Audyt sieci radiowej dla budynków domów pomocy społecznej (DPS) Powiatu Koszalińskiego

`

Spis treści

Wstęp

Poniższy dokument jest wynikiem przeprowadzonego audytu sieci radiowej w budynkach domów pomocy społecznej (DPS) Powiatu Koszalińskiego. Celem poniższego dokumentu jest dostarczenie informacji niezbędnych do zaprojektowania i wybudowania wysokowydajnej i bezpiecznej sieci WLAN w technologii WiFi ze 100% pokryciem na obszarze budynków wymienionych w tabeli poniżej i terenach bezpośrednio do nich przylegających.

Zestawienie budynków domów pomocy społecznej Powiaty Koszalińskiego objętych audytem:

Lp.	Dom pomocy społecznej	Nazwa budynku	Kubatura budynku m³	Powierzchnia użytkowa budynku m²	Powierzchnia zabudowy budynku m²
1	Dom Pomocy Społecznej w Nowych Bielicach	PAŁAC	5 270	1 140	546
		ŁĄCZNIK	2438	541	220,2
		KUCHNIA	3 720,4	819	385,7
		ADMINISTRACYJNO-PENSJONATOWY	3 080	682	387
		PRALNIA	2037,3	460,7	308,6
		DOMEK „MARIA"	1626 (bez poddasza) 2075 (z poddaszem)	427,60	508,5
		AGREGATOROWNIA Z WARSZTATEM	329,35	57,05	71
		MAGAZYN	3 477	753,4	820
2	Dom Pomocy Społecznej w Cetuniu	BUDYNEK GŁÓWNY	15000	2293	731,95
3	Dom Pomocy Społecznej w Parsowie	PAŁAC	11369	2573	982,89
		MIESZKALNO-ADMINISTRACYJNY	4044	943,20	402,30
		PORTIERNIA	110,78	41,03	46,5
		GARAŻ	180,15	37,5	42,5
4	Dom Pomocy Społecznej w Mielnie	BUDYNEK GŁÓWNY	8056	2152,50	653
		MIESZKALNY	1205,26	226,40	199,09
		SOCJALNO-WARSZTATOWY	1375,07	308,2	263
		AMFITEATR LETNI	290	60	62
		HANGAR	466	125	128
		KRĘGIELNIA	1895,26	241,9	273

Nowa sieć WLAN ma umożliwić funkcjonowanie systemu informatycznego umożliwiającego wsparcie zarządzania DPS oraz wykonywanie teleporad i wideo spotkań. W sieci przesyłane będą dane wrażliwe. W planowanej sieci WLAN musza działać następujące urządzenia i usługi:

- słuchawki VoWLAN,
- tablety,
- smartfony,
- laptopy,
- terminale,
- kolektory danych,
- urządzenia medyczne,
- systemy przyzywowe oraz lokalizacyjne.

Założenia podstawowe audytu

Audyt został stworzony w oparciu o podstawowe założenia przedstawione przez Zamawiającego dla sieci WLAN w każdym obiekcie powinien zawierać:

- Pokrycie zasięgiem pozwalające na roaming bez przerwy w dostępie do sieci, w szczególności dla urządzeń głosowych.
- Minimalny próg sygnału na poziomie -62dBm przy SNR 25dBm.
- W każdym punkcie budynku powinna być widoczność przynajmniej trzech access pointów na odpowiednim poziomie, o ile jest to możliwe ze względów technicznych i ekonomicznych.
- Na terenach wskazanych przez poszczególnych dyrektorów DPS, przylegających do audytowanych budynków, musi zostać zapewniony zasięg umożliwiający wykorzystanie usług konferencyjnych.
- Zakłada, że mogą wystąpić zakłócenia wspólnotowe dla pracujących urządzeń.
- Zakłada wsparcie dla QoS w sieci bezprzewodowej (wsparcie dla protokołów SIP oraz H.323, konfigurowalne polityki QoS, wsparcie dla WMM, CAC czy U-APSD).
- Zakłada zasilanie zgodne ze standardem IEEE 802.3at PoE+.

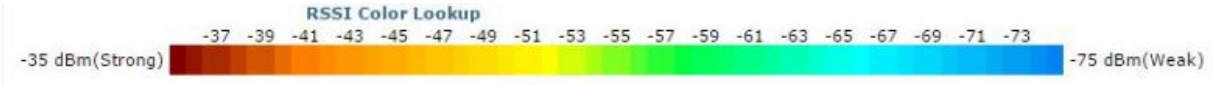
Zamawiający określił również sposoby zarzadzania rozwiązaniem:

- Centralne rozwiązanie całą infrastrukturą bezprzewodową poprzez kontroler sieci bezprzewodowej.
- Możliwość na żądanie oraz ciągłego sprawdzania dostępności, przepustowości, strat pakietów i opóźnień interfejsu radiowego oraz wykonywania testowych połączeń telefonicznych pod kątem sprawdzania opóźnień i strat pakietów.
- Dostęp dla gości przez Captive Portal.

Zakres prac audytowych

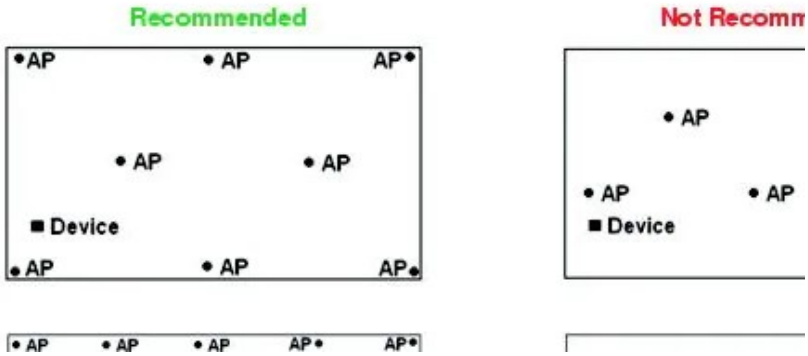
Po uzgodnieniach z Zamawiającym ustalony został zakres audytu, który obejmuje:

- Analizę planów wszystkich budynków dostarczonych przez Dyrektorów DPS.
- Wykonanie badań sieci w budynkach DPS. Ze względu na to, że w obecnej chwili w każdym z budynków DPS sieć bezprzewodowa nie występuje bądź jest to sieć ograniczona jedynie do części administracyjno biurowej nie można przeprowadzić pełnych badań sieci. W audycie zawarte zostały pomiary tylko fragmentów, gdzie nadawana jest sieć WLAN.
- Na postawie wizyty lokalnej oraz uzgodnień z Zamawiającym oraz wojewódzkim konserwatorem zabytków zostały wykonane zadania:
    - Możliwość podłączenia każdego budynku do szerokopasmowego Internetu. Po ustaleniach z Zamawiającym w audycie zostały zawarte informacje o możliwościach podłączenia budynków DPS przez Orange oraz lokalnego operatora Gawex. Ze względu na to, że lokalny operator Gawex nie ma w żadnej lokalizacji infrastruktury światłowodowej w dalszej części będzie uwzględniony tylko operator Orange.
    - Wyznaczoną optymalną liczbę punktów dostępowych, wyznaczono miejsca montażu punktów dostępowych. Po ustaleniach z Zamawiającym w audycie znalazły się mapy rozmieszczenia access pointów wraz z planowanym rozłożeniem sygnały radiowego. Zostało wykonane koncepcyjne planowanie radiowe, które może zostać uwzględnione w przyszłym projekcie nowej sieci bezprzewodowej. Planowanie radiowe pozwala na określenie przybliżonej potrzebnej liczby urządzeń, która pozwoli pokryć sygnałem cały obszar. Symulacje zasięgu przedstawiają przewidywane kierunki propagacji sygnału na zdefiniowanych wcześniej planach budynków. Symulacja radiowa pozwala na uwzględnienie wszelkiego rodzaju przeszkód, które mogą pojawić się na drodze fali radiowej. Ściany w zależności od swojej grubości mogą w różny sposób wpływać na dostępność sygnału. W planowaniu została również wykorzystana wysokość budynków i pomieszczeń, w których mają zostać zainstalowane urządzenia. W heat mapach przedstawiających zasięg sygnału radiowego pochodzącego od każdego access pointa jest zastosowana taka sama skala mocy sygnału jak na poniższej skali, kolor czerwony oznacza sygnał najmocniejszy, kolor niebieski sygnał najsłabszy. Kolor niebieski (-75 dBm), mimo że jest oznaczony, jako słaby nadal pozwala na transmisję danych.



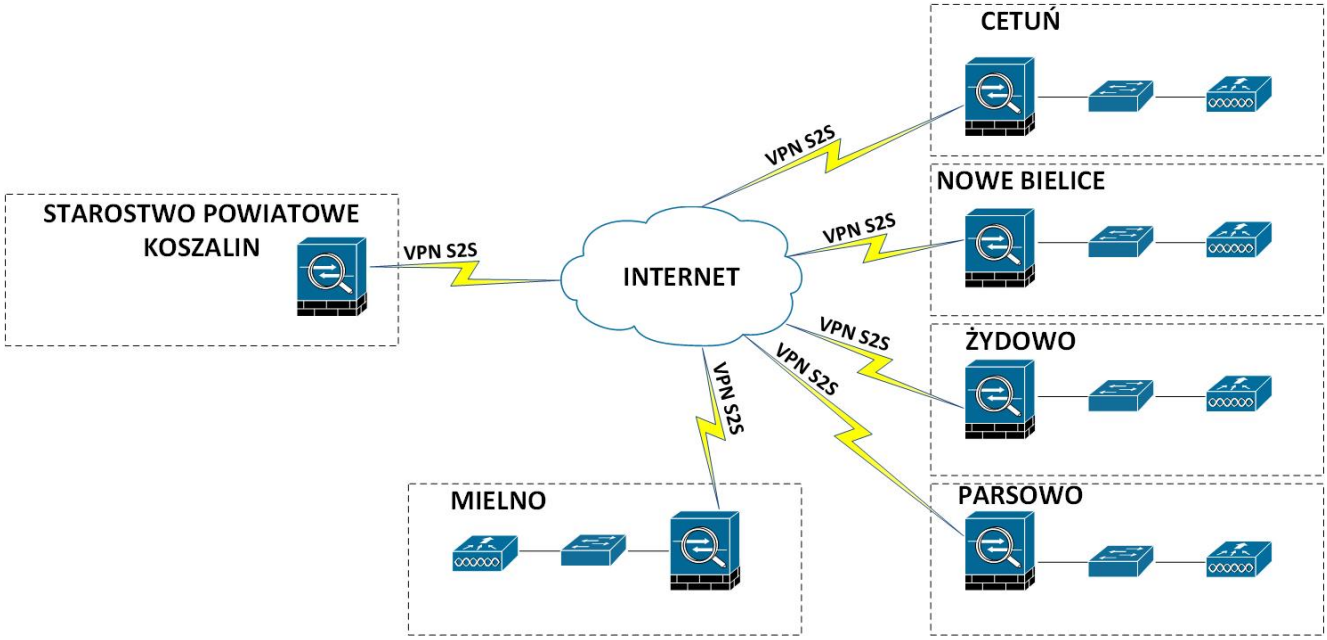
    - Planowanie radiowe zostało przeprowadzone zgodnie z założeniami uzgodnionymi z Zamawiającym. Ma obejmować wszystkie obszary, gdzie poruszają się mieszkańcy oraz wszystkie obszary magazynowe i wskazane przez administrację. Założeniem przyjętym dla obszarów mieszkalnych jest takie rozmieszczenie access pointów, aby zrealizować poprawną triangulację, która będzie wykorzystywana do lokalizacji. Poziomy mocy sygnału jakie zostały ustalone to -65 dBm wewnątrz budynków, tak aby w przyszłości możliwe było również zrealizowanie telefonii voip. Dla usług typu „data” przyjmowany poziom sygnału to -70 dBm. Mimo tego, że w zamówieniu audytowym Zamawiający określił poziom mocy sygnału na -62 dBm ze względów techniczno ekonomicznych można go obniżyć do wartości przedstawionych powyżej.

Zalecane rozmieszczanie access pointów dla celów lokalizacyjnych:



- Wyznaczone opcje zasilania punktów dostępowych. Po uzgodnieniu z Zamawiającym w audycie przyjęte zostało, że wszystkie access pointy będą zasilane za pomocą PoE/PoE+ ze switchy znajdujących się punktów dystrybucyjnych. Nie będzie to wymagało tworzenia lokalnego zasilania dla każdego punktu i mocowania dodatkowych zasilaczy.
- Pomiary sieci bezprzewodowej oraz analizę widma przeprowadzono licencjonowanym oprogramowaniem. Pomiary sieci bezprzewodowej wykonano za pomocą VisiWave site survey tool, pomiary widma wykonane zostały za pomocą MetaGeek Chanalyzer. Licencje są własnością wykonawcy audytu.
- Wyspecyfikowano ewentualne problemy projektowe jakie mogą wystąpić na etapie projektowania, wykonywania lub eksploatacji sieci. Po uzgodnieniach z Zamawiającym w audycie znajdą się przykłady miejsc dla każdej lokalizacji jakie mogą stworzyć problemy przede wszystkim w czasie instalacji takie, jak np.: gruba ściana przez jaką będzie niezbędne przewiercenie kabli.
- Wskazane miejsca przeznaczone pod główną serwerownię oraz pośrednie punkty dystrybucyjne. Wskazano proponowane przebiegi tras kablowych z zachowaniem wytycznych dotyczących maksymalnej długości przewodów sieciowych. Po uzgodnieniu z Zamawiającym w audycie znajdują się mapy kondygnacji w każdej lokalizacji, gdzie zaznaczone zostały koncepcyjnie wybrane miejsca, gdzie możliwe będzie zainstalowanie szaf rack, do których będzie zbiegać się okablowanie. Dodatkowo na planach wrysowane zostały zaproponowane trasy kablowe, które będą służyć jako wskazówka dla przyszłego projektanta sieci.
- Wykonanie planowania radiowego pod usługi lokalizacyjne inne niż wireless, np.: Bluetooth. Po uzgodnieniach z Zamawiającym jedyne usługi lokalizacyjne jakie mają być realizowane w przyszłym projekcie to usługi oparte o sieć bezprzewodową. Z tego powodu punkt zostaje pominięty.
- Wykonanie audytu posiadanej sieci LAN oraz projekt sieci LAN pod sieć WLAN. Po uzgodnieniach z Zamawiającym w audycie znalazły się informacje o obecnym stanie sieci w każdej lokalizacji. Ze względu na to, że audyt nie jest projektem a jedynie koncepcją nowej sieci LAN, znalazły się w nim jedynie propozycje jak nowa sieć może wyglądać. Zaproponowane zostały nowe miejsca do wykorzystania pod serwerownie oraz pośrednie punkty dystrybucyjne. Ze względu na to, że obecny stan sieci LAN w każdej lokalizacji jest praktycznie nieistniejący bądź w bardzo niewielkim stopniu w częściach administracyjnych należy przyjąć w przyszłym projekcie schemat wybudowania całej sieci LAN (zarówno pod WLAN, jak i dla części biurowych) całkowicie od zera. Należy założyć, że na styku sieci z Internetem będzie stał firewall,

do którego będzie podłączony switch core, a za nim będą podłączone switche dostępowe w architekturze gwiazdy. Do switchy dostępowych będą podłączone access poitny. Ze względu na bardzo słabe możliwości, jeżeli chodzi o podłączanie internetowe w większości lokalizacji, po uzgodnieniu z Zamawiającym ustalone zostało, że każda z lokalizacji będzie oddzielną „wyspą", która będzie zarządzana lokalnie oraz będzie posiadać swój własny kontroler sieci bezprzewodowej. W przyszłości zależy na tym, aby połączyć każdą z lokalizacji z centralnym punktem jakim jest budynek Starostwa Powiatowego w Koszalinie za pomocą tuneli vpn site to site.



Tak jak zostało to opisane powyżej schemat przedstawia proponowane opcje połączenia każdej z lokalizacji za pomocą vpnów site to site do centralnego firewalla w starostwie powiatowym.

- Dodatkowym elementem jaki należałoby rozważyć jest zainstalowanie centralnego punktu monitorowania wszystkich systemów, np.: w oparciu o SNMP czy Netflow. Zamawiający zdecyduje na etapie projektu/zamówienia czy niezbędne będzie zakupienie dedykowanego serwera fizycznego pod usługi monitoringu czy będzie możliwe wykorzystanie istniejących zasobów w starostwie powiatowym. Usługa taka może zostać zrealizowana za pomocą dedykowanych serwerów danego producenta sprzętu sieciowego, bądź za pomocą dostępnych systemów monitorowania. Do zainstalowania serwera monitorującego, który w większości przypadków jest dostarczany w postaci maszyny wirtualnej niezbędne będzie posiadanie środowiska wirtualizującego, np.: Vmware, które będzie zainstalowane na fizycznym serwerze. Poniżej przedstawiona została wstępna specyfikacja oraz wycena takiego rozwiązania:

L.p.	Wymagania	Opis	Ilość
1	Procesor	2,5GHz, 8 rdzeni/16 wątków, 9,6GT/s, 11MB pamięci podręcznej,	1
2	Pamięć	min. 16GB pamięci	1

3	Dysk	min. 900 GB SSD	2
		Cena:	zł 9995,00

- Każdy z punktów będzie zarządzany niezależnie przez lokalnego administratora. Tak jak było to opisane powyżej ze względu na słabej jakości łącza każda z lokalizacji będzie niezależenie zarządzanym punktem. Dostęp dla pracowników działu informatyki ze starostwa powiatowego może zostać zrealizowany za pomocą podłączenia każdego punktu vpnem site to site. Drugą opcją może być dostęp remote vpn, który będzie uruchomiony w każdej lokalizacji i pozwoli na dostęp do zasobów zewnętrznych dla każdego autoryzowanego użytkownika.
- Określenie przyszłych zabezpieczeń sieci WLAN. Nowa sieć WLAN powinna być oparta o najnowsze rozwiązania security takie jak:
  - WPA2/WPA3,
  - 802.1X,
  - dedykowane portale gościnne, portale gościnne realizowane za pomocą specjalnych serwerów uwierzytelniających,
  - wsparcie dla uwierzytelniania za pomocą certyfikatów,
  - obsługa funkcjonalności związanej z profilowaniem urządzeń użytkujących sieć WLAN i definiowaniem dostępu na podstawie profili,
  - wsparcie dla funkcji analizy stanu urządzeń i działania bazujące na bieżącym stanie urządzeń (np. posiadane poprawki Microsoft Windows) ,
  - na styku sieci WLAN z Internetem powinno zostać zastosowane urządzenie typu next-generation firewall gwarantujące funkcje filtrowania adresów URL, rozpoznawaniu aplikacji oraz zagrożeń na podstawie reguł IPS oraz na podstawie behawioralnej.
- Określone zostały optymalne parametry proponowanych urządzeń zostały przedstawione poniżej:

Kontroler sieci bezprzewodowej:

- urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
  - zarządzanie politykami bezpieczeństwa,
  - wykrywanie zagrożeń w sieci bezprzewodowej,
  - zarządzanie pasmem radiowym,
  - zarządzanie mobilnością,
  - zarządzanie jakością transmisji.
- obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji,
- dostarczenie odpowiedniej licencji na obsługę AP wraz ze wsparciem producenta na okres min. 3 lat,
- min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45),
- opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu,
- obsługa ruchu tunelowanego,
- obsługa min. 1000 klientów sieci bezprzewodowej,
- zarządzanie pasmem radiowym punktów dostępowych:

    - automatyczna adaptacja do zmian w czasie rzeczywistym,
    - optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia),
    - dynamiczne przydzielanie kanałów radiowych,
    - wykrywanie, eliminacja i unikanie interferencji,
    - równoważenie obciążenia punktów dostępowych,
    - tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych,
    - automatyczna dystrybucja klientów pomiędzy punkty dostępowe,
    - mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych,
    - dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu, parametry radiowe,
- mapowanie SSID do segmentów VLAN w sieci przewodowej,
- możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID),
- obsługa sieci kratowych,
- komunikacja między punktami dostępowymi bez medium kablowego,
- separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi),
- automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji),
- obsługa mechanizmów bezpieczeństwa:
    - 802.11i, WPA3, WPA2, WPA, WEP,
    - 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST),
    - obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników,
- kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID,
- obsługa dostępu gościnnego (IPv4 i IPv6):
    - przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony),
    - przekierowanie użytkowników do strony logowania na zewnętrznym serwerze,
- współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych,
- obsługa NTP wersji 4 (IPv4 oraz IPv6),
- obsługa Hotspot 2.0,
- obsługa redundancji rozwiązania (N+1):
    - dodatkowa opcja: obsługa redundancji 1:1 (active/standby) zapewniającej:
        - utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera,
        - synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej.

Access point wewnętrzny i zewnętrzny:

- obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance):

    - obsługa OFDMA (uplink/downlink), TWT, BSS Coloring,
    - obsługa MU-MIMO – min. 2x2:2,
    - obsługa kanałów 20, 40 MHz dla 802.11n,
    - obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax,
    - obsługa beamforming dla klientów 802.11a/g/n/ac/ax,
    - obsługa MRC (Maximal Ratio Combining),
- obsługa szerokiego zakresu kanałów radiowych:
    - dla zakresu 2.4 GHz: min. 13 kanałów,
    - dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów,
    - dla zakresu 5GHz (extended UNII-2): min. 8 kanałów,
- konfigurowalna moc nadajnika:
    - dla zakresu 2.4 GHz: do 100 mW,
    - dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW,
    - dla zakresu 5GHz (extended UNII-2): do 200 mW,
- zarządzanie przez kontroler WLAN z funkcjonalnościami:
    - automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN,
    - optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany),
    - obsługa min. 16 BSSID,
    - definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID,
    - uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w,
    - obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN),
    - możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników,
    - obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h,
    - obsługa IPv6,
    - obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ,
    - obsługa mechanizmów QoS:
        - ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik,
        - obsługa WMM, TSPEC, U-APSD,
    - współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne,
    - wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM,
    - wsparcie IEEE 802.11i, WPA3, WPA2, WPA,
    - wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP),
- konfiguracja polityk bezpieczeństwa per SSID:

    - obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS),
    - współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID),
    - tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe,
    - obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC),
    - obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym,
    - obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta,
    - wsparcie SSH, SNMP, NTP, SYSLOG,
- interfejs Gigabit Ethernet (10/100/1000),
- interfejs konsoli RJ45,
- Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at),
- anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych,
- dla access pointów zewnętrznych:
    - zgodność z IP67,
    - min. praca przy temperaturach między -35^{o}C a 60^{o}C,
- certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint.

Switche core:

- typ i liczba portów:
    - Min: 12 SFP/SFP+,
- opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb):
    - min. 4x1G SFP,
    - min. 4x1/10G SFP+,
- porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
    - Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,
    - Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
- możliwość tworzenia stosów,
- parametry wydajnościowe:
    - szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
    - bufor pakietów – min.: 8MB,
    - pamięć DRAM – min.: 4GB,
    - pamięć flash – min.: 8GB,
    - obsługa:
        - min. 3.000 sieci VLAN
        - min.: 16.000 adresów MAC

- obsługa protokołu NTP,
- przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - Obsługa protokołu STP,
- obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
- możliwość uruchomienia funkcji serwera DHCP,
- mechanizmy związane z bezpieczeństwem sieci:
    - autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    - autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    - możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    - możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    - obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
- obsługa protokołów routingu:
    - routing statyczny dla IPv4 i IPv6,
- przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
- zarządzanie:
    - port konsoli,
    - dedykowany port Ethernet do zarządzania out-of-band
    - plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    - obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
    - port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU.

Switche dostępowe:

- typ i liczba portów:
    - min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP,
- moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami),
- porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
    - porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U,

    - porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax,
- możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    - przepustowość w ramach stosu – min.:60Gb/s,
    - min: 4 urządzenia w stosie,
    - zarządzanie poprzez jeden adres IP,
- parametry wydajnościowe:
    - szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate),
    - bufor pakietów – min: 4MB,
    - pamięć DRAM – min: 1GB,
    - pamięć flash – min: 2GB,
    - obsługa:
        - 1024 sieci VLAN,
        - min: 16.000 adresów MAC,
- obsługa protokołu NTP,
- przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    - IEEE 802.1w Rapid Spanning Tree,
- funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,
- obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
- możliwość uruchomienia funkcji serwera DHCP,
- obsługa protokołów routingu:
    - routing statyczny dla IPv4 i IPv6,
- przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
- zarządzanie:
    - port konsoli,
    - dedykowany port Ethernet do zarządzania out-of-band,
    - plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    - obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
    - port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
- możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU.

Firewall:

- Wymagania ogólne:

- Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
- System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
- System musi wspierać IPv4 oraz IPv6 w zakresie:
  - Firewall.
  - Ochrony w warstwie aplikacji.
  - Protokołów routingu dynamicznego.

- Redundancja, monitoring i wykrywanie awarii
  - W przypadku systemu pełniącego funkcje: firewall, IPSec, kontrola aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
  - Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
  - Monitoring stanu realizowanych połączeń VPN.
- Interfejsy, dysk, zasilanie:
  - System realizujący funkcję Firewall musi dysponować minimum:
    - min. 4 portami Gigabit Ethernet RJ-45,
    - min. 2 gniazdami SFP 1 Gbps.
  - System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
  - System musi być wyposażony w zasilanie AC.
- Parametry wydajnościowe:
  - W zakresie Firewall'a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
  - Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps
  - Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0,5 Gbps.
  - Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps.
- Funkcje Systemu Bezpieczeństwa:
  - W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
    - Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
    - Kontrola Aplikacji.
    - Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
    - Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
    - Ochrona przed atakami - Intrusion Prevention System.
    - Kontrola stron WWW.

        - Zarządzanie pasmem (QoS, Traffic shaping).
        - Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
        - Funkcja lokalnego serwera DNS ze wsparciem dla DNS
- Polityki, Firewall:
    - Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
    - System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
        - Translację jeden do jeden oraz jeden do wielu.
        - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
        - W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
        - Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
- Połączenia VPN:
    - System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
        - Wsparcie dla IKE v1 oraz v2.
        - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
        - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
        - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
        - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
        - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
        - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
    - System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
        - Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
        - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
        - Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
- Routing i obsługa łączy WAN:
    - W zakresie routingu rozwiązanie powinno zapewniać obsługę:
        - Routingu statycznego.
        - Policy Based Routingu.
        - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
- Zarządzanie pasmem:

    - System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
    - Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
    - System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- Ochrona przed malware:
    - Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
    - System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
    - System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
    - System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
- Ochrona przed atakami:
    - Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
    - System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
    - Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    - Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
    - System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
    - Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
    - Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
- Kontrola aplikacji:
    - Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    - Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    - Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
    - Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
    - Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- Kontrola WWW:
    - Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 20 milionów adresów URL pogrupowanych w kategorie tematyczne.

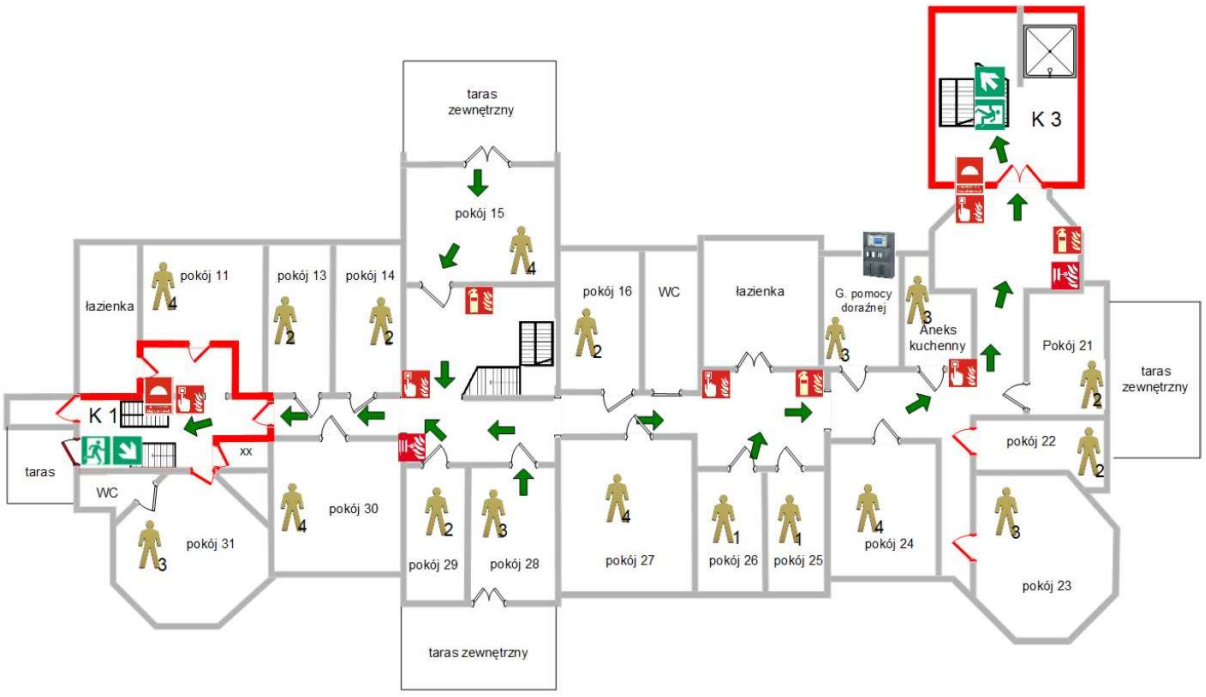
    - W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
    - Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
    - Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
    - Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- Zarządzanie:
    - Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
    - Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
    - System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
    - Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
    - Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI
- Logowanie:
    - Musi istnieć możliwość logowania do serwera SYSLOG.
- Serwisy i licencje:
    - W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów.
- Gwarancja oraz wsparcie:
    - Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres min: 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne
- Rozszerzone wsparcie serwisowe:
    - System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 36 miesięcy.

Załącznik nr 1 DPS Cetuń

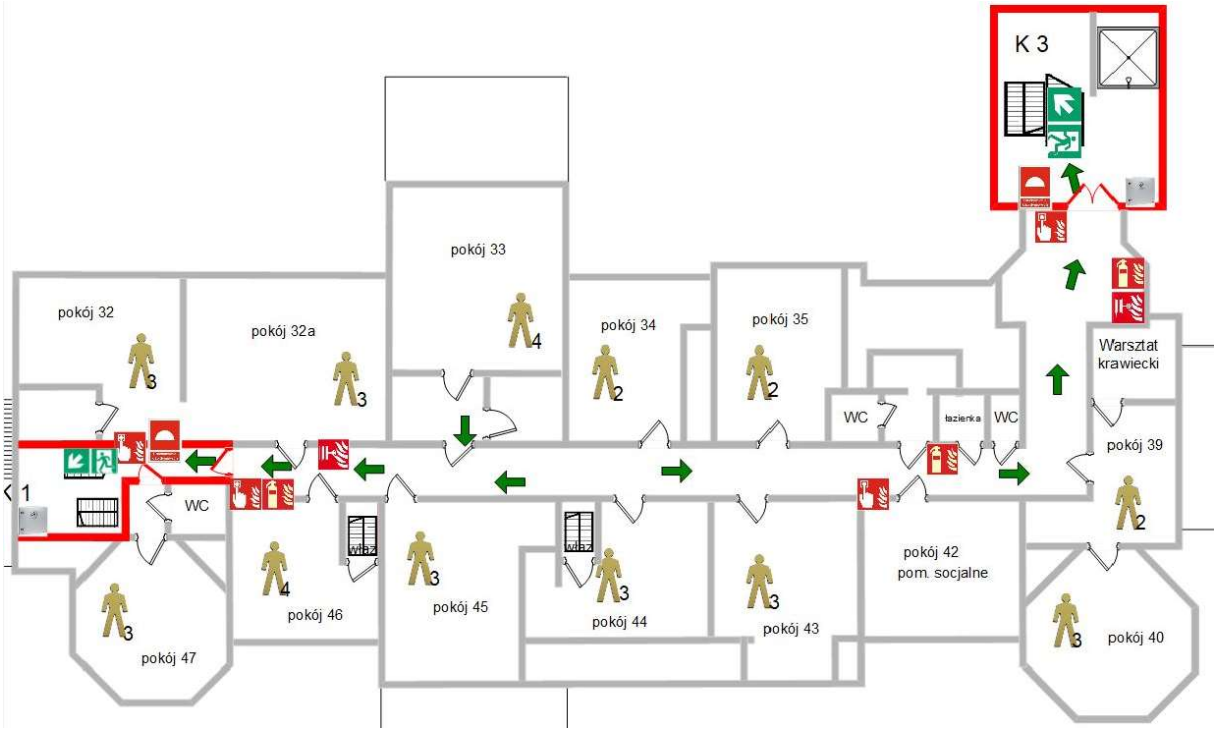
DPS Cetuń jest to pałac objęty ochroną konserwatorską. Na całość składa się pięć kondygnacji użytkowych. Dodatkowo pensjonariusze poruszają się po obszarze zewnętrznym, który również został uwzględniony w audycie.

Plany kondygnacji

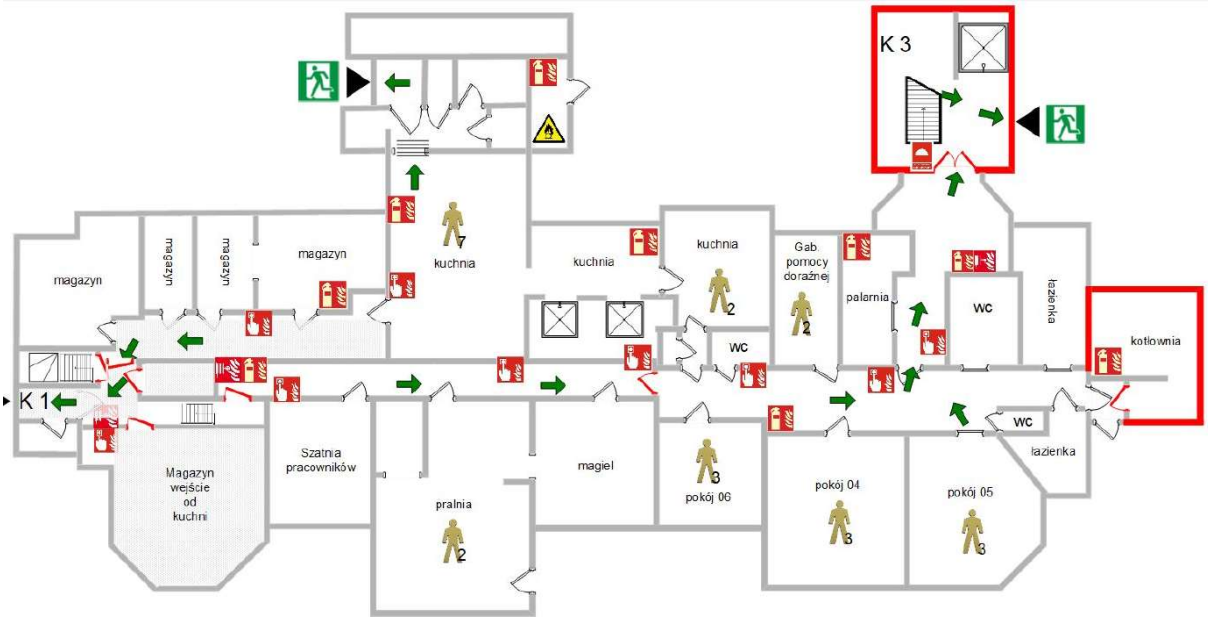
Rysunek 1: Plan parteru



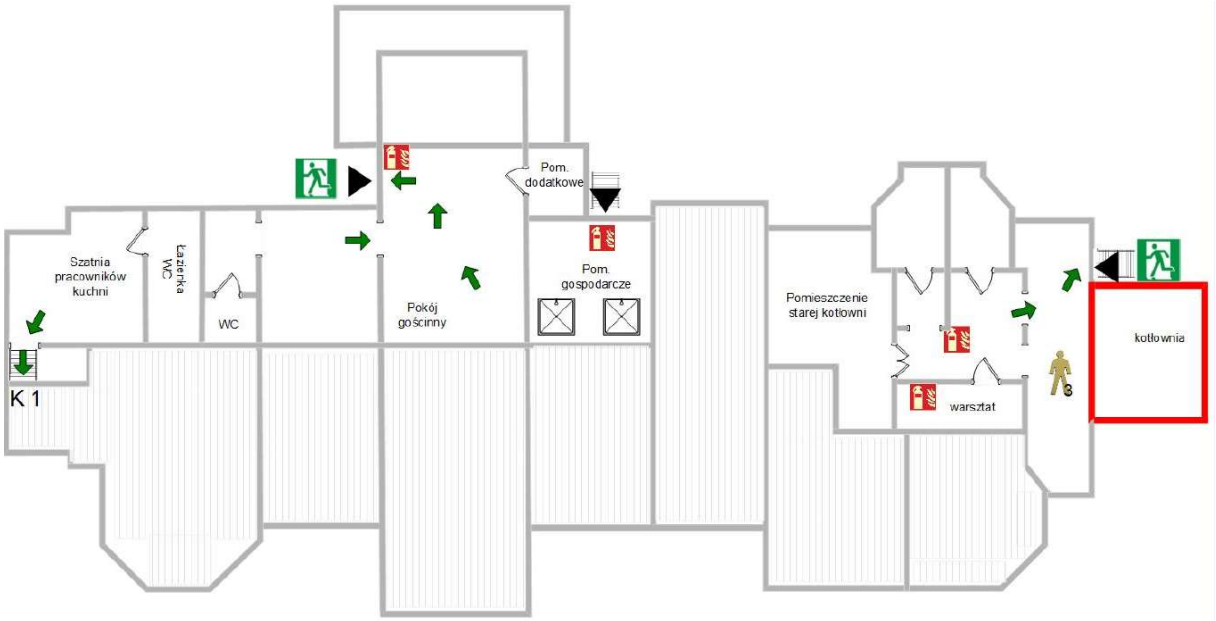
Rysunek 2: Plan pierwszego piętra



Rysunek 3: Plan drugiego pietra



Rysunek 4: Plan niskiego parteru



Rysunek 5: Plan piwnicy

Obecny stań sieci

W obecnej chwili w Cetuniu jest rozprowadzona sieć LAN oraz WLAN, ale tylko w obrębie pomieszczeń administracyjnych. Należy również zaznaczyć, że sieć nie jest doprowadzona do wszystkich pracowników. Brak jakiejkolwiek infrastruktury sieciowej, z której mogliby skorzystać mieszkańcy. Internet doprowadzony jest satelitarnie, a urządzenia z jakich korzystają pracownicy są rozwiązaniami domowymi takimi jak małe niezarządzalne switche, wbudowane access pointy w routery. Dodatkowo wiek oraz brak gwarancji producenta tych urządzeń również nie gwarantuje stabilności oraz poprawności ich działania. W budynku nie ma wyznaczonych punktów dystrybucyjnych, czy głównej serwerowni, brak infrastruktury ethernetowej oraz światłowodowej. Jedyna istniejąca infrastruktura jest to monitoring, który jest odrębny i nie podlegał audytowi. Ze względu na przyszłe prace i chęć wprowadzenia zaawansowanego systemu sieci bezprzewodowej niezbędne będzie wybudowanie całkowicie nowej infrastruktury sieci LAN. Żadne z obecnie używanych urządzeń nie będzie się nadawać do przyszłego wykorzystania.

Rysunek 6: Szafa od monitoringu na poziomie niskiego parteru

Rysunek 7: Miejsce instalacji kamery do monitoringu

Rysunek 8: Miejsce instalacji kamery do monitoringu

Uwagę należy zwrócić na to, że kamery zostały rozmieszczone na terenie całego obiektu oraz wydana została zgoda konserwatorska na przeprowadzenie prac w tym zakresie. Jest to ważne dla przyszłych uzgodnień projektowych.

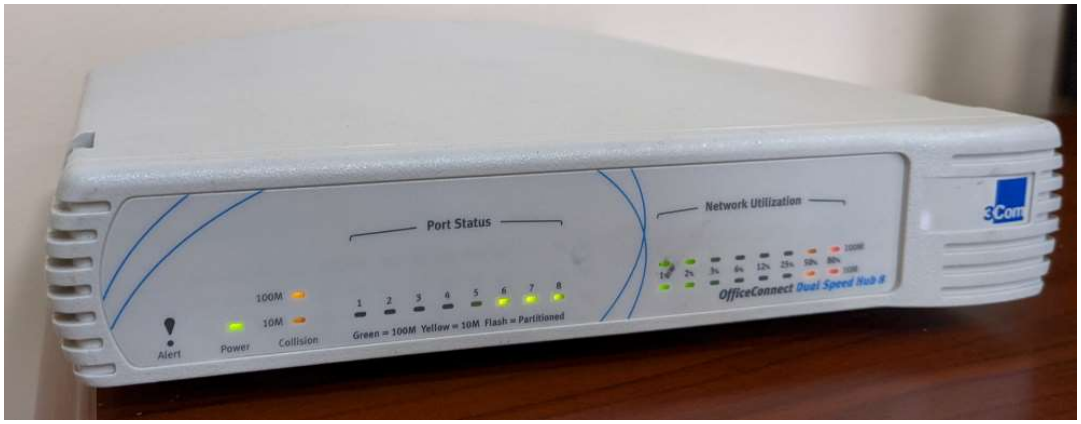
Rysunek 9: Miejsce instalacji anteny satelitarnej na tarasie na pierwszym piętrze

Obecnie zainstalowane urządzenia

Rysunek 10: Modem satelitarny TOOWAY doprowadzający Internet dla administracji

Rysunek 11: Niezarządzalny switch w biurze

Rysunek 12: Router w biurze



Rysunek 13: Niezarządzalny switch w biurze

Powyżej zostały przedstawione obecnie wykorzystywane urządzenia, które nie są rozwiązaniami profesjonalnymi.

Rysunek 14: Serwer w biurze administracji

Ze względu na brak serwerowni serwer zamknięty jest w kredensie w pokoju Dyrektor.

Stan istniejącej sieci WLAN

W obecnej chwili jest propagowana lokalnie sieć bezprzewodowa obsługująca pojedyncze pokoje administracji.

AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
DIRECT-Vw pass-PHILIPS TV	#6		local:2e:d0:5a:0f:cf:70	1	144	WPA2	n	11	11	11	0	1
kuchnia	#2		EdimaxTech:b9:1c:22	11	54	WPA2	g	24	35	4	0	12
linksys	#4		TpLinkTech:d9:e7:66	1	450	WPA2	n	15	18	11	0	5
linksys3	#5		TpLinkTech:d9:ec:e8	11	217	WPA2	n	6	6	6	0	1

Rysunek 15: Lista widocznych sieci

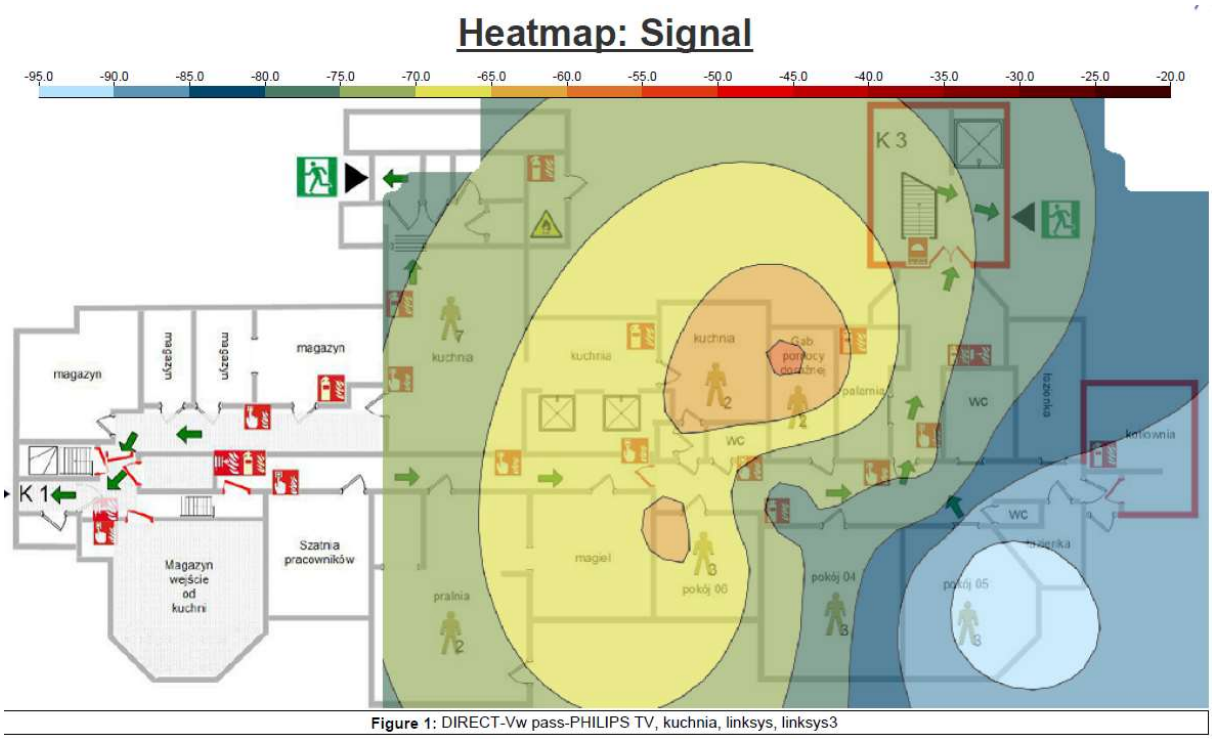
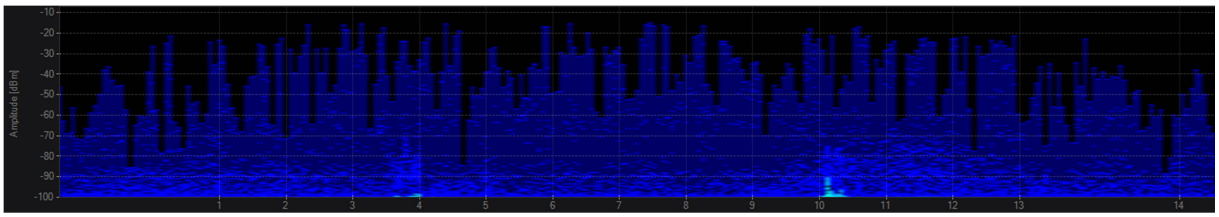


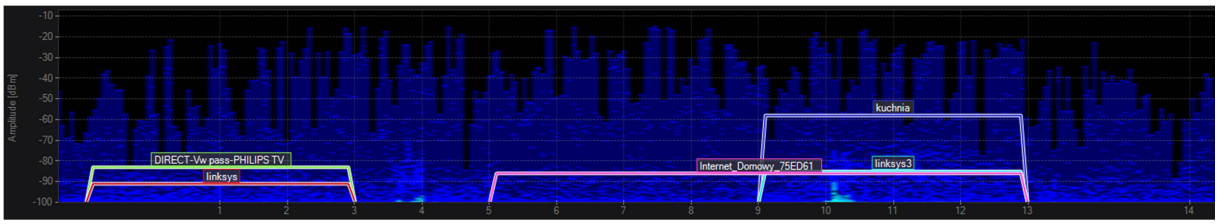
Figure 1: DIRECT-Vw pass-PHILIPS TV, kuchnia, linksys, linksys3

Rysunek 16: Widok sieci z poziomu niskiego parteru

Mały router bezprzewodowy jest umieszczony w pokoju biurowym obok kuchni.



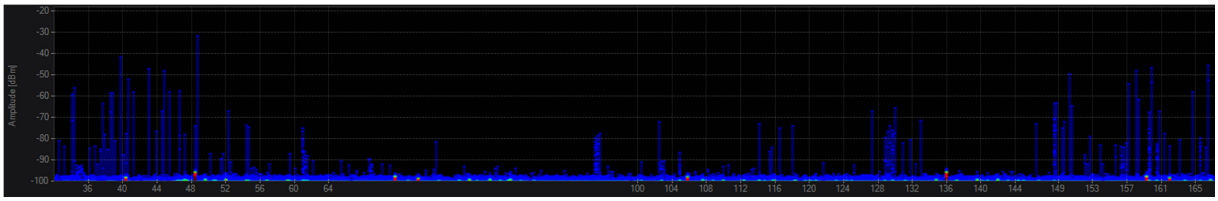
Rysunek 17: Pomiar widma w paśmie 2,4GHz na niskim parterze



Rysunek 18: Pomiar widma w paśmie 2,4GHz na niskim parterze z zaznaczonymi widocznymi sieciami

ESSID	AP Alias	Channels	Signal Strength (dBm)	BSSID Count	Security	Max Rate (Mbps)	Vendors	802.11
linksys		1	-91	1	WPA2-Personal	216,7	Tp-Link Technologies Co.,Ltd.	b, g, n
TP-Link_ECE7_5G		42 [36]	-86	1	WPA2-Personal	1300,0	Tp-Link Technologies Co.,Ltd.	n, ac
Internet_Domowy_75ED61		11-7	-86	1	WPA2-Personal	300,0	Asiatelco Technologies Co.	b, g, n
linksys3		11	-85	1	WPA2-Personal	216,7	Tp-Link Technologies Co.,Ltd.	b, g, n
DIRECT-Vw pass-PHILIPS TV		1	-83	1	WPA2-Personal	144,4		g, n
kuchnia		11	-58	1	WPA2-Personal	54,0	Edimax Technology Co. Ltd.	b, g

Rysunek 19: Lista widocznych sieci

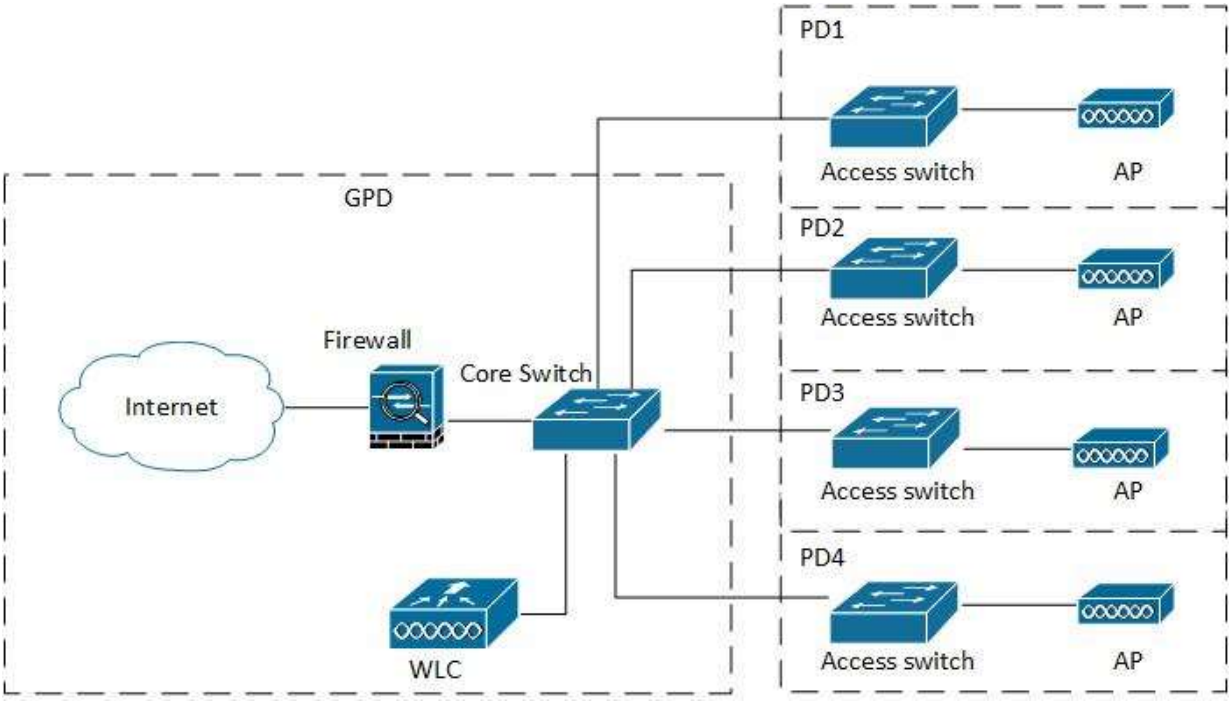


Rysunek 20: Pomiar widma w pasmie 5GHz

Jak widać na powyższych obrazkach jedynie co można zaobserwować do sygnały pochodzące z obecnie propagowanych sieci. Nie występują zakłócenia w tym paśmie. Dla 5GHz można na poziomie szumów zobaczyć małe czerwone zakłócenia, które nie mają żadnego wpływu na sieć bezprzewodową, najprawdopodobniej pochodzą one od operatora telekomunikacyjnego.

Koncepcja nowej sieci LAN

Nowa sieć LAN powinna zostać wykonana z założeniem, że w obecnej chwili w Cetuniu nie ma żadnej infrastruktury. Należy wybrać miejsca, gdzie będzie możliwe zrobienie nowej serwerowni oraz punkty pośrednie dystrybucyjne. Należy rozprowadzić nowe połączenia światłowodowe pomiędzy wszystkimi punktami pośrednimi a główną serwerownią. Na styku nowej sieci LAN z Internetem powinno znaleźć się urządzenie zabezpieczające sieć wewnętrzną – firewall. W każdym punkcie dystrybucyjnym należy umieścić przełącznik dostępowy co najmniej 24 portowy PoE/PoE+, tak aby podłączyć wszystkie access pointy. Każdy z punktów następnie zostanie podłączony do switcha corowego w głównej serwerowni. Należy przyjąć architekturę gwiazdy, w której każdy pośredni punkt dystrybuujmy będzie bezpośrednio podłączony do GPD. W głównej serwerowni będzie również zainstalowany kontroler sieci bezprzewodowej.



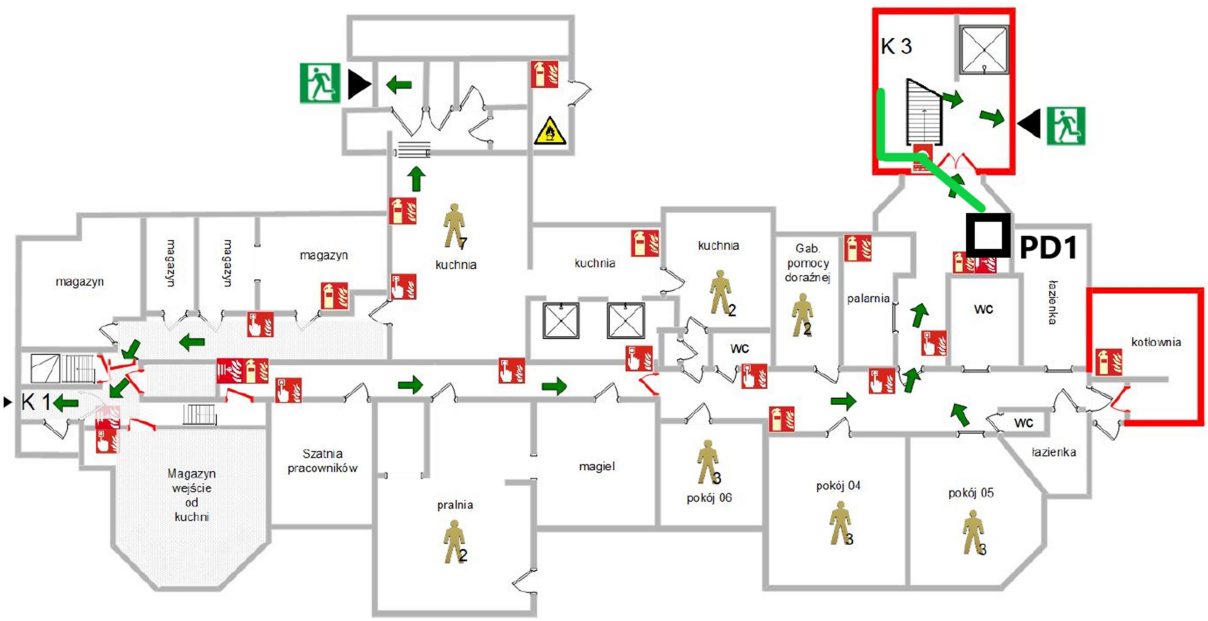
Rysunek 21: Schemat nowej sieci

Punkty dystrybucyjne

Poniżej przedstawione zostały miejsca instalacji głównej serwerowni, punktów dystrybucyjnych oraz połączeń światłowodach. Na planach zaznaczone zostały jako zielone linie.

Niski Parter – PD1

Przewidziana została jedna szafa PD1. Trasa światłowodu do głównej serwerowni zostanie poprowadzana klatką schodową do pierwszego pietra, gdzie zejdzie się z resztą kabli do GPD.



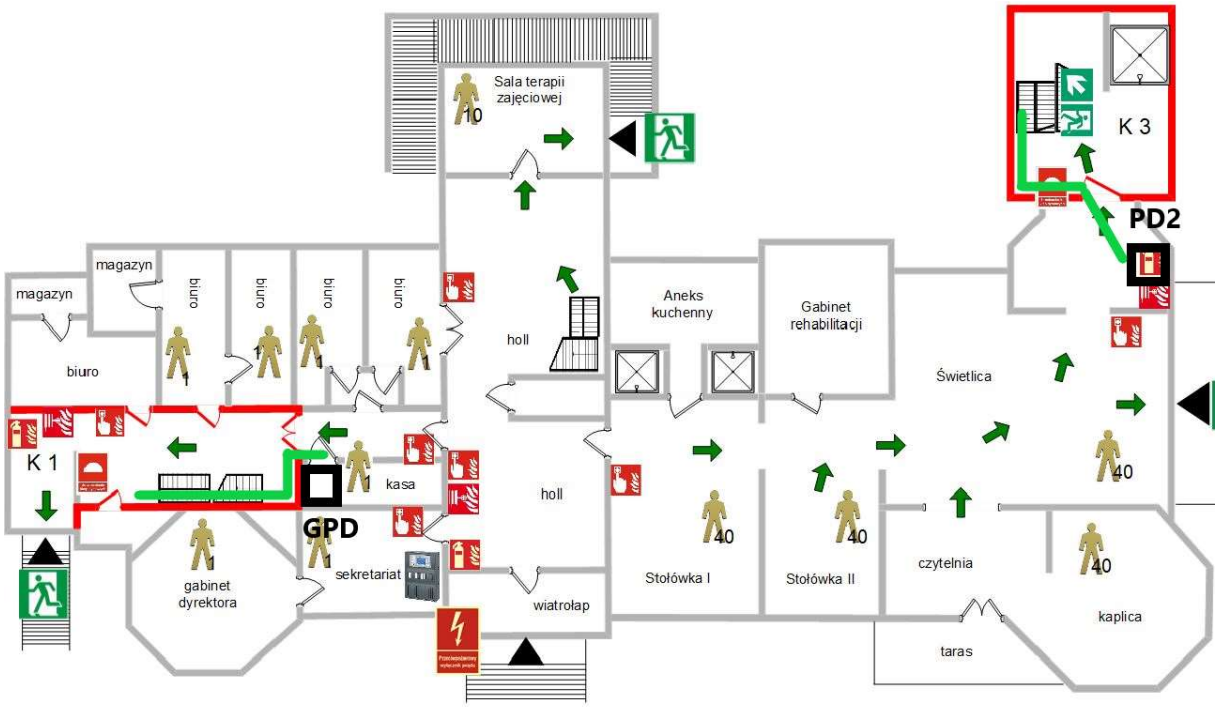
Rysunek 22: Koncepcja trasy światłowodu i instalacji szafy PD1

Parter – PD2, GPD

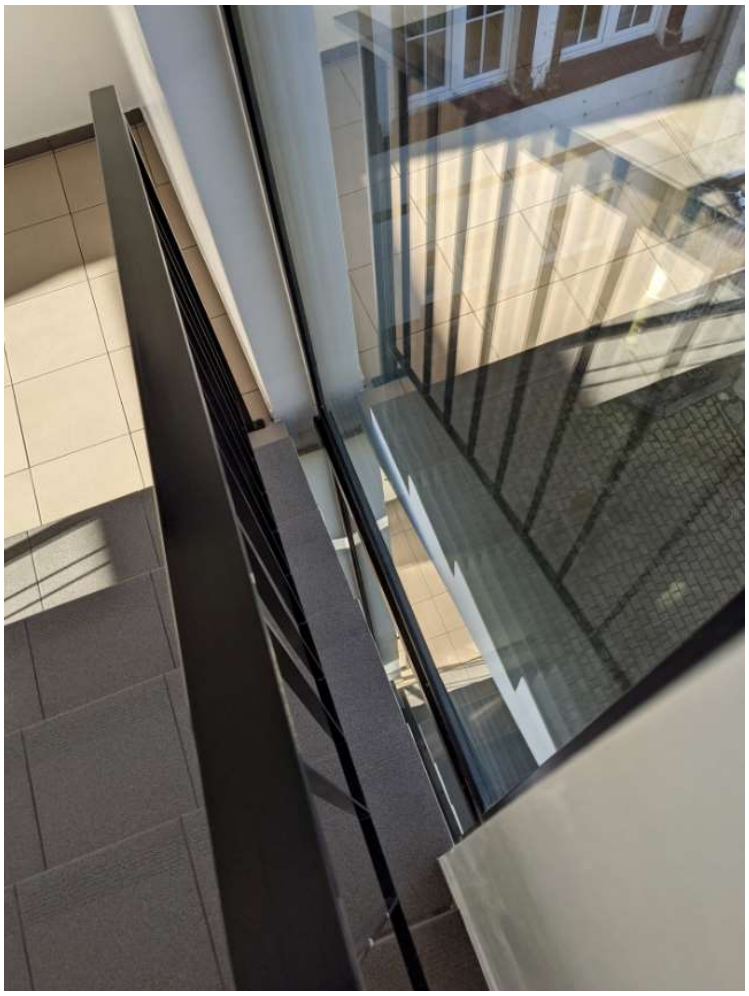
Na niskim parterze przewidziany został jeden punkt dystrybucyjny PD2 oraz GPD, główna serwerownia, w pomieszczeniu kasy. Połączenie światłowodowe z PD2 do GDP zostanie poprowadzone przez pierwsze piętro tak aby nie trzeba było przechodzić przez salon i jadalnie, gdzie są zabytkowe malowidła na ścianach. Nowa klatka schodowa ma przebicie przez wszystkie piętra, także można ją wykorzystać jako dobą trasę kablową łączącą wszystkie piętra.

Rysunek 23: Miejsce instalacji szafy GDP

Ze względu na to, że w pałacu jest brak wolnych pomieszczeń, które mogły by zostać przeznaczone na nową serwerownię sugerowane jest wykorzystanie pomieszczenia kasy. Jest to pomieszczenie na parterze, pomiędzy biurami administracji, z dobrym dostępem do korytarza, którym będzie poprowadzone przewody.



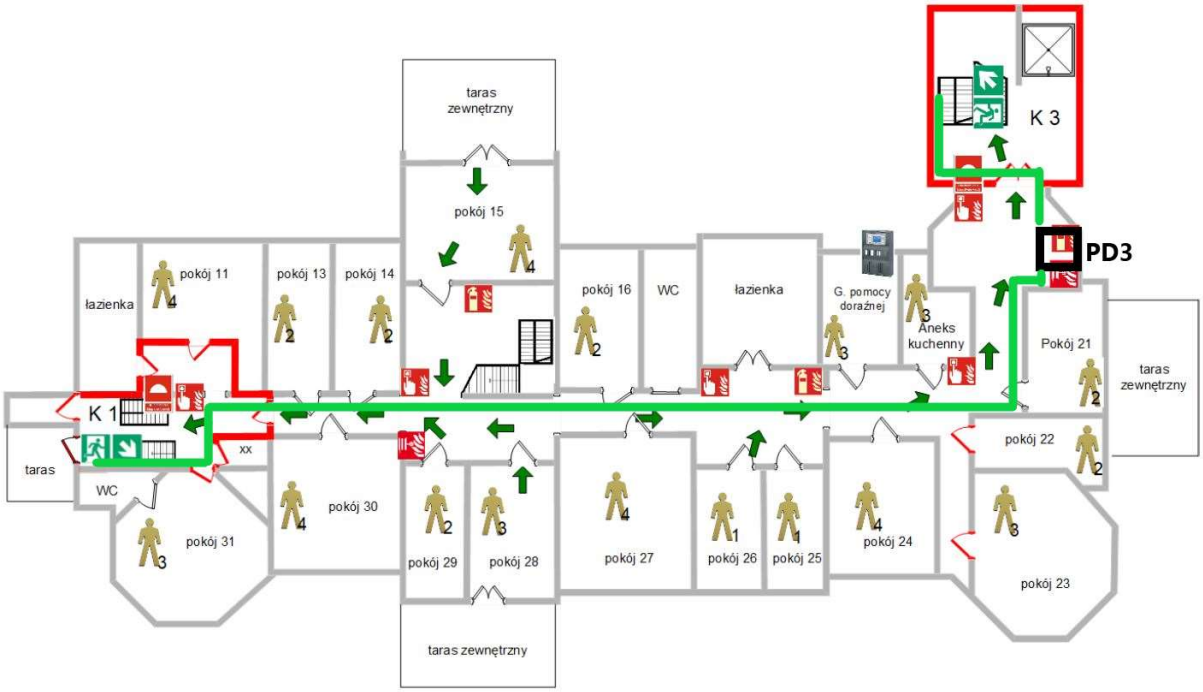
Rysunek 24: Koncepcja trasy światłowodu i instalacji szafy GDP i PD1



Rysunek 25: Proponowane zejście ze światłowodem korytem przy oknie

Pierwsze piętro – PD3

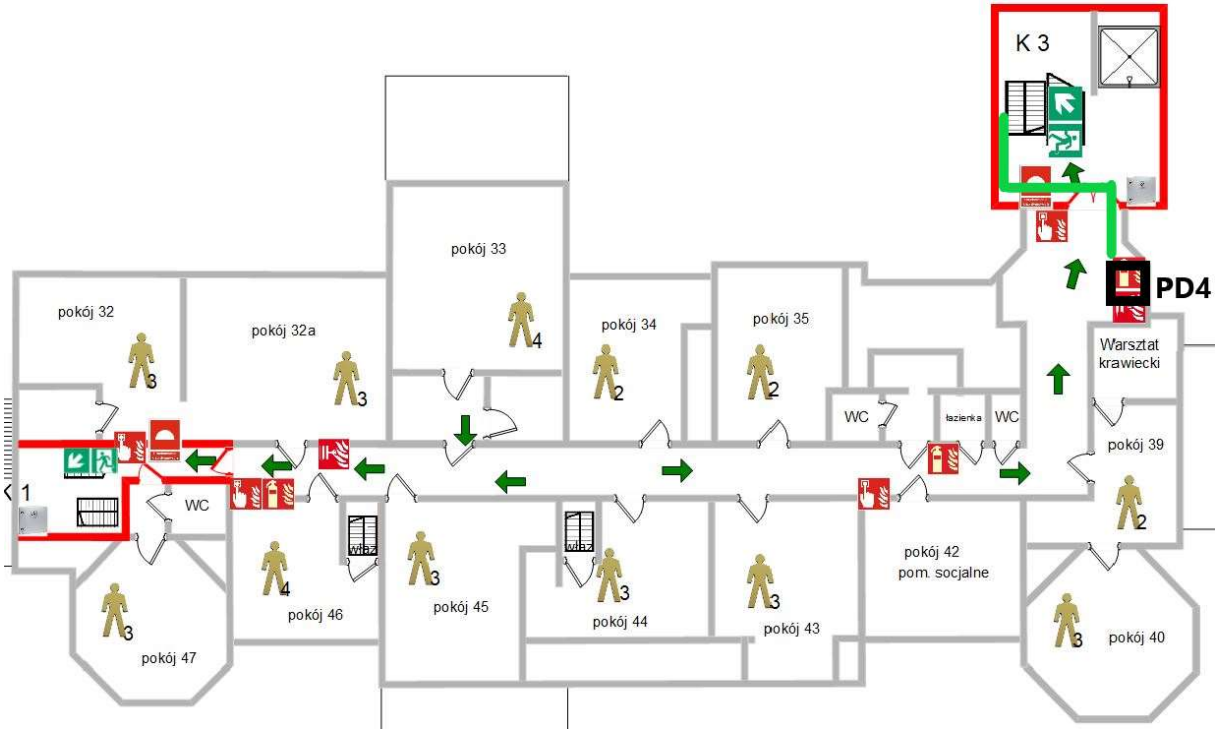
Na pierwszym piętrze przewidziany jest jeden punkt PD3 umiejscowiony w części nowej klatki schodowej. Ze wszystkich pięter zejdą się tu również światłowody i zostaną przeciągnięte do drugiej klatki schodowej, aby następnie zejść na parter i wejść do GPD.



Rysunek 26: Koncepcja trasy światłowodu i instalacji szafy PD3

Drugie piętro – PD4

Na drugim piętrze szafka PD4 tak samo jak na pozostałych zostatała zaproponowana w części nowej klatki schodowej. Światłowód zejdzie na pierwsze piętro po ścianie klatki przy oknie.



Rysunek 27: Koncepcja trasy światłowodu i instalacji szafy PD4

Rysunek 28: Zejście światłowodu z drugiego piętra

Rysunek 29: Zejście światłowodu z drugiego piętra

Informacje dodatkowe

Montaż szaf rakowych w wybranych punktach:

- w poszczególnych PD, które mają zostać zainstalowane na korytarzu – kolor szafy biały lub jasno szary, tak aby wkomponować się w kolor ścian,
- zalecane jest, aby szafa miała jak najmniejszy rozmiar, który umożliwi zainstalowanie w niej sprzętów, przewidywany rozmiar dla każdego piętra 6U-9U,
- w GPD w pomieszczeniu kasy, nie ma wymogu kolorystycznego,

Rysunek 30: Planowane miejsce instalacji szafy PD

Przykładowe miejsce instalacji nowej szafy na niskim parterze, analogiczne na pozostałych piętrach szafy powinny zostać zainstalowane w tych samych miejscach.

Prowadzenie kabli światłowodowych

Z poszczególnych PD rozmieszczonych na każdym piętrze, wyjście nową klatka schodową i przejście nową trasą kablową po pierwszym piętrze do starej klatki schodowej, a następnie zejście do parteru i przejście przez ścianę do pomieszczenia kasy wraz z uwzględnieniem ominięcia szybów kominowych. Nowe kable światłowodowe mają być umieszczone na całej długości w korytkach kablowych o najmniejszym przekroju. Koryta mają zostać dołożone pod istniejącymi już instalacjami, tak aby stworzyć spójną całość. Muszą iść w rogach ścian, wzdłuż korytarzy, tam, gdzie będzie to konieczne mają zostać pomalowane w odpowiednim kolorze. Okablowanie światłowodowe ze wszystkich PD umieszczonych obok nowej klatki schodowej zostanie sprowadzone na pierwsze piętro, a następie

przeprowadzone korytami do drugiej klatki schodowej skąd wejdzie do pomieszczenia kasy do głównej serwerowni.

Rysunek 31: Przykładowe poprowadzenie tras kablowych w korytach

Prowadzenie kabli ethernetowych:

- Kable ethernetowe muszą być prowadzone w korytach kablowych dołożonych do istniejącej infrastruktury,
- Koryta muszą być zamaskowane kolorem, jeżeli będzie taka potrzeba,
- Instalacja access pointów będzie pod sufitem czy to w pokoju, czy na korytarzu.

Koryta kablowe nowe powinny stykać się ze starymi, tak aby zajmować jak najmniej miejsca:

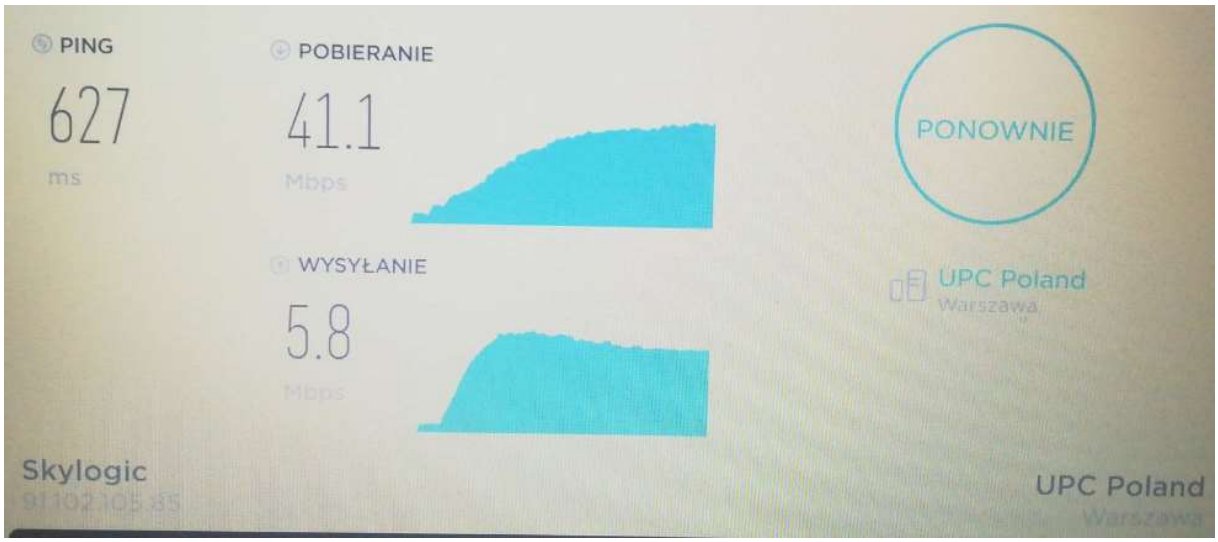
Rysunek 32: Przykładowe poporwadzenia tras kablowych w korytach

Koryta powinny iść zawsze na styku ściany i sufitu, tak aby nie dopuścić do sytuacji, że pojawi się nowa listwa na środku sufitu

Przepusty przez ściany również powinny być w miejscach, gdzie są obecnie, jeżeli nie ma to powinny zostać zrobione tak aby były jak najmniej widoczne.

Analiza możliwości przyłączenia do zewnętrznej szerokopasmowej sieci internetowej

W obecnej chwili łącze internetowe jest doprowadzone satelitarnie.



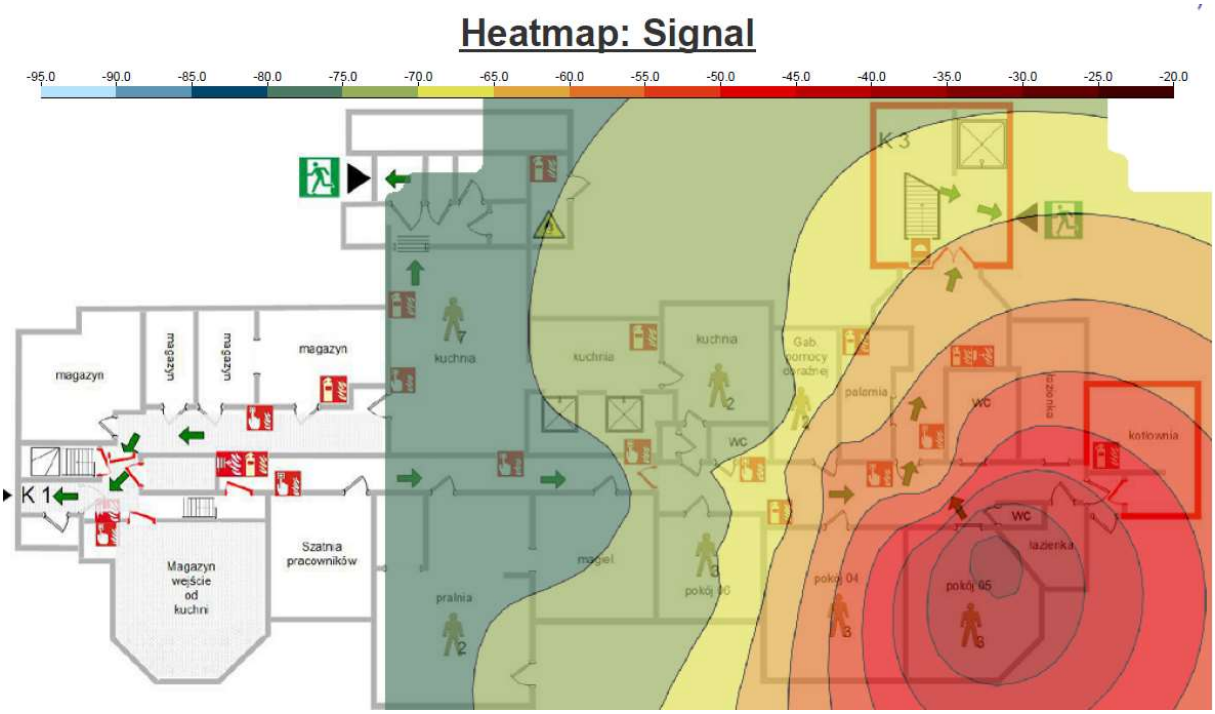
Rysunek 33: Test prędkości wykonany z komputera podłączonego do obecnej sieci LAN

Ze względu na lokalizację w Cetuniu w obecnej chwili nie ma możliwości innego podłączenia Internetu. Nie ma w okolicy łącz światłowodowych, Orange jest jedynie w stanie zapewnić Internet mobilny. Dla przyszłego rozwiązania dobrze byłoby, aby operator mógł nadać dla DPC Cetuń stałą adresację publiczną. Patrząc na obecne osiągi łącz internetowych przeprowadzanie jakichkolwiek wideokonferencji będzie niemożliwe. Dla audio i video opóźnienie na łączu powinno nie przekraczać 20 ms.

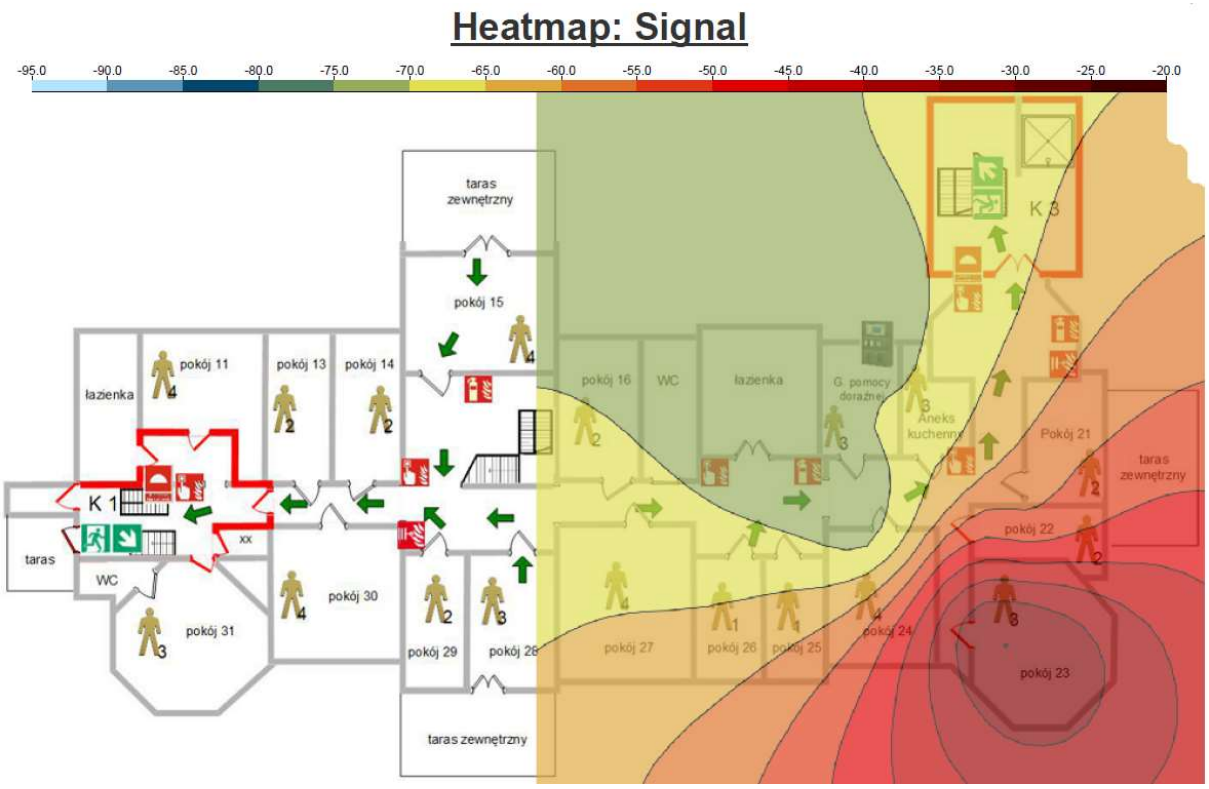
Koncepcja rozmieszczenia nowych punktów dostępowych wraz z doporowadzeniem tras kablowych oraz protokół pomiarowy stanowiący podstawę do opracowania dokumentacji

Poniżej przedstawione zostały miejsca instalacji nowych access pointów wraz z planowanym zasięgiem. Cały obszar budynkowy powinien zostać objęty sygnałem radiowym a część zewnętrzna tylko we wskazanych miejscach. Sygnałem radiowym mają zostać objęte wszystkie kondygnacje. W częściach biurowych i magazynowych ma być dostępna sieć bezprzewodowa, z której mogą korzystać pracownicy DPS-u. W częściach mieszkalnych ma być zapewniona triangulacja urządzeń co pozwoli na uruchomienie systemu lokalizacji pacjentów. Wszystkie miejsca instalacji zostały uzgodnione z konserwatorem zabytków.

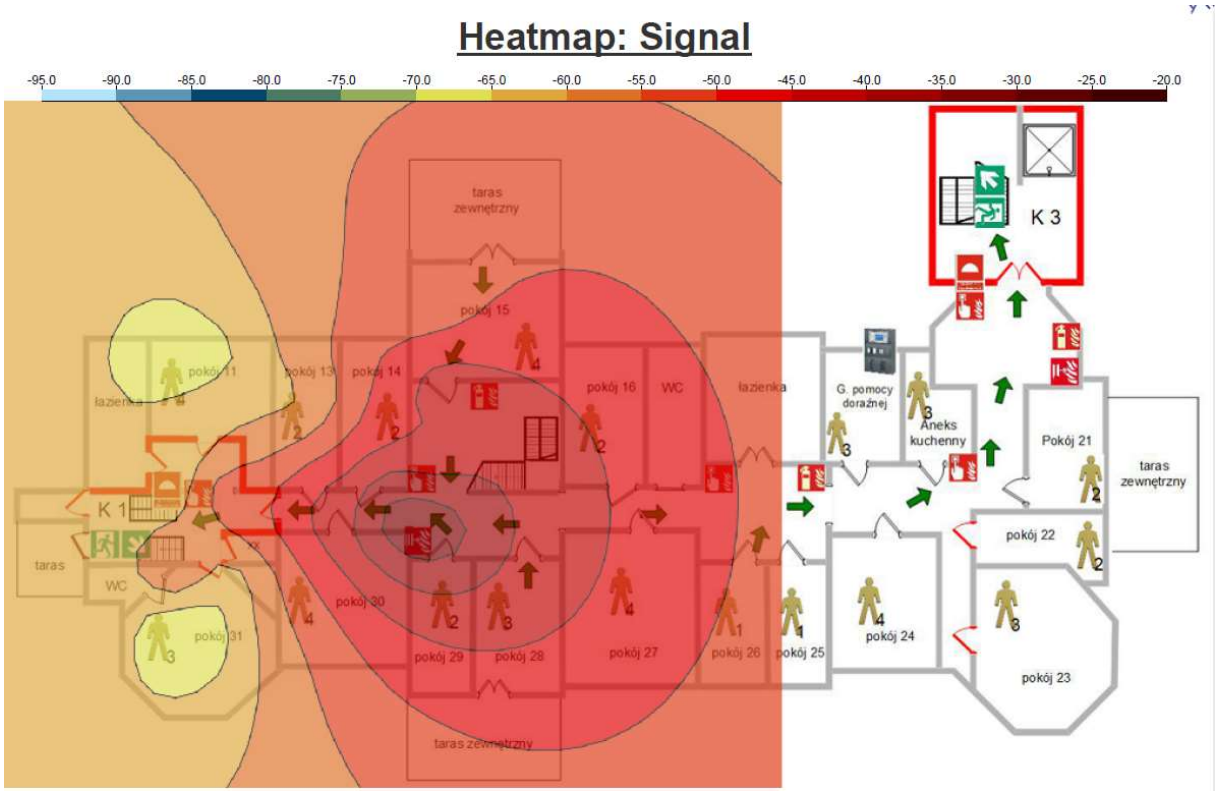
Wykonane zostały badania tłumienia ścian, które pozwoliło na późniejsze przygotowanie rozmieszczenia access pointów na terenie całego DPS-u.



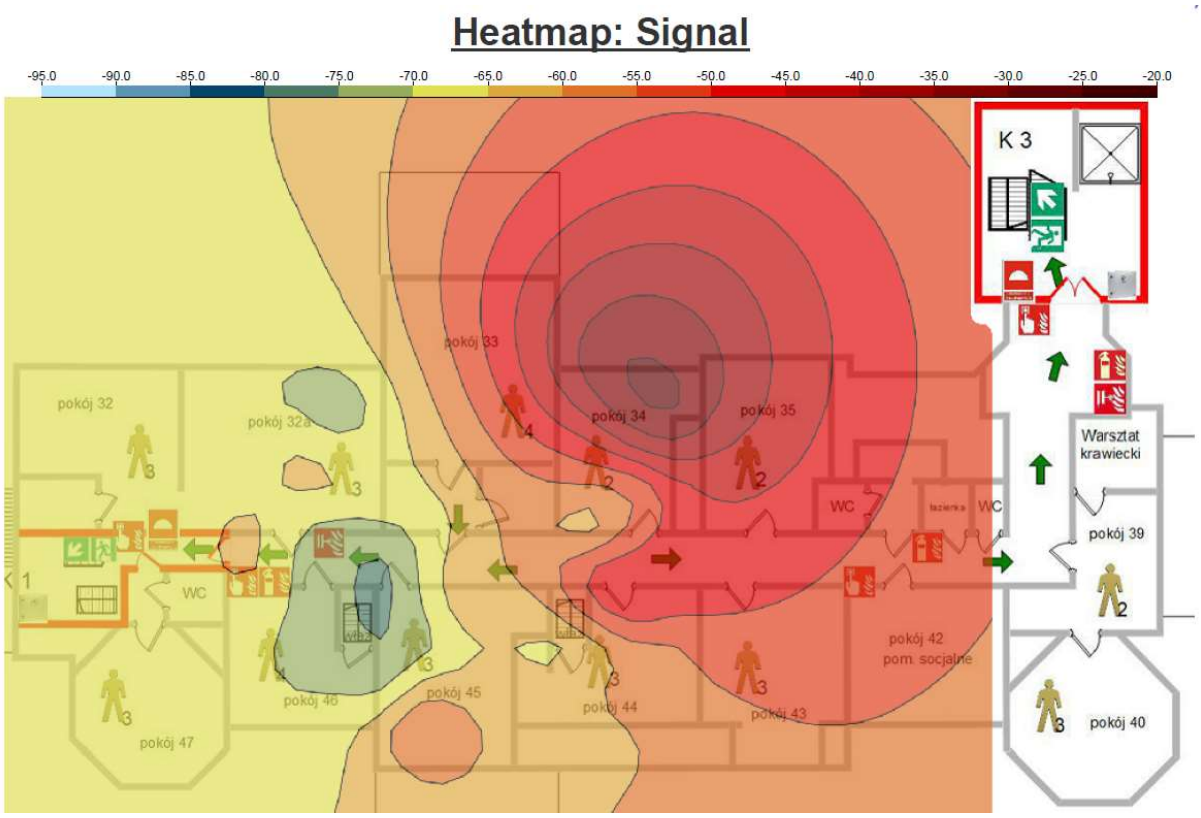
Rysunek 34: Badanie przeprowadzone na niskim parterze, w którym access point był umieszczony w pokoju narożnym.



Rysunek 35: Badanie na pierwszym piętrze, w którym access point był umieszczony w pokoju narożnym



Rysunek 36: Badanie na pierwszym piętrze, w którym access point był umieszczony na korytarzu

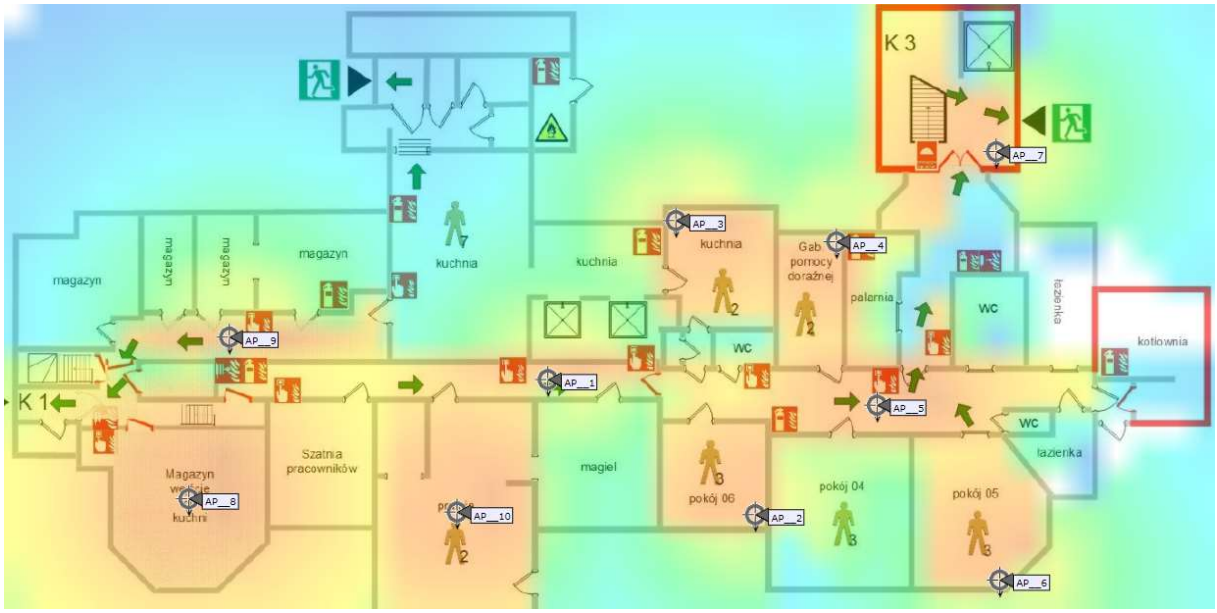


Rysunek 37: Badanie przeprowadzone na drugim piętrze, w którym access point był umieszczony w pokoju mieszkalnym

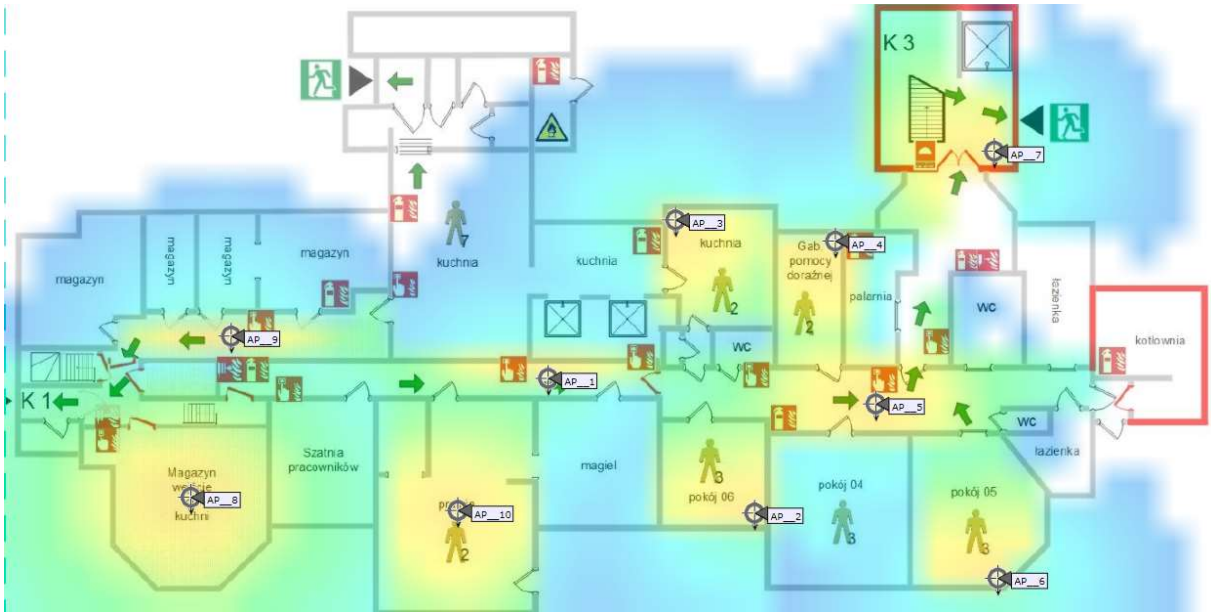
Jak można zaobserwować spadek sygnału radiowego przechodzącego przez ściany pałacu jest znaczny. Przy access pointach umieszczonych w pokojach poziom sygnału na korytarzu w niektórych przypadkach spadł o 15 dBm. Ściany w pałacu w Cetuniu mają różną grubość w zależności od poziomu, na niskim parterze i na parterze mogą dochodzić nawet do 25 cm. Na wyższych piętrach pomiędzy pokojami grubość ścian jest mniejsza.

Planowanie radiowe

Niski Parter



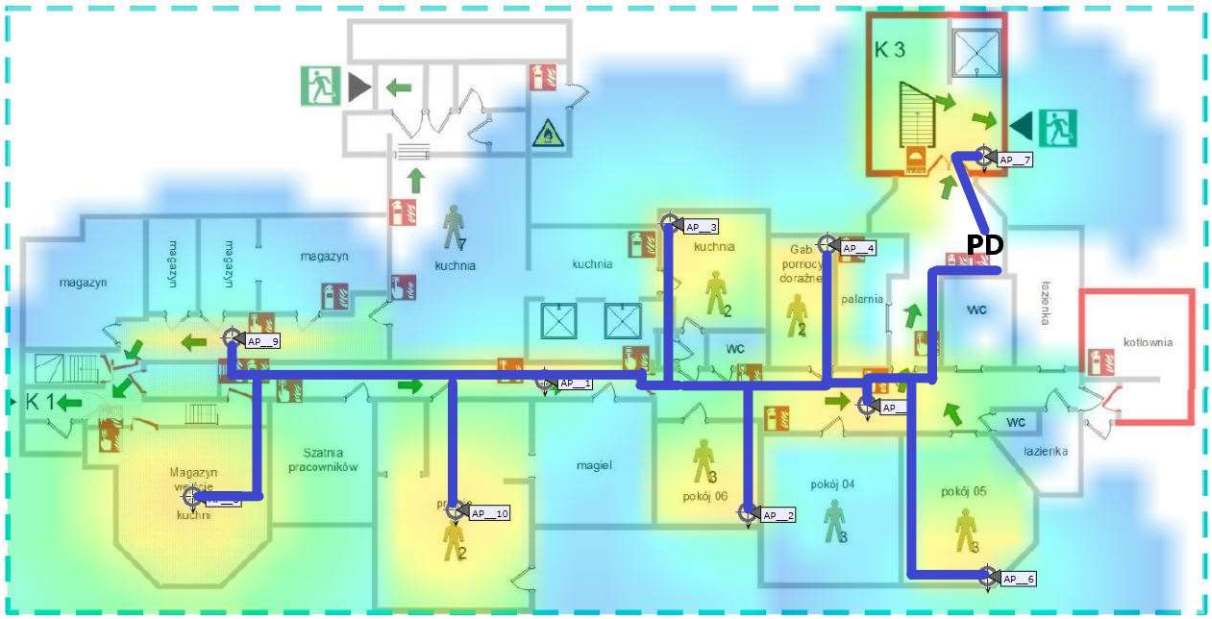
Rysunek 38: Planowanie dla częstotliwości 2,4GHz



Rysunek 39: Planowanie dla częstotliwości 5GHz

W obszarze niskiego parteru zostało zaproponowanych dziesięć access pointów. Okablowanie z całej kondygnacji zejdzie się do szafki PD1 w korytach kablowych wzdłuż korytarza.

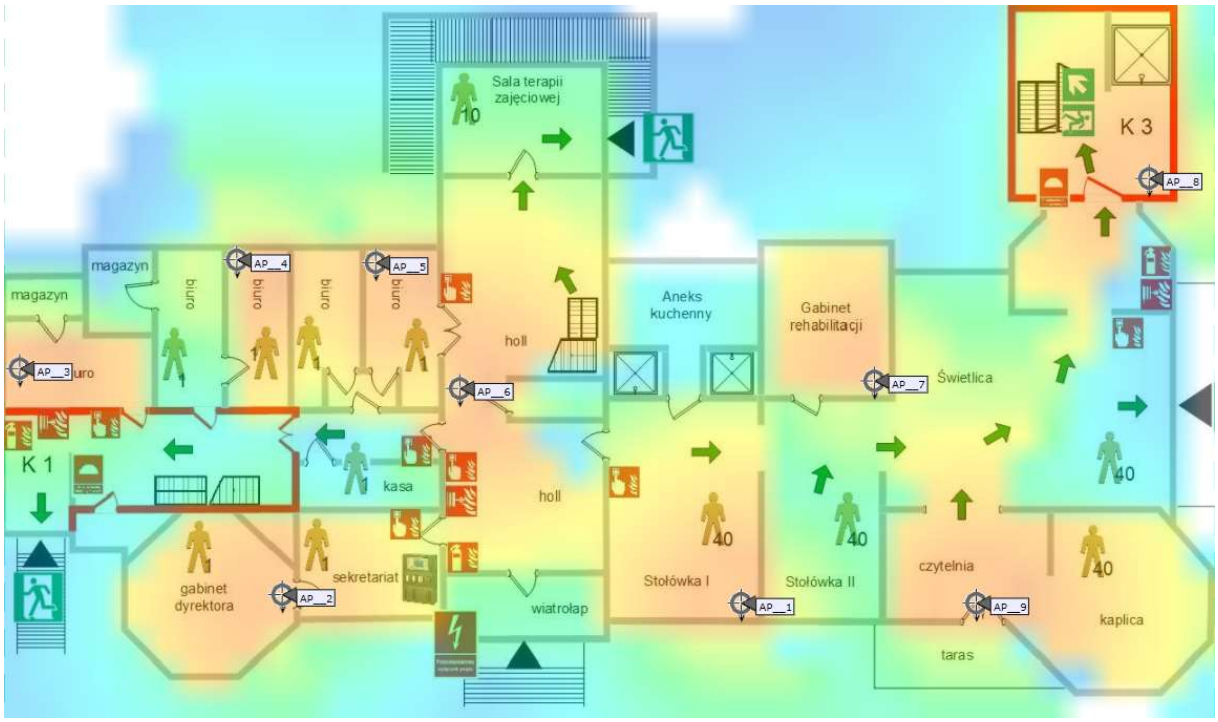
Trasy kablowe



Rysunek 40: Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	40
AP2	35
AP3	35
AP4	35
AP5	25
AP6	35
AP7	10
AP8	60
AP9	60
AP10	55

Parter

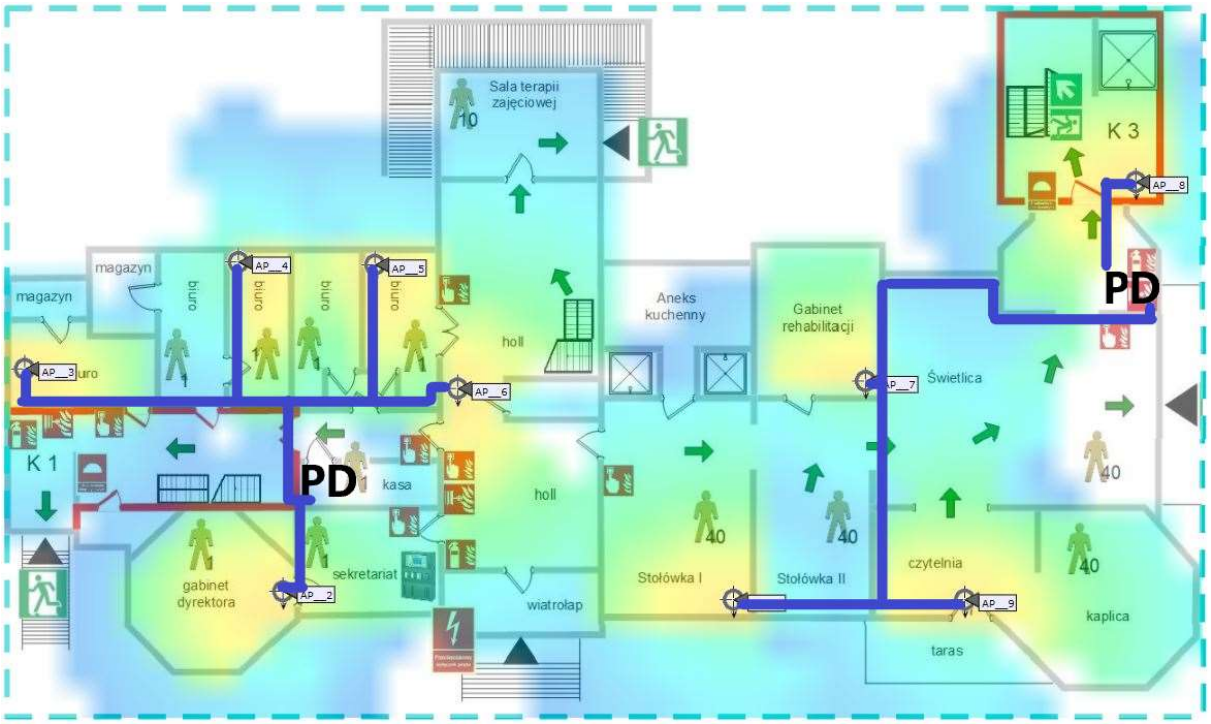


Rysunek 41: Planowanie dla częstotliwości 2,4GHz

Rysunek 42: Planowanie dla częstotliwości 5GHz

Na parterze zaproponowanych zostało dziewięć access pointów. Okablowanie z części biurowej + z holu głównego zejdzie się do GPD w kasie. Z prawej części parterowej pałacu proponujemy zejście do PD2. Ze względu, że stołówka, jak i świetlica, są to obszary odnowione zgodnie w wymaganiami konserwatora zalecane jest prowadzenie okablowania za gzymsami tak jak na zdjęciu poniżej. Wszystkie dokładne opisy tras kablowych zawarte są w dokumencie zaleceń konserwatorskich.

Trasy kablowe



Rysunek 43: Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	50
AP2	15
AP3	35
AP4	25
AP5	25
AP6	25
AP7	35
AP8	10
AP9	50

Na parterze okablowanie po lewej stronie pałacu zejdzie się PD w pomieszczeniu kasy. Okablowanie musi iść pokojami, a nie korytarzem, tak jak zostało to zaznaczone na rysunku powyżej. Wybrane miejsca pod access pointy znajdujące się w stołówce, gabinecie rehabilitacji oraz czytelni na etapie projektu muszą zostać poddane badaniom konserwatorskim polichromii w celu ostatecznego ustalenia, czy ich instalacje będzie możliwa. Z tych miejsc okablowanie przechodząc przez świetlice musi zostać umieszczone na gzymsie i tak ukryte, aby nie było widać przewierceń przez ściany. Dla tych miejsc niezbędne będzie wystąpienie o badania konserwatorskie przed rozpoczęciem prac instalacyjno-projektowych.

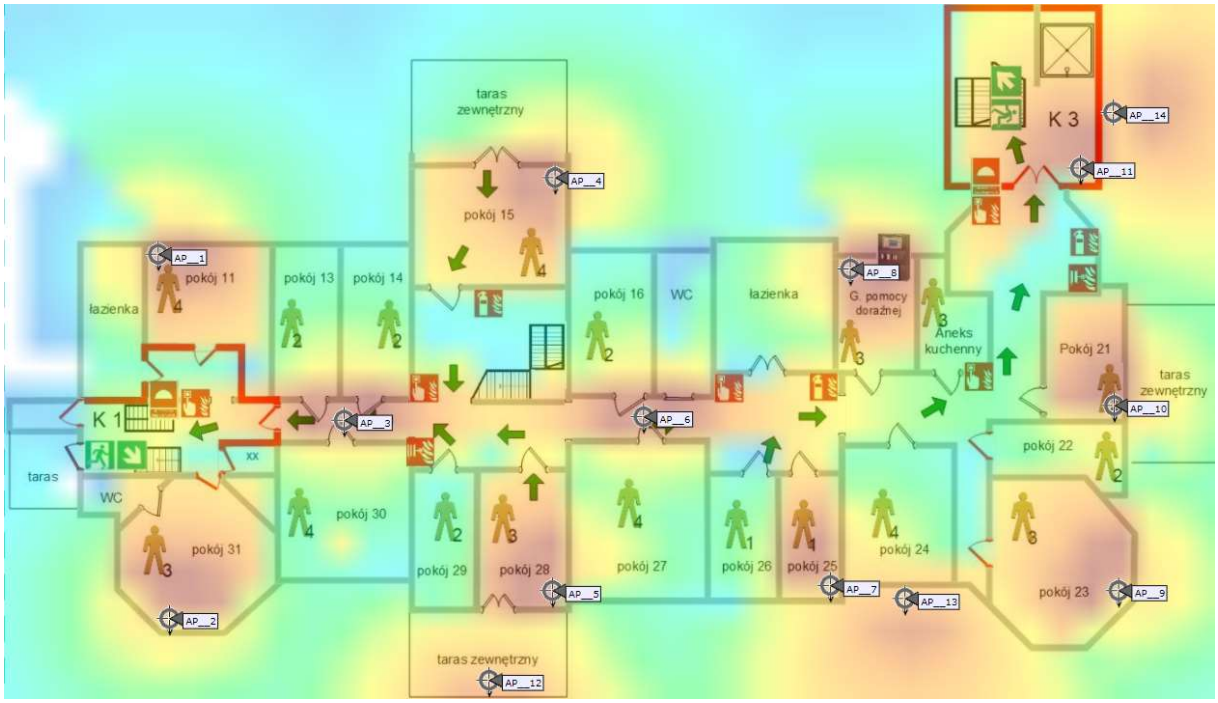
Rysunek 44: Wybrane miejsce instalacji access pointa w stołówce w rogu pomieszczenia

Rysunek 45: Wybrane miejsce instalacji access pointa w czytelni jak najbliżej ściany obok listwy

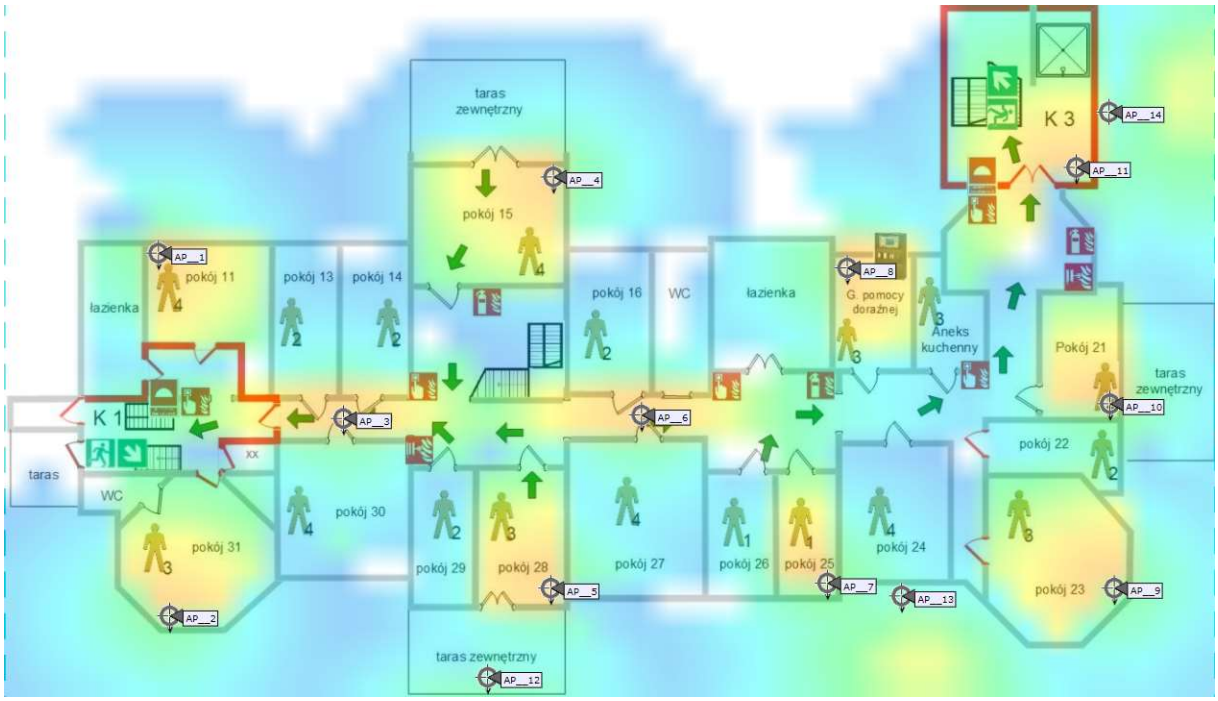
Rysunek 46: Koryto kablowe powinno przejść na styku ściany oraz sufitu

Rysunek 47: Gzyms na jakim musi zostać położone okablowanie

Pierwsze piętro + obszar zewnętrzny



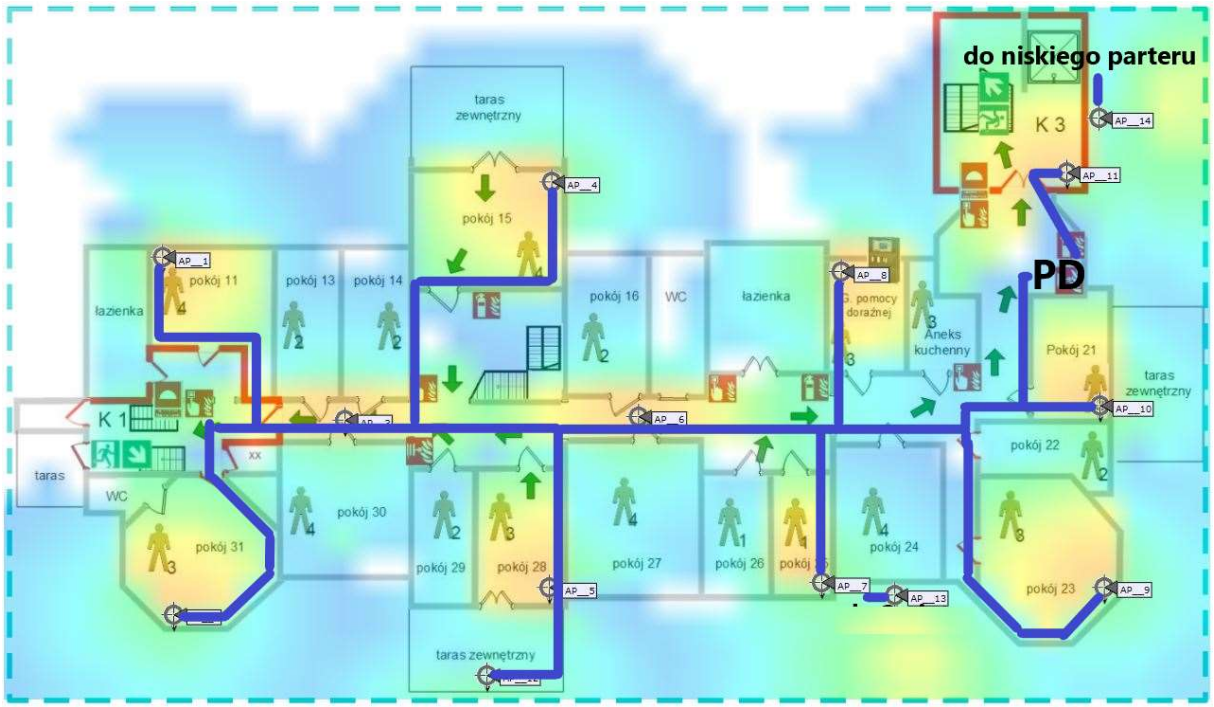
Rysunek 48: Planowanie dla częstotliwości 2,4GHz



Rysunek 49: Planowanie dla częstotliwości 5GHz

Na pierwszym piętrze zaproponowanych zostało jedenaście access pointów wewnętrznych oraz trzy zewnętrzne mocowane do elewacji (AP12, AP13 i AP14). Całe okablowanie na pierwszym piętrze zejdzie się wzdłuż korytarza do szafki PD3. Dodatkowo okablowanie światłowodowe z nowej klatki schodowej będzie puszczone nowym korytkiem wzdłuż korytarza do lewej klatki schodowej, aby dojść do GDP. Wszystkie dodatkowe ustalenia dotyczące rozmieszczenia znajdują się w części zaleceń konserwatorskich.

Trasy kablowe



Rysunek 50: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	85
AP2	85
AP3	75
AP4	75
AP5	70
AP6	50
AP7	45
AP8	35
AP9	35
AP10	20
AP11	10
AP12	85
AP13	50
AP14	25

Rysunek 51: Na pierwszym piętrze okablowanie powinno iść w korytach stykających się z istniejącą infrastrukturą

Access pointy zewnętrzne

Rysunek 52: Urządzenie powinno zostać umieszczone obok lampy ewakuacyjnej, okablowanie do PD na niskim parterze.

Access pointy na elewacji frontowej

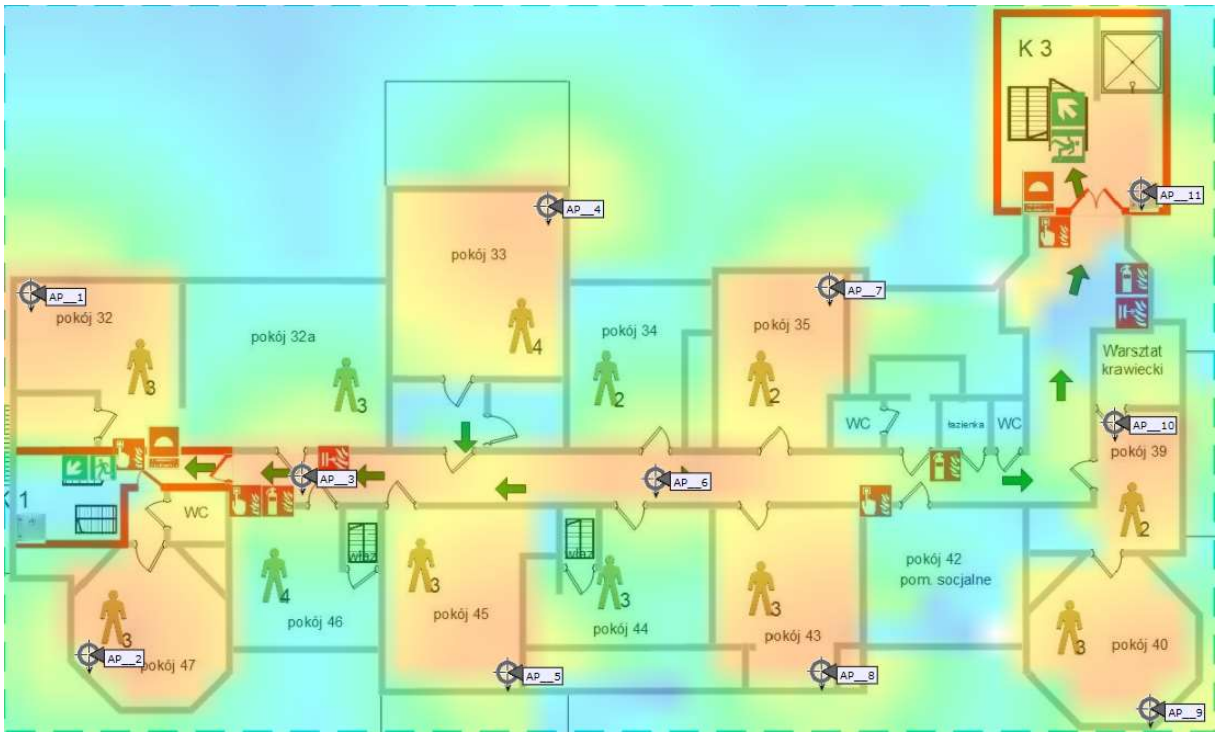
Rysunek 53: Miejsce instalacji access pointa

Na środku pod gzymsem, zlicowane ze ścianą, okablowanie przebije się z tarasu bezpośrednio do urządzenia, powinno zostać pomalowane w kolorze zgodnym z zaleceniami konserwatorskimi.

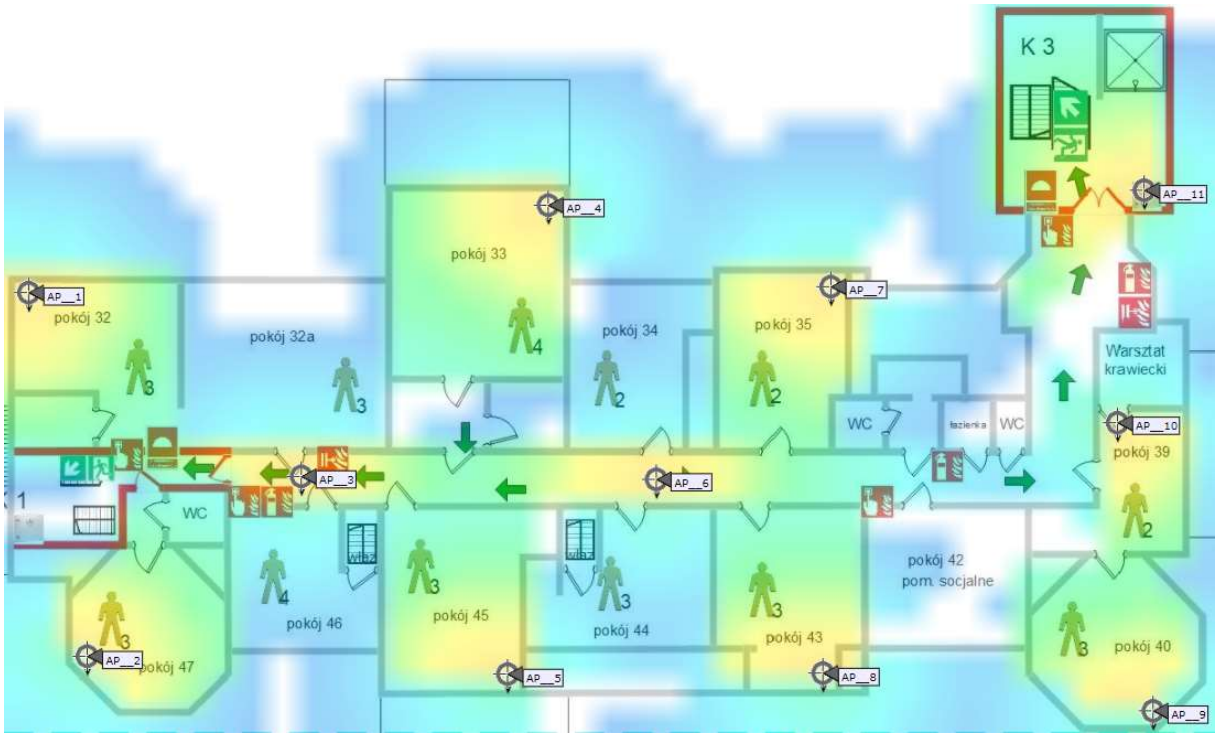
Rysunek 54: Miejsce instalacji access pointa

Drugi access point nad oknem na pierwszym piętrze, pod gzymsem na środku, okablowanie wejdzie bezpośrednio do pokoju na pierwszym piętrze, powinno zostać pomalowane w kolorze zgodnym z zaleceniami konserwatorskimi.

Drugie piętro



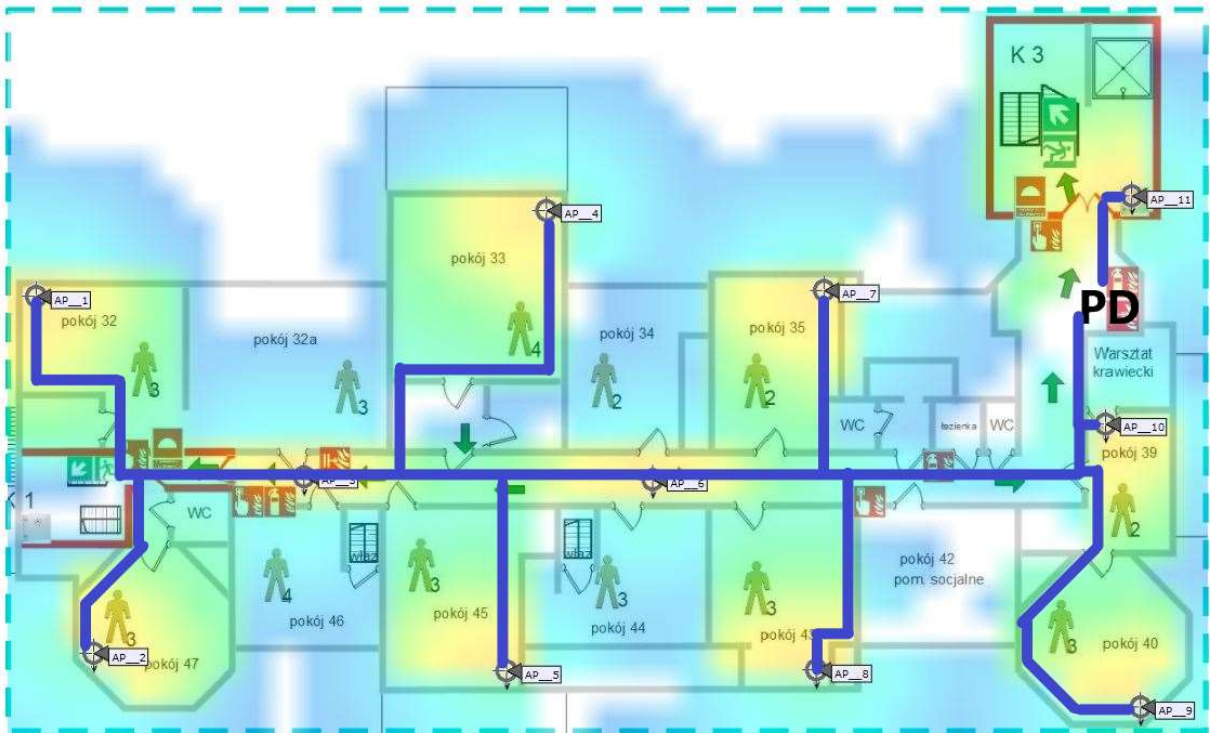
Rysunek 55: Planowanie dla częstotliwości 2,4GHz



Rysunek 56: Planowanie dla częstotliwości 5GHz

Na drugim piętrze zaproponowanych zostało jedenaście access pointów wewnętrznych. Całe okablowanie pochodzące od wszystkich access pointów będzie prowadzone korytarzem w nowych korytach kablowych do szafki PD4 w nowej klatce schodowej.

Planowanie tras kablowych



Rysunek 57: Na drugim piętrze całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	85
AP2	85
AP3	70
AP4	70
AP5	65
AP6	40
AP7	40
AP8	40
AP9	35
AP10	25
AP11	10

Podsumowanie

Liczba wszystkich urządzeń:

- Kontroler sieci bezprzewodowej: 1.
- Access pointy: 44, w tym 3 zewnętrzne.
- Switche: 1 core, 4 access.
- Firewall: 1.

Ze względu na zabytkowy charakter obiektu oraz na jego wiek należy mieć na uwadze:

- Grube ceglane ściany dochodzące do 50 cm szerokości, co może powodować trudności w prowadzeniu kabli, obserwowany znaczny spadek sygnału na korytarzu przy umiejscowieniu access pointa wewnątrz pokoju.
- Brak jakiejkolwiek infrastruktury, z której można by skorzystać w czasie projektowania, czy instalacji nowej sieci.
- Brak istniejących tras kablowych oraz przepustów.
- Część obiektu pod opieką konserwatorem zabytków.
- Brak doprowadzonego zasilania do wybranych punktów dostępowych.
- Równocześnie problemem dla wprowadzenia nowoczesnych usług może okazać się niedostatek parametrów połączenia internetowego oraz brak możliwości redundancji w tym zakresie.

Minimalne wymagania techniczne sprzętu

Kontroler sieci bezprzewodowej	• urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
	  ○ zarządzanie politykami bezpieczeństwa
	  ○ wykrywanie zagrożeń w sieci bezprzewodowej
	  ○ zarządzanie pasmem radiowym
	  ○ zarządzanie mobilnością
	  ○ zarządzanie jakością transmisji
	• obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji
	• min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45)
	• opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
	• obsługa ruchu tunelowanego
	• obsługa min. 1000 klientów sieci bezprzewodowej
	• zarządzanie pasmem radiowym punktów dostępowych:
	  ○ automatyczna adaptacja do zmian w czasie rzeczywistym
	  ○ optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
	  ○ dynamiczne przydzielanie kanałów radiowych
	  ○ wykrywanie, eliminacja i unikanie interferencji
	  ○ równoważenie obciążenia punktów dostępowych

	○ tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych ○ automatyczna dystrybucja klientów pomiędzy punkty dostępowe ○ mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych ○ dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe • mapowanie SSID do segmentów VLAN w sieci przewodowej • możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID) • automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji) • obsługa mechanizmów bezpieczeństwa: ○ 802.11i, WPA3, WPA2, WPA, WEP ○ 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST) ○ obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników • kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID • obsługa dostępu gościnnego (IPv4 i IPv6) ○ przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) ○ przekierowanie użytkowników do strony logowania na zewnętrznym serwerze • współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych • obsługa NTP wersji 4 (IPv4 oraz IPv6) • obsługa Hotspot 2.0 • obsługa redundancji rozwiązania
Access point wewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów

	• konfigurowalna moc nadajnika
	  ○ dla zakresu 2.4 GHz: do 100 mW
	  ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
	  ○ dla zakresu 5GHz (extended UNII-2): do 200 mW
	• zarządzanie przez kontroler WLAN z funkcjonalnościami:
	  ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
	  ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
	  ○ obsługa min. 16 BSSID
	  ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
	  ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
	  ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
	  ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
	  ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
	  ○ obsługa IPv6
	  ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
	  ○ obsługa mechanizmów QoS:
	  ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
	  ▪ obsługa WMM, TSPEC, U-APSD
	  ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
	  ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
	  ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA
	  ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)
	• konfiguracja polityk bezpieczeństwa per SSID
	  ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS)
	  ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
	  ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o

	nazwy domenowe o obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) o obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym o obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; o wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych
Access point zewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) o obsługa OFDMA (uplink/downlink), TWT, BSS Coloring o obsługa MU-MIMO – min. 2x2:2 o obsługa kanałów 20, 40 MHz dla 802.11n o obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax o obsługa beamforming dla klientów 802.11a/g/n/ac/ax o obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: o dla zakresu 2.4 GHz: min. 13 kanałów o dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów o dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika o dla zakresu 2.4 GHz: do 100 mW o dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW o dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: o automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN o optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) o obsługa min. 16 BSSID o definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID o uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w o obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów

	do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • dla access pointów zewnętrznych: ○ zgodność z IP67 ○ min. praca przy temperaturach między -35^{o}C a 60^{o}C • certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint

Switch core	• Typ i liczba portów:
	  o Min: 12 SFP/SFP+
	• Opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb):
	  o min. 4x1G SFP
	  o min. 4x1/10G SFP+
	• Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
	  o Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
	  o Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
	• Możliwość tworzenia stosów
	• Parametry wydajnościowe:
	  o Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
	  o Bufor pakietów – min.: 8MB
	  o Pamięć DRAM – min.: 4GB
	  o Pamięć flash – min.: 8GB
	  o Obsługa
	  ▪ min. 3.000 sieci VLAN
	  ▪ min.: 16.000 adresów MAC
	• Obsługa protokołu NTP
	• Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
	  o Obsługa protokołu STP
	• Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
	• Możliwość uruchomienia funkcji serwera DHCP
	• Mechanizmy związane z bezpieczeństwem sieci:
	  o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
	  o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
	  o Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	  o Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176

	○ Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard • Obsługa protokołów routingu: ○ Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie ○ Port konsoli ○ Dedykowany port Ethernet do zarządzania out-of-band ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
Switch access	• Typ i liczba portów: ○ min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP • Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami) • Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: ○ Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U ○ Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: ○ Przepustowość w ramach stosu – min.:60Gb/s ○ min: 4 urządzenia w stosie ○ Zarządzanie poprzez jeden adres IP • Parametry wydajnościowe:

	○ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) ○ Bufor pakietów – min: 4MB ○ Pamięć DRAM – min: 1GB ○ Pamięć flash – min: 2GB ○ Obsługa ▪ 1024 sieci VLAN ▪ min: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: ○ IEEE 802.1w Rapid Spanning Tree • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Obsługa protokołów routingu: ○ Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie ○ Port konsoli ○ Dedykowany port Ethernet do zarządzania out-of-band ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
Firewall	• Wymagania Ogólne ○ Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych,

	komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. o System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. o System musi wspierać IPv4 oraz IPv6 w zakresie: ▪ Firewall. ▪ Ochrony w warstwie aplikacji. ▪ Protokołów routingu dynamicznego. • Redundancja, monitoring i wykrywanie awarii o W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. o Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. o Monitoring stanu realizowanych połączeń VPN. • Interfejsy, Dysk, Zasilanie: o System realizujący funkcję Firewall musi dysponować minimum: ▪ min. 4 portami Gigabit Ethernet RJ-45. ▪ min. 2 gniazdami SFP 1 Gbps. o System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. o System musi być wyposażony w zasilanie AC. • Parametry wydajnościowe: o W zakresie Firewall'a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. o Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps o Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0,5 Gbps. o Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps. • Funkcje Systemu Bezpieczeństwa: o W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. ▪ Kontrola Aplikacji.

	▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. ▪ Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). ▪ Funkcja lokalnego serwera DNS ze wsparciem dla DNS • Polityki, Firewall o Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. o System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. ▪ W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. ▪ Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. • Połączenia VPN o System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site. o System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

	▪ Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. ▪ Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. • Routing i obsługa łączy WAN o W zakresie routingu rozwiązanie powinno zapewniać obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu. ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. • Ochrona przed malware • Ochrona przed atakami o Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • Kontrola aplikacji • Kontrola WWW • Zarządzanie • Logowanie • Serwisy i licencje o W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. • Gwarancja oraz wsparcie
Okablowanie etherentowe	• Min. Cat 6 ekranowana

Zalecenia konserwatorskie dla Domu Pomocy Społecznej w Cetuniu

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152;
e-mail: koszal

ZN.K.5183.76.2021.KB

Koszalin, 28

DOM POMOCY SPOŁECZN
CETUŃ nr 6, 76-
adres do k
Network Experts
ul. Chojnowska 8, 03-58

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń sieci bezprzewodowej – punków dostępowych, instalacji okablowani dystrybucyjnych, w Domu Pomocy Społecznej w Cetuniu, Cetuń 6, 76- w związku z opracowywaniem dokumentacji dotyczącej „Opracowania radiowej dla budynków DPS Powiatu Koszalińskiego".

Odpowiadając na pismo z dnia 17.05.2021 r. (data wpływu 18.05.2021 r 17.06.2021 r. (data wpływu 21.06.2021 r.), uzupełnione pismem z dnia 25.0 wpływu 25, 28.06.2021 r.), w oparciu o wizję lokalną przeprowadzoną w dniu Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie, działają art. 27 Ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabyt z 2021 r. poz. 710 ze zm.) przekazuje następujące zalecenia konserwatorskie:

1. Pałac w Cetuniu gm. Polanów, jest zabytkiem architektury i budownic do rejestru zabytków pod nr A-1626 decyzją z dnia 03.03.2017 r., obszarze parku w Cetuniu wpisanego do rejestru zabytków pod nr z dnia 08.06.1978 roku. Przedmiotowa nieruchomość podlega ochron podstawie art. 6 ust. 1 lit. c, g oraz art. 7 ust. 1 ustawy z dnia 23.07.200 zabytków i opiece nad zabytkami (t.j. Dz.U. z 2021 r. poz. 710 ze zm. określonych w tej ustawie. Zgodnie z art. 36 ust. 1 przywołanej ustawy badań konserwatorskich, robót budowlanych oraz umieszcza technicznych na zabytku wpisanym do rejestru zabytków wym

przedstawione na załączonych rzutach piwnic, niskiego parteru, parteru oraz fotografiach elewacji i wnętrz pałacu.

3. Zaleca się prowadzenie kabli instalacyjnych w osłonach do kolorystycznie i umieszczonych możliwie dyskretnie u zbiegu ścia z ograniczeniem do minimum trasy ich przebiegu. Ponadto zaleca się og minimum wielkości urządzeń do transmisji sieci bezprzewodowej i szaf kolorystyczne obudowy urządzeń z podłożem.

4. W pomieszczeniach w których zachował się oryginalny wystrój sztukato (świetlica, stołówka, hall, klatka schodowa), detal, itp., zaleca się prze badań konserwatorskich (odkrywek) przed zakończeniem prac p w miejscach wyznaczonych do prowadzenia kabli i umieszczania urz dyplomowanego konserwatora zabytków, w celu sprawdzenia, czy urządzeń nie naruszy oryginalnego wystroju pomieszczeń.

Z up. ZACHODNIOPO
WOJEWÓDZKIEGO KONSERWA
Kierownik Delegatury

mgr Dorota Raczk

Otrzymują:

Uzupełnienie zaleceń konserwatorskich dla Cetunia

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152; fa
e-mail: koszalin

ZN.K.5183.76.2021.KB

Koszalin, 30 cz

DOM POMOCY SPOŁECZNE
CETUŃ nr 6, 76-01
adres do kor
Network Experts sp
ul. Chojnowska 8, 03-583

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń sieci bezprzewodowej – punków dostępowych, instalacji okablowania dystrybucyjnych, w Domu Pomocy Społecznej w Cetuniu, Cetuń 6, 76-0 w związku z opracowywaniem dokumentacji dotyczącej „Opracowania radiowej dla budynków DPS Powiatu Koszalińskiego".

W uzupełnieniu do pisma ZWKZ znak ZN.K.5183.76.2021.KB z dnia 28 Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie Kierown w Koszalinie przekazuje w załączeniu 1 egzemplarz dokumentacji pt. „ dokumentacji konserwatorskiej do wydania zaleceń pod budowę nowej sieci Pomocy Społecznej w Cetuniu".

Z up. ZACHODNIOPO
WOJEWÓDZKIE GOKONSER
Kierownik Jeleg
mgr Jarosław Rac

Uzupełnienie dokumentacji konserwatorskiej do wydania zaleceń budowę nowej sieci wifi w Domu Pom Społecznej w Cetuniu

W czasie wizyty lokalnej w Cetuniu ustalone zostały nowe miejsca instalacji access pointów kablowe.

Ustalenia końcowe

Montaż szaf rakowych w wybranych punktach:

- w poszczególnych PD, które mają zostać zainstalowane na korytarzu – kolor szafy b jasno szary, tak aby wkomponować się w kolor ścian
- zalecane jest, aby szafa miała jak najmniejszy rozmiar, który umożliwi zainstalowar sprzętów, przewidywany rozmiar dla każdego piętra 6U-9U
- w GPD w pomieszczeniu kasy, nie ma wymogu kolorystycznego

Przykładowe miejsce instalacji nowej szafy na niskim parterze.

Prowadzenie kabli światłowodowych

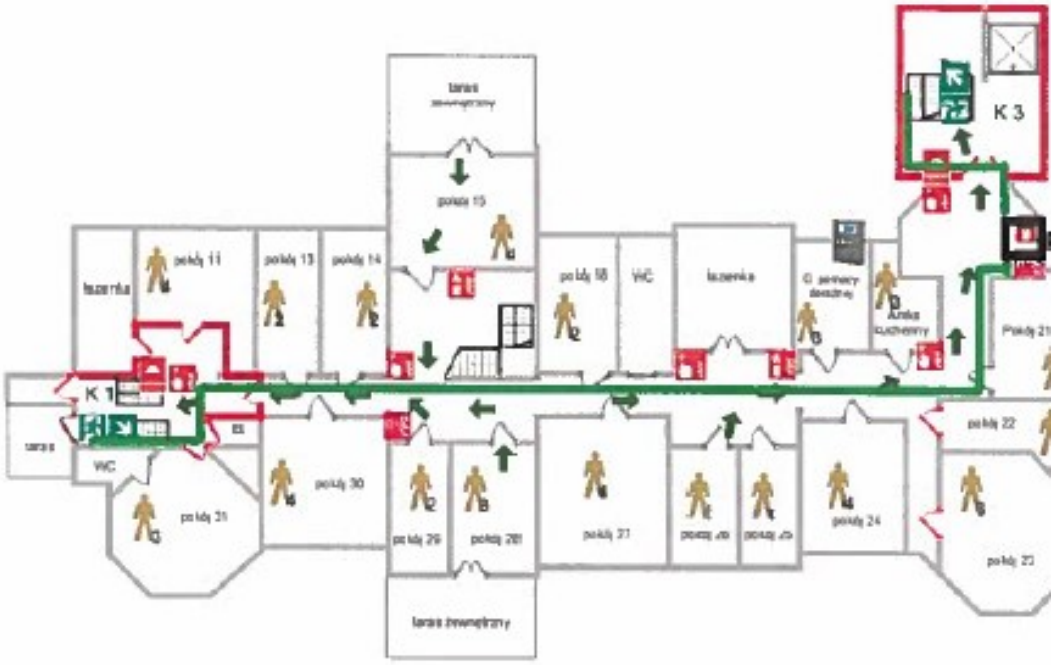
Z poszczególnych PD rozmieszczonych na każdym piętrze, wyjście nową klatka schodową i nową trasą kablową po pierwszym piętrze do starej klatki schodowej a następnie zejście do przejście przez ścianę do pomieszczenia kasy wraz z uwzględnieniem ominięcia szybów kom Nowe kable światłowodowe mają być umieszczone na całej długości w korytkach kabl najmniejszym przekroju. Koryta mają zostać dołożone pod istniejącymi już instalacjami, stworzyć spójną całość. Muszą iść w rogach ścian, wzdłuż korytarzy, tam, gdzie będzie to k mają zostać pomalowane w odpowiednim kolorze. Okablowanie światłowodowe ze wszy umieszczonych obok nowej klatki schodowej zostanie sprowadzone na pierwsze piętro, a przeprowadzone korytami do drugiej klatki schodowej skąd wejdzie do pomieszczenia kasy d serwerowni.

Miejsca instalacji szafek na każdym piętrze oraz zaznaczenie przewidzianych tras światłowod

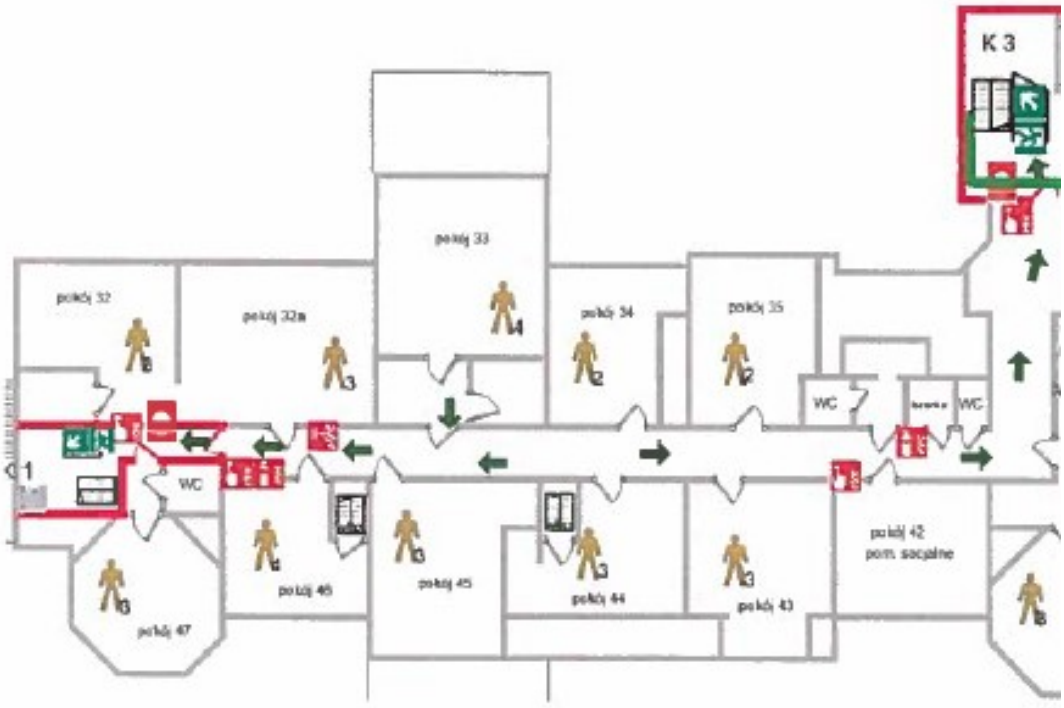
Parter

Niski parter

Pierwsze piętro



Drugie piętro



Aktualizacja rozmieszczenia access pointów wraz z zaznaczonymi trasami kablowymi do najl
punktu dystrybucyjnego.

- Kable ethernetowe muszą być prowadzone w korytach kablowych dołożonych do is
  infrastruktury
- Koryta muszą być zamaskowane kolorem, jeżeli będzie taka potrzeba
- Instalacja access pointów będzie pod sufitem czy to w pokoju czy na korytarzu

Koryta kablowe nowe powinny stykać się ze starymi, tak aby zajmować jak najmniej miejsca

Koryta powinny iść zawsze na styku ściany i sufitu, tak aby nie dopuścić do sytuacji, że pojav
nowa listwa na środku sufitu

Przepusty przez ściany również powinny być w miejscach, gdzie są obecnie, jeżeli nie ma to
zostać zrobione tak aby były jak najmniej widoczne

Piwnica

- brak planowanych urządzeń

Niski parter

Na niskim parterze całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścia

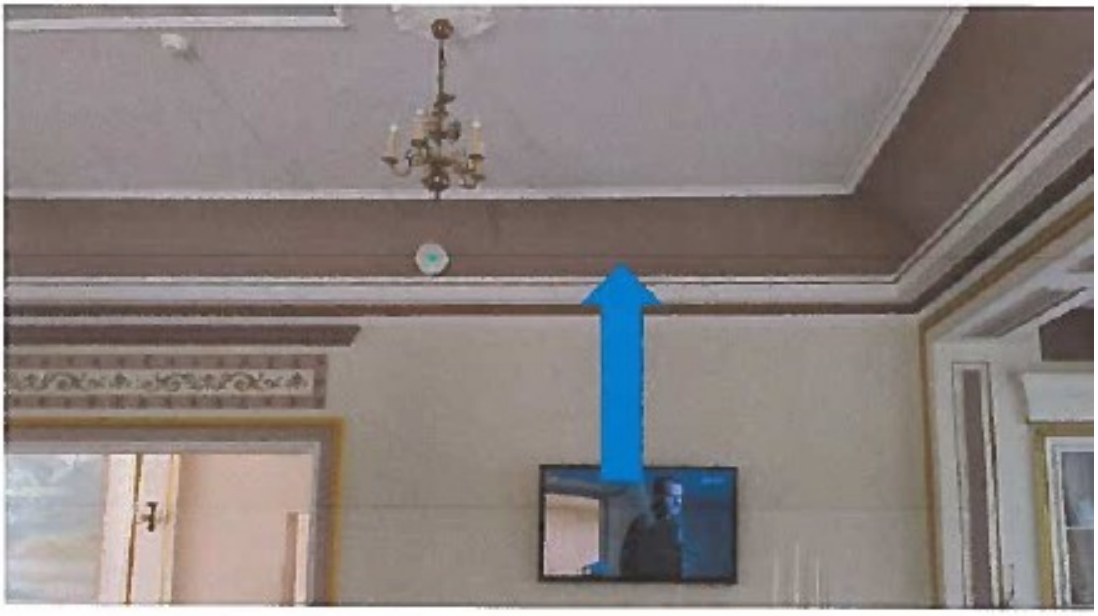
Parter

będzie możliwa. Z tych miejsc okablowanie przechodząc przez świetlice musi zostać umieszcz
gzymsie i tak ukryte, aby nie było widać przewierceń przez ściany. Dla tych miejsc niezbędne
wystąpienie o badania do konserwatora.

Access point w stołówce powinien zostać umieszczony w samym rogu

Access point w czytelni powinien zostać umieszczony jak najbliżej ściany obok listwy

Koryto kablowe powinno przejść na styku ściany oraz sufitu



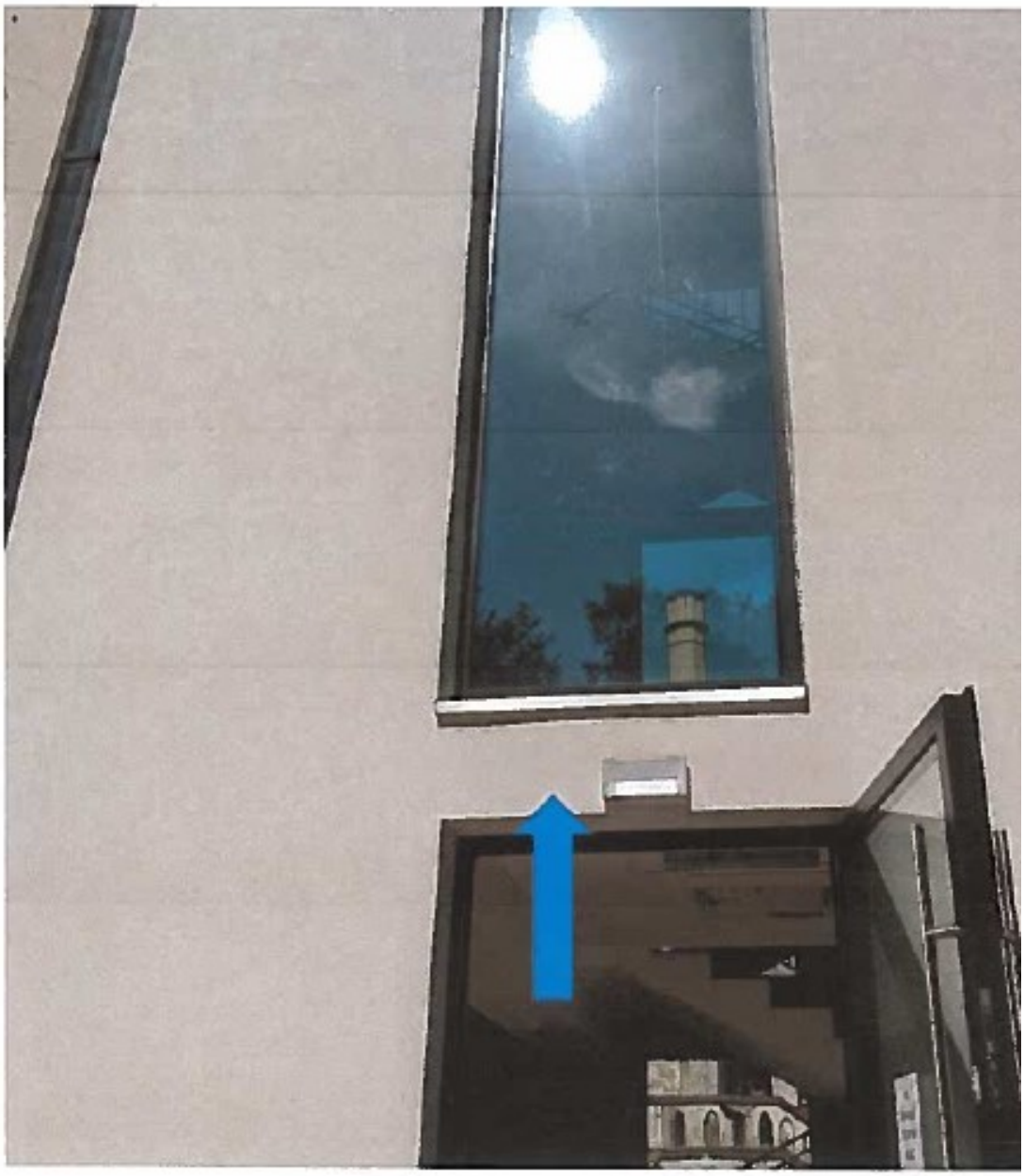
Gzyms na jakim musi zostać położone okablowanie

Pierwsze piętro

Na pierwszym piętrze okablowanie musi iść w korytach stykających się z istniejącą infrastrukt

Access pointy zewnętrzne

Na elewacji nowej klatki schodowej



Urządzenie powinno zostać umieszczone obok lampy ewakuacyjnej, okablowanie do PD na
parterze

Access pointy na elewacji frontowej

Na środku pod gzymsem, zlicowane ze ścianą, okablowanie przebije się z tarasu bezpośrednio urządzenia, powinno zostać pomalowane w kolorze z zbadań konserwatorskich

Drugi access point nad oknem na pierwszym piętrze, pod gzymsem na środku, okablowanie w bezpośrednio do pokoju na pierwszym piętrze, powinno zostać pomalowane w kolorze z zbad

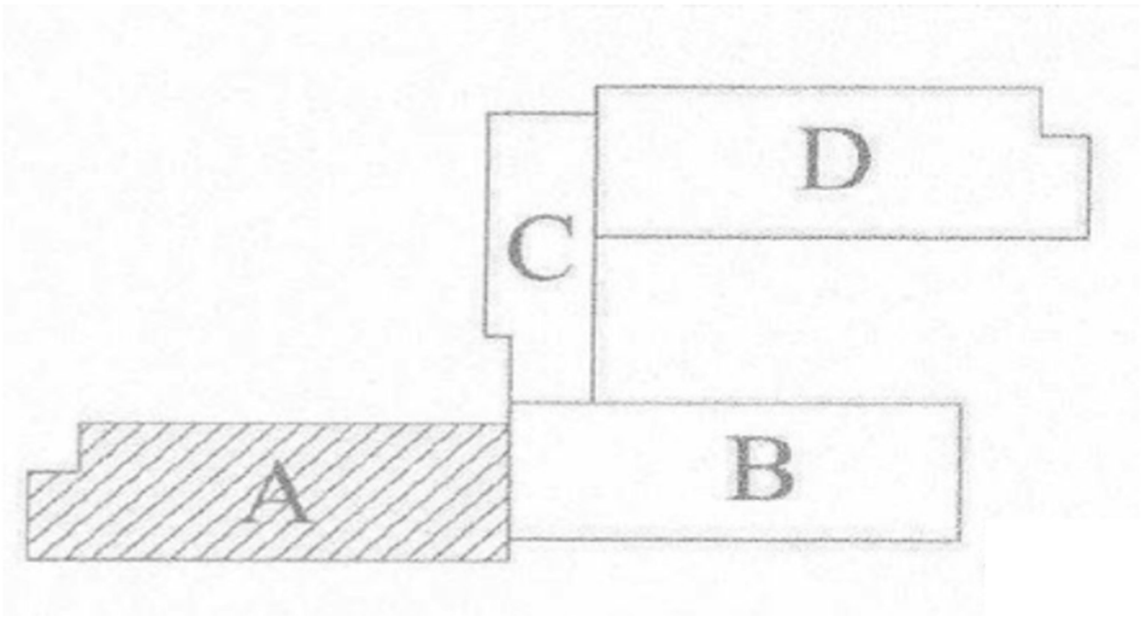
Drugie piętro

Na drugim piętrze całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścia

Załącznik nr 2 DPS Żydowo

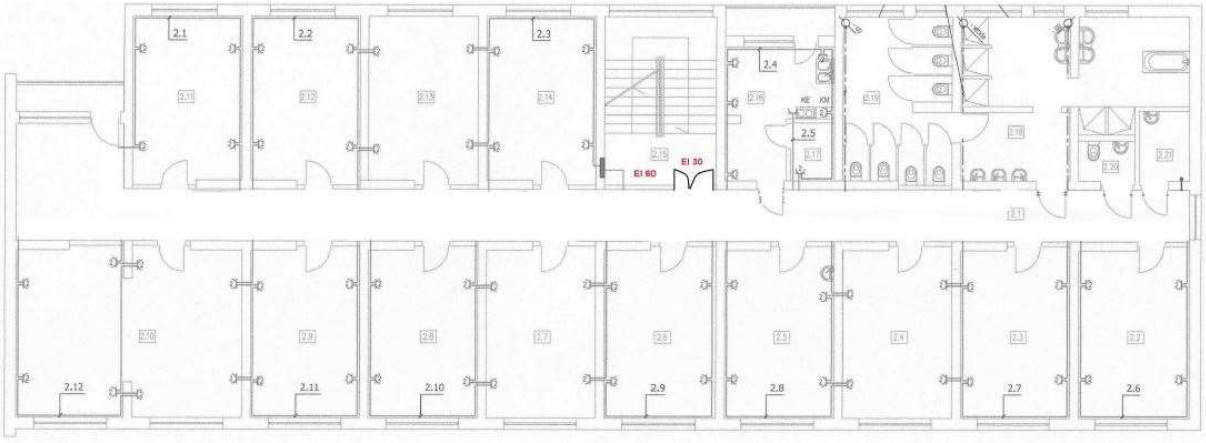
DPS Żydowo składa się z dwóch części: budynku głównego oraz budynku administracyjnego oddalonego o kilkaset metrów. Budynek główny składa się z części piwnicznej, parterowej oraz dwóch piętrowych skrzydeł (A i D).

Plany budynków

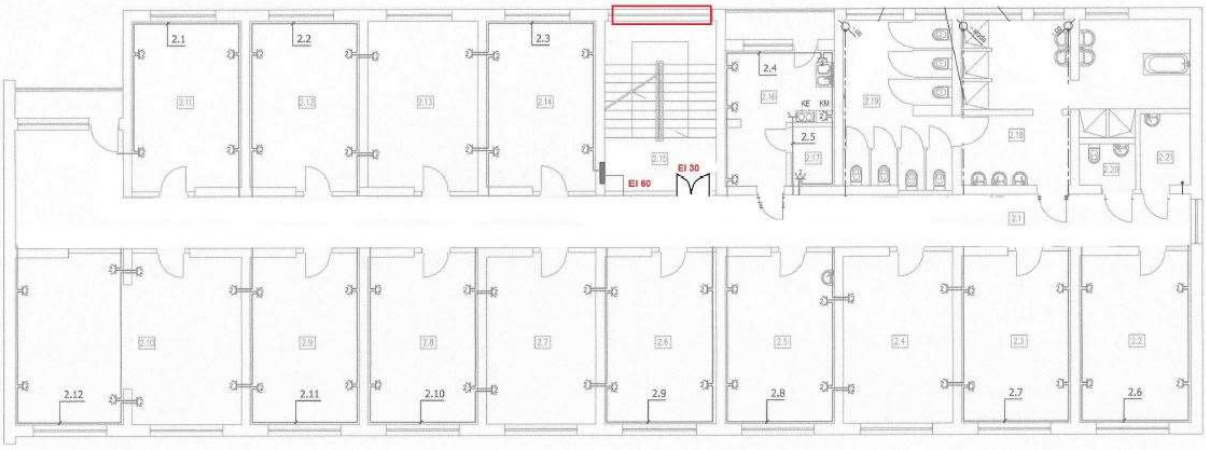


Rysunek 1: Podział budynku głównego na bloki A, B, C, D

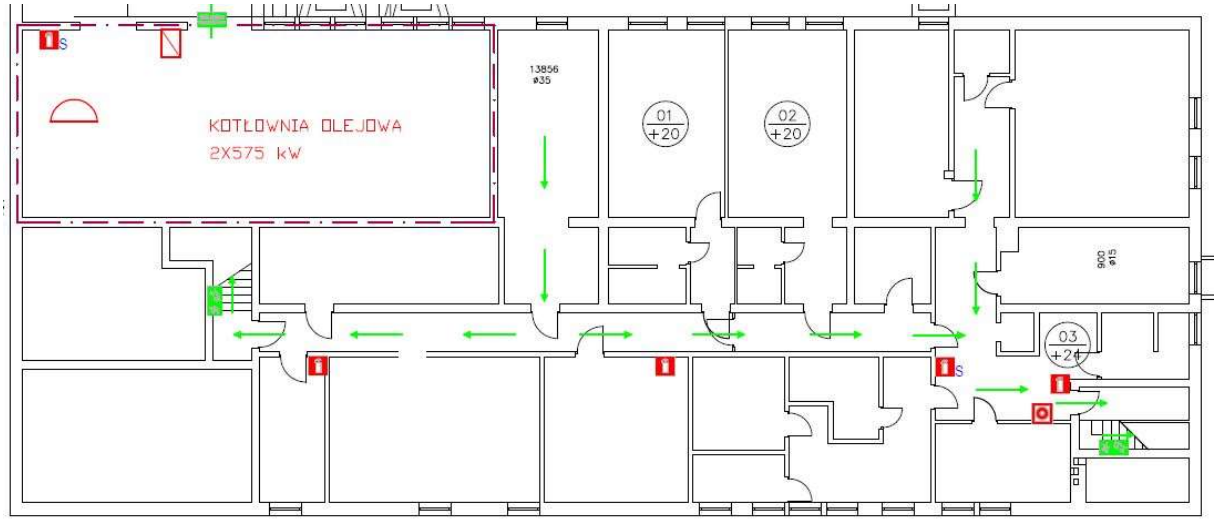
Rysunek 2: Budynek główny parter



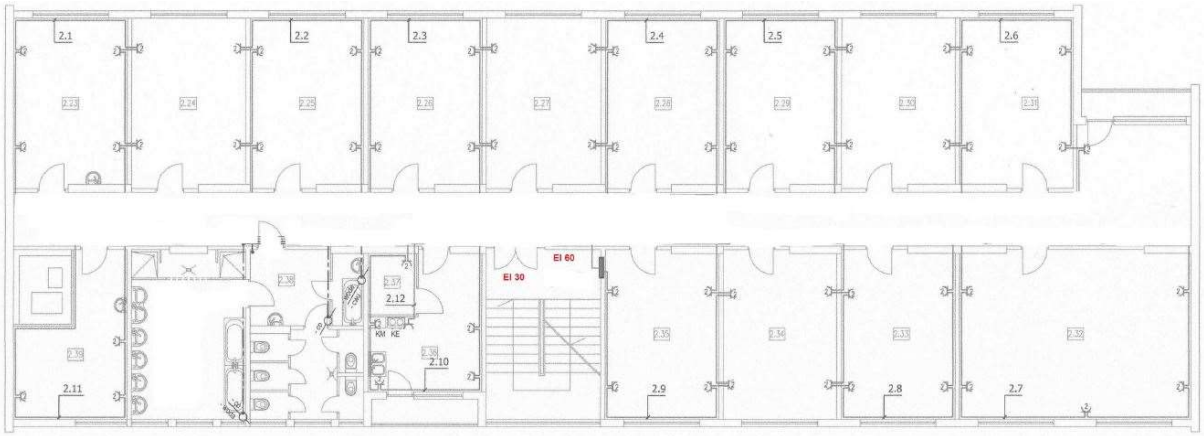
Rysunek 3: Plan A1



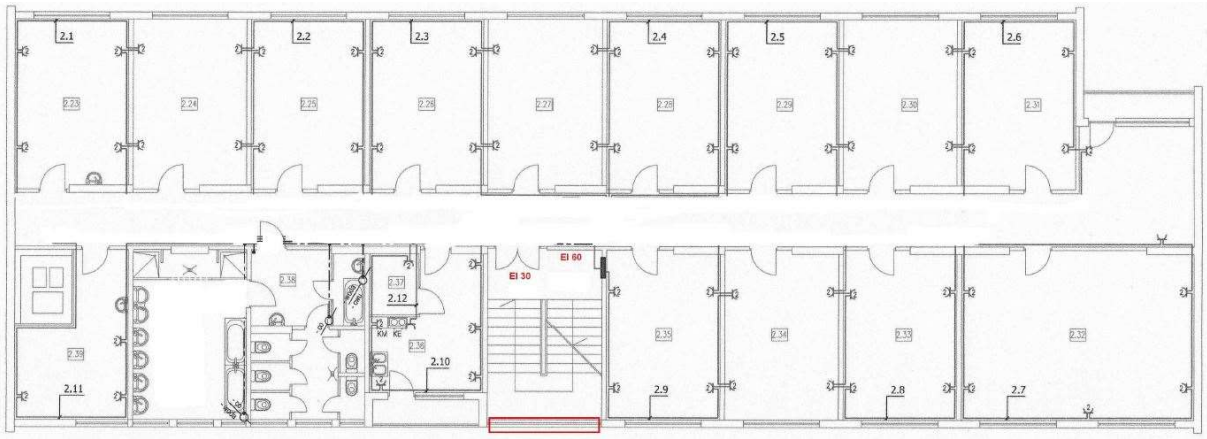
Rysunek 4: Plan A2



Rysunek 5: Plan B-1



Rysunek 6: Plan D1



Rysunek 7: Plan D2

Obecny stań sieci

W obecnej chwili w Żydowie są doprowadzone dwa łącza internetowe, jedno do budynku administracji a drugie do budynku głównego. W żadnym z budynków nie ma wydzielonego miejsca na serwerownię. Cała sieć LAN jest oparta o rozwiązania domowe, brak zarządzalnych urządzeń. W budynku głównym sieć LAN jest rozprowadzona jedynie przy pomieszczeniach administracyjnych. Brak infrastruktury sieciowej ethernetowej i światłowodowej, z której mogli by korzystać mieszkańcy poza jedną salą komputerową obok pomieszczeń administracji. Dodatkowo budka strażnicza na wjeździe jest połączona z częścią biurową za pomocą radiolinii. Ze względu na przyszłe prace i chęć wprowadzenia zaawansowanego systemu sieci bezprzewodowej niezbędne będzie wybudowanie całkowicie nowej infrastruktury sieci LAN. Żadne z obecnie używanych urządzeń nie będzie się nadawać do przyszłego wykorzystania. Dotyczy się to również części budynku administracyjnego.

Rysunek 8: Radiolinia łącząca budynek główny z pomieszczeniem strażników na wjeździe

Rysunek 9: Pomieszczenie biurowe, do którego wchodzi radiolinia

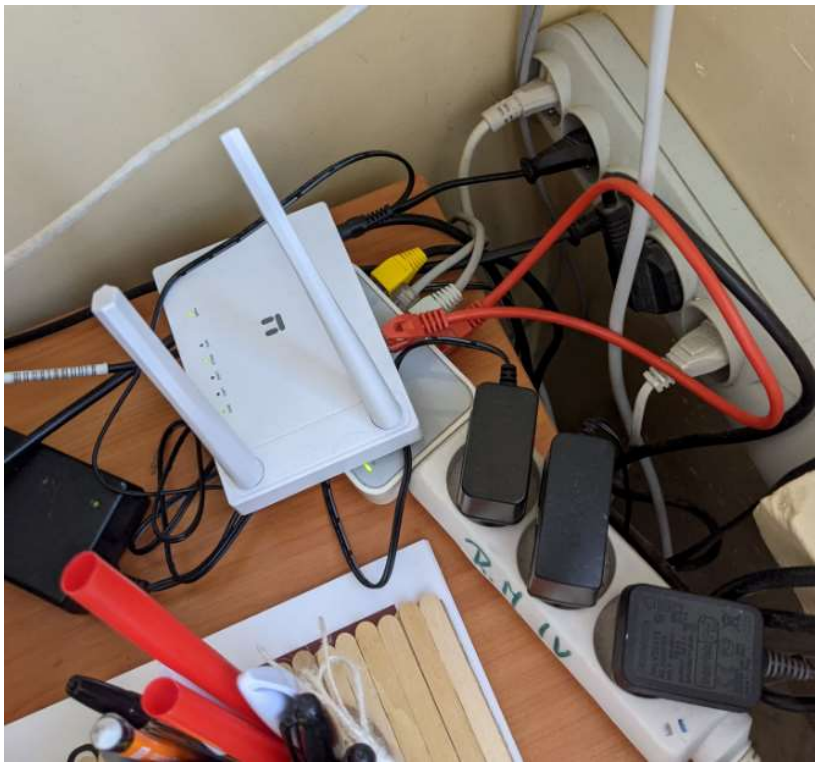
Rysunek 10: Szafa rack monitoringu

Jest rozprowadzone okablowanie pod monitoring, które zakończone jest w małych szafach dystrybucyjnych, nie podlegało to audytowi, jako że jest to niezależna sieć.

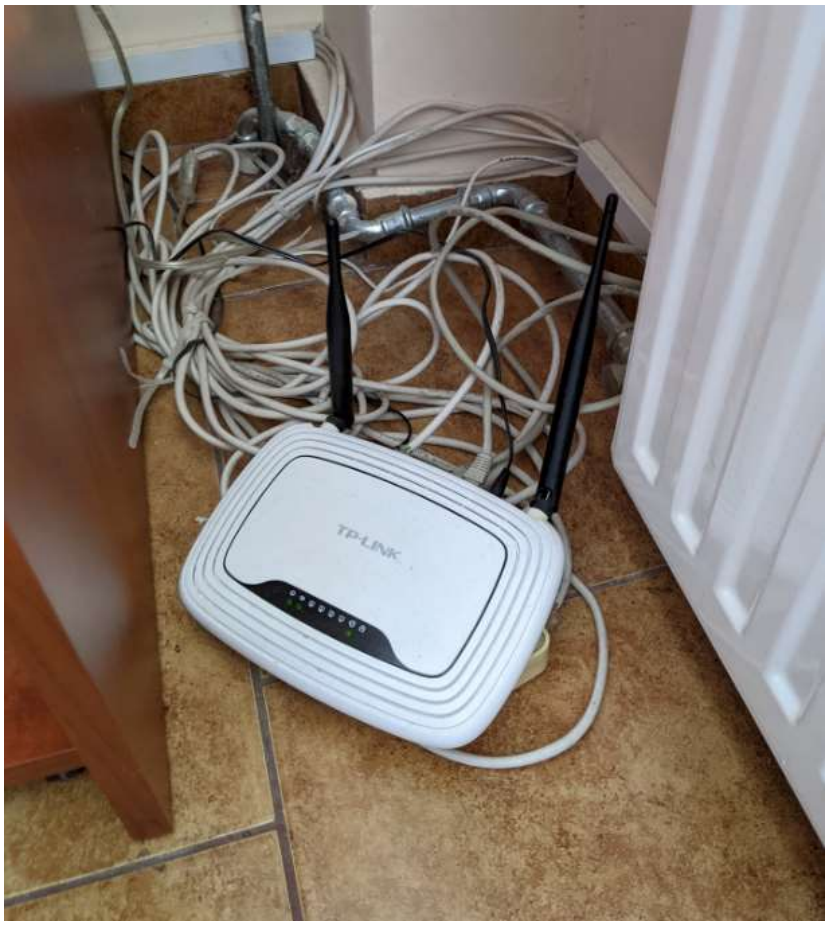
Rysunek 11: Modem operatora w części administracyjnej

Rysunek 12: Małe niezarządzalne switche w części biurowej

Rysunek 13: Drugie łącze internetowe w części administracyjnej budynku głównego



Rysunek 14: Urządzenia w części biurowej



Rysunek 15: Urządzenia w części biurowej

Wifi w obecnej chwili jest realizowane z pomocą małych routerów domowych.

Rysunek 16: Podłączenie linii telefonicznej

Rysunek 17: Podłączenie linii telefonicznej

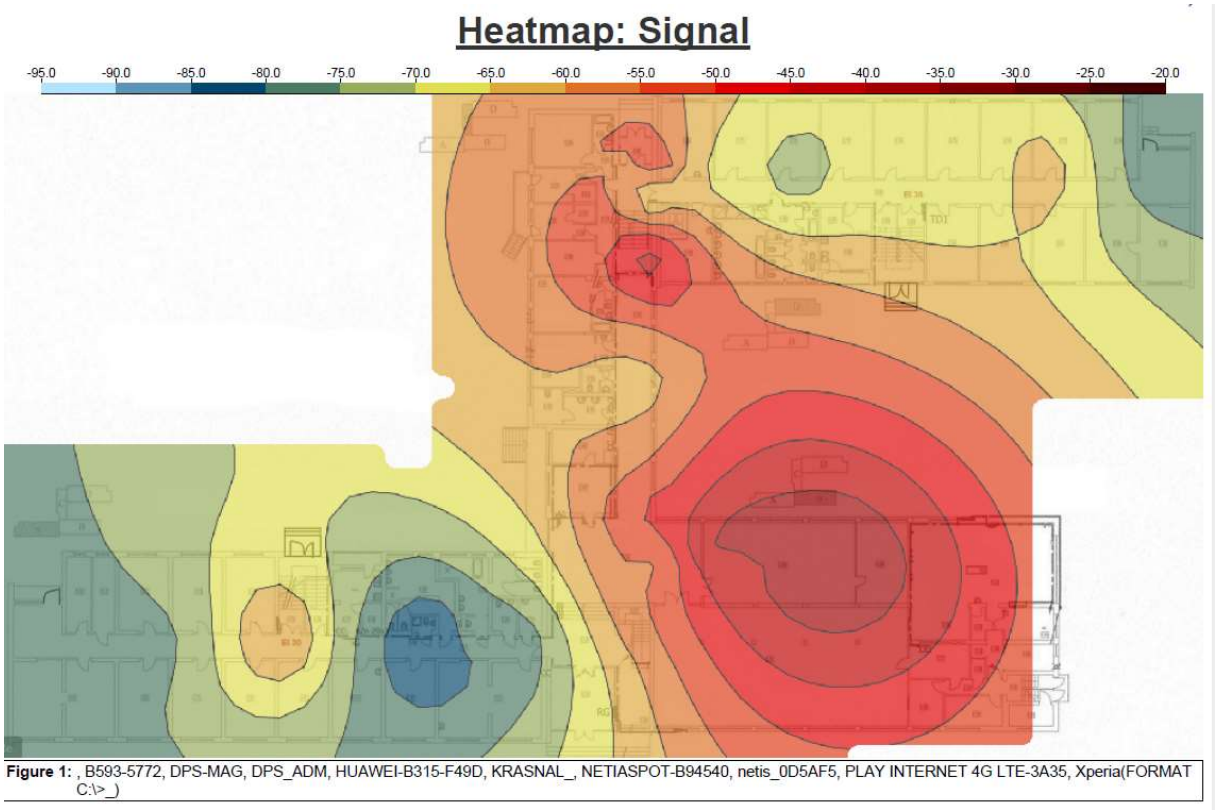
Z budynku administracji jest połączenie do budynku głównego przez stróżówkę za pomocą położonej niedawno linii telefonicznej. Nowe mocowania pozwolą na dołożenie ewentualnie nowych połączeń światłowodowych.

Stan istniejącej sieci WLAN

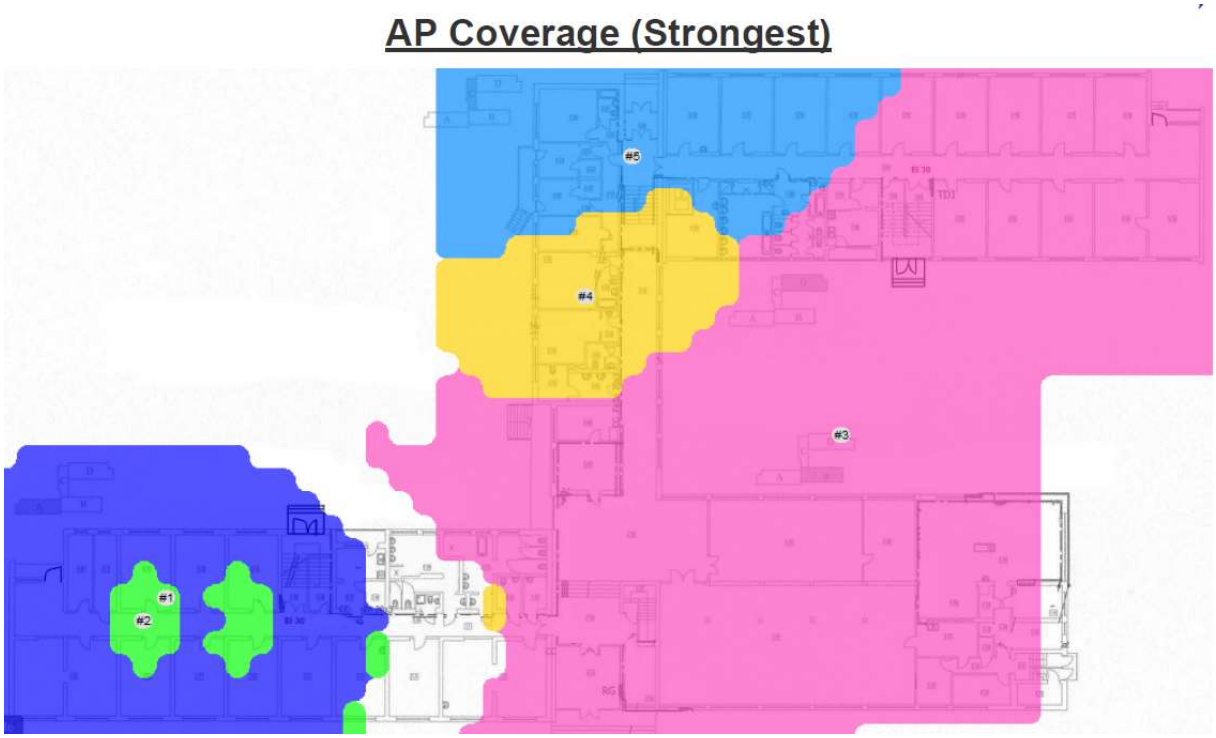
AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
	#10		14:d1:69:be:3a:38	1/40MHz	300	WPA2	n	14	20	11	0	3
B593-5772	#8		HuaweiTech:59:76:b4	4	54	WPA2	g	10	14	5	0	4
DPS-MAG	#6		ac:84:c6:0c:e3:bb	10/40MHz	300	WPA2	n	12	22	5	0	13
DPS_ADM	#5		TpLinkTech:0e:ef:98	6/40MHz	300	WPA2	n	23	50	6	0	20
HUAWEI-B315-F49D	#7		HuaweiTech:8c:f4:9d	11	144	WPA2	n	4	9	0	0	5
KRASNAL_	#1		local:9e:bf:c0:37:48:3b	11	144	WPA2	n	21	33	7	0	7
NETIASPOT-B94540	#4		Vtech Tele:b9:45:48	1	144	WPA2	n	20	52	7	0	25
netis_0D5AF5	#3		04:5e:a4:0d:5a:f5	8/40MHz	300	WPA2	n	28	56	7	0	37
PLAY INTERNET 4G LTE-3A35	#9		14:d1:69:be:3a:35	1/40MHz	300	WPA2	n	10	13	7	0	2
Xperia(FORMAT C:\>_)	#2		SonyMobile:cb:6a:d6	11	54	WEP	g	16	32	5	0	9

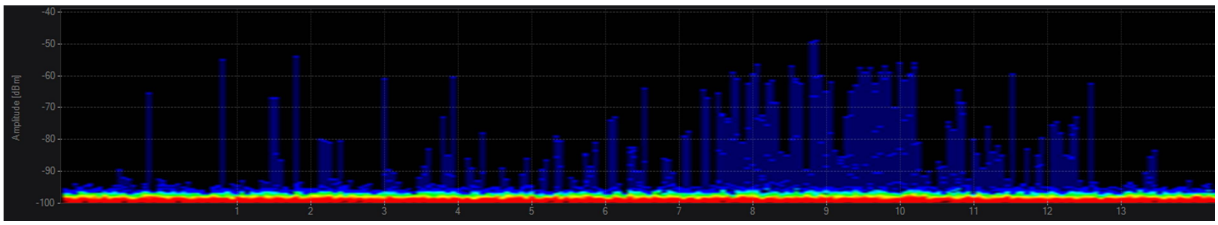
Rysunek 18: Lista widocznych sieci bezprzewodowych na parterze budynku głównego



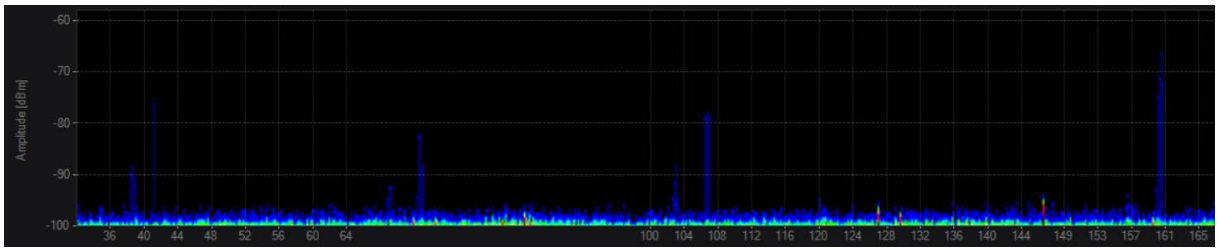
Rysunek 19: Sygnał sieci radiowych na parterze budynku głównego



Rysunek 20: Najmocniejszy access point w danym obszarze



Rysunek 21: Pomiar widma w paśmie 2,4GHz



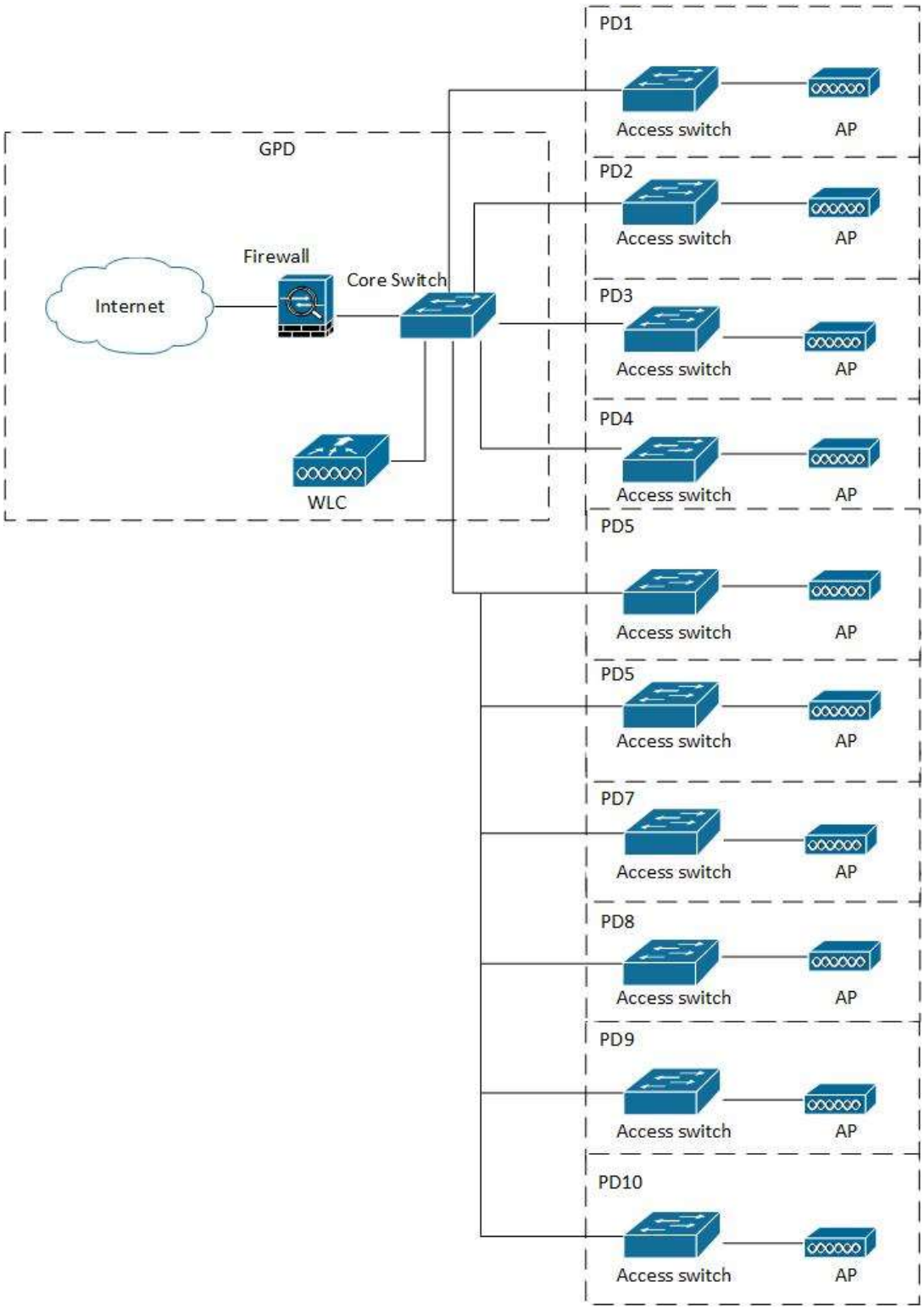
Rysunek 22: Pomiar widma w paśmie 5GHz

Jak można zaobserwować w Żydowie nie ma zakłóceń ani w paśmie 2,4GHz ani w 5GHz. Można zaobserwować duże zaszumienie, ale jest ono tak niskie (poniżej -90dBm), także nie będzie miało to wpływu na pracę urządzeń wifi.

Koncepcja nowej sieci LAN

Nowa sieć LAN powinna zostać wykonana z założeniem, że w obecnej chwili w Żydowie nie ma żadnej infrastruktury. Należy wybrać miejsca, gdzie będzie możliwe zrobienie nowej serwerowni oraz punkty pośrednie dystrybucyjne. Należy rozprowadzić nowe połączenia światłowodowe pomiędzy wszystkimi punktami pośrednimi a główną serwerownią. Na styku nowej sieci LAN z Internetem powinno znaleźć się urządzenie zabezpieczające sieć wewnętrzną – firewall. W każdym punkcie

dystrybucyjnym należy umieścić przełącznik dostępowy co najmniej 24 portowy PoE/PoE+, tak aby podłączyć wszystkie access pointy. Każdy z punktów następnie zostanie podłączony do switcha corowego w głównej serwerowni. Należy przyjąć architekturę gwiazdy, w której każdy pośredni punkt dystrybuujmy będzie bezpośrednio podłączony do GPD. W głównej serwerowni będzie również zainstalowany kontroler sieci bezprzewodowej.

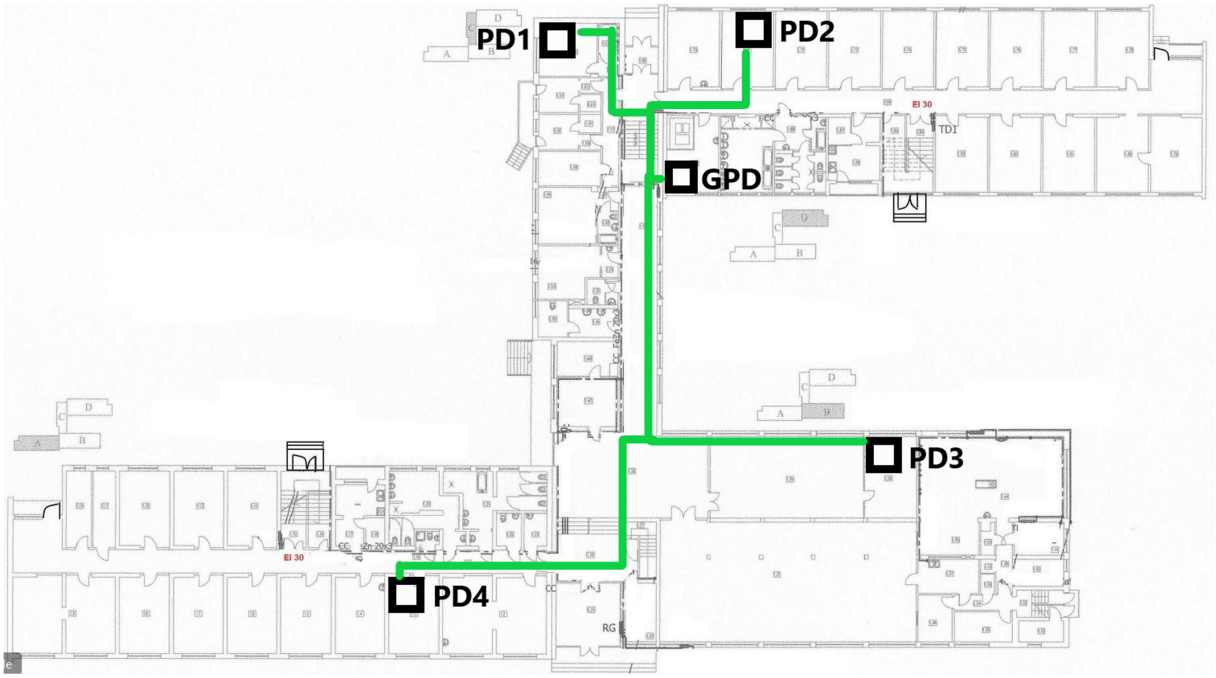


Rysunek 23: Schemat nowej sieci LAN

Punkty dystrybucyjne

Poniżej przedstawione zostały miejsca instalacji głównej serwerowni, punktów dystrybucyjnych oraz połączeń światłowodach. Na planach zaznaczone zostały jako zielone linie.

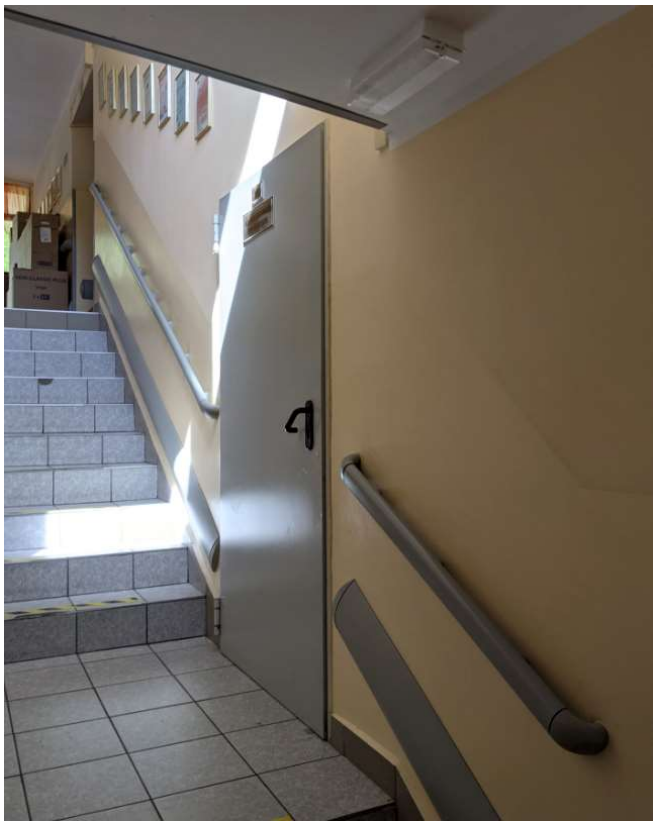
Budynek główny



Rysunek 24: Koncepcja tras światłowodów i instalacji szaf rackowych w budynku głównym

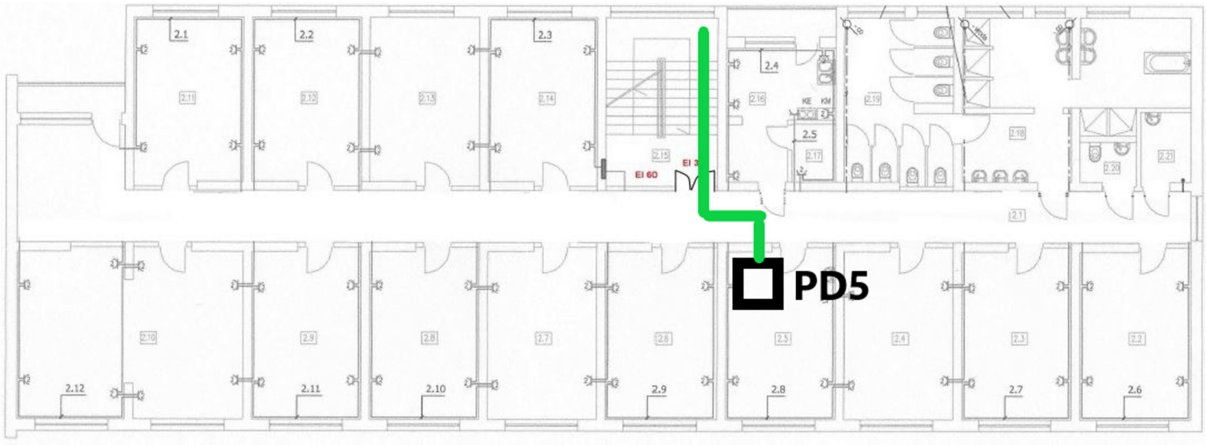
Lista punktów:

- GPD – w specjalnie wybranym miejscu
- PD1 – sala komputerowa
- PD2 – pokój socjalny budynek D parter
- PD3 – sala za sceną
- PD4 – pokój socjalny w parterowej części A

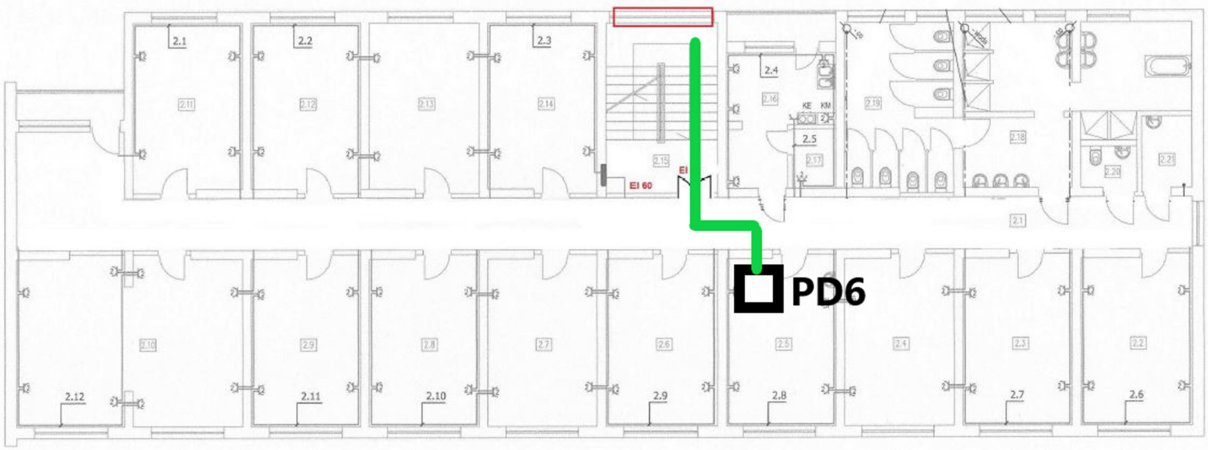


Rysunek 25: Miejsce pod nową główną serwerownię zostało zaproponowane przez pracowników administracyjnych DPS Żydowo. Jest to pomieszczenie odizolowane, przy ścianie szczytowej, gdyby zaszła potrzeba podłączenie klimatyzacji.

Rysunek 26: Proponowane miejsce na szafę rack w pomieszczeniu socjalnym na ścianie koło drzwi – parter A

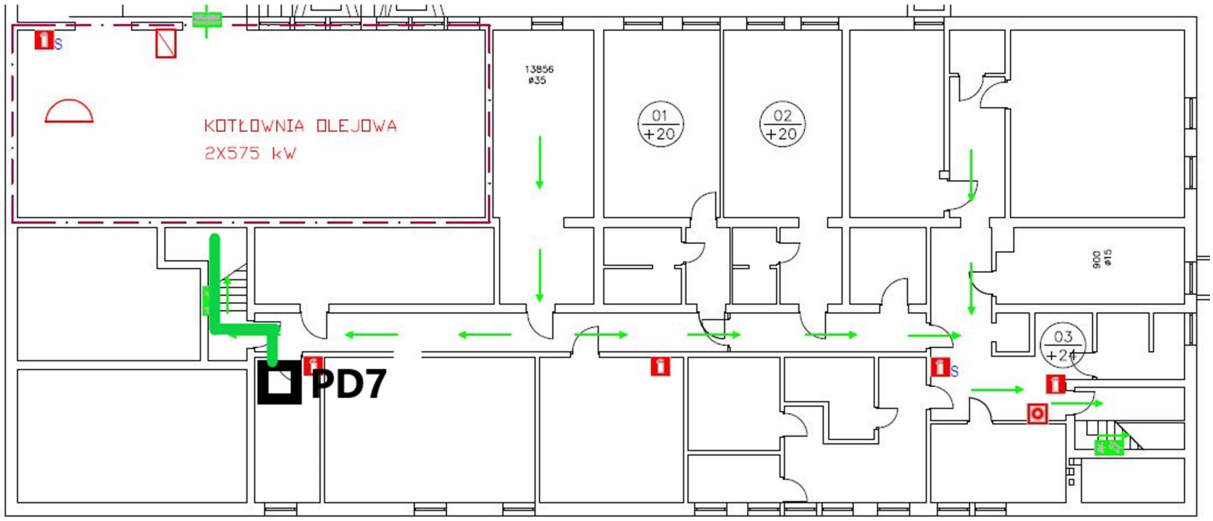


Rysunek 27: Koncepcja trasy światłowodu i instalacji szafy PD5 – budynek A, pierwsze piętro, pokój socjalny, zejście klatką schodową na parter i do GPD

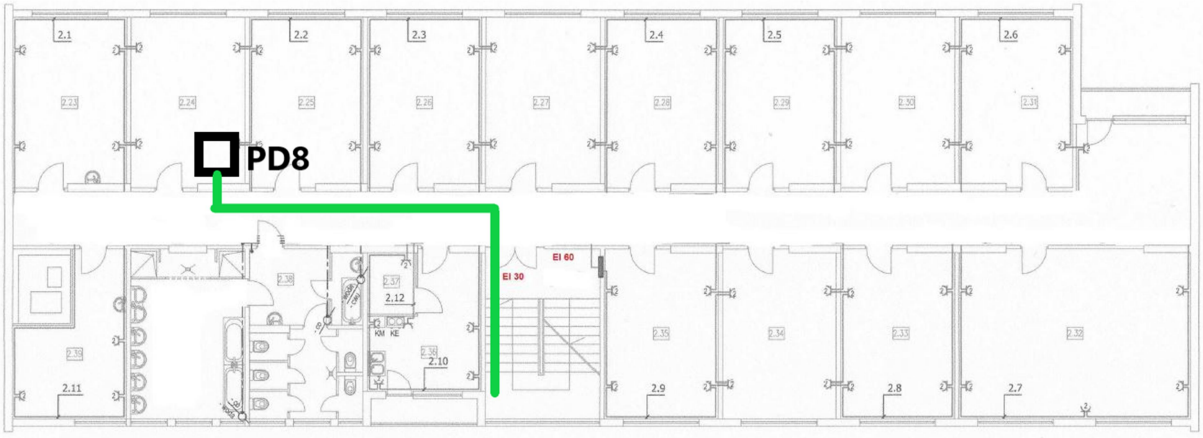


Rysunek 28: Koncepcja trasy światłowodu i instalacji szafy PD6 – budynek A, drugie piętro, pokój socjalny. Zejście do GPD klatką schodową na parter

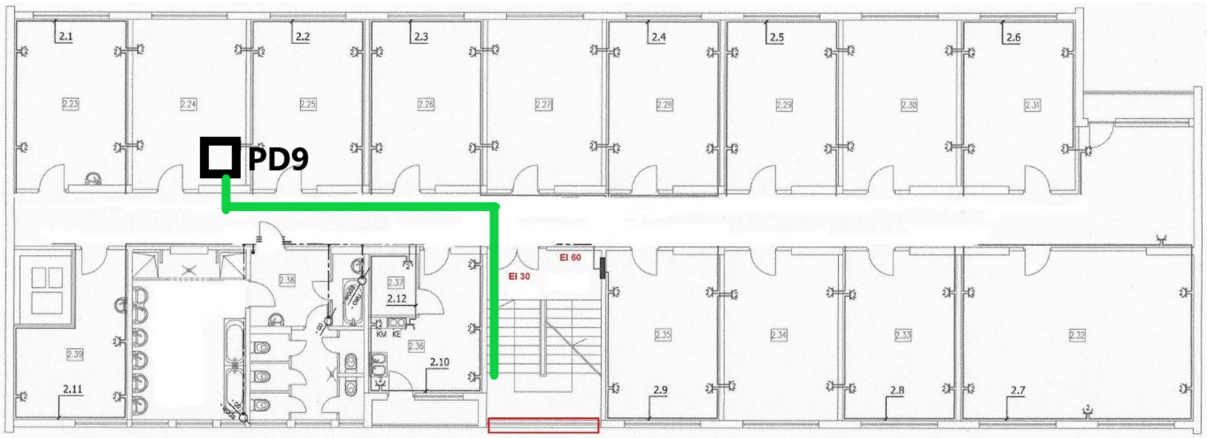
Tak samo jak na parterze budynku A proponowane miejsce na szafkę na ścianie koło drzwi w pomieszczeniu socjalnym.



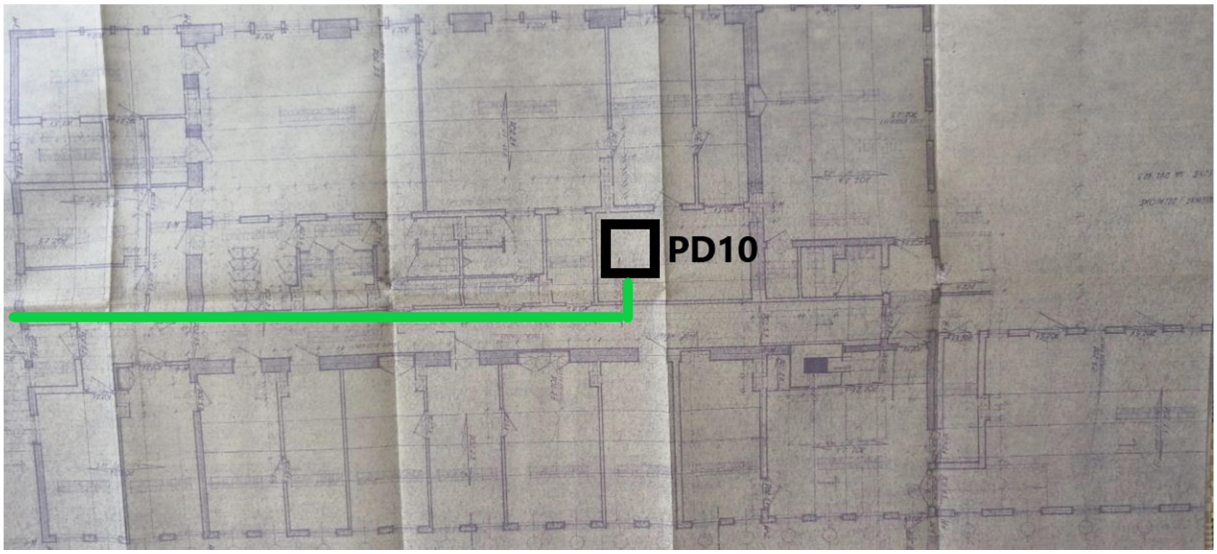
Rysunek 29: Koncepcja trasy światłowodu i instalacji szafy PD7 – piwnica w części B, pokój komputerowy



Rysunek 30: Koncepcja trasy światłowodu i instalacji szafy PD8 – budynek D, pierwsze piętro, pokój socjalny, zejście do GDP klatką schodową



Rysunek 31: Koncepcja trasy światłowodu i instalacji szafy PD9 – budynek D, drugie piętro, pokój socjalny, zejście do GDP klatką schodową



Rysunek 32: Koncepcja trasy światłowodu i instalacji szafy PD10 – pomieszczenie xero

Jedyny otrzymany plan budynku administracji jest z przed wielu lat dlatego należy mieć na uwadze, że rozkład ścian może różnić się od tego co jest w rzeczywistości.

Budynek administracji powinien zostać bezpośrednio podłączony z budynkiem głównym ze względu na wspólne systemy jakie mają zostać uruchomione w ramach przyszłego projektu. Jeżeli jest to możliwe należy wykorzystać telefoniczną trasę kablową łączącą obie lokalizacje. Najlepszym rozwiązaniem byłoby przekopanie światłowodu pomiędzy oba budynkami. Ze względu na koszty całej operacji może być to za drogie rozwiązanie.

Analiza możliwości przyłączenia do zewnętrznej szerokopasmowej sieci internetowej

Ze względu na lokalizację Żydowa w obecnej chwili brak możliwości podłączenia Internetu światłowodowego. W przyszłości rozważane jest doprowadzenie go z pobliskiego Polanowa.

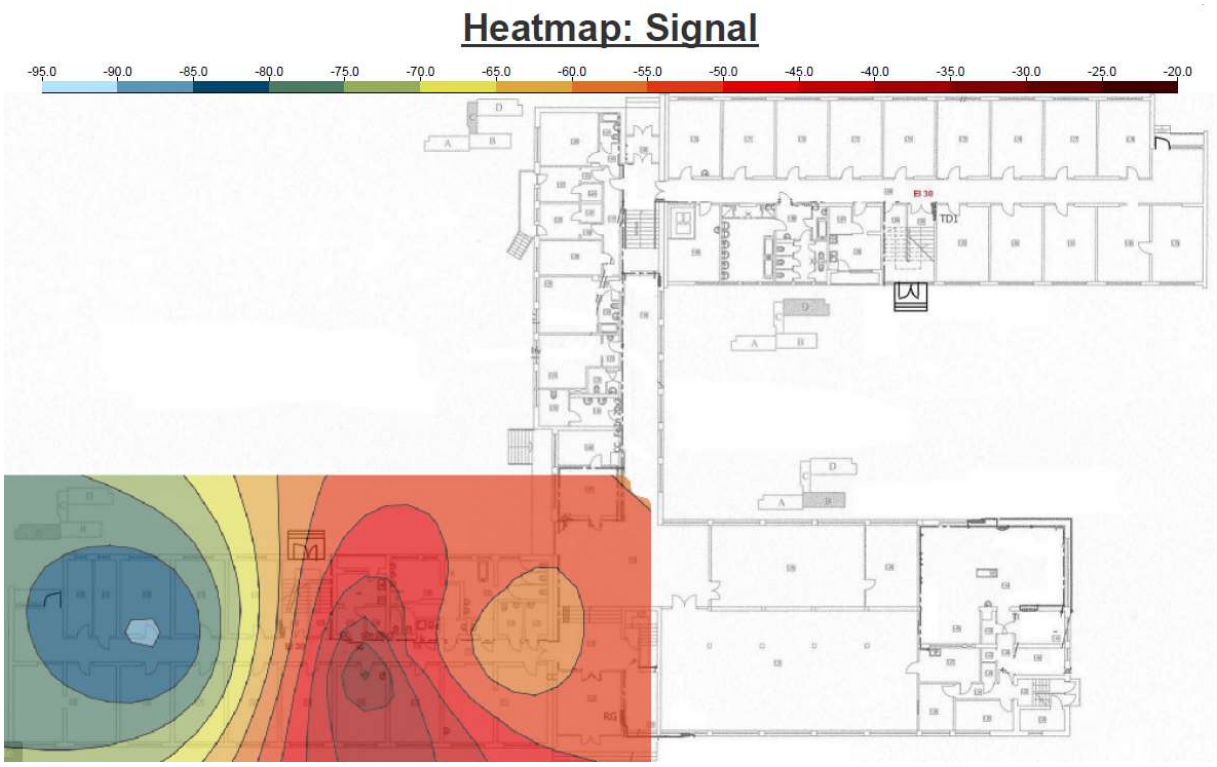
Rysunek 33: Test prędkości wykonany z komputera podłączonego do obecnej sieci LAN.

W związku z połączeniem internetowym o prędkości 10Mb/s niezalecane jest przeprowadzanie więcej niż dwa połączenia video w tym samym momencie. Rekomendowany jest QoS to zrealizowania przez operatorów.

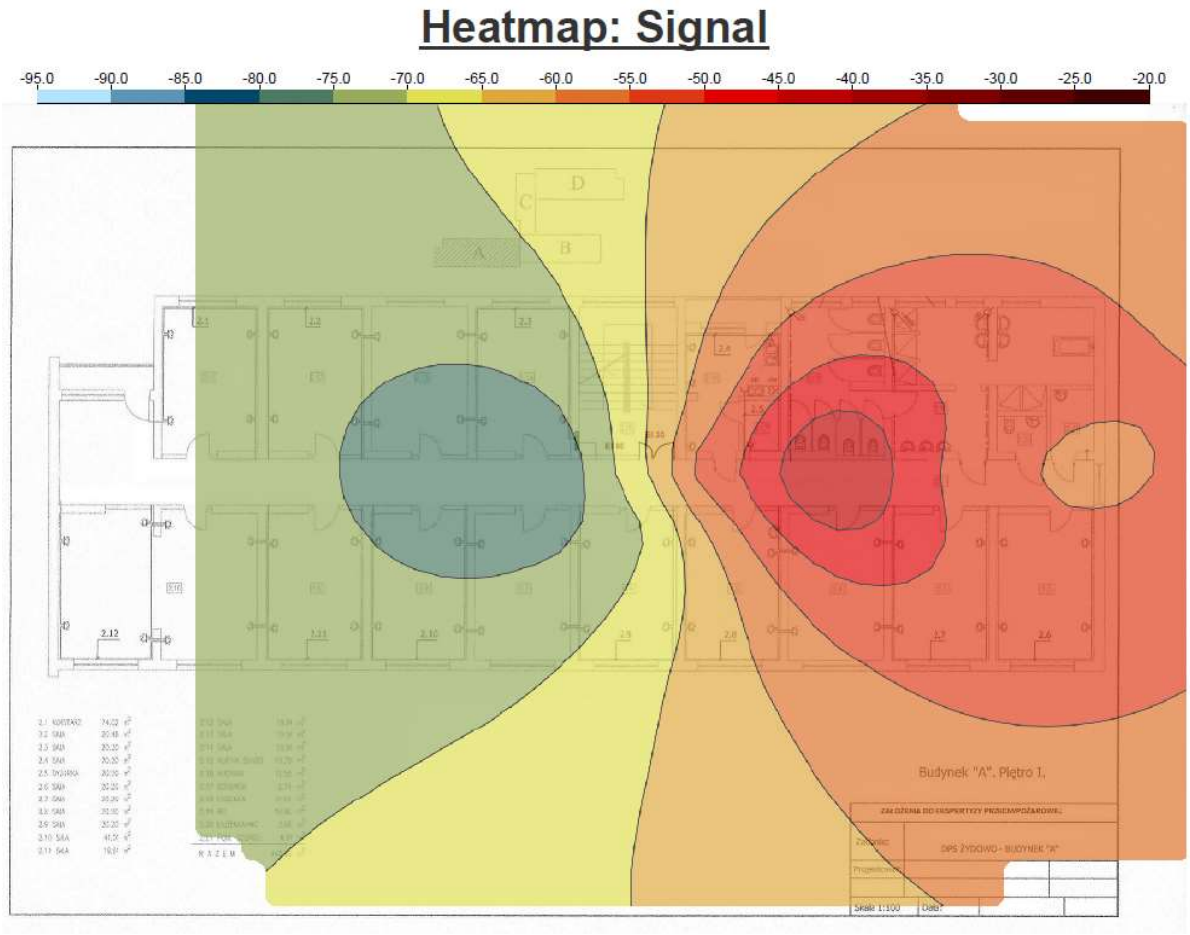
Koncepcja rozmieszczenia nowych punktów dostępowych wraz z doporowadzeniem tras kablowych oraz protokół pomiarowy stanowiący podstawę do opracowania dokumentacji

Poniżej przedstawione zostało planowanie radiowe dla wszystkich budynków w Żydowie. Cały obszar budynkowy powinien zostać objęty sygnałem radiowym a część zewnętrzna tylko we wskazanych miejscach. Budynek nie ma żadnych ograniczeń, jeżeli chodzi o prowadzenie tras kablowych oraz instalację nowych urządzeń. Sygnałem radiowym powinny z zachowaniem triangulacji w celu lokalizacji pacjentów powinny zostać objęte wszystkie obszary mieszkalne oraz części wspólne, w których przebywają. W częściach biurowych oraz magazynowych sygnał ma być dostępny na założonym poziomie.

Wykonane zostały badania tłumienia ścian, które pozwoliło na późniejsze przygotowanie rozmieszczenia access pointów na terenie całego DPSu. Ze względu na specjalny charakter budynku mieszkalnego możliwe było jedynie przeprowadzenie dwóch pomiarów.



Rysunek 34: Badanie przeprowadzone na parterze, w którym access point umieszczony w pokoju lekarskim



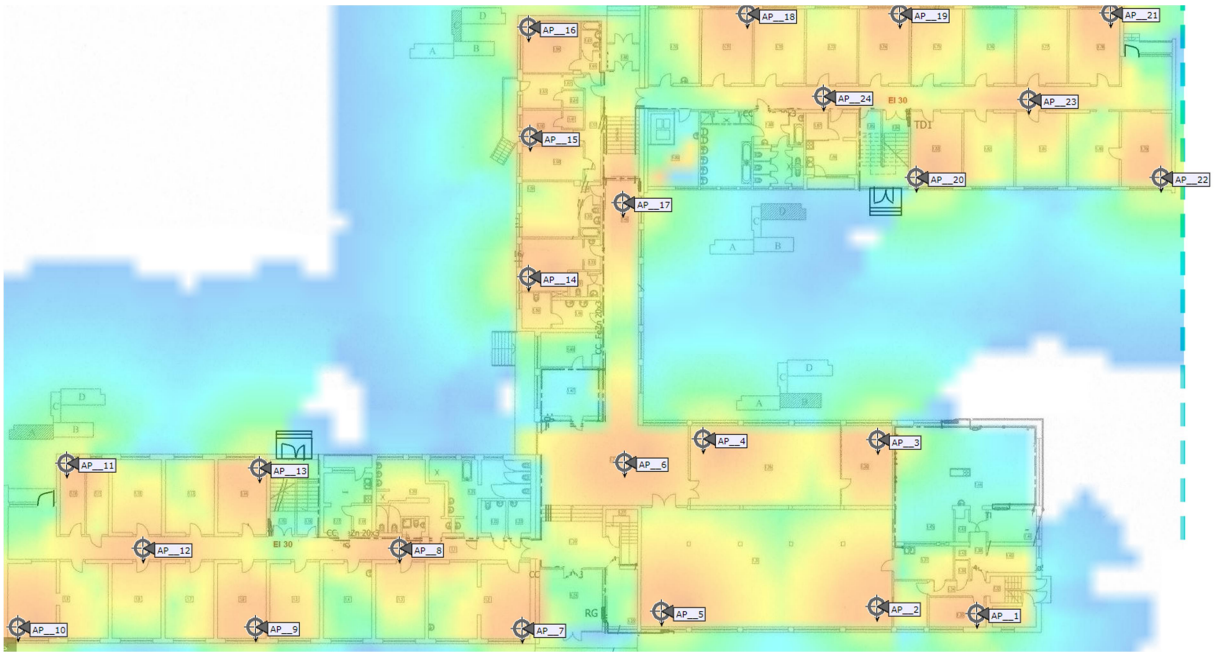
Rysunek 35: Badanie przeprowadzone na pierwszym piętrze, w którym access point był umieszczony w pokoju lekarskim.

Jak można zaobserwować przy access poincie umieszczonym w pokoju, sygnał utrzymuje się na bardzo dobrym poziomie jedynie w najbliższych pokojach. Przy pomiarach w dalszej części korytarza obserwuje się znaczny spadek poziomu sygnału nawet o 15 dBm. Ściany wykonane są w cegły oraz ich grubość nie przekracza w większości miejsc 20 cm grubości.

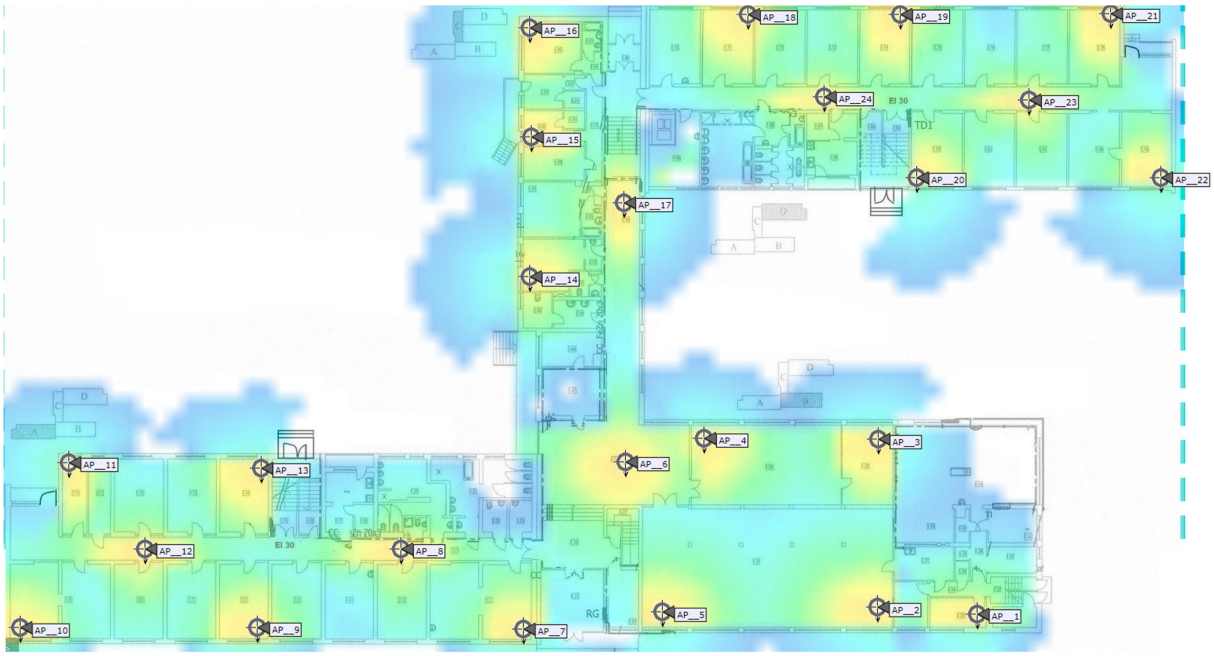
Planowanie radiowe

Budynek główny

Parter



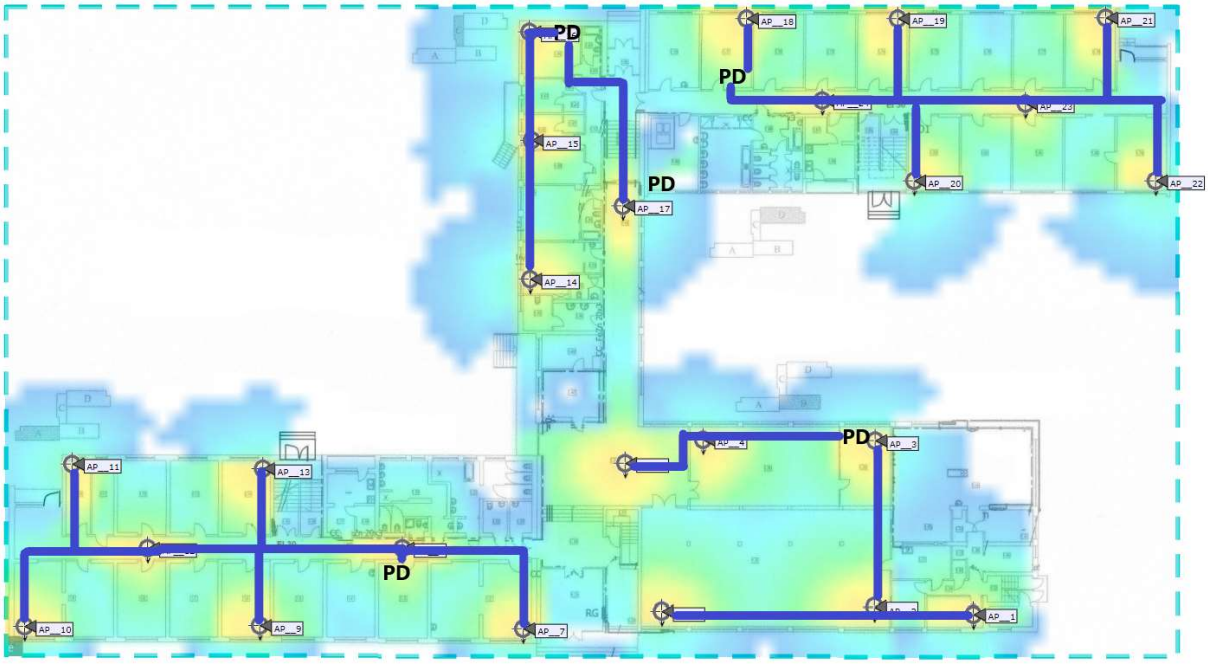
Rysunek 36: Planowanie dla częstotliwości 2,4GHz



Rysunek 37: Planowanie dla częstotliwości 5GHz

Na parterze zaproponowane zostały dwadzieścia cztery access pointy, rozmieszczone, tak aby zapewniona była triangulacja na całym obszarze. Trasy kablowe z każdej części budynku proponujemy prowadzić do najbliższego punktu dystrybucyjnego korytarzami. W żadnym punkcie nie ma przekroczonej odległości 100 m do najbliższego punktu dystrybucyjnego.

Planowane trasy kablowe

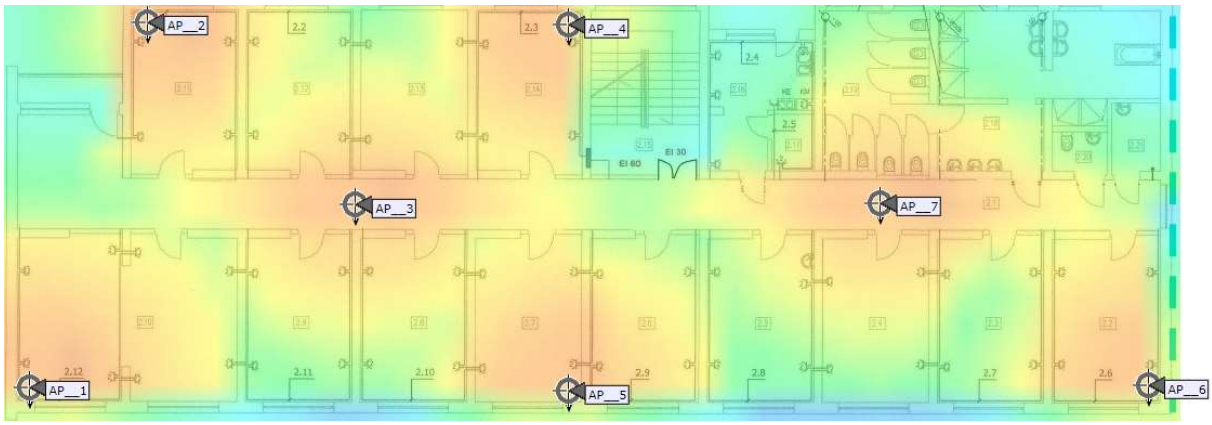


Rysunek 38: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

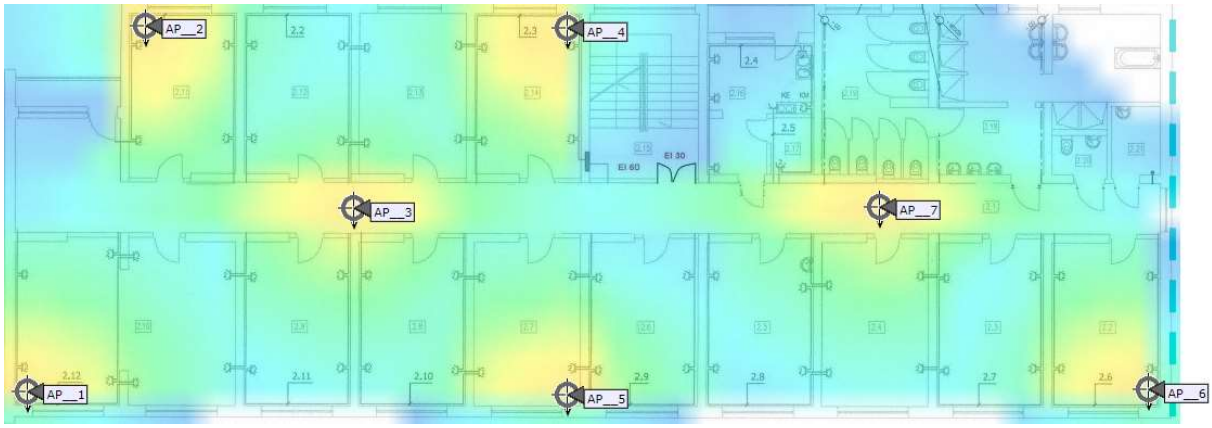
Numer AP	Szacowana długość okablowania [m]
AP1	30
AP2	20
AP3	5
AP4	20
AP5	30
AP6	30
AP7	15
AP8	10
AP9	20
AP10	40
AP11	40
AP12	35
AP13	35
AP14	30
AP15	20
AP16	5
AP17	30
AP18	5
AP19	30
AP20	30
AP21	40
AP22	40
AP23	35

AP24	25

Budynek A1

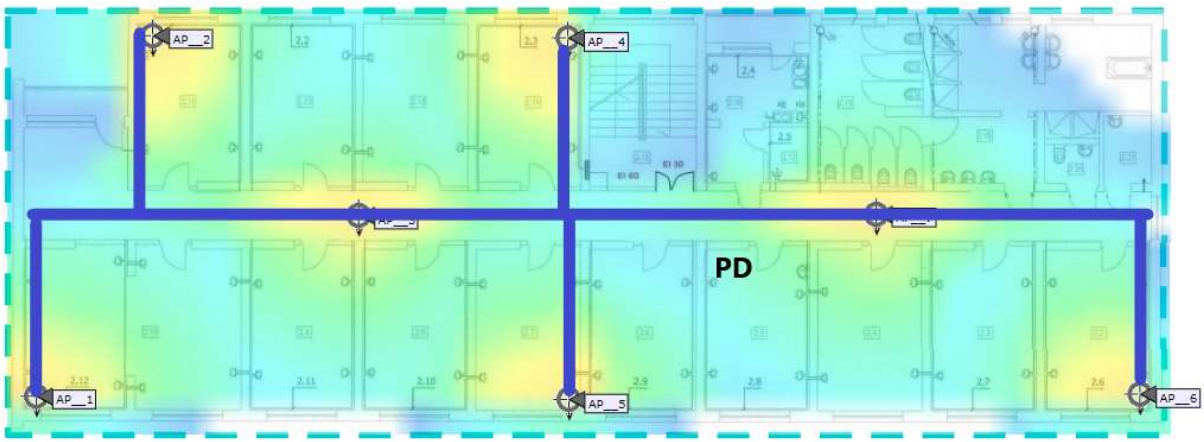


Rysunek 39: Planowanie dla częstotliwości 2,4GHz



Rysunek 40: Planowanie dla częstotliwości 5GHz

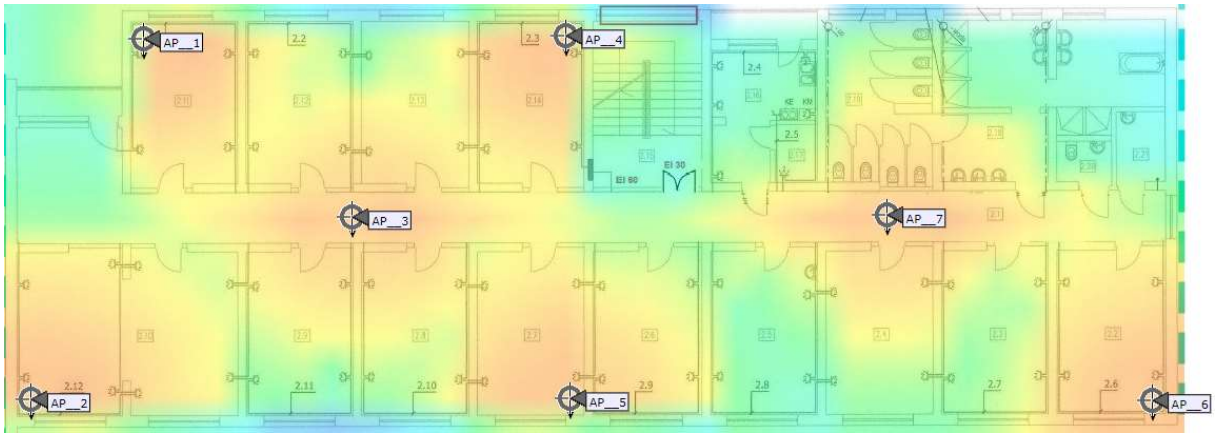
Planowane trasy kablowe



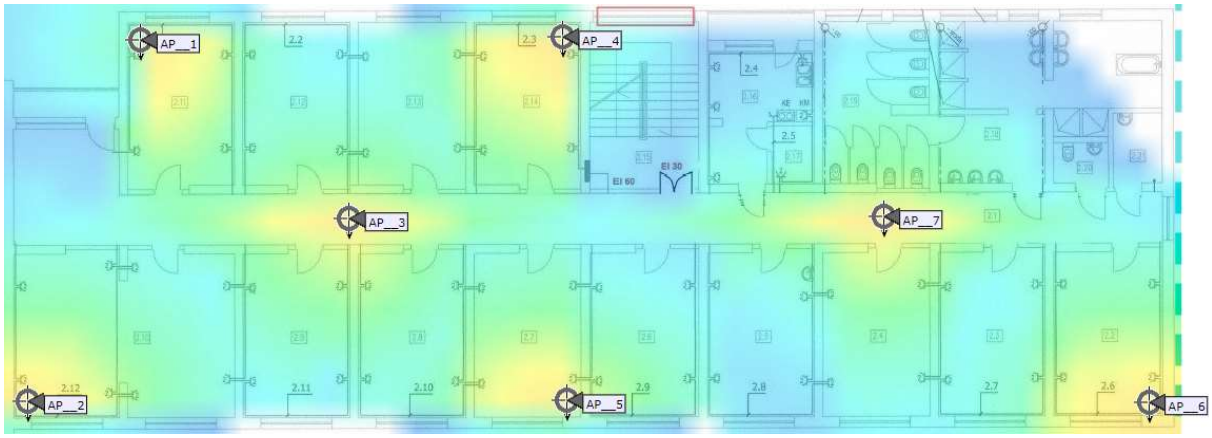
Rysunek 41: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	35
AP2	35
AP3	25
AP4	25
AP5	25
AP6	25
AP7	10

Budynek A2



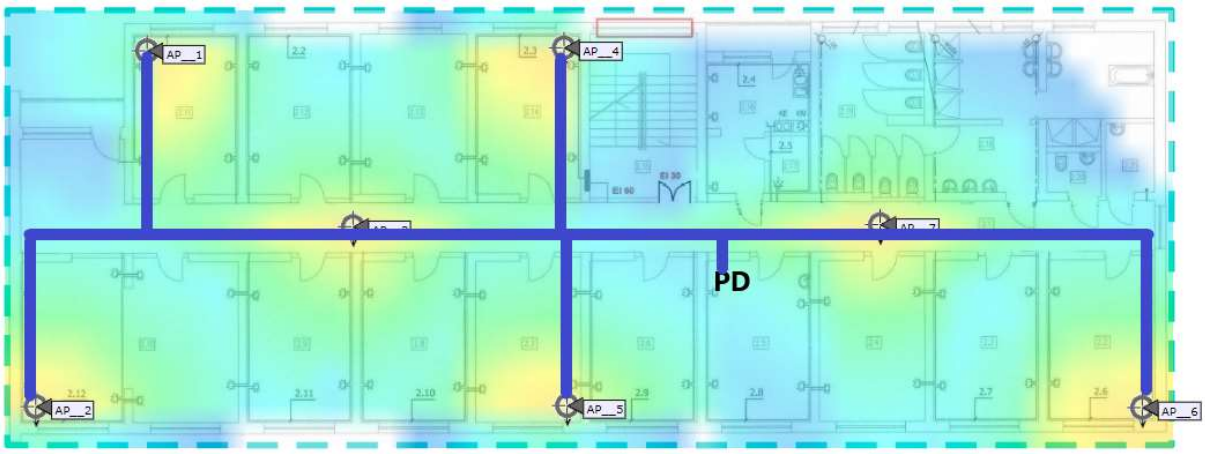
Rysunek 42: Planowanie dla częstotliwości 2,4GHz



Rysunek 43: Planowanie dla częstotliwości 5GHz

W budynku A na każdej kondygnacji zaproponowanych zostało po siedem access pointów. Na każdym piętrze wszystkie access potny zejdą się do punktu dystrybucyjnego znajdującego się na danym piętrze w pomieszczeniu socjalnym. Kable zostaną poprowadzone korytarzem.

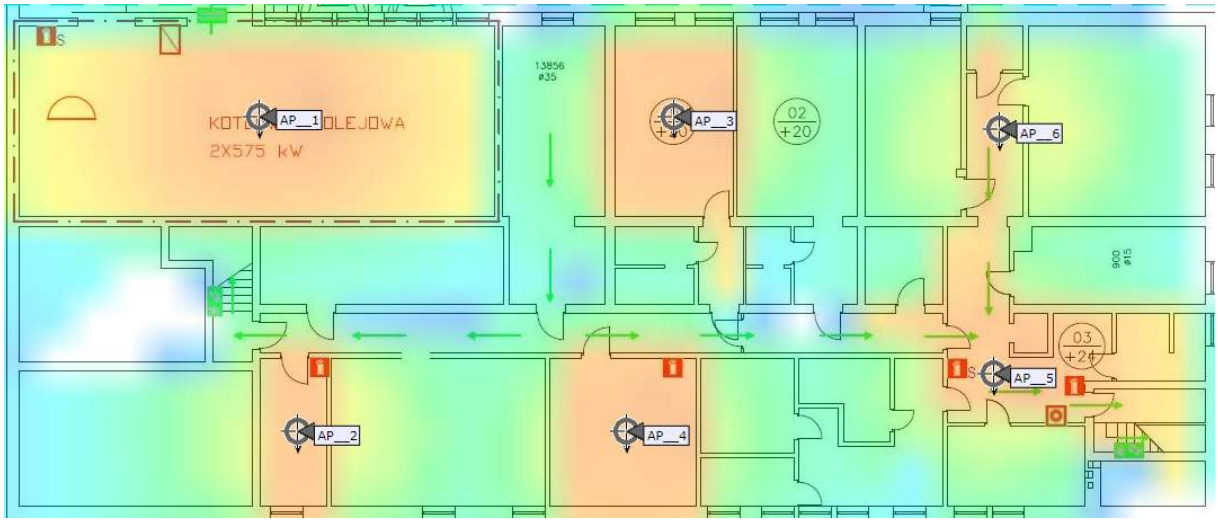
Planowane trasy kablowe



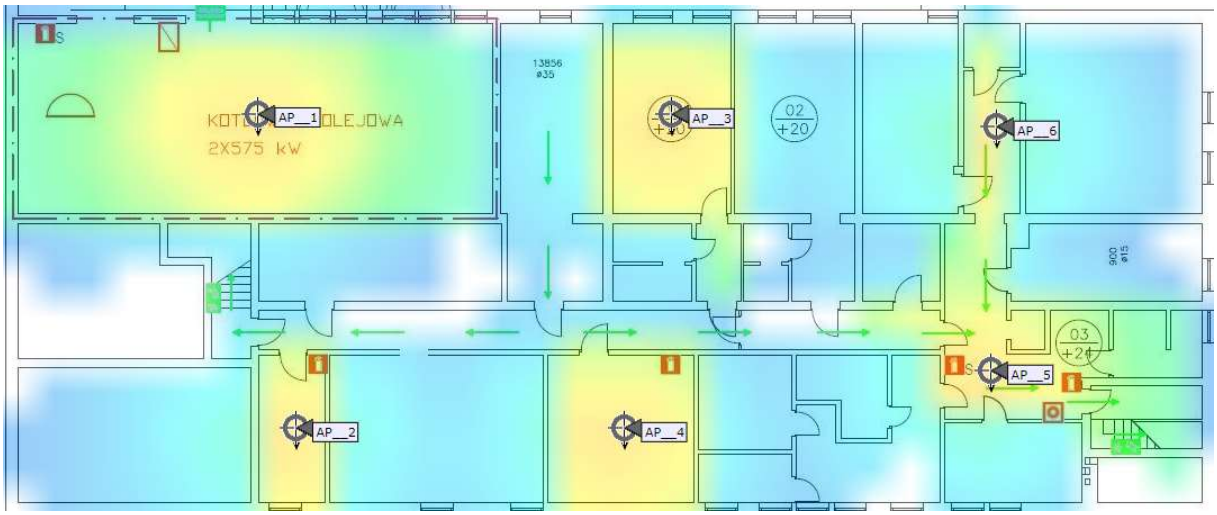
Rysunek 44: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	35
AP2	35
AP3	25
AP4	25
AP5	25
AP6	25
AP7	10

Budynek B -1



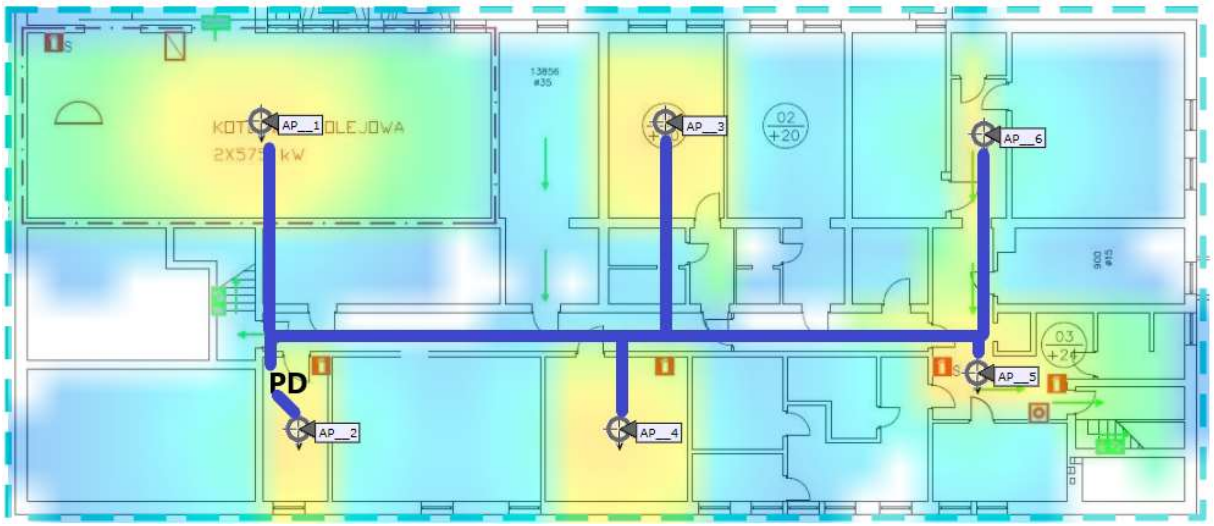
Rysunek 45: Planowanie dla częstotliwości 2,4GHz



Rysunek 46: Planowanie dla częstotliwości 5GHz

W piwnicy budynku B po konsultacjach z pracownikami DPS zaproponowanych jest sześć sztuk urządzeń. Proponujemy zejść z okablowaniem w części piwnicznej do małego punktu dystrybucyjnego w pomieszczeniu biurowym, tam, gdzie przewidziany jest AP2.

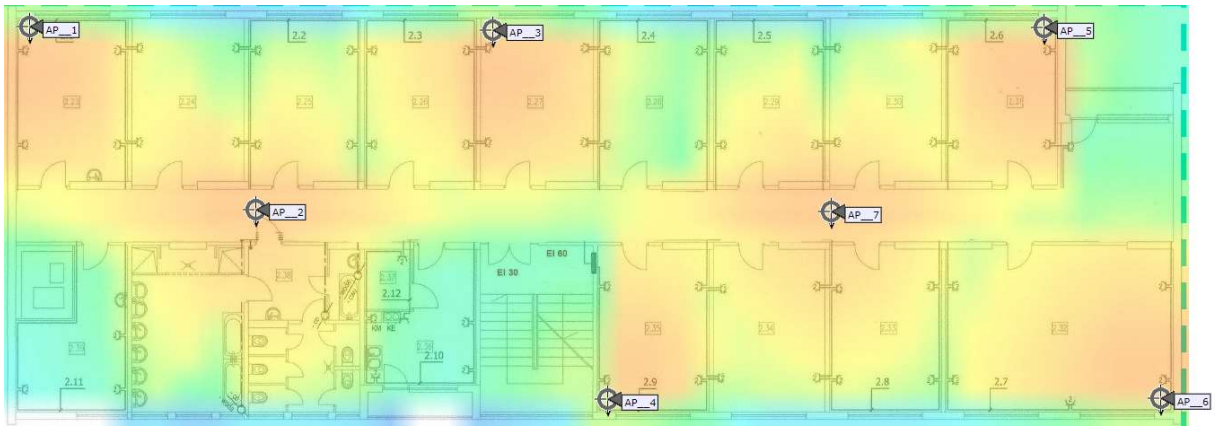
Planowane trasy kablowe



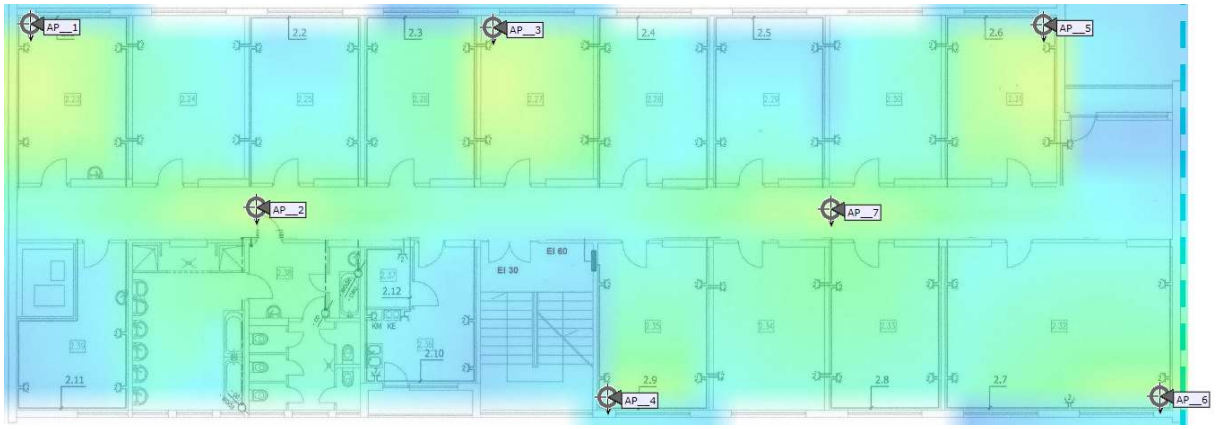
Rysunek 47: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	15
AP2	5
AP3	25
AP4	25
AP5	40
AP6	40

Budynek D1

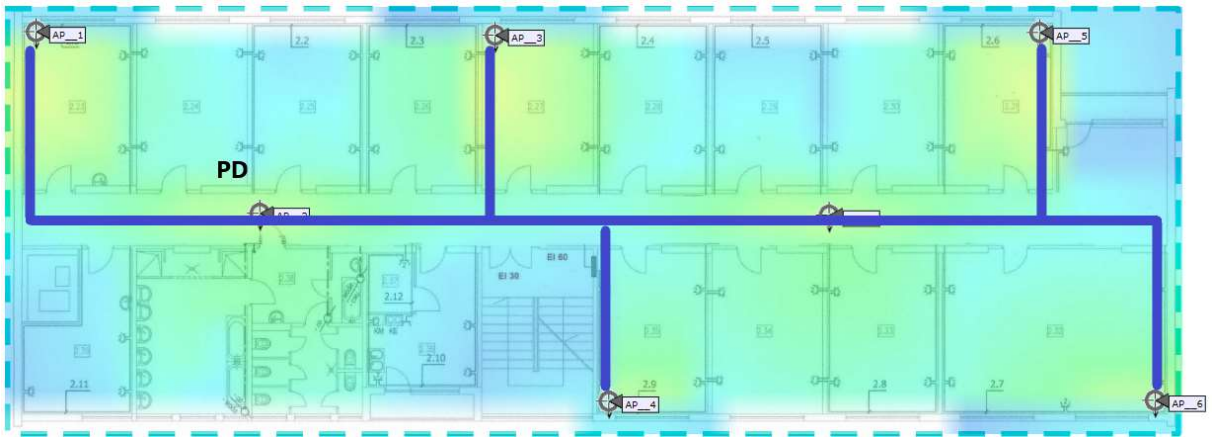


Rysunek 48: Planowanie dla częstotliwości 2,4GHz



Rysunek 49: Planowanie dla częstotliwości 5GHz

Planowane trasy kablowe

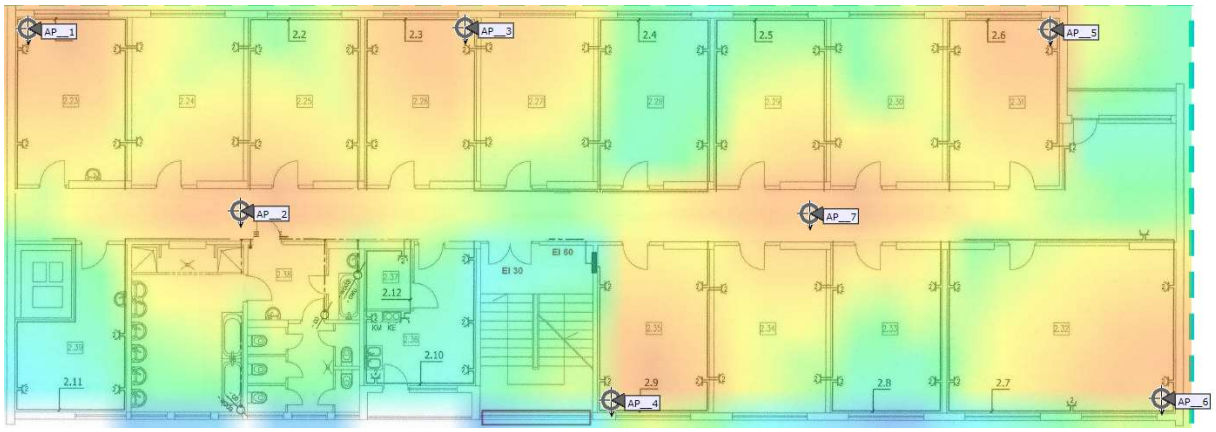


Rysunek 50: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	20
AP2	5
AP3	20
AP4	25

AP5	40
AP6	45
AP7	25

Budynek D2

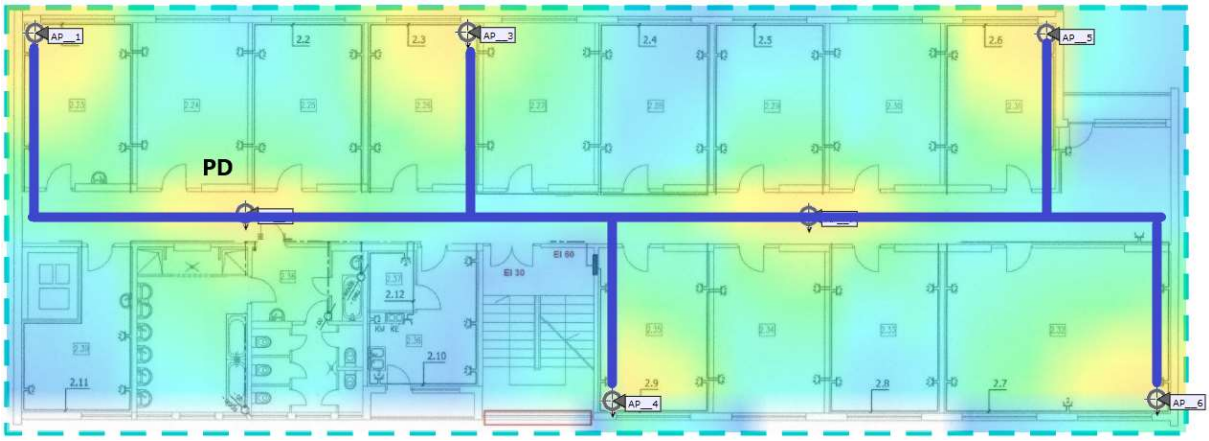


Rysunek 51: Planowanie dla częstotliwości 2,4GHz

Rysunek 52: Planowanie dla częstotliwości 5GHz

Na każdej kondygnacji budynku D zaproponowanych zostało po siedem access pointów. Tak samo jak w przypadku budynku A okablowanie zostanie poprowadzone korytarzami do punktów dystrybucyjnych znajdujących się w pomieszczeniach socjalnych.

Planowane trasy kablowe

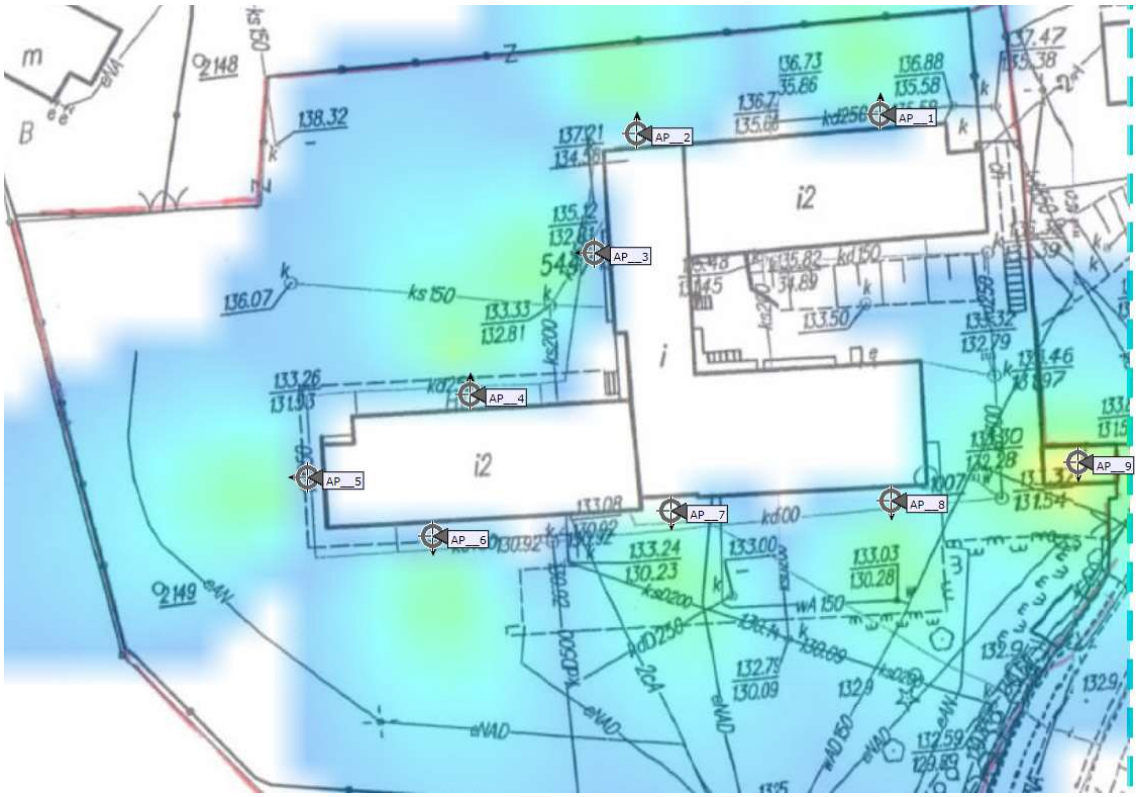


Rysunek 53: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	20
AP2	5
AP3	20
AP4	25
AP5	40
AP6	45
AP7	25

Obszar zewnętrzny + budynek ochrony na wejściu

Rysunek 54: Planowanie dla częstotliwości 2,4GHz



Rysunek 55: Planowanie dla częstotliwości 5GHz

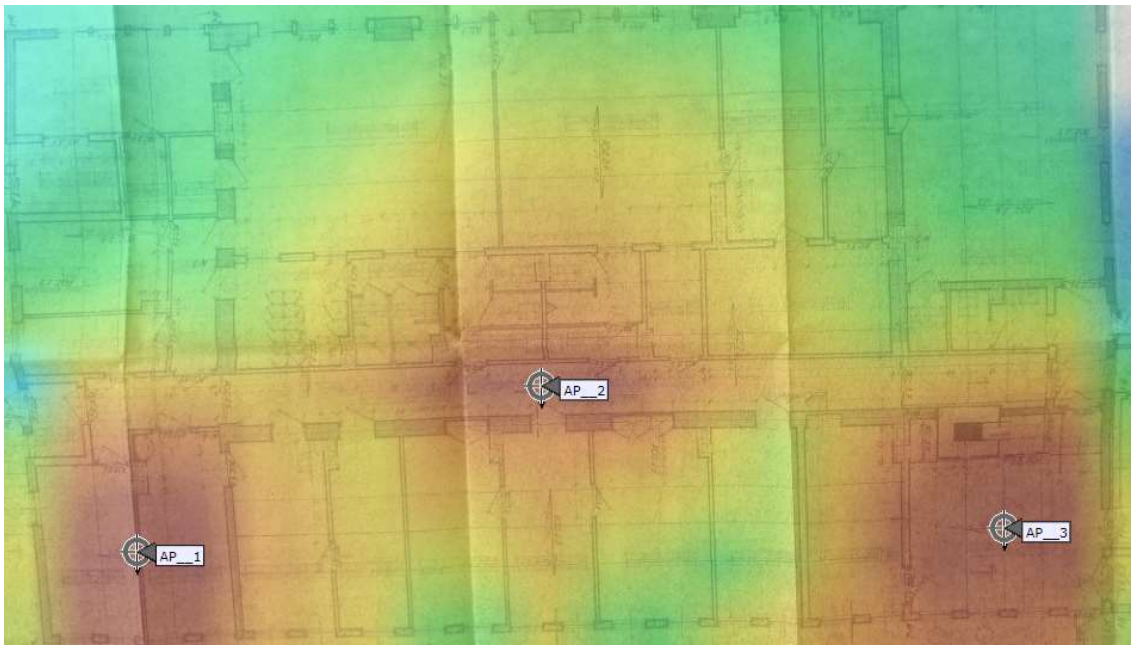
W celu doświetlenia obszary zewnętrznego w wokół budynku głównego zaproponowanych zostało osiem access pointów. Będą one zamocowane do elewacji budynku. AP9 jeżeli nie przekroczy to kosztów całego projektu powinien zostać zainstalowany w strażnicy przy wejściu a jego okablowanie doprowadzone z budynku głównego. Okablowanie z każdego punktu powinno zejeść się do najbliższego punktu dystrybucyjnego.

Rysunek 56: Całe okablowanie zejdzie się w korytkach do najbliższego punktu PD, wzdłuż styku ścian/sufitu.

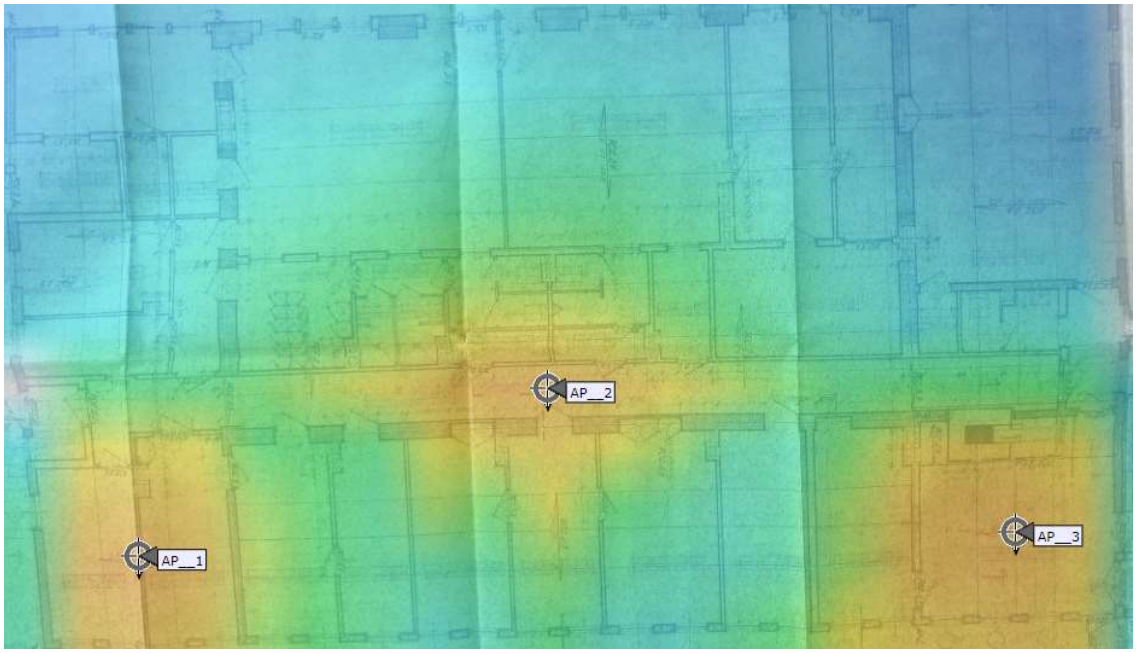
Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	50
AP2	15
AP3	15
AP4	35
AP5	40
AP6	35
AP7	40
AP8	60
AP9	90

Budynek administracji

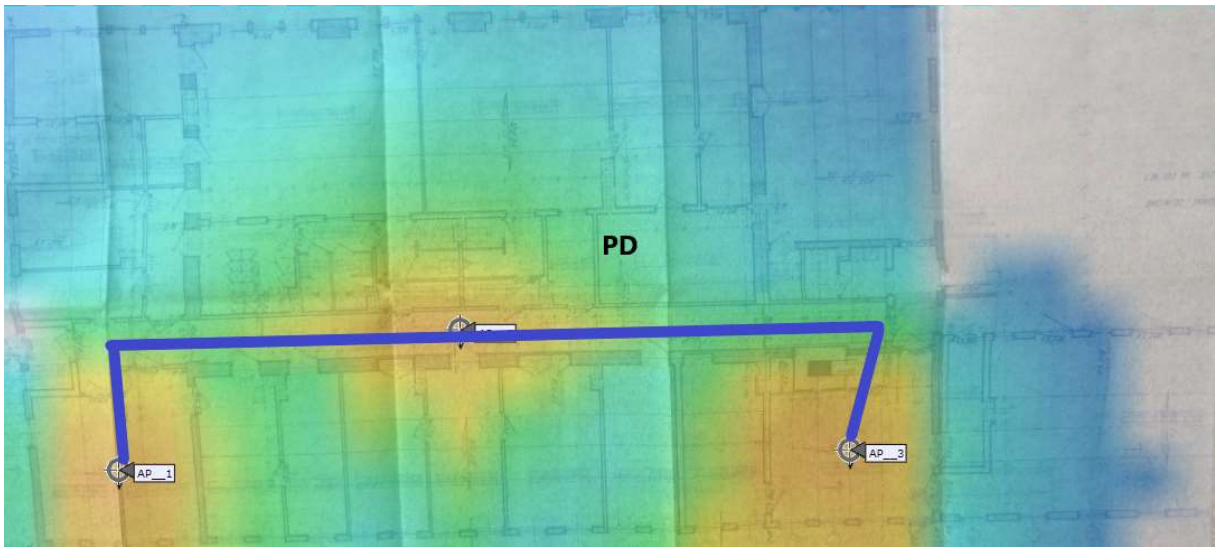


Rysunek 57: Planowanie dla częstotliwości 2,4GHz



Rysunek 58: Planowanie dla częstotliwości 5GHz

W części biurowej zostały zaproponowane trzy access pointy. Całe okablowanie powinno zejść się do małej serwerowni w pomieszczeniu xero.



Rysunek 59: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Planowane trasy kablowe

Numer AP	Szacowana długość okablowania [m]
AP1	40
AP2	20
AP3	20

Podsumowanie

Liczba wszystkich urządzeń:

- Kontroler sieci bezprzewodowej: 1.
- Access pointy: 70, w tym 8 zewnętrznych.
- Switche: 1 core, 10 access.
- Firewall: 1.

Na etapie projektowania oraz instalacji należ mieć na uwadze:

- Brak jakiejkolwiek infrastruktury, z której można by skorzystać w czasie projektowania, czy instalacji nowej sieci.
- Brak istniejących tras kablowych oraz przepustów.
- Brak doprowadzonego zasilania do wybranych punktów dostępowych.
- Niezbędne będzie zabezpieczenie wszystkich urządzeń przed niepowołanym dostępem.
- Brak przygotowanego pomieszczania pod serwerownię.
- Brak połączenia budynku głównego z budynkiem biurowym.
- Równocześnie problemem dla wprowadzenia nowoczesnych usług może okazać się niedostatek parametrów połączenia internetowego oraz brak możliwości redundancji w tym zakresie.

Minimalne wymagania techniczne sprzętu

Kontroler sieci bezprzewodowej	• urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
	  ○ zarządzanie politykami bezpieczeństwa
	  ○ wykrywanie zagrożeń w sieci bezprzewodowej
	  ○ zarządzanie pasmem radiowym
	  ○ zarządzanie mobilnością
	  ○ zarządzanie jakością transmisji
	• obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji
	• min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45)
	• opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
	• obsługa ruchu tunelowanego
	• obsługa min. 1000 klientów sieci bezprzewodowej
	• zarządzanie pasmem radiowym punktów dostępowych:
	  ○ automatyczna adaptacja do zmian w czasie rzeczywistym
	  ○ optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
	  ○ dynamiczne przydzielanie kanałów radiowych
	  ○ wykrywanie, eliminacja i unikanie interferencji
	  ○ równoważenie obciążenia punktów dostępowych
	  ○ tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
	  ○ automatyczna dystrybucja klientów pomiędzy punkty dostępowe
	  ○ mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
	  ○ dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
	• mapowanie SSID do segmentów VLAN w sieci przewodowej
	• możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
	• automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
	• obsługa mechanizmów bezpieczeństwa:
	  ○ 802.11i, WPA3, WPA2, WPA, WEP
	  ○ 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
	  ○ obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
	• kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
	• obsługa dostępu gościnnego (IPv4 i IPv6)

	○ przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) ○ przekierowanie użytkowników do strony logowania na zewnętrznym serwerze • współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych • obsługa NTP wersji 4 (IPv4 oraz IPv6) • obsługa Hotspot 2.0 • obsługa redundancji rozwiązania
Access point wewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników

	○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych
Access point zewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax

	○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID

	○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • dla access pointów zewnętrznych: ○ zgodność z IP67 ○ min. praca przy temperaturach między -35^{o}C a 60^{o}C • certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint
Switch core	• Typ i liczba portów: ○ Min: 12 SFP/SFP+ • Opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb): ○ min. 4x1G SFP ○ min. 4x1/10G SFP+ • Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: ○ Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U ○ Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość tworzenia stosów • Parametry wydajnościowe: ○ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) ○ Bufor pakietów – min.: 8MB

	○ Pamięć DRAM – min.: 4GB ○ Pamięć flash – min.: 8GB ○ Obsługa ▪ min. 3.000 sieci VLAN ▪ min.: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: ○ Obsługa protokołu STP • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Mechanizmy związane z bezpieczeństwem sieci: ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL ○ Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC ○ Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 ○ Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard • Obsługa protokołów routingu: ○ Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie ○ Port konsoli ○ Dedykowany port Ethernet do zarządzania out-of-band ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Switch access	• Typ i liczba portów:
	  o min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP
	• Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami)
	• Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
	  o Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
	  o Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
	• Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
	  o Przepustowość w ramach stosu – min.:60Gb/s
	  o min: 4 urządzenia w stosie
	  o Zarządzanie poprzez jeden adres IP
	• Parametry wydajnościowe:
	  o Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
	  o Bufor pakietów – min: 4MB
	  o Pamięć DRAM – min: 1GB
	  o Pamięć flash – min: 2GB
	  o Obsługa
	  ▪ 1024 sieci VLAN
	  ▪ min: 16.000 adresów MAC
	• Obsługa protokołu NTP
	• Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
	  o IEEE 802.1w Rapid Spanning Tree
	• Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
	• Możliwość uruchomienia funkcji serwera DHCP
	• Obsługa protokołów routingu:
	  o Routing statyczny dla IPv4 i IPv6
	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN

	• Zarządzanie
	  ○ Port konsoli
	  ○ Dedykowany port Ethernet do zarządzania out-of-band
	  ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
	  ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
	  ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
	• Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Firewall	• Wymagania Ogólne
	  ○ Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
	  ○ System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
	  ○ System musi wspierać IPv4 oraz IPv6 w zakresie:
	  ▪ Firewall.
	  ▪ Ochrony w warstwie aplikacji.
	  ▪ Protokołów routingu dynamicznego.
	• Redundancja, monitoring i wykrywanie awarii
	  ○ W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
	  ○ Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
	  ○ Monitoring stanu realizowanych połączeń VPN.
	• Interfejsy, Dysk, Zasilanie:
	  ○ System realizujący funkcję Firewall musi dysponować minimum:

	▪ min. 4 portami Gigabit Ethernet RJ-45. ▪ min. 2 gniazdami SFP 1 Gbps. o System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. o System musi być wyposażony w zasilanie AC. • Parametry wydajnościowe: o W zakresie Firewall'a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. o Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps o Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0,5 Gbps. o Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps. • Funkcje Systemu Bezpieczeństwa: o W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. ▪ Kontrola Aplikacji. ▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. ▪ Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). ▪ Funkcja lokalnego serwera DNS ze wsparciem dla DNS • Polityki, Firewall o Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. o System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. ▪ W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. ▪ Możliwość wykorzystania w polityce bezpieczeństwa

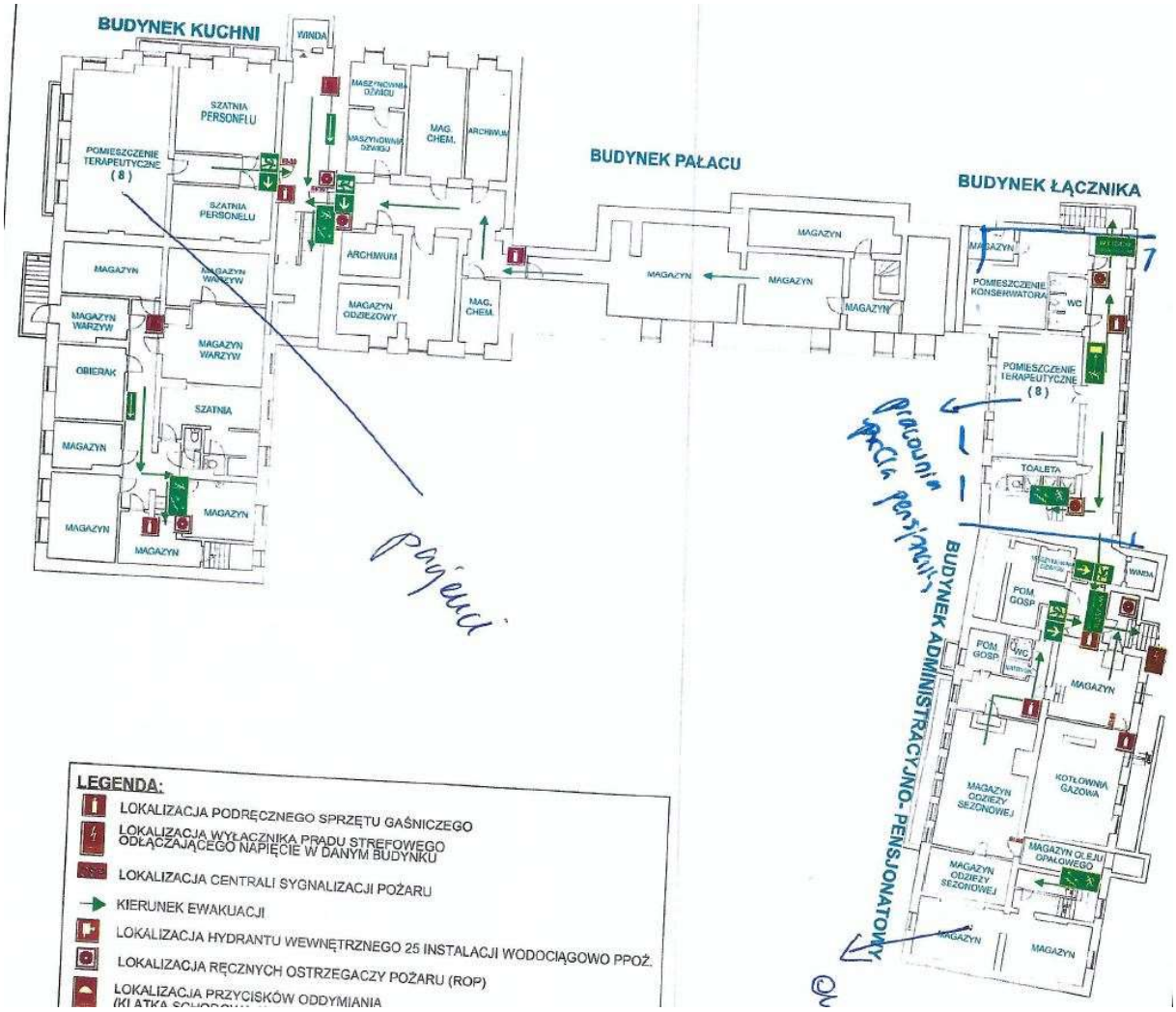
	zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
	• Połączenia VPN
	  ○ System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Wsparcie dla IKE v1 oraz v2.
	  ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	  ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	  ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	  ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	  ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	  ▪ Mechanizm „Split tunneling" dla połączeń Client-to-Site.
	  ○ System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
	  ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
	  ▪ Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
	• Routing i obsługa łączy WAN
	  ○ W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	  ▪ Routingu statycznego.
	  ▪ Policy Based Routingu.
	  ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	• Ochrona przed malware
	• Ochrona przed atakami
	  ○ Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
	• Kontrola aplikacji

	• Kontrola WWW • Zarządzanie • Logowanie • Serwisy i licencje ○ W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. • Gwarancja oraz wsparcie
Okablowanie etherentowe	• Min. Cat 6 ekranowana

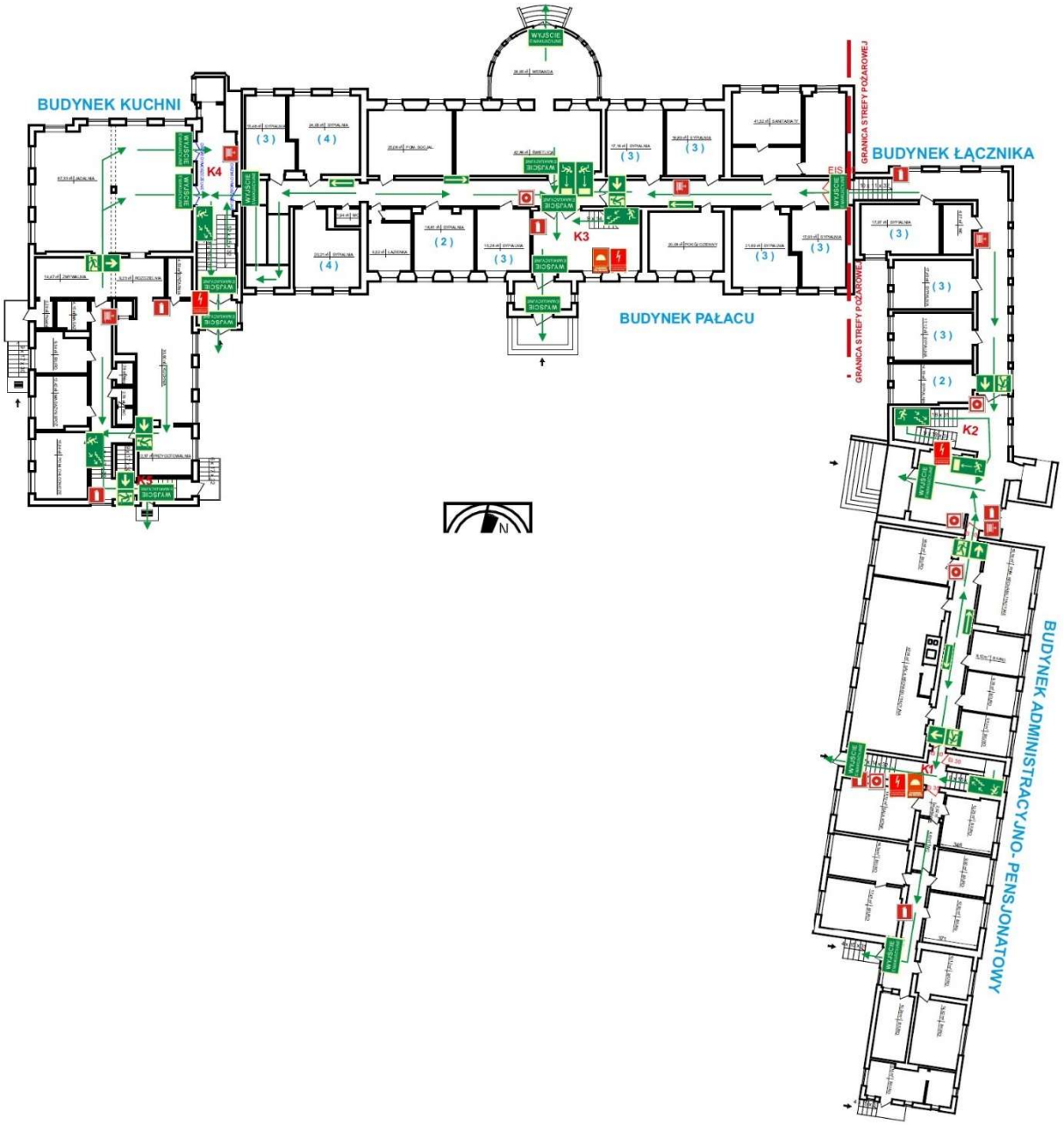
Załącznik nr 3 DPS Nowe Bielice

DPS Nowe Bielice składa się z trzech obszarów: Budynek główny, budynek Maria oaz budynek pralnia. Cześć budynku głównego jest częścią pałacową i podlega pod ochronę konserwatorską.

Plany budynków

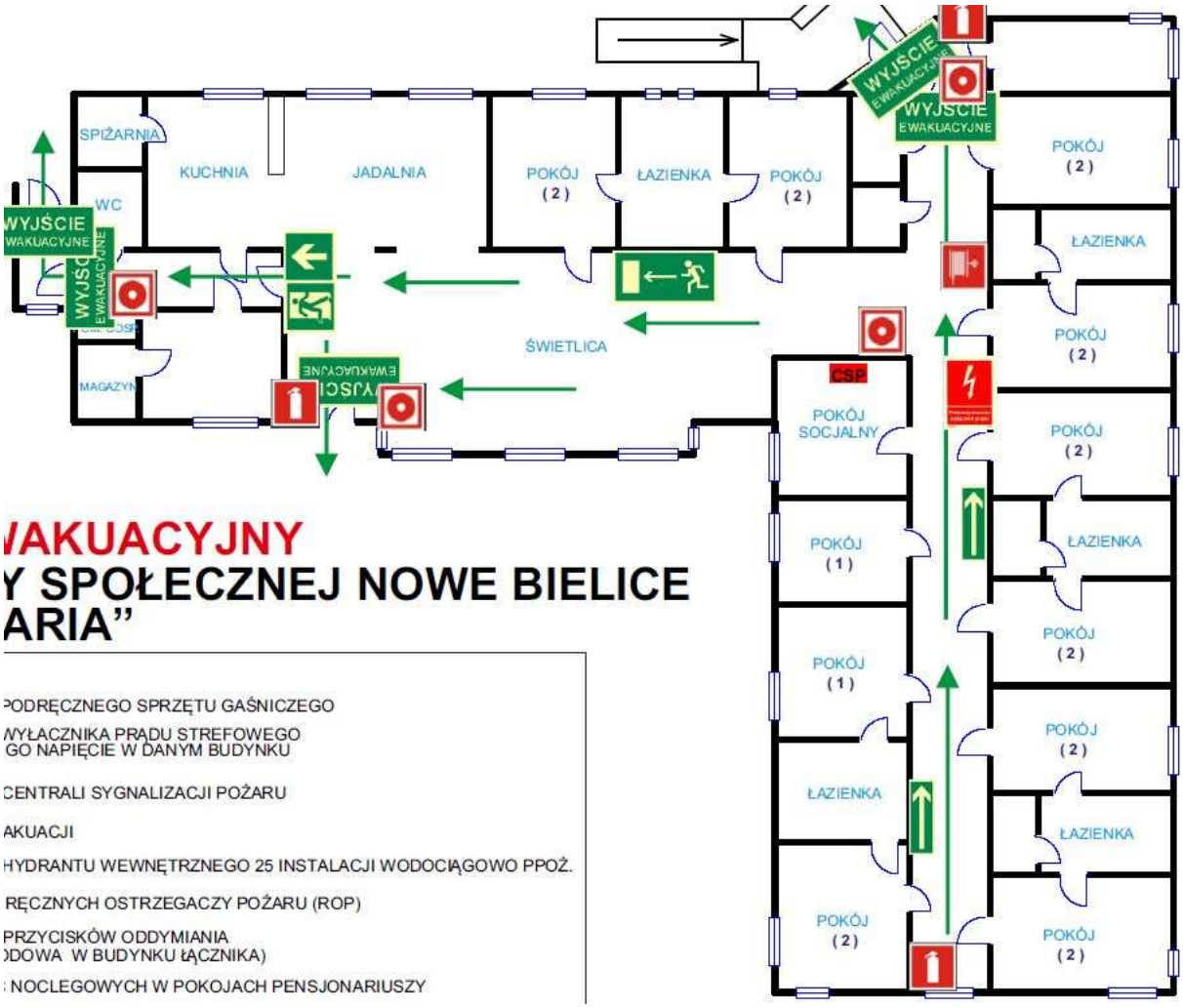


Rysunek 1: Plan piwnicy



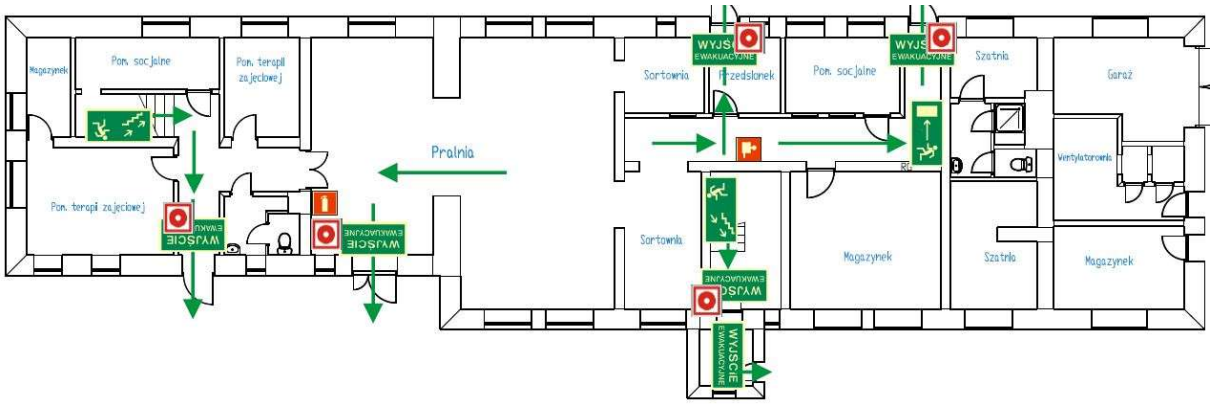
Rysunek 2: Plan parteru

Rysunek 3: Plan pierwszego pietra

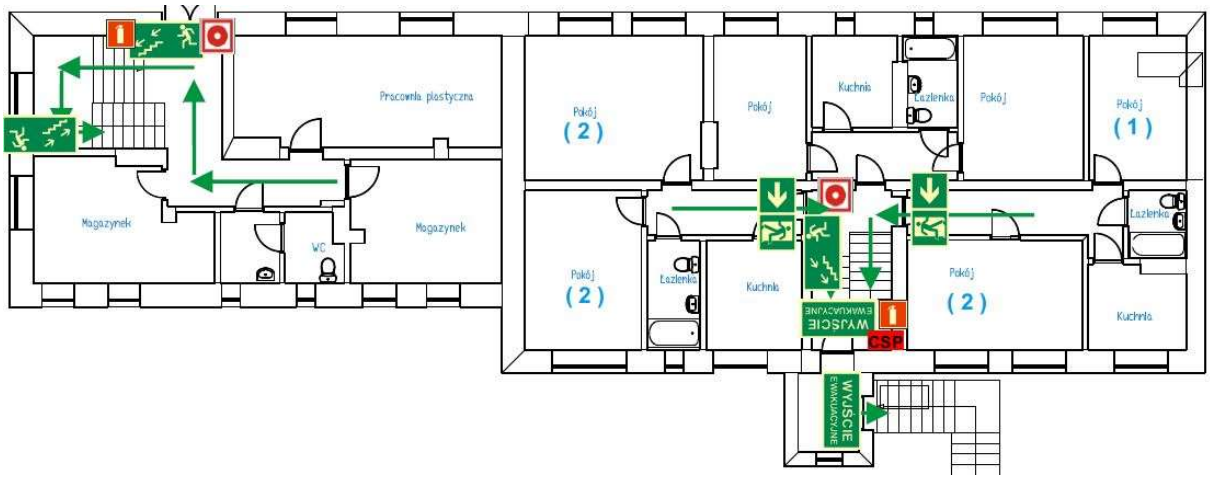


Rysunek 4: Plan budynku Maria

Budynek pralni



Rysunek 5: Plan parteru

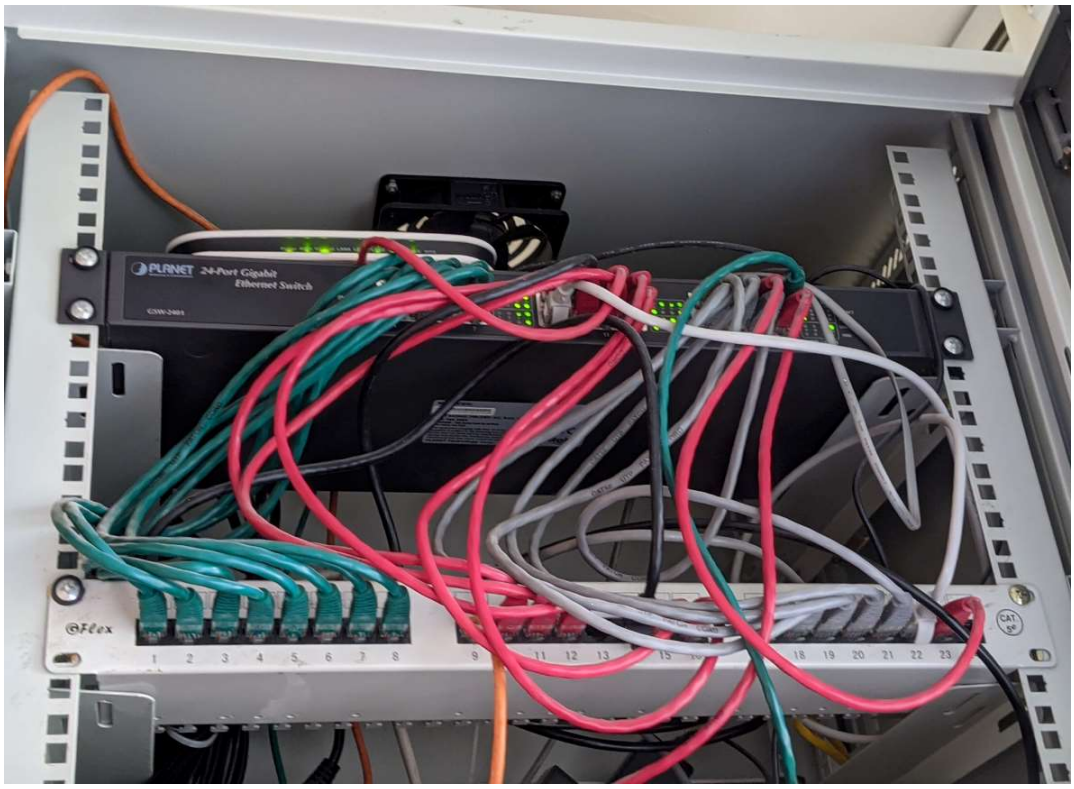


Rysunek 6: Plan pierwszego piętra

Obecny stań sieci

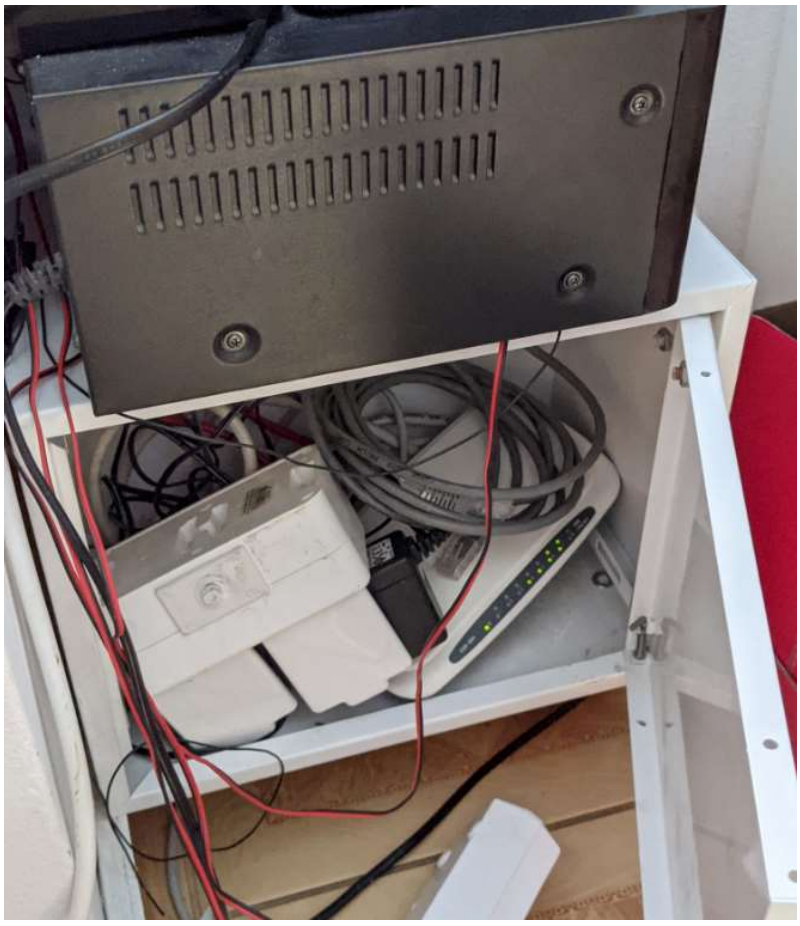
W obecnej chwili w Nowych Bielicach jest rozprowadzona sieć LAN oraz WLAN, ale tylko w obrębie pomieszczeń administracyjnych. Należy również zaznaczyć, że sieć nie jest doprowadzona do wszystkich pracowników. Brak jakiejkolwiek infrastruktury sieciowej, z której mogliby skorzystać mieszkańcy. Internet jest doprowadzony przez linię telefoniczną. W budynku administracyjnym jest szafa rack, w której znajduje się switch dla części biurowej. W innych częściach sieć LAN jest rozprowadzona za pomocą radiolinii i wykorzystuje urządzenia domowe takie jak małe niezarządzalne switche, wbudowane access pointy w routery. W budynku nie ma wyznaczonych punktów dystrybucyjnych, czy głównej serwerowni, brak infrastruktury ethernetowej oraz światłowodowej. Jedyna istniejąca infrastruktura jest to monitoring, który jest odrębny i nie podlegał audytowi. Ze względu na przyszłe prace i chęć wprowadzenia zaawansowanego systemu sieci bezprzewodowej niezbędne będzie wybudowanie całkowicie nowej infrastruktury sieci LAN. Żadne z obecnie używanych urządzeń nie będzie się nadawać do przyszłego wykorzystania.

Rysunek 7: Serwerownia w budynku administracyjnym, szafa górna to LAN, a dolna to monitoring



Rysunek 8: Szafa rack w części administracyjnej

Rysunek 9: Szafa z monitoringiem



Rysunek 10: Szafa pośrednia znajdująca się w biurach kuchni

Rysunek 11: Szafa w kuchni, która jest zakończeniem radiolinii

Rysunek 12: Podłączenie budynku Maria

Rysunek 13: Podłączenie budynku Maria

Rysunek 14: Podłączenie budynku Maria

Rysunek 15: Radiolinia do budynku pralni

Rysunek 16: Radiolinia do części kuchennej

Rysunek 17: Radiolinia do części kuchennej

Obecny stan sieci WLAN

AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
	#8		8c:5a:c1:aa:69:69	1/40MHz	300	WPA2	n	7	7	6	0	2
CyfrowyPolsat	#11		EdimaxTech:e7:a4:8e	10/40MHz	300	WPA2	n	7	7	7	0	1
dps	#7		RealtekSem:42:45:f8	8/40MHz	300	WPA2	n	6	7	4	0	2
DWR-116_E36FC2	#10		DLinkIntl:e3:6f:c3	10/40MHz	300	WPA2	n	4	4	4	0	1
DWR-116_E5121C	#5		DLinkIntl:e5:12:1d	9/40MHz	300	WPA2	n	9	14	6	0	6
Internet_Domowy_6E3E52	#4		AsiatelcoT:6e:3e:52	10/40MHz	300	WPA2	n	1	1	1	0	1
MW40V_492D	#3		f0:51:36:65:49:2d	4/40MHz	300	WPA2	n	17	22	7	0	7
PARTER	#6		ZioncomEle:00:56:cc	7/40MHz	300	WPA2	n	7	9	6	0	3
wlan-test	#1	AP74a0.2f92.c82	CiscoSyste:8b:3e:ff	36	867	WPA2	ac	46	60	16	0	9
wlan-test	#2	AP74a0.2f92.c82	CiscoSyste:8b:3e:f0	11	144	WPA2	n	48	57	28	0	9
WLAN1-M76E81	#9		8c:5a:c1:aa:69:65	1/40MHz	300	WPA2	n	8	8	8	0	1

Rysunek 18: Sieci widoczne w budynku kuchni na pierwszym piętrze

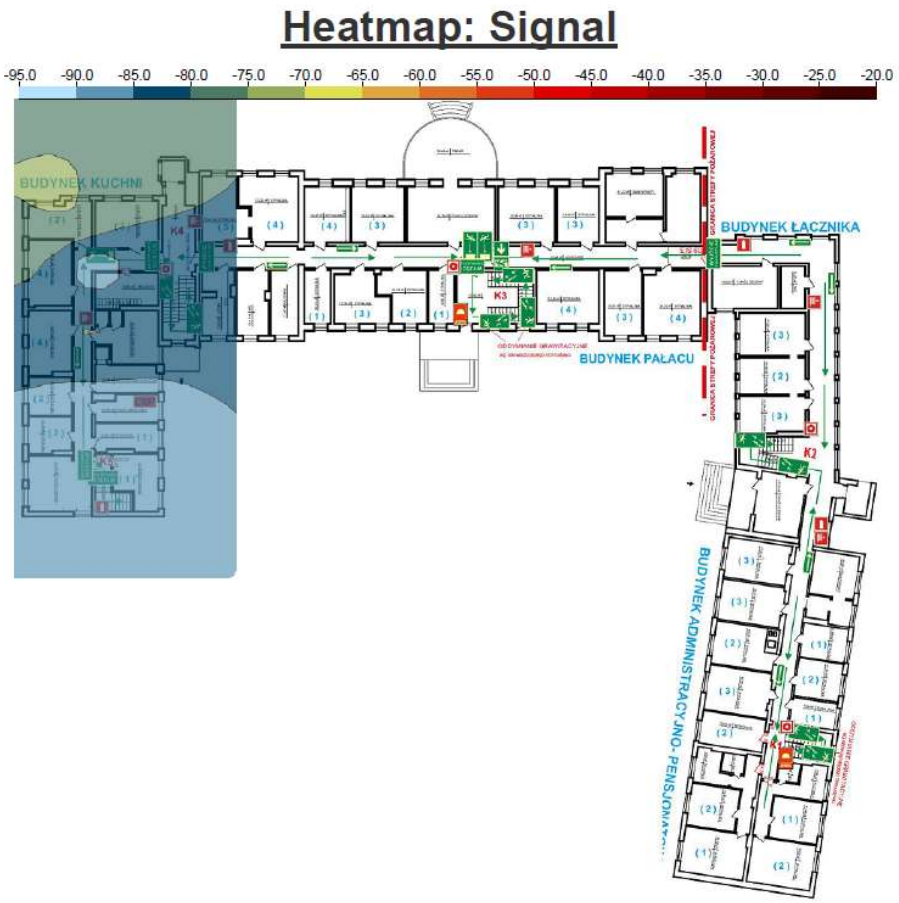


Figure 1: , CyfrowyPolsat, dps, DWR-116_E36FC2, DWR-116_E5121C, Internet_Domowy_6E3E52, MW40V_492D, PARTER, WLAN1-M76E81

Rysunek 19: Sieci propagowane na pierwszym piętrze

AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
anowi 2.4G	#7		64:09:ac:51:cd:44	6	300	WPA2	n	6	6	6	0	1
DIRECT-a0-HP M281 LaserJet	#4		local:d6:6a:6a:ee:ef:a0	6	144	WPA2	n	15	20	6	0	4
dps	#3		RealtekSem:42:45:f8	8/40MHz	300	WPA2	n	18	31	13	0	5
DWR-116_E5121C	#6		DLinkIntl:e5:12:1d	9/40MHz	300	WPA2	n	6	7	5	0	3
MW40V_492D	#5		f0:51:36:65:49:2d	4/40MHz	300	WPA2	n	6	6	6	0	1
wlan-test	#1	AP74a0.2f92.c82	CiscoSyste:8b:3e:ff	36	867	WPA2	ac	30	42	15	0	5
wlan-test	#2	AP74a0.2f92.c82	CiscoSyste:8b:3e:f0	11	144	WPA2	n	26	49	10	0	9

Rysunek 20: Sieci widoczne w części pałacowej na pierwszym piętrze

Heatmap: Signal

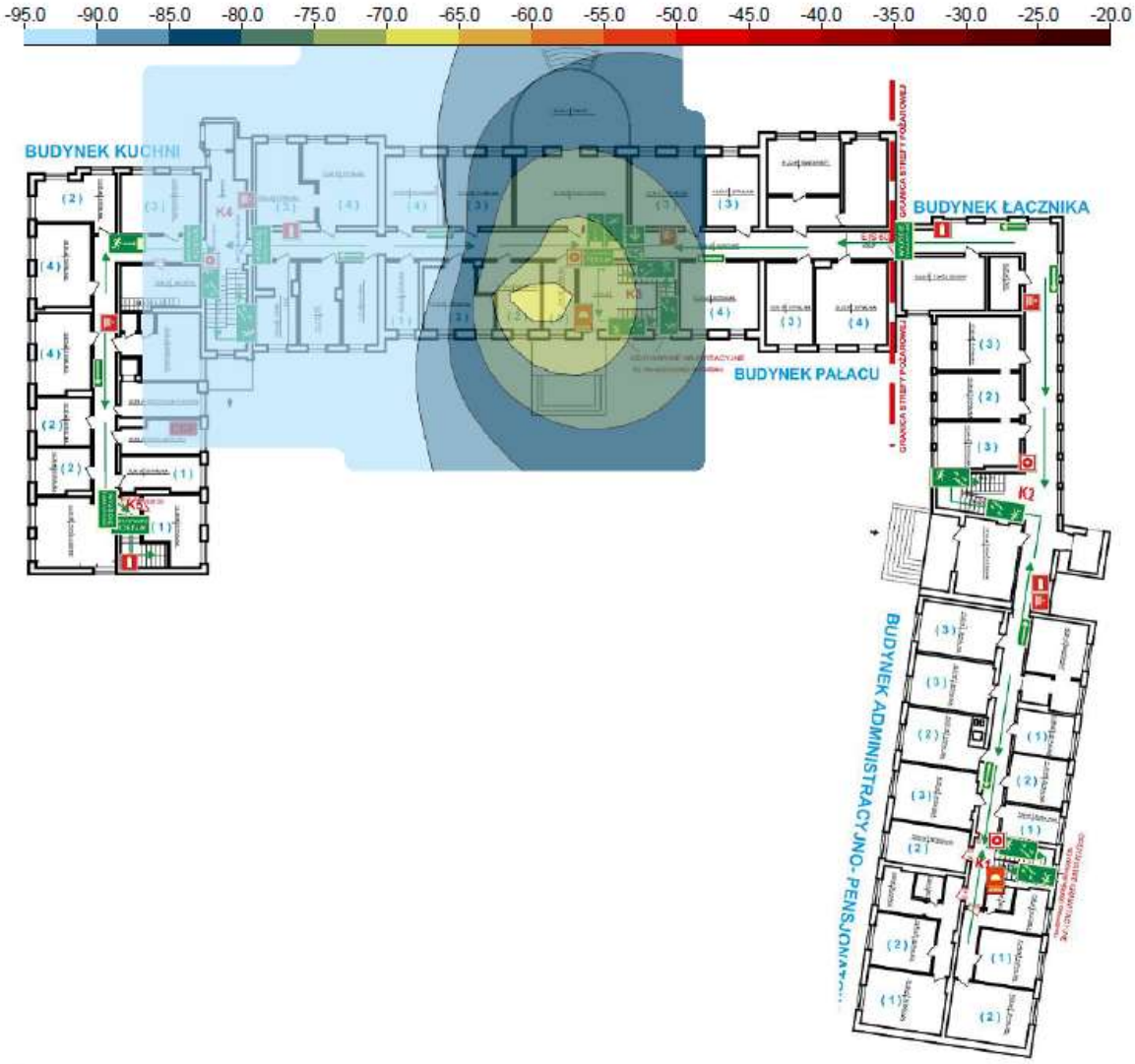
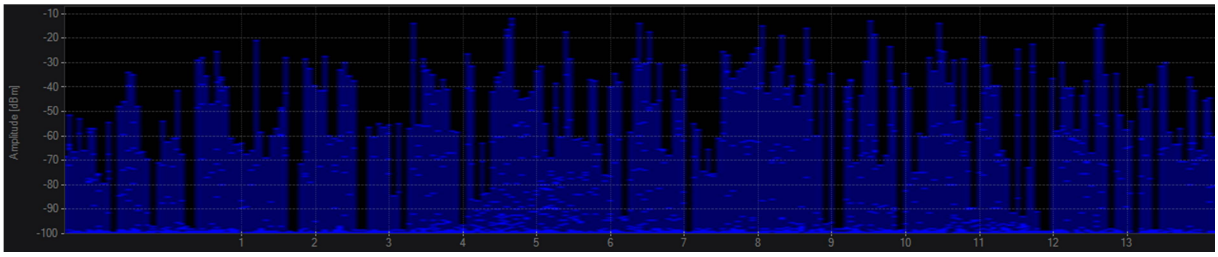


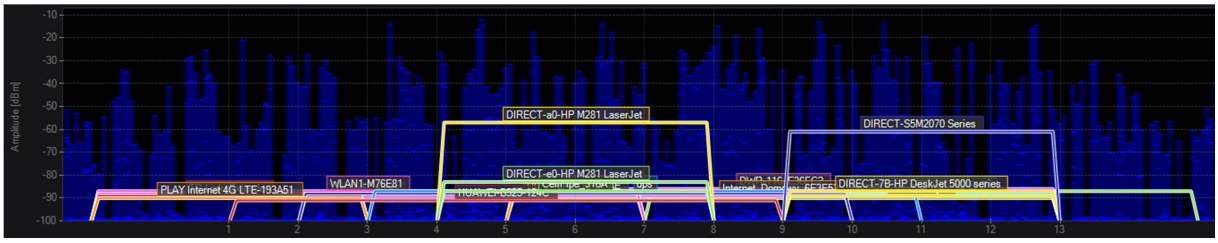
Figure 1: anowi 2.4G, DIRECT-a0-HP M281 LaserJet, dps, DWR-116_E5121C, MW40V_492D

Rysunek 21: Sieci propagowane na pierwszym piętrze

Pomiary zakłóceń w części biurowej



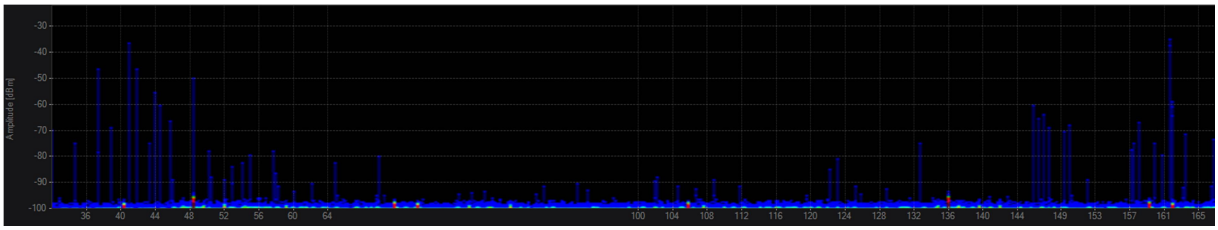
Rysunek 22: Pomiar widma w pąśmie 2,4GHz



Rysunek 23: Pomiar widma w pąśmie 2,4GHz z zaznaczonymi sieciami

ESSID	AP Alias	Channels	Signal Strength (dBm)	BSSID Count	Security	Max Rate (Mbps)	Vendors	802.11
DWR-116_E5121C		9+13	-87	1	WPA2-Personal	300,0	D-Link International	b, g, n
Internet_Domowy_6E3E52-EXT		11	-88	1	WPA2-Personal	144,4	D-Link International	b, g, n
PARTER		8-4	-89	1	WPA2-Personal	300,0	Zioncom Electronics (Shenzhen)	b, g, n
		1+5	-88	1	WPA2-Personal	300,0		b, g, n
TP-Link_Extender		1	-89	1	WPA2-Personal	288,9		b, g, n, ac
PLAY Internet 4G LTE-193A51		1	-90	1	WPA2-Personal	144,4	zte corporation	b, g, n
DomSieciAjKo		11	-89	1	WPA2-Personal	144,4	Tp-Link Technologies Co.,Ltd.	b, g, n
HUAWEI-B525-124C		7-3	-91	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
DIRECT-S5M2070 Series		11	-61	1	WPA2-Personal	54,0		g
DIRECT-e0-HP M281 LaserJet		6	-83	1	WPA2-Personal	144,4		g, n
CellPipe_916A		6	-87	1	WPA-Personal	54,0		b, g
DIRECT-a0-HP M281 LaserJet		6	-57	1	WPA2-Personal	144,4		g, n
DIRECT-7B-HP DeskJet 5000 series		11	-87	1	WPA2-Personal	144,4		g, n
dps		9-5	-87	1	WPA2-Personal	300,0	Realtek Semiconductor Corp.	b, g, n
HUAWEI-B315-DFAE		8-4	-88	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
dom		1	-89	1	WPA2-Personal	144,4	Tp-Link Technologies Co.,Ltd.	b, g, n
WLAN1-M76E81		1+5	-87	1	WPA2-Personal	300,0		b, g, n
Internet_Domowy_6E3E52		11-7	-89	1	WPA2-Personal	300,0	Asiatelco Technologies Co.	b, g, n
DWR-116_E36FC2		11-7	-86	1	WPA2-Personal	300,0	D-Link International	b, g, n
CyfrowyPolsat		11-7	-90	1	WPA2-Personal	300,0	Edimax Technology Co. Ltd.	b, g, n
MW40V_492D		5-1	-90	1	WPA2-Personal	300,0	TCT mobile ltd	b, g, n

Rysunek 24: Lista widocznych sieci

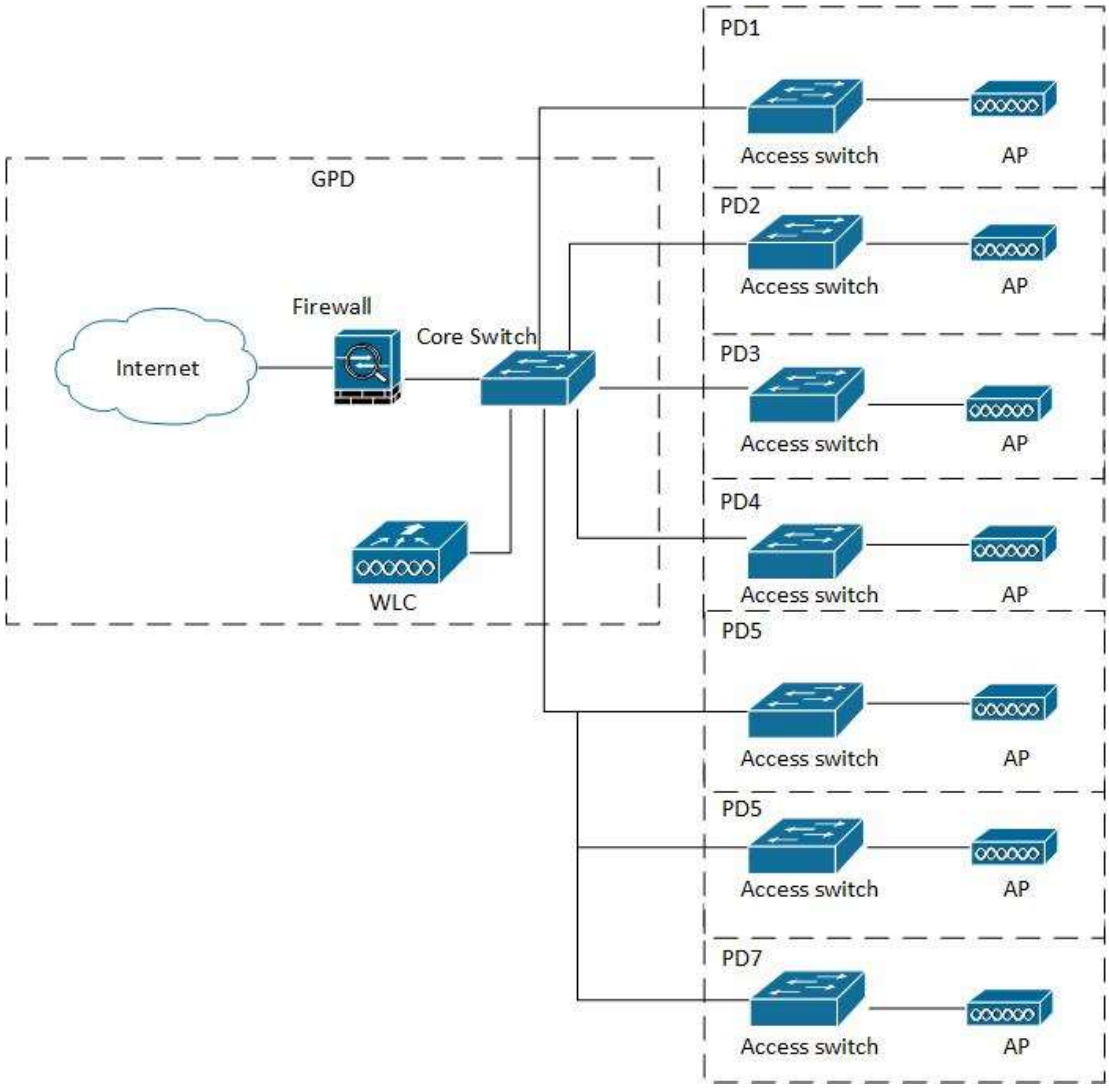


Rysunek 25: Pomiar widma dla pasma 5GHz

Jak widać na powyższych obrazkach jedynie co można zaobserwować do sygnały pochodzące z obecnie propagowanych sieci. Nie występują zakłócenia w tym paśmie. Dla 5GHz można na poziomie szumów zobaczyć małe czerwone zakłócenia, które nie mają żadnego wpływu na sieć bezprzewodową, najprawdopodobniej pochodzą one od operatora telekomunikacyjnego.

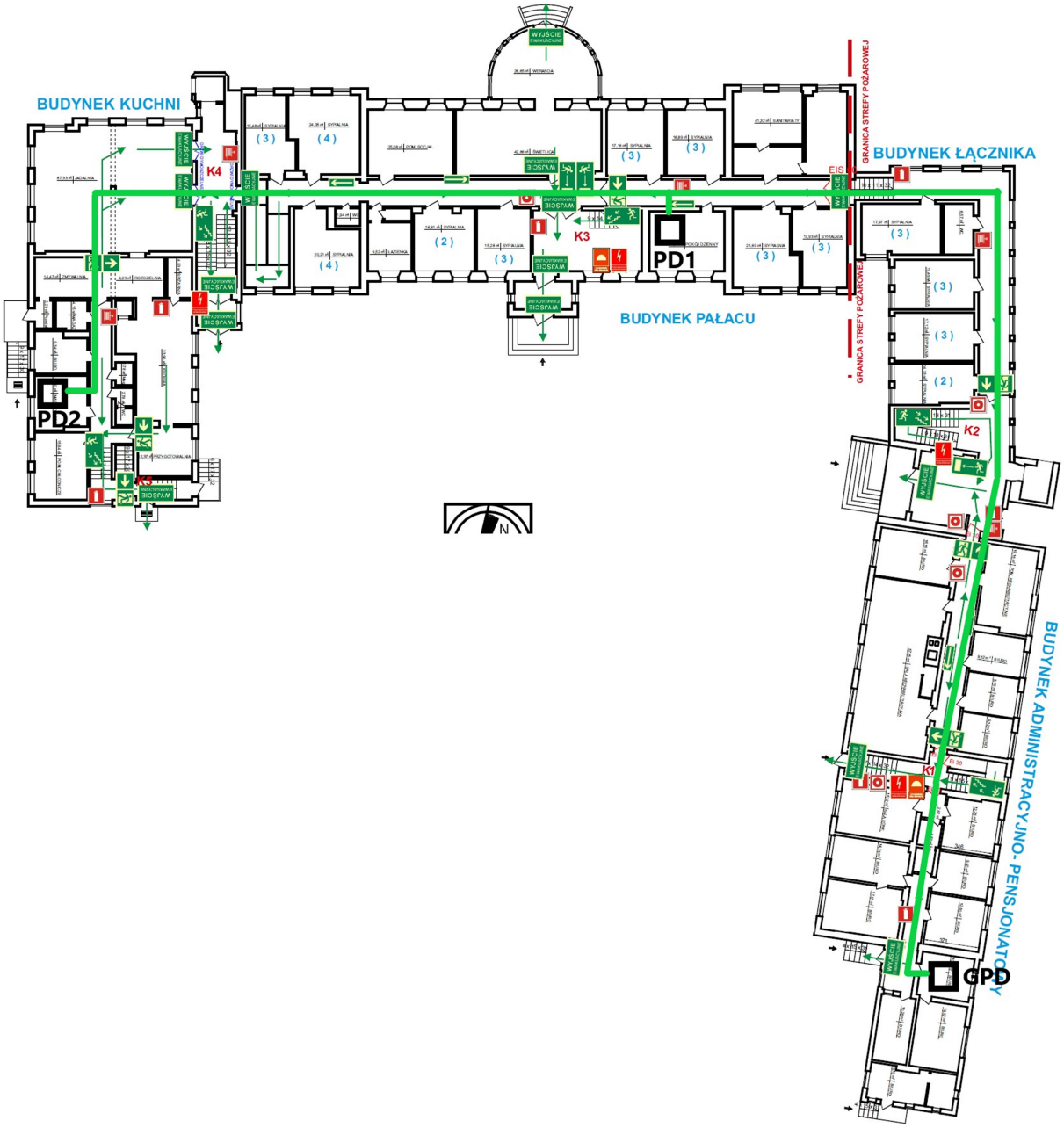
Koncepcja nowej sieci LAN

Nowa sieć LAN powinna zostać zbudowana całkowicie od nowa. W części administracyjnej jest rozprowadzone okablowanie schodzące się do jednego punktu, ale jest to jedyne miejsce, gdzie taka infrastruktura jest. W pozostałej części mieszkalnej oraz pałacowej nie ma żadnej infrastruktury ani ethernetowej, ani światłowodowej. Niezbędne będzie zainstalowanie nowych szaf rackowych. Należy rozprowadzić nowe połączenia światłowodowe pomiędzy wszystkimi punktami pośrednimi, a główną serwerownią. Na styku nowej sieci LAN z Internetem powinno znaleźć się urządzenie zabezpieczające sieć wewnętrzną – firewall. W każdym punkcie dystrybucyjnym należy umieścić przełącznik dostępowy, co najmniej 24 portowy PoE/PoE+ tak, aby podłączyć wszystkie access pointy. Każdy z punktów następnie zostanie podłączony do switcha corowego w głównej serwerowni. Należy przyjąć architekturę gwiazdy, w której każdy pośredni punkt dystrybuujmy będzie bezpośrednio podłączony do GPD. W głównej serwerowni będzie również zainstalowany kontroler sieci bezprzewodowej.



Rysunek 26: Schemat nowej sieci

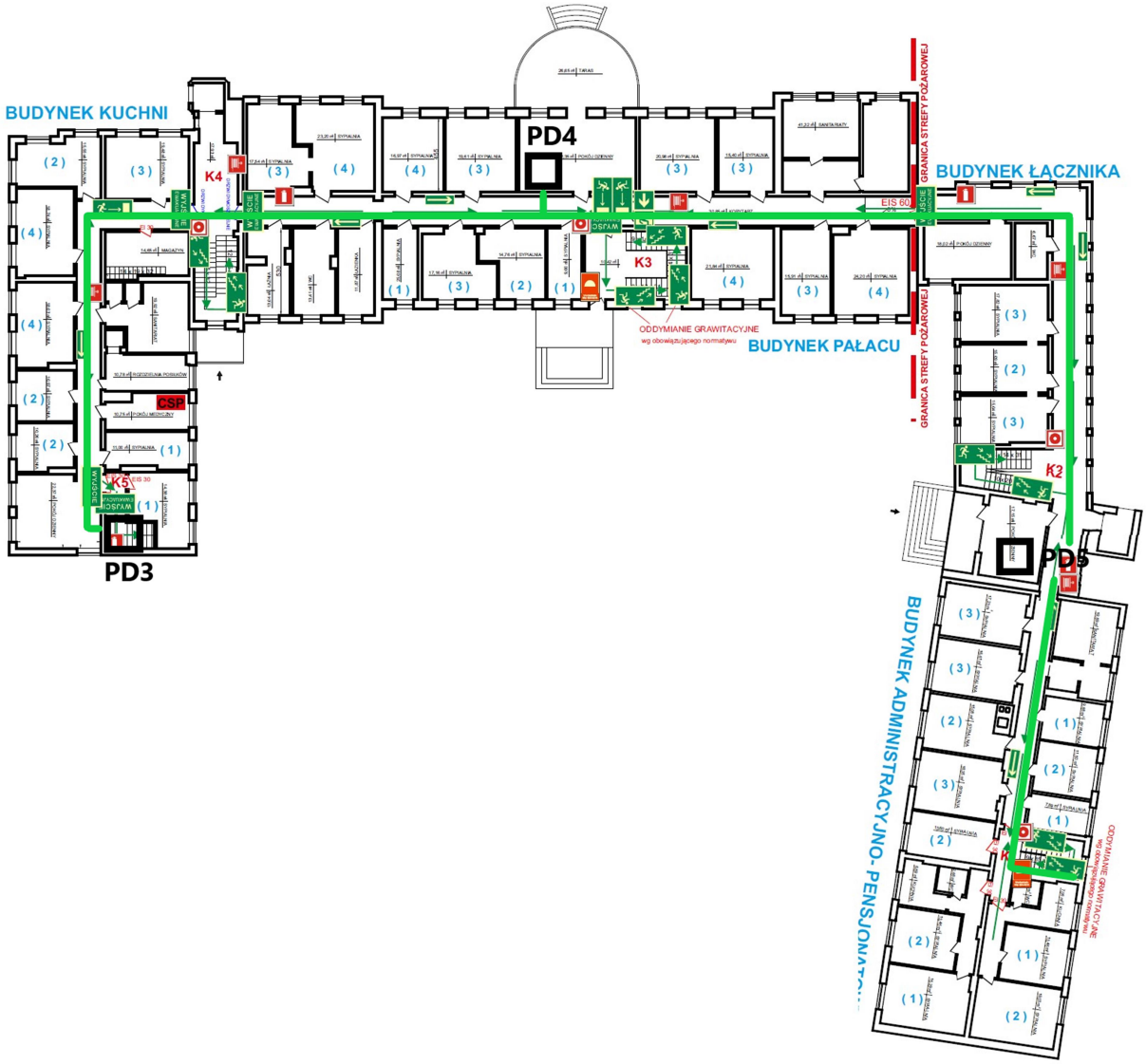
Punkty dystrybucyjne



Rysunek 27: Koncepcja tras światłowodowych i instalacji szaf rackowych na parterze

Lista wszystkich punktów dystrybucyjnych:

- GPD – pomieszczenie xero w części administracyjnej
- PD1 – pokój socjalny
- PD2 – pomieszczenie biurowe w kuchni



Rysunek 28: Koncepcja tras światłowodowych i instalacji szaf rackowych na pierwszym piętrze

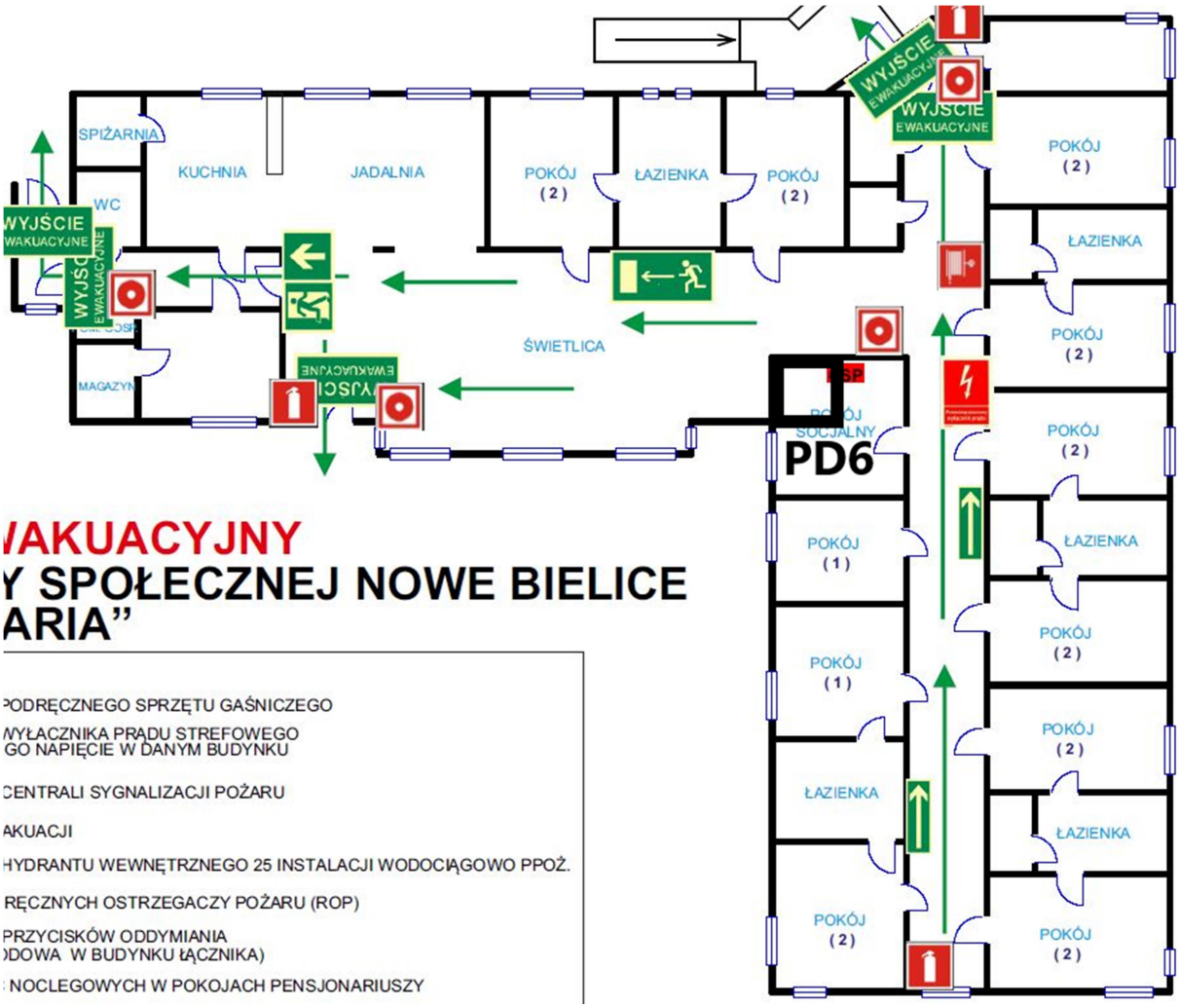
Lista wszystkich punktów dystrybucyjnych:

- PD3 – klatka schodowa, za zamkniętymi drzwiami w części mieszkalnej budynku kuchni
- PD4 – pomieszczenie socjalne
- PD5 – pomieszczenie socjalne

Rysunek 29: Proponowane miejsce instalacji PD3 za drzwiami na klatkę schodową

Rysunek 30: Proponowane miejsce instalacji PD4 – pomieszczenie socjalne, instalacja szafki na ścianie

Budynek Maria

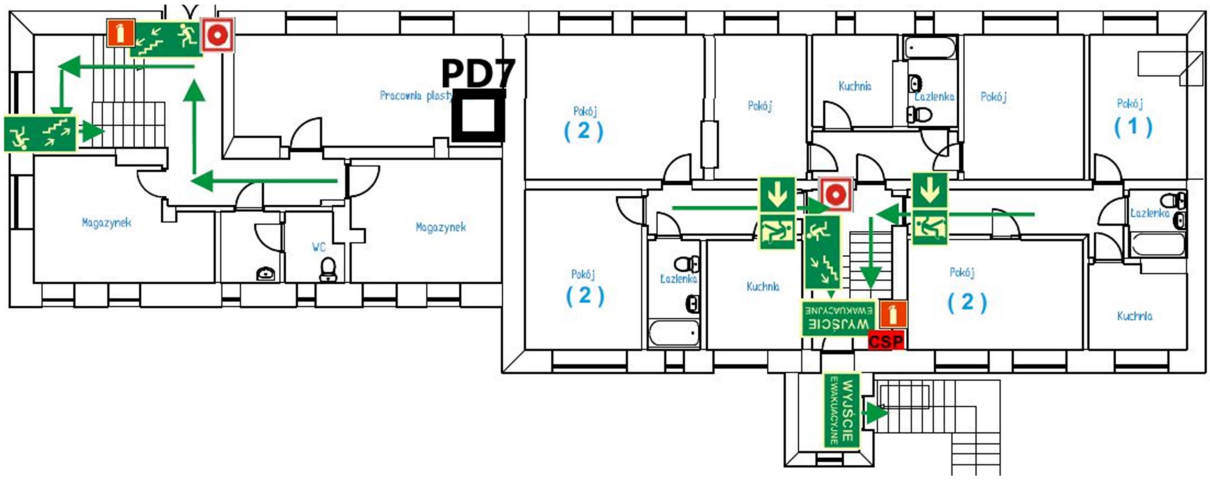


Rysunek 31: Koncepcja trasy światłowodu i instalacji szafyPD6 – pomieszczenie socjalne

Należy zwrócić uwagę, że w obecnej chwili nie ma żadnego połączenia pomiędzy budynkiem Maria, a budynkiem głównym. Niezbędne będzie położenie nowego światłowodu w celu połączenia obu lokalizacji. Projektant będzie musiał oszacować koszty wkopania takiego połączenia.

Rysunek 32: Proponowane miejsce instalacji szafy PD6 – ściana w pomieszczeniu socjalnym

Budynek pralni



Rysunek 33: Proponowane miejsce instalacji PD7 – pomieszczenie plastyczne

Tak samo jak w przypadku budynku Maria budynek pralni nie ma połączenia kablowego z budynkiem głównym. Jest z części biurowej puszczona radiolinia, z którą są czasem kłopoty. Zalecane jest stworzenie nowego połączenia światłowodowego pomiędzy tymi lokalizacjami.

Analiza możliwości przyłączenia do zewnętrznej szerokopasmowej sieci internetowej

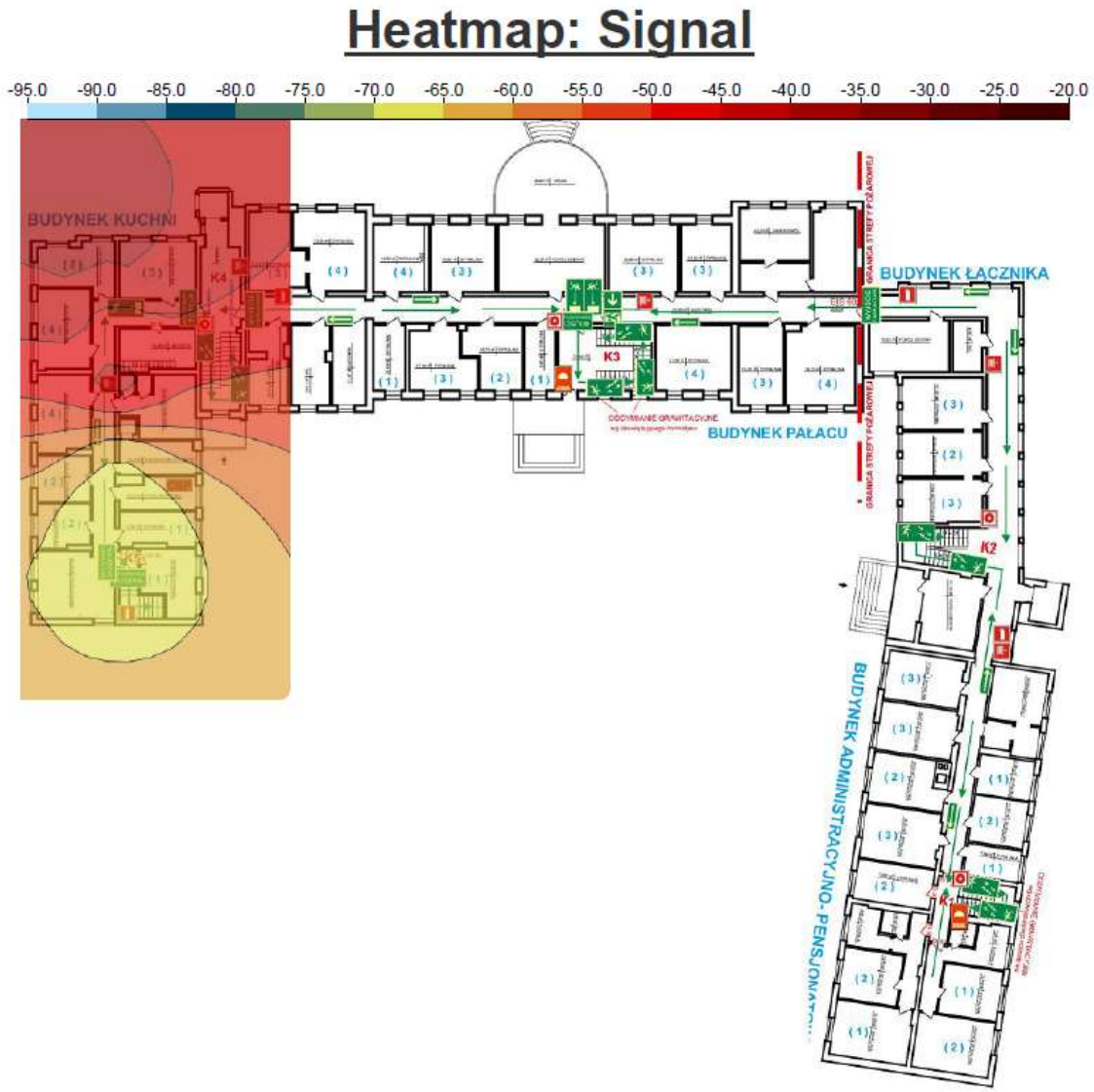
W obecnej chwili dostęp do Internetu jest realizowany za pomocą łącza telefonicznego od Orange. Brak możliwości wymiany tego łącza na łącze światłowodowe. Możliwe jest jedno połączenie video do zrealizowania. Możliwa wymiana łącza internetowego na łącze mobilne.

Rysunek 34: Test prędkości łącza internetowego z komputera stacjonarnego.

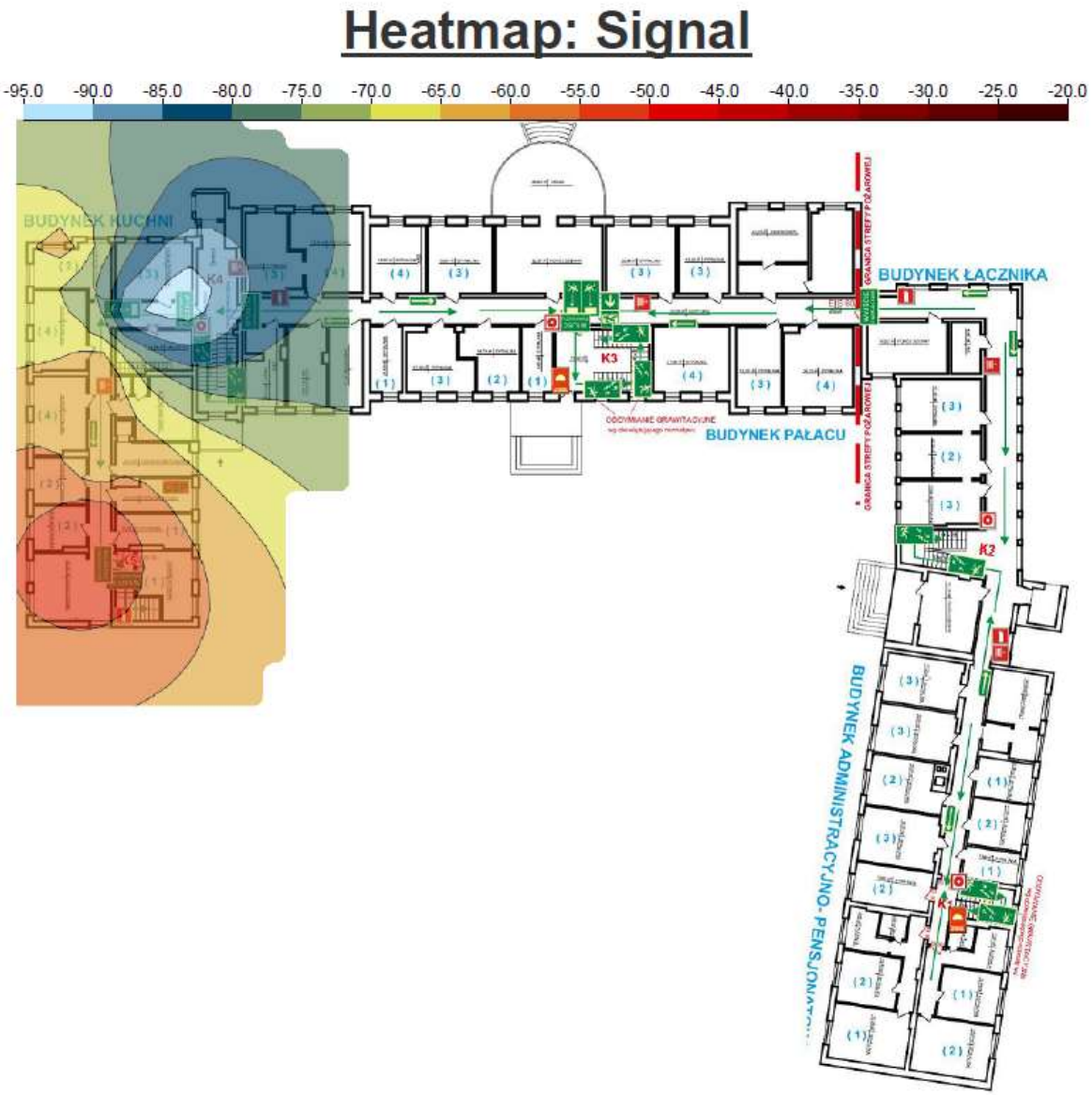
Koncepcja rozmieszczenia nowych punktów dostępowych wraz z doporowadzeniem tras kablowych oraz protokół pomiarowy stanowiący podstawę do opracowania dokumentacji

Poniżej przedstawione zostało planowanie radiowe dla całego kompleksu mieszkalno-biurowego DPS-u w Nowych Bielicach. Cały obszar budynkowy powinien zostać objęty sygnałem radiowym a część zewnętrzna tylko we wskazanych miejscach. Uwzględniony został budynek główny, którego jedną z części jest zabytkowa część pałacowa oraz budynek mieszkalny „Maria" i budynek mieszkalno treningowy pralni. W strefach, gdzie przebywają mieszkańcy została zaprojektowana triangulacja access pointów co pozwoli na ich poprawną lokalizację. W części biurowej i magazynowej urządzenia zostały tak rozmieszczone, aby wszędzie był sygnał na odpowiednim poziomie.

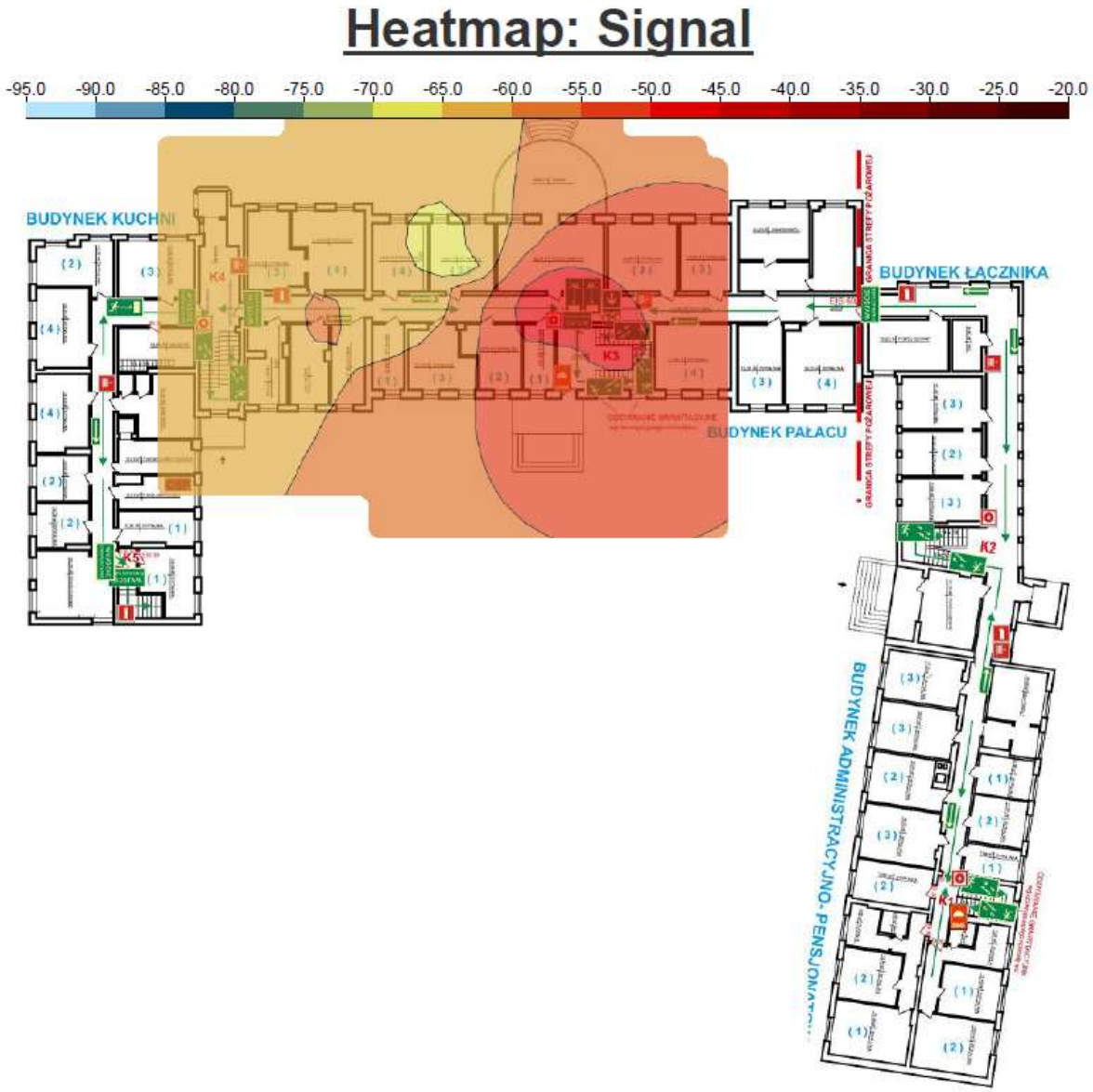
Wykonane zostały badania tłumienia ścian, które pozwoliło na późniejsze przygotowanie rozmieszczenia access pointów na terenie całego DPS-u.



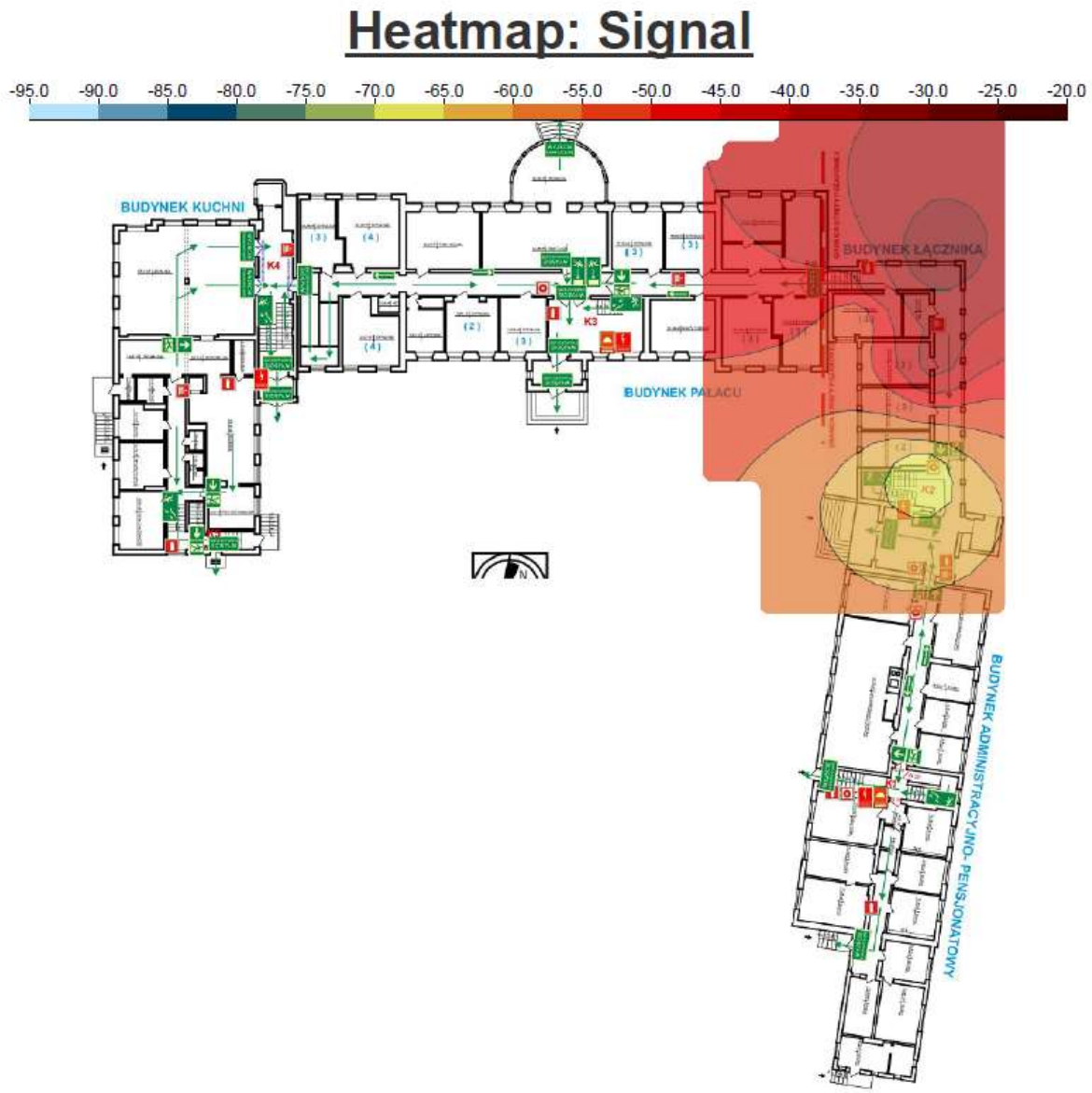
Rysunek 35: Badanie przeprowadzone na pierwszym piętrze, w którym access point był umieszczony w narożnym pokoju



Rysunek 36: Badanie przeprowadzone na pierwszym piętrze, w którym access point był umieszczony na końcu w części wspólnej

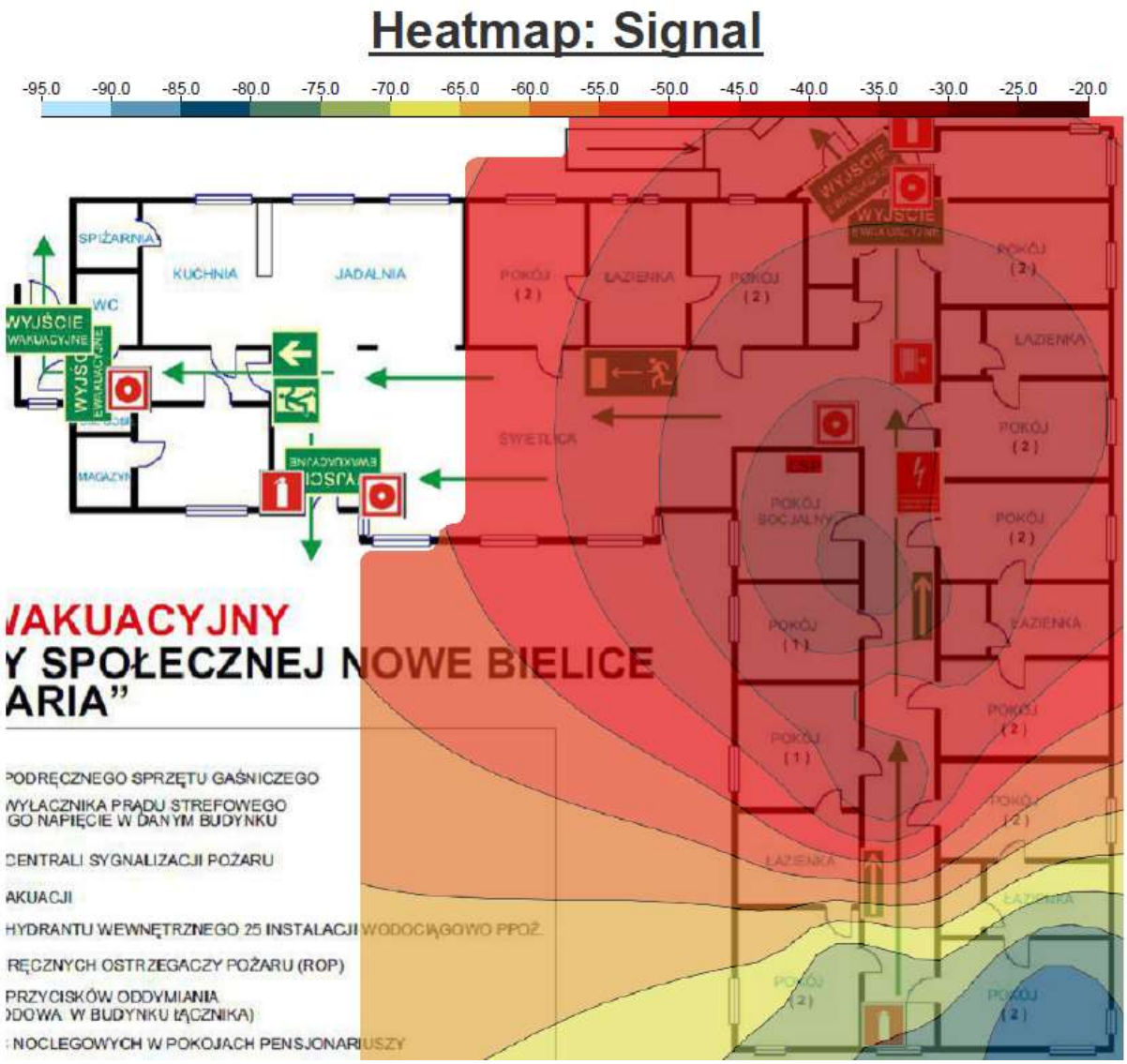


Rysunek 37: Badanie przeprowadzone na pierwszym piętrze, w którym access point był umieszczony w pokoju wspólnym



Rysunek 38: Badanie przeprowadzone na pierwszym piętrze, w którym access point był umieszczony na korytarzu w narożniku.

Jak można zaobserwować na powyższych heat mapach niezależnie czy jest to część pałacowa czy nowsza tłumienność sygnału jest podobna. W najbliższym otoczeniu access pointa sygnał jest bardzo dobry, niestety po przebiciu się przez ściany obserwowany jest znaczny spadek nawet o 15 dBm. Ściany są wykonane z cegły i mają różną szerokość w zależności od miejsca, najmniejszą wartość należy przyjąć ok 10 cm.

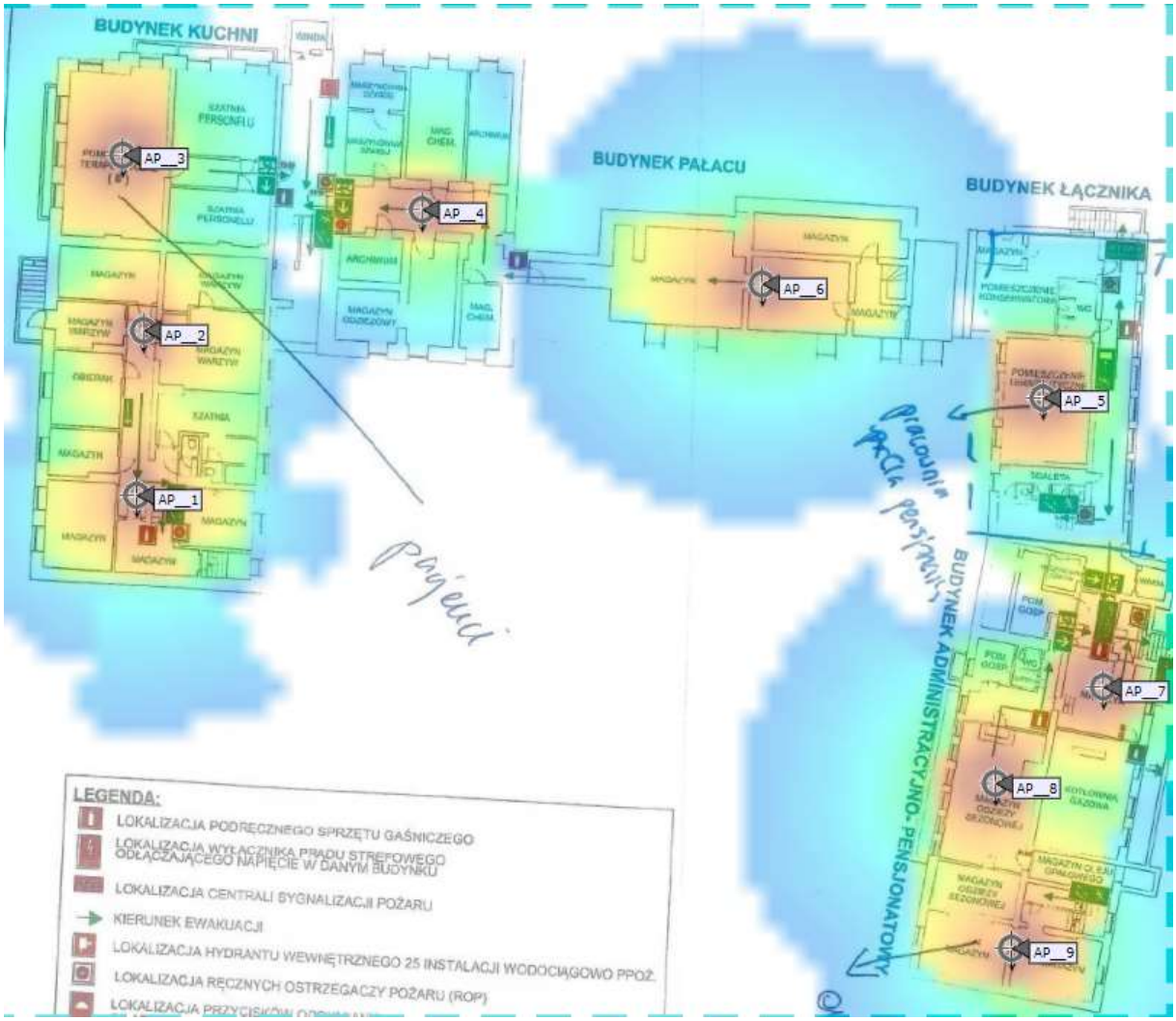


Rysunek 39: Badanie przeprowadzone w budynku „Maria”, w którym access point był umieszczony na korytarzu

Budynek „Maria” jest budynkiem nowym, w którym nie ma ścian o dużej tłumienności. W czasie badania access point był umieszczony na korytarzu. Widać, że w najbliższym otoczeniu access pointa sygnał bez problemów przechodzi do najbliższych pokojów. Jest to nowy budynek, nie ma tu ścian o dużej tłumienności sygnału.

Pałac

Piwnica



Rysunek 40: Planowanie dla częstotliwości 2,4GHz

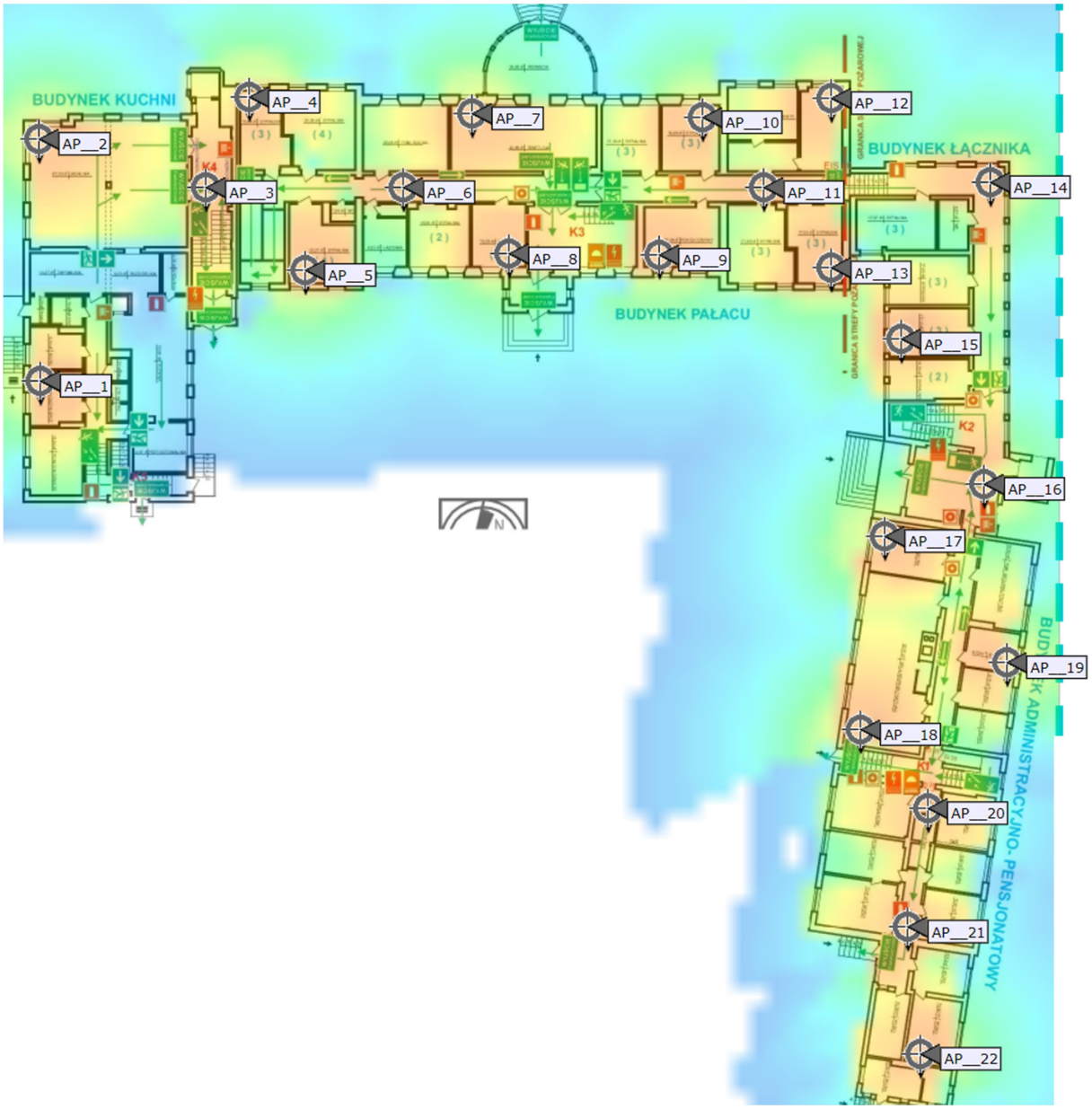
Rysunek 41: Planowanie dla częstotliwości 5GHz

W piwnicy znajdują się dwa pomieszczenia, gdzie przebywają pensjonariusze oraz magazyny. Okablowanie z każdego punktu powinno zostać przebite przez strop lub przejść klatką schodową na parter do najbliższego punktu dystrybucyjnego na paterze. Ze względu, że poza pomieszczeniami terapeutycznymi (AP3 i AP5) są to magazyny, to w ramach ograniczenia budżetu będzie można ograniczyć liczbę access pointów w magazynach do jedynie niezbędnych znajdujących się pod budynkiem administracji.

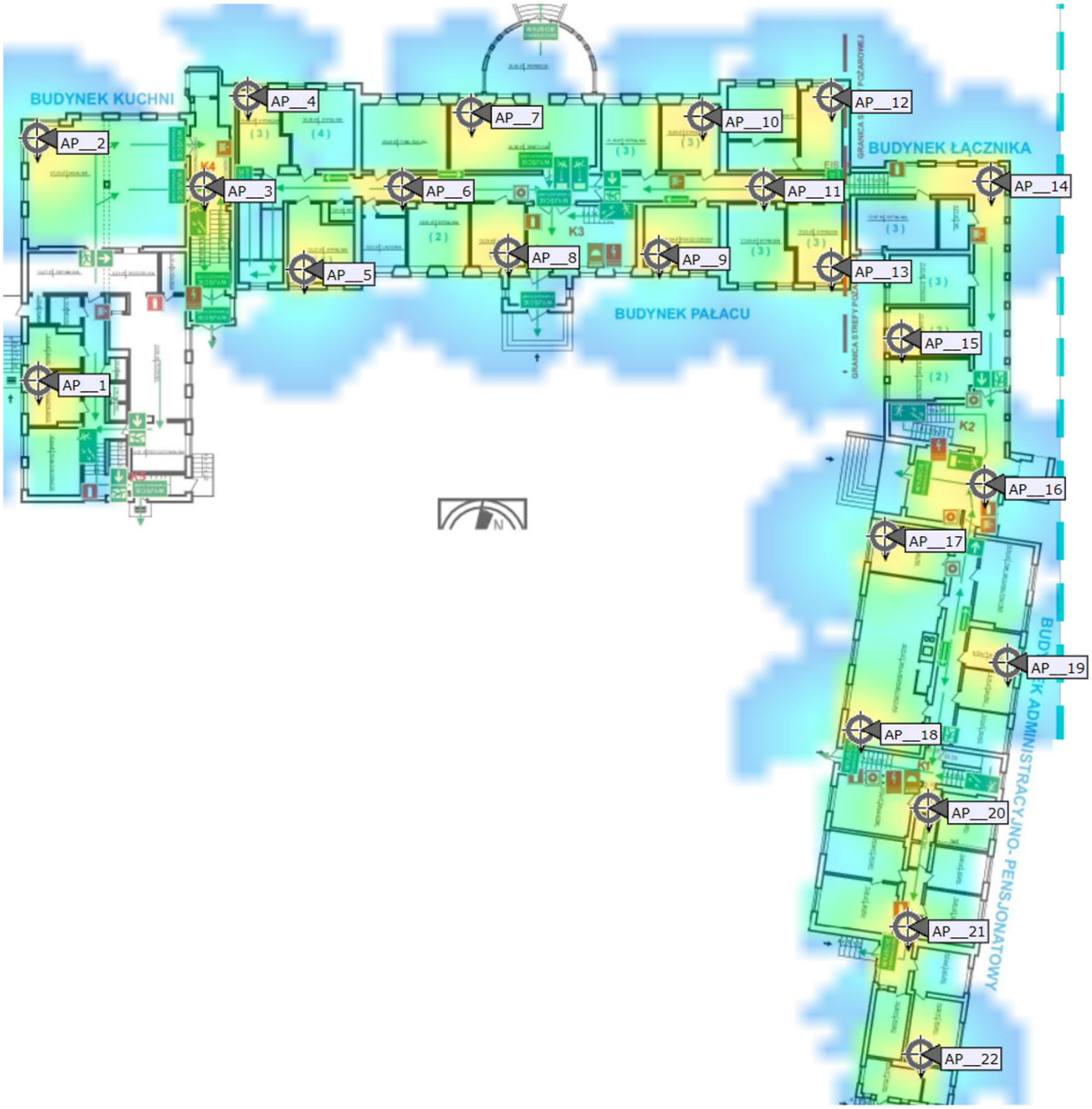
Rysunek 42: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	70
AP2	80
AP3	70
AP4	80
AP5	60
AP6	90
AP7	40
AP8	50
AP9	60

Parter



Rysunek 43: Planowanie dla częstotliwości 2,4GHz



Rysunek 44: Planowanie dla częstotliwości 5GHz

Na parterze zostały zaproponowane dwadzieścia dwa access pointy zarówno w części pałacowej mieszkalnej jak i administracyjnej. W każdej części parteru zaproponowana została szafa rack jako pośredni punkt dystrybucyjny. W żadnym przypadku odległość access point - punkt dystrybucyjny nie przekroczy 100 m. Trasy kablowe proponujemy prowadzić wzdłuż głównych korytarzy. Kable będzie trzeba ukryć w korytach kablowych. Ze względu na zabytkowy charakter obiektu koryta kablowe trzeba zamaskować.

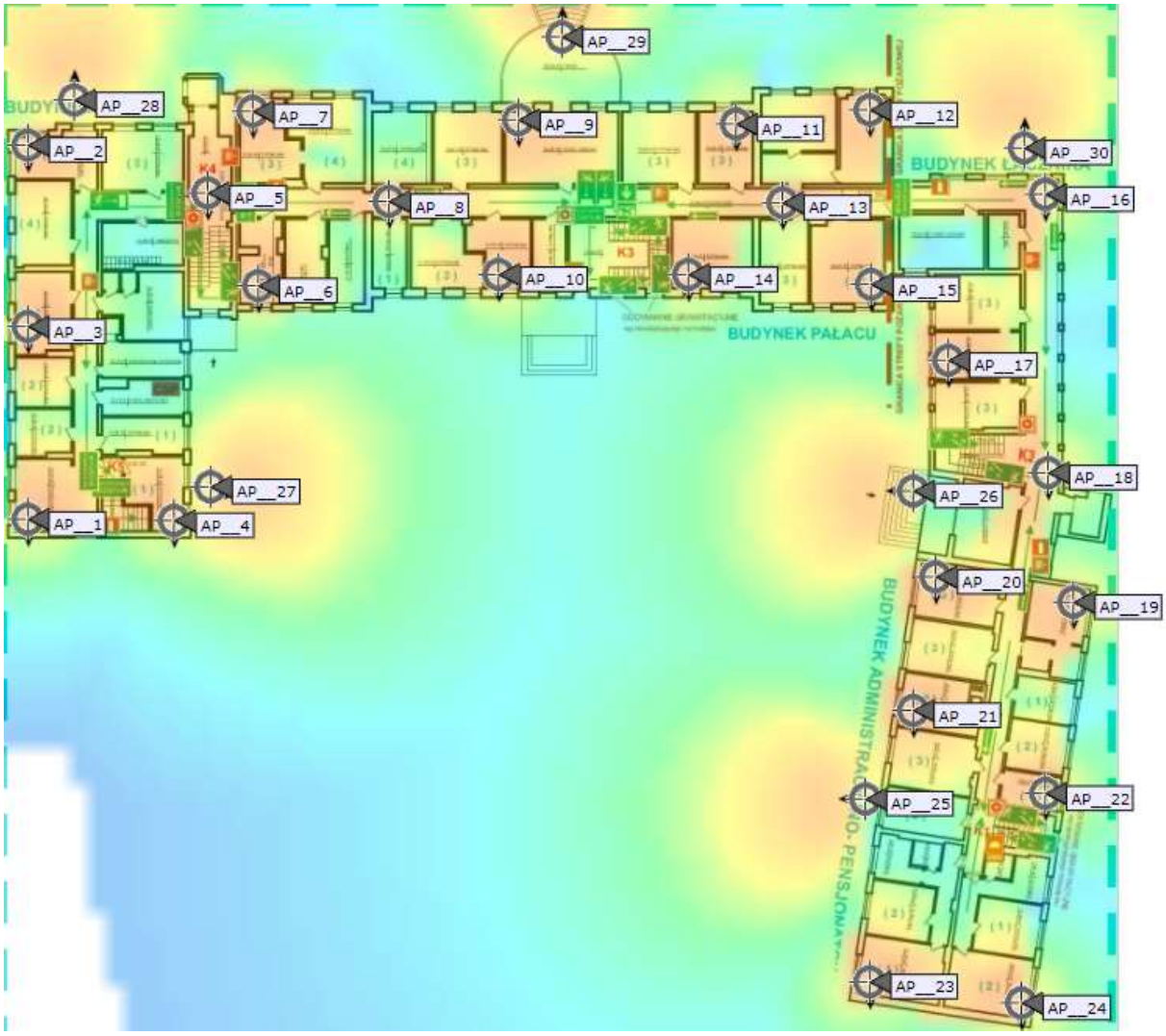
Planowane trasy kablowe

Rysunek 45: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	5
AP2	30
AP3	35
AP4	55
AP5	55
AP6	30
AP7	30
AP8	25
AP9	15
AP10	5

AP11	15
AP12	30
AP13	35
AP14	45
AP15	55
AP16	70
AP17	65
AP18	50
AP19	55
AP20	20
AP21	10
AP22	10

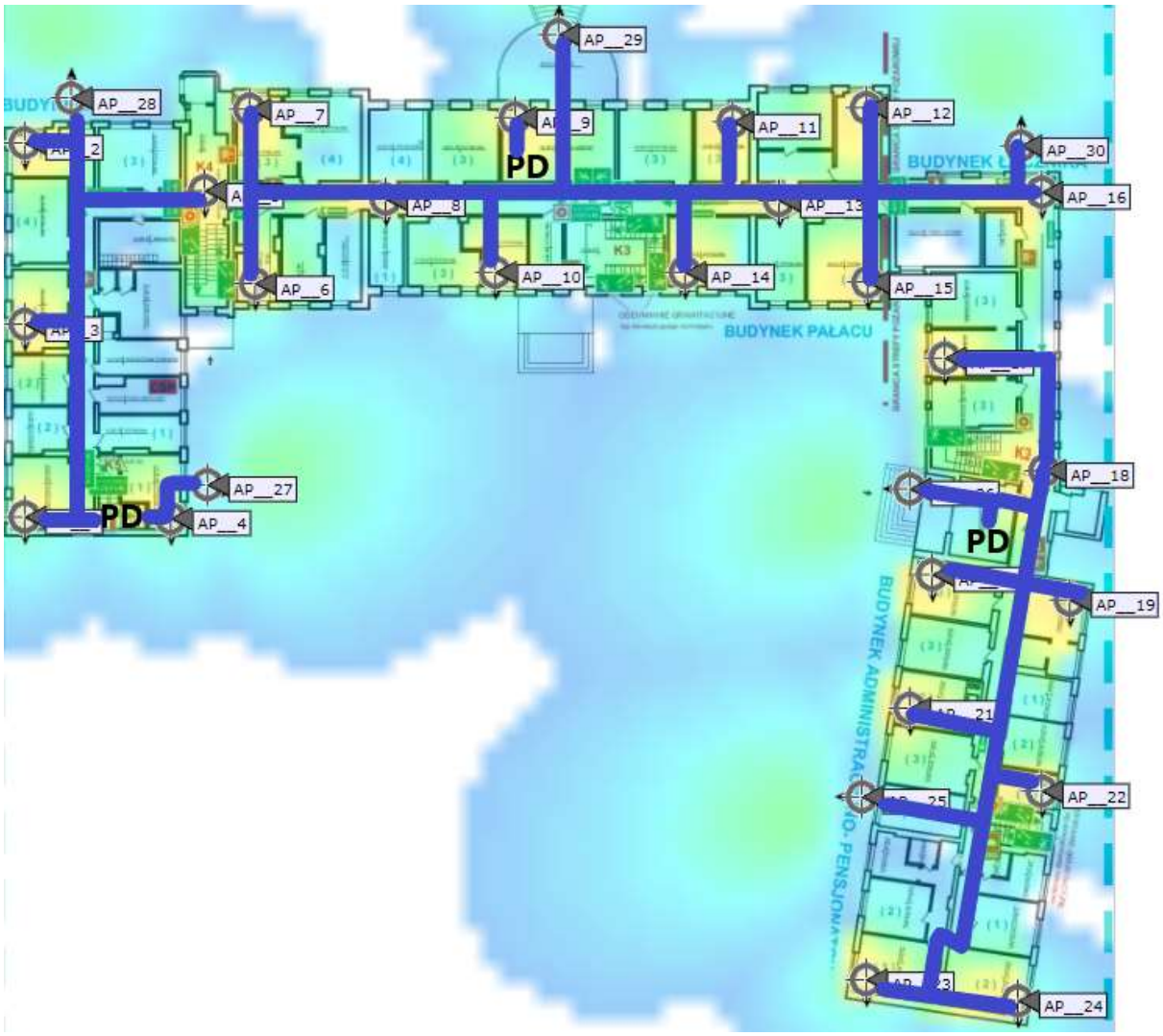
Pierwsze piętro



Rysunek 46: Planowanie dla częstotliwości 2,4GHz

Rysunek 47: Planowanie dla częstotliwości 5GHz

Na pierwszym piętrze zostało zaproponowanych trzydzieści access pointów. AP25-AP30 są to access pointy zewnętrzne z przeznaczeniem do oświetlenia obszaru wokół pałacu, gdzie przebywają mieszkańcy. Trasy kablowe tak samo jak na parterze powinny iść korytarzami do najbliższego punktu dystrybucyjnego.



Rysunek 48: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	5
AP2	35
AP3	20
AP4	5
AP5	45
AP6	45
AP7	45
AP8	35
AP9	5
AP10	15
AP11	25
AP12	45
AP13	35
AP14	25
AP15	45

AP16	55
AP17	30
AP18	20
AP19	20
AP20	20
AP21	35
AP22	45
AP23	60
AP24	60
AP25	45
AP26	10
AP27	10
AP28	50
AP29	25
AP30	50

Całe okablowanie pochodzące od urządzeń w pokojach będzie zbiegać się do głównej trasy kablowej na korytarzu. Wszystko będzie umieszczone w korytach kablowych na styku ściany/sufitu tak, aby w jak najmniejszym stopniu było widoczne.

Nowe miejsca instalacji access pointów zewnętrznych

Rysunek 49: Miejsce instalacji na elewacji pałacu

Urządzenie nad wejściem do werandy, na środku nad drzwiami, zlicowane ze ścianą, okablowanie zostanie wyprowadzone ze środka do najbliższej głównej trasy kablowej.

Access point po lewej stronie

Rysunek 50: Miejsce instalacji na elewacji budynku

Przymocowane do elewacji budynku łącznika, na równo z górną krawędzią okna, możliwe blisko krawędzi okna, okablowanie wejdzie bezpośrednio na korytarz i do najbliższego punktu dystrybucyjnego.

Access point po prawej stronie

Rysunek 51: Miejsce instalacji na elewacji budynku

Analogicznie jak w przypadku strony lewej. Przymocowane do elewacji budynku kuchni, na równo z górną krawędzią okna, możliwe blisko krawędzi okna, okablowanie wejdzie bezpośrednio do pomieszczenia jadalni.

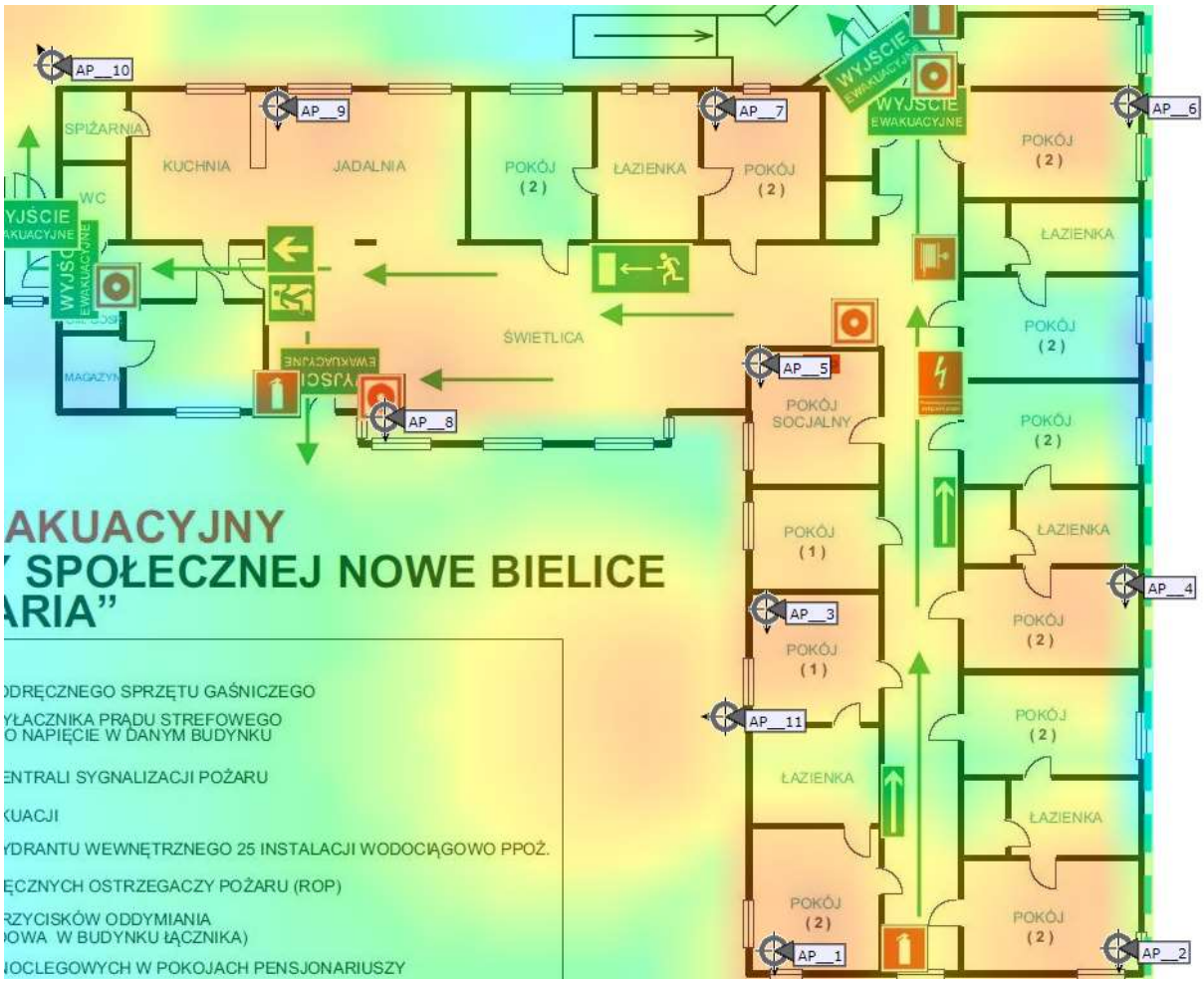
Rysunek 52: Miejsce instalacji szafy rack w pomieszczeniu socjalnym na parterze

Rysunek 53: Miejsce instalacji na pierwszym piętrze w pomieszczeniu świetlicy lub w pomieszczeniu socjalnym obo

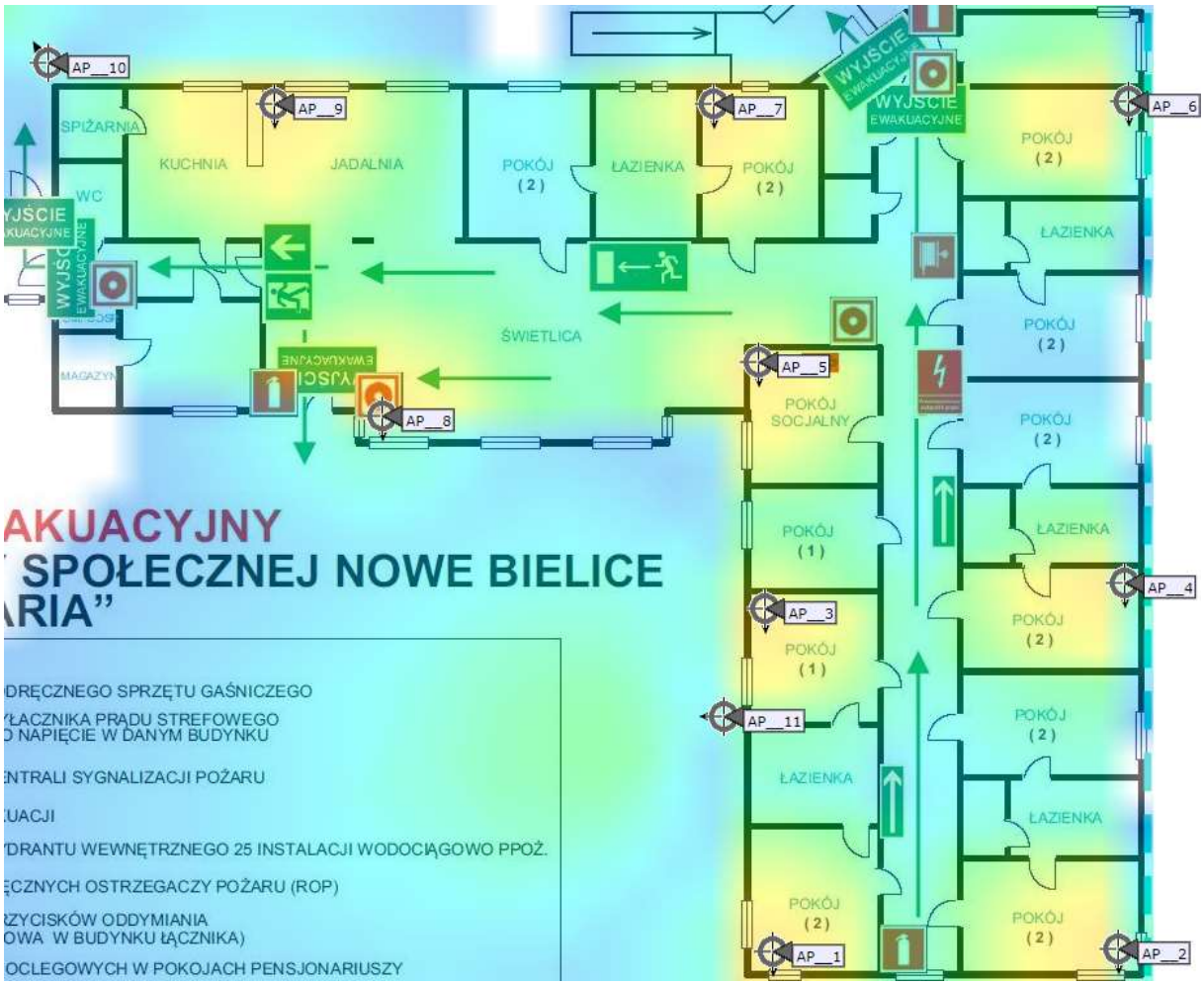
Rysunek 54: Instalacja punktów dostępowych pod sufitem w pokojach

Rysunek 55: Instalacja punktów dostępowych pod sufitem na korytarzach

Budynek Maria



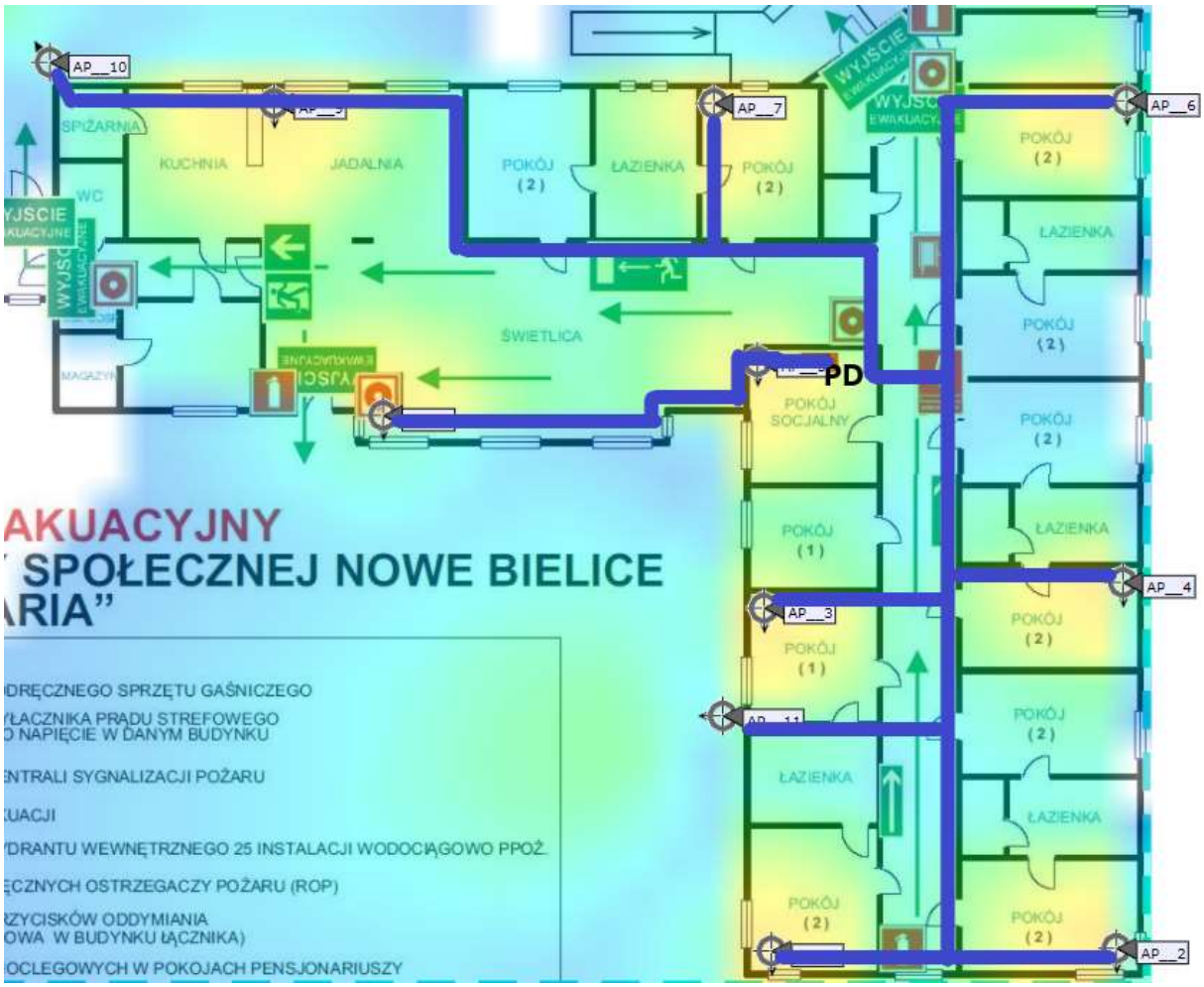
Rysunek 56: Planowanie dla częstotliwości 2,4GHz



Rysunek 57: Planowanie dla częstotliwości 5GHz

W budynku Maria przewidzianych zostało jedenaście access pointów. W tym AP10 i AP11 są to urządzenia zewnętrzne. Całość okablowania powinna zejść się do pomieszczenia socjalnego, gdzie przewidziany jest punkt dystrybucyjny.

Planowane trasy kablowe

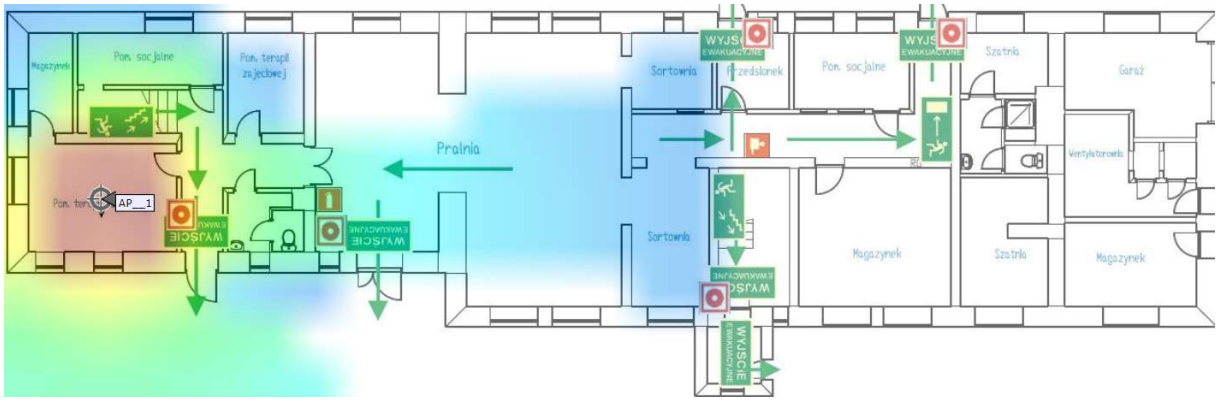


Rysunek 58: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

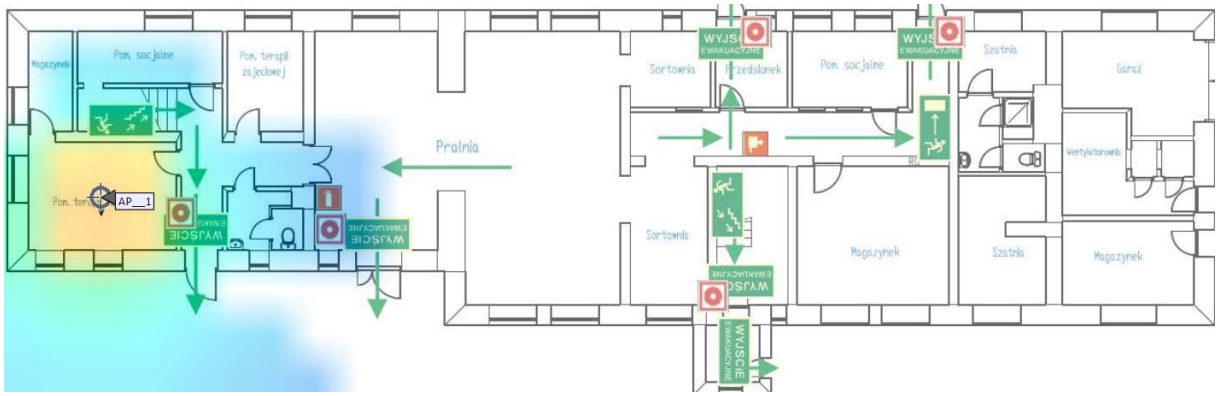
Numer AP	Szacowana długość okablowania [m]
AP1	30
AP2	30
AP3	20
AP4	20
AP5	5
AP6	20
AP7	20
AP8	20
AP9	30
AP10	50
AP11	25

Budynek pralni

Parter



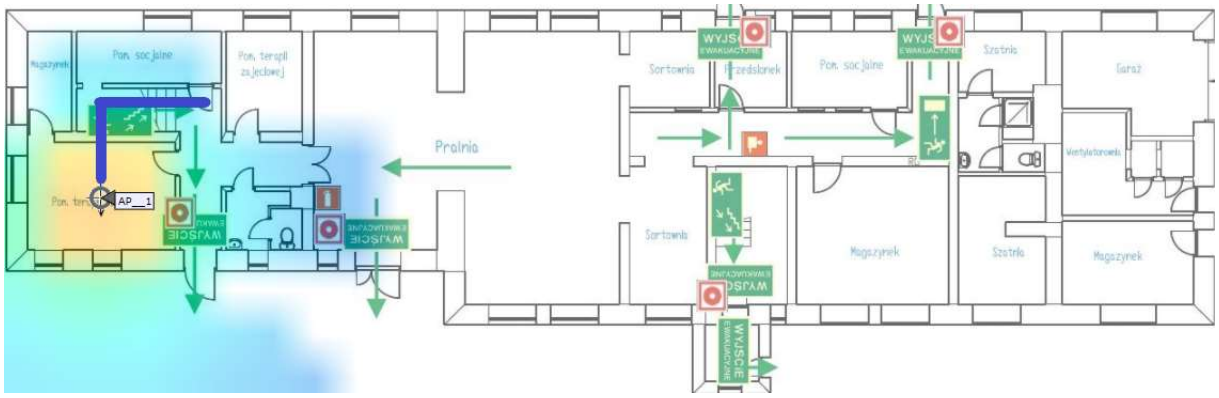
Rysunek 59: Planowanie dla częstotliwości 2,4GHz



Rysunek 60: Planowanie dla częstotliwości 5GHz

W budynku pralni na parterze przewidziany jest jeden access point.

Planowane trasy kablowe



Rysunek 61: Całe okablowanie zejdzie się w korytkach do punktu PD na pierwszym pietrze, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	30

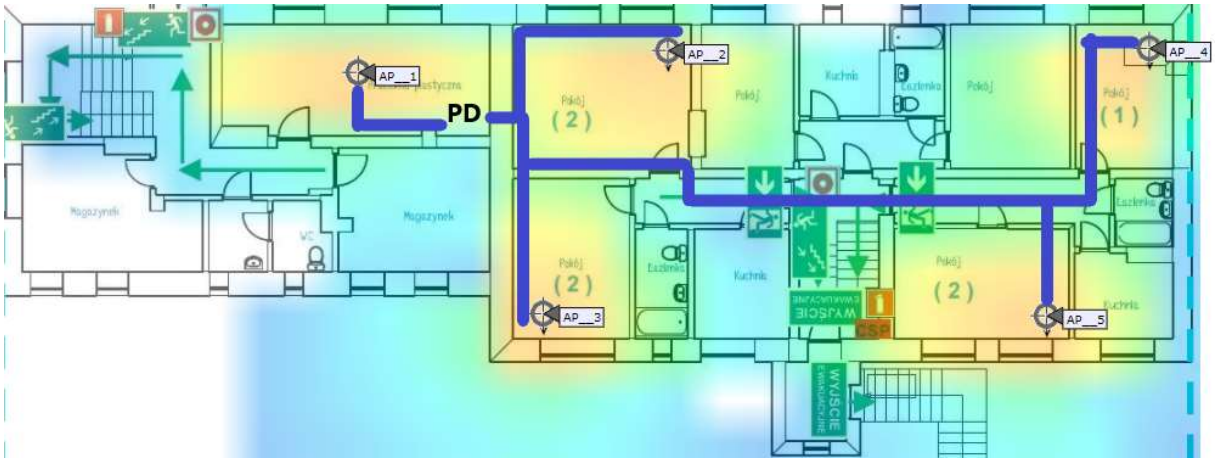
Pierwsze piętro

Rysunek 62: Planowanie dla częstotliwości 2,4GHz

Rysunek 63: Planowanie dla częstotliwości 5GHz

W budynku pralni na pierwszym piętrze przewidzianych jest pięć access pointów. Całość okablowania powinna zejść się do pomieszczenia plastycznego, gdzie przewidziany jest punkt dystrybucyjny.

Planowane trasy kablowe



Rysunek 64: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	5
AP2	25
AP3	25
AP4	55
AP5	55

Podsumowanie

Liczba wszystkich urządzeń:

- Kontroler sieci bezprzewodowej: 1.
- Access pointy: 78 w tym 8 zewnętrznych.
- Switche: 1 core, 7 access.
- Firewall: 1.

Możliwe do wystąpienia problemy

Ze względu na zabytkowy charakter obiektu oraz na jego wiek należy mieć na uwadze:

- Grube ceglane ściany do kilkudziesięciu cm. grubości, co może powodować trudności w prowadzeniu kabli
- Brak jakiejkolwiek infrastruktury, z której można by skorzystać w czasie projektowania, czy instalacji nowej sieci.
- Brak istniejących tras kablowych oraz przepustów.
- Część obiektu pod nadzorem konserwatora zabytków.
- Brak doprowadzonego zasilania do wybranych punktów dostępowych.
- Instalacja będzie obejmować trzy budynki, które w obecnej chwili nie są ze sobą połączone światłowodem.
- Instalacja urządzeń w piwnicach.
- Równocześnie problemem dla wprowadzenia nowoczesnych usług może okazać się niedostatek parametrów połączenia internetowego oraz brak możliwości redundancji w tym zakresie.

Minimalne wymagania techniczne sprzętu

Kontroler sieci bezprzewodowej	• urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
	  ○ zarządzanie politykami bezpieczeństwa
	  ○ wykrywanie zagrożeń w sieci bezprzewodowej
	  ○ zarządzanie pasmem radiowym
	  ○ zarządzanie mobilnością
	  ○ zarządzanie jakością transmisji
	• obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji
	• min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45)
	• opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by

	zabezpieczyć przed awarią pojedynczego interfejsu
	• obsługa ruchu tunelowanego
	• obsługa min. 1000 klientów sieci bezprzewodowej
	• zarządzanie pasmem radiowym punktów dostępowych:
	  ○ automatyczna adaptacja do zmian w czasie rzeczywistym
	  ○ optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
	  ○ dynamiczne przydzielanie kanałów radiowych
	  ○ wykrywanie, eliminacja i unikanie interferencji
	  ○ równoważenie obciążenia punktów dostępowych
	  ○ tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
	  ○ automatyczna dystrybucja klientów pomiędzy punkty dostępowe
	  ○ mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
	  ○ dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
	• mapowanie SSID do segmentów VLAN w sieci przewodowej
	• możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
	• automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
	• obsługa mechanizmów bezpieczeństwa:
	  ○ 802.11i, WPA3, WPA2, WPA, WEP
	  ○ 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
	  ○ obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
	• kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
	• obsługa dostępu gościnnego (IPv4 i IPv6)
	  ○ przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)
	  ○ przekierowanie użytkowników do strony logowania na zewnętrznym serwerze
	• współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych
	• obsługa NTP wersji 4 (IPv4 oraz IPv6)
	• obsługa Hotspot 2.0
	• obsługa redundancji rozwiązania

Access point wewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance)

	○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM

	○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych
Access point zewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN

	○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z

	określeniem czasu ważności konta; o wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • dla access pointów zewnętrznych: o zgodność z IP67 o min. praca przy temperaturach między -35^{o}C a 60^{o}C • certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint
Switch core	• Typ i liczba portów: o Min: 12 SFP/SFP+ • Opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb): o min. 4x1G SFP o min. 4x1/10G SFP+ • Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: o Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U o Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość tworzenia stosów • Parametry wydajnościowe: o Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) o Bufor pakietów – min.: 8MB o Pamięć DRAM – min.: 4GB o Pamięć flash – min.: 8GB o Obsługa ▪ min. 3.000 sieci VLAN ▪ min.: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: o Obsługa protokołu STP • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP

	• Mechanizmy związane z bezpieczeństwem sieci:
	  o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
	  o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
	  o Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
	  o Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
	  o Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
	• Obsługa protokołów routingu:
	  o Routing statyczny dla IPv4 i IPv6
	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
	• Zarządzanie
	  o Port konsoli
	  o Dedykowany port Ethernet do zarządzania out-of-band
	  o Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
	  o Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
	  o Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
	• Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Switch access	• Typ i liczba portów:
	  o min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP
	• Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami)
	• Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
	  o Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
	  o Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T,

	1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: o Przepustowość w ramach stosu – min.:60Gb/s o min: 4 urządzenia w stosie o Zarządzanie poprzez jeden adres IP • Parametry wydajnościowe: o Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) o Bufor pakietów – min: 4MB o Pamięć DRAM – min: 1GB o Pamięć flash – min: 2GB o Obsługa ▪ 1024 sieci VLAN ▪ min: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: o IEEE 802.1w Rapid Spanning Tree • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Obsługa protokołów routingu: o Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie o Port konsoli o Dedykowany port Ethernet do zarządzania out-of-band o Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją o Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 o Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika

	danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
Firewall	• Wymagania Ogólne o Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. o System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. o System musi wspierać IPv4 oraz IPv6 w zakresie: ▪ Firewall. ▪ Ochrony w warstwie aplikacji. ▪ Protokołów routingu dynamicznego. • Redundancja, monitoring i wykrywanie awarii o W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. o Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. o Monitoring stanu realizowanych połączeń VPN. • Interfejsy, Dysk, Zasilanie: o System realizujący funkcję Firewall musi dysponować minimum: ▪ min. 4 portami Gigabit Ethernet RJ-45. ▪ min. 2 gniazdami SFP 1 Gbps. o System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. o System musi być wyposażony w zasilanie AC. • Parametry wydajnościowe: o W zakresie Firewall’a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. o Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps o Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji:

	nie mniej niż 0,5 Gbps. o Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps. • Funkcje Systemu Bezpieczeństwa: o W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. ▪ Kontrola Aplikacji. ▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. ▪ Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). ▪ Funkcja lokalnego serwera DNS ze wsparciem dla DNS • Polityki, Firewall o Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. o System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. ▪ W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. ▪ Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików. • Połączenia VPN o System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: ▪ Wsparcie dla IKE v1 oraz v2. ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. ▪ Monitorowanie stanu tuneli VPN i stałego

	utrzymywania ich aktywności. ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. ▪ Mechanizm „Split tunneling" dla połączeń Client-to-Site. o System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: ▪ Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. ▪ Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. • Routing i obsługa łączy WAN o W zakresie routingu rozwiązanie powinno zapewniać obsługę: ▪ Routingu statycznego. ▪ Policy Based Routingu. ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. • Ochrona przed malware • Ochrona przed atakami o Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. • Kontrola aplikacji • Kontrola WWW • Zarządzanie • Logowanie • Serwisy i licencje o W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. • Gwarancja oraz wsparcie
Okablowanie etherentowe	• Min. Cat 6 ekranowana

Zalecenia konserwatorskie dla Domu Pomocy Społecznej w Nowych Bielicach

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152; f
e-mail: koszalin

ZN.K.5183.78.2021.KB

Koszalin, 28 c

DOM POMOCY
w NOWY(
ul. Parkowa 22, 76-03
adres do ko
Network Experts sp
ul. Chojnowska 8, 03-583

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń sieci bezprzewodowej – punków dostępowych, instalacji okablowania dystrybucyjnych, w Domu Pomocy Społecznej w Nowych Bielicach, 76-039 E związku z opracowywaniem dokumentacji dotyczącej „Opracowania audytu s dla budynków DPS Powiatu Koszalińskiego".

Odpowiadając na pismo z dnia 17.05.2021 r. (data wpływu 18.05.2021 r.), 17.06.2021 r. (data wpływu 21.06.2021 r.), uzupełnione pismem z dnia 25.06. wpływu 25,28.06.2021 r.), w oparciu o wizję lokalną przeprowadzoną w dniu 7 Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie, działając art. 27 Ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytk z 2021 r. poz. 710 ze zm.) przekazuje następujące zalecenia konserwatorskie:

1. Pałac w Nowych Bielicach gm. Biesiekierz, jest zabytkiem architektury i wpisanym do rejestru zabytków pod nr 386 decyzją z dnia 14.04.19 otoczeniem (parkiem). Przedmiotowa nieruchomość podlega ochroni podstawie art. 6 ust. 1 lit. c, g oraz art. 7 ust. 1 ustawy z dnia 23.07.2003 zabytków i opiece nad zabytkami (t.j. Dz.U. z 2021 r. poz. 710 ze zm.), określonych w tej ustawie. Zgodnie z art. 36 ust. 1 przywołanej ustawy, badań konserwatorskich, robót budowlanych oraz umieszczan technicznych na zabytku wpisanym do rejestru zabytków wyma

Delegatura w Koszalinie i Network Experts sp. z o.o. sp.k. przedstawione na załączonych rzutach parteru, i I piętra, oraz fotog i wnętrz pałacu.

3. Zaleca się prowadzenie kabli instalacyjnych w osłonach kolorystycznie i umieszczonych możliwie dyskretnie u zbiegu ś z ograniczeniem do minimum trasy ich przebiegu. Ponadto zaleca się minimum wielkości urządzeń do transmisji sieci bezprzewodowej i sz kolorystyczne obudowy urządzeń i szaf z podłożem.

4. Nie wnosi się zastrzeżeń ze stanowiska konserwatorskiego do p rozmieszczenia i rozprowadzenia punktów dystrybucyjnych, punktó światłowodów, oraz kabla ethernetowego w budynkach wzniesionyc usytuowanych na terenie parku. Z uwagi na usytuowa w otoczeniu zabytku, wpisanym do rejestru zabytków wraz z pałacer 36 ust. 1 pkt 2 Ustawy o ochronie zabytków i opiece nad zabytkar robót budowlanych i umieszczanie urządzeń technicznych w ot wpisanym do rejestru zabytków wymaga również uzyskar wojewódzkiego konserwatora zabytków w formie decyzji administrac

Z up. ZACHODNIOPOMOI
WOJEWÓDZKIEGO KONSERWATORA
Kierownik Delegatury w K

mgr Dorota Raczkows

Uzupełnienie zaleceń konserwatorskich dla Nowych Bielic

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152; fax:
e-mail: koszalin@v

ZN.K.5183.78.2021.KB

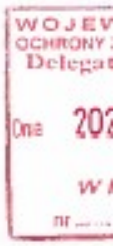
Koszalin, 28 cze

DOM POMOCY S
w NOWYCH
ul. Parkowa 22, 76-039 I
adres do kore
Network Experts sp.
ul. Chojnowska 8, 03-583 V

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń d sieci bezprzewodowej – punków dostępowych, instalacji okablowania dystrybucyjnych, w Domu Pomocy Społecznej w Nowych Bielicach, 76-039 Bi związku z opracowywaniem dokumentacji dotyczącej „Opracowania audytu sie dla budynków DPS Powiatu Koszalińskiego".

W uzupełnieniu do pisma ZWKZ znak ZN.K.5183.78.2021.KB z dnia 28. Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie Kierownik w Koszalinie przekazuje w załączeniu 1 egzemplarz dokumentacji pt. U dokumentacji konserwatorskiej do wydania zaleceń pod budowę nowej sieci w Pomocy Społecznej w Nowych Bielicach".

Z up. ZACHODNIOP
WOJEWÓDZKIEGO KONSER
Kierownik Delegatury
mgr Dorota Raz



Uzupełnienie dokumentacji konserwatorskiej do wydania zalece budowę nowej sieci wifi w Domu Po Społecznej w Nowych Bielicach

W czasie wizyty lokalnej w Nowych Bielicach ustalone zostały nowe miejsca instalacji acces oraz trasy kablowe.

Ustalenia końcowe:

Miejsca instalacji access pointów wewnętrznych nie ulegają zmianie w stosunku do z wcześniej wniosku, to samo dotyczy wybranych miejsc instalacji szaf dystrybucyjnych.

Całe okablowanie pochodzące od urządzeń w pokojach będzie zbiegać się do głównej tras na korytarzu. Wszystko będzie umieszczone w korytach kablowych na styku ściany/sufitu jak najmniejszym stopniu było widoczne.

Nowe miejsca instalacji access pointów zewnętrznych:

Access point po lewej stronie

Przymocowane do elewacji budynku łącznika, na równo z górną krawędzią okna, możliw
krawędzi okna, okablowanie wejdzie bezpośrednio na korytarz i do najbliższego punktu
dystrybucyjnego.

Access point po prawej stronie

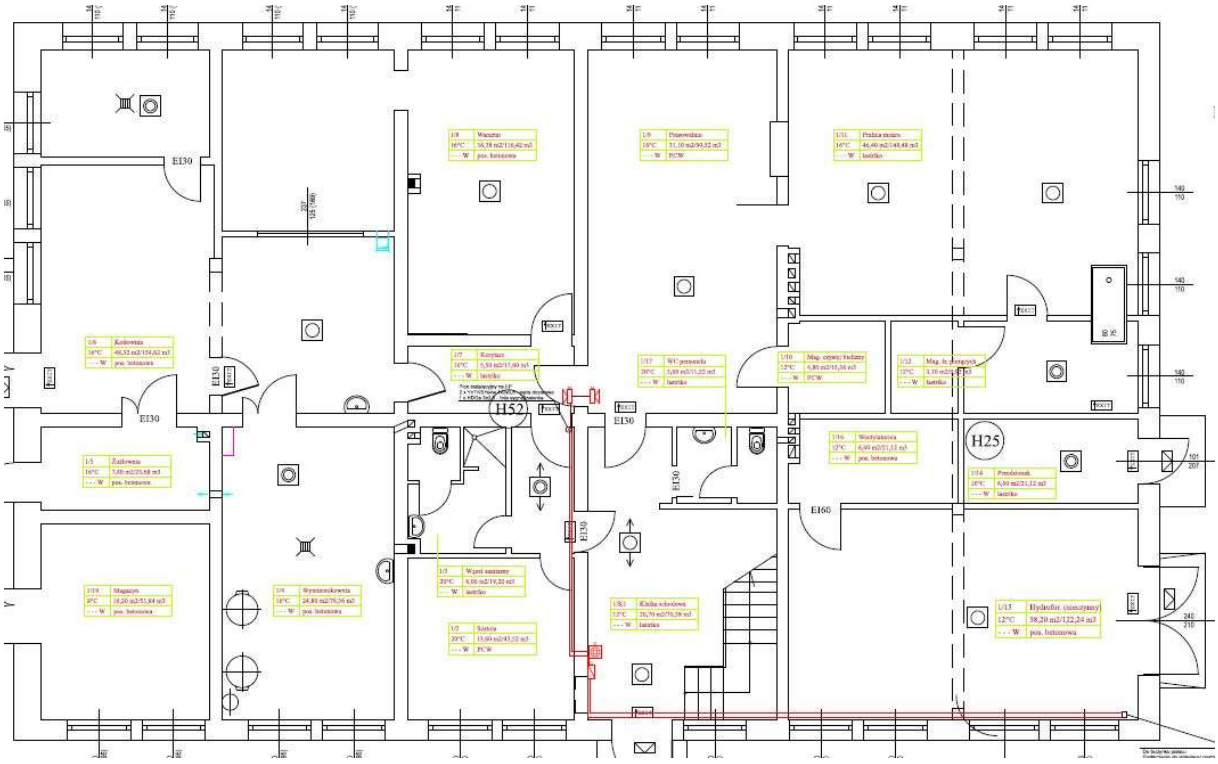
Analogicznie jak w przypadku strony lewej. Przymocowane do elewacji budynku kuchni, n
górną krawędzią okna, możliwe blisko krawędzi okna, okablowanie wejdzie bezpośrednio
pomieszczenia jadalni.

Załącznik nr 4 DPS Parsowo

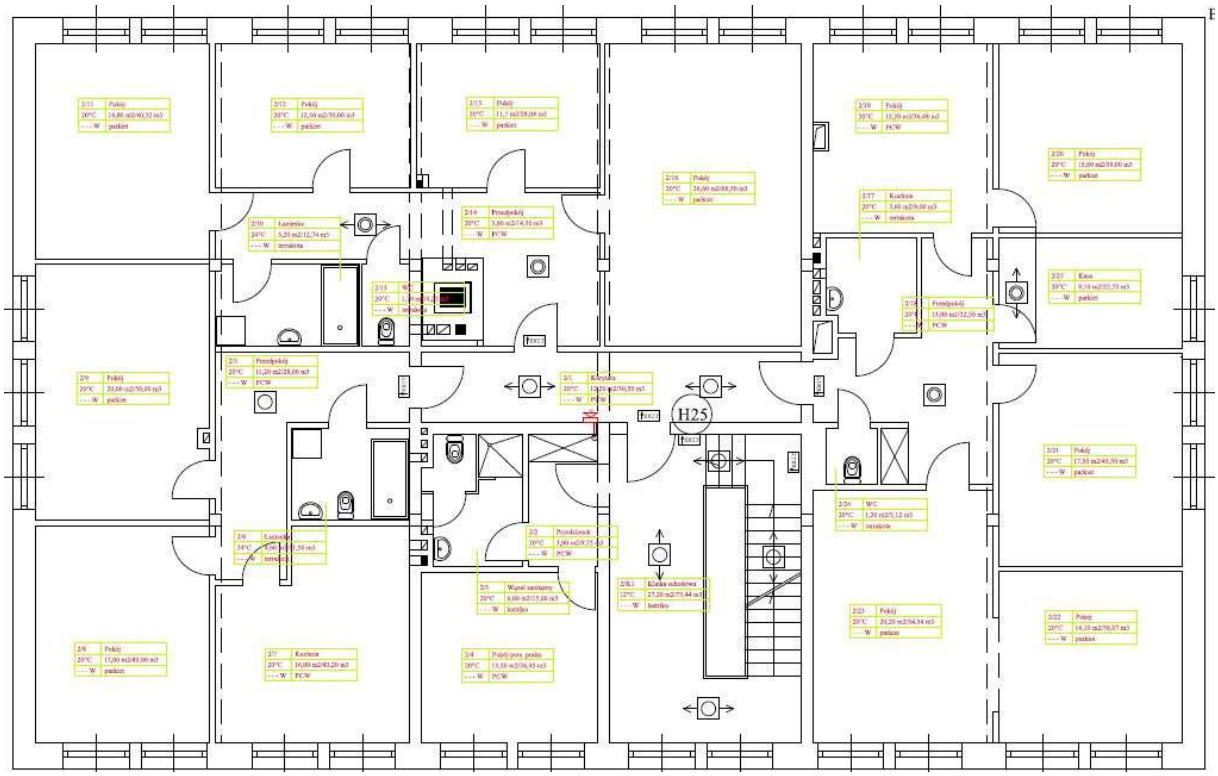
DPS Parsowo składa się z dwóch części mieszkalno – administracyjnych: cześć pałacowa oraz cześć biurowo – hotelowa. Obie części są objęte nadzorem konserwatorskim.

Plany budynków

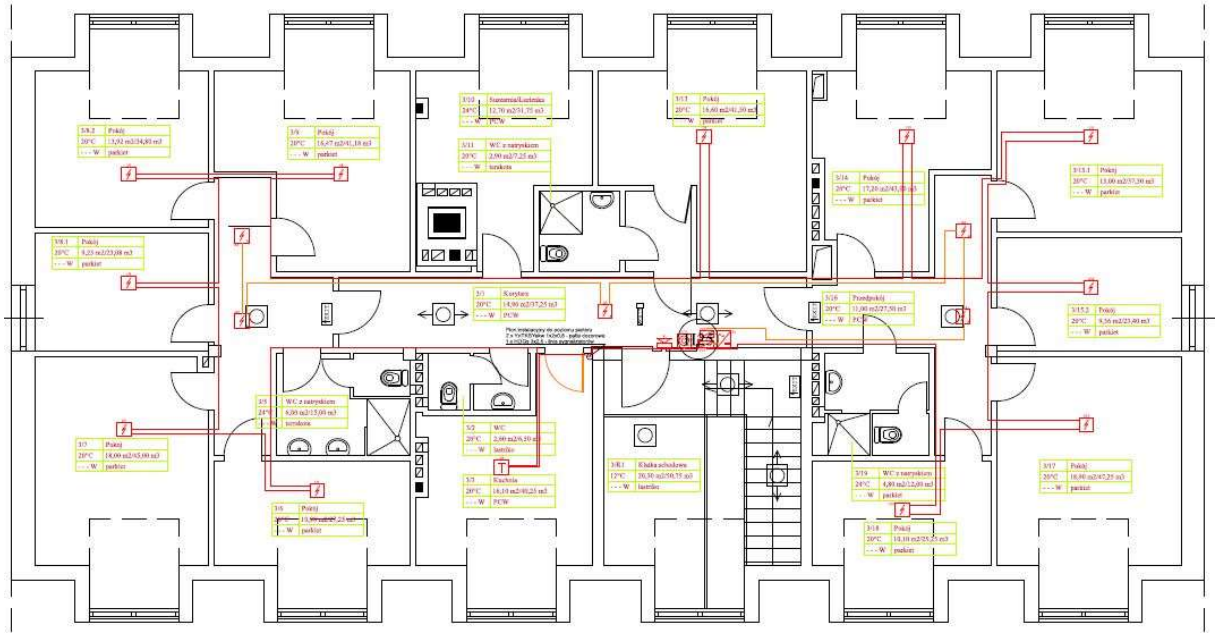
Budynek administracji



Rysunek 1: Plan parteru

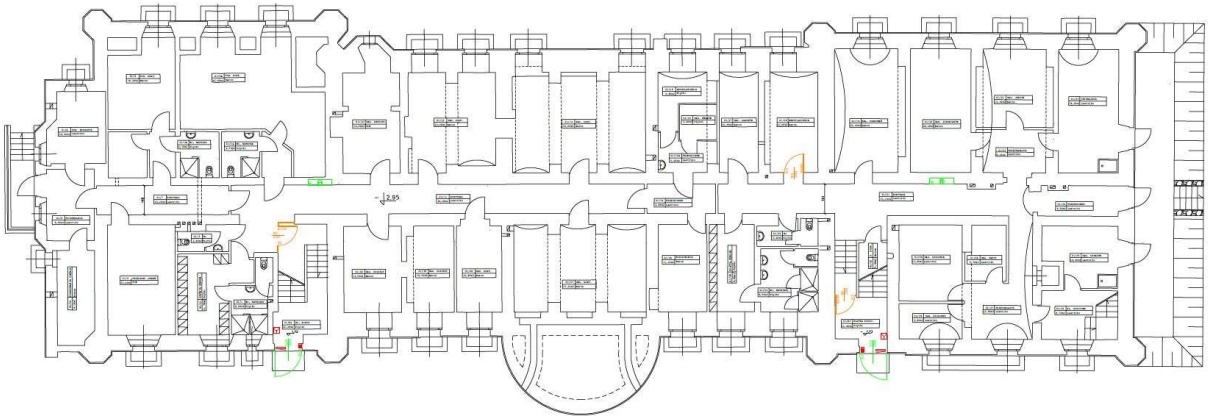


Rysunek 2: Plan pierwszego piętra

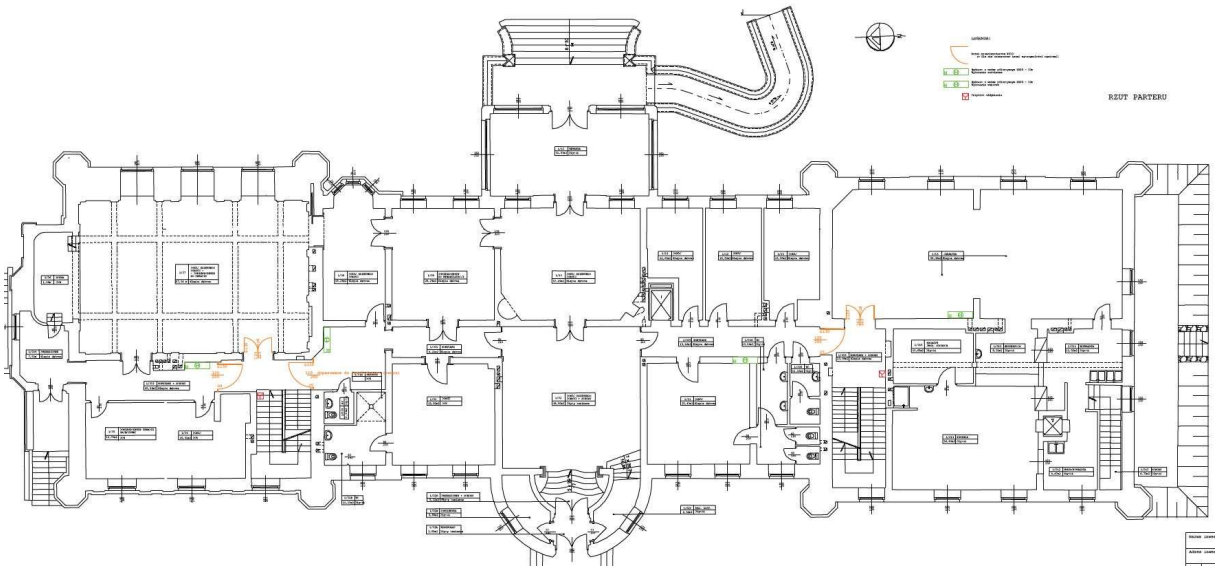


Rysunek 3: Plan drugiego piętra

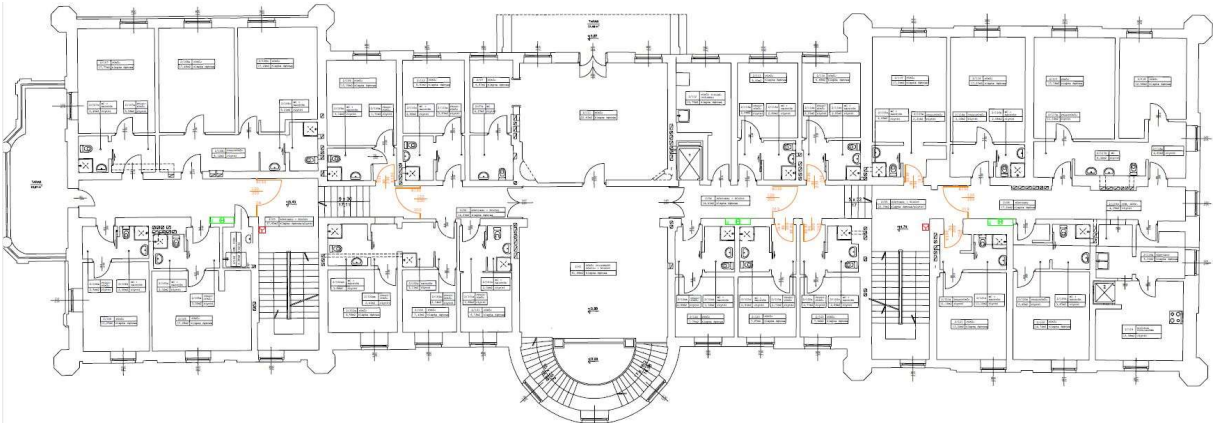
Pałac



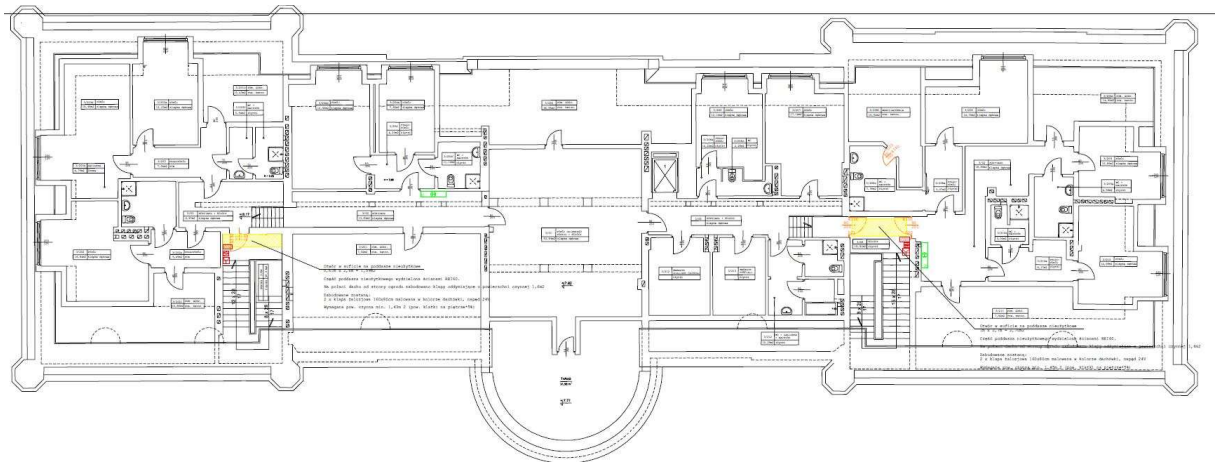
Rysunek 4: Plan piwnicy



Rysunek 5: Plan parteru



Rysunek 6: Plan pierwszego piętra



Rysunek 7: Plan poddasza

Obecny stań sieci

W obecnej chwili w Parsowie jest rozprowadzona sieć LAN oraz WLAN, ale tylko w obrębie pomieszczeń administracyjnych. Należy również zaznaczyć, że sieć nie jest doprowadzona do wszystkich pracowników. Brak jakiejkolwiek infrastruktury sieciowej, z której mogli by skorzystać mieszkańcy. Internet jest doprowadzony mobilnie od Orange. W części pałacowej brak jakiejkolwiek infrastruktury sieciowej. Jedynym pomieszczeniem, gdzie jest dorowadzony Internet jest sala terapeutyczna w piwnicy i jest to realizowane za pomocą radiolinii z budynku administracji. Sieć LAN w biurach wykorzystuje urządzenia domowe takie jak małe niezarządzalne switche, wbudowane access pointy w routery. W budynku nie ma wyznaczonych punktów dystrybucyjnych czy głównej serwerowni, brak infrastruktury ethernetowej oraz światłowodowej. Jedyna istniejąca infrastruktura jest to monitoring, który jest odrębny i nie podlegał audytowi. Ze względu na przyszłe prace i chęć wprowadzenia zaawansowanego systemu sieci bezprzewodowej niezbędne będzie wybudowanie całkowicie nowej infrastruktury sieci LAN. Żadne z obecnie używanych urządzeń nie będzie się nadawać do przyszłego wykorzystania. Pomiędzy budynkiem administracji a pałacem jest przepust kablowy, który można by wykorzystać w przeszłym rozwiązaniu.

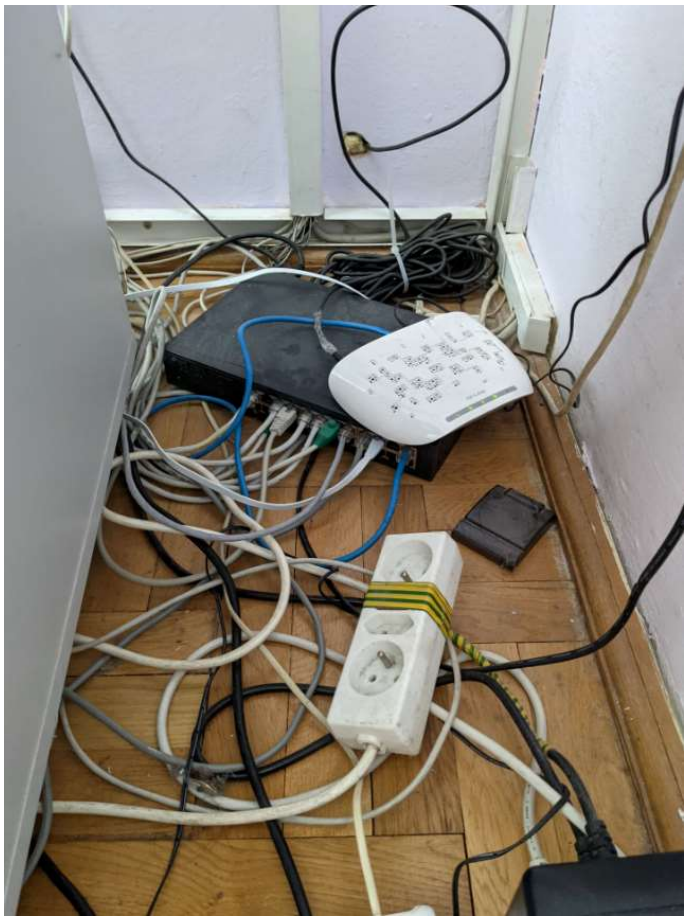
Rysunek 8: Obecne okablowanie w części pałacowej w Parsowie zostało wkute w ściany

Rysunek 9: Router i access point w części terapeutycznej

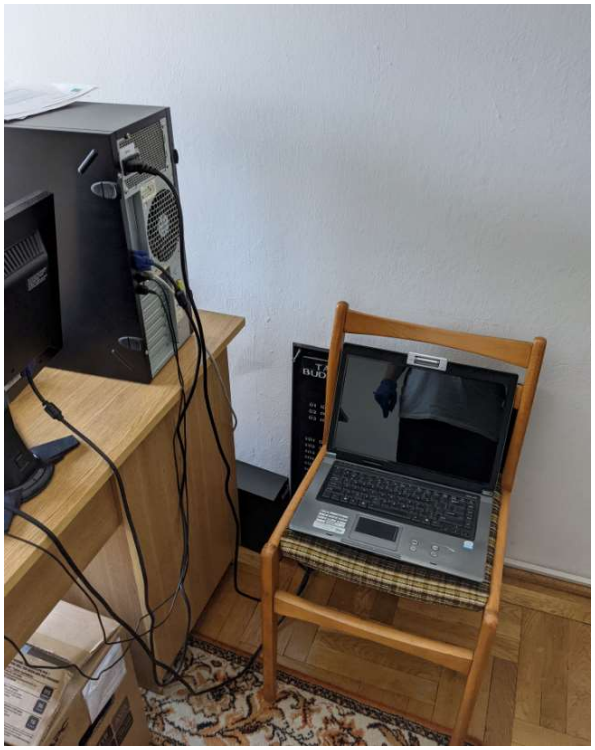
Rysunek 10: Miejsce wejścia przepustu do części pałacowej

Rysunek 11: Radiolinia pomiędzy częścią pałacową a administracyjną

Rysunek 12: Radiolinia pomiędzy częścią pałacową a administracyjną

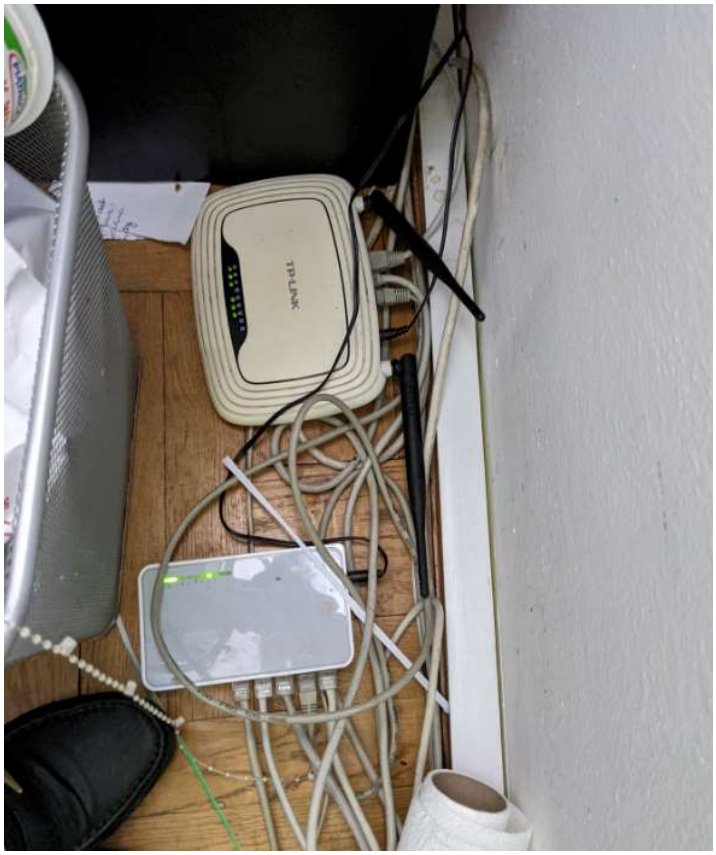


Rysunek 13: Router/access point w części administracyjnej



Rysunek 14: Serwer w pomieszczeniu kasy

Rysunek 15: Główne łącze internetowe



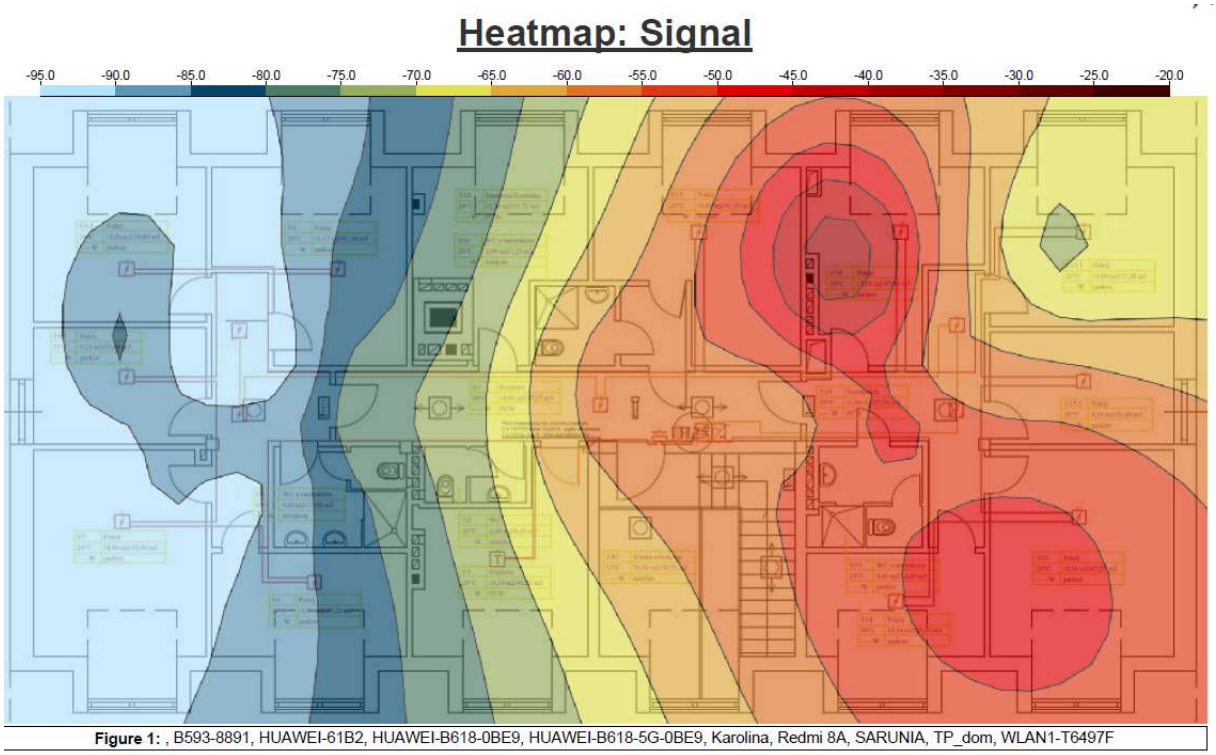
Rysunek 16: Router/access point oraz niezarządzalny switch w budynku administracji

Stan istniejącej sieci WLAN

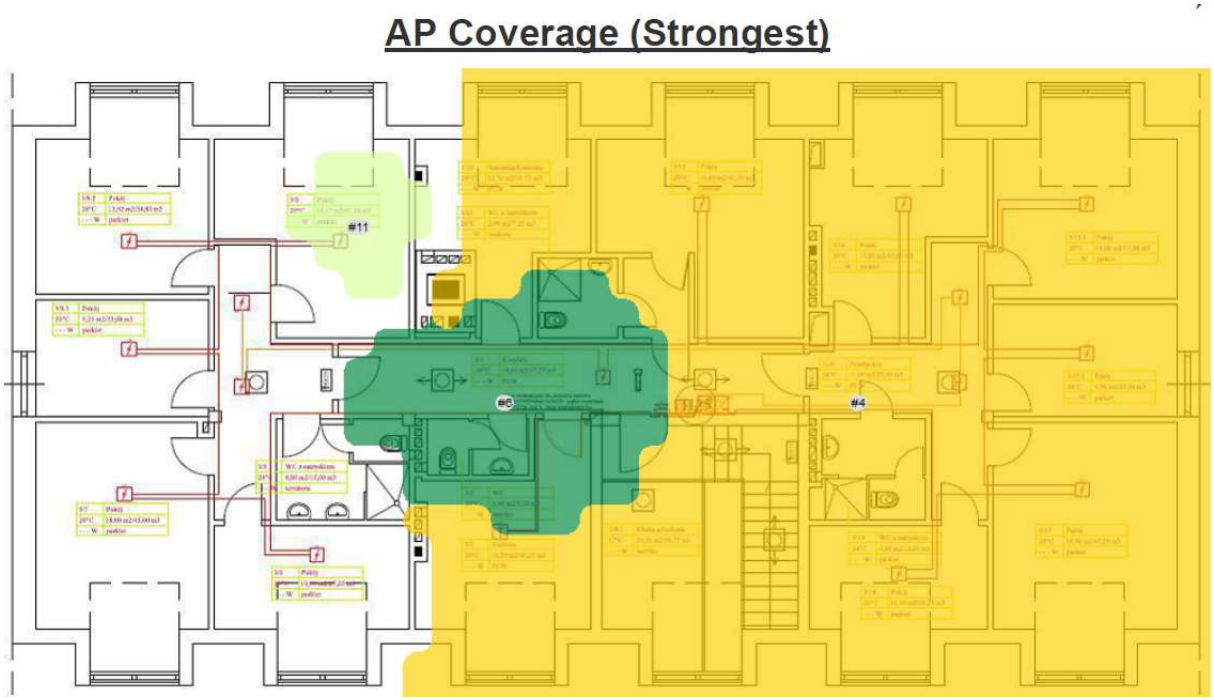
AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
	#5		TpLinkTech:4b:28:df	5/40MHz	150	WPA2	n	10	18	5	0	14
	#7		TpLinkTech:89:b1:52	5/40MHz	150	WPA2	n	7	9	5	0	5
B593-8891	#12		HuaweiTech:61:93:be	8	144	WPA2	n	5	5	5	0	1
DIRECT-45-HP DeskJet 5000 series	#11		local:fa:b4:6a:07:2e:45	11	144	WPA2	n	14	19	10	0	5
HUAWEI-61B2	#4		HuaweiTech:45:61:b2	9/40MHz	300	WPA2	n	32	61	3	0	24
HUAWEI-B618-0BE9	#6		90:2b:d2:1d:0b:e9	4/40MHz	300	WPA2	n	15	38	4	0	21
HUAWEI-B618-5G-0BE9	#10		90:2b:d2:1d:0b:eb	36/80MHz	1300	WPA2	ac	16	16	16	0	1
Karolina	#14		AsiatelcoT:6e:56:76	1/40MHz	300	WPA2	n	0	0	0	0	0
Redmi 8A	#8		local:a6:ab:fd:af:34:e6	1	72	WPA2	n	8	9	7	0	2
SARUNIA	#13		b4:1c:30:71:db:6f	1/40MHz	450	WPA2	n	5	6	4	0	2
TP_dom	#2		TpLinkTech:91:28:2c	10/40MHz	300	WPA2	n	9	14	4	0	8
wlan-test	#1	AP74a0.2f92.c82	CiscoSyste:8b:3e:ff	36	867	WPA2	ac	25	40	17	0	17
wlan-test	#3	AP74a0.2f92.c82	CiscoSyste:8b:3e:f0	11	144	WPA2	n	25	40	3	0	24
WLAN1-T6497F	#9		HuaweiTech:7f:64:fc	2	144	WPA2	n	6	6	6	0	1

Rysunek 17: Sieci widoczne w budynku administracji na drugim piętrze



Rysunek 18: Heat map ukazuje jak rozkłada się moc sygnałów na drugim piętrze z przenośnych access pointów mobilnych mieszkańców

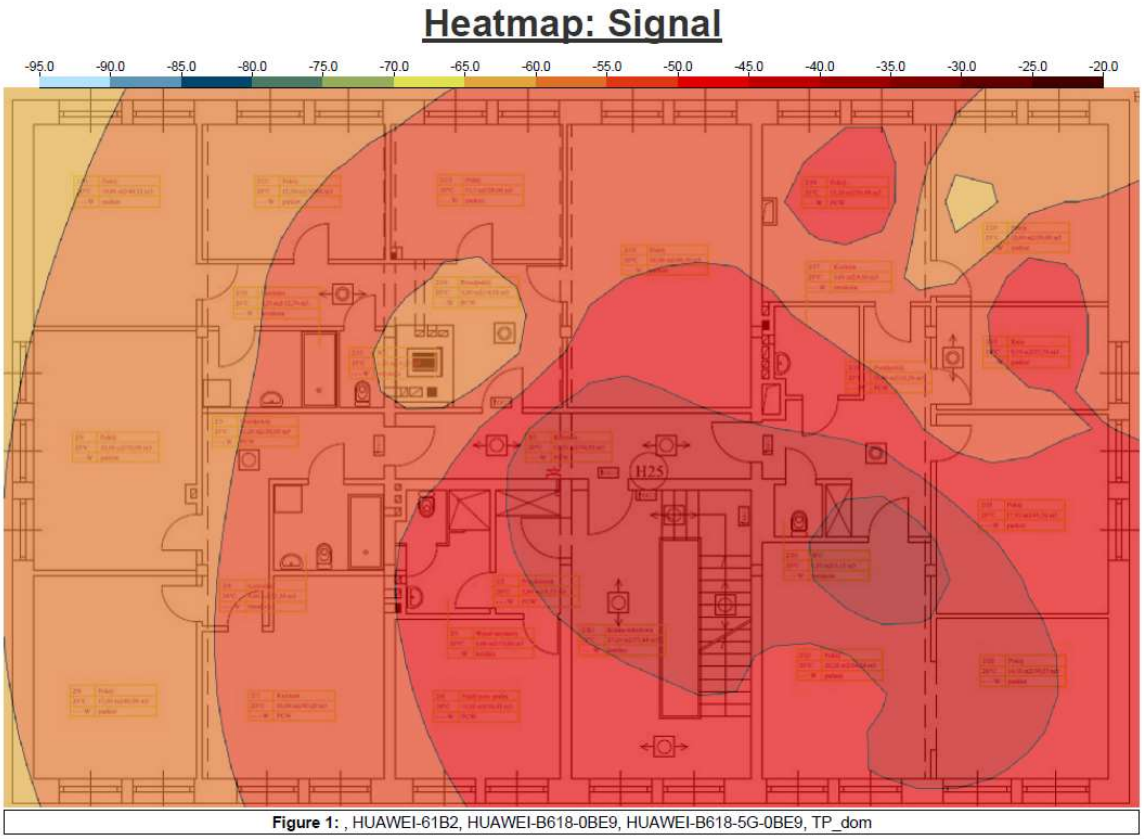


Rysunek 19: Rozkład mocy nadawanych sieci na drugim piętrze

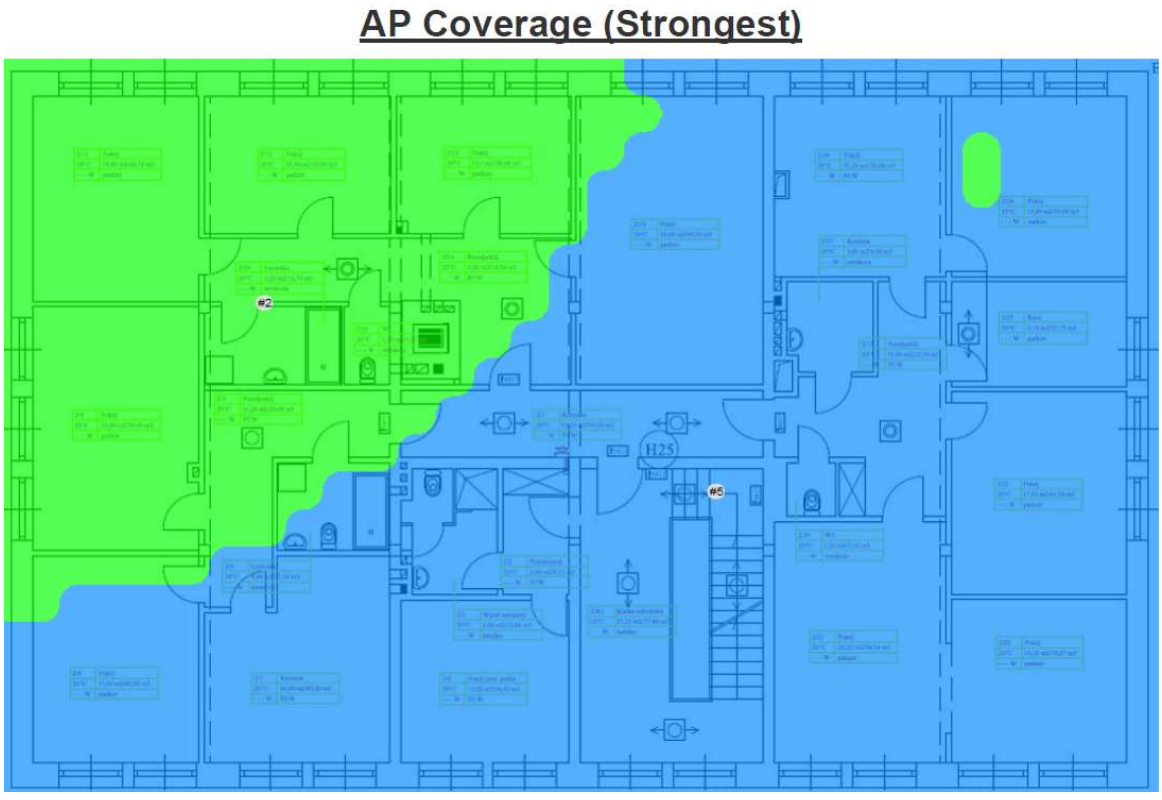
AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
	#4		TpLinkTech:89:b1:52	5/40MHz	150	WPA2	n	16	31	4	0	11
	#6		TpLinkTech:4b:28:df	5/40MHz	150	WPA2	n	15	20	8	0	3
HUAWEI-61B2	#3		HuaweiTech:45:61:b2	9/40MHz	300	WPA2	n	9	15	0	0	9
HUAWEI-B618-0BE9	#5		90:2b:d2:1d:0b:e9	4/40MHz	300	WPA2	n	46	61	26	0	14
HUAWEI-B618-5G-0BE9	#1		90:2b:d2:1d:0b:eb	36/80MHz	1300	WPA2	ac	36	53	15	0	13
TP_dom	#2		TpLinkTech:91:28:2c	10/40MHz	300	WPA2	n	28	43	10	0	14

Rysunek 20: Sieci widoczne w budynku administracji na pierwszym piętrze

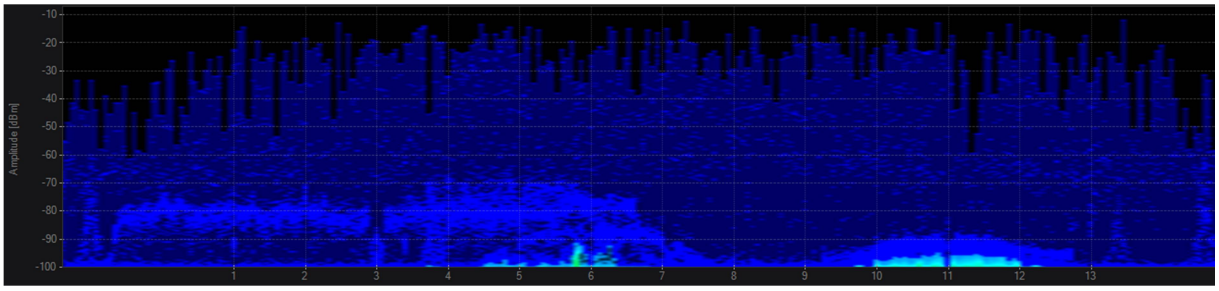


Rysunek 21: Heat mapa z rozkładem mocy sygnalu w części biurowej

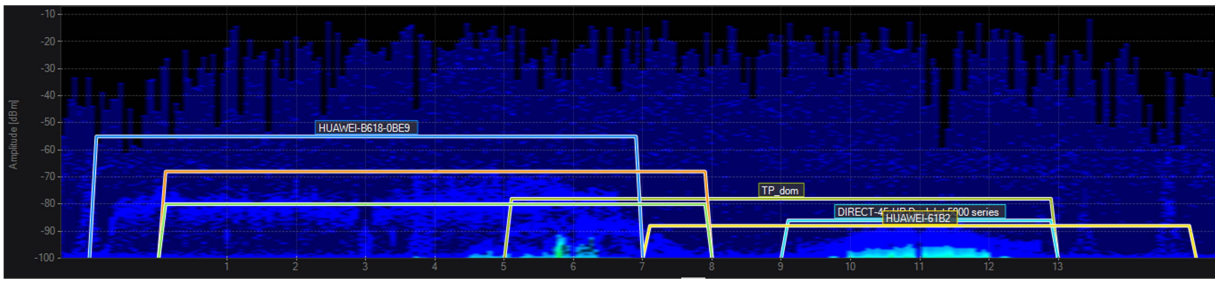


Rysunek 22: Rozkład mocy nadawanych sieci na pierwszym piętrze

Pomiar widma w Parsowie



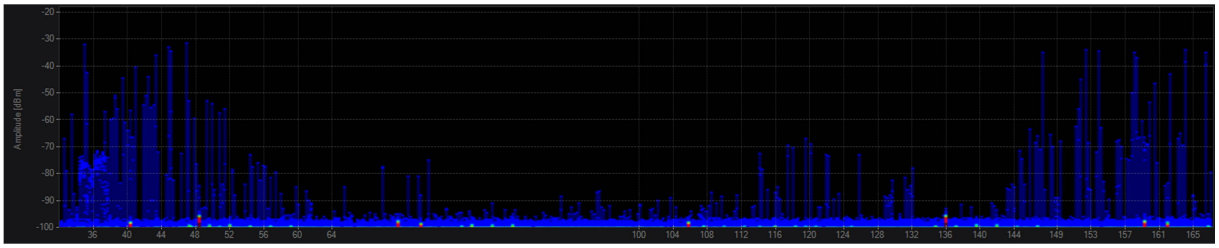
Rysunek 23: Pomiar widma dla 2,4GHz



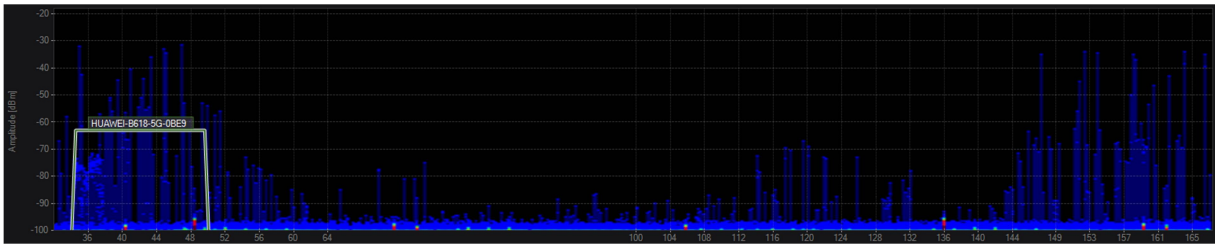
Rysunek 24: Pomiar widma dla 2,4GHz wraz z zaznaczonymi sieciami

ESSID	AP Alias	Channels	Signal Strength (dBm)	BSSID Count	Security	Max Rate (Mbps)	Vendors	802.11
DIRECT-45-HP DeskJet 5000 series		11	-86	1	WPA2-Personal	144,4		g, n
HUAWEI-B618-0BE9		5-1	-55	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
		6-2	-80	1	WPA2-Personal	150,0	Tp-Link Technologies Co.,Ltd.	b, g, n
		6-2	-68	1	WPA2-Personal	150,0	Tp-Link Technologies Co.,Ltd.	b, g, n
HUAWEI-61B2		9+13	-88	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
TP_dom		11-7	-78	1	WPA2-Personal	300,0	Tp-Link Technologies Co.,Ltd.	b, g, n
HUAWEI-B618-5G-0BE9		42 [36]	-63	1	WPA2-Personal	1300,0	Huawei Technologies Co.,Ltd	n, ac

Rysunek 25: Lista widocznych sieci



Rysunek 26: Pomiar widma dla 5GHz

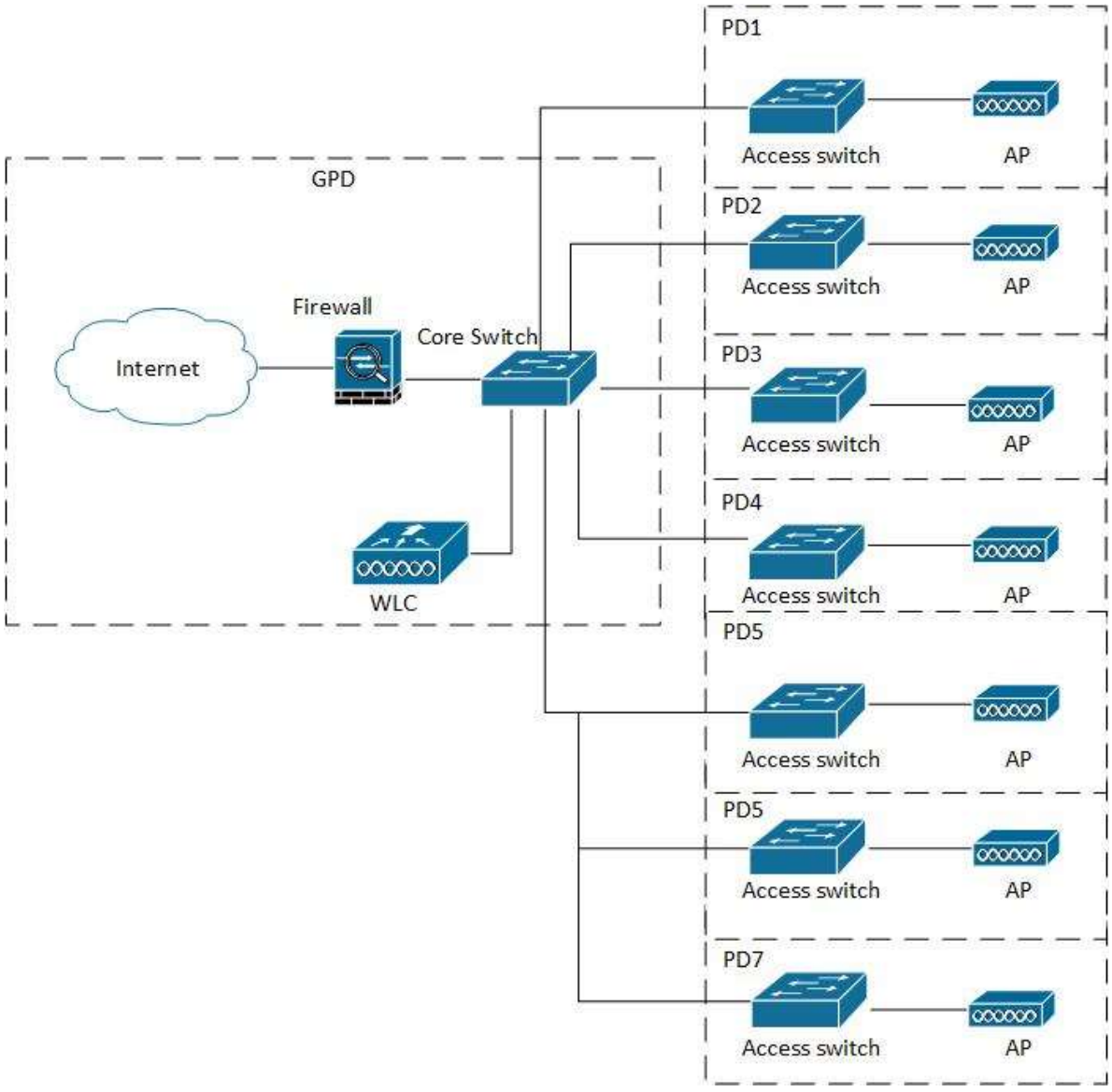


Rysunek 27: Pomiar widma dla 5GHz wraz z zaznaczonymi sieciami

Jak widać na powyższych obrazkach jedynie co można zaobserwować do sygnały pochodzące z obecnie propagowanych sieci. Nie występują zakłócenia w tym paśmie. Dla 5GHz można na poziomie szumów zobaczyć małe czerwone zakłócenia, które nie mają żadnego wpływu na sieć bezprzewodową, najprawdopodobniej pochodzą one od operatora telekomunikacyjnego.

Koncepcja nowej sieci LAN

Nowa sieć LAN powinna zostać zbudowana całkowicie od nowa. W części administracyjnej jest rozprowadzone okablowanie schodzące się do jednego punktu, ale jest to jedyne miejsce, gdzie taka infrastruktura jest. W pozostałej części mieszkalnej oraz pałacowej nie ma żadnej infrastruktury ani ethernetowej, ani światłowodowej. Niezbędne będzie zainstalowanie nowych szaf rackowych. Należy rozprowadzić nowe połączenia światłowodowe pomiędzy wszystkimi punktami pośrednimi, a główną serwerownią. Na styku nowej sieci LAN z Internetem powinno znaleźć się urządzenie zabezpieczające sieć wewnętrzną – firewall. W każdym punkcie dystrybucyjnym należy umieścić przełącznik dostępowy co najmniej 24 portowy PoE/PoE+, tak aby podłączyć wszystkie access pointy. Każdy z punktów następnie zostanie podłączony do switcha corowego w głównej serwerowni. Należy przyjąć architekturę gwiazdy, w której każdy pośredni punkt dystrybuujmy będzie bezpośrednio podłączony do GPD. W głównej serwerowni będzie również zainstalowany kontroler sieci bezprzewodowej.

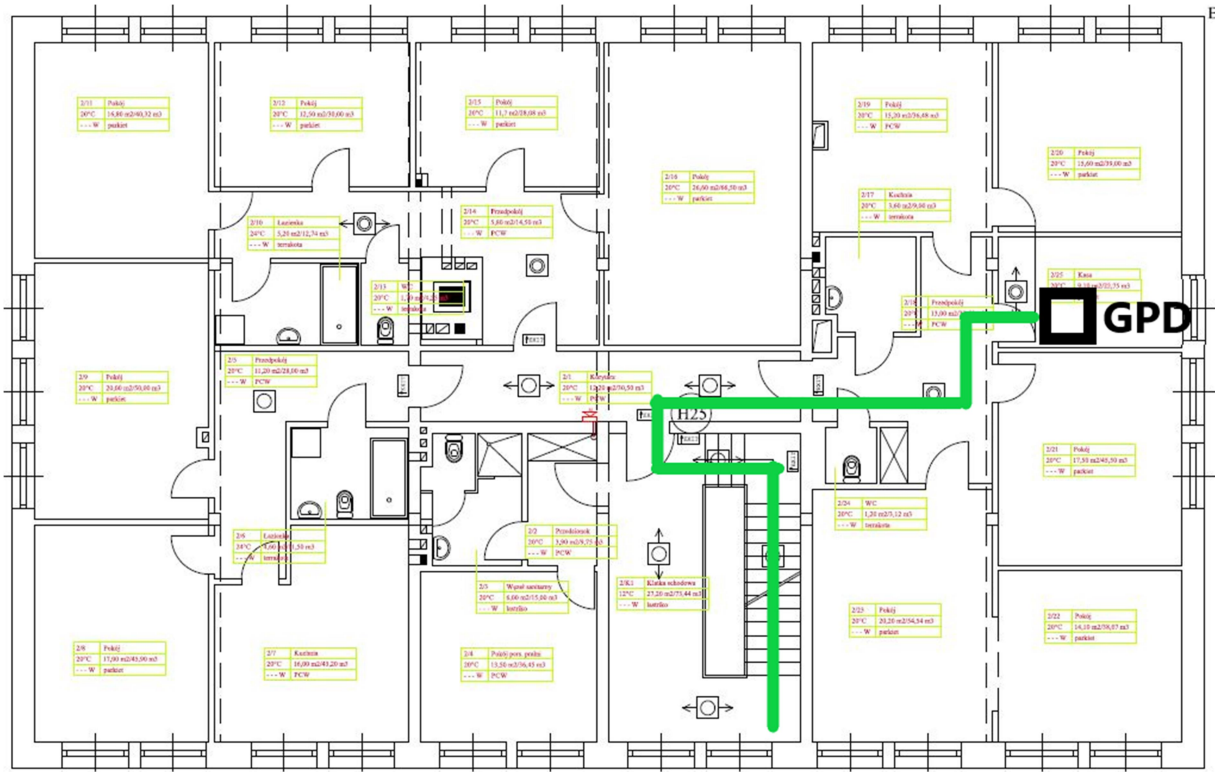


Rysunek 28: Schemat nowej sieci LAN

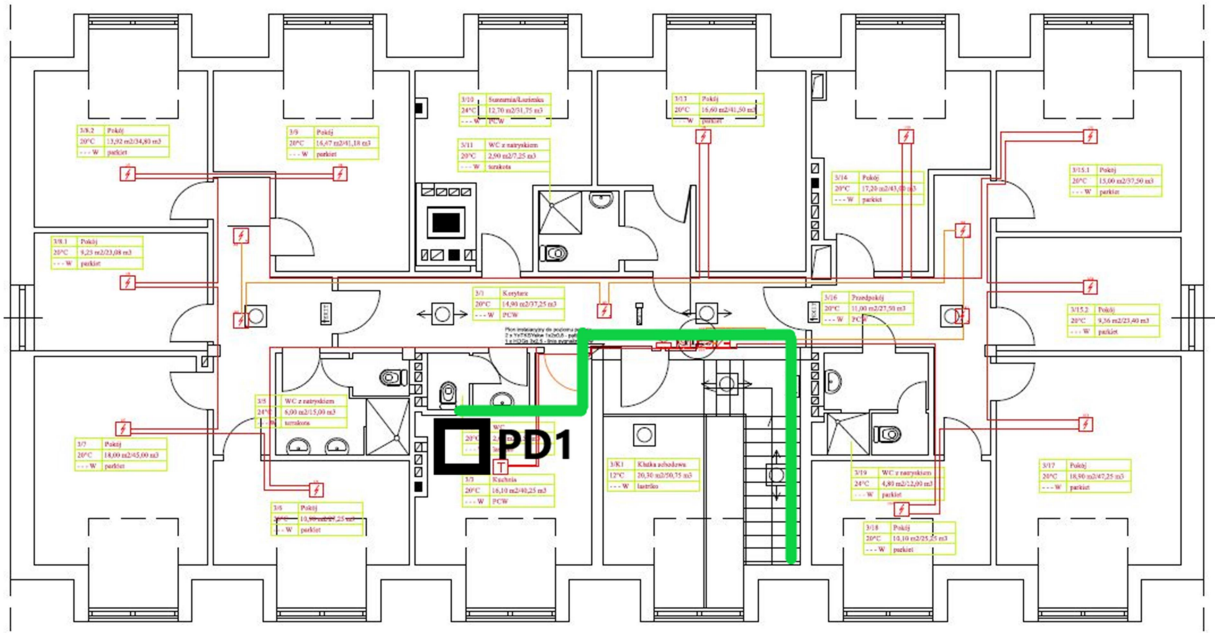
Punkty dystrybucyjne

Prowadzenie kabli światłowodowych

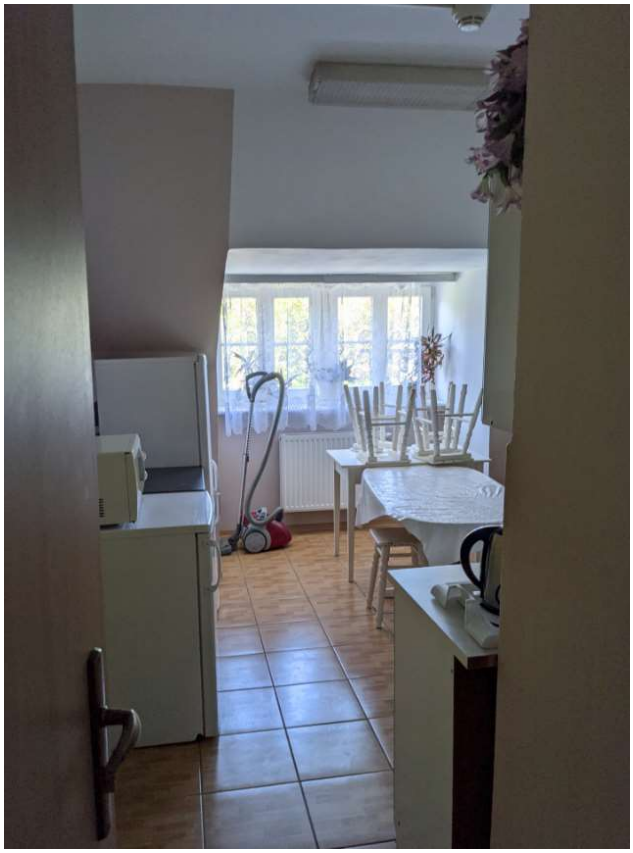
Kable światłowodowe ze wszystkich PD w całym pałacu zejdą się do PD4, skąd dalej przepustem zostaną doprowadzone do budynku administracji. Całe okablowanie zostanie doprowadzone do lewej klatki schodowej skąd dalej przez korytarz oraz pomieszczenia mieszkalne zostanie dalej przebite do PD4, znajdującego się w małym pomieszczeniu pod schodami. Okablowanie zostanie ukryte w korytach kablowych o jak najmniejszym przekroju. W razie potrzeby koryta zostaną pomalowane w odpowiednim kolorze. Koryta zostaną umieszczone w samym rogu na styku ściany oraz sufitu.



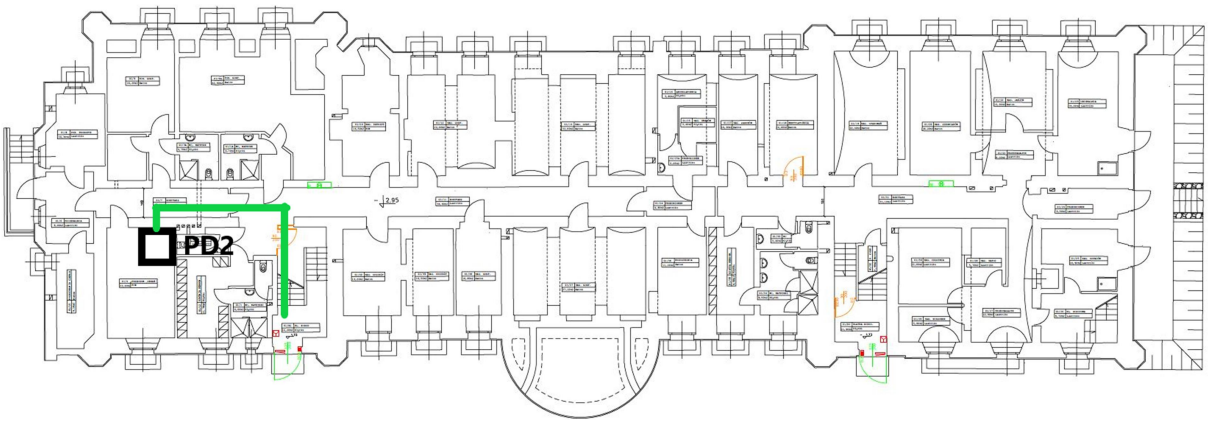
Rysunek 29: Koncepcja trasy światłowodu i instalacji szafy GPD – pomieszczenie kasy, ze względu na brak jakiegokolwiek wolnego pomieszczania, nowa główna serwerownia została zaproponowana w pomieszczeniu kasy, które również w obecnej chwili spełnia tą rolę.



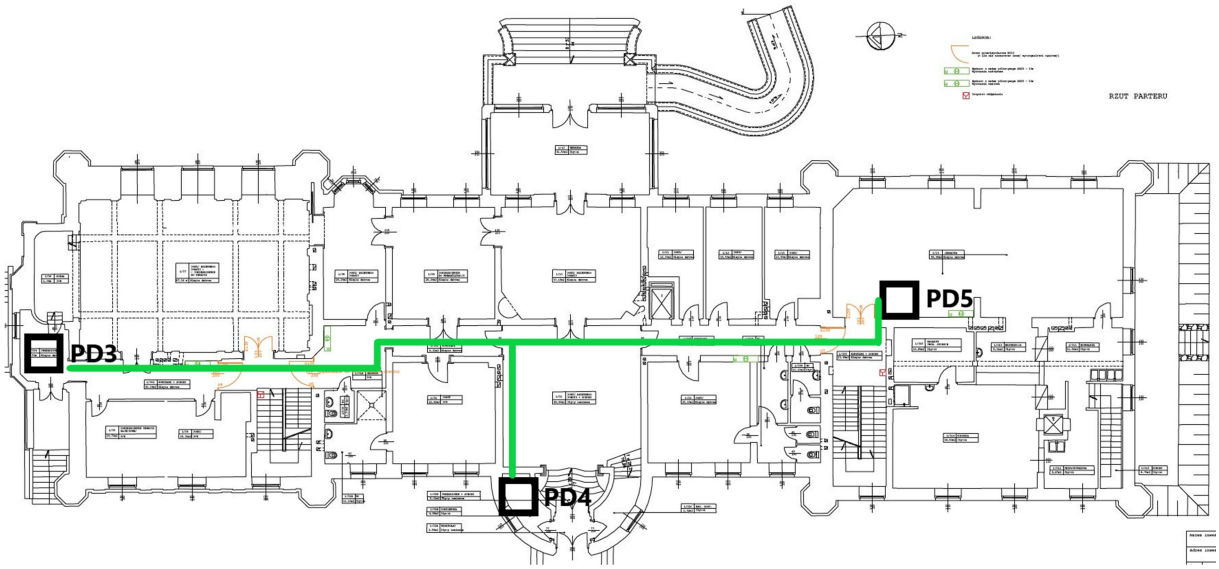
Rysunek 30: Koncepcja trasy światłowodu i instalacji szafy PD1 – część mieszkalna, pokój socjalny, zejście po klatce schodowej do GPD



Rysunek 31: Miejsce instalacji szafy PD1 – pomieszczenie kuchni

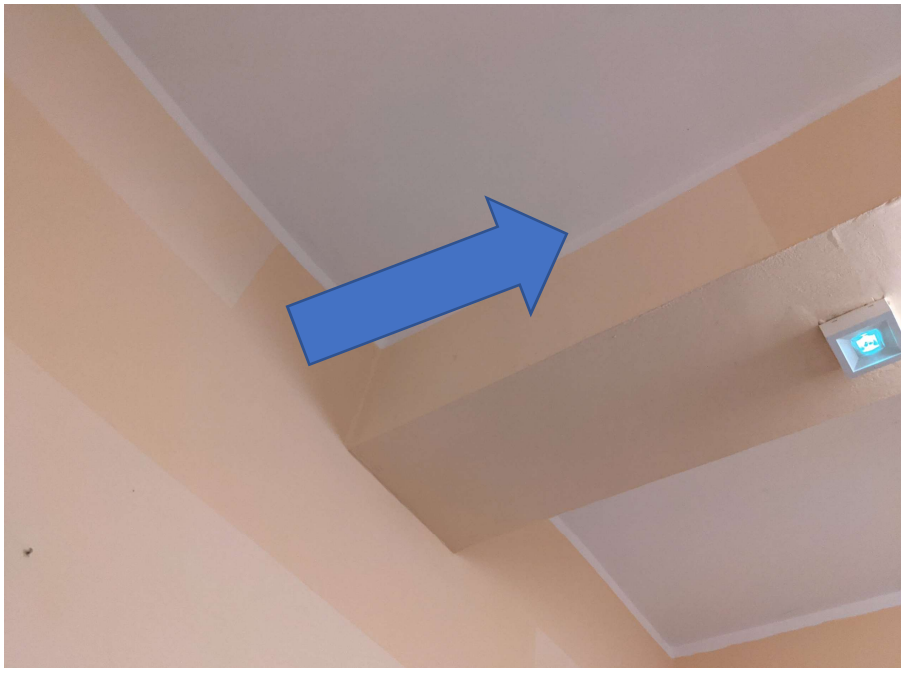


Rysunek 32: Koncepcja trasy światłowodu i instalacji szafyPD2 – pokój zajęciowy, zejście z kablami do PD4, które będzie łącznikiem do GDP



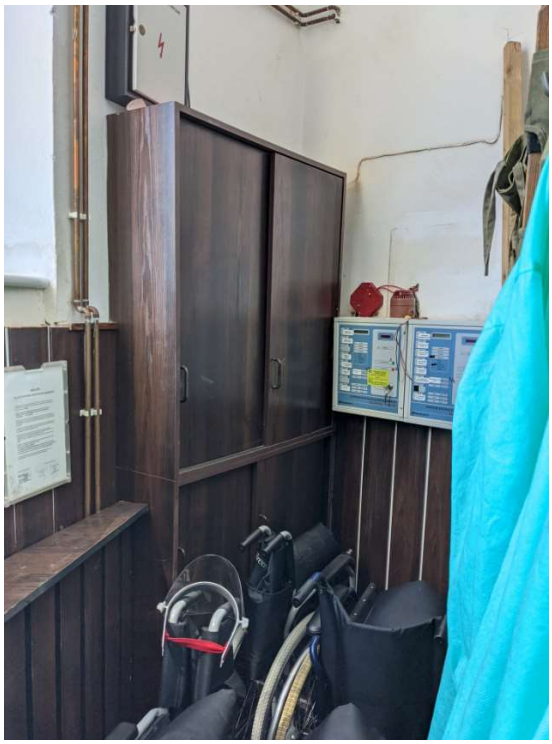
Rysunek 33: Koncepcja trasy światłowodu i instalacji szafy PD3 – magazynek, zejście z kablami do PD4, a następnie do GPD, PD4 – w tym miejscu wchodzi przepust łączący pałac z budynkiem administracji, będzie to punkt połączenia obu lokalizacji, od projektanta będzie zależeć czy przepuścić wszystko do GPD, czy zainstalować tu krosownicę światłowodową, PD5 – jadalnia, zejście z kablami korytarzem do PD4, PD5 zostanie przeniesione z pomieszczeni jadalni na korytarz i jeżeli będzie to możliwe pod względem projektowym umieszczone we wnęce jak na zdjęciu poniżej

Rysunek 34: Miejsce instalacji szafy PD5

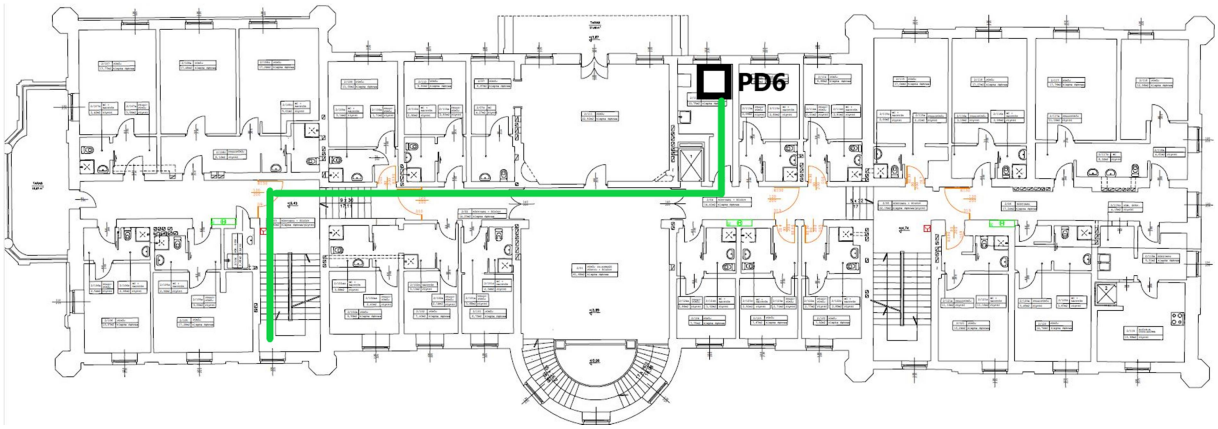


Rysunek 35: Proponowana trasa instalacji koryt kablowych

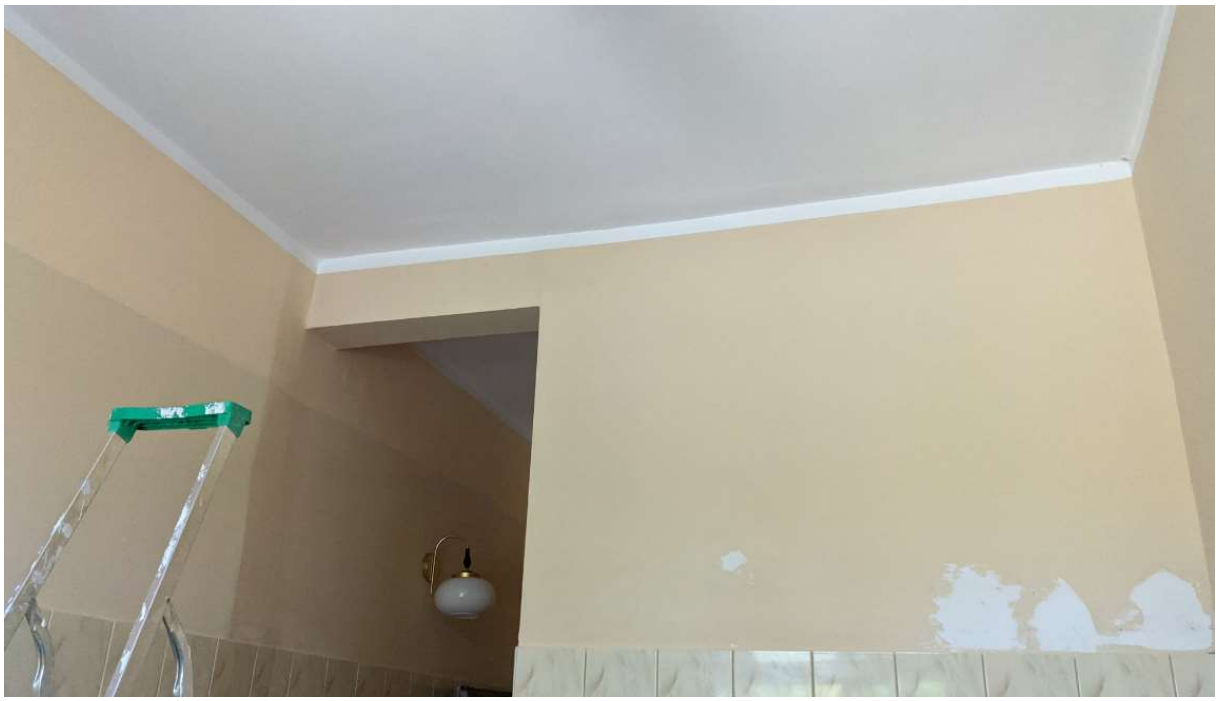
W takich korytarzach jak ten pomiędzy PD4, a PD3 należy brać pod uwagę, że koryta musza być instalowane w rogach na styku ścian i sufitu, tak żeby nie przechodzić przez środek pomieszczenia. Należy taż pamiętać, że koryta powinny być na ile to możliwe jak najmniej widoczne.



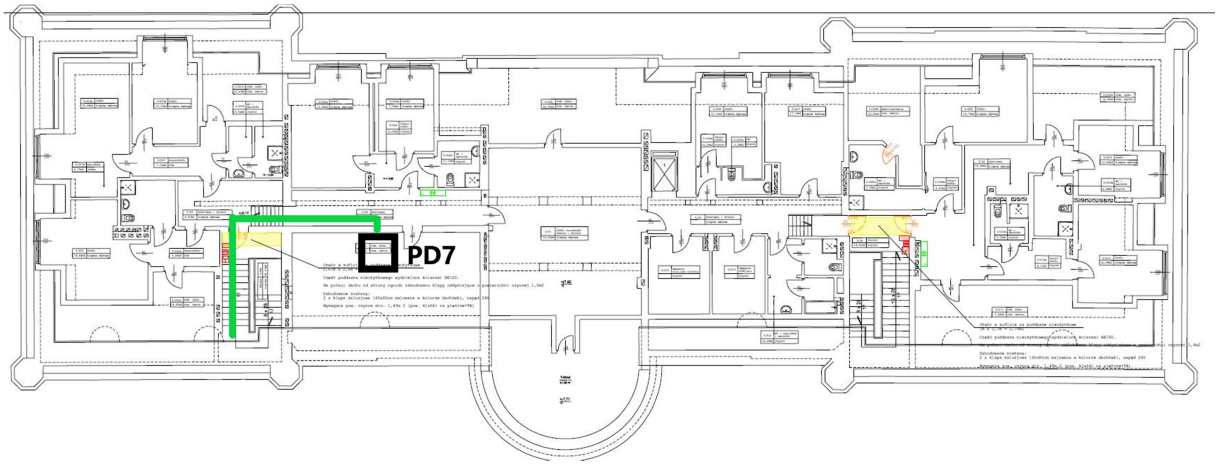
Rysunek 36: Koncepcja trasy światłowodu i instalacji szafy PD4 – punkt stuku pałacu z budynkiem administracji



Rysunek 37: Koncepcja trasy światłowodu i instalacji szafy PD6 – pomieszczenie pielęgniarskie, zejście z kablami do PD4 po lewej klatce schodowej



Rysunek 38: Proponowane miejsce instalacji szafy PD6 – ściana w pokoju pielęgniarskim



Rysunek 39: Koncepcja trasy światłowodu i instalacji szafy PD7 – nowe pomieszczenie Sali komputerowej, zejście z kablami do PD4 przez lewą klatkę schodową

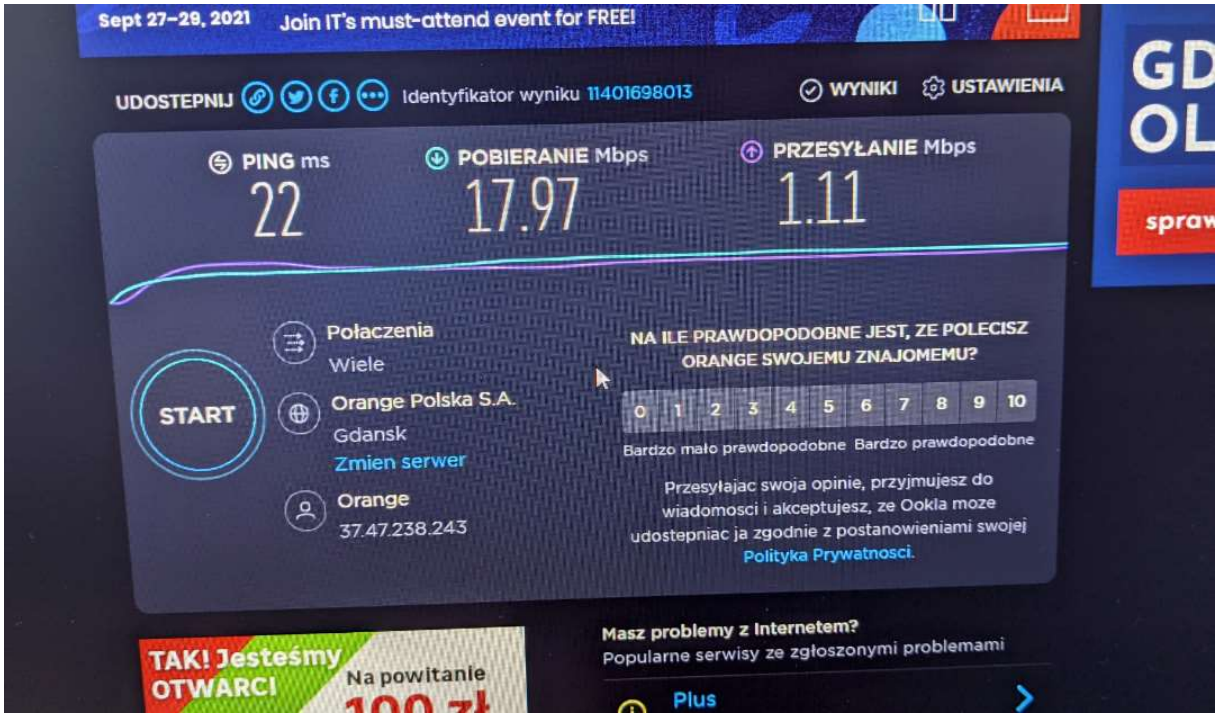
Jeżeli będzie to możliwe, to zamiast puszczać na około światłowód w korycie po klatce schodowej dopuszcza się przebicie stropu.

Rysunek 40: Miejsce przebicia stropu

Rysunek 41: Proponowane miejsce instalacji szafy PD7 – nowa sala komputerowa.

Analiza możliwości przyłączenia do zewnętrznej szerokopasmowej sieci internetowej

W obecnej chwili Internet w Parsowie jest doprowadzony mobilnie od Orange. Ze względu na położenie brak możliwości doprowadzenia światłowodu. Można przeprowadzić 3 video konferencje na raz. Możliwa jest zamiana łącza internetowego na łącze stacjonarne od Orange.



Rysunek 42: Test prędkości łącza internetowego przeprowadzony z komputera stacjonarnego.

Koncepcja rozmieszczenia nowych punktów dostępowych wraz z doporowadzeniem tras kablowych oraz protokół pomiarowy stanowiący podstawę do opracowania dokumentacji

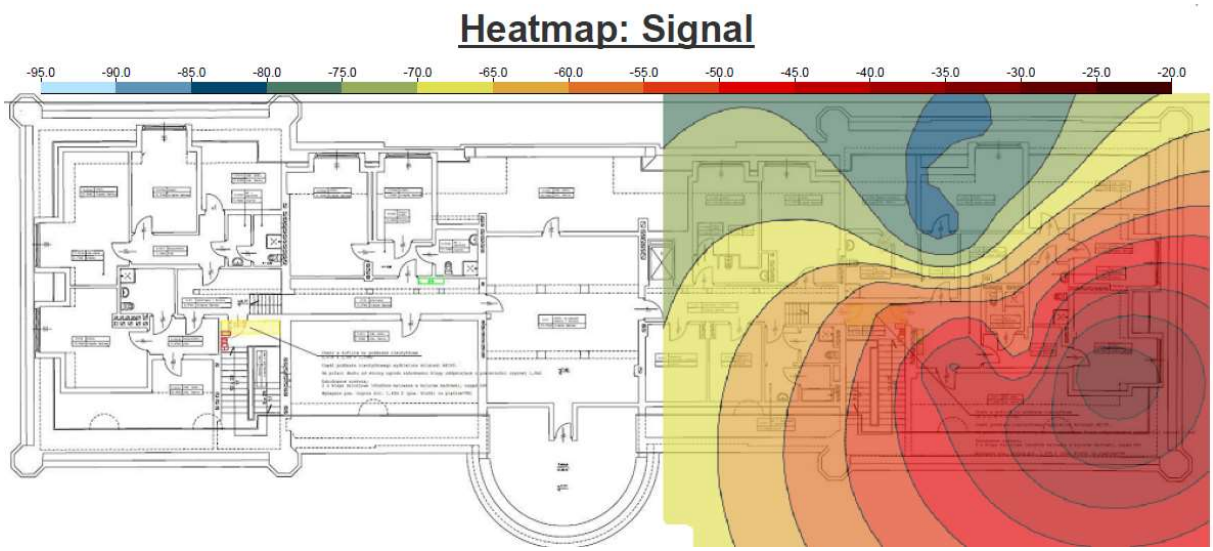
W Parsowie planowaniem radiowym objęty został zarówno pałac wraz z obszarami zewnętrznymi jak budynek administracji. W części administracyjnej po konsultacji z pracownikami i z Zamawiającym ustalone zostało, że części biura i mieszkalna będą pokryte sygnałem radiowym w całości natomiast część parterowa tylko we wskazanych miejscach. W część pałacowej piętra mieszkalne w całości wraz z zachowaniem triangulacji do lokalizacji natomiast część piwniczna tylko we wskazanych miejscach terapeutycznych oraz magazynowych.

Aktualizacja rozmieszczenia access pointów wraz z zaznaczonymi trasami kablowymi do najbliższego punktu dystrybucyjnego.

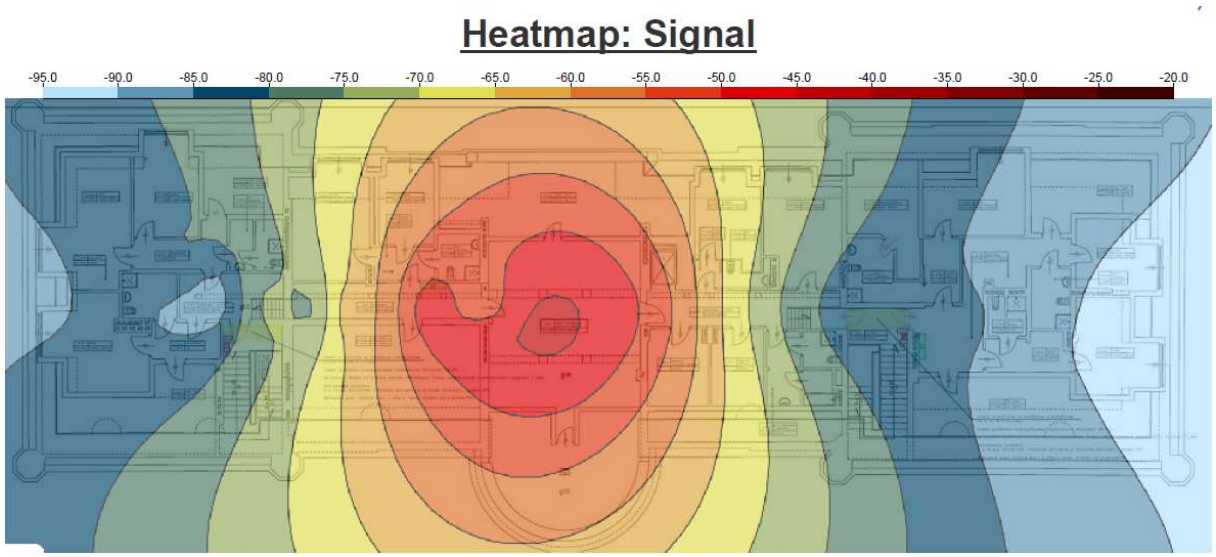
- Kable ethernetowe muszą być prowadzone w korytach kablowych dołożonych do istniejącej infrastruktury.
- Koryta muszą być zamaskowane kolorem, jeżeli będzie taka potrzeba.
- Instalacja access pointów będzie pod sufitem czy to w pokoju, czy na korytarzu.

Badania sieci radiowej

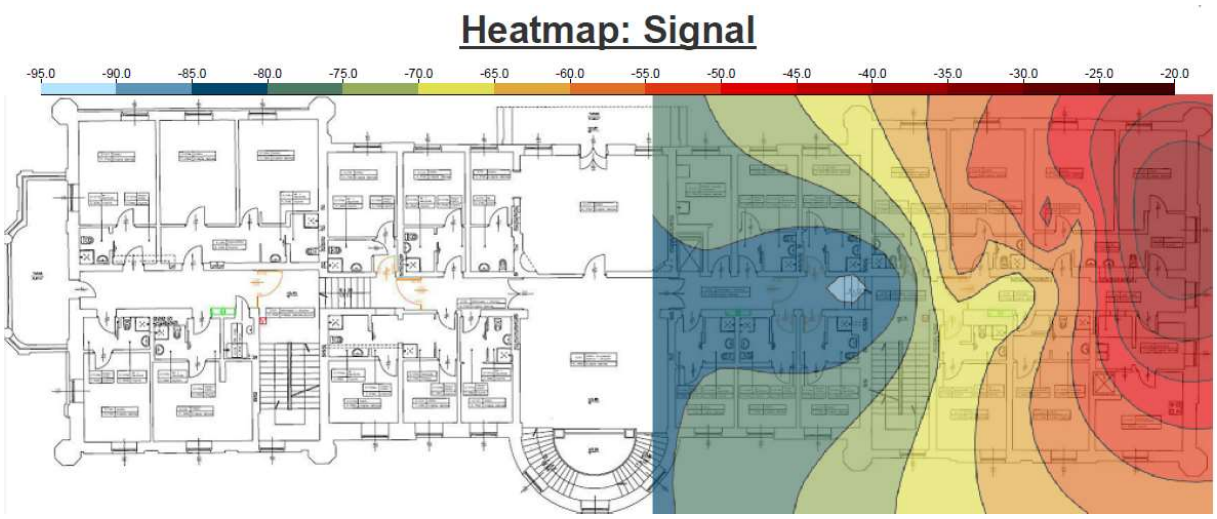
Wykonane zostały badania tłumienia ścian, które pozwoliło na późniejsze przygotowanie rozmieszczenia access pointów na terenie całego DPS-u.



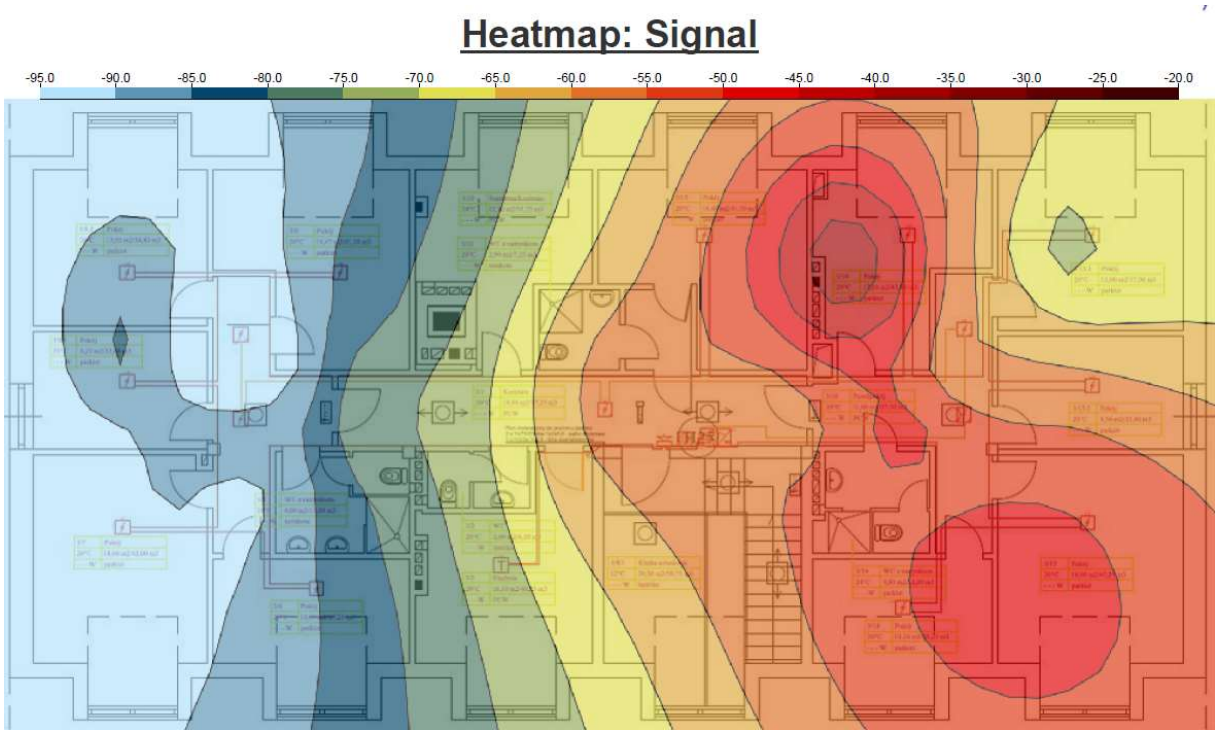
Rysunek 43: Badanie na poddaszu, w którym access point został umieszczony w narożnym pokoju mieszkalnym



Rysunek 44: Badanie na poddaszu, w którym, access point został umieszczony na środku korytarza



Rysunek 45: Badanie na pierwszym piętrze, w którym access point został umieszczony w narożnym pokoju

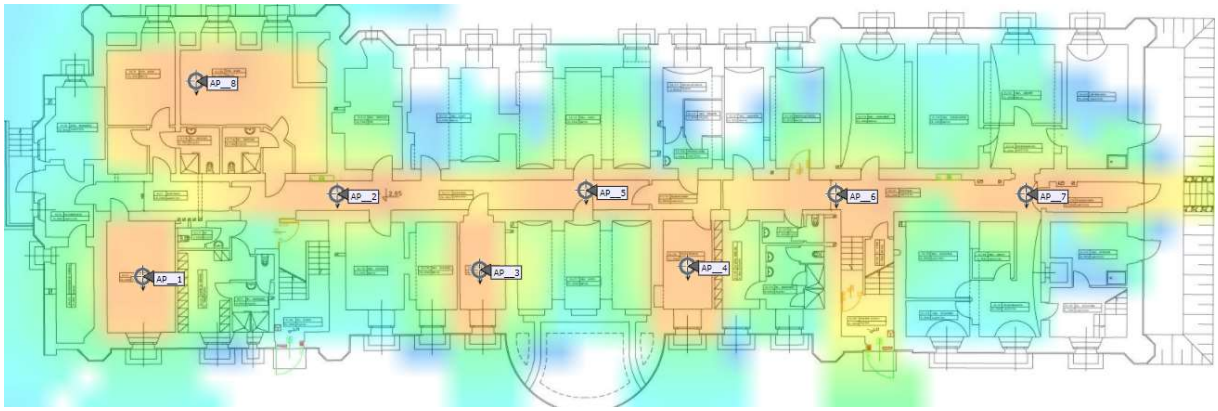


Rysunek 46: Badanie na drugim piętrze, w którym access point został umieszczony w pokoju mieszkalnym

W czasie badania w części pałacowej można zaobserwować bardzo duży spadek sygnału spowodowany grubymi (czasem do 25 cm) ścianami. W części administracyjnej jest lepiej, ale należy mieć na uwadze, szczególnie na drugi piętrze spadziste dachy.

Pałac

Piwnica

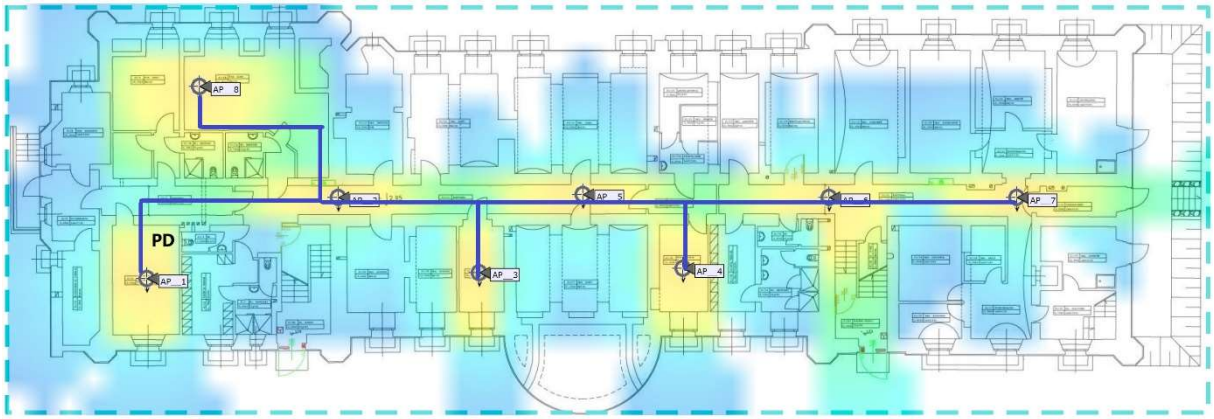


Rysunek 47: Planowanie dla częstotliwości 2,4GHz

Rysunek 48: Planowanie dla częstotliwości 5GHz

W piwnicy pałacu przewidzianych zostało osiem access pointów, tylko w pomieszczeniach zajęciowych lub socjalnych i w częściach magazynowych. Całe okablowanie z piwnicy powinno zejść się do szafy w pomieszczeniu terapii tam, gdzie jest przewidziany AP1.

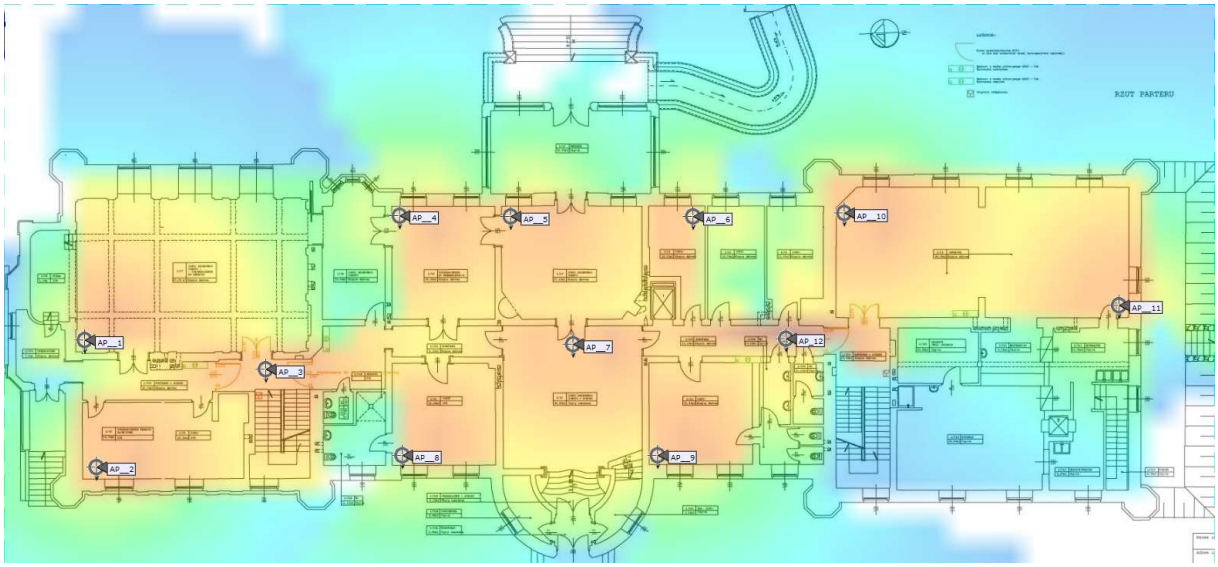
Planowane trasy kablowe



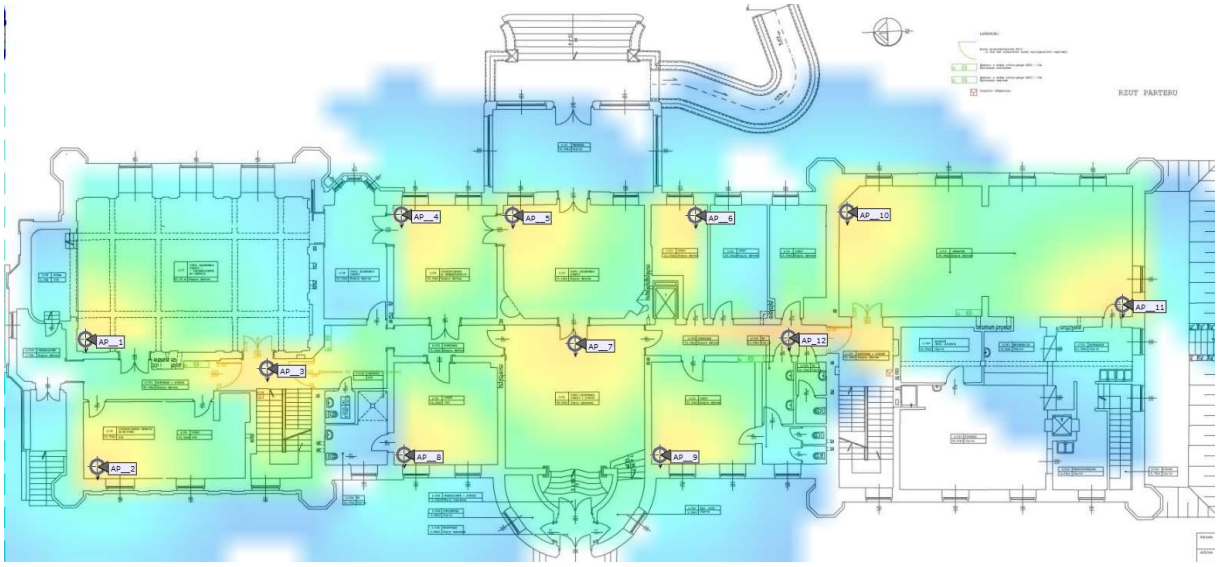
Rysunek 49: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	5
AP2	15
AP3	25
AP4	35
AP5	30
AP6	40
AP7	55
AP8	25

Parter



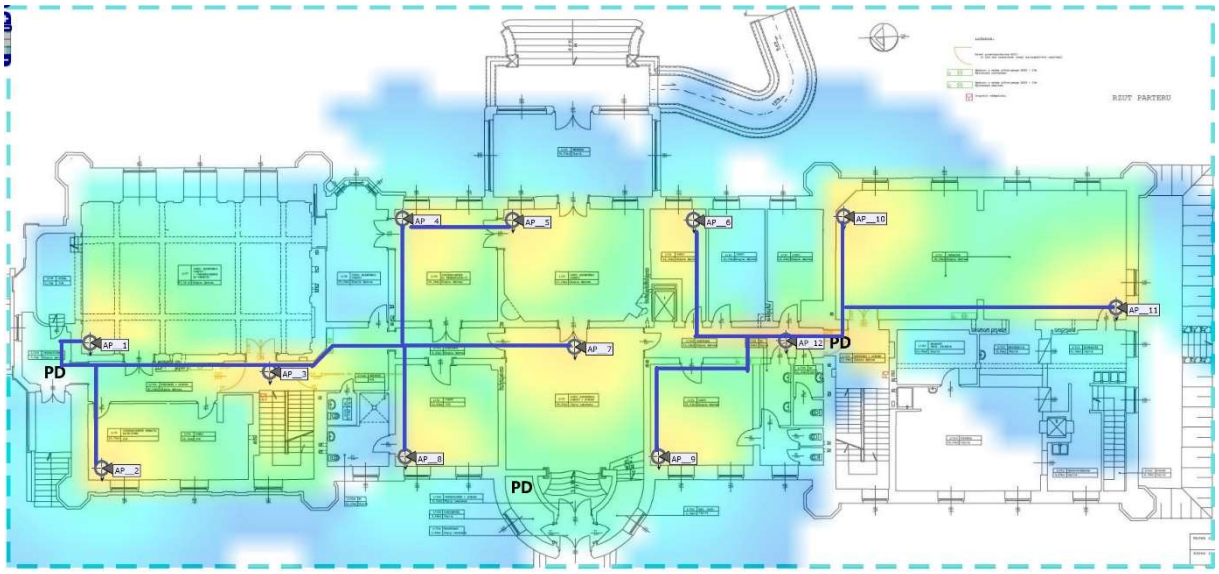
Rysunek 50: Planowanie dla częstotliwości 2,4GHz



Rysunek 51: Planowanie dla częstotliwości 5GHz

Na parterze przewidzianych zostało dwanaście access pointów. Zaproponowane zostały punkty dystrybucyjne, do których mogą zejść się access pointy. Ze względu na utrudnione przechodzenie z kablami przez ściany proponujmy umieścić okablowanie w korytach wzdłuż korytarza.

Planowanie tras kablowych



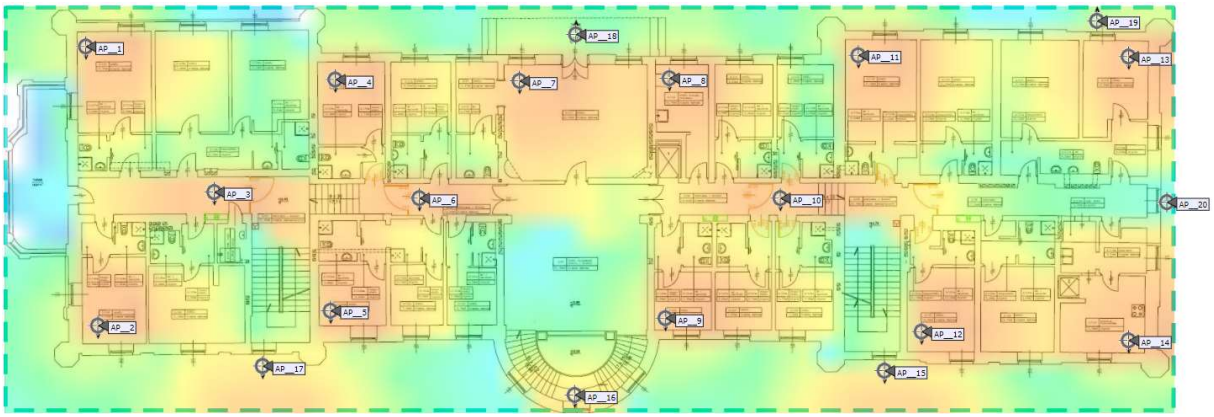
Rysunek 52: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	5
AP2	15
AP3	20
AP4	40
AP5	45
AP6	40
AP7	55
AP8	35
AP9	30
AP10	40
AP11	50
AP12	5

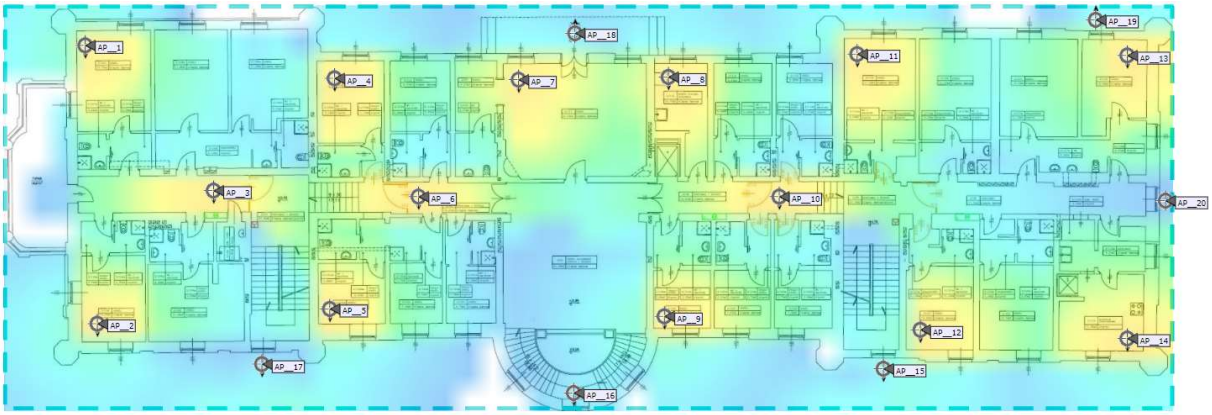
Na parterze okablowanie zejdzie się do wskazanych PD. Access point w sali balowej może zostać zainstalowany na płasko do ściany nad gzymsem. Okablowanie powinno przejść bezpośrednio do pomieszczenia magazynowego, gdzie znajduje się szafa. Na etapie prac projektowych należy wykonać odkrywkowe badania konserwatorskie dla tego punktu. Tak jak przypadku okablowania światłowodowego całe okablowanie ethernetowe będzie umieszczone w zamaskowanych korytach kablowych. Będzie ono prowadzone na styku ściany i sufitu.

Rysunek 53: Access point w rogu sali balowej, musi zostać zlicowany ze ścianą

Pierwsze piętro



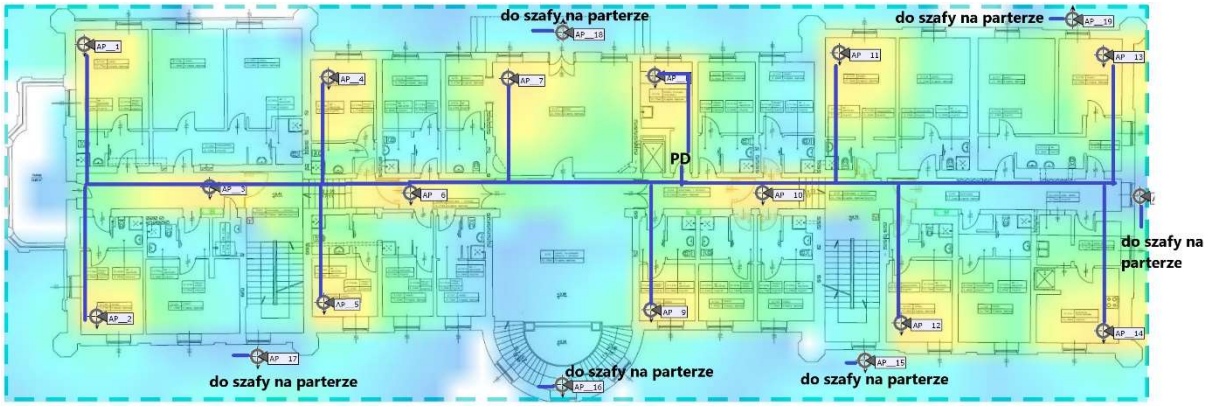
Rysunek 54: Planowanie dla częstotliwości 2,4GHz



Rysunek 55: Planowanie dla częstotliwości 5GHz

Na pierwszym piętrze przewidziane zostały dwadzieścia access pointów, w tym AP15-AP20 są to urządzenia zewnętrzne do mocowania na elewacji budynku. Ze względu, że na pierwszym piętrze jest tylko zaproponowany jeden punkt dystrybucyjny całe okablowanie proponujemy puścić wzdłuż korytarza.

Planowanie tras kablowych



Rysunek 56: Na pierwszym piętrze całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	65
AP2	65
AP3	60
AP4	50
AP5	50
AP6	45
AP7	30
AP8	10
AP9	15
AP10	15
AP11	30
AP12	30
AP13	55

AP14	55
AP15	40
AP16	20
AP17	40
AP18	55
AP19	40
AP20	40

Nowe umiejscowienie access pointów zewnętrznych

Cześć przednia pałacu – lewa

Rysunek 57: Access point możliwy do umieszczenia obok lampy ewakuacyjnej, zlicowany z elewacją, okablowanie do środka do najbliższego PD na parterze.

Cześć przednia pałacu – prawa

Rysunek 58: Analogicznie po prawej stronie, możliwa instalacja obok lampy nad drzwiami, zejście z okablowaniem do PD na parterze

Access point środkowy

Rysunek 59: Możliwy do umieszczenia pod tablicą pałacową, zlicowany z elewacją. Okablowanie przez ścianę do pomieszczenia pod schodami

Część boczna pałacu

Rysunek 60: Access point możliwy do zainstalowania obok lampy, okablowanie do PD na parterze lub piwnicy do ustalenia w czasie prac projektowych

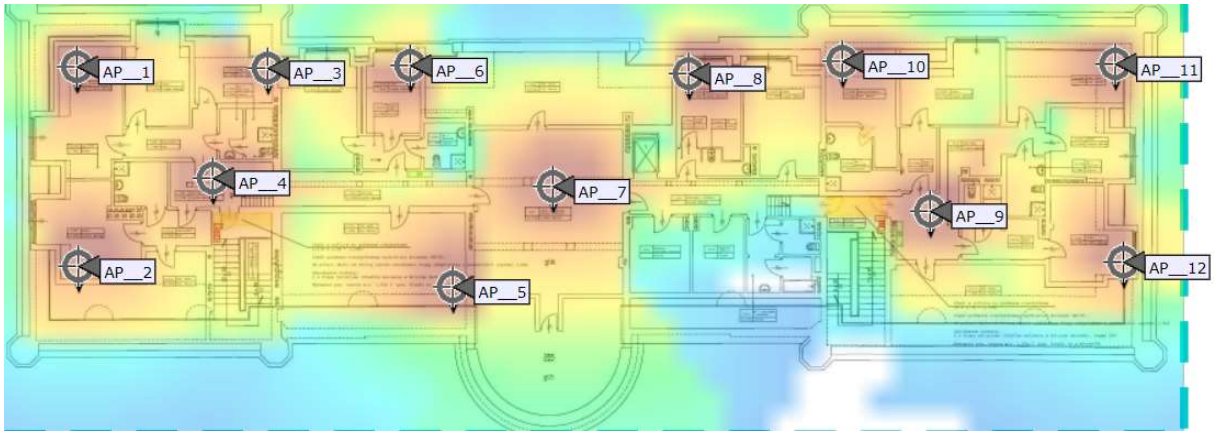
Część tylna pałacu – lewa

Rysunek 61: Możliwe do instalacji urządzenie pod oknem pod szarym pasem, zlicowane do elewacji, okablowanie do PD na parterze

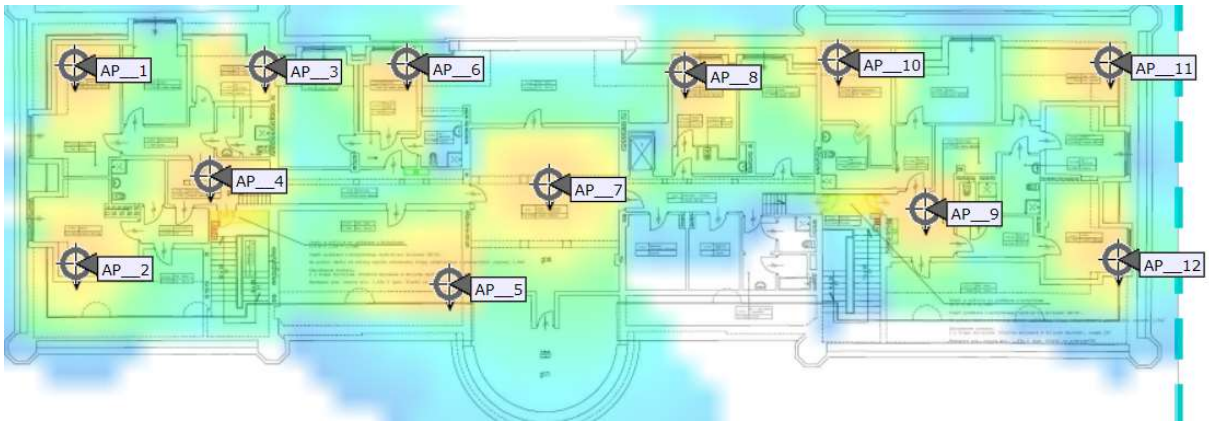
Część środkowa

Rysunek 62: Access point możliwy do instalacji nad lampą ewakuacyjną, zlicowany do elewacji, okablowanie do PD na parterze

Poddasze



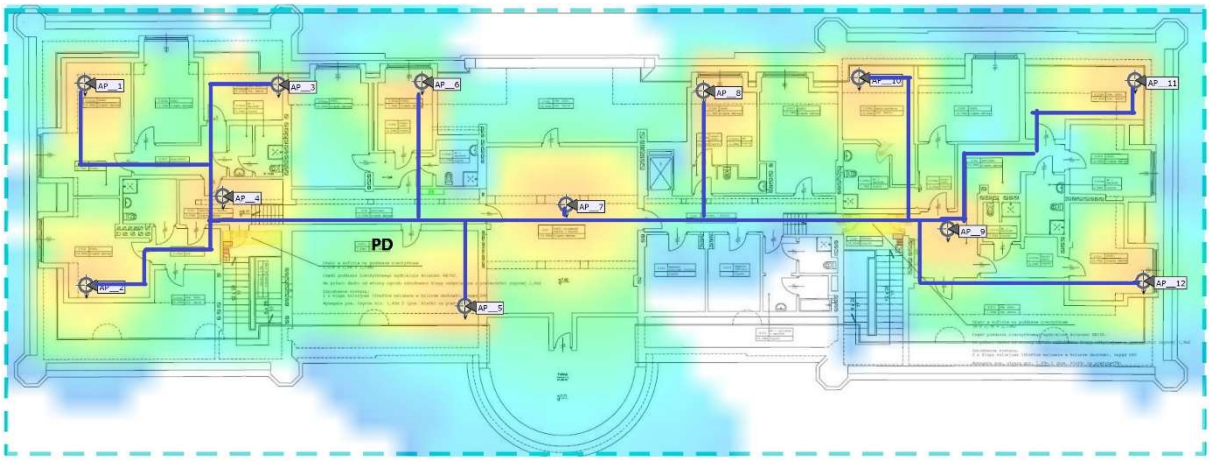
Rysunek 63: Planowanie dla częstotliwości 2,4GHz



Rysunek 64: Planowanie dla częstotliwości 5GHz

Na poddaszu zaproponowanych zostało dwanaście urządzeń. Jest tam przewidziany jeden punkt dystrybucyjny w nowej pracowni komputerowej. Wszystkie access pointy powinny zejść się do tego miejsca wzdłuż korytarza w korytkach kablowych.

Planowane trasy kablowe

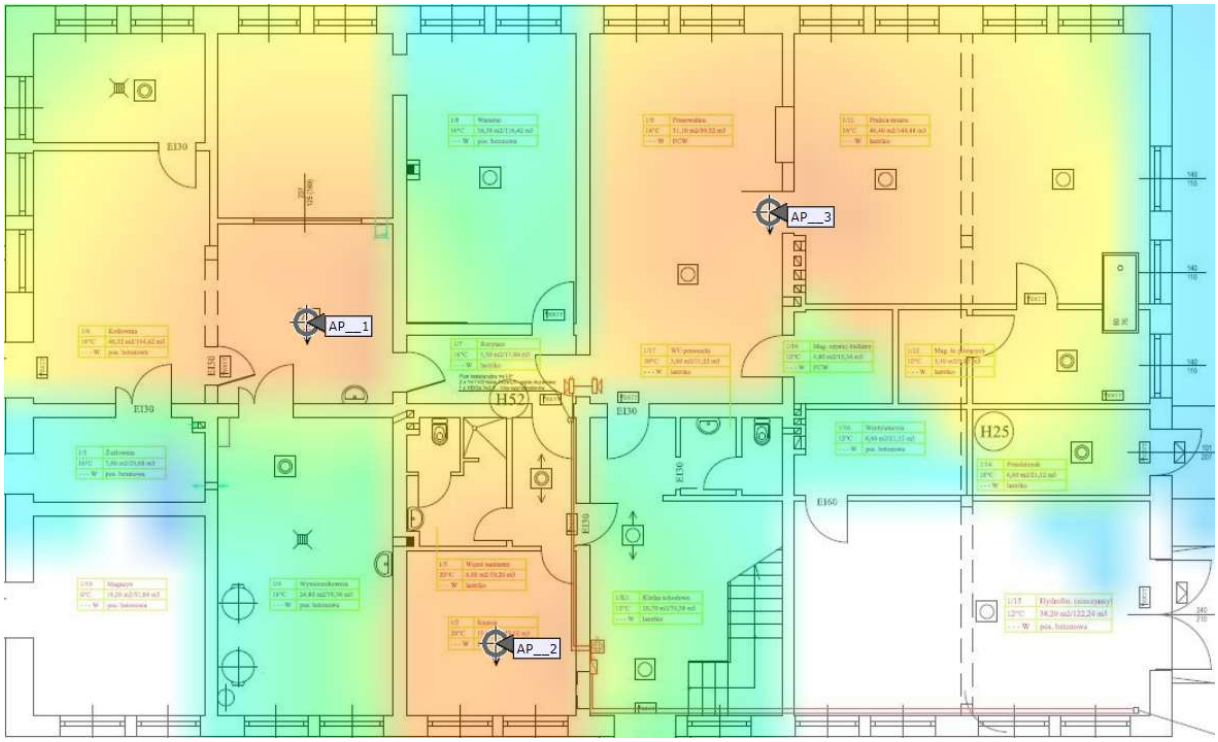


Rysunek 65: Na drugim piętrze całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

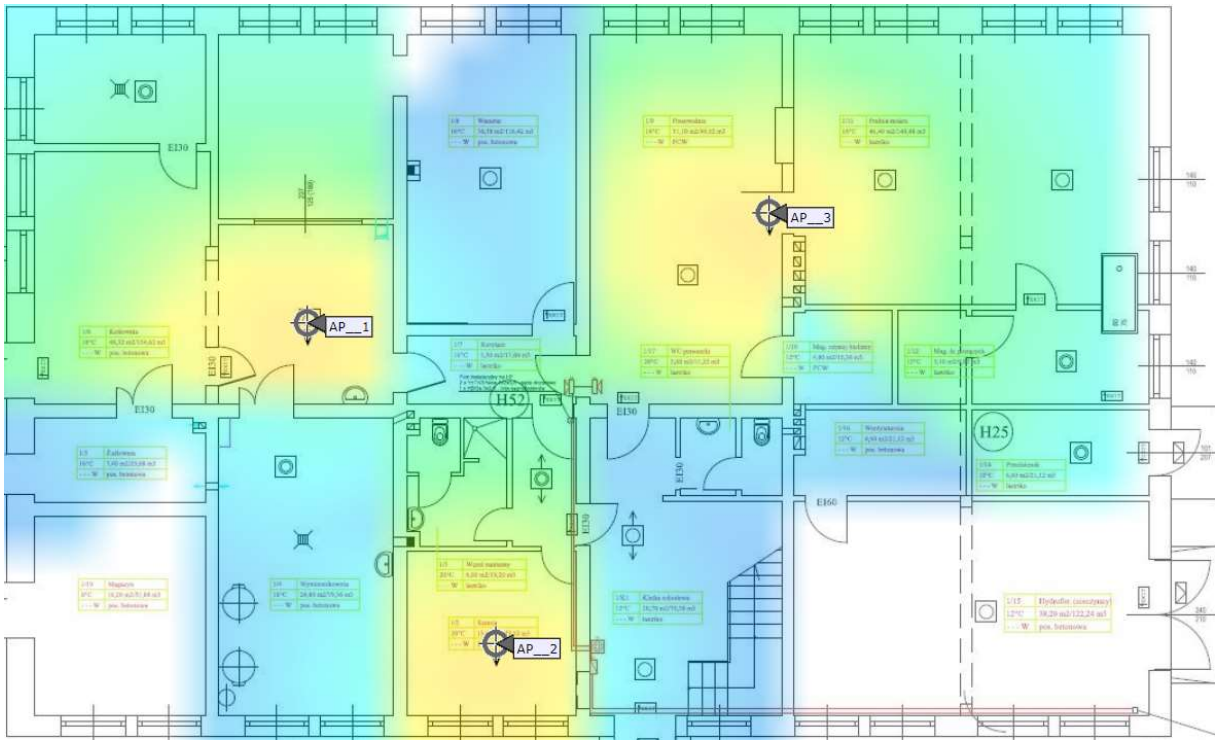
Numer AP	Szacowana długość okablowania [m]
AP1	25
AP2	25
AP3	25
AP4	15
AP5	15
AP6	25
AP7	35
AP8	35
AP9	40
AP10	50
AP11	50
AP12	50

Budynek administracji

Parter



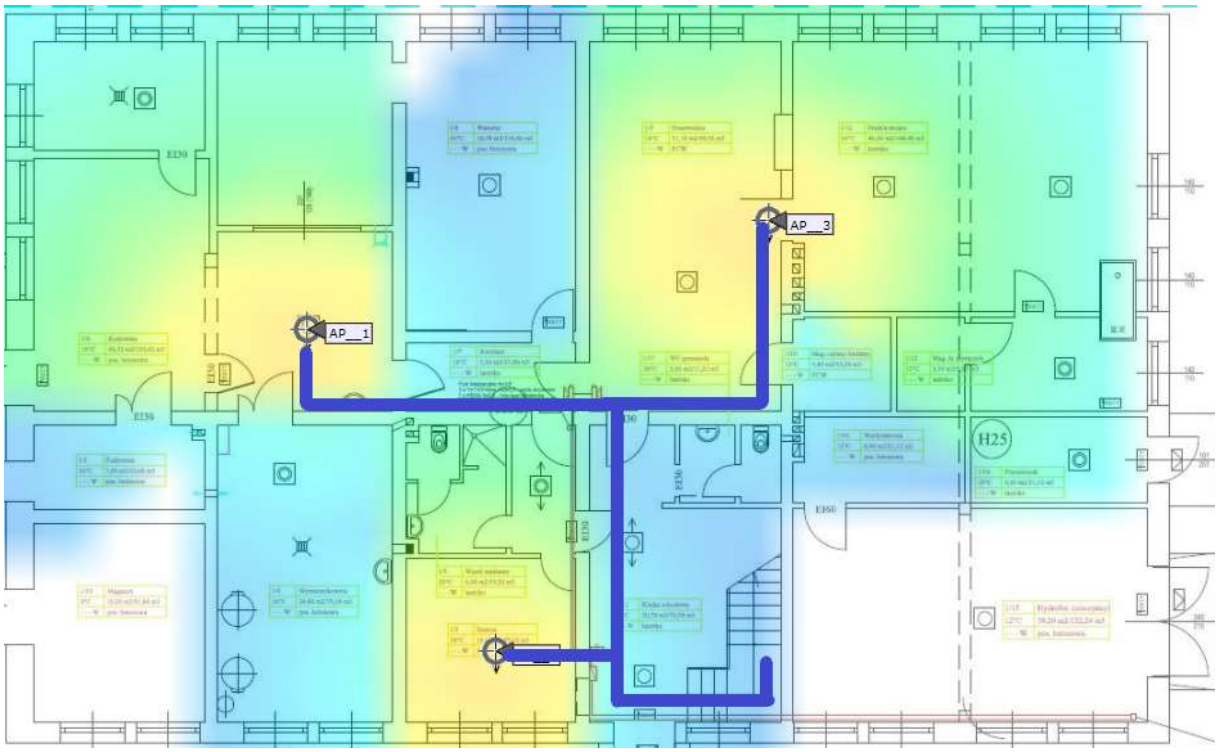
Rysunek 66: Planowanie dla częstotliwości 2,4GHz



Rysunek 67: Planowanie dla częstotliwości 5GHz

W budynku administracji na parterze zaproponowane zostały trzy urządzenia. Access pointy z parteru powinny zejść się do GPD w biurze. Trasa kablowa powinna przebiegać klatką schodową.

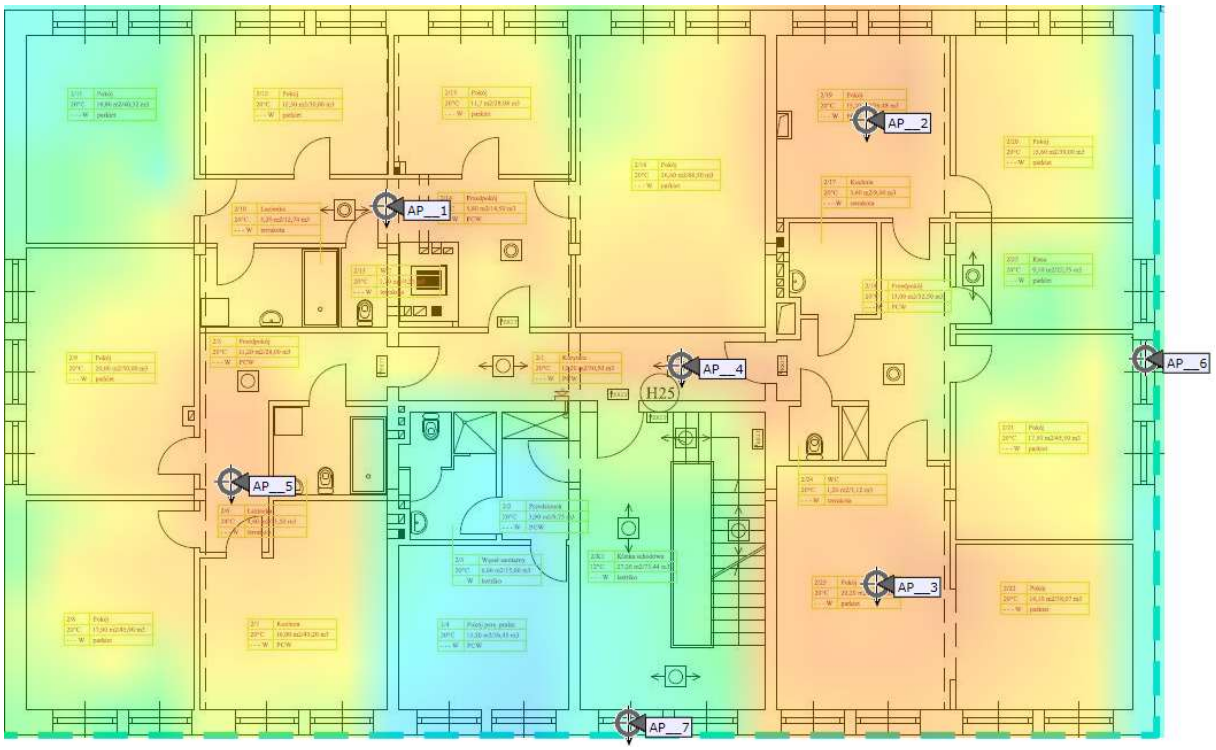
Planowane trasy kablowe



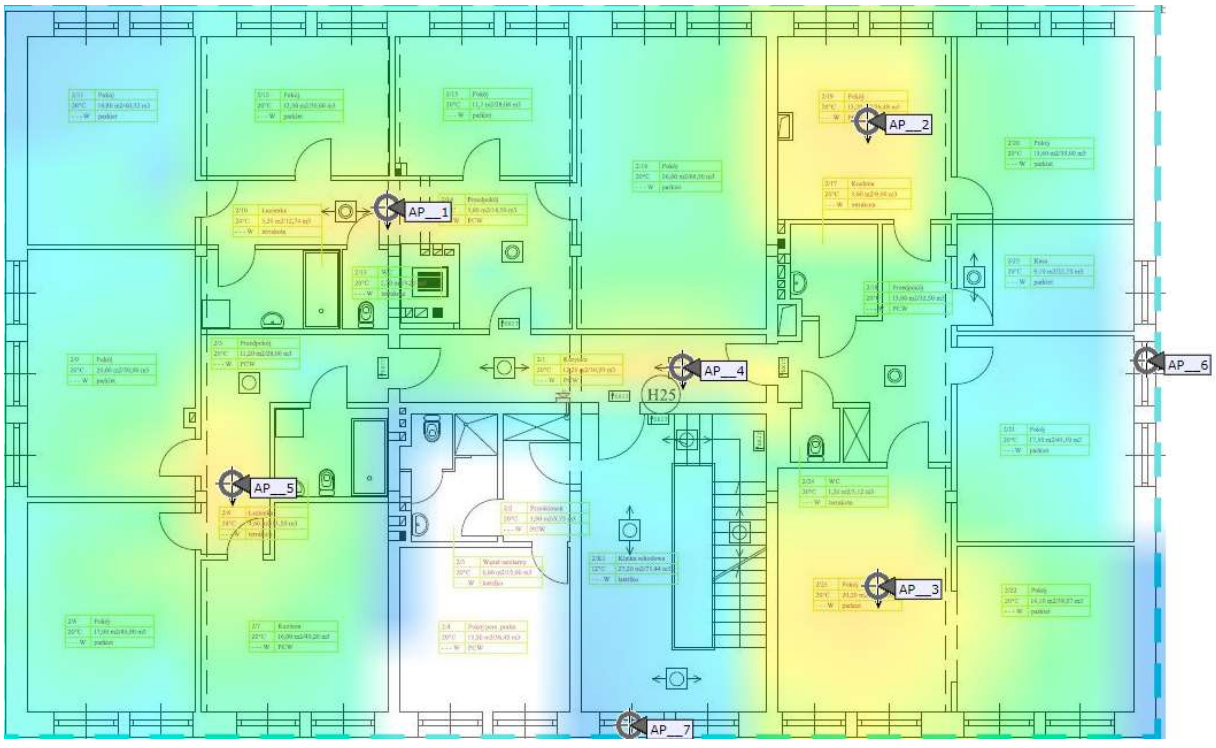
Rysunek 68: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	80
AP2	70
AP3	75

Pierwsze piętro



Rysunek 69: Planowanie dla częstotliwości 2,4GHz



Rysunek 70: Planowanie dla częstotliwości 5GHz

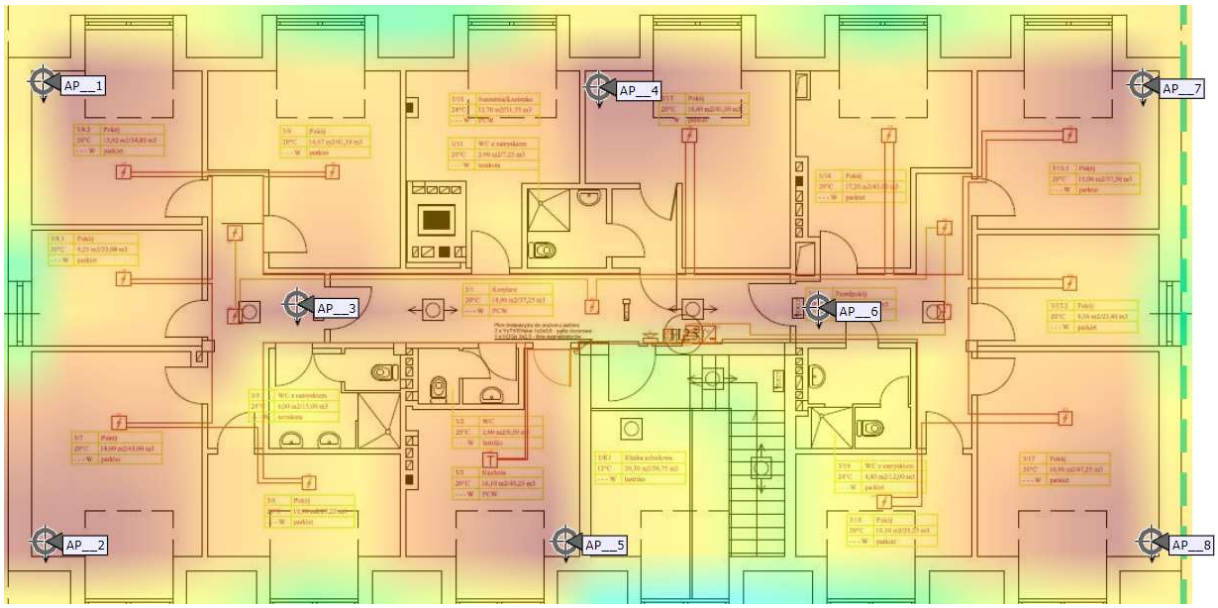
Na pierwszym piętrze w części biurowej przewidzianych zostało siedem urządzeń, w tym dwa zewnętrzne (AP6 i AP7). Cale okablowanie zejdzie się do GPS w pomieszczeniu kasy.

Planowane trasy kablowe

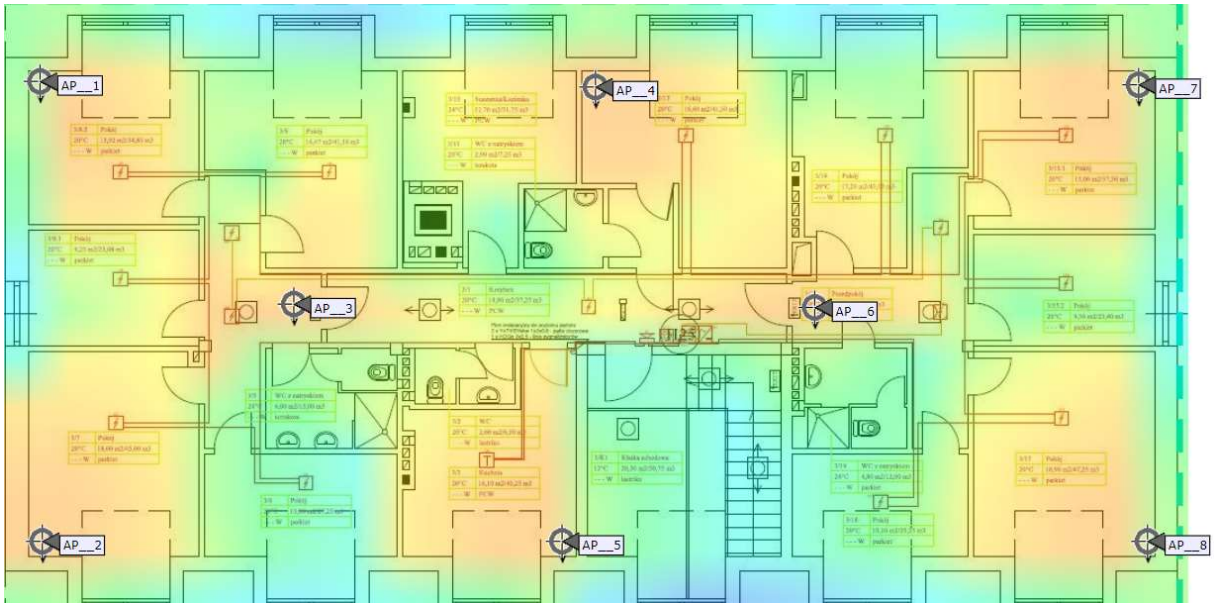
Rysunek 71: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	35
AP2	20
AP3	20
AP4	20
AP5	35
AP6	10
AP7	35

Drugie piętro



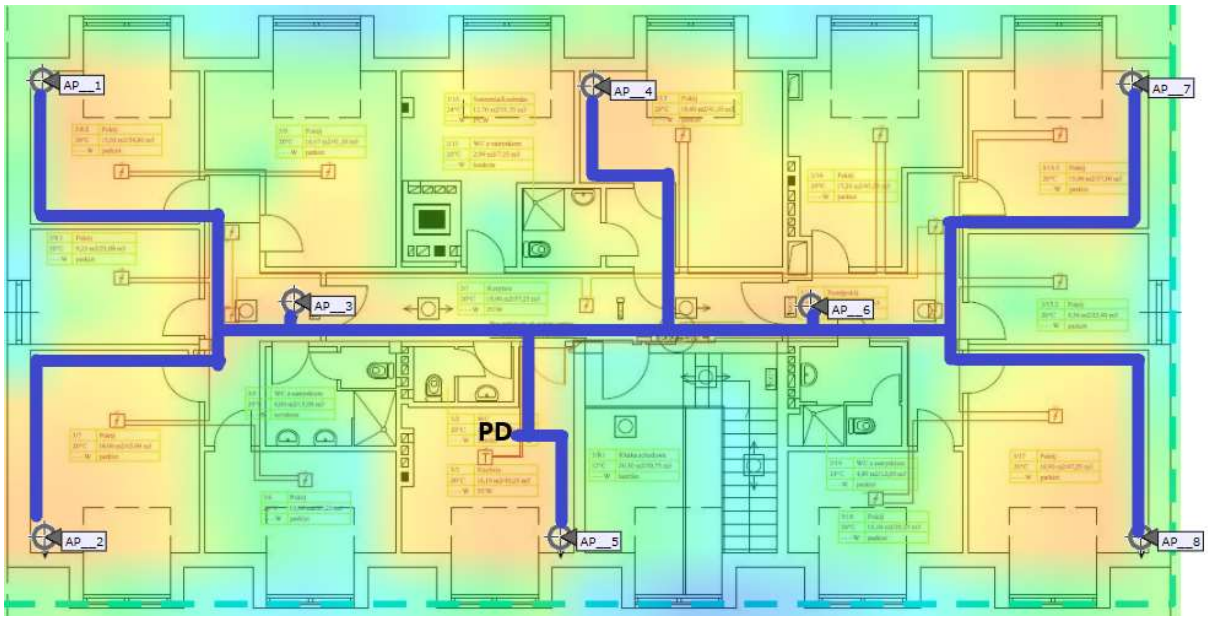
Rysunek 72: Planowanie dla częstotliwości 2,4GHz



Rysunek 73: Planowanie dla częstotliwości 5GHz

Na drugim piętrze w części hotelowej przewidzianych zostało osiem urządzeń. Okablowanie z access pointów na drugim piętrze zejdzie się do szafy umieszczonej w pomieszczeniu kuchni.

Planowane trasy kablowe



Rysunek 74: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	30
AP2	30
AP3	15
AP4	15
AP5	5
AP6	15
AP7	30
AP8	30

Informacje dodatkowe:

Montaż szaf rakowych w wybranych punktach:

- w poszczególnych PD, które mają zostać zainstalowane na korytarzu – kolor szafy biały lub jasno szary, tak aby wkomponować się w kolor ścian,
- zalecane jest, aby szafa miała jak najmniejszy rozmiar, który umożliwi zainstalowanie w niej sprzętów, przewidywany rozmiar dla każdego piętra 6U-9U.

Podsumowanie

Liczba wszystkich urządzeń:

- Kontroler sieci bezprzewodowej: 1.
- Access pointy: 71 w tym 9 zewnętrznych.
- Switche: 1 core, 7 access.
- Firewall: 1.

Możliwe do wystąpienia problemy:

Ze względu na zabytkowy charakter obiektu oraz na jego wiek należy mieć na uwadze:

- Grube ceglane ściany do kilkudziesięciu cm szerokości, co może powodować trudności w prowadzeniu kabli.
- Brak jakiejkolwiek infrastruktury, z której można byłoby skorzystać w czasie projektowania czy instalacji nowej sieci.
- Brak istniejących tras kablowych oraz przepustów.
- Część obiektu pod konserwatorem zabytków.
- Brak doprowadzonego zasilania do wybranych punktów dostępowych.
- Niezbędne będzie połączenie części pałacowej wraz z budynkiem administracji.
- Równocześnie problemem dla wprowadzenia nowoczesnych usług może okazać się niedostatek parametrów połączenia internetowego oraz brak możliwości redundancji w tym zakresie.

Minimalne wymagania techniczne sprzętu

Kontroler sieci bezprzewodowej	• urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
	  ○ zarządzanie politykami bezpieczeństwa
	  ○ wykrywanie zagrożeń w sieci bezprzewodowej
	  ○ zarządzanie pasmem radiowym
	  ○ zarządzanie mobilnością
	  ○ zarządzanie jakością transmisji
	• obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji
	• min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45)
	• opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
	• obsługa ruchu tunelowanego
	• obsługa min. 1000 klientów sieci bezprzewodowej
	• zarządzanie pasmem radiowym punktów dostępowych:
	  ○ automatyczna adaptacja do zmian w czasie rzeczywistym
	  ○ optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
	  ○ dynamiczne przydzielanie kanałów radiowych
	  ○ wykrywanie, eliminacja i unikanie interferencji
	  ○ równoważenie obciążenia punktów dostępowych
	  ○ tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
	  ○ automatyczna dystrybucja klientów pomiędzy punkty dostępowe
	  ○ mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
	  ○ dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
	• mapowanie SSID do segmentów VLAN w sieci przewodowej
	• możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
	• automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
	• obsługa mechanizmów bezpieczeństwa:
	  ○ 802.11i, WPA3, WPA2, WPA, WEP
	  ○ 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
	  ○ obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
	• kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
	• obsługa dostępu gościnnego (IPv4 i IPv6)

	○ przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) ○ przekierowanie użytkowników do strony logowania na zewnętrznym serwerze • współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych • obsługa NTP wersji 4 (IPv4 oraz IPv6) • obsługa Hotspot 2.0 • obsługa redundancji rozwiązania
Access point wewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników

	○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych
Access point zewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax

	○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID

	○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • dla access pointów zewnętrznych: ○ zgodność z IP67 ○ min. praca przy temperaturach między -35^{o}C a 60^{o}C • certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint
Switch core	• Typ i liczba portów: ○ Min: 12 SFP/SFP+ • Opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb): ○ min. 4x1G SFP ○ min. 4x1/10G SFP+ • Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: ○ Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U ○ Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość tworzenia stosów • Parametry wydajnościowe: ○ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) ○ Bufor pakietów – min.: 8MB

	○ Pamięć DRAM – min.: 4GB ○ Pamięć flash – min.: 8GB ○ Obsługa ▪ min. 3.000 sieci VLAN ▪ min.: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: ○ Obsługa protokołu STP • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Mechanizmy związane z bezpieczeństwem sieci: ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN ○ Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL ○ Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC ○ Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 ○ Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard • Obsługa protokołów routingu: ○ Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie ○ Port konsoli ○ Dedykowany port Ethernet do zarządzania out-of-band ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Switch access	• Typ i liczba portów:
	  o min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP
	• Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami)
	• Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
	  o Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
	  o Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
	• Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
	  o Przepustowość w ramach stosu – min.:60Gb/s
	  o min: 4 urządzenia w stosie
	  o Zarządzanie poprzez jeden adres IP
	• Parametry wydajnościowe:
	  o Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
	  o Bufor pakietów – min: 4MB
	  o Pamięć DRAM – min: 1GB
	  o Pamięć flash – min: 2GB
	  o Obsługa
	  ▪ 1024 sieci VLAN
	  ▪ min: 16.000 adresów MAC
	• Obsługa protokołu NTP
	• Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
	  o IEEE 802.1w Rapid Spanning Tree
	• Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
	• Możliwość uruchomienia funkcji serwera DHCP
	• Obsługa protokołów routingu:
	  o Routing statyczny dla IPv4 i IPv6
	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN

	• Zarządzanie
	  ○ Port konsoli
	  ○ Dedykowany port Ethernet do zarządzania out-of-band
	  ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
	  ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
	  ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
	• Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Firewall	• Wymagania Ogólne
	  ○ Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
	  ○ System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
	  ○ System musi wspierać IPv4 oraz IPv6 w zakresie:
	  ▪ Firewall.
	  ▪ Ochrony w warstwie aplikacji.
	  ▪ Protokołów routingu dynamicznego.
	• Redundancja, monitoring i wykrywanie awarii
	  ○ W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
	  ○ Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
	  ○ Monitoring stanu realizowanych połączeń VPN.
	• Interfejsy, Dysk, Zasilanie:
	  ○ System realizujący funkcję Firewall musi dysponować minimum:

	▪ min. 4 portami Gigabit Ethernet RJ-45. ▪ min. 2 gniazdami SFP 1 Gbps. o System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. o System musi być wyposażony w zasilanie AC. • Parametry wydajnościowe: o W zakresie Firewall'a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. o Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps o Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0,5 Gbps. o Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps. • Funkcje Systemu Bezpieczeństwa: o W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. ▪ Kontrola Aplikacji. ▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. ▪ Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). ▪ Funkcja lokalnego serwera DNS ze wsparciem dla DNS • Polityki, Firewall o Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. o System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. ▪ W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. ▪ Możliwość wykorzystania w polityce bezpieczeństwa

	zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
	• Połączenia VPN
	  ○ System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Wsparcie dla IKE v1 oraz v2.
	  ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	  ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	  ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	  ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	  ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	  ▪ Mechanizm „Split tunneling" dla połączeń Client-to-Site.
	  ○ System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
	  ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
	  ▪ Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
	• Routing i obsługa łączy WAN
	  ○ W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	  ▪ Routingu statycznego.
	  ▪ Policy Based Routingu.
	  ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	• Ochrona przed malware
	• Ochrona przed atakami
	  ○ Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
	• Kontrola aplikacji

	• Kontrola WWW • Zarządzanie • Logowanie • Serwisy i licencje ○ W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. • Gwarancja oraz wsparcie
Okablowanie etherentowe	• Min. Cat 6 ekranowana

Zalecenia konserwatorskie dla Domu Pomocy Społecznej w Parsowie

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152; fa
e-mail: koszalin@

ZN.K.5183.77.2021.KB

Koszalin, 28 cz

DOM POMOCY
im. Alojzego Młodzika w Parsowie v
PARSOWO 25, 76-039
adres do kor
Network Experts sp.
ul. Chojnowska 8, 03-583

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń d sieci bezprzewodowej – punków dostępowych, instalacji okablowania dystrybucyjnych, w Domu Pomocy Społecznej im. Anselma Alojzego Młodzika Parsowo 25, 76-039 Biesiekierz, w związku z opracowywaniem dokumentacj „Opracowania audytu sieci radiowej dla budynków DPS Powiatu Koszalińskiego

Odpowiadając na pismo z dnia 17.05.2021 r. (data wpływu 18.05.2021 r.), 17.06.2021 r. (data wpływu 21.06.2021 r.), uzupełnione pismem z dnia 25.06.2 wpływu 25.28.06.2021 r.), w oparciu o wizję lokalną przeprowadzoną w dniu 2 Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie, działając n art. 27 Ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytka z 2021 r. poz. 710 ze zm.) przekazuje następujące zalecenia konserwatorskie:

1. Pałac w Parsowie gm. Biesiekierz, jest zabytkiem architektury i b wpisanym do rejestru zabytków pod nr A-440 (dawniej: 387) decyzj kwietnia 1964 r. wraz z otoczeniem (park krajobrazowy) i wystrojem wn ozdobne). Przedmiotowa nieruchomość podlega ochronie prawnej na pc 6 ust. 1 lit. c, g oraz art. 7 ust. 1 ustawy z dnia 23.07.2003 r. o ochron i opiece nad zabytkami (t.j. Dz.U. z 2021 r. poz. 710 ze zm.), na zasadach w tej ustawie. Zgodnie z art. 36 ust. 1 przywołanej ustawy, prowad

2. ZWKZ akceptuje ze stanowiska konserwatorskiego wersję II ro i rozprowadzenia punktów dystrybucyjnych, punktów dostępowych, św oraz kabla ethernetowego, w miejscach uzgodnionych podczas w przeprowadzonej w dniu 22.06.2021 r. przez przedstawiciela WUOZ Delegatura w Koszalinie i Network Experts sp. z o.o. sp.k. w przedstawione na załączonych rzutach piwnic, parteru, I i II piętra, oraz elewacji i wnętrz pałacu.

3. Zaleca się prowadzenie kabli instalacyjnych w osłonach do kolorystycznie i umieszczonych możliwie dyskretnie u zbiegu ścia z ograniczeniem do minimum trasy ich przebiegu. Ponadto zaleca się og minimum wielkości urządzeń do transmisji sieci bezprzewodowej i szaf kolorystyczne obudowy urządzeń i szaf z podłożem.

4. W pomieszczeniach reprezentacyjnych, w których zachował się orygi sztukatorski i malarski (dawna sala balowa, hall, klatka schodowa), deta się przeprowadzenie badań konserwatorskich (odkrywek) przed zakoń projektowych, w miejscach wyznaczonych do prowadzenia kabli i urządzeń, przez dyplomowanego konserwatora zabytków, w celu spra umieszczenie urządzeń nie naruszy oryginalnego wystroju pomieszczeń.

5. Nie wnosi się zastrzeżeń ze stanowiska konserwatorskiego do prze rozmieszczenia i rozprowadzenia punktów dystrybucyjnych, punktów (światłowodów, oraz kabla ethernetowego na parterze, I i II piętrze wzniesionego budynku administracyjnego. Z uwagi na usytuowa w otoczeniu zabytku, wpisanym do rejestru zabytków wraz z pałacem, 36 ust. 1 pkt 2 Ustawy o ochronie zabytków i opiece nad zabytkami, robót budowlanych i umieszczanie urządzeń technicznych w otocz wpisanym do rejestru zabytków wymaga również uzyskania wojewódzkiego konserwatora zabytków w formie decyzji administracyjn

Z up. ZACHODNIOPOMO
WOJEWÓDZKIEGO KONSERWATOR
Kierownik Delegatury w K

mgr Dorota Raczkows

Uzupełnienie zaleceń konserwatorskich dla Parsowa

Wojewódzki Urząd
Ochrony Zabytków w Szczecinie

Delegatura w Koszalinie
ul. Zwycięstwa 125
75-602 Koszalin

www.wkz.szczecin.pl

tel. 94/3408152;
e-mail: koszali

ZN.K.5183.77.2021.KB

Koszalin, 30

DOM POMOC
im. Alojzego Młodzika w Parsowie
PARSOWO 25, 76-0
adres do k
Network Experts
ul. Chojnowska 8, 03-58

Dotyczy: wydania zaleceń konserwatorskich dotyczących instalacji urządzeń sieci bezprzewodowej – punków dostępowych, instalacji okablowani dystrybucyjnych, w Domu Pomocy Społecznej im. Anselma Alojzego Młodzil Parsowo 25, 76-039 Biesiekierz, w związku z opracowywaniem dokument „Opracowania audytu sieci radiowej dla budynków DPS Powiatu Koszalińskie

W uzupełnieniu do pisma ZWKZ znak ZN.K.5183.77.2021.KB z dnia Zachodniopomorski Wojewódzki Konserwator Zabytków w Szczecinie Kierow w Koszalinie przekazuje w załączeniu 1 egzemplarz dokumentacji pt. dokumentacji konserwatorskiej do wydania zaleceń pod budowę nowej siec Pomocy Społecznej w Parsowie".

Z up. ZACHODNIOPOM
WOJEWÓDZKI KONSERWA
Kierownik Delegatury
mgr Sonata Raczko

W czasie wizyty lokalnej w Parsowie ustalone zostały nowe miejsca instalacji access pointó
trasy kablowe.

Ustalenia końcowe

Zaktualizowane ustalenie dotyczą jedynie części pałacowej, cześć administracyjna pozostaj
niezmienna z oryginalnego dokumentu.

Montaż szaf rakowych w wybranych punktach:

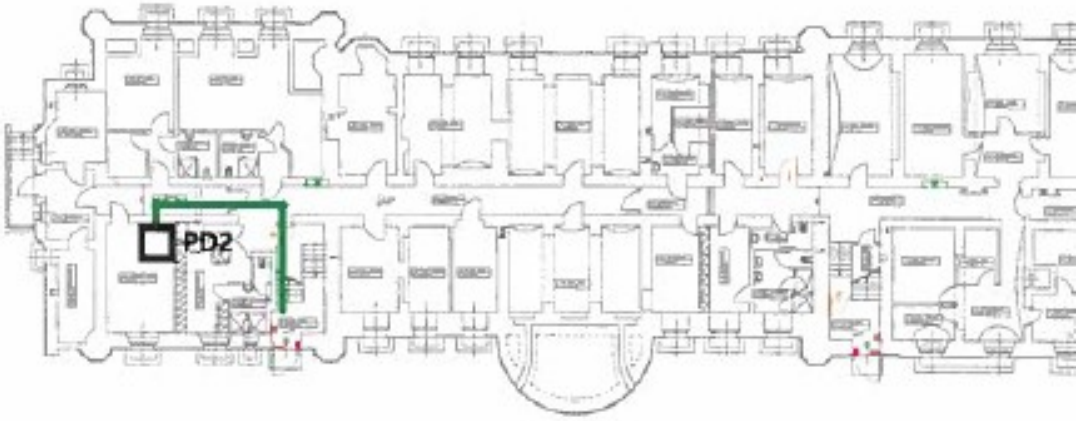
- w poszczególnych PD, które mają zostać zainstalowane na korytarzu – kolor szafy b
  jasno szary, tak aby wkomponować się w kolor ścian
- zalecane jest, aby szafa miała jak najmniejszy rozmiar, który umożliwi zainstalowan
  sprzętów, przewidywany rozmiar dla każdego piętra 6U-9U

Prowadzenie kabli światłowodowych

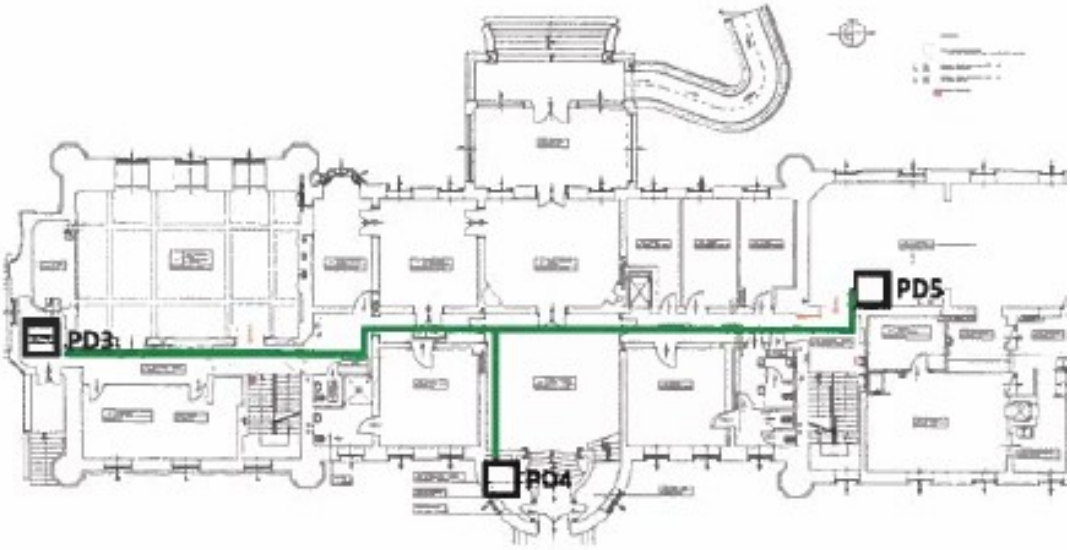
Kable światłowodowe ze wszystkich PD w całym pałacu zejdą się do PD4, skąd dalej p
zostaną doprowadzone do budynku administracji. Całe okablowanie zostanie doprowadzon
klatki schodowej skąd dalej przez korytarz oraz pomieszczenia mieszkalne zostanie dalej p
PD4, znajdującego się w małym pomieszczeniu pod schodami. Okablowanie zostanie ukryte
kablowych o jak najmniejszym przekroju. W razie potrzeby koryta zostaną poma
odpowiednim kolorze. Koryta zostaną umieszczone w samym rogu na styku ściany oraz sufi

Miejsca instalacji szafek na każdym piętrze oraz zaznaczenie przewidzianych tras światłowo

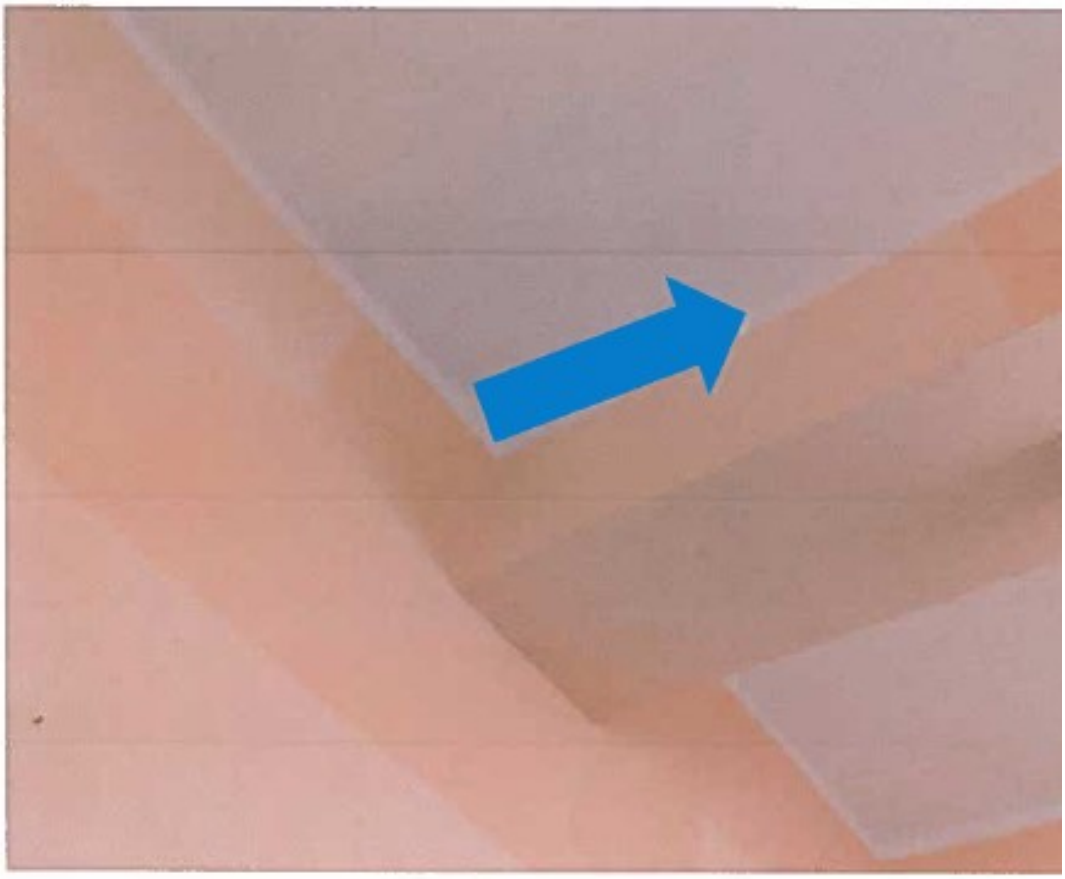
Piwnica



Parter

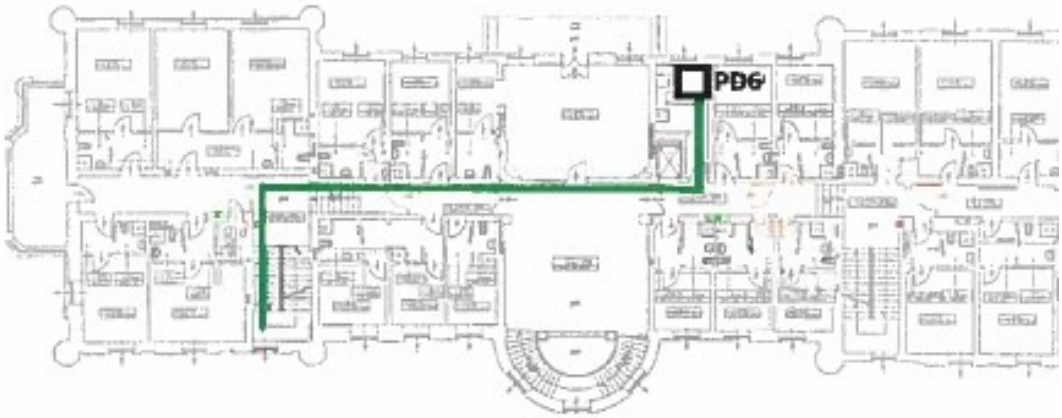


PD5 zostanie przeniesione z pomieszczeni jadalni na korytarz i jeżeli będzie to możliwe pod v
projektowym umieszczone we wnęce jak na zdjęciu poniżej.



W takich korytarzach jak ten pomiędzy PD4 a PD3 należy brać pod uwagę, że koryta n
instalowane w rogach na styku ścian i sufitu, tak żeby nie przechodzić przez środek pomi
Należy taż pamiętać, że koryta powinny być na ile to możliwe jak najmniej widoczne.

Pierwsze pietro



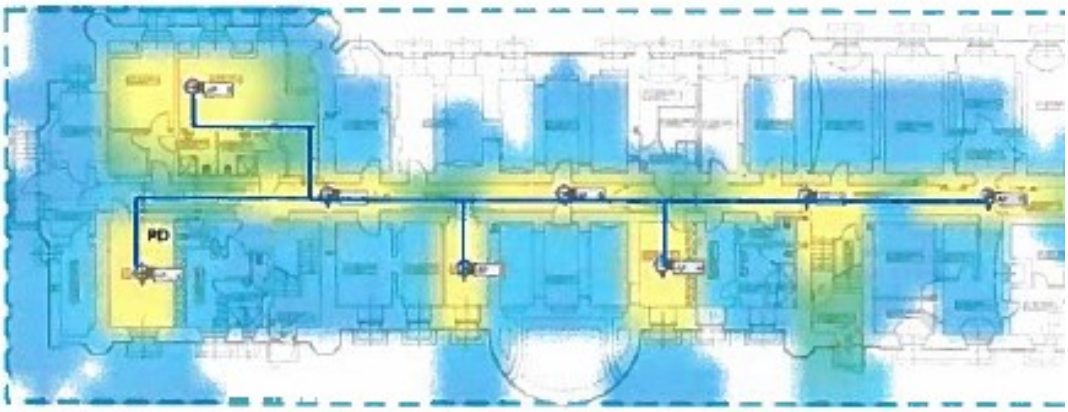
Drugie piętro

Jeżeli będzie to możliwe, to zamiast puszczać na około światłowód w korycie po klatce scho
dopuszcza się przebicie stropu.

Aktualizacja rozmieszczenia access pointów wraz z zaznaczonymi trasami kablowymi do najb
punktu dystrybucyjnego.

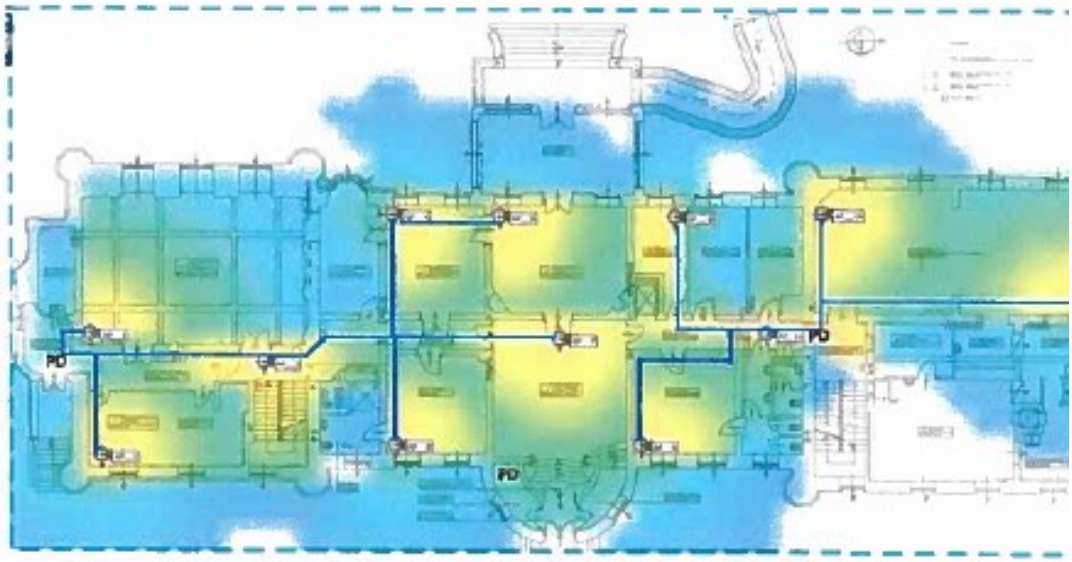
- Kable ethernetowe muszą być prowadzone w korytach kablowych dołożonych do ist
  infrastruktury
- Koryta muszą być zamaskowane kolorem, jeżeli będzie taka potrzeba
- Instalacja access pointów będzie pod sufitem czy to w pokoju czy na korytarzu

Piwnica



W piwnicy całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

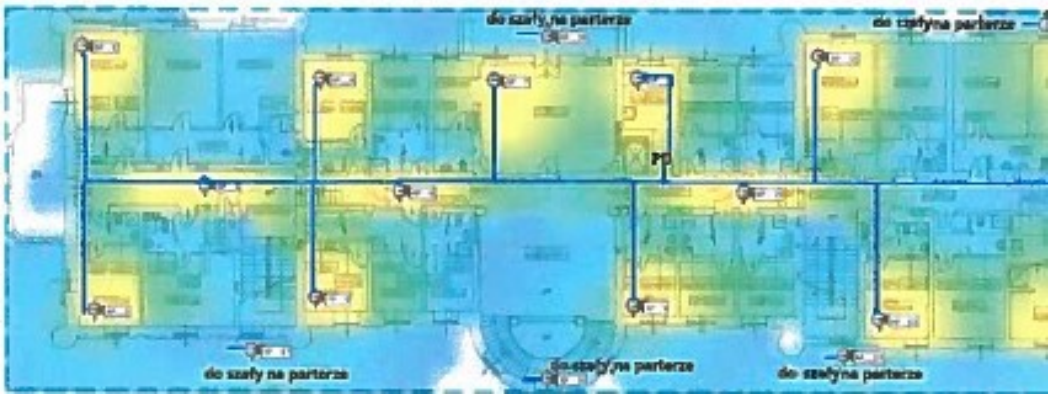
Parter



Na parterze okablowanie zejdzie się do wskazanych PD. Access point w sali balowej mo
zainstalowany na płasko do ściany nad gzymsem. Okablowanie powinno przejść bezpośr
pomieszczenia magazynowego, gdzie znajduje się szafa. Na etapnie prac projektowych należy
odkrywkowe badania konserwatorskie dla tego punktu.Tak jak przypadku oka

Access point w rogu sali balowej

Pierwsze piętro



Cześć przednia pałacu – prawa

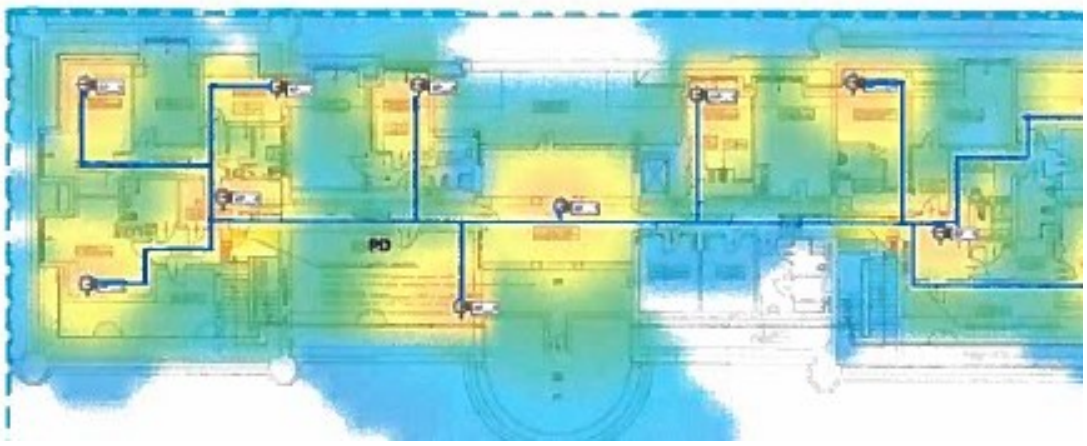
Access point środkowy

Część boczna pałacu

Część środkowa

Access point możliwy do instalacji nad lampą ewakuacyjną, zlicowany do elewacji, okablowa
PD na parterze.

Drugie piętro

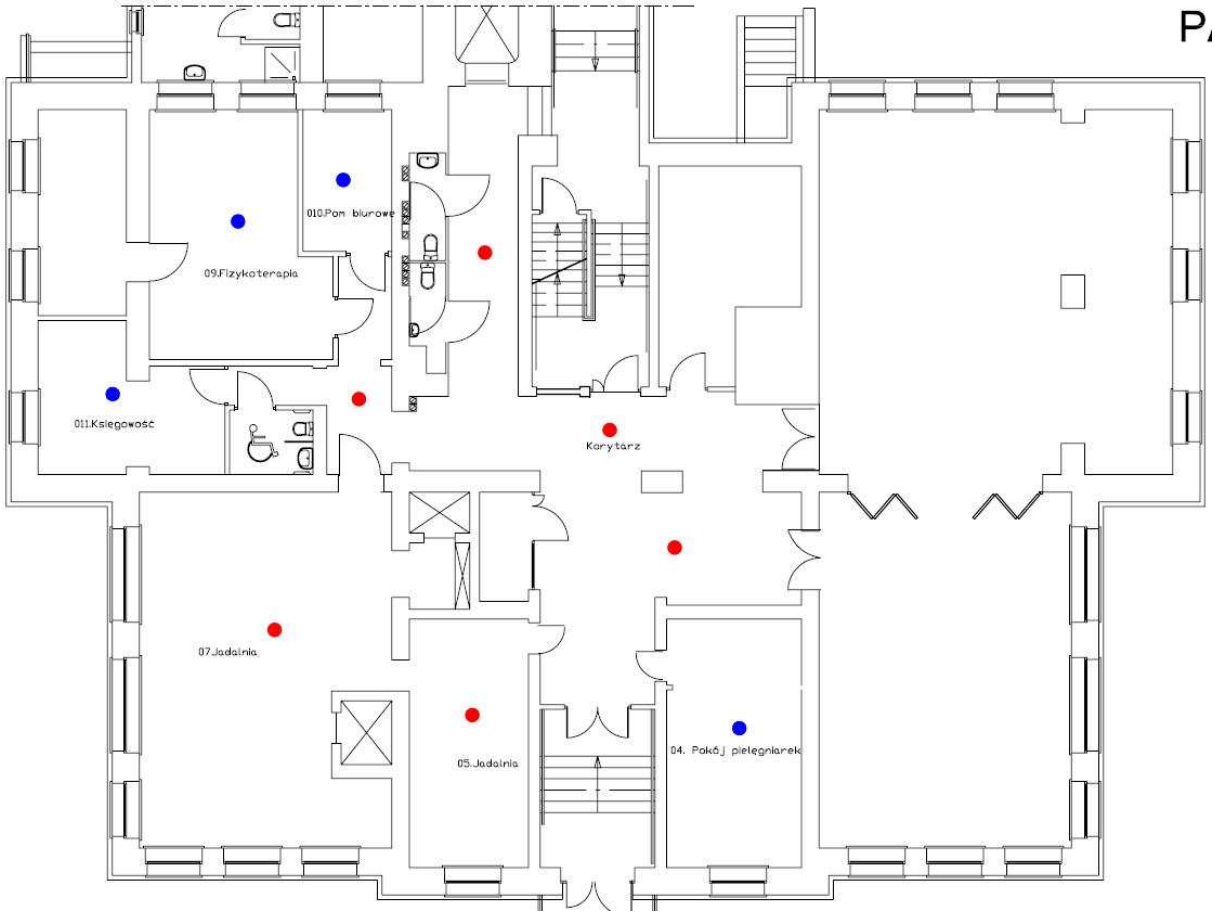


Załącznik nr 5 DPS Mielno

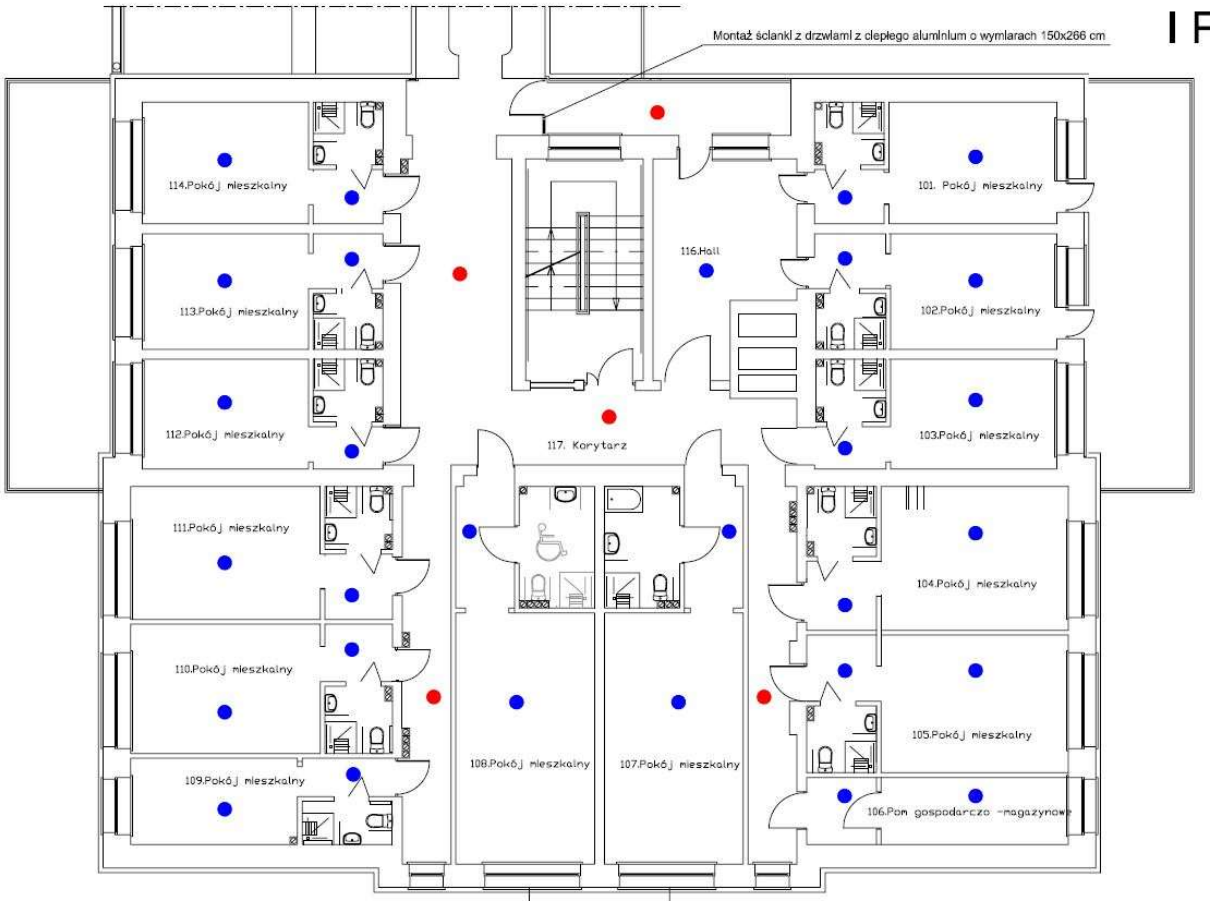
DPS Mielono składa się z dwóch części: budynek mieszkalny oraz budynek administracyjny.

Plany budynków

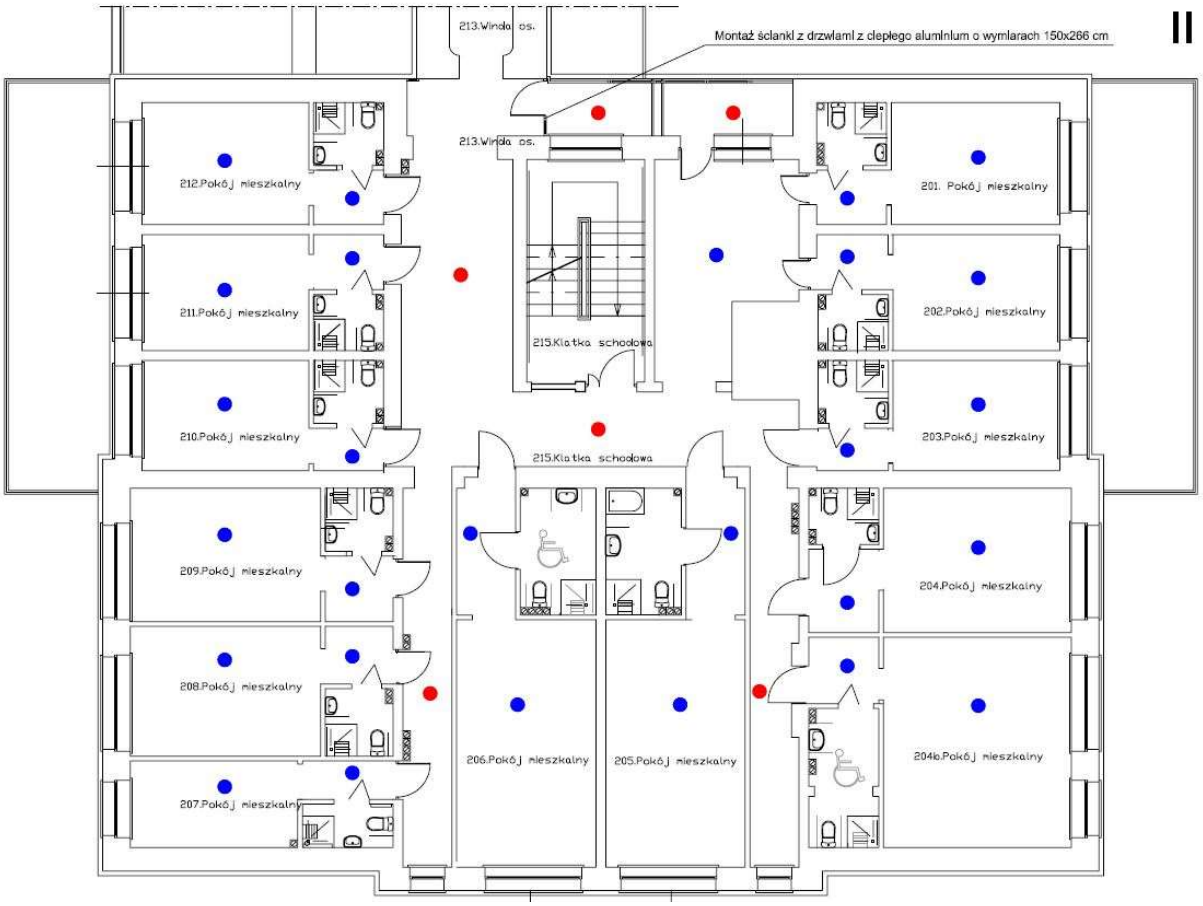
Budynek główny



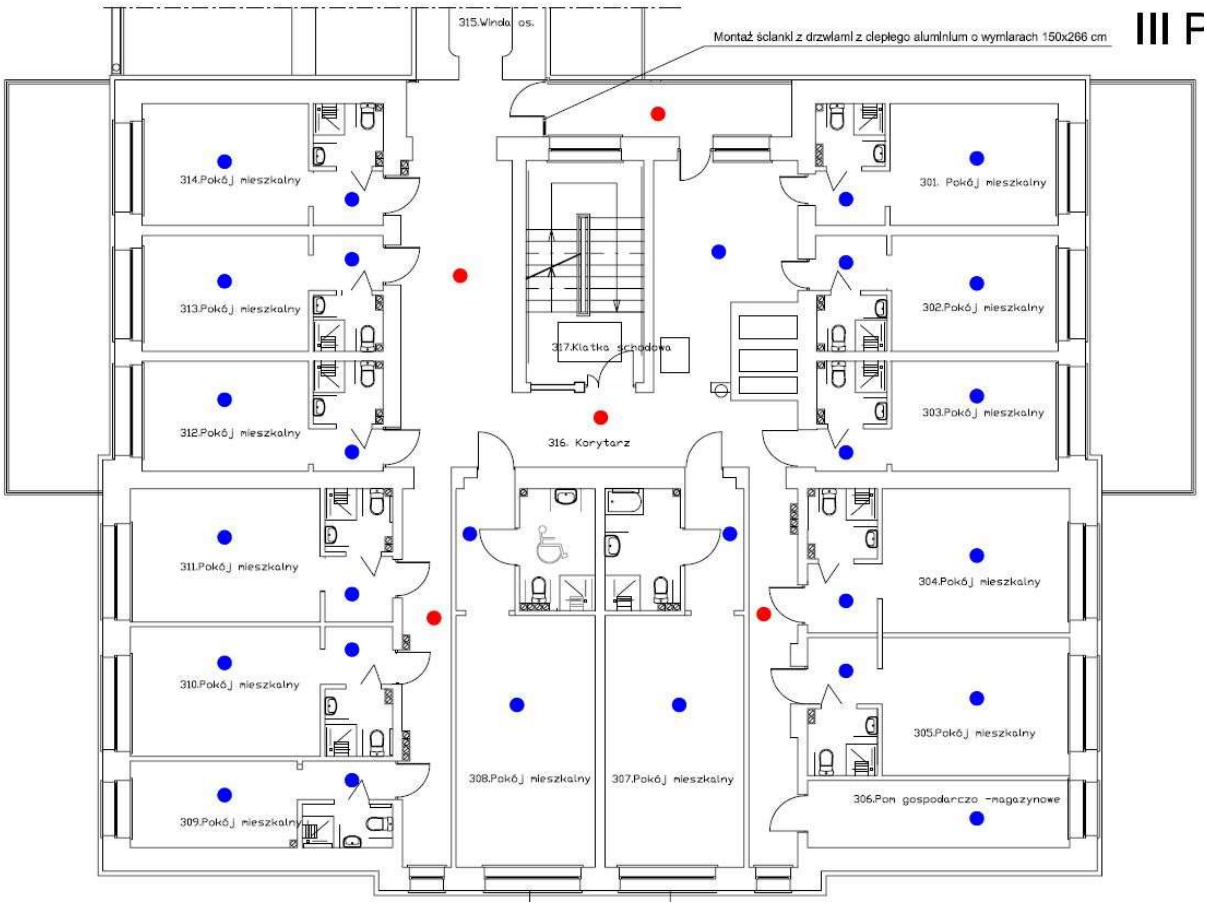
Rysunek 1: Plan parteru



Rysunek 2: Plan pierwszego piętra

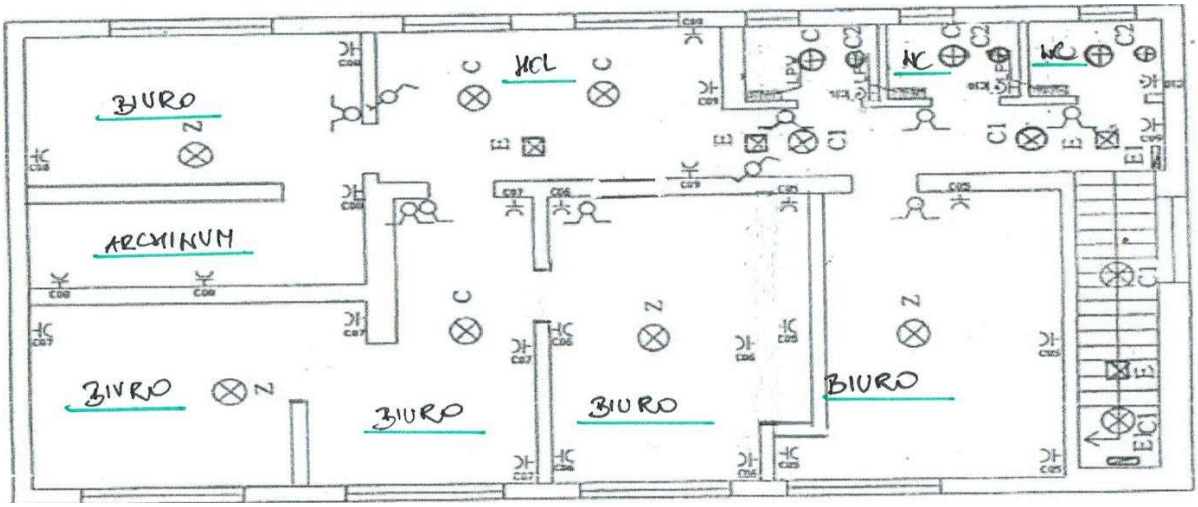


Rysunek 3: Plan drugiego piętra



Rysunek 4: Plan trzeciego piętra

Budynek administracji



Rysunek 5: Plan piętra

Obecny stań sieci

W obecnej chwili w Mielnie jest rozprowadzona sieć LAN oraz WLAN, ale tylko w obrębie pomieszczeń administracyjnych, w budynku głównym tylko w Sali wspólnej znajduje się komputer stacjonarny oraz w części biurowej. Poza tym nie ma infrastruktury z jakiej mogli by skorzystać mieszkańcy. Internet jest doprowadzony przez Orange. W budynku administracji znajduje się wisząca szafa rack, która jest centralnym punktem sieci. Pomiędzy budynkami jest zrobiony przepust kablowy, drożny z zaznaczeniem, że ma kolanka 90 stopni. W budynku głównym jest na klatce schodowej zainstalowana szafa rack, do której schodzi się okablowanie z parteru. W budynku brak jakichkolwiek wolnych pomieszczeń do wykorzystania na przyszłą serwerownię. Ze względu na przyszłe prace i chęć wprowadzenia zaawansowanego systemu sieci bezprzewodowej niezbędne będzie wybudowanie całkowicie nowej infrastruktury sieci LAN. Żadne z obecnie używanych urządzeń nie będzie się nadawać do przyszłego wykorzystania.

Rysunek 6: Podłączenie sieci LAN w sali spotkań

Rysunek 7: Szafa rack na klatce schodowej pomiędzy parterem, a pierwszym piętrem

Rysunek 8: Szafa rack w budynku administracji.

Stan sieci WLAN

AP List

SSID	#	Name	MAC	Ch	Rate	Sec.	Mode	Ave SNR	Max SNR	Min SNR	# Assoc Points	# Non-Assoc
	#2		local:46:d9:e7:cd:bc:83	11	130	WEP	n	8	14	3	0	6
DPS-GOSC	#5		local:6a:31:97:ae:51:41	8	144	WPA2	n	15	36	5	0	10
DPS-Mielno	#6		ZyxelCommC:ae:51:40	8	144	WPA2	n	14	37	3	0	10
FunBox2-0B97	#15		34:db:9c:bb:0b:97	11	144	WPA2	n	5	7	3	0	2
Hotspot Zielone WzgÃ³rze	#14		UbiquitiNe:cd:bc:83	11	130	WEP	n	10	14	7	0	4
HUAWEI-06D6	#13		HuaweiTech:b1:06:d6	8/40MHz	300	WPA2	n	29	49	6	0	24
HUAWEI-9610	#7		94:37:f7:ce:96:10	6	144	WPA2	n	7	12	0	0	10
HUAWEI-B315-8EAE-1	#8		local:ca:14:51:68:8e:af	4/40MHz	300	WPA2	n	11	15	7	0	2
HUAWEI-B525-5FE5	#16		fc:87:43:08:5f:e5	4/40MHz	300	WPA2	n	6	10	3	0	3
HUAWEI-B525-E607	#18		ec:8c:9a:6d:e6:07	2/40MHz	300	WPA2	n	12	18	5	0	2
MarlinMielno2	#1		TpLinkTech:7a:d9:31	10/40MHz	300	WPA2	n	6	7	4	0	4
SETUP	#4		local:e2:51:1a:8b:57:41	11	11	Clear	b/Ad hoc	23	24	22	0	2
Spokojne Wczasy 2 Pietro	#10		NetcoreTec:ba:ee:6f	4/40MHz	300	WPA2	n	7	9	5	0	2
VIllaOazaMielno	#9		HuaweiTech:68:8e:ae	4/40MHz	300	WPA2	n	8	10	6	0	2
VILLASPOKOJNA26	#11		HuaweiTech:58:94:dd	2	144	WPA2	n	11	11	11	0	1
wlan-test	#3	AP74a0.2f92.c82	CiscoSyste:8b:3e:f0	11	144	WPA2	n	42	70	12	0	26
wlan-test	#12	AP74a0.2f92.c82	CiscoSyste:8b:3e:ff	36	867	WPA2	ac	41	60	16	0	24
WLAN1-BQE80E	#17		HuaweiTech:3e:02:b5	1	144	WPA2	n	11	11	11	0	1

Rysunek 9: Sieci widoczne na pierwszym piętrze budynku mieszkalnego

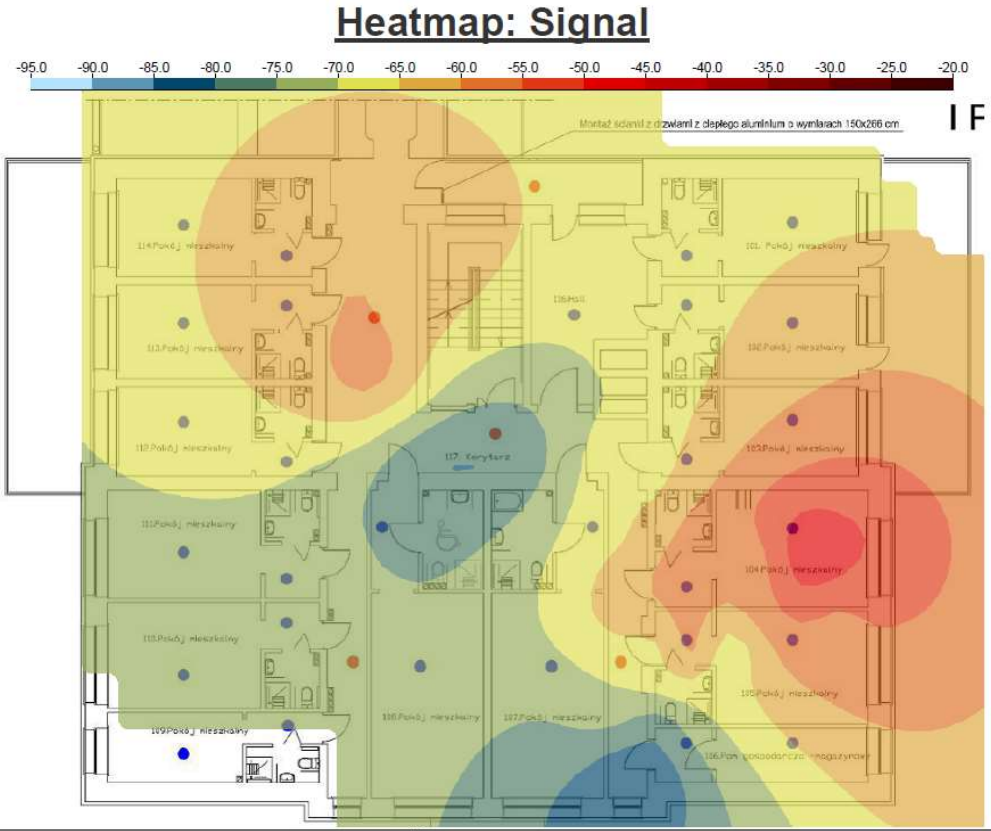
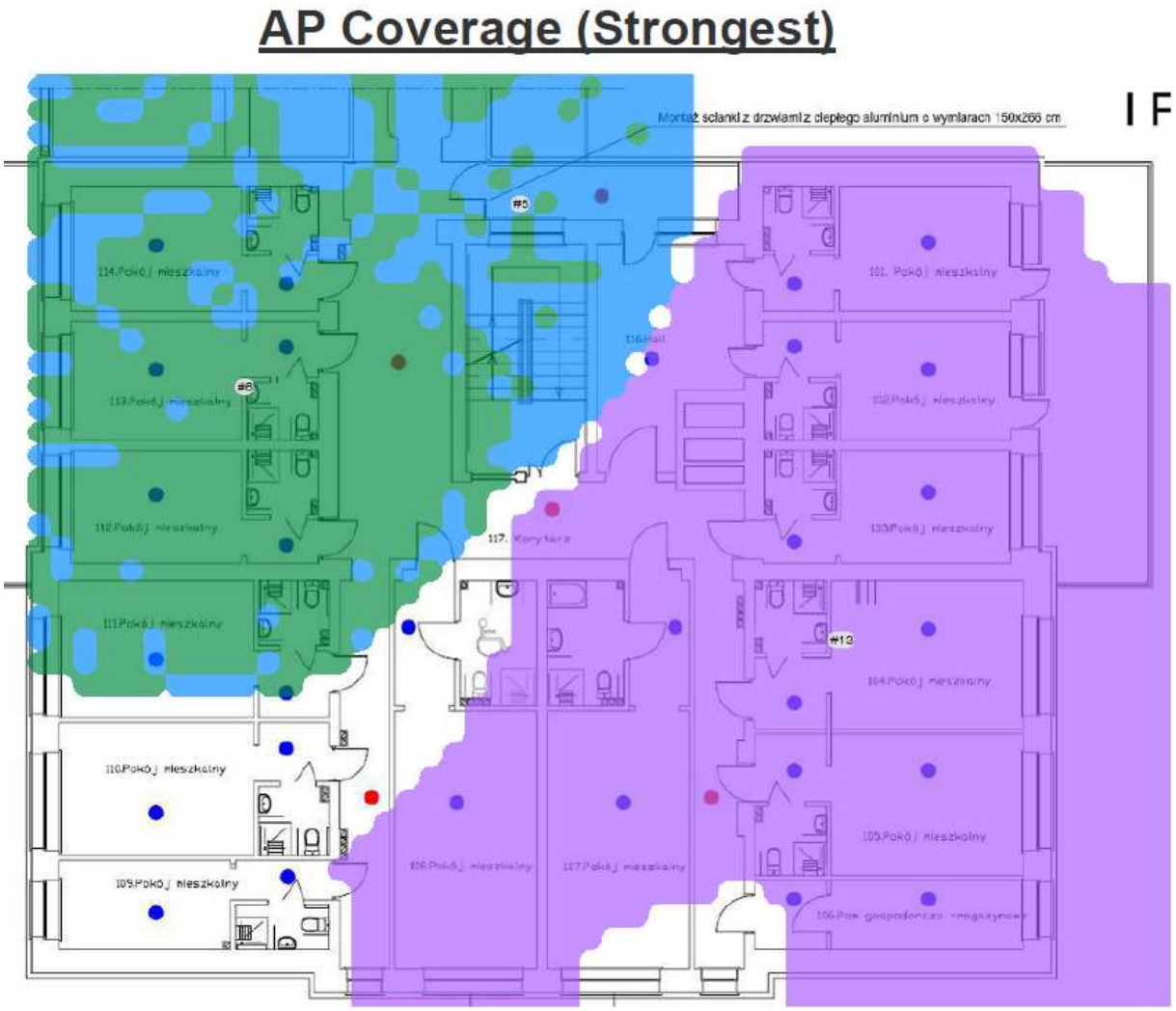
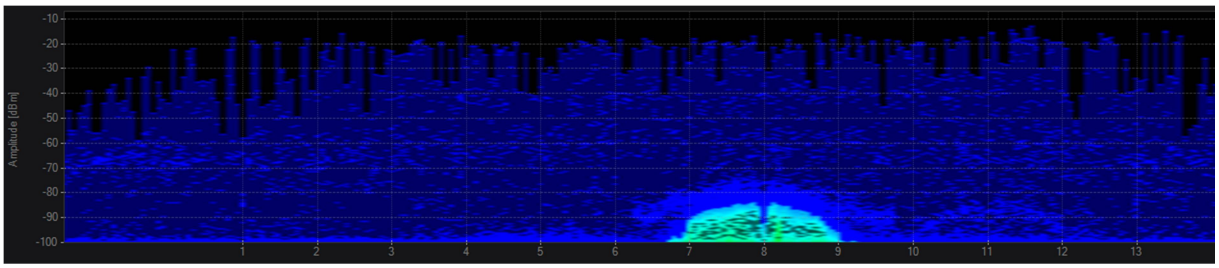


Figure 1: , DPS-GOSC, DPS-Mielno, FunBox2-0B97, Hotspot Zielone WzgÃ³rze, HUAWEI-06D6, HUAWEI-9610, HUAWEI-B315-8EAE-1, HUAWEI-B525-5FE5, HUAWEI-B525-E607, MarlinMielno2, SETUP, Spokojne Wczasy 2 Pietro, VIllaOazaMielno, VILLASPOKOJNA26, WLAN1-BQE80E

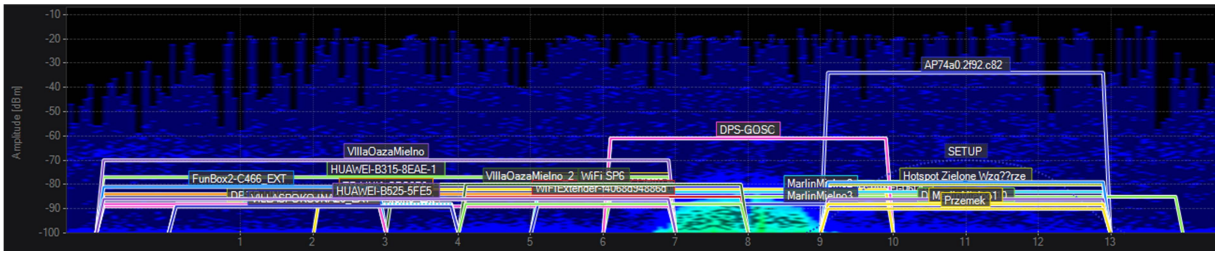
Rysunek 10: Rozkład sygnału widocznych sieci radiowych na pierwszym piętrze



Rysunek 11: Widoczność najmocniejszych access pointów na pierwszym piętrze



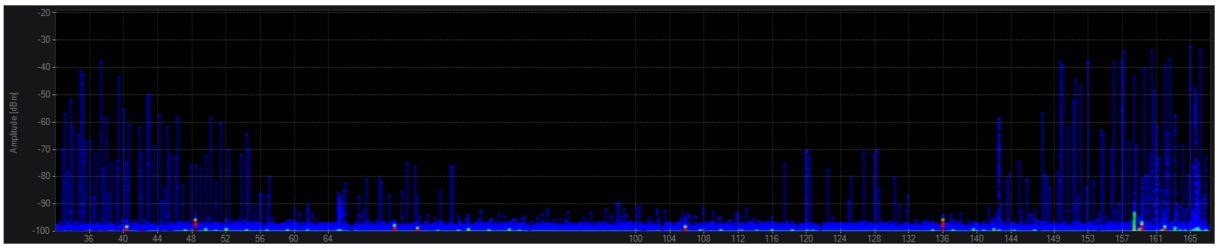
Rysunek 12: Pomiar widma w paśmie 2,4GHz



Rysunek 13: Pomiar widma z zaznaczonymi sieciami

ESSID	AP Alias	Channels	Signal Strength (dBm)	BSSID Count	Security	Max Rate (Mbps)	Vendors	802.11
DPS-Mielno		8	-61	1	WPA2-Personal	144,4	Zyxel Communications Corporati	b, g, n
Spokojne Wczasy 2 Pietro		4+8	-82	1	WPA2-Personal	300,0	Netcore Technology Inc.	b, g, n
HUAWEI-B315-8EAE-1		5-1	-77	1	WPA2-Personal	300,0		b, g, n
VILLASPOKOJNA26		2	-88	1	WPA2-Personal	144,4	Huawei Technologies Co.,Ltd	b, g, n
MarlinMielno2		11-7	-83	1	WPA2-Personal	300,0	Tp-Link Technologies Co.,Ltd.	b, g, n
TP-LINK_CFC0F6		1+5	-84	1	WPA2-Personal	300,0	Tp-Link Technologies Co.,Ltd.	b, g, n
VillaOazaMielno_Ext		5-1	-89	1	WPA2-Personal	300,0	Tecnomen Oy	b, g, n
MarlinMielno3		11-7	-88	1	WPA2-Personal	300,0	Tp-Link Technologies Co.,Ltd.	b, g, n
		11	-86	1	WPA2-Personal	144,4	Ubiquiti Networks Inc.	b, g, n
WiFiExtender-f4068d94886d		6	-85	1	WPA2-Personal	144,4	devolo AG	b, g, n
TP-LINK_Extender_3E5FDE		2	-88	1	Open	144,4	Tp-Link Technologies Co.,Ltd.	b, g, n
FunBox2-C466_EXT		1	-81	1	WPA2-Personal	144,4	Tp-Link Technologies Co.,Ltd.	b, g, n
Przemek		11	-90	1	WPA2-Personal	144,4	Ubiquiti Networks Inc.	b, g, n
		6	-88	1	WPA2-Personal	216,7	Ubiquiti Networks Inc.	b, g, n
HUAWEI-B525-5FE5		5-1	-86	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
VILLASPOKOJNA26_EXT		2	-89	1	WPA2-Personal	144,4		b, g, n
		1	-88	1	WPA2-Personal	144,4	Ubiquiti Networks Inc.	b, g, n
PPO453		1+5	-86	1	WPA2-Personal	300,0	Tp-Link Technologies Co.,Ltd.	b, g, n
WiFi SP6		6	-80	1	WPA2-Personal	216,7	Ubiquiti Networks Inc.	b, g, n
MarlinMielno1		11	-88	1	WPA2-Personal	288,9		b, g, n
DWR-116_5D2210		11	-88	1	WPA2-Personal	130,0	D-Link International	b, g, n
DPS		1, 11	-88	2	WPA2-Personal	288,9	, Sagemcom Broadband SAS	b, g, n
		11	-79	1	WPA2-Personal	130,0	Ubiquiti Networks Inc.	b, g, n
Hotspot Zielone Wzg?7rze		11	-80	1	WPA2-Personal	130,0	Ubiquiti Networks Inc.	b, g, n
VillaOazaMielno_2		5	-80	1	WPA2-Personal	144,4	Tecnomen Oy	b, g, n
VillaOazaMielno		5-1	-70	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n
SETUP		11	-70	1	Open	11,0		b
DPS-GOSC		8	-61	1	WPA2-Personal	144,4		b, g, n
HUAWEI-06D6		8+12	-85	1	WPA2-Personal	300,0	Huawei Technologies Co.,Ltd	b, g, n

Rysunek 14: Lista widocznych sieci

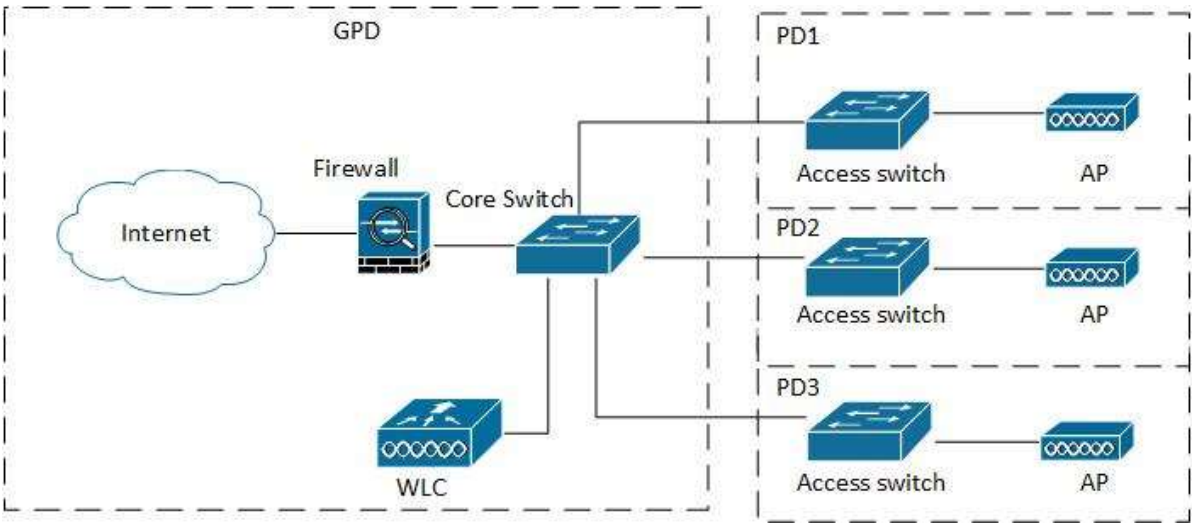


Rysunek 15: Pomiar widma w paśmie 5GHz

Jak widać na powyższych obrazkach jedynie co można zaobserwować sygnały pochodzące z obecnie propagowanych sieci. Nie występują zakłócenia w tym paśmie. Dla 5GHz można na poziomie szumów zobaczyć małe czerwone zakłócenia, które nie mają żadnego wpływu na sieć bezprzewodową, najprawdopodobniej pochodzą one od operatora telekomunikacyjnego.

Koncepcja nowej sieci LAN

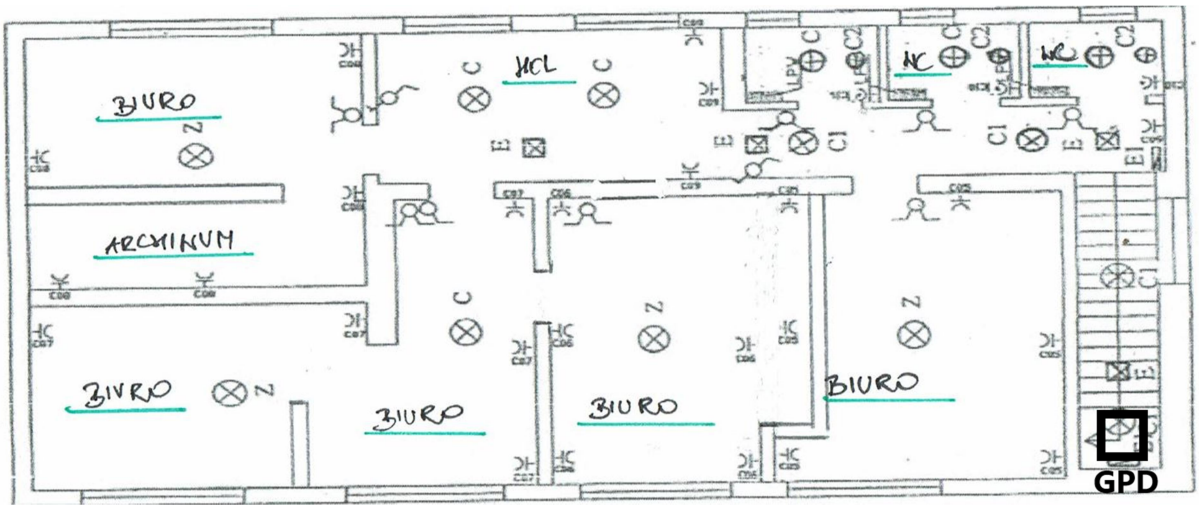
Nowa sieć LAN będzie oparta o rozbudowę tego co obecnie jest w Mielnie oraz jej rozbudowę, szczególnie jeżeli chodzi o budynek mieszkalny. W obecnej chwili poza kilkoma punktami nie ma tam żadnej infrastruktury. Niezbędne będzie doprowadzić nowe połączenie światłowodowe istniejącym przepustem pomiędzy budynkami. Internet jest doprowadzony od Orange. Należy rozprowadzić nowe połączenia światłowodowe pomiędzy wszystkimi punktami pośrednimi, a główną serwerownią. Na styku nowej sieci LAN z Internetem powinno znaleźć się urządzenie zabezpieczające sieć wewnętrzną – firewall. W każdym punkcie dystrybucyjnym należy umieścić przełącznik dostępowy co najmniej 24 portowy PoE/PoE+, tak aby podłączyć wszystkie access pointy. Każdy z punktów następnie zostanie podłączony do switcha corowego w głównej serwerowni. Należy przyjąć architekturę gwiazdy, w której każdy pośredni punkt dystrybuujmy będzie bezpośrednio podłączony do GPD. W głównej serwerowni będzie również zainstalowany kontroler sieci bezprzewodowej.



Rysunek 16: Schemat nowej sieci LAN

Punkty dystrybucyjne

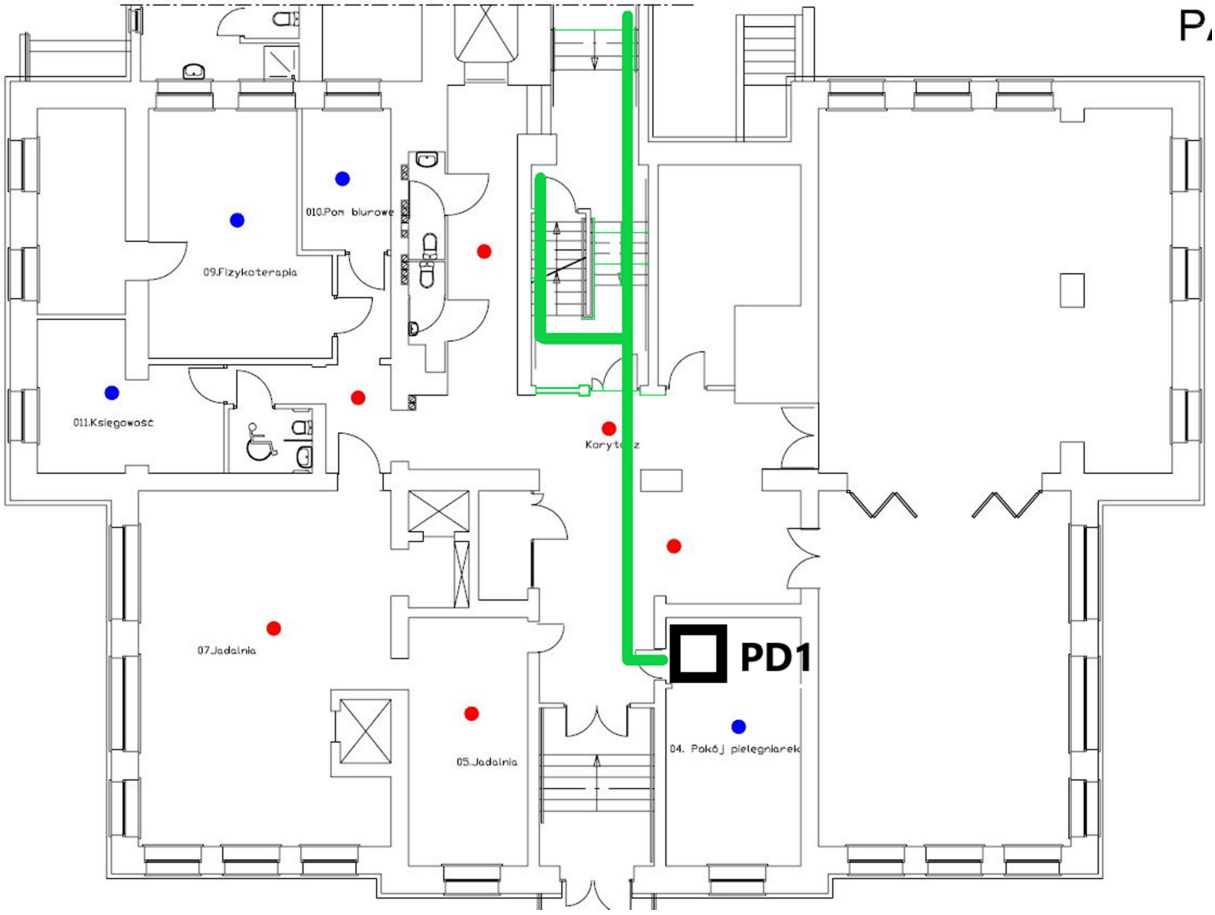
Budynek administracji



Rysunek 17: Koncepcja trasy światłowodu i instalacji szafy GPD – na klatce schodowej w budynku biurowym

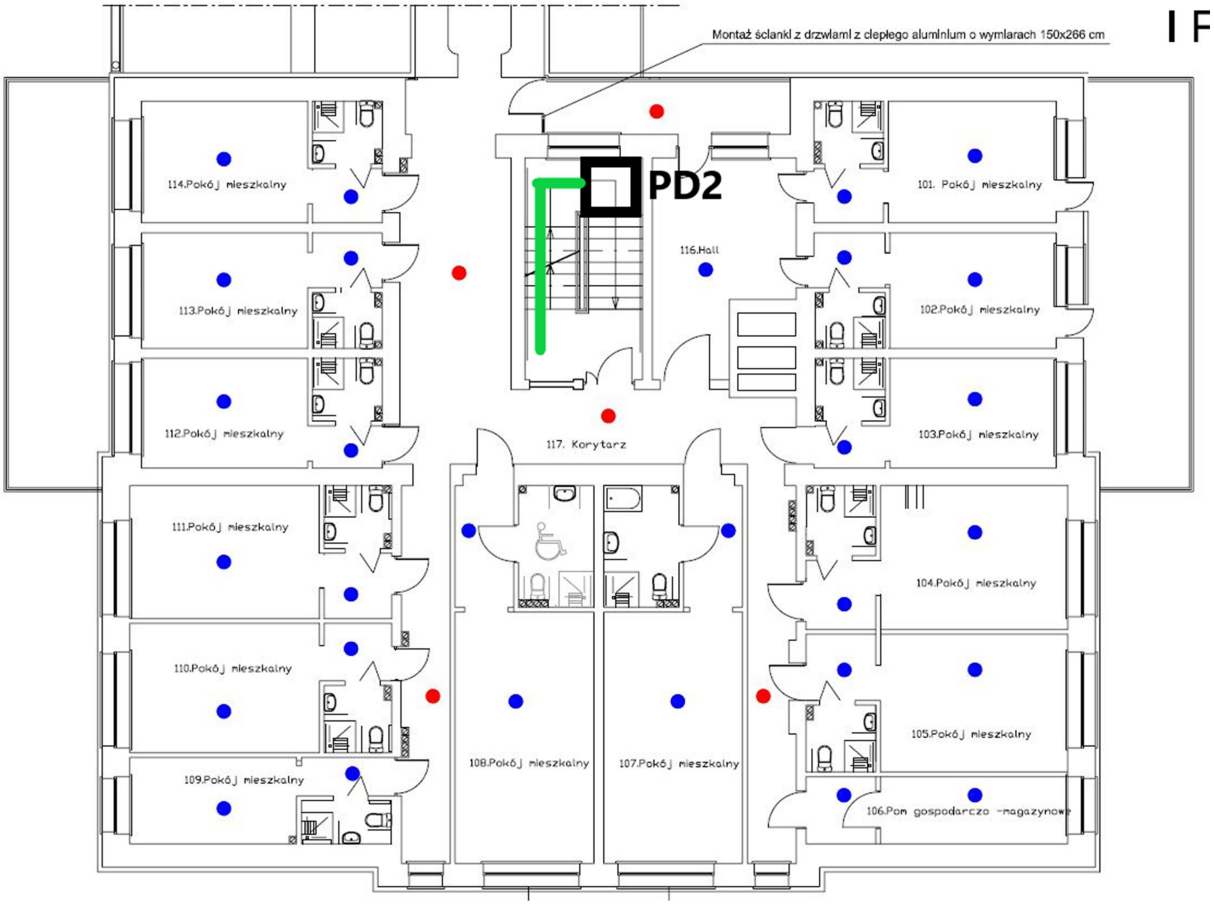
Budynek główny

Parter



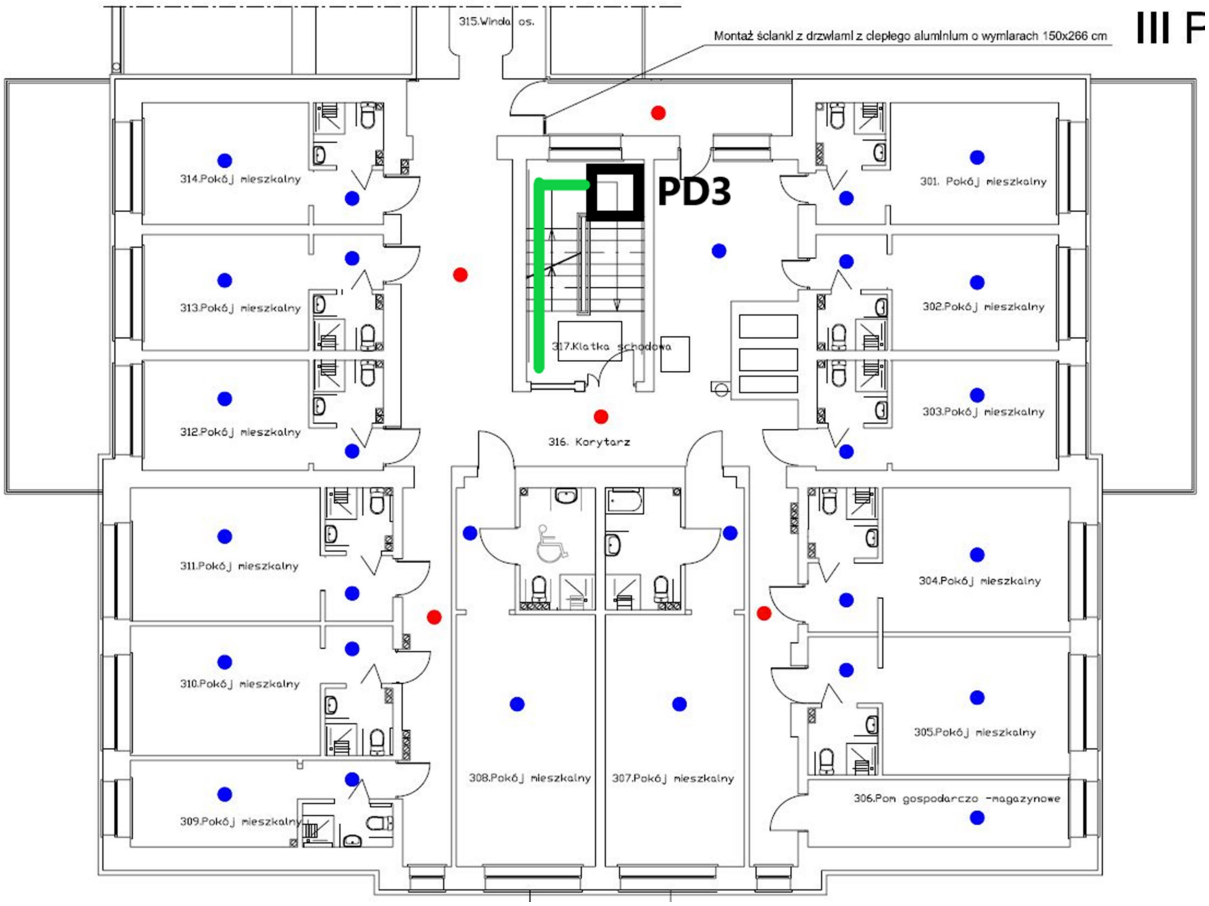
Rysunek 18: Koncepcja trasy światłowodu i instalacji szafy PD1 – nowy punkt na parterze w pomieszczeniu pielęgniarskim, zejście do GDP światłowodem

Pierwsze piętro



Rysunek 19: Koncepcja trasy światłowodu i instalacji szafyPD2 – rozbudowa istniejącego punktu, zejście do GDP światłowodem

Trzecie piętro



Rysunek 20: Koncepcja trasy światłowodu i instalacji szafy PD3 – punkt pomiędzy drugim a trzecim piętrem, zejście do GDP światłowodem

Analiza możliwości przyłączenia do zewnętrznej szerokopasmowej sieci internetowej

W obecnej chwili Internet jest doprowadzony stacjonarnie od Orange. Przy takich parametrach łącza można założyć kilkanaście połączeń video w jednym momencie. Zalecane jest, aby DPS miał nadaną stałą adresację publiczną.

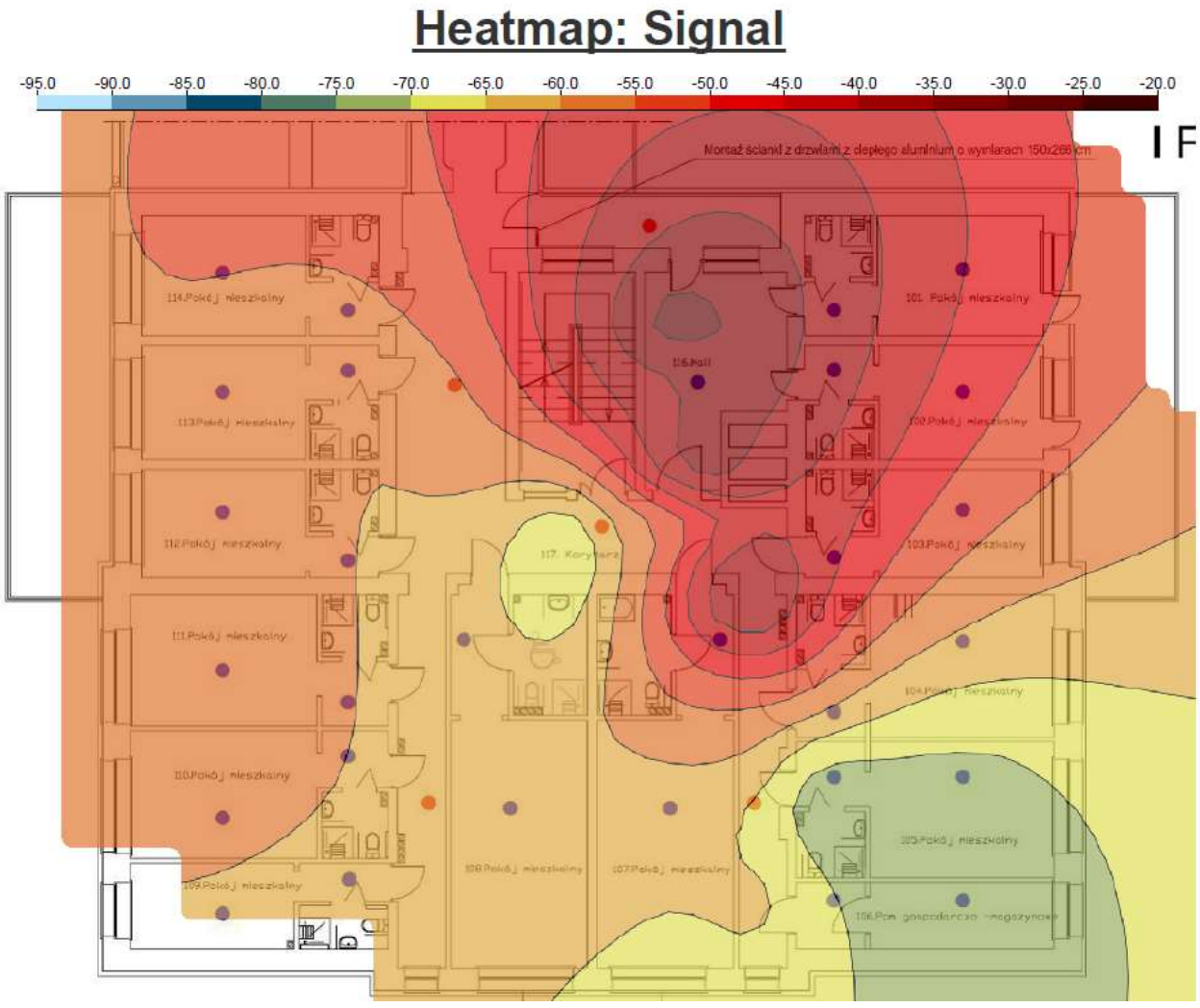
Rysunek 21: Test łącza internetowego wykonany z komputera stacjonarnego podłączonego do sieci LAN

Koncepcja rozmieszczenia nowych punktów dostępowych wraz z doporowadzeniem tras kablowych oraz protokół pomiarowy stanowiący podstawę do opracowania dokumentacji

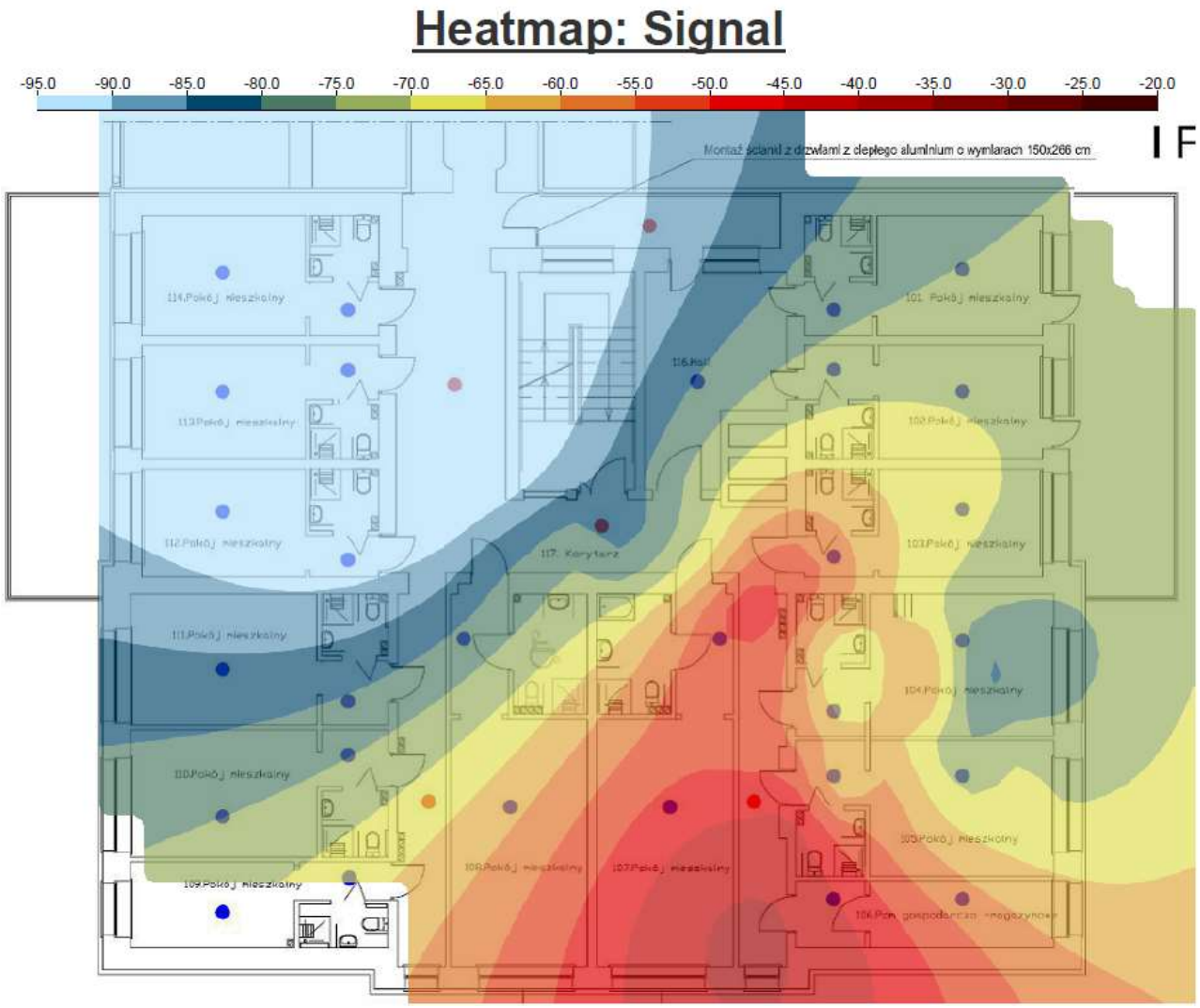
Cały obszar budynkowy powinien zostać objęty sygnałem radiowym a część zewnętrzna tylko we wskazanych miejscach. W planowaniu radiowym uwzględnione zostały dwa budynki (mieszkalny oraz administracyjny) jak i obszar zewnętrzny. W budynku mieszkalnym wszystkie piętra zostały objęte sygnałem radiowym z zachowaniem triangulacji w celu lokalizowania mieszkańców. W części administracyjnej uwzględnione zostało całe pierwsze piętro części biurowej oraz biuro księgowości na parterze.

Badanie sieci radiowej

Wykonane zostały badania tłumienia ścian, które pozwoliło na późniejsze przygotowanie rozmieszczenia access pointów na terenie całego DPS-u.



Rysunek 22: Badanie zostało przeprowadzone na pierwszym piętrze, w którym access point został umieszczony w przedsionku pokojów na pierwszym piętrze

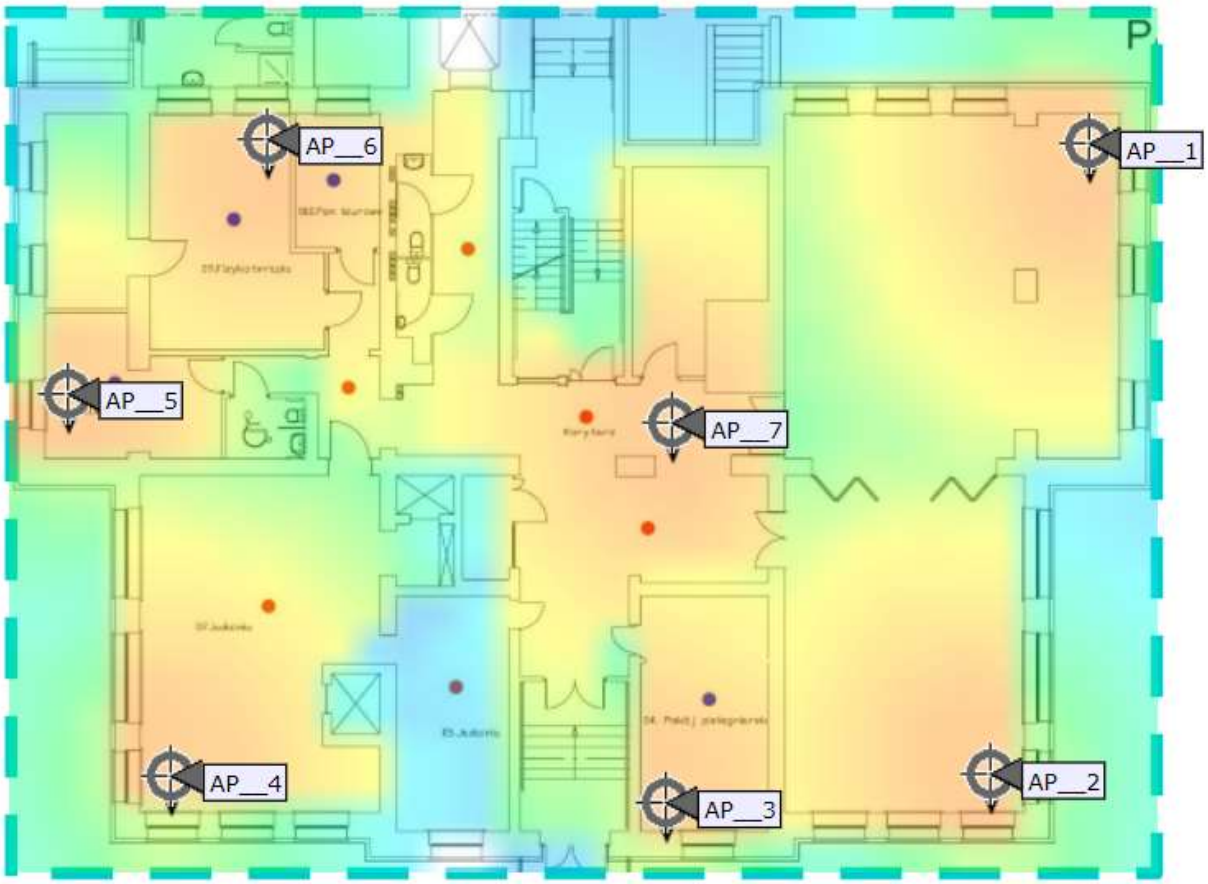


Rysunek 23: Badanie zostało przeprowadzone na pierwszym piętrze, w którym access point został umieszczony na końcu korytarza na pierwszym piętrze

Badania sieci radiowej ze względu ograniczenia epidemiologicznego zostały wykonane jedynie na pierwszym piętrze. Budynek mieszkalny w Mielnie jest budyniem w miarę nowym wykonanym z cegły, także nie ma dużej tłumienności ścian, których grubość nie przekracza 20 cm.

Budynek mieszkalny

Parter

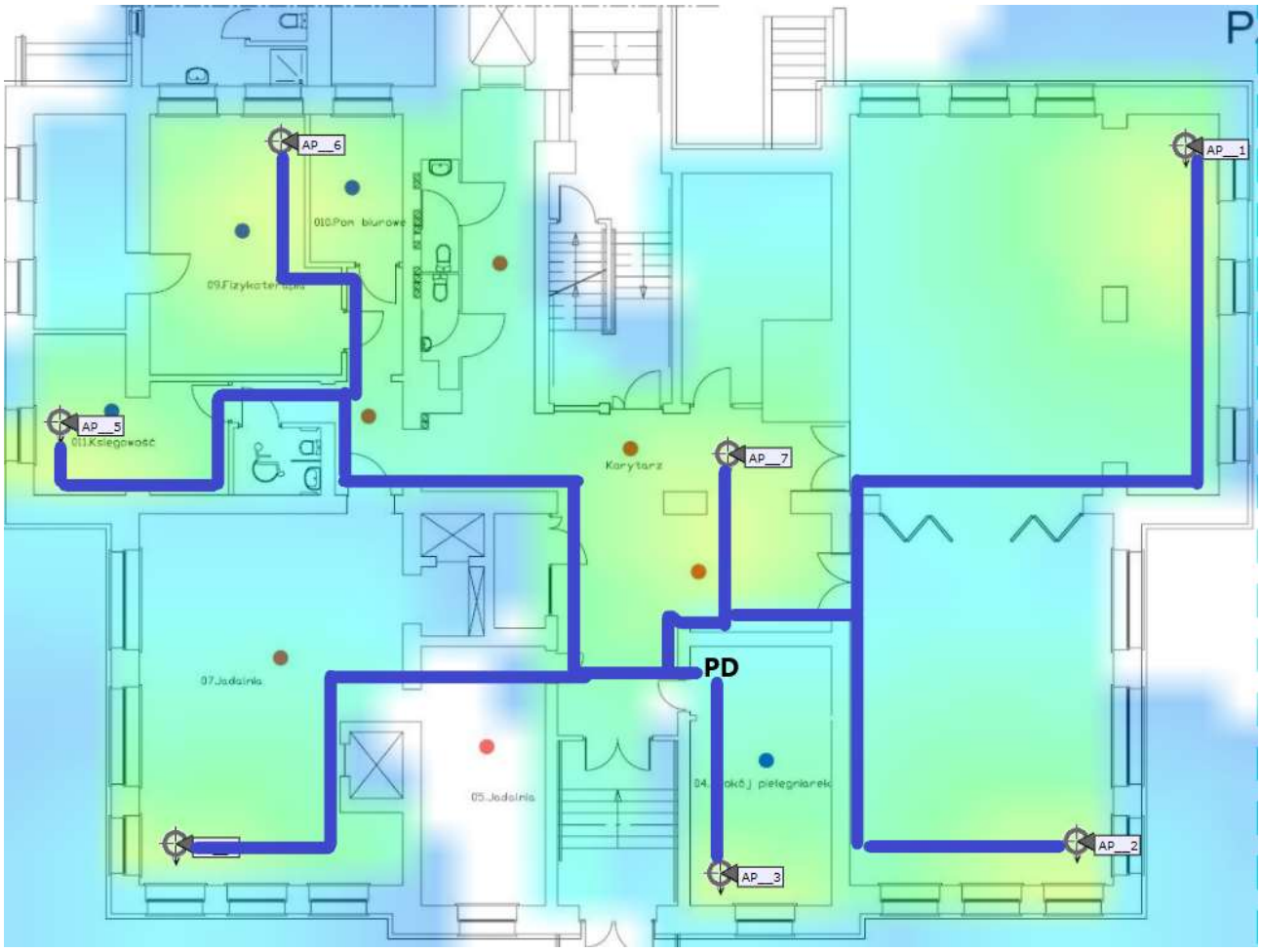


Rysunek 24: Planowanie dla częstotliwości 2,4GHz

Rysunek 25: Planowanie dla częstotliwości 5GHz

Na parterze zaproponowanych zostało siedem access pointów. Zejście z okablowaniem w plastikowych korytach do PD znajdującego się w pomieszczeniu pielęgniarskim.

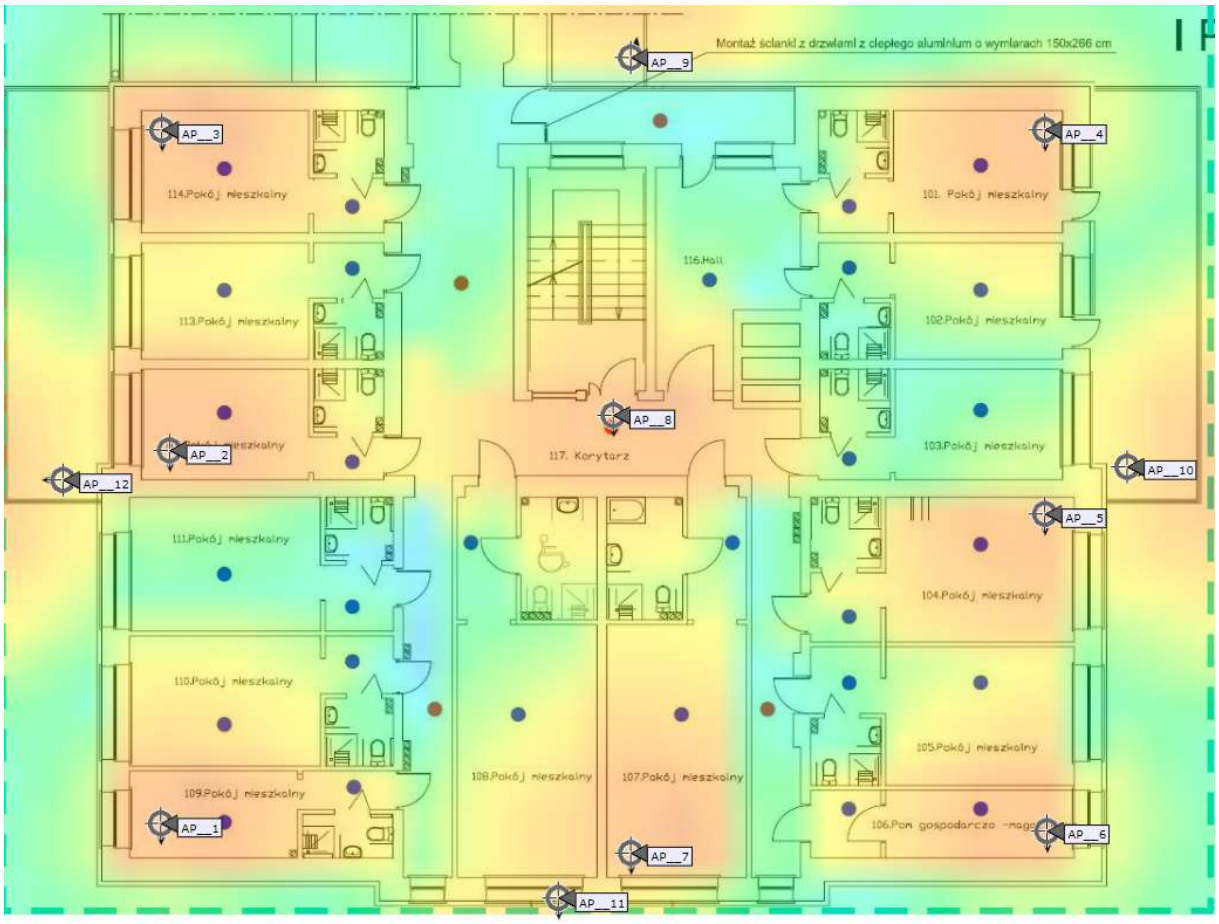
Planowane trasy kablowe



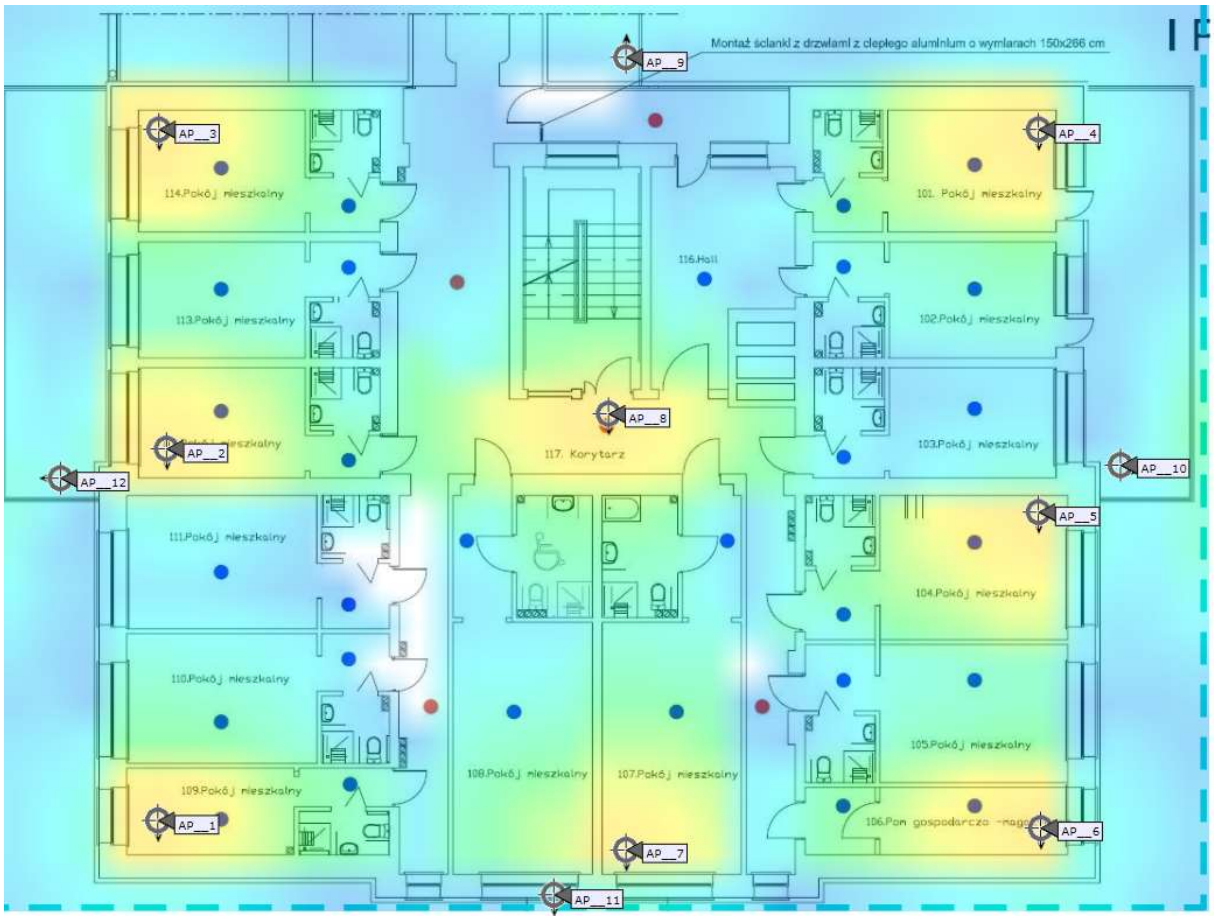
Rysunek 26: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	35
AP2	25
AP3	5
AP4	35
AP5	35
AP6	35
AP7	10

Pierwsze piętro



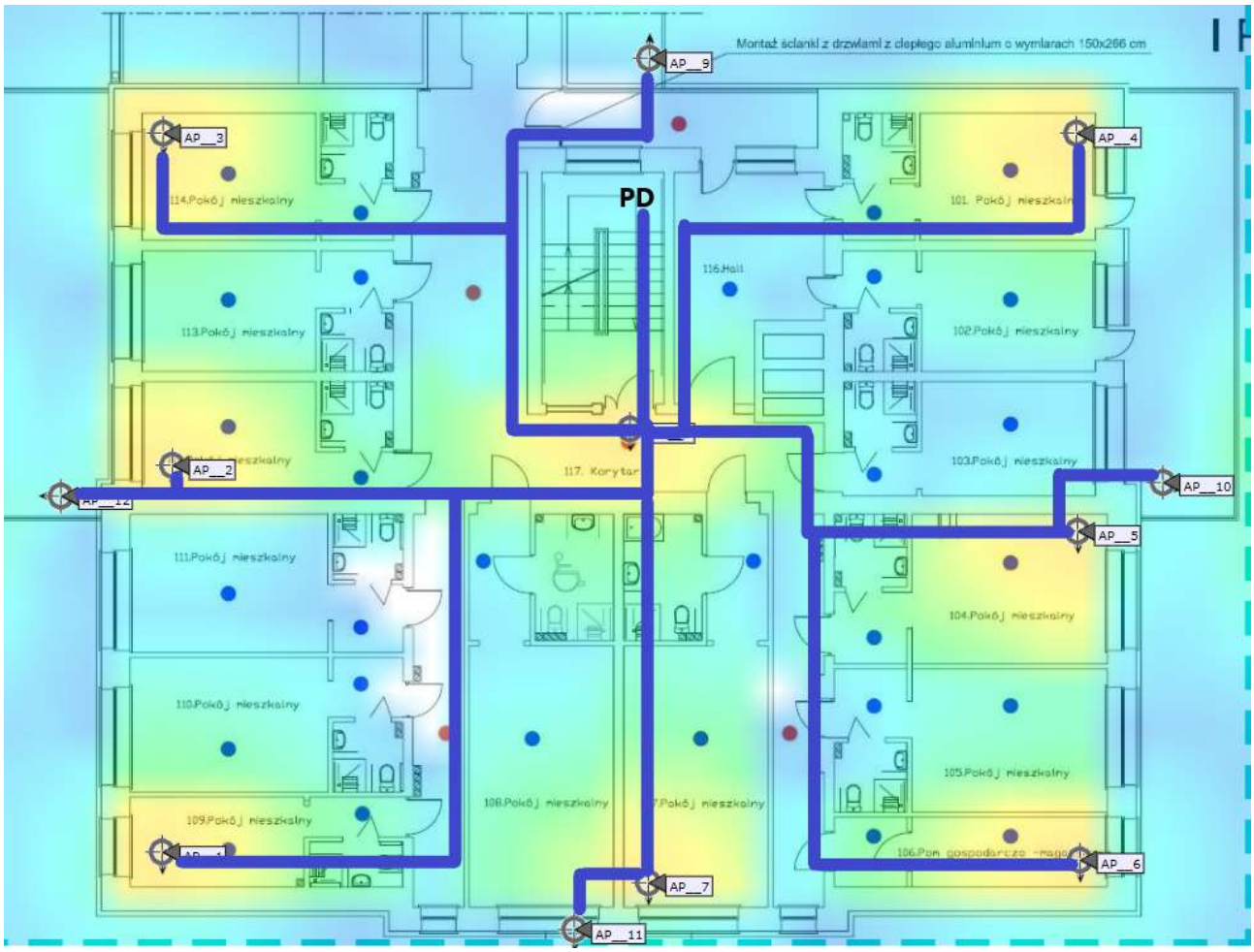
Rysunek 27: Planowanie dla częstotliwości 2,4GHz



Rysunek 28: Planowanie dla częstotliwości 5GHz

Na pierwszym piętrze zaproponowanych zostało osiem access pointów wewnętrznych oraz cztery zewnętrzne (AP9-AP12). Zejście z okablowaniem do szafy znajdującej się korytarzu pomiędzy parterem, a pierwszym piętrem.

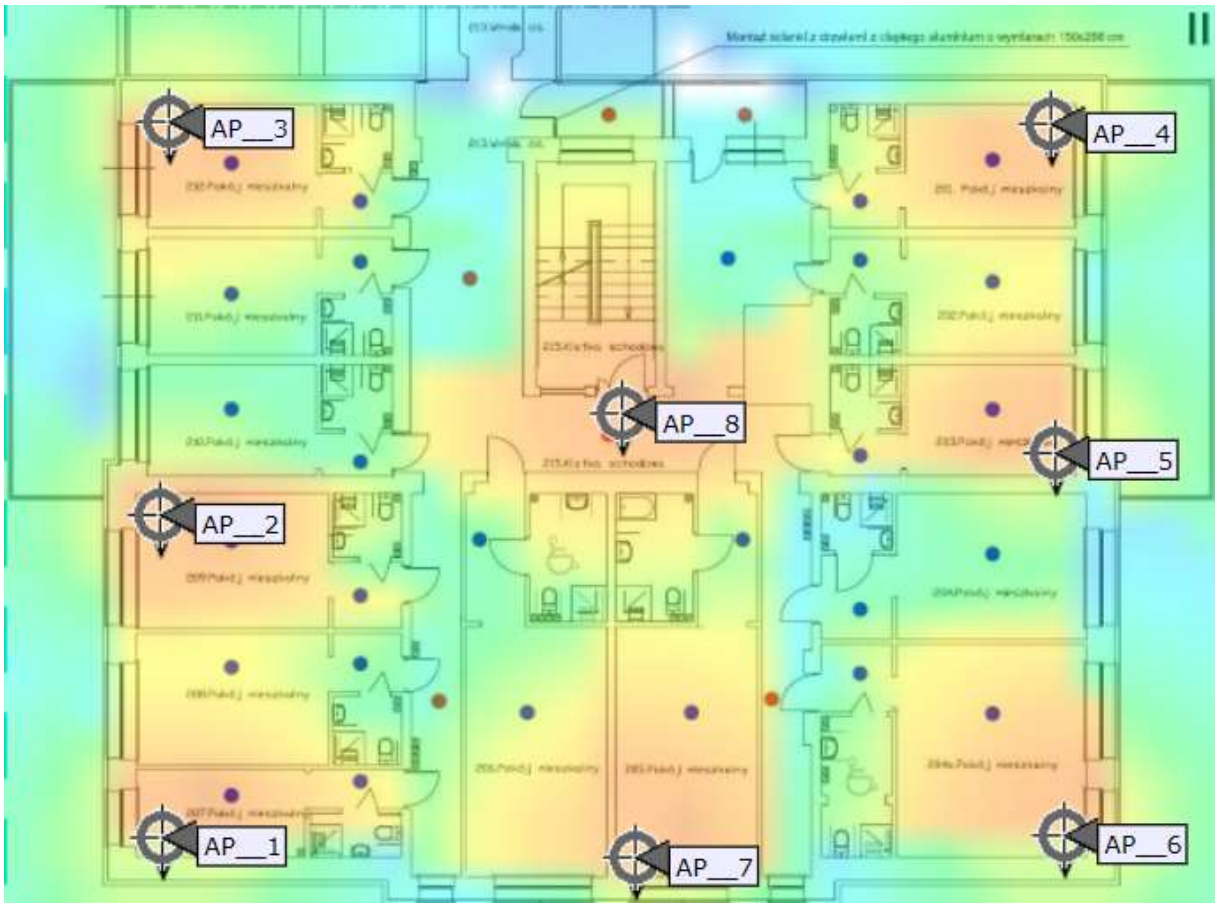
Planowane trasy kablowe



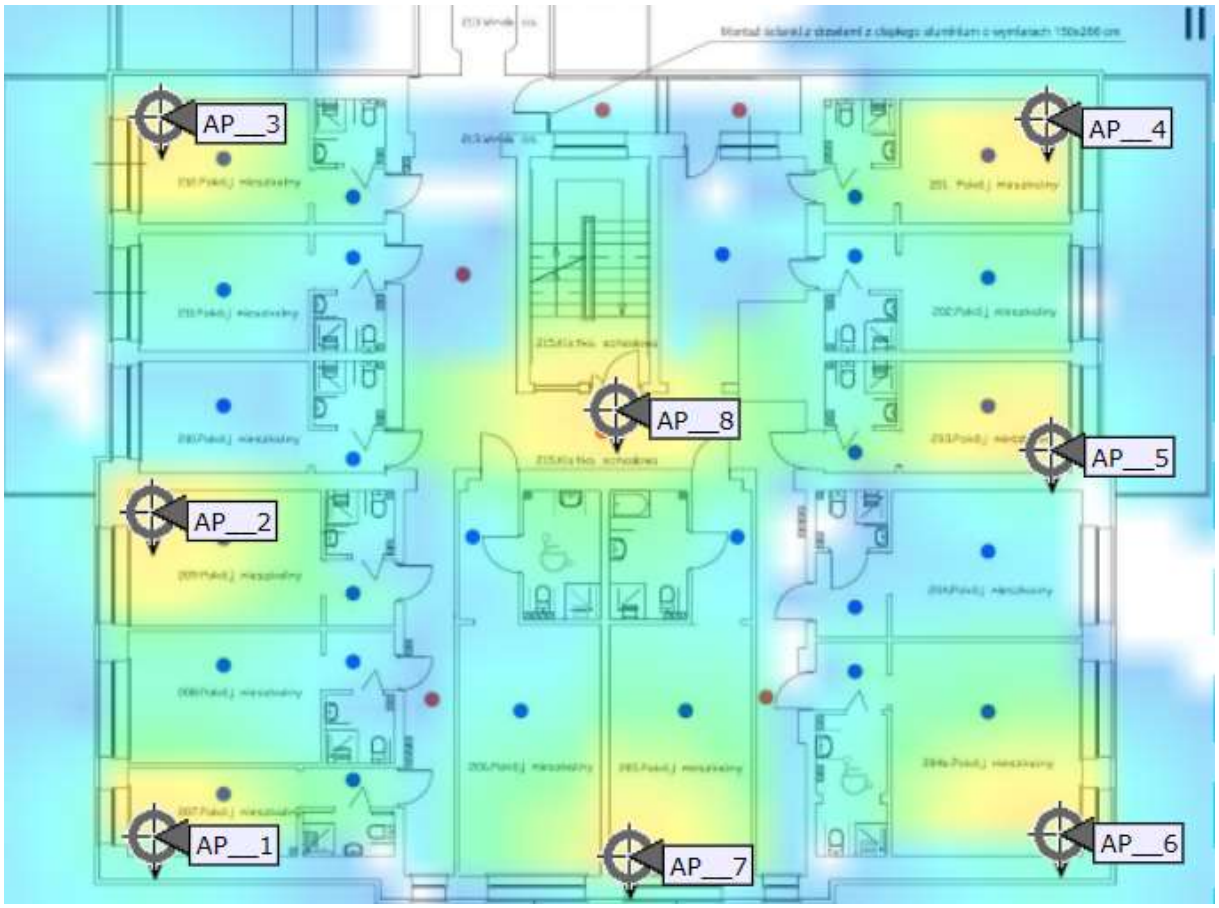
Rysunek 29: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu.

Numer AP	Szacowana długość okablowania [m]
AP1	50
AP2	35
AP3	35
AP4	35
AP5	35
AP6	50
AP7	30
AP8	15
AP9	50
AP10	50
AP11	50
AP12	50

Drugie piętro



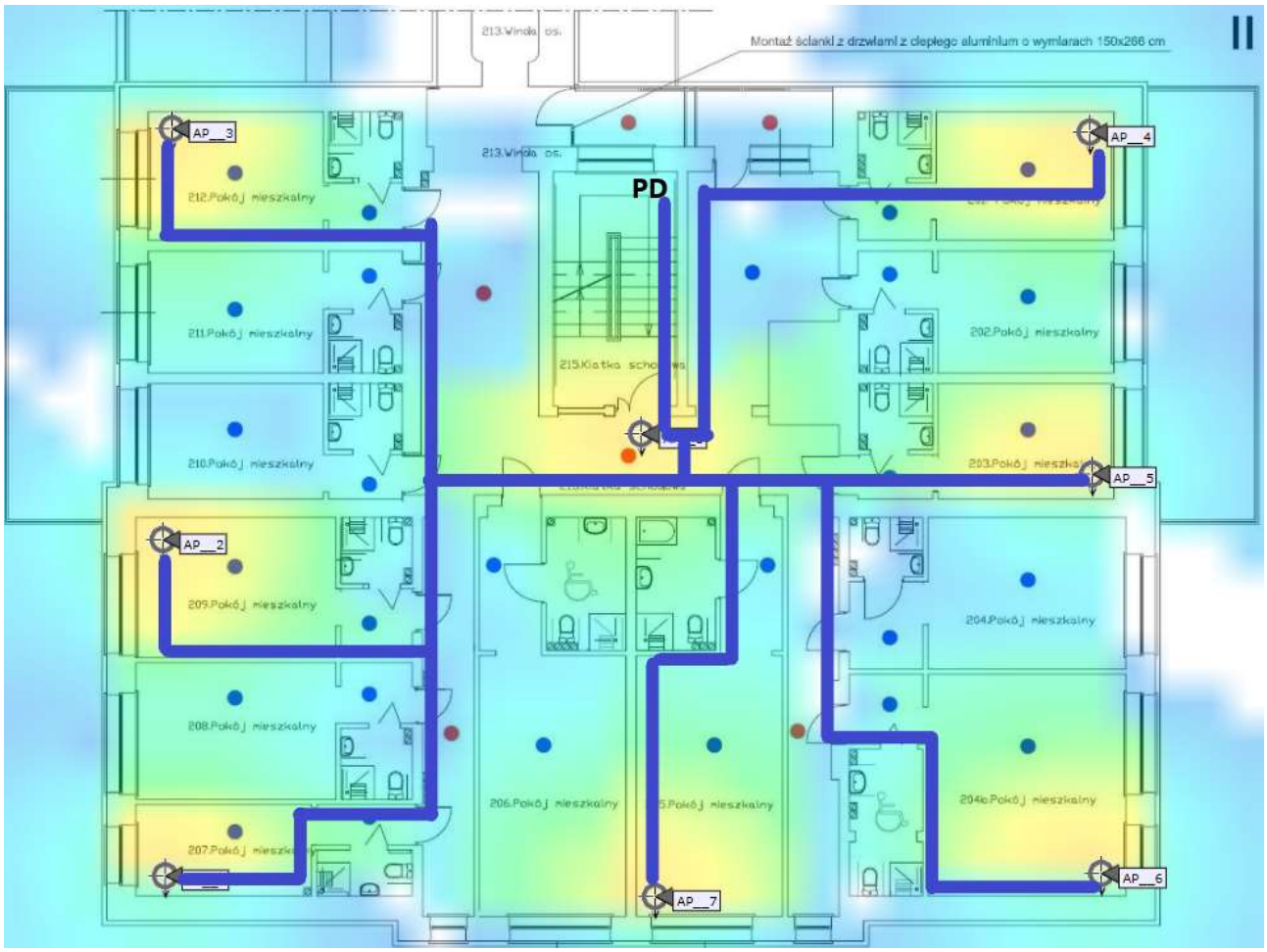
Rysunek 30: Planowanie dla częstotliwości 2,4GHz



Rysunek 31: Planowanie dla częstotliwości 5GHz

Na drugim piętrze zaproponowanych zostało osiem access pointów. Zejście z kablami do szafy rack znajdującej się pomiędzy drugi, a trzecim piętrem.

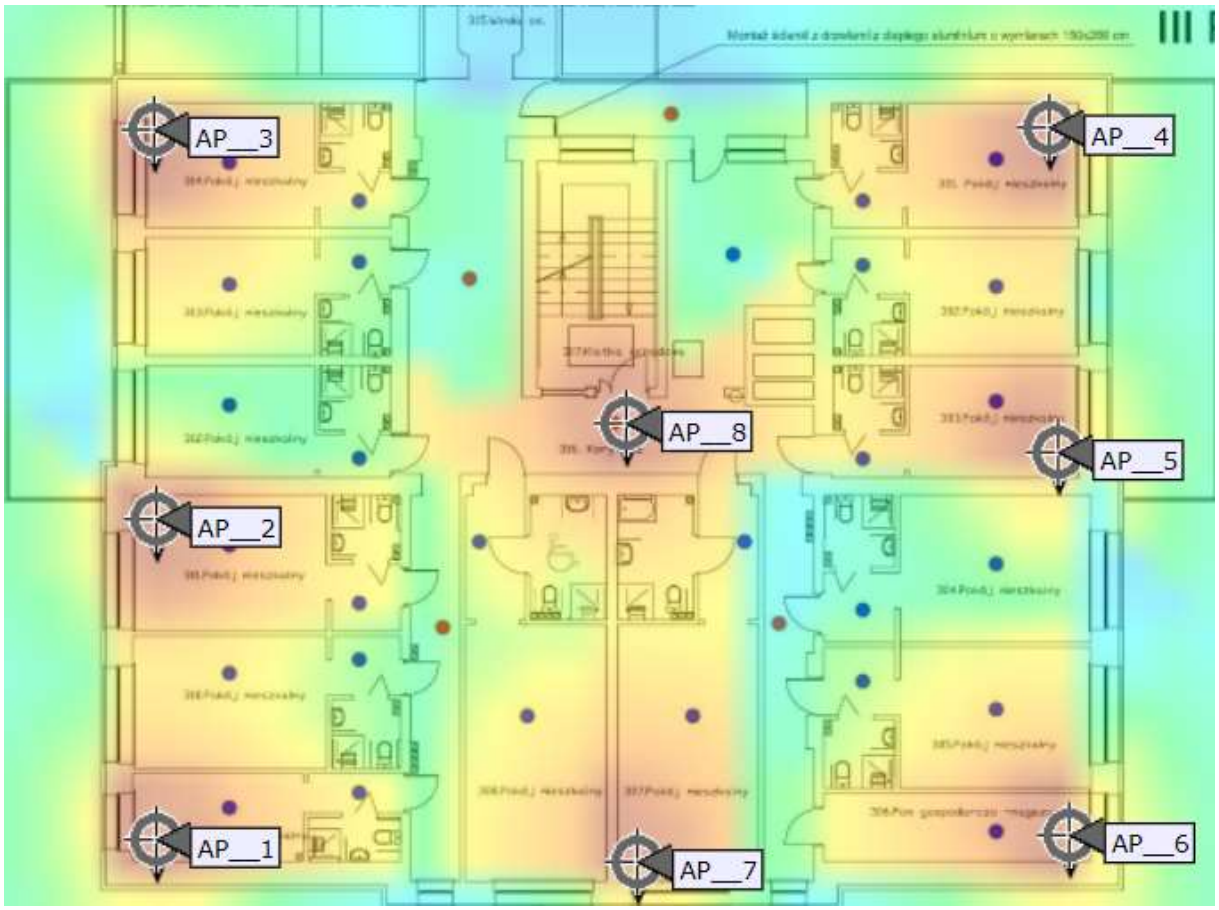
Planowane trasy kablowe



Rysunek 32: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	50
AP2	35
AP3	35
AP4	35
AP5	35
AP6	50
AP7	30
AP8	15

Trzecie piętro



Rysunek 33: Planowanie dla częstotliwości 2,4GHz

Rysunek 34: Planowanie dla częstotliwości 5GHz

Na trzecim piętrze zaproponowanych zostało osiem access pointów. Zejście z kablami do PD pomiędzy drugim a trzecim piętrem.

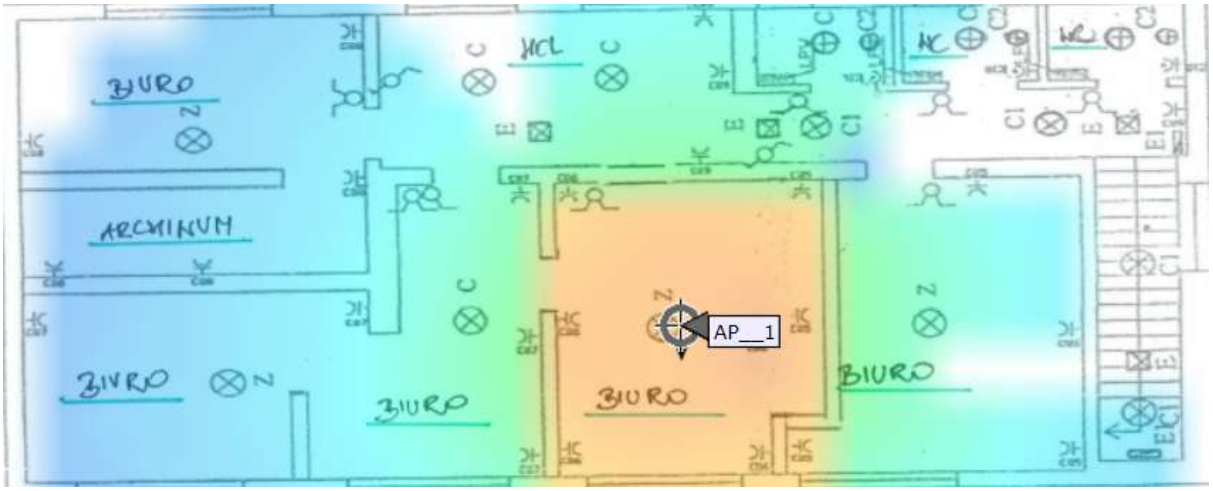
Planowane trasy kablowe

Rysunek 35: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	50
AP2	35
AP3	35
AP4	35
AP5	35
AP6	50
AP7	30
AP8	15

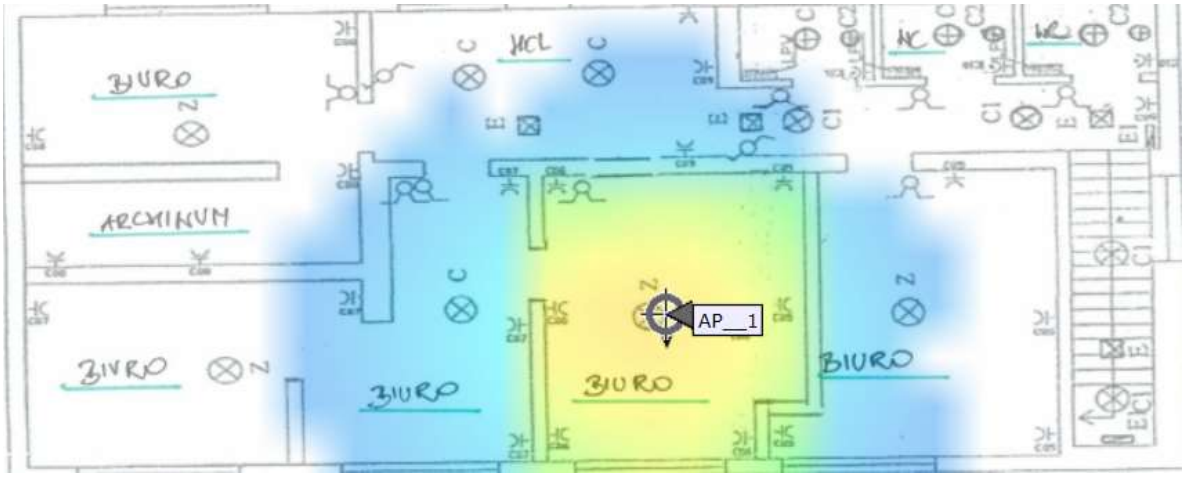
Budynek administracji

Parter



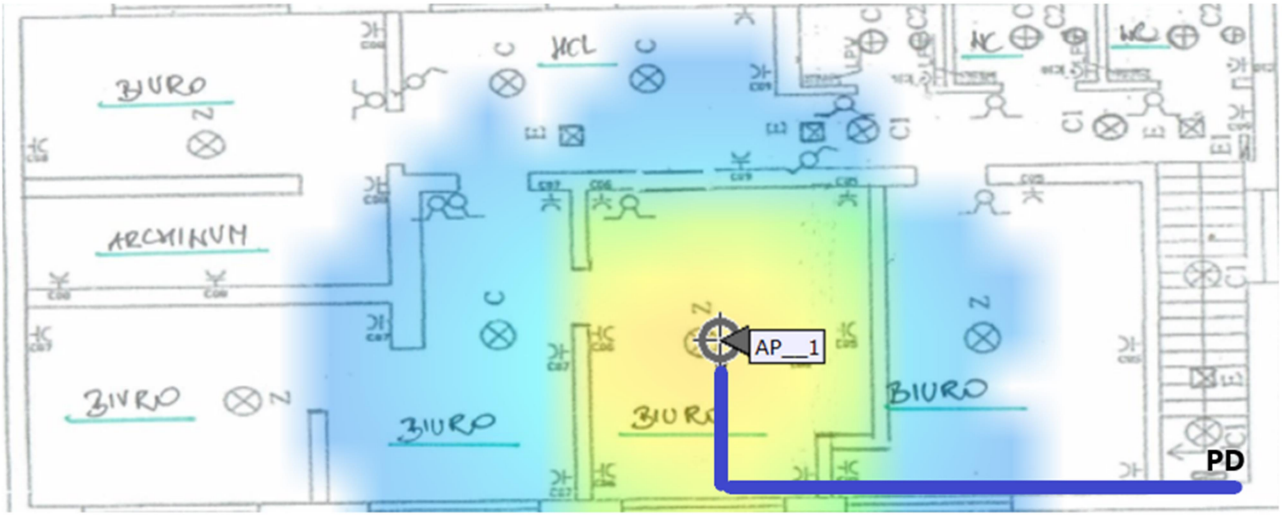
Rysunek 36: Planowanie dla częstotliwości 2,4GHz

Planowanie dla częstotliwości 5GHz



Rysunek 37: Na parterze został zaproponowany jeden access point w dziale księgowości. Zejście do GPD

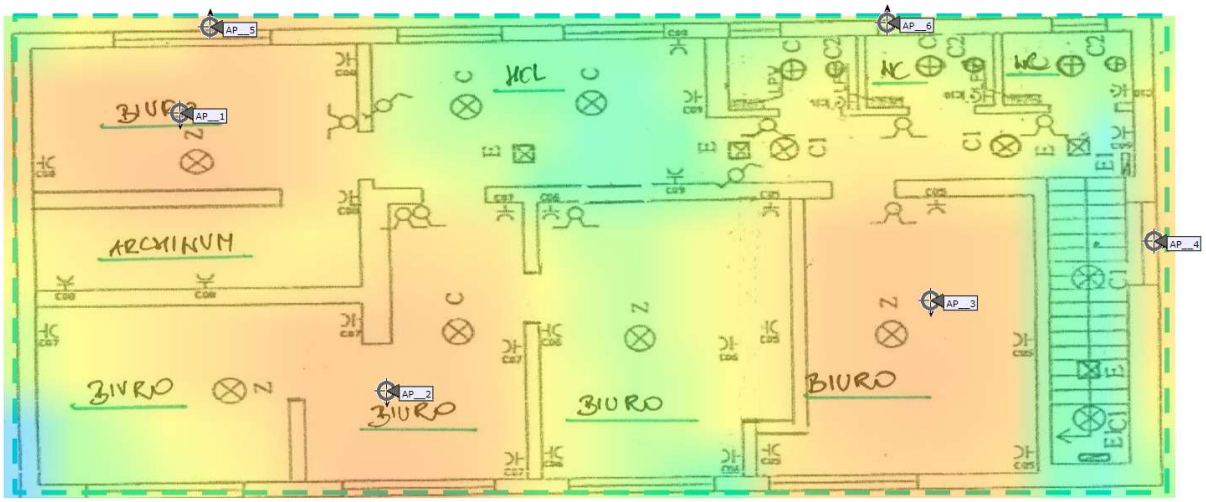
Planowane trasy kablowe



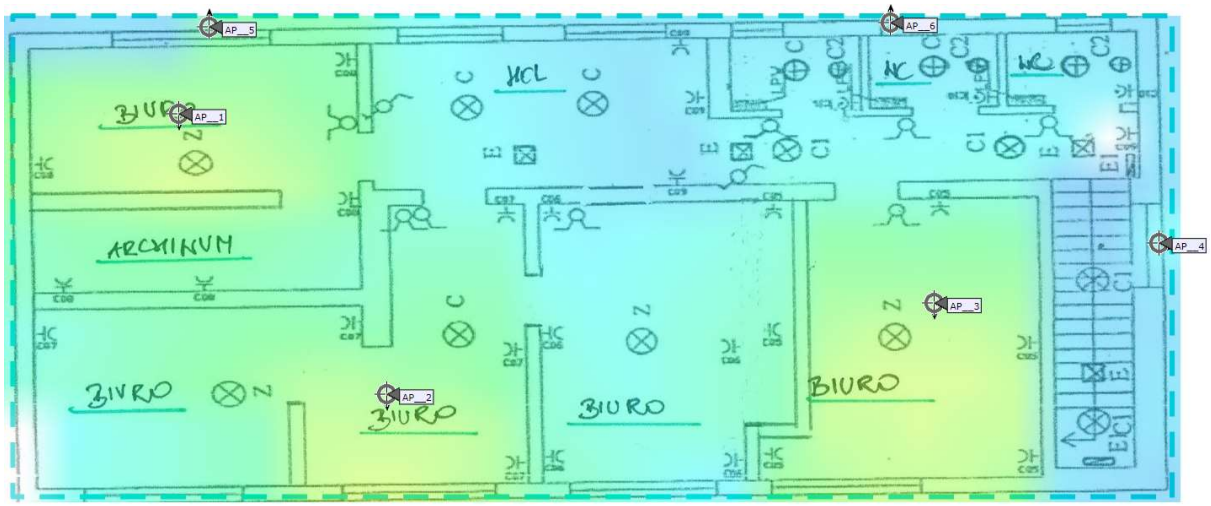
Rysunek 38: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	30

Pierwsze piętro



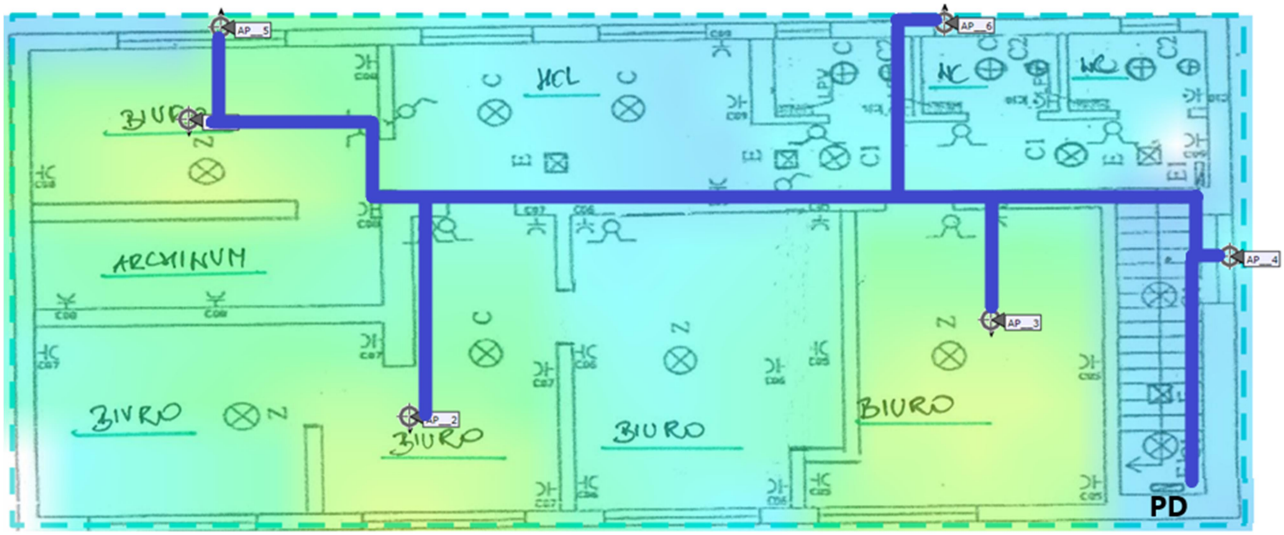
Rysunek 39: Planowanie dla częstotliwości 2,4GHz



Rysunek 40: Planowanie dla częstotliwości 5GHz

Na pierwszym piętrze w budynku administracji zaproponowane zostały trzy access pointy z zejściem kabli do GDP.

Planowane trasy kablowe



Rysunek 41: Całe okablowanie zejdzie się w korytkach do punktu PD, wzdłuż styku ścian/sufitu

Numer AP	Szacowana długość okablowania [m]
AP1	30
AP2	25
AP3	15
AP4	10
AP5	20
AP6	35

Podsumowanie

Liczba wszystkich urządzeń:

- Kontroler sieci bezprzewodowej: 1
- Access pointy: 42 w tym 7 zewnętrznych
- Switche: 1 core, 3 access
- Firewall: 1

Możliwe do wystąpienia problemy

Na etapie projektu oraz instalacji należy mieć na uwadze:

- Brak jakiejkolwiek infrastruktury, z której można by skorzystać w czasie projektowania czy instalacji nowej sieci.
- Brak istniejących tras kablowych oraz przepustów.
- Brak doprowadzonego zasilania do wybranych punktów dostępowych.
- Równocześnie problemem dla wprowadzenia nowoczesnych usług może okazać się niedostatek. parametrów połączenia internetowego oraz brak możliwości redundancji w tym zakresie.

Minimalne wymagania techniczne sprzętu

Kontroler sieci bezprzewodowej	• urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
	  ○ zarządzanie politykami bezpieczeństwa
	  ○ wykrywanie zagrożeń w sieci bezprzewodowej
	  ○ zarządzanie pasmem radiowym
	  ○ zarządzanie mobilnością
	  ○ zarządzanie jakością transmisji
	• obsługa min.: 50 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia o kolejne przez dodanie odpowiedniej licencji
	• min. 2 interfejsy 1G (SFP/SFP+ lub RJ-45)
	• opcja dodatkowa: obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
	• obsługa ruchu tunelowanego
	• obsługa min. 1000 klientów sieci bezprzewodowej
	• zarządzanie pasmem radiowym punktów dostępowych:
	  ○ automatyczna adaptacja do zmian w czasie rzeczywistym
	  ○ optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
	  ○ dynamiczne przydzielanie kanałów radiowych
	  ○ wykrywanie, eliminacja i unikanie interferencji
	  ○ równoważenie obciążenia punktów dostępowych
	  ○ tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
	  ○ automatyczna dystrybucja klientów pomiędzy punkty dostępowe
	  ○ mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
	  ○ dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
	• mapowanie SSID do segmentów VLAN w sieci przewodowej
	• możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
	• automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
	• obsługa mechanizmów bezpieczeństwa:
	  ○ 802.11i, WPA3, WPA2, WPA, WEP
	  ○ 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
	  ○ obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
	• kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
	• obsługa dostępu gościnnego (IPv4 i IPv6)

	○ przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony) ○ przekierowanie użytkowników do strony logowania na zewnętrznym serwerze • współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych • obsługa NTP wersji 4 (IPv4 oraz IPv6) • obsługa Hotspot 2.0 • obsługa redundancji rozwiązania
Access point wewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax ○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników

	○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID ○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • anteny zintegrowane dookólne dla access pointów wewnętrznych, anteny sektorowe dla access pointów zewnętrznych
Access point zewnętrzny	• obsługa standardów 802.11a/b/g/n/ac/ax (potwierdzona przez Wi-Fi Alliance) ○ obsługa OFDMA (uplink/downlink), TWT, BSS Coloring ○ obsługa MU-MIMO – min. 2x2:2 ○ obsługa kanałów 20, 40 MHz dla 802.11n ○ obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax ○ obsługa beamforming dla klientów 802.11a/g/n/ac/ax

	○ obsługa MRC (Maximal Ratio Combining) • obsługa szerokiego zakresu kanałów radiowych: ○ dla zakresu 2.4 GHz: min. 13 kanałów ○ dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów ○ dla zakresu 5GHz (extended UNII-2): min. 8 kanałów • konfigurowalna moc nadajnika ○ dla zakresu 2.4 GHz: do 100 mW ○ dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW ○ dla zakresu 5GHz (extended UNII-2): do 200 mW • zarządzanie przez kontroler WLAN z funkcjonalnościami: ○ automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN ○ optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany) ○ obsługa min. 16 BSSID ○ definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID ○ uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w ○ obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN) ○ możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników ○ obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h ○ obsługa IPv6 ○ obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ○ obsługa mechanizmów QoS: ▪ ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik ▪ obsługa WMM, TSPEC, U-APSD ○ współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne ○ wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM ○ wsparcie IEEE 802.11i, WPA3, WPA2, WPA ○ wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP) • konfiguracja polityk bezpieczeństwa per SSID

	○ obsługa WPA2 i WPA3 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników-lokalny RADIUS) ○ współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID) ○ tworzenie list kontroli dostępu opartych o adresy IPv4 oraz o nazwy domenowe ○ obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC) ○ obsługa dostępu gościnnego z wbudowanym lub zewnętrznym portalem gościnnym ○ obsługa kreowania użytkowników gościnnych za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta; ○ wsparcie SSH, SNMP, NTP, SYSLOG • interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at). • dla access pointów zewnętrznych: ○ zgodność z IP67 ○ min. praca przy temperaturach między -35^{o}C a 60^{o}C • certyfikacja WiFi Alliance: 802.11 a/b/g/n/ac/ax, WMM, Passpoint
Switch core	• Typ i liczba portów: ○ Min: 12 SFP/SFP+ • Opcja dodatkowa: slot na moduł rozszerzeń z możliwością obsadzenia modułami (zależnie od potrzeb): ○ min. 4x1G SFP ○ min. 4x1/10G SFP+ • Porty SFP/SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb: ○ Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U ○ Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax • Możliwość tworzenia stosów • Parametry wydajnościowe: ○ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) ○ Bufor pakietów – min.: 8MB

	o Pamięć DRAM – min.: 4GB o Pamięć flash – min.: 8GB o Obsługa ▪ min. 3.000 sieci VLAN ▪ min.: 16.000 adresów MAC • Obsługa protokołu NTP • Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: o Obsługa protokołu STP • Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego • Możliwość uruchomienia funkcji serwera DHCP • Mechanizmy związane z bezpieczeństwem sieci: o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN o Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL o Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC o Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 o Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard • Obsługa protokołów routingu: o Routing statyczny dla IPv4 i IPv6 • Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN • Zarządzanie o Port konsoli o Dedykowany port Ethernet do zarządzania out-of-band o Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją o Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 o Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB • Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Switch access	• Typ i liczba portów:
	  ○ min. 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink min: 2x10G SFP
	• Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami)
	• Porty SFP/SFP+ możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
	  ○ Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
	  ○ Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
	• Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
	  ○ Przepustowość w ramach stosu – min.:60Gb/s
	  ○ min: 4 urządzenia w stosie
	  ○ Zarządzanie poprzez jeden adres IP
	• Parametry wydajnościowe:
	  ○ Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
	  ○ Bufor pakietów – min: 4MB
	  ○ Pamięć DRAM – min: 1GB
	  ○ Pamięć flash – min: 2GB
	  ○ Obsługa
	  ▪ 1024 sieci VLAN
	  ▪ min: 16.000 adresów MAC
	• Obsługa protokołu NTP
	• Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
	  ○ IEEE 802.1w Rapid Spanning Tree
	• Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
	• Możliwość uruchomienia funkcji serwera DHCP
	• Obsługa protokołów routingu:
	  ○ Routing statyczny dla IPv4 i IPv6
	• Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN

	• Zarządzanie
	  ○ Port konsoli
	  ○ Dedykowany port Ethernet do zarządzania out-of-band
	  ○ Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
	  ○ Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
	  ○ Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
	• Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Firewall	• Wymagania Ogólne
	  ○ Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
	  ○ System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
	  ○ System musi wspierać IPv4 oraz IPv6 w zakresie:
	  ▪ Firewall.
	  ▪ Ochrony w warstwie aplikacji.
	  ▪ Protokołów routingu dynamicznego.
	• Redundancja, monitoring i wykrywanie awarii
	  ○ W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
	  ○ Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
	  ○ Monitoring stanu realizowanych połączeń VPN.
	• Interfejsy, Dysk, Zasilanie:
	  ○ System realizujący funkcję Firewall musi dysponować minimum:

	▪ min. 4 portami Gigabit Ethernet RJ-45. ▪ min. 2 gniazdami SFP 1 Gbps. o System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. o System musi być wyposażony w zasilanie AC. • Parametry wydajnościowe: o W zakresie Firewall'a obsługa nie mniej niż 1.0 mln. jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę. o Przepustowość Stateful Firewall: nie mniej niż 0,5 Gbps o Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0,5 Gbps. o Wydajność szyfrowania IPSec VPN nie mniej niż 0,5 Gbps. • Funkcje Systemu Bezpieczeństwa: o W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: ▪ Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. ▪ Kontrola Aplikacji. ▪ Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. ▪ Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. ▪ Ochrona przed atakami - Intrusion Prevention System. ▪ Kontrola stron WWW. ▪ Zarządzanie pasmem (QoS, Traffic shaping). ▪ Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). ▪ Funkcja lokalnego serwera DNS ze wsparciem dla DNS • Polityki, Firewall o Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. o System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: ▪ Translację jeden do jeden oraz jeden do wielu. ▪ Dedykowany ALG (Application Level Gateway) dla protokołu SIP. ▪ W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. ▪ Możliwość wykorzystania w polityce bezpieczeństwa

	zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
	• Połączenia VPN
	  ○ System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Wsparcie dla IKE v1 oraz v2.
	  ▪ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
	  ▪ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
	  ▪ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
	  ▪ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
	  ▪ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
	  ▪ Mechanizm „Split tunneling” dla połączeń Client-to-Site.
	  ○ System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
	  ▪ Opcja dodatkowa: Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
	  ▪ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
	  ▪ Opcja dodatkowa: Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
	• Routing i obsługa łączy WAN
	  ○ W zakresie routingu rozwiązanie powinno zapewniać obsługę:
	  ▪ Routingu statycznego.
	  ▪ Policy Based Routingu.
	  ▪ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
	• Ochrona przed malware
	• Ochrona przed atakami
	  ○ Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
	• Kontrola aplikacji

	• Kontrola WWW • Zarządzanie • Logowanie • Serwisy i licencje ○ W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. • Gwarancja oraz wsparcie
Okablowanie etherentowe	• Min. Cat 6 ekranowana