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

2 stycznia 2012

Spis treści

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 serwerownie, pomieszczenia administracyjne oraz biura członków zarządu. Na każdym piętrze znajduje się sala konferencyjna.

Ze względów bezpieczeństwa dostep 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 kondygnacja przeznaczone są na serwerownie, pomieszczenia administracyjne i pomieszczenia członków zarządu. Na każdym piętrze zlokalizowana będzie sala konferencyjna, oraz kuchnia i pomieszczenia sanitarne.

2.1.1 Budynek 1

Na parterze mieści się serwerownia i pomieszczenia pracowników administracyjnych. Kolejne dwie kondygnacje zajmują programiści aplikacji webowych, a na ostatnim piętrze mają swoją siedzibę programiści aplikacji na systemy mobilne.

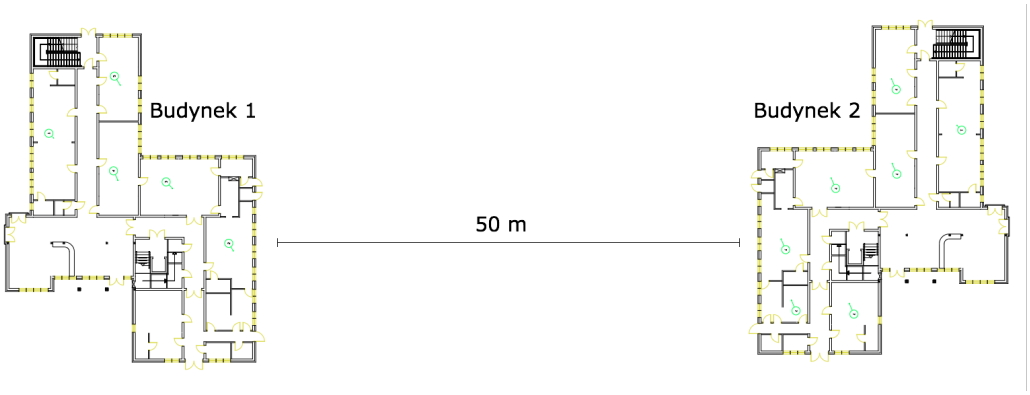
2.1.2 Budynek 2

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

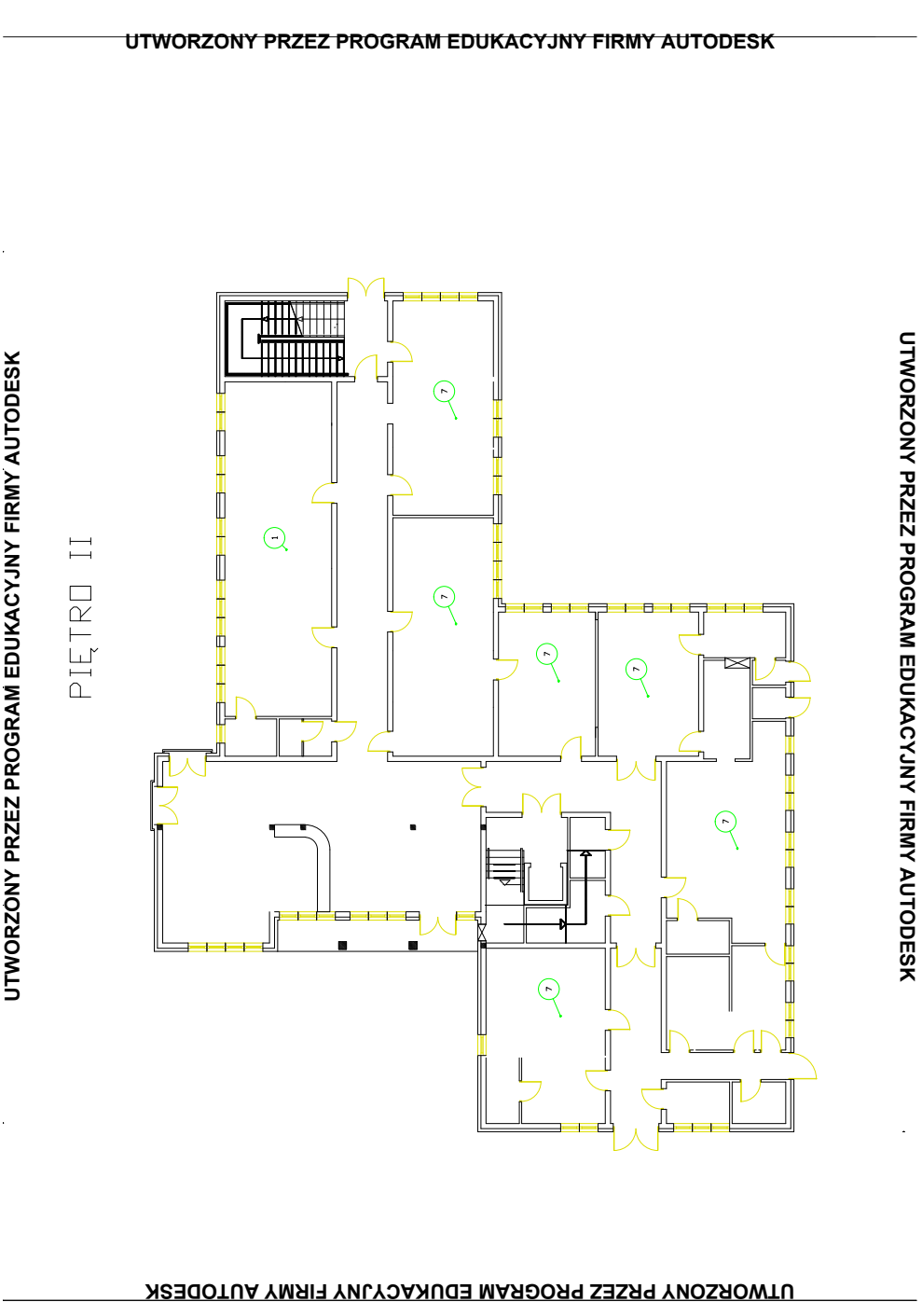
Tabela 1: Oznaczenia pomieszczeń



Rysunek 1: Wzajemne położenie budynków

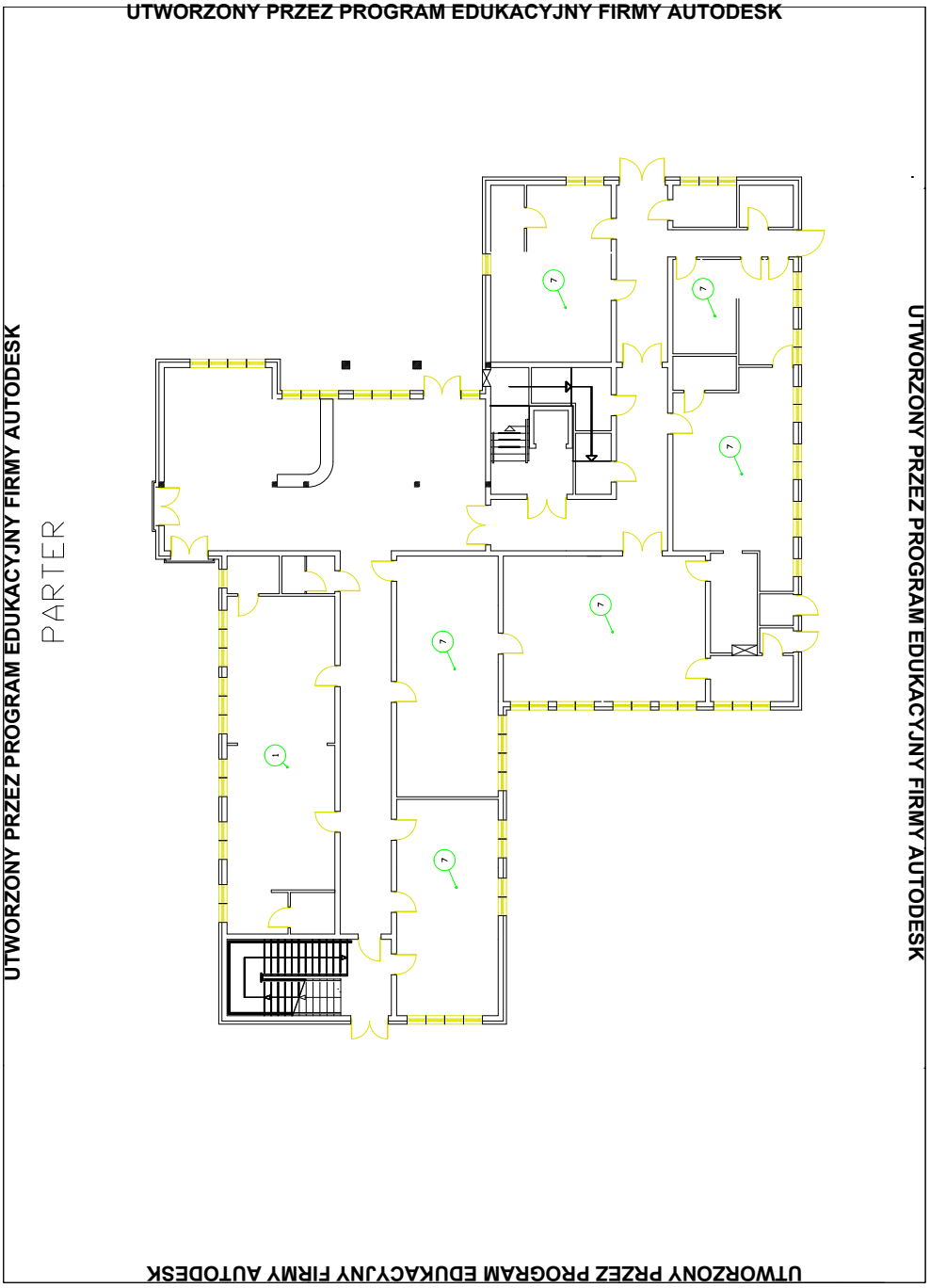
Rysunek 2: Budynek 1 - Parter

Rysunek 3: Budynek 1 - Piętro I

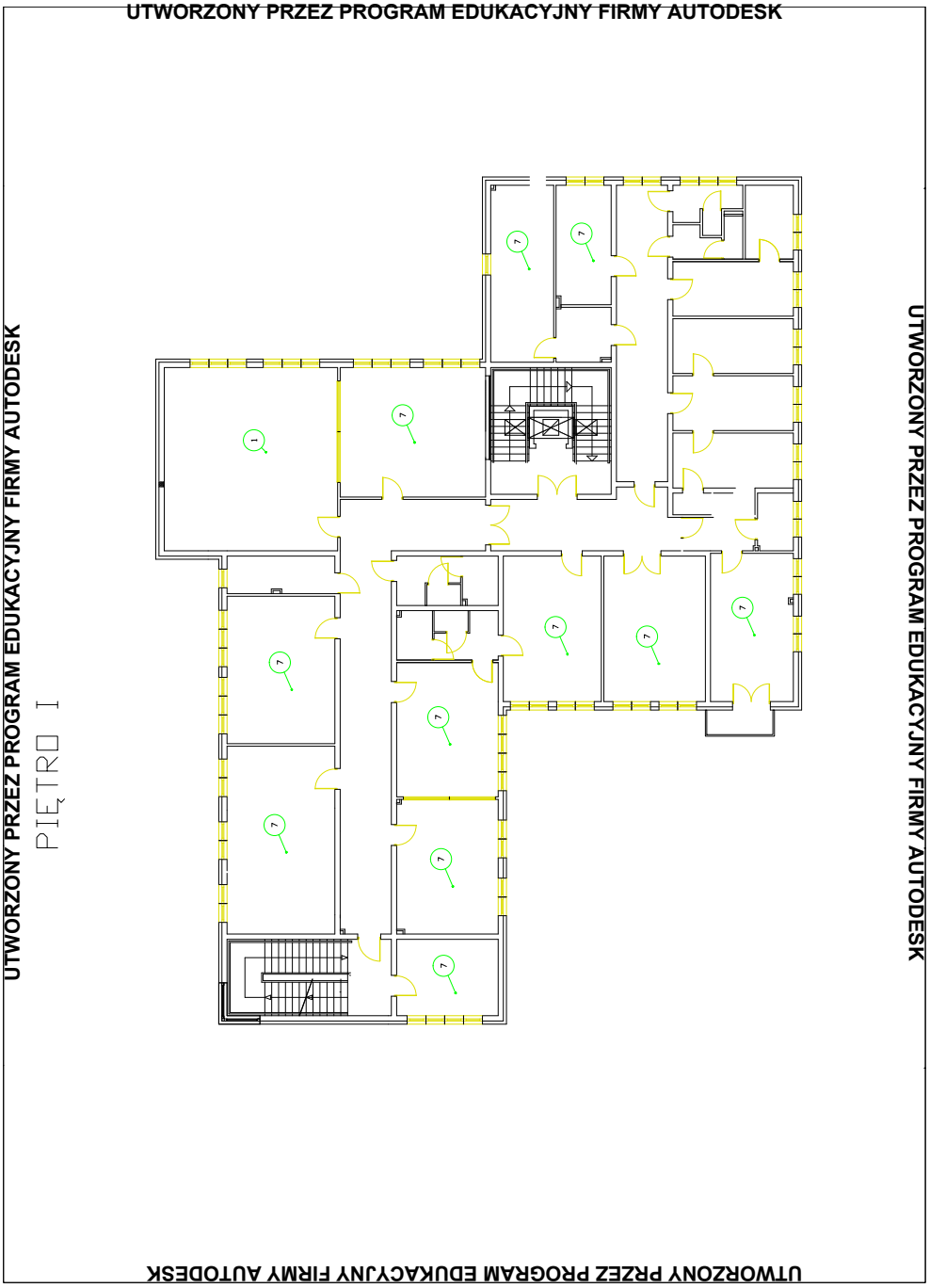


Rysunek 4: Budynek 1 - Piętro II

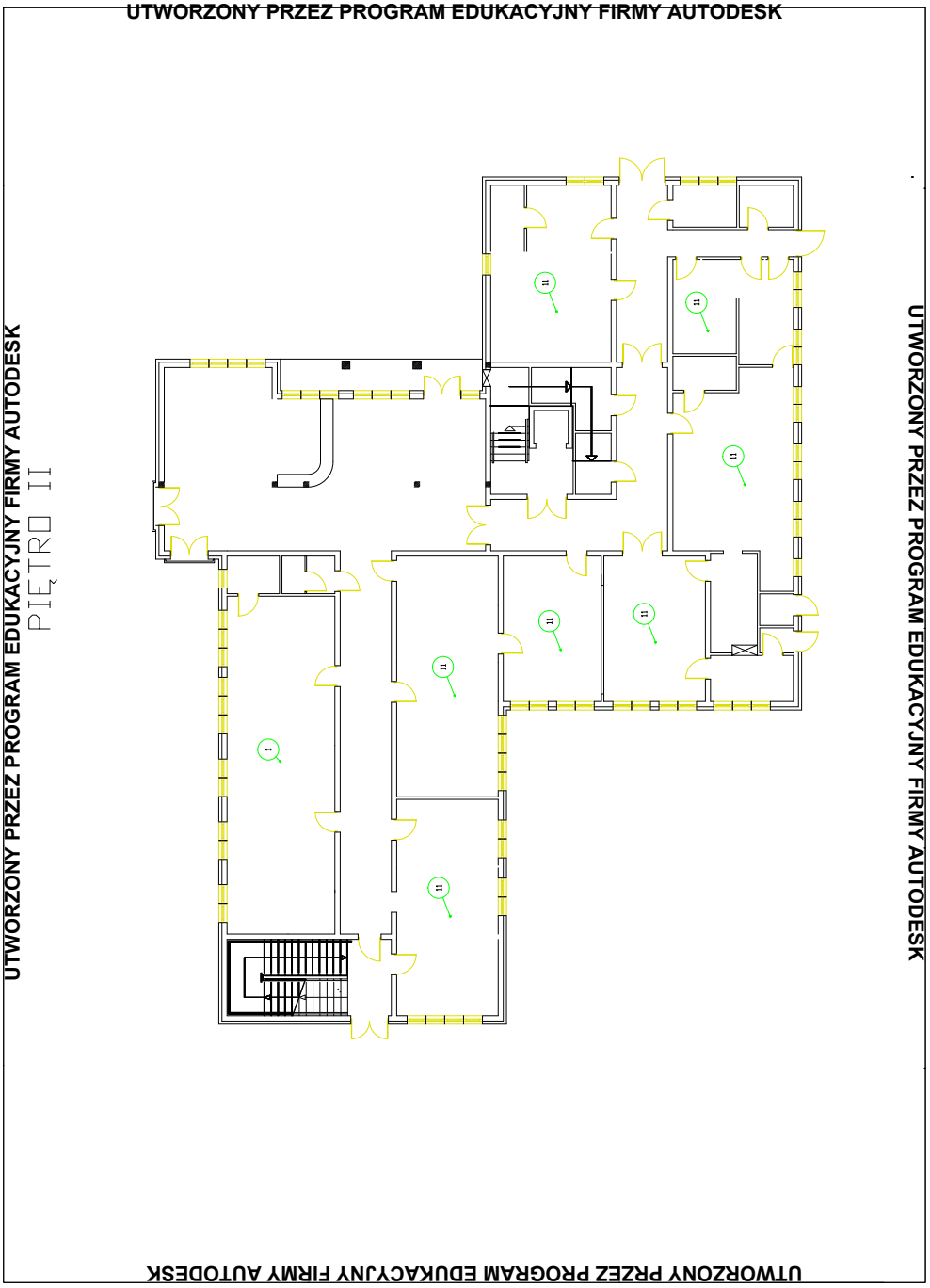
Rysunek 5: Budynek 1 - Piętro III



Rysunek 6: Budynek 2 - Parter



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 wchodzą: 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 repozytowiów kodu źródłowego, przprowadzanie testów oprogramowania, składownie 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 videokonferencji Skype
- Pogram 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 duzej firmy informatycznej nalezy wziac pod uwagę bardzo wiele czynników, ale przede wszystkim zapewnić ciagły dostęp do zasobów, a także jak największa 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 *dwonload* i *upload* kodu z serwera
4. Przeglądanie witryn internetowych
5. Współdzielenie plików miedzy 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. Urządzenie limitujące ruch sieciowy

3.3 Tele i wideokonference

Z racji świadczonych usług dla klientów międzynarodowych niezbędne jest zapewnienie odpowiedniej przepustowości sieci do prowadzenia tele oraz videokonferencji. 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 bezpiczeństwa i zablokowanie dostępu do sieci wewnętrznej firmy osobom postronnym. Sieć bezprzewodowa wykoanna 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 $WPA - PSK$.

Ze względu na charakter i wymagania pracy osób zajmujacych się produkcją oprogramowania dla urządzeń mobilnych, zachodzi potrzeba utworzenia bezpicznej 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 zabezpiecznenia stacji roboczych przed złośliwym oprogramowaniem, użyty zostanie program antywirusowy ESET Nod32. Jest to opragramowanie zapewniające duży poziom bezpieczeństwa, jednocześnie nie obciążając zbytnio systemu komputerowego. Kolejna zaletą jest możliwość instalacji go na systemach Linux.

3.6 VLAN

Biorąc pod uwagę specyfike 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 instniejących 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 ograniczy 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 uwage 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 przepsutowości łącza dla pojedynczego użytkownika. W najgorszym hipotetycznym przypadku potrzebuje on przepustowości rzędu 11/7 Mb/s. Takie zapotrzebowanie na łącze jest jednak bradzo mało prawdopodobne. Mimo tego, należy wziąc 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 przepsutowości 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 zwiekszenai zatrudnionej liczby pracowników, umowa powinna byc zawarta na czas nieokreślony. Daje to możliwość w każdej chwili zwiększenia przepustowości łącza do wymaganej, lub w przypadku redukcji kosztów na zminiejszenie.

3.10 Okablowanie

- Zważając na fakt, iż dwie siedziby firmy znajdują się w pewnej odległości od siebie, a niezbędny jest stały i szybki dostep do serwerów

znajdujących się w jednym z budynków połączenie między dwoma budnykami firmy będzię zrealizowane za pomocą światłowodu 10 Gb/s

- 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 kategori 6.

- Okablowanie poziomie zostanie zrealizowane w technologi 100Base-T Fast Ethernet, skrętka foliowana UTP kategori 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 - głowne oraz zapasowe. W celu obsługi podłączenia z Internetem wykorzystane zostną dwa routery (po jednym na pzyłącze) wspierające protokół $VRRP$ zapewniający niezawodność połączenia.

Bużet 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 kolizji w sieci, 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 połącenia z internetem, dzierżawa dwóch łączy od niezaleznych 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 łącza : tele i widekonferencje - wysoki priorytet, przeglądanie stron www - niski - zastosowanie menadżera pasma.

8. Estetyka wykonania instalacji - ukrycie kabli w podwieszanym suficie i podłodze lub w korytkach.

9. Zapenienie 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 (łaty bezpieczeństwa), zastosowanie plastikowych osłon przewodów.

5 Projekt sieci

Kolejnym etapem naszego projektu jest projekt logiczny sieci. Na Rysunku **TODO** przedstawiony zostało wzajemne położenie względem siebie budynków, które dla ulatwienia 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 na *VLany*, odpowiadające odpowiednio każdemu zespołowi programistów. Pozwoli to na łatwe dołączanie osób do różnych teamó'w (np. testerów orpogramowania), bez konieczności fizycznego przenoszenia komputea do pomieszczenia danego pomieszczenia.

Na każdym piętrze dostepna będzie drukarka sieciowa, posiadająca adres z puli odpowedniego *VLanu*.

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

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

Dwa routery znjadujące się w *B1* odpowiedzialne będą za zapewnienie niezawodnego połączenia z internetem. Pomiędzy ruoterami zastosowany zosatnie protokół VRRP, pozwalający na stworzenie klastra dostepowego, określanego jako wirtualny router.

Oznaczenia :

- **TODO**

Podział na Vlany :

- **TODO**

TODO legenda vlany

TODO vlany

TODO wstawic legende do rysunku bo cygan nie umial podzielic pliku

TODO wstawic rysunek

5.2 Konfiguracja adresacji *IP*

W celu zapewnienia odpowiedniej puli adresów, zapewniajacej możliwość skalowalności i robudowy sieci 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, Maska : 255.255.255.0
- VLan ZarzadIAdministracja : 10.1.2.0 - 10.1.2.255, Maska : 255.255.255.0
- VLan Team1 10.1.3.0 - 10.1.3.255, Maska : 255.255.255.0
- VLan Team2 10.1.4.0 - 10.1.4.255, Maska : 255.255.255.0
- VLan Team3 10.1.5.0 - 10.1.5.255, Maska : 255.255.255.0
- VLan Team4 10.1.6.0 - 10.1.6.255, Maska : 255.255.255.0
- VLan Team5(Testerzy) 10.1.7.0 - 10.1.7.255, Maska : 255.255.255.0

5.3 Projekt fizyczny

TODO

5.4 Podłączenie do internetu

TODO

5.5 Bezpieczeństwo

Projekt sieci powinien przewidywać zabezpieczenie jej przed następującymi czynnikami:

- Ataki z zewnątrz :
  - podsłuchanie ramek typu bradcast
  - Ataki DoS
  - Ataki MAC flooding
  - Vlan leaking
- Utrata danych

- Wirusy
- Czynniki fizyczne
  - Uszkodzenia kabli
  - Pożar

TODO

5.6 Kosztorys

TODO