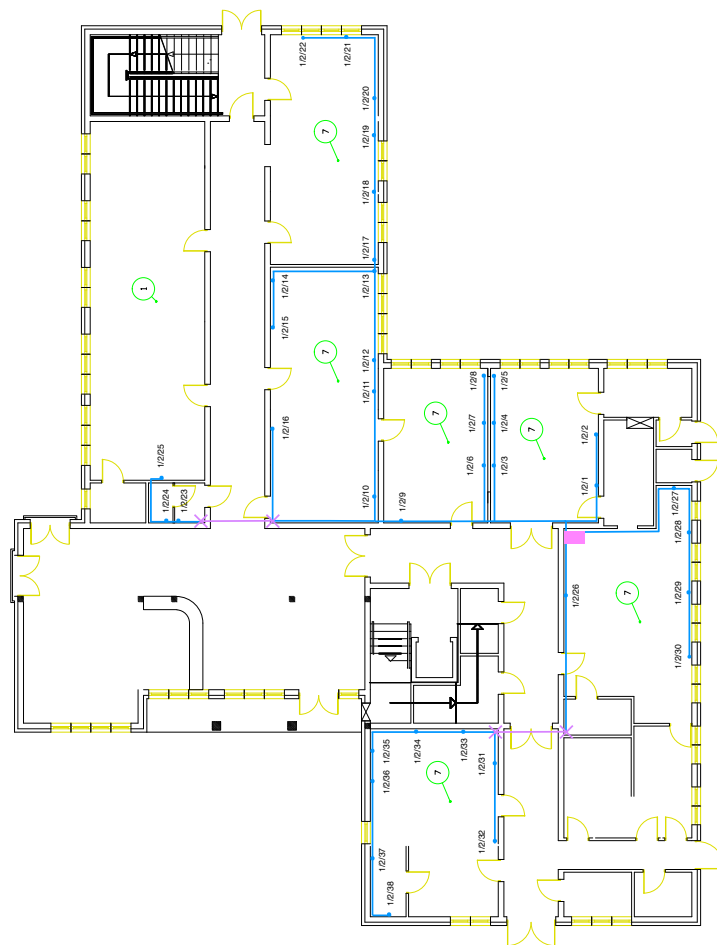
Rysunek 12: Budynek 1 - Parter

PIĘTRO I



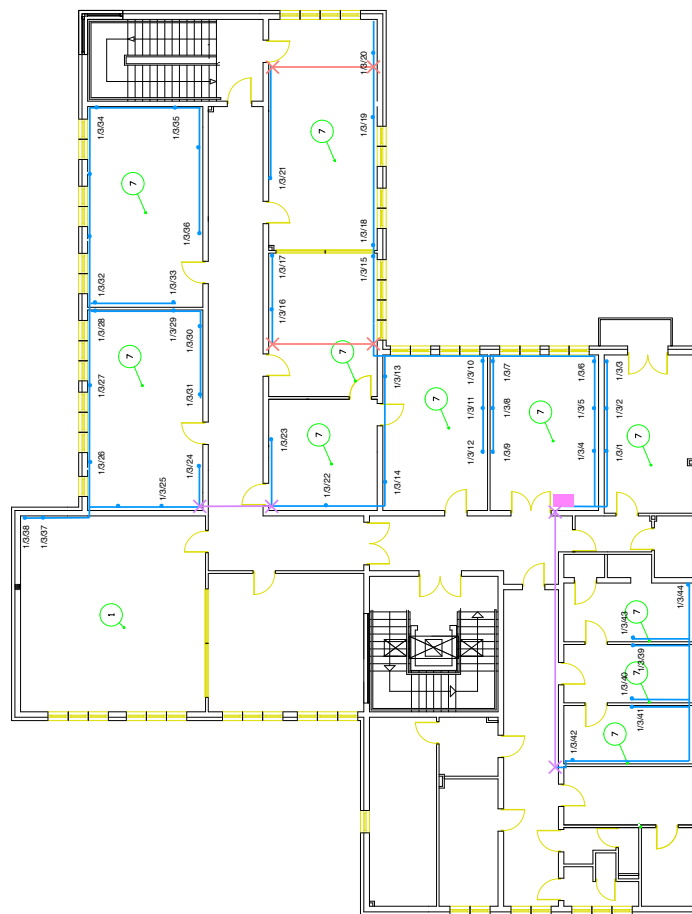
Rysunek 13: Budynek 1 - Piętro I

PIĘTRO II



Rysunek 14: Budynek 1 - Piętro II

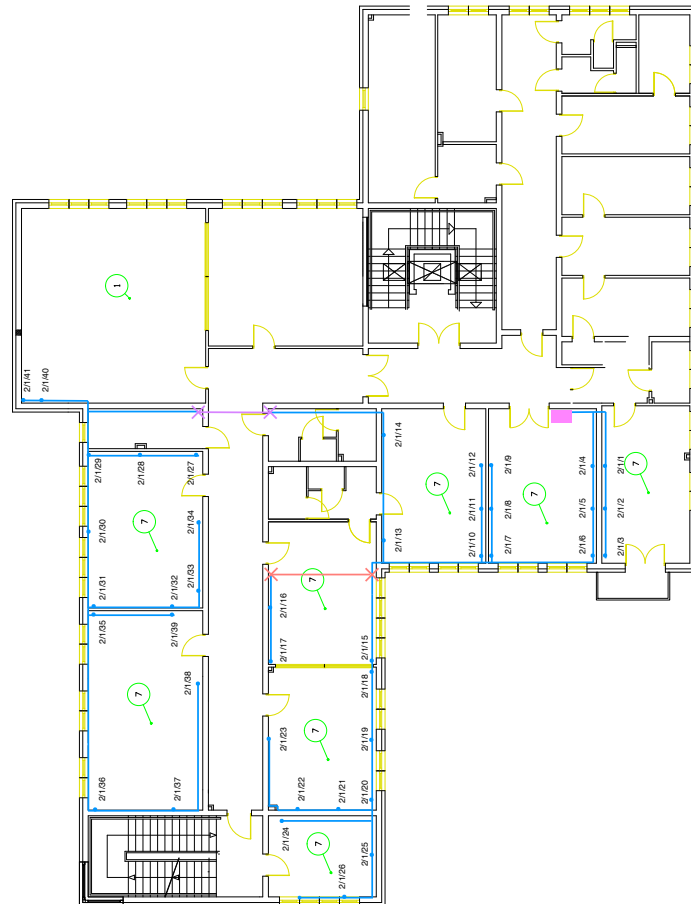
PIĘTRO III



Rysunek 15: Budynek 1 - Piętro III

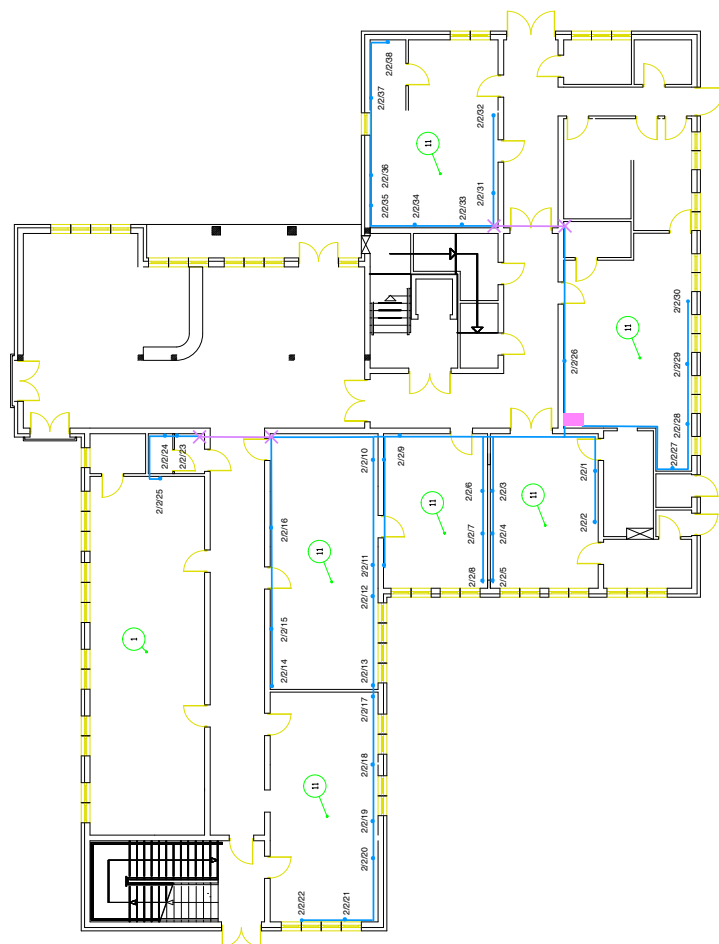
Rysunek 16: Budynek 2 - Parter

PIĘTRO I



Rysunek 17: Budynek 2 - Piętro I

PIĘTRO II



Rysunek 18: Budynek 2 - Piętro II

5.3.2 Umiejscownienie urządzeń w szafach

Na piętrach 1-3 budynku B1 oraz 1,2 budynku B2 umieszczone zostały identyczne szafy wiszące (4U), każda z nich zawiera przełącznik warstwy drugiej oraz dwa 24-portowe patch panele.



Rysunek 19: Schemat szafy wiszącej

W serwerowni mieszczącej się na parterze budynku B1 została umieszczona szafa stojąca (18U). Zawiera ona przełączniki: B1S0 - podłączony do serwerów oraz B1S1 wraz z dwoma 24-portowymi patch panelami, który łączy z siecią komputery z parteru. Ponadto w szafie znajdują się przełączniki warstwy trzeciej, routery wraz z firewallami, serwery, a także awaryjny zasilacz.



Rysunek 20: Schemat szafy stojącej na parterze budynku B1

Na parterze budynku B2 znajduje się większa szafa niż na piętrach, wynika to z konieczności umieszczenia przełączników warstwy trzeciej.



Rysunek 21: Schemat szafy wiszącej na parterze budynku B2

5.3.3 Tabela połączeń

Poniższe tabele prezentują sposób w jaki zostały przyporządkowane gniazda do kolejnych portów przełącznika warstwy drugiej dla poszczególnych pięter w budynkach (odległość podawana jest w metrach).

Gniazdo	Port Switch	Switch	Odległość
1/0/1	Fa0/1	B1S1	10
1/0/2	Fa0/2	B1S1	10
1/0/3	Fa0/3	B1S1	13
1/0/4	Fa0/4	B1S1	13

1/0/5	Fa0/5	B1S1	13
1/0/6	Fa0/6	B1S1	21
1/0/7	Fa0/7	B1S1	22
1/0/8	Fa0/8	B1S1	26
1/0/9	Fa0/9	B1S1	26
1/0/10	Fa0/10	B1S1	29
1/0/11	Fa0/11	B1S1	31
1/0/12	Fa0/12	B1S1	33
1/0/13	Fa0/13	B1S1	36
1/0/14	Fa0/14	B1S1	38
1/0/15	Fa0/15	B1S1	24
1/0/16	Fa0/16	B1S1	32
1/0/17	Fa0/17	B1S1	34
1/0/18	Fa0/18	B1S1	20
1/0/19	Fa0/19	B1S1	20
1/0/20	Fa0/20	B1S1	23

Tabela 2: Gniazdo - Switch, Budynek 1, parter

Gniazdo	Port Switch	Switch	Odległość
1/1/1	Fa0/1	B1S2	4
1/1/2	Fa0/2	B1S2	6
1/1/3	Fa0/3	B1S2	7
1/1/4	Fa0/4	B1S2	4
1/1/5	Fa0/5	B1S2	5
1/1/6	Fa0/6	B1S2	7
1/1/7	Fa0/7	B1S2	11
1/1/8	Fa0/8	B1S2	13
1/1/9	Fa0/9	B1S2	14
1/1/10	Fa0/10	B1S2	11
1/1/11	Fa0/11	B1S2	13
1/1/12	Fa0/12	B1S2	15
1/1/13	Fa0/13	B1S2	16
1/1/14	Fa0/14	B1S2	24
1/1/15	Fa0/15	B1S2	19
1/1/16	Fa0/16	B1S2	22
1/1/17	Fa0/17	B1S2	23

1/1/18	Fa0/18	B1S2	20
1/1/19	Fa0/19	B1S2	23
1/1/20	Fa0/20	B1S2	25
1/1/21	Fa0/21	B1S2	27
1/1/22	Fa0/22	B1S2	29
1/1/23	Fa0/23	B1S2	31
1/1/24	Fa0/24	B1S2	30
1/1/25	Fa0/25	B1S2	27
1/1/26	Fa0/26	B1S2	30
1/1/27	Fa0/27	B1S2	30
1/1/28	Fa0/28	B1S2	29
1/1/29	Fa0/29	B1S2	34
1/1/30	Fa0/30	B1S2	37
1/1/31	Fa0/31	B1S2	40
1/1/32	Fa0/32	B1S2	43
1/1/33	Fa0/33	B1S2	45
1/1/34	Fa0/34	B1S2	48
1/1/35	Fa0/35	B1S2	41
1/1/36	Fa0/36	B1S2	44
1/1/37	Fa0/37	B1S2	49
1/1/38	Fa0/38	B1S2	52
1/1/39	Fa0/39	B1S2	58
1/1/40	Fa0/40	B1S2	35
1/1/41	Fa0/41	B1S2	35
1/1/42	Fa0/42	B1S2	23
1/1/43	Fa0/43	B1S2	21
1/1/44	Fa0/44	B1S2	20
1/1/45	Fa0/45	B1S2	11
1/1/46	Fa0/46	B1S2	12
1/1/47	Fa0/47	B1S2	14

Tabela 3: Gniazdo - Switch, Budynek 1, piętro 1

Gniazdo	Port Switch	Switch	Odległość
1/2/1	Fa0/1	B1S3	4
1/2/2	Fa0/2	B1S3	6
1/2/3	Fa0/3	B1S3	10

1/2/4	Fa0/4	B1S3	12
1/2/5	Fa0/5	B1S3	14
1/2/6	Fa0/6	B1S3	11
1/2/7	Fa0/7	B1S3	12
1/2/8	Fa0/8	B1S3	14
1/2/9	Fa0/9	B1S3	16
1/2/10	Fa0/10	B1S3	18
1/2/11	Fa0/11	B1S3	26
1/2/12	Fa0/12	B1S3	27
1/2/13	Fa0/13	B1S3	31
1/2/14	Fa0/14	B1S3	35
1/2/15	Fa0/15	B1S3	37
1/2/16	Fa0/16	B1S3	28
1/2/17	Fa0/17	B1S3	31
1/2/18	Fa0/18	B1S3	34
1/2/19	Fa0/19	B1S3	36
1/2/20	Fa0/20	B1S3	38
1/2/21	Fa0/21	B1S3	41
1/2/22	Fa0/22	B1S3	42
1/2/23	Fa0/23	B1S3	24
1/2/24	Fa0/24	B1S3	25
1/2/25	Fa0/25	B1S3	27
1/2/26	Fa0/26	B1S3	3
1/2/27	Fa0/27	B1S3	6
1/2/28	Fa0/28	B1S3	9
1/2/29	Fa0/29	B1S3	11
1/2/30	Fa0/30	B1S3	14
1/2/31	Fa0/31	B1S3	13
1/2/32	Fa0/32	B1S3	20
1/2/33	Fa0/33	B1S3	13
1/2/34	Fa0/34	B1S3	15
1/2/35	Fa0/35	B1S3	17
1/2/36	Fa0/36	B1S3	18
1/2/37	Fa0/37	B1S3	21
1/2/38	Fa0/38	B1S3	23

Tabela 4: Gniazdo - Switch, Budynek 1, piętro 2

Gniazdo	Port Switch	Switch	Odległość
1/3/1	Fa0/1	B1S4	4
1/3/2	Fa0/2	B1S4	6
1/3/3	Fa0/3	B1S4	7
1/3/4	Fa0/4	B1S4	4
1/3/5	Fa0/5	B1S4	5
1/3/6	Fa0/6	B1S4	7
1/3/7	Fa0/7	B1S4	11
1/3/8	Fa0/8	B1S4	13
1/3/9	Fa0/9	B1S4	14
1/3/10	Fa0/10	B1S4	11
1/3/11	Fa0/11	B1S4	13
1/3/12	Fa0/12	B1S4	15
1/3/13	Fa0/13	B1S4	16
1/3/14	Fa0/14	B1S4	24
1/3/15	Fa0/15	B1S4	19
1/3/16	Fa0/16	B1S4	22
1/3/17	Fa0/17	B1S4	23
1/3/18	Fa0/18	B1S4	20
1/3/19	Fa0/19	B1S4	25
1/3/20	Fa0/20	B1S4	28
1/3/21	Fa0/21	B1S4	33
1/3/22	Fa0/22	B1S4	24
1/3/23	Fa0/23	B1S4	29
1/3/24	Fa0/24	B1S4	30
1/3/25	Fa0/25	B1S4	29
1/3/26	Fa0/26	B1S4	34
1/3/27	Fa0/27	B1S4	37
1/3/28	Fa0/28	B1S4	40
1/3/29	Fa0/29	B1S4	43
1/3/30	Fa0/30	B1S4	45
1/3/31	Fa0/31	B1S4	48
1/3/32	Fa0/32	B1S4	41
1/3/33	Fa0/33	B1S4	44
1/3/34	Fa0/34	B1S4	49
1/3/35	Fa0/35	B1S4	52
1/3/36	Fa0/36	B1S4	58
1/3/37	Fa0/37	B1S4	35

1/3/38	Fa0/38	B1S4	35
1/3/39	Fa0/39	B1S4	23
1/3/40	Fa0/40	B1S4	21
1/3/41	Fa0/41	B1S4	20
1/3/42	Fa0/42	B1S4	11
1/3/43	Fa0/43	B1S4	23
1/3/44	Fa0/44	B1S4	23

Tabela 5: Gniazdo - Switch, Budynek 1, piętro 3

Gniazdo	Port Switch	Switch	Odległość
2/0/1	Fa0/1	B2S1	10
2/0/2	Fa0/2	B2S1	10
2/0/3	Fa0/3	B2S1	13
2/0/4	Fa0/4	B2S1	13
2/0/5	Fa0/5	B2S1	13
2/0/6	Fa0/6	B2S1	21
2/0/7	Fa0/7	B2S1	22
2/0/8	Fa0/8	B2S1	26
2/0/9	Fa0/9	B2S1	26
2/0/10	Fa0/10	B2S1	29
2/0/11	Fa0/11	B2S1	31
2/0/12	Fa0/12	B2S1	33
2/0/13	Fa0/13	B2S1	36
2/0/14	Fa0/14	B2S1	38
2/0/15	Fa0/15	B2S1	24
2/0/16	Fa0/16	B2S1	32
2/0/17	Fa0/17	B2S1	34
2/0/18	Fa0/18	B2S1	20
2/0/19	Fa0/19	B2S1	20
2/0/20	Fa0/20	B2S1	23
2/0/21	Fa0/21	B2S1	4
2/0/22	Fa0/22	B2S1	6
2/0/23	Fa0/23	B2S1	9
2/0/24	Fa0/24	B2S1	11
2/0/25	Fa0/25	B2S1	14

Tabela 6: Gniazdo - Switch, Budynek 2, parter

Gniazdo	Port Switch	Switch	Odległość
2/1/1	Fa0/1	B2S2	4
2/1/2	Fa0/2	B2S2	6
2/1/3	Fa0/3	B2S2	7
2/1/4	Fa0/4	B2S2	4
2/1/5	Fa0/5	B2S2	5
2/1/6	Fa0/6	B2S2	7
2/1/7	Fa0/7	B2S2	11
2/1/8	Fa0/8	B2S2	13
2/1/9	Fa0/9	B2S2	14
2/1/10	Fa0/10	B2S2	11
2/1/11	Fa0/11	B2S2	13
2/1/12	Fa0/12	B2S2	15
2/1/13	Fa0/13	B2S2	16
2/1/14	Fa0/14	B2S2	24
2/1/15	Fa0/15	B2S2	19
2/1/16	Fa0/16	B2S2	22
2/1/17	Fa0/17	B2S2	23
2/1/18	Fa0/18	B2S2	20
2/1/19	Fa0/19	B2S2	23
2/1/20	Fa0/20	B2S2	25
2/1/21	Fa0/21	B2S2	27
2/1/22	Fa0/22	B2S2	29
2/1/23	Fa0/23	B2S2	31
2/1/24	Fa0/24	B2S2	30
2/1/25	Fa0/25	B2S2	27
2/1/26	Fa0/26	B2S2	30
2/1/27	Fa0/27	B2S2	30
2/1/28	Fa0/28	B2S2	29
2/1/29	Fa0/29	B2S2	34
2/1/30	Fa0/30	B2S2	37
2/1/31	Fa0/31	B2S2	40
2/1/32	Fa0/32	B2S2	43
2/1/33	Fa0/33	B2S2	45
2/1/34	Fa0/34	B2S2	48
2/1/35	Fa0/35	B2S2	41
2/1/36	Fa0/36	B2S2	44

2/1/37	Fa0/37	B2S2	49
2/1/38	Fa0/38	B2S2	52
2/1/39	Fa0/39	B2S2	58
2/1/40	Fa0/40	B2S2	35
2/1/41	Fa0/41	B2S2	35

Tabela 7: Gniazdo - Switch, Budynek 2, piętro 1

Gniazdo	Port Switch	Switch	Odległość
2/2/1	Fa0/1	B2S3	4
2/2/2	Fa0/2	B2S3	6
2/2/3	Fa0/3	B2S3	10
2/2/4	Fa0/4	B2S3	12
2/2/5	Fa0/5	B2S3	14
2/2/6	Fa0/6	B2S3	11
2/2/7	Fa0/7	B2S3	12
2/2/8	Fa0/8	B2S3	14
2/2/9	Fa0/9	B2S3	16
2/2/10	Fa0/10	B2S3	18
2/2/11	Fa0/11	B2S3	26
2/2/12	Fa0/12	B2S3	27
2/2/13	Fa0/13	B2S3	31
2/2/14	Fa0/14	B2S3	35
2/2/15	Fa0/15	B2S3	37
2/2/16	Fa0/16	B2S3	28
2/2/17	Fa0/17	B2S3	31
2/2/18	Fa0/18	B2S3	34
2/2/19	Fa0/19	B2S3	36
2/2/20	Fa0/20	B2S3	38
2/2/21	Fa0/21	B2S3	41
2/2/22	Fa0/22	B2S3	42
2/2/23	Fa0/23	B2S3	24
2/2/24	Fa0/24	B2S3	25
2/2/25	Fa0/25	B2S3	27
2/2/26	Fa0/26	B2S3	3
2/2/27	Fa0/27	B2S3	6
2/2/28	Fa0/28	B2S3	9

2/2/29	Fa0/29	B2S3	11
2/2/30	Fa0/30	B2S3	14
2/2/31	Fa0/31	B2S3	13
2/2/32	Fa0/32	B2S3	20
2/2/33	Fa0/33	B2S3	13
2/2/34	Fa0/34	B2S3	15
2/2/35	Fa0/35	B2S3	17
2/2/36	Fa0/36	B2S3	18
2/2/37	Fa0/37	B2S3	21
2/2/38	Fa0/38	B2S3	23

Tabela 8: Gniazdo - Switch, Budynek 2, piętro 2

5.4 Połączenie pionowe

SwitchL2	SwitchL3	Odległość
B1S1	B1RS1	0,5
B1S1	B1RS2	0,5
B1S2	B1RS1	3
B1S2	B1RS2	3
B1S3	B1RS1	6
B1S3	B1RS2	6
B1S4	B1RS1	9
B1S4	B1RS2	9
B2S1	B2RS1	0,5
B2S1	B2RS2	0,5
B2S2	B2RS1	3
B2S2	B2RS2	3
B2S3	B2RS1	6
B2S3	B2RS2	6

Tabela 9: SwitchL2 - SwitchL3

5.5 Podłączenie do internetu

Jednym z najważniejszych punktów projektu sieci jest połączenie z internetem. Zapewnienie wydajnego łącza o wymaganej przepustowości stanowi priorytet przy wyborze dostawcy usług internetowych. W tym celu można wybrać ofertę dzierżawienia łącza od dwóch firm : UPC (główne) i Netia (zapasowe). Obie firmy oferują symetryczne lub niesymetryczne łącza dedykowane dla firm, pomoc techniczną oraz brak ograniczeń w ilości pobieranych i wysyłanych danych. Pula adresów stałych, sposób podłączenia internetu oraz parametry łącza są sprawą indywidualną, negocjowaną z usługodawcą.

Podłączenie routerów cisco do usługodawcy UPC będzie wymagało zainstalowania w routerze karty rozszerzeń DOCSIS, a Netii - VDSL2.

5.6 Bezpieczeństwo

Projekt sieci powinien przewidywać zabezpieczenie jej przed następującymi czynnikami:

- Ataki z zewnątrz
- Utrata danych
- Wirusy
- Czynniki fizyczne
 - Uszkodzenia kabli
 - Pożar

Podstawową ochronę przeciw atakom z zewnątrz ma pełnić urządzenie UTM NETASQ U70, będące sprzętowym firewall'em. Poza zaporą ogniową urządzenie oferuje również ochronę IPS, a także filtry antyspamowe i antywirusowe, monitoring sieci, blokowanie adresów URL oraz autoryzację połączenia. Razem z zabezpieczeniami na routerach oraz możliwością zdefiniowania QoS, pełnić będą rolę limiterów sieciowych, zabezpieczających przed ściąganiem szkodliwego oprogramowania, nielegalnych plików oraz pozwolą na ustawienie priorytetu ruchu w sieci.

By ochronić stacje robocze przed wirusami, zalecane przez nas jest komercyjne oprogramowanie *NOD32*, posiadające odpowiednie wersje zarówno pod system Windows jak i Linux. W skład pakietu wchodzi również aplikacje SpyWare i RootKit. *NOD32* umożliwia również blokowanie niebezpiecznych aplikacji i witryn internetowych.

Projektowaną sieć należy zabezpieczyć przed czynnikami fizycznymi jak uszkodzenia kabli, przegrzanie serwerów (ewentualne pożary). W celu uniknięcia mechanicznych uszkodzeń okablowania (czynnik ludzki, gryzonie), przewody prowadzone są w korytkach naciennych, listwach przypodłogowych, używane są gniazda RJ-45 podtynkowe. W serwerowni, gdzie przez ciągłą pracę serwerów, temperatura otoczenia może gwałtownie wzrosnąć, zalecane jest założenie klimatyzacji oraz umieszczenie gaśnicy proszkowej, odpowiedniej do gaszenia pożarów w instalacjach elektrycznych. Takie gaśnice powinny się również znaleźć na każdym piętrze budynków zgodnie z wymogami BHP.

Ze względu na charakterystykę oferowanych usług przez firmę zabezpieczenie kodu przechowywanego na serwerach systemu kontroli wersji, a także danych przechowywanych w bazie danych jest jednym z najważniejszych czynników. Obowiązkowe jest tworzenie kopii zapasowych codziennie w nocy, by nie obciążać zbytnio ruchu sieciowego. By chronić dane przed atakami z zewnątrz dostęp do nich zagwarantowany zostanie tylko i wyłącznie z sieci wewnętrznej.

Access Pointy, gwarantujące dostęp do internetu użytkownikom z zewnątrz (np. klientom), zawierać się będą w jednej sieci VLAN, nie mającej dostępu do zasobów wewnętrznych. Zabezpieczone zostaną kluczem WPA2-PSK.

Urządzenia mobilne, korzystające z połączenia z internetem przez WiFi, zgrupowane będą w osobny VLAN, a ich autoryzacja odbywać się będzie po adresach MAC.

5.7 Kosztorys

5.8 Koszt okablowania, szaf, etc...

Nazwa	Ilość	Cena netto	Cena bruttokoszt	Koszt
Kabel instalacyjny UTP 4x2 kat.6	22	352	433	9526
SZAFA 19 PRO-ALFA 4U ACT	5	150	185	925
Gniazdo natynkowe 1xRJ 45 kat.6e kompletne biały	260	4,5	5,6	1456
Patch panel 24P Intellinet UTP Cat6 1U 520959	14	111	137	1918
Światłowod gotowy 50/125 4G SC/SC dł.100m.	1	470	577	577
19in RackMount for Catalyst 3560,2960,ME-3400 Compact Switch	8	154	187	1496
RECESSED 1RU RACK MOUNT FOR 3550, 3560, and 3750	4	103	126	504
Patch cord kat.6 UTP, CU, AWG 26/7, szary 0,5m	370	7,8	9,7	3589
Zestaw montażowy do szafy 19" dla urządzenia U30/U70	2	101	121	242
SZAFA 10 DELTA/10 9U/255 RBA-09-AS3-CAX-C1 TRITON	1	257	315	315
SZAFA 19 DELTA/S 18U/600x600mm stojąca TRITON	1	1035	1273	1273
IWP-8P8C50-STP-CAT6-RJ45		100	1	100
ATEN CL-1000MA KVM Konso-la LCD 17 + kl+touchpad	1	2319	2852	2852
ActiveJet UPS ACP 2000 RACK 19 (SINUSOIDA)+	1	1416	1742	1742
LISTWA-LE 80 (79,5X20,5MM)	15	21	26	390
LISTWA-KANAŁ EKD 80X40	30	20	25	750
Molex Premise Networks : 19"	2	390	780	
Patch cord światłowodowy	4	70	280	

5.9 Koszt urządzeń

Urządzenie	Ilość	Cena jednostki	Koszt
Cisco Catalyst WS-C3550-12T	4	4000	16000
CISCO1921-ADSL2/K9	2	3200	6400
Netsaq U70	2	7000	14000
NETGEAR WNCE2001	8	150	1200
Cisco Catalyst 2960-48TT-L	8	4875	39000
SOLAR 110 X5	4	5453	21812
VDSL2/ADSL/2/2+ EHWIC Annex A	1	2347	2347
Cisco HWIC-CABLE-E/J-2=	1	71347	71347

5.10 Całkowity koszt

Typ	Koszt
Urządzenia	102106
Okablowanie, etc	30446
Suma	132552

6 Karty katalogowe

6.1 Przełącznik warstwy 3

Cisco Catalyst WS-C3550-12T Managed Switch 12 Ports

- **Cisco Part Number:** WS-C3550-12T
- **Speed:** 10/100/1000Mbps
- **Flash Memory:** 8MB Memory
- **RAM Memory:** 32MB Memory
- **Ports:** 10 x 10/100/1000 + 2 x GBIC
- **Interfaces:** 10 x 10Base-TX-RJ-45, 1x RS-232-RJ-45-1-Management
- **Cisco IOS:** Enhanced Multilayer Software Image (EMI)



Rysunek 22: Przełącznik Cisco Catalyst WS-C3550-12T

6.2 Przełącznik warstwy 2

Cisco Catalyst 2960-48TT-L 48 10/100 Ports + 2 1000BT LAN
Base Image

- **Ports:** 2x 10BASE-T/100BASE-TX/1000BASE-T, 48x 10BASE-T/100BASE-TX
- **Flash Memory:** 32 MB Flash
- **RAM Memory:** 64 MB DRAM



Rysunek 23: Przełącznik Cisco Catalyst 2960-48TT-L

6.3 Router

CISCO1921-ADSL2/K9

- **Ports:** 2 Ethernet
- **Speed:** 10/100Mbps
- **Slots:** 2 x EHWICn1 x DEHWIC

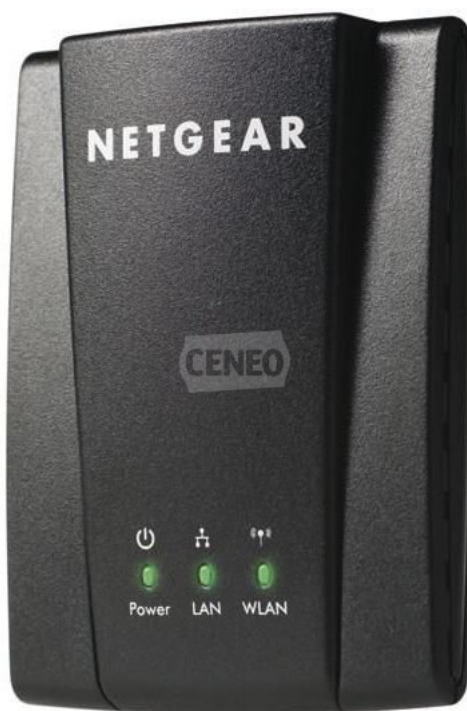


Rysunek 24: CISCO1921-ADSL2/K9

6.4 Access Point

Access Point NETGEAR WNCE2001

- **Standard:** IEEE 802.11n 2.0
- **Ports:** 1 x 10BASE-T/100BASE-TX/1000BASE-T



Rysunek 25: Access Point NETGEAR WNCE2001

6.5 Firewall

UTM NETASQ U70

- **Capacity:** 600Mbps
- **Ports:** 6 x 10/100
- **Systems:** Firewall, IPS, Antispam, Antivirus



Rysunek 26: UTM NETASQ U70

6.6 Serwer

SOLAR 110 X5 1*E1220/4G/2*500G/DVR/R134SH/W8F

- **Processor:** Intel Xeon E3-1220
- **Ram:** 4GB
- **HDD:** 2 x 500GB



OLAF

Rysunek 27: UTM NETASQ U70