PROGRAM FUNKCJONALNO-UŻYTKOWY DLA ZADANIA „BUDOWA ŻYWIECKIEJ ŚWIATŁOWODOWEJ SIECI SZEROKOPASMOWEJ”

PROGRAM FUNKCJONALNO-UŻYTKOWY

(opracowany zgodnie z art. 31 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych i zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 2 września 2004r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno użytkowego)

Zamawiający:
Gmina Żywiec

Adres:
34-300 Żywiec,
Rynek 2

Nazwa zamówienia:
„Budowa żywieckiej światłowodowej sieci szerokopasmowej”

Adres:
Zgodnie z listą obiektów zawartych w programie funkcjonalno-użytkowym

Nazwa zamówienia wg CPV:
32.41.30.00 - Sieć zintegrowana

Kod zamówienia wg CPV:

71320000-7	Usługi inżynieryjne w zakresie projektowania
71220000-6	Usługi projektowania architektonicznego
71323100-9	Usługi projektowania systemów zasilania energią elektryczną
72224100-2	Usługi w zakresie planowania wdrażania systemu
72720000-3	Usługi w zakresie rozległej sieci komputerowej
45231000-5	Roboty budowlane w zakresie budowy rurociągów, ciągów komunikacyjnych i linii energetycznych
45.23.20.00-2	Roboty pomocnicze w zakresie rurociągów i kabli
45311000-0	Roboty w zakresie okablowania oraz instalacji elektrycznych
45111200-0	Roboty w zakresie przygotowania terenu pod budowę i roboty ziemne
45211360-0	Roboty budowlane w zakresie rozwoju miast
45231600-1	Roboty budowlane w zakresie budowy linii komunikacyjnych
45232000-2	Roboty pomocnicze w zakresie rurociągów i kabli
45100000-8	Przygotowanie terenu pod budowę
45000000-7	Roboty budowlane
45400000-1	Roboty wykończeniowe w zakresie budynków
45262700-8	Przebudowa budynków
45312100-8	Instalowanie przeciwpożarowych systemów alarmowych
45312330-9	Montaż anten radiowych
45312200-9	Instalowanie przeciwwłamaniowych systemów alarmowych
45314000-1	Instalowanie urządzeń telekomunikacyjnych
45314300-4	Instalowanie infrastruktury okablowania
45421000-4	Roboty w zakresie stolarki budowlanej
45410000-4	Roboty tynkarskie
45430000-0	Pokrywanie podłóg i ścian
45262300-4	Betonowanie
45262400-5	Wznoszenie konstrukcji ze stali konstrukcyjnej
45262500-6	Roboty murarskie
45262600-7	Różne specjalistyczne roboty budowlane
45442100-8	Roboty malarskie
45450000-6	Roboty budowlane wykończeniowe, pozostałe
45310000-3	Roboty w zakresie instalacji elektrycznych
45330000-9	Hydraulika i roboty sanitarne
45331210-1	Instalowanie wentylacji
45231400-9	Roboty budowlane w zakresie linii energetycznych
45233220-7	Roboty budowlane w zakresie nawierzchni dróg

Autor opracowania: Tomasz Kuca
Wrzesień 2012

Spis treści programu funkcjonalno-użytkowego

2.8. Zadania Wykonawcy związane z wdrożeniem systemów zarządzania i monitoringu parametrów warstwy aktywnej sieci miejskiej zintegrowanych w pomieszczeniach centrum Zarządzania Siecią
- 2.8.1. Elementy składowe systemu Zarządzania Siecią.
- 2.8.2. Infrastruktura uzupełniająca Centrum Zarządzania Siecią.
- 2.8.3. Wymagania ogólne w dziedzinie niezawodności i wydajności.
- 2.8.4. Wymagania ogólne w dziedzinie bezpieczeństwa.
- 2.8.5. Wymagania ogólne w dziedzinie zarządzania.
- 2.8.6. Wymagania dla sprzętu aktywnego i oprogramowania Centrum wraz z zestawieniem zalecanych parametrów
  - 2.8.6.1. Wymagania dla urządzeń zabezpieczenia systemów zarządzania
  - 2.8.6.2. Wymagania dla oprogramowania zarządzającego urządzeniami w sieci
  - 2.8.6.3. Wymagania na urządzenie systemu monitoringu i analizy zdarzeń w sieci:
  - 2.8.6.4. Wymagania dla systemu autentykacji, autoryzacji oraz accoutingu

3. Warunki odbioru robót.

3.1. Odbiór dokumentacji projektowej:
3.2. Odbiór prac związanych z wykonawstwem kanalizacji teletechnicznej i mikrokabli
3.3. Odbiór prac wdrożeniowych poszczególnych systemów i urządzeń
3.4. Odbiór dokumentacji powykonawczej oraz odbiór końcowy

II. CZĘŚĆ INFORMACYJNA PROGRAMU FUNKCJONALNO-UŻYTKOWEGO

1. Oświadczenie zamawiającego stwierdzające jego prawo do dysponowania nieruchomością na cele budowlane
2. Przepisy prawne i normy związane z projektowaniem i wykonaniem zamierzenia budowlanego
3. Inne posiadane informacje i dokumenty niezbędne do zaprojektowania robót budowlanych
4. Zalecenia konserwatorskie konserwatora zabytków
5. Porozumienia, zgody lub pozwolenia związane z realizacją inwestycji
6. Dodatkowe wytyczne inwestorskie i uwarunkowania związane z budową i jej przeprowadzeniem

III. ZAŁĄCZNIKI PROGRAMU FUNKCJONALNO-UŻYTKOWEGO

Rysunek 1.0. Mapa i przebiegu relacji kablowych wg typu kanalizacji
Rysunek 2.0 Wstępny schemat rozpływu kabli optycznych
Rysunek 3.0. Model atomowy połączeń międzywęzłowych sieci miejskiej
Rysunek 4.0 Rzut piętra planowanej serwerowni

Załącznik A. Lista wszystkich punktów węzłowych sieci miejskiej
Załącznik B. Zestawienie szacowanych długości relacji kablowych
Załącznik C. Zestawienie ilościowe materiałów i urządzeń

I. Cześć opisowa programu funkcjonalno-użytkowego

1.1. Podstawa opracowania

Wykonawca opracował niniejszą dokumentację na podstawie sumy własnych doświadczeń zebranych podczas innych inwestycji miejskich, inwentaryzacji w terenie, danych ankietowych zebranych na etapie przygotowawczym, wiadomości i uzgodnień branżowych oraz informacji uzyskanych od poszczególnych jednostek miejskich, a także w oparciu o aktualne normy i przepisy.

Wykonawca oświadcza, że dostarczone opracowanie jest kompletne oraz zgodne z wyżej wymienioną umową, obowiązującymi przepisami i aktami normatywnymi.

- Zlecenie Gminy Żywiec na podstawie umowy
- Wizje lokalne i informacje ankietowe pozyskane w trakcie prac koncepcyjnych
- Informacje uzyskane od odpowiednich jednostek administracji publicznej
- Uzgodnione z Zamawiającym oraz uprawnionymi pracownikami Miejskiego Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. - przebiegi tras kabli światłowodowych zawarte na Mapie przebiegu tras (rys.1 z załącznika)
- Normy branżowe i standardy telekomunikacyjne

Zadanie opisywane w niniejszym dokumencie realizowane jest w ramach zadania inwestycyjnego p.t. „Budowa żywieckiej światłowodowej sieci szerokopasmowej”.

1.2. Opis ogólny przedmiotu zamówienia

Przedmiotem zamówienia jest: zaprojektowanie infrastruktury i budowa sieci szerokopasmowej w mieście Żywiec wraz z niezbędnym okablowaniem światłowodowym, urządzeniami aktywnymi i radiowymi, infrastrukturą węzłów sieci, wdrożeniem systemów bezpiecznej transmisji danych w standardzie Ethernet oraz wdrożeniem systemów zarządzania i monitoringu sieci miejskiej.

W zakres zadania objętego zamówieniem wchodzić będą prace projektowe, prace budowlane związane z budowa kanalizacji teletechnicznej przyłączy i niezbędnych studni kablowych, prace wykonawcze przy układaniu kabli światłowodowych w kanalizacji sanitarnej i deszczowej oraz wszelkie prace wdrożeniowe związane z implementacja systemów sieciowych. Lista zadań cząstkowych obejmuje:

- wykonanie kompletnej dokumentacji projektowej wraz z uzyskaniem niezbędnych pozwoleń i dokumentów administracyjnych umożliwiających rozpoczęcie budowy zgodnie z wymogami prawa;
- wykonanie niezbędnej dokumentacji powykonawczej wszystkich elementów sieci;
- wybudowanie magistrali szkieletowej w postaci kabli światłowodowych do wybranych węzłów lokalnych LPD oraz przyłączy budynkowych do jednostek samorządu terytorialnego,
- wybudowanie kanalizacji łącznikowej relacji Straż Miejska – Urząd Miasta na podstawie istniejącego projektu budowlanego;
- rozbudowa lub modernizacja (zwielokrotnienie otworów wiązkami mikrorurek) istniejącej kanalizacji teletechnicznej będącej w zasobach Zamawiającego, możliwej do wykorzystania w projekcie;
- modernizacja i dostosowanie pomieszczeń przeznaczonych na węzły sieci;
- zaprojektowanie oraz wykonanie Centrum Zarządzania Siecią z dostosowaniem wskazanego przez Zamawiającego pomieszczenia oraz z wyposażeniem w niezbędną infrastrukturę;
- zaprojektowanie i wykonanie sieci światłowodowej poprzez instalację specjalnych kabli światłowodowych w teletechnicznej dostosowanych do stosowania w kanalizacji ściekowej wraz z wykonaniem niezbędnych miejsc rozdziału i zakończeń (mufy, przełącznice, szafki, itd.);
- zaprojektowanie i wdrożenie sieciowej warstwy aktywnej (przełączników) niezbędnej do utworzenia systemu bezpiecznej transmisji danych standardu Ethernet o strukturze warstwowej działającej z przepustowościami 10Gb/s w rdzeniu sieci oraz 10/100/1000Mb/s do poszczególnych jednostek wraz z zapewnieniem wymaganej redundancji łącz światłowodowych dla strategicznych węzłów sieci;

- zaprojektowanie i wdrożenie warstwy aktywnej (routery, firewalle, etc) niezbędnej do utworzenia wysokodostępnego, bezpiecznego, wydajnego, redundantnego punktu styku z siecią Internet wraz z niezbędną infrastrukturą;
- zaprojektowanie i wdrożenie sieci nowo wybudowanych Radiowych Punktów Dostępowych (Hotspotów) wykonywanych w wybranych lokalizacjach punktów węzłowych i abonenckich do dystrybucji publicznych usług elektronicznych e-Administracji oraz do dystrybucji ograniczonego dostępu szerokopasmowego do sieci Internet dla mieszkańców. Zadaniem Wykonawcy będzie również włączenie tych punktów do podsystemu punktów typu PIAP;
- wdrożenie systemów zarządzania i monitoringu parametrów zbudowanego systemu transmisji Ethernet wraz z zabudową niezbędnych platform serwerowych, urządzeń dedykowanych, terminali administratorów i infrastruktury towarzyszącej;

Wszystkie elementy i materiały niezbędne do budowy sieci szerokopasmowej dostarczy Wykonawca.

1.3. Charakterystyczne parametry określające wielkość przedsięwzięcia

Miejska Sieć Szerokopasmowa Żywiec [MSS Żywiec] to światłowodowa sieć metropolitalna budowana przy użyciu nowoczesnych technologii przez jednostki samorządu terytorialnego z nadrzędną rolą Urzędu Miasta. Sieć ta ma zapewnić otwarty dostęp do jej zasobów oraz zasobów Internetu i sieci ogólnokrajowych jednostkom samorządu terytorialnego pozostającego w gestii Beneficjenta z terenu objętego siecią.

Najważniejszym z warunków początkowych jest oparcie szkieletu sieci na budowanej **magistrali światłowodowej** uzupełnionej o pozostałą infrastrukturę pozwalającą na rozprowadzenie sieci światłowodowej w obrębie miasta. W skład tej infrastruktury wchodzić będą:

- Magistralne kable światłowodowe układane w kanalizacji deszczowej i sanitarnej udostępnionej przez MPWIK Sp z o.o. Żywiec
- Kanalizacja łącznikowa do wyprowadzenia kabli światłowodowych z kanalizacji deszczowej i sanitarnej
- Przyobiektowe studnie SK-2, SKR-1, SKR-2, z tworzyw sztucznych lub opcjonalnie – słupki dystrybucyjne
- Pomieszczenia i wyposażenie węzłów (Głównych Punktów Dystrybucji, Punktów Agregacji, Lokalnych Punktów Dostępowych, Punktów Abonenckich, Radiowych Punktów Dostępowych, etc.)

Topologia Miejskiej Sieci Szerokopasmowej Żywiec powinna przewidywać występowanie jedynie warstwy szkieletowej (magistralnej) i warstwy dystrybucyjnej. Warstwa dostępowa (ostatnia mila światłowodowa) nie będzie budowana w ramach projektu.

Poszczególne warstwy stykać się będą ze sobą w punktach węzłowych, umożliwiających konfiguracje sieci w myśl projektu oraz rekonfiguracje uwzględniająca aktualne zapotrzebowanie. Wytyczne projektowe dla poszczególnych zagadnień zamieszczono w dalszej części dokumentu.

Wstępną lista punktów do podłączenia obejmuje **33 punktów o** różnym charakterze ulokowanych w 22 obiektach samorządowych, łączących często kilka funkcji sieciowych, a ich wykaz znajduje się w aneksie A. Do wykonania połączeń między poszczególnymi węzłami sieci **przewiduje się ułożenie wzmacnianych kabli światłowodowych typu SWAA** w kanalizacji deszczowej i sanitarnej o pojemności zależnej od miejsca w strukturze sieci. Projektowana sieć, przepustowość i pojemność traktów kanalizacji i technologie użyte do budowy sieci powinny umożliwić łatwy dostęp dla innych Użytkowników pragnących skorzystać z zasobów sieci w przyszłości.

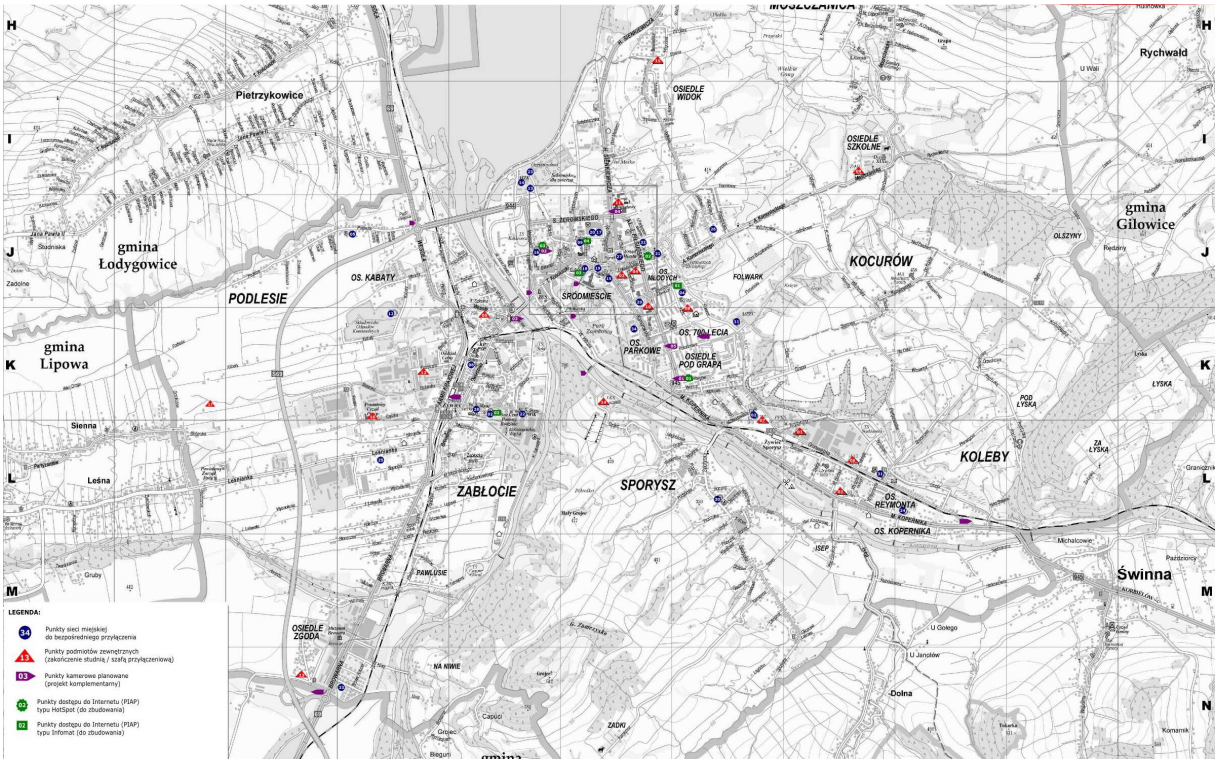
Wśród punktów sieciowych do wykonania znajdzie się:

- 10 punktów stanowiących samodzielne punkty końcowe (Punkty Abonenckie PA),
- 7 punktów abonenckich PA pełniących również łączoną rolę pasywnych punktów węzłowych (Lokalnych Punktów Dostępowych LPD) oraz 2 punkty LPD bez podłączenia punktu abonenckiego,
- 1 Główny Punkt Dystrybucji posiadający zintegrowane dodatkowe funkcje Centrum Zarządzania Siecią (CZS) i Centralnego Punktu Styku z Internetem (IXC) ulokowany w Urzędzie Miasta Żywiec
- 2 radiowe punkty dostępowe (HotSPOT) ulokowanych na obiektach sieciowych realizujących już inne funkcje w sieci miejskiej, 2 radiowe punkty dostępowe (HotSPOT) ulokowane na niezależnych obiektach

Z uwagi na integrację niektórych funkcji węzłów przewiduje się **wykorzystanie 22 obiektów** należących do jednostek publicznych pełniących role punktów węzłowych sieci o różnym znaczeniu dla budowanej sieci (węzły końcowe, główne, agregujące, etc) a ich wykaz wraz z przyjętą numeracją znajduje się w załączniku A. Do obiektów tych będzie trzeba przewidzieć doprowadzenie kanalizacji teletechnicznej przyłącza obiektowego i kabli o pojemności odpowiedniej do łącznego charakteru węzła sieci.

Do pozostałych obiektów zarządzanych przez inne podmioty niż Beneficjent, które nie zostaną włączone do sieci w I etapie budowy przewidzieć należy możliwość ich dołączenia poprzez realizacje odrębnych projektów komplementarnych. Należy przewidzieć możliwość wykonania przyłączy do najbliższej studzienki przyobiektowej (bez projektu i budowy przyłącza do tych obiektów).

Lokalizację jednostek samorządowych zaznaczono na dołączonej mapie (rys.1) wraz z przyjętą numeracją punktów i zaznaczeniem charakteru węzła. Na wspominanej mapie zaznaczono również pozostałe charakterystyczne punkty ważne z punktu widzenia sieci miejskiej.



Rysunek 1. Mapa lokalizacji punktów sieci miejskiej w Żywcu

Na etapie prac koncepcyjnych zaproponowano przebieg tras kabli światłowodowych wykorzystujących udostępnioną przez MWPIK Żywiec kanalizację deszczową i sanitarną wraz z określeniem pojemności kabli. Proponowane przebiegi trasowe pokazują jedynie trasy optymalne i mogą różnić się od ostatecznie zaprojektowanych z tolerancja wynikająca z istniejących przeszkód projektowych lub wykonawczych.

Łączna długość tras kabli światłowodowych magistralnych przewidzianych do wykonania przez Wykonawcę wynosi **16,05 km**. Długości szacunkowe, które podano powyżej nie określają dokładnie zakresu zadania a do podanej długości kabli magistralnych należy doliczyć jeszcze przyłącza obiektowe do 22 obiektów o długości **rzędu 2,5-3km**. Długości faktyczne kabli wyliczy Wykonawca po wykonaniu projektów wykonawczych. Na etapie przygotowania projektu może się okazać, że przebieg musi być inny od proponowanego ze względów technicznych.

Przewidziane jest również zmodernizowanie wydzielonego **Centrum Zarządzania Siecią,** w którym znajdzie się infrastruktura teletechniczna i pomieszczenia administratorów sieci.

W oparciu o wybudowaną kanalizacje teletechniczną, połączenia radiowe, punkty węzłowe oraz niezbędną infrastrukturę sieć ta ma zapewnić szerokopasmowy, bezpieczny dostęp do Internetu dla mieszkańców miasta. Dostęp do Internetu realizowany będzie poprzez punkty PIAP. Ograniczony dostęp do Internetu oraz nieograniczony do elektronicznych usług administracji publicznej zrealizowany zostanie poprzez wybudowanie **4 nowych Radiowych Punktów Dostępowych (HotSpot)** gwarantujące dostęp do Internetu z ograniczeniem pasma i czasu przyłączenia jednego użytkownika. Stacje radiowe działać będą w paśmie nielicencjonowanym 2,4Ghz z mocą do 100mW zgodnie ze standardem WiFi. Poszczególne stacje zostaną dołączone do podsystemu sieciowego łączącego punkty PIAP miasta w celu zunifikowania treści i zarządzania punktami dostępu.

Projektowana struktura ma również ułatwiać integracje struktur telekomunikacyjnych miasta, pozostałych jednostek samorządu terytorialnego i miejskich spółek komunalnych oraz być podstawą do rozwoju miejskich systemów monitoringu wizyjnego oraz innych systemów umożliwiających racjonalne i nowoczesne zarządzanie infrastrukturą miejską. Wybudowaną sieć metropolitalną poprzez punkty styku z operatorami krajowymi powinno być łatwo zintegrować z planowanymi systemami ogólnokrajowymi. Projekt ma być również komplementarny do działań prowadzonych w województwie śląskim nad wybudowaniem Śląskiej Sieci Szerokopasmowej, która ma dotrzeć również do Żywca.

1.4. Aktualne uwarunkowania wykonania przedmiotu zamówienia

Zadanie powinno być realizowane przez Wykonawcę z uwzględnieniem wymogów prawa budowlanego i zgodnie z zasadami sztuki inżynierskiej. Wykaz norm i standardów, które należy spełnić zawarto w dalszej części dokumentu.

Podawane w dokumentacji i w niniejszym dokumencie długości trasowe oraz ilości poszczególnych elementów potrzebnych do realizacji zadania są wielkościami przybliżonymi i nie mogą być przedmiotem zamówienia. Przedmiotem zamówienia jest wybudowanie światłowodowego połączeń światłowodowych do określonych lokalizacji. Wykonawca musi wybudować taką długość kanalizacji i kabla światłowodowego, aby podłączyć wszystkie lokalizacje i wykonać całe zadanie. Nie będzie rozliczany z długości kanalizacji, ani z długości kabli. Podobne wymagania dotyczą pozostałych systemów i warstwy aktywnej sieci.

1.4.1. Równoważność rozwiązań technicznych

Rozwiązania przyjęte w dokumentacji przetargowej i koncepcyjnej zostały dobrane w oparciu o rozwiązania i systemy dostępne na rynku podczas prac koncepcyjnych po analizie dostępnych rozwiązań uznano je za optymalne do spełnienia wymagań jakościowych i funkcjonalnych Zamawiającego. Wskazanie w dokumentacji projektu nazwy handlowej lub marki wraz z ich rozwiązaniami technicznymi, certyfikatami i deklaracjami należy rozumieć jako określenie standardu spełniającego w sposób optymalny oczekiwania w stosunku do systemu. Wskazane marki i eksploatacyjne cechy techniczne lub nazwy handlowe, certyfikaty i deklaracje określają wymaganą klasę produktu, a nie jego producenta. Dopuszcza się rozwiązania równoważne, za pisemną zgodą Zamawiającego, pod warunkiem, że są one co najmniej równorzędne konstrukcyjnie, funkcjonalnie i technicznie w stosunku do opisanych w dokumentacji projektowej oraz posiadają parametry nie gorsze niż określone przez Projektanta. Zaoferowane przez Wykonawcę urządzenia równoważne nie mogą jednak zmienić założeń technologicznych. Do obowiązków Wykonawcy należeć będzie przedstawienie pełnej dokumentacji technicznej i kompletnych zestawień porównawczych ułatwiających Projektantowi dokonanie oceny rozwiązań równoważnych. W szczególności w/w dokumentacja techniczna powinna stanowić załączniki oferty w postępowaniu przetargowym.

1.4.2. Standaryzacja użytych rozwiązań i wymagania związane z trwałością

Wszystkie elementy składające się na system okablowania światłowodowego muszą być certyfikowane przez tego samego producenta okablowania i pochodzić z jednolitej oferty reprezentującej kompletny system w takim zakresie, aby zostały spełnione warunki niezbędne do uzyskania bezpłatnego certyfikatu gwarancyjnego systemu okablowania światłowodowego.

Z uwagi na wymagania Zamawiającego w odniesieniu do trwałości projektów infrastrukturalnych całość rozwiązania światłowodowego ma być objęta jednolitą, spójną 5-letnią gwarancją systemową Producenta, obejmującą całą część kablową systemu (kable i elementy okablowania światłowodowego liniowego oraz stacyjnego: przełącznice, adaptery, pigtaile i patchcordy, osłony złączowe, stelaże zapasu kabli, etc). Gwarancja ma być udzielona przez Producenta bezpośrednio Zamawiającemu.

Udzielona Gwarancja ma obejmować tzw. gwarancję systemową: Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź 5-letniej eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione. W celu uzyskania tego rodzaju gwarancji cały system w tym okablowanie światłowodowe musi być zaprojektowane przez projektanta z odpowiednim przeszkoleniem (ukończone kursy projektowe odpowiedniego poziomu) oraz zainstalowany przez firmę instalacyjną posiadającą odpowiedni status uprawniający do udzielenia gwarancji producenta oraz dysponującą zasobami maszynowymi i narzędzi dedykowanych do instalacji elementów systemu kablowego.

Wniosek o udzielenie gwarancji składany przez firmę instalacyjną do Producenta ma zawierać: listę zainstalowanych elementów systemu zakupionych w autoryzowanej sieci sprzedaży w Polsce, imienną listę instalatorów (ukończony kurs instalatora systemu), listę maszyn i narzędzi użytych do prac instalacyjnych w zakresie instalacji elementów w kanalizacji ściekowej i deszczowej, wyciąg z dokumentacji powykonawczej podpisanej przez uprawnionego projektanta (ukończony kurs projektanta systemu) oraz protokół z audytu gwarancyjnego przeprowadzonego przez uprawnionego przedstawiciela Producenta systemu światłowodowego.

1.4.3. Nadzór nad realizacją i właściwą jakością materiałów używanych przez Wykonawcę

Zamawiający dopuszcza możliwość wykorzystania dodatkowych organów kontroli inwestorskiej w postaci nadzoru inspektora nadzoru, specjalnie powołanego Inżyniera Kontraktu lub innych, które uzna za stosowne. Wykonawca prac budowlanych w dowolnym momencie tych prac na żądanie Zamawiającego musi również okazać wszelkie dokumenty i certyfikaty, a także dostarczyć na własny koszt próbki użytych lub planowanych do użycia materiałów przeznaczonych do wykorzystania w trakcie inwestycji.

Szczegółowe wymagania Zamawiającego opisujące przedmiot Zamówienia znajdują się w dalszej części niniejszego dokumentu. Odstępstwa od zapisów dokumentacji Zamawiającego powinny uzyskać jego pisemną akceptację, po audycie proponowanych zmian przez firmę sprawującą nadzór autorski. Zamawiający zastrzega sobie prawo do poddania w dowolnym momencie ocenie dokumentacji projektowej na zgodność z przepisami prawa budowlanego oraz na zgodność w wymaganiami Zamawiającego określonymi w w/w dokumentach.

W szczególnych przypadkach Zamawiający zastrzega sobie prawo do częściowego audytu gwarancyjnego dokumentacji, projektów i prac budowlanych - przeprowadzanego w dowolnym momencie przez uprawnionego przedstawiciela Producenta w celu dokonania oceny prawidłowości użytych materiałów oraz jakości wykonywanych prac i ich zgodność z przyjętymi standardami.

W celu zapewnienia odpowiedniej jakości używanych materiałów i prac wykonawczych Zamawiający przewiduje wykorzystanie procedur testowania. W związku z tym, Zamawiający zastrzega sobie możliwość przeprowadzenia audytów i testów na różnych etapach wdrożenia, w obecności pracowników Zamawiającego i przedstawiciela Inżyniera Kontraktu. W szczególności Wykonawca musi zapewnić w ramach wynagrodzenia możliwość przeprowadzenia dla materiałów planowanych do wykorzystania podczas prac budowlanych — następujących testów:

a) Testy i badania fabryczne (Factory Acceptance Test - FAT)
Dla dowolnej z partii rur kablowych i kabli światłowodowych wymaga się zapewnienia możliwości przeprowadzenia, w obecności pracownika lub przedstawiciela Zamawiającego testów fabrycznych elementów systemu przed wysłaniem ich do Zamawiającego.

b) Testy i badania odbiorowe (Site Acceptance Test -SAT)
Dla wybudowanej kanalizacji teletechnicznej i dla innych kluczowych elementów systemu światłowodowego wymaga się zapewnienia możliwości przeprowadzenia, w obecności pracownika lub przedstawiciela Zamawiającego, standardowych testów odbiorowych elementów systemu wg harmonogramu prac i wymagań odbiorowych Zamawiającego. Nieobecność przedstawicieli Zamawiającego nie zwalnia Wykonawcy z obowiązku prowadzenia własnych badań odbiorowych, potwierdzanych w protokołach odbioru zamieszczanych, jako załączniki dokumentacji powykonawczej, zgodnie z wymaganiami odbiorowymi Zamawiającego. W szczególności Zamawiający wymaga wykonania minimum 4 audytów typu SAT z udziałem przedstawicieli Producenta systemu udzielającego gwarancji systemowej (20%, 50%, 90% stanu prac i odbiorowy).

Wszelkie koszty związane z wykonaniem testów FAT i SAT, a także z wizytą przedstawicieli Zamawiającego u Producenta systemu pokrywane są przez Wykonawcę. Na życzenie Zamawiającego Wykonawca musi udostępnić próbki materiałów planowanych do użycia w projekcie do zbadania przez Zamawiającego lub służby Inżyniera Kontraktu.

1.4.4. Wykorzystanie zasobów własnych Zamawiającego

Zakłada się możliwość jak największego wykorzystania posiadanego zasobu teletechnicznego będącego w gestii Urzędu Miasta, a w szczególności wykorzystanie i integracje wybudowanej do tej pory kanalizacji teletechnicznej w postaci pustych rur RHDPE oraz rur prefabrykowanych mikrokanalizacji.

Pod uwagę bierze się również współpracę z Miejskim Przedsiębiorstwem Wodociągów i Kanalizacji Sp. z o.o w zakresie układania kabli światłowodowych w istniejącej kanalizacji deszczowej i sanitarnej pozostającej w gestii tej spółki. Kwestie wymiany zasobów reguluje dokument Porozumienia wraz z wytycznymi technicznymi.

Zadaniem projektanta będzie **wykorzystanie** w projekcie zasobów istniejących Inwestora, zinwentaryzowanych podczas prac koncepcyjnych oraz **zinwentaryzowanie bieżącego stanu infrastruktury** telekomunikacyjnej należącej do miasta (z uwagi na planowane nowe inwestycje wykraczające poza termin zakończenia prac koncepcyjnych).

Z przeprowadzonej analizy informacji przesłanych przez poszczególne podmioty miejskie, jednostki samorządowe oraz ze spółek infrastrukturalnych wynika, iż administracja publiczna i instytucje publiczne korzystają w ograniczonym stopniu z szerokopasmowych technologii społeczeństwa informacyjnego. Istniejąca infrastruktura sieciowa będąca w posiadaniu Inwestora jest oparta na systemie radiowym z 1 stacją bazową i kilkunastoma stacjami końcowymi i służy do przesyłu sygnałów pomiędzy jednostkami samorządu terytorialnego. W technologii radiowej w pasmach nielicencjonowanych działa również kilka radiowych punktów dostępowych (hotspotów) w miejscach publicznych. Zauważalnym minusem technologii radiowej stało się ograniczenie dostępnej przepustowości łącz radiowych, które w przyszłości nie pozwoliłoby na rozwój szerokopasmowych usług elektronicznych planowanych do wdrożenia przez Urząd Miasta.

Podczas prac projektowych przeprowadzonych na etapie tworzenia koncepcji budowy sieci doziemnej kanalizacji teletechnicznej napotkano na szereg problemów z pozyskaniem zgód właścicieli terenów przez które przechodzić miały trasy planowanej kanalizacji teletechnicznej. Na problemy projektowe miał wpływ również zabytkowy charakter śródmieścia Żywca o charakterystycznych brukowanych ulicach z bardzo wąskimi chodnikami lub ich brakiem. Spowodowało to konieczność poszukania innego medium dla kabli światłowodowych.

Zamawiający informuje, iż do tej pory przeprowadzono i zrealizowano tylko 2 zadania związane z telekomunikacją realizując budowę kanalizacji teletechnicznej. Były to zadania: „Budowa odcinka teletechnicznej kanalizacji kablowej i kabli światłowodowych dla potrzeb monitoringu oraz transmisji danych na terenie miasta Żywiec w relacji budynek Urzędu Miejskiego – MZEC „EKOTERM” przy ul. Folwark w Żywcu - wraz z montażem stalowego kontenera technicznego” oraz „Budowa teletechnicznej kanalizacji kablowej i kabli światłowodowych relacji Urząd Miejski – Park Zamkowy – Straż Miejska dla potrzeb monitoringu i transmisji danych na terenie miasta Żywca”. Urząd Miasta jest inwestorem w zakończonym postępowaniu przetargowym na wybudowanie połączenia Ekoterm Sp. z o.o. z Urzędem Miasta długości ok. 1,8 km jednakże kabel ten wykorzystywany będzie do odrębnych celów pozostałych systemów teleinformatycznych i na potrzeby systemu monitoringu CCTV. Do dyspozycji pozostają wolne otwory rury prefabrykowanej mikrokanalizacji zbudowanej na tej relacji.

Przed przystąpieniem do prac projektowych należy przeprowadzić **weryfikację stanu istniejącej** infrastruktury teletechnicznej. W ramach oceny, należy skupić się w głównej mierze na istniejących rurach przeznaczonych dla okablowania światłowodowego, wymienionych poniżej oraz wybudowanych po dacie zamknięcia prac koncepcyjnych. Należy sprawdzić stan oraz drożność ułożonych rur RHDPE40 i ocenić możliwość prowadzenia w nich okablowania światłowodowego oraz wiązek mikrokanalizacji.

Pozostałymi zasobami możliwymi do wykorzystania są przestrzenie na pomieszczenia teletechniczne w budynkach użyteczności publicznej jednostek samorządowych oraz spółek infrastrukturalnych. Miejsca te były wybierane pod kątem wymagań dla lokalizacji poszczególnych punktów sieci oraz możliwości ich wykorzystania na podstawie uzgodnień z właścicielami pomieszczeń oraz wizji lokalnych.

Wstępne propozycje lokalizacji punktów węzłowych oraz miejsca montażu infrastruktury sieciowej zawiera załącznik A. Informacje te muszą **zostać zweryfikowane** przez projektanta w ramach uzgodnienia z jednostką administrującą pomieszczeniem w celu dostosowania do stanu faktycznego na dzień wykonania projektu budowlanego i wykonawczego. Zalecane jest dokonanie wizji lokalnej w proponowanych obiektach przez Wykonawców.

1.4.5. Uwarunkowania związane z trybem postępowania przetargowego

Inwestycja zostanie przeprowadzona w trybie „zaprojektuj i wybuduj” i z uwagi na długi okres jej trwania Zamawiający przewiduje podzielenie prac na etapy zgodne z przyjętym w koncepcji harmonogramem i planem wydatków (budżetem) miasta. Zamawiający informuje, że przewiduje zapłaty częściowe dla Wykonawcy za odebrane i zakończone etapy wg harmonogramu prac, który zostanie przedstawiony przez Wykonawcę po zakończeniu prac projektowych. Harmonogram prac musi być zgodny z planem wydatków miasta.

Całość zadania zgodnie z wytycznymi unijnymi powinna zakończyć się nie dłużej **niż do 30 czerwca 2014r**. Przewidywany harmonogram prac zamieszczono **jako załącznik B** niniejszego dokumentu.

1.4.6. Uwarunkowania związane z dofinansowaniem projektu ze środków unijnych

Z uwagi na starania Zamawiającego o objęcie projektu dofinansowaniem ze środków Regionalnego Programu Operacyjnego Województwa Śląskiego (w ramach Działania 2.1. Infrastruktura społeczeństwa informacyjnego), Wykonawca musi uwzględnić w pracach projektowych aktualne, specyficzne wymagania związane z charakterem projektów związanych z budową Społeczeństwa Informacyjnego.

Zamawiający informuję, że na dzień ogłoszenia postępowania przetargowego aktualny zapis tych wymagań został uwzględniony w dokumentacji koncepcyjnej sporządzonej na potrzeby projektu i ujęty w niniejszym programie funkcjonalno-użytkowym. Dokumentami nadrzędnymi w odniesieniu do wymagań związanych z wytycznymi Regionalnego Programu Operacyjnego Województwa Śląskiego dla projektów budowanych w ramach w/w Działania 2.1 – są jednak dokumenty pozostające w gestii przez Zarząd Województwa Śląskiego. Zadaniem Wykonawcy będzie zachowanie zgodności z aktualną wersją wytycznych zawartych w tych dokumentach.

Zgodnie z wymaganiami projektów dotowanych wszystkie elementy dostarczone w ramach projektu muszą posiadać trwałe oznaczenie informujące o objęciu wykonanych elementów dofinansowaniem. Zadaniem oznakowania elementów obarczony jest Wykonawca, wzór oznakowania Zamawiający zdefiniuje Wykonawcy przed rozpoczęciem prac.

Z uwagi na rozdział wydatków znajdujących się w projekcie na część kwalifikowaną i niekwalifikowalną Zamawiający informuję, iż będzie żądał od Wykonawcy rozdzielania zadań objętych kwalifikowalnością i niezależnego ich rozliczania. Szczegółowe wytyczne zostaną przedstawione w Specyfikacji Istotnych Warunków Zamówienia lub zostaną uzgodnione po wyłonieniu Wykonawcy.

Z uwagi na planowane wdrożenie przez Zamawiającego sieci Radiowych Punktów Dostępu do Internetu typu HotSpot oraz istotne ograniczenia nakładane na projekty tego typu przez Urząd Komunikacji Elektronicznej oraz regulacje unijne, wymaga się aby Wykonawca części projektowej i wykonawczej uwzględnił i dostosował projekt do najbardziej aktualnych wymagań prezentowanych w dokumentach i komunikatach UKE (zob. „Stanowisko Prezesa UKE w sprawie świadczenia bezpłatnej lub za cenę niższą niż cena rynkowa usługi dostępu do sieci Internet przez jednostki samorządu terytorialnego”). Zamawiający informuje, iż wystąpi o stosowne ostateczne decyzje do UKE na własny koszt w trybie przewidzianym w postanowieniach Ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (wraz z późniejszymi zmianami), jednakże obowiązkiem Wykonawcy jest zapewnienie maksymalnej zgodności z aktualnymi wytycznymi, nawet jeśli wiązałoby to się ze zmianami w projekcie na dowolnym etapie wykonania.

1.4.7. Uwarunkowania związane z oczekiwaną gwarancją i serwisem gwarancyjnym świadczonym przez Wykonawcę

1.4.7.1. Definicja pojęć podstawowych

Celem opisania warunków świadczenia usług serwisowych definiuje się następujące pojęcia:

- **USTERKA** – zdarzenie, w którym uszkodzeniu uległ jeden (lub więcej) element przedmiotu zamówienia, nie wpływając na funkcjonalność i wydajność przedmiotu zamówienia, ale niezgodny ze stanem określonym w Umowie (np. uszkodzenie jednego z elementów redundantnych).
- **AWARIA** – zdarzenie, w którym uszkodzeniu uległ jeden (lub więcej) element przedmiotu zamówienia, ograniczające wydajność i funkcjonalność przedmiotu zamówienia i uniemożliwiające Zamawiającemu korzystanie z przedmiotu zamówienia zgodnie z jego SIWZ / Instrukcją użytkowania.
- **AWARIA NIEKRYTYCZNA** – Awaria, która negatywnie wpływa na wydajność i funkcjonalność przedmiotu zamówienia nie obejmująca węzłów rdzeniowych, punktów agregacji lub obejmująca mniej niż 6 węzłów końcowych sieci.

- **AWARIA KRYTYCZNA** – Awaria, która uniemożliwia Zamawiającemu korzystanie z przedmiotu zamówienia dotycząca węzłów rdzeniowych, punktów agregacji lub obejmująca więcej niż 5 węzłów końcowych sieci.
- **ZGŁOSZENIE AWARII LUB USTERKI** – ciąg działań ze strony Zamawiającego mający na celu powiadomienie Serwisu Wykonawcy o zaistniałej Awarii lub Usterce, wykonany zgodnie z warunkami gwarancji.
- **DOSTĘPNOŚĆ SERWISU** – dni i godziny, w jakich Serwis Wykonawcy przyjmuje Zgłoszenia Awarii i Usterek nadsyłane przez upoważnionych pracowników Zamawiającego oraz realizuje czynności serwisowe.
- **REAKCJA SERWISU** – nawiązanie kontaktu przez przedstawiciela Serwisu Wykonawcy ze zgłaszającym Awarię i/lub Usterkę przedstawicielem Zamawiającego w celu przeprowadzenia wstępnej diagnostyki i w miarę możliwości przekazania zaleceń. Kontakt może mieć formę bezpośrednią lub telefoniczną.
- **USUNIĘCIE AWARII LUB USTERKI** – przywrócenie funkcjonalności i wydajności elementu przedmiotu zamówienia, w którym wystąpiła Awaria lub Usterka do stanu, w jakim znajdowało się ono przed wystąpieniem Awarii lub Usterki. W razie braku możliwości naprawy uszkodzonych urządzeń, dopuszcza się podstawienie przez Wykonawcę, Urządzenia Zastępczego do czasu ostatecznej naprawy uszkodzonego urządzenia.
- **CZAS REAKCJI SERWISU** – maksymalny czas, jaki może upłynąć pomiędzy pierwszym Zgłoszeniem Awarii lub Usterki a Reakcją Serwisu Wykonawcy.
- **CZAS USUNIĘCIA USTERKI LUB AWARII** – czas, jaki może upłynąć pomiędzy pierwszym Zgłoszeniem Usterki lub Awarii a jej usunięciem. Czas Usunięcia Usterki lub Awarii liczony jest w okresie Dostępności Serwisu Wykonawcy.
- **URZĄDZENIE ZASTĘPCZE** – urządzenia lub podzespoły, które Wykonawca udostępnia w ramach gwarancji Zamawiającemu, jeżeli nie jest możliwe w ustalonym czasie Usunięcie Usterki lub Awarii w drodze naprawy uszkodzonych urządzeń lub podzespołów. Urządzenie Zastępcze musi mieć parametry takie same lub lepsze jak urządzenie, które uległo awarii.
- **ROZWIĄZANIE ZASTĘPCZE** - rozwiązanie pozwalające na użytkowanie przedmiotu zamówienia bez ograniczenia co funkcjonalności i wydajności, do czasu pełnego Usunięcia Usterki lub Awarii.
- **DNI ROBOCZE** – przez dni robocze rozumie się dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.
- **GODZINY ROBOCZE** – przez godziny robocze rozumie się godziny od 7:30 do 15:30 w Dni Robocze.

1.4.7.2. Ogólne wymagania dla warunków gwarancji

Głównym zadaniem Wykonawcy związanym z obowiązkami gwarancyjnymi będzie zapewnienie prawidłowego (nie ograniczone czasowo i funkcjonalnie) działania przedmiotu zamówienia, a także udzielenie Zamawiającemu wsparcia serwisowego poprzez telefoniczne wsparcie techniczne umożliwiające zgłaszanie usterek i awarii w godzinach roboczych. Wykonawca zapewni także autoryzowany serwis producenta dla urządzeń dostarczonych w ramach przedmiotu zamówienia, a w przypadku wystąpienia 3 awarii podlegających gwarancji, licząc awarie dla każdego urządzenia z osobna, wymieni dane urządzenie na nowe.

1. Wykonawca udzieli gwarancji na wykonane przez siebie prace i dostarczone elementy na okres minimum **60 miesięcy**.
2. Poszczególne elementy i podsystemy wobec których Zamawiający wymaga krótszych okresów gwarancyjnych posiadają wymagania specyficzne ujęte w opisie wymagań poszczególnych systemów i urządzeń.
3. Dla systemu okablowania światłowodowego Wykonawca na własny koszt pozyska także rozszerzoną gwarancję materiałową gwarantowaną przez jego Producenta i wynoszącą **minimum 60 miesięcy.**
4. W ramach udzielonej gwarancji Wykonawca usunie wszelkie nieprawidłowości w zrealizowanym przedmiocie zamówienia.
5. Okres gwarancji rozpoczyna się od momentu podpisania protokołu odbioru końcowego przez Zamawiającego.
6. Wszelkie prace gwarancyjne nie wymagają jakichkolwiek dodatkowych opłat ze strony Zamawiającego, w szczególności kosztów dojazdu, delegacji, dostawy, podmiany urządzeń.
7. W ramach gwarancji Wykonawca zapewni serwis gwarancyjny w tym dostęp do aktualizacji oprogramowania dla dostarczonych urządzeń i oprogramowania zarządzającego. Wszystkie koszty gwarancji wraz z serwisem gwarancyjnym są włączone do ceny ofertowej.
8. Czas na usunięcie awarii liczy się od momentu zgłoszenia awarii lub usterki Wykonawcy w formie pisemnej (dopuszcza się także faksem, e-mailem wraz z potwierdzeniem telefonicznym otrzymania).
9. Zamawiający może dochodzić roszczeń z tytułu gwarancji także po upływie terminu gwarancji, jeżeli zgłoszenie Awarii lub Usterek nastąpiło przed upływem tego terminu.
10. W przypadku, jeżeli Wykonawca nie usunie Awarii lub Usterki w terminie określonym przez Zamawiającego w Tabeli 3, to Zamawiający może zlecić usunięcie ich stronie trzeciej na koszt Wykonawcy. Koszty ich usuwania będą pokrywane w pierwszej kolejności z zatrzymanej kwoty będącej zabezpieczeniem należytego wykonania umowy.
11. W przypadku niemożności usunięcia Awarii lub Usterki w zadeklarowanym terminie Wykonawca może dostarczyć Rozwiązanie Zastępcze pozwalające na użytkowanie przedmiotu zamówienia. Odbiór uszkodzonego i dostawa sprawnego sprzętu odbywać się będzie w okresie gwarancji na koszt i ryzyko Wykonawcy.

12. W przypadku stwierdzenia, w okresie gwarancji, istnienia Awarii lub Usterek nie nadających się do usunięcia, Zamawiający może żądać wykonania przedmiotu umowy po raz drugi, zachowując prawo domagania się od Wykonawcy naprawienia szkody wynikłej z opóźnienia.
13. Wykonawca zobowiązuje się wobec Zamawiającego do spełnienia wszelkich roszczeń wynikłych z tytułu nienależytego wykonania przedmiotu umowy na podstawie obowiązujących przepisów Kodeksu Cywilnego.
14. Wymiana rzeczy wadliwej lub dokonanie istotnej naprawy przez Wykonawcę w ramach gwarancji powoduje rozpoczęcie na nowo biegu gwarancji dla danej rzeczy zgodnie z art. 581. § 1 Kodeksu Cywilnego.

1.4.7.3. Zobowiązania szczegółowe Wykonawcy w ramach gwarancji

1. Wykonawca poinformuje w formie pisemnego powiadomienia Zamawiającego w terminie 14 dni o zmianie siedziby lub firmy (nazwy) Wykonawcy, osób reprezentujących Wykonawcę, ogłoszeniu upadłości Wykonawcy, oraz zawieszeniu działalności Wykonawcy,
2. Wykonawca wykona naprawę przedmiotu zamówienia w siedzibie Zamawiającego, w przypadku konieczności zabrania urządzenia dostarczonego w ramach przedmiotu zamówienia zobowiązuje się do podstawienia, właściwego skonfigurowania i uruchomienia urządzenia zastępczego, które będzie mogło w pełni przejąć funkcje uszkodzonego urządzenia. Zamawiający dopuszcza, aby wymianę uszkodzonego urządzenia na sprawne dokonywał nieautoryzowany serwis Wykonawcy przy zachowaniu rygoru, że naprawy tych uszkodzonych urządzeń będzie dokonywał już autoryzowany serwis producenta (jeżeli taka wymiana nie jest sprzeczna z warunkami gwarancji producenta urządzenia),
3. Wykonawca wymieni / naprawi dostarczone w ramach postępowania urządzenia i kable światłowodowe,
4. Wykonawca naprawi / udrożni kanalizację techniczną wybudowaną w ramach przedmiotu zamówienia,
5. Wykonawca dokona wstępnej analizy rodzaju usterki lub awarii (gwarancyjna, niegwarancyjna),
6. Wykonawca naprawi / usunie awarie i usterki gwarancyjne.

Z uwagi na wymagania Zamawiającego w odniesieniu do trwałości projektów infrastrukturalnych całość rozwiązania światłowodowego ma zostać objęta jednolitą, spójną gwarancją systemową jego Producenta, obejmującą system mikrokanalizacji (mikrokable oraz mikrokanalizację z osprzętem połączeniowym) wraz z elementami okablowania światłowodowego liniowego oraz stacyjnego (przełącznice, adaptery, pigtaile i patchcordy, osłony złączowe, stelaże zapasu kabli i mikrokabli, etc). Udzielona Gwarancja ma obejmować tzw. gwarancję systemową: Producent zagwarantuje, że jeśli w jego produktach podczas dostawy, instalacji bądź eksploatacji wykryte zostaną wady lub usterki fabryczne, to produkty te zostaną naprawione bądź wymienione. Gwarancja ta ma zostać udzielona przez Producenta bezpośrednio Zamawiającemu. Okres gwarancji rozszerzonej na w/w system światłowodowy powinien wynosić **minimum 60 miesięcy** od daty odbioru końcowego.

Wykonawca na własny koszt pozyska stosowane uprawnienia gwarancyjne od Producenta zaoferowanego przez siebie systemu. Wykonawca na własny koszt spełni wszystkie wymagania Producenta systemu (w zakresie rodzaju dostarczanych materiałów, wymagań jakościowych na prowadzone prace wykonawcze, procedur odbiorowych i testowych, etc) w celu uzyskania tego rodzaju gwarancji rozszerzonej.

Zamawiający wyraża zgodę na uzupełnienie systemu warstwy aktywnej o urządzenia i oprogramowanie konieczne do ustanowienia zdalnego dostępu na potrzeby serwisu urządzeń przez Wykonawcę. Ewentualne dodatkowe koszty związane z ustanowieniem zdalnego dostępu muszą zostać uwzględnione w cenie oferty – dotyczy to tej części urządzeń i oprogramowania, które zostaną zainstalowane u Zamawiającego. Wymagania techniczne dotyczące zdalnego dostępu na potrzeby serwisu oprogramowania:

a) połączenie za pomocą VPN,
b) ograniczenie liczby adresów IP z jakich może być nawiązane połączenie zdalne,
c) możliwość ograniczenia czasowego nawiązywania połączeń zdalnych oraz blokowania zdalnego dostępu przez Zamawiającego.

Zamawiający dopuszcza użycie własnego przeszkolonego personelu do wymiany uszkodzonych urządzeń po dostarczeniu przez Wykonawcę urządzenia zastępczego (nie dotyczy awarii krytycznych). Wówczas czas reakcji serwisu Wykonawcy, liczy się od momentu zgłoszenia przez Zamawiającego awarii do czasu dostarczenia urządzenia zastępczego. Jeżeli podmiana urządzania nie usunie zgłoszonej awarii/ usterki czas reakcji serwisu Wykonawcy liczy się od czasu ponownego zgłoszenia awarii/usterki. Działania te nie mogą być powodem utraty gwarancji, ani podstawą do żadnych roszczeń finansowych, chyba że wymiana została wykonana niezgodnie z instrukcją dostarczoną przez Wykonawcę. Wymianie mogą podlegać jedynie całe urządzenia (urządzania aktywne, wymienne interfejsy sieciowe). Za utrzymywanie odpowiednich stanów magazynowych odpowiada Wykonawca.

Do usterek lub awarii gwarancyjnych Zamawiający zalicza:

1. wszystkie awarie elektroniki,
2. wszystkie awarie urządzeń z „wbudowanym oprogramowaniem” (urządzenia aktywne itp.),
3. awarie zasilaczy,
4. awarie mechaniczne wynikające z niewłaściwego montażu przez Wykonawcę, wad konstrukcyjnych i materiałowych.

Przez naprawę dla urządzenia Zamawiający rozumie:
1. naprawę urządzenia na miejscu lub
2. podmianę urządzenia na inne sprawne, działające w przedmiocie zamówienia i tożsame funkcjonalnie.

Do usterek lub awarii gwarancyjnych Zamawiający nie zalicza mechanicznych uszkodzeń (o ile nie wynikają z niewłaściwego montażu, wad konstrukcyjnych i materiałowych).

1.4.7.4. Oczekiwany czas realizacji postanowień gwarancyjnych

Wykonawca w ramach gwarancji na wykonane usługi i prace budowlane zapewni odpowiednio szybki poziom reakcji na zgłoszenie przez Zamawiającego zdarzenia wymagającego interwencji Wykonawcy. W szczególności Zamawiający oczekuje terminów reakcji służb Wykonawcy nie dłuższych niż określonych w poniższej tabeli.

Czas reakcji serwisu	**3 godziny robocze od momentu zgłoszenia awarii/usterki.**			
Czas naprawy od zgłoszenia awarii/usterki (w godzinach lub dniach roboczych):	Typ sprzętu	Awaria krytyczna	Awaria niekrytyczna	Usterka
	Kanalizacja teletechniczna	-	-	10 dni
	Urządzenia aktywne	1 dzień	3 dni	10 dni
	Kable światłowodowe	3 dni	5 dni	14 dni
	pozostałe urządzenia	5 dni	7 dni	14 dni

Tabela 3. Oczekiwany czas realizacji postanowień gwarancyjnych

Zapis „pozostałe urządzenia” dotyczy innych, nie wymienionych w tabeli urządzeń, dostarczonych przez Wykonawcę w ramach projektu.

1.5. Ogólne właściwości funkcjonalno-użytkowe

W technologicznym podejściu do projektu budowy sieci zakłada się możliwość jak największego wykorzystania posiadanego potencjału teletechnicznego będącego w gestii Urzędu Miasta i spółek infrastrukturalnych miasta Żywiec. W oparciu o teletechniczną istniejącą kanalizację sanitarna i deszczową, punkty węzłowe oraz niezbędną infrastrukturę zbudowana sieć ma zapewnić integracje struktur telekomunikacyjnych miasta, pozostałych jednostek samorządu terytorialnego oraz miejskich spółek komunalnych. Wybudowaną sieć metropolitalną poprzez punkty styku z operatorami krajowymi łatwo będzie również zintegrować z planowanymi systemami ogólnokrajowymi.

Zakłada się zaprojektowanie Miejskiej Sieci Szerokopasmowej mającej na celu:
- lepsze wykorzystanie i współdziałanie systemów informatycznych placówek i jednostek położonych na terenie miasta Żywiec (przez połączenie budynków UM, szkół i placówek oświatowych, gminnych placówek kultury i filii bibliotek
- tworzenie wszelkiego rodzaju łączy transmisji danych wykorzystywanych dla potrzeb komunikacji, monitorowania, nadzoru i sterowania w oparciu o technologie przewodowe i bezprzewodowe,
- wspólny szerokopasmowy dostęp do sieci Internet,
- tworzenie bezpiecznych (niejawnych) wirtualnych sieci dla różnych instytucji,
- wewnętrzne połączenia głosowe i wideo w technologii IP.
- wykorzystanie sieci szerokopasmowej na cele systemów teleinformatycznych oraz telemetrycznych firm i spółek miejskich (ciepłownictwo, woda, kanalizacja, media, etc)
- wykorzystanie sieci szerokopasmowej na potrzeby transmisji sygnałów Monitoringu Miejskiego oraz na potrzeby ewentualnego Centrum Zarządzania Kryzysowego
- wykorzystanie sieci szerokopasmowej do dystrybucji systemów bazodanowych informacji przestrzennej (GIS i inne), również we współpracy z ewentualnymi projektami regionalnymi GIS,
- wdrażanie innego rodzaju usług ze szczególnym naciskiem na programy ponad regionalne.

Miejska Sieć Szerokopasmowa Żywiec ma na celu:
- zbudowanie infrastruktury szkieletowej wykorzystującej kable światłowodowe o odpowiedniej pojemności,

- wykonanie Publicznych Punktów Dostępu do Internetu (Public Internet Access Points),
- wykonanie Centrum Zarządzania Siecią
- wykonanie Operatorskich Punktów Styku z Internetem
- wykonanie Operatorskich Punktów Dostępowych
- umożliwienie podłączenia budynków administracji samorządowej i instytucji oświatowych
- umożliwienie późniejszego podłączenia punktów monitoringu miasta (kamery cyfrowe)

Połączenia te maja być realizowane poprzez wybudowanie infrastruktury teletechnicznej w postaci sieci szkieletowej w technologii światłowodowo o odpowiedniej pojemności. Projektowana sieć, przepustowość i pojemność traktów kanalizacji i technologie użyte do budowy sieci powinny umożliwić łatwy dostęp dla innych Użytkowników pragnących skorzystać z zasobów sieci w przyszłości (po zakończeniu okresu trwałości wymaganej charakterem dofinansowania projektu).

2. OGÓLNY OPIS WYMAGAŃ ZAMAWIAJĄCEGO W STOSUNKU DO PRZEDMIOTU ZAMÓWIENIA

2.1. Zadania Wykonawcy związane z wykonaniem prac projektowych

Na podstawie materiałów określających koncepcję budowy sieci, które będą realizowane w ramach zadania Wykonawca zobowiązany jest do zaprojektowania całości rozwiązań dla budowy sieci szerokopasmowej wraz z wykonaniem pełnozakresowej i pełnobranżowej dokumentacji projektowej zawierającej projekty budowlane i wykonawcze dla m.in. światłowodowej sieci kablowej, potrzebnej kanalizacji łącznikowej, instalacji radiowych i innych elementów wchodzących w zakres.

Do zadań Wykonawcy należy przygotowanie i opracowanie kompletnej dokumentacji projektowej zgodnie z wymogami ustawy Prawo Budowlane z dnia 7 lipca 1994 z późniejszymi zmianami. Dokumentacja ta musi umożliwić budowę kanalizacji teletechnicznej i linii światłowodowych zgodnie z obowiązującym Prawem Budowlanym oraz wymaganiami gestora kanalizacji ściekowej i deszczowej. Dokumentacja musi posiadać wszystkie potrzebne uzgodnienia i decyzje administracyjne. Opracowanie tej dokumentacji musi zostać wykonane w formie elektronicznej i papierowej.

Z uwagi na charakter projektu wykonywanego na zlecenie jednostki samorządu terytorialnego Zamawiający oczekuje, że wszelkie prace projektowe i uzgodnienia administracyjne będą także prowadzone zgodnie z zapisami Ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych z dnia 7 maja 2010r wraz z jej ewentualnymi aktualizacjami, które mogą się dokonać w trakcie trwania prac projektowych. Zadaniem Wykonawcy prac projektowych będzie również wskazanie Zamawiającemu ewentualnych powinności i formalności, które należy dopełnić w wyniku zapisów tej ustawy a bezpośrednio nie związanych z obowiązkami Wykonawcy wynikającymi z zakresu prac projektowych.

2.1.1. Zakres prac projektowych

Zakresem projektowania, jeśli nie zaznaczono inaczej - objęto wszystkie węzły sieci miejskiej wymienione w załączniku A. Łączna długość trasowa do zaprojektowania szacowana jest na 16,05 km magistral i tras dystrybucyjnych oraz przyłączy różnej długości do 22 obiektów sieciowych o śr. długości do 100-200m (łącznie blisko **19,0 km** tras)

W ramach prac projektowych do obowiązku Wykonawcy należy:

- weryfikacja istniejących zasobów kanalizacji teletechnicznej Inwestora oraz włączenie jej i uwzględnienie w projekcie sieci miejskiej.
- dokonanie wizji lokalnych i uzgodnień posadowienia infrastruktury technicznej węzłów sieci miejskiej w jednostkach samorządowych wg wykazu z Załącznika A. Propozycje lokalizacji pomieszczeń wraz z wstępnym miejscem posadowienia znaleźć można w ostatniej kolumnie tabeli w Załączniku A.
- weryfikacja istniejącego projektu budowlanego do zadania p.t. „Budowa teletechnicznej kanalizacji kablowej i kabli światłowodowych relacji Urząd Miejski - Park Zamkowy - Straż Miejska dla potrzeb monitoringu i transmisji danych na terenie miasta Żywiec” stanowiący załącznik F niniejszego dokumentu wraz z zintegrowaniem go w ramach bieżącej dokumentacji projektowej.
- wykonanie projektu wykonawczego i/lub budowlanego przebiegu tras kabli światłowodowych w oparciu o technologię układania kabli światłowodowych w istniejącej kanalizacji deszczowej i ściekowej wraz uzyskaniem pozwolenia i szczegółowych warunków technicznych z jednostki zarządzającej kanalizacją wodną na terenie gminy Żywiec (MPWIK Sp. z o.o. w Żywcu), wraz z uzyskaniem pozwolenia na budowę i ze wszystkimi uzgodnieniami i wymaganymi prawem decyzjami administracyjnymi (o ile okaże się potrzebne).
- wykonanie projektów szczegółowych dla rozwiązań technicznych przejść kablami światłowodowymi dla miejsc charakterystycznych sieci kanalizacji ściekowej i deszczowej tj. dla wszelkich obiektów technicznych (np. studzienek, komór przelewowych, kanalizacji przełazowej i nieprzełazowej, wejść do budynków, nawiązań między kanalizacją ściekową a deszczową, etc) wraz z uzyskaniem akceptacji Zamawiającego oraz służb technicznych MPWIK Sp. z o.o.
- uzyskania Decyzji lokalizacji inwestycji celu publicznego - jeśli będzie konieczne, w trybie administracyjnym zgodnym z aktualnymi przepisami oraz z w zgodzie z wymaganiami Megaustawy w zakresie decyzji o ustaleniu Lokalizacji Inwestycji Celu publicznego dla Regionalnych Sieci Szerokopasmowych,
- uzyskania Decyzji Środowiskowej i wykonania raportu oddziaływania na środowisko - jeśli będą konieczne

- uzyskania wypisów z rejestru gruntów oraz wykazu właścicieli gruntów,
- pozyskanie na rzecz Zamawiającego pozwoleń właścicieli poszczególnych nieruchomości wymaganej zgody (należy zawrzeć stosowne umowy z właścicielami gruntów, istniejącej infrastruktury kanalizacji deszczowej i sanitarnej, etc), koszt odszkodowań i zgód właścicieli po stronie Wykonawcy.
- opracowanie map do celów projektowych.
- zakup map do celów opiniodawczych i projektowych - jeśli będzie konieczne
- pokrycie opłat za uzgodnienia branżowe, opinie, ekspertyzy.
- pokrycie opłat za decyzje i pozwolenia administracyjne.
- pokrycie opłat i wykonanie czynności związanych z koniecznością zmiany decyzji o Lokalizacji Inwestycji Celu Publicznego - jeśli będzie konieczne,
- pokrycie wszystkich innych kosztów związanych z opracowaniem projektu
- uzgodnienie przebiegu tras w obiektach i lokalizacji przełącznic dla wszystkich lokalizacji węzłowych i końcowych.
- zaprojektowanie rozpływu kabli i włókien światłowodowych. Propozycja rozpływu włókien pomiędzy poszczególnymi punktami sieci została zaznaczona na Schemacie rozpływu włókien (rys.2).
- wykonanie niezbędnych projektów (jeśli będą wymagane prawem) modernizacji pomieszczeń węzłów sieci miejskiej wraz z infrastrukturą towarzyszącą (lokalizowanych w obiektach samorządu lub w obiektach, z którymi Zamawiający ma podpisane porozumienia upoważniające go do wykorzystania pomieszczeń na cele sieci miejskiej).
- wykonanie projektu modernizacji lub projektu budowlanego pomieszczenia przeznaczonego na Centrum Zarządzania Siecią (serwerowni) wraz z infrastrukturą towarzyszącą.
- wykonanie projektów specjalistycznych których konieczność opracowania może wyniknąć trakcie projektowania
- opracowanie szczegółowych przedmiarów robot i kosztorysów inwestorskich oraz harmonogramu rzeczowo-finansowego prac budowlanych i wdrożeniowych z podziałem na etapy realizacji ze szczególnym uwzględnieniem prac zanikowych lub ulegających zakryciu.
- wykonania Informacji dotyczącej Bezpieczeństwa i Ochrony Zdrowia podczas prac wykonawczych uwzględniającą charakter prac związany z miejscem układania kabli światłowodowych w kanalizacji deszczowej i ściekowej;
- sporządzenia Specyfikacji Technicznej Wykonania i Odbioru Robót Budowlanych uwzględniającej charakter prac w kanalizacji i określającej dokładną metodykę prowadzenia prac kablowych w rurach kanalizacyjnych oraz dla poszczególnych typów obiektów technicznych.
- wykonanie dokumentacji powykonawczej dla robót budowlanych oraz dokonanie niezbędnej aktualizacji dokumentacji geodezyjnej. Opracowanie tej dokumentacji musi zostać wykonane także w formie elektronicznej.
- wykonanie dokumentacji powykonawczej wdrożonych systemów informatycznych oraz wszelkich innych systemów związanych z działaniem sieci miejskiej (np. systemy podtrzymania zasilania, itd.).

Zamawiający zakłada, że prace projektowe będą prowadzone równolegle przez kilka zespołów projektowych Wykonawcy w zależności od branży, w terminach przewidzianych w harmonogramie prac (Załącznik nr B). Zadaniem Wykonawcy będzie także koordynacja zakresów, jednorodności oraz spójnego wyglądu dostarczonej dokumentacji.

Wszystkie elementy dokumentacji projektowej muszą uzyskać akceptację Zamawiającego i powołanego przez Zamawiającego Inżyniera Kontraktu przed rozpoczęciem prac wykonawczych. Ocena i zatwierdzanie prac projektowych następować będzie sukcesywnie w miarę przekazywania poszczególnych elementów dokumentacji projektowej i zakończy się odbiorem końcowym dokumentacji projektowej.

Zamawiający zastrzega sobie prawo do powołania dodatkowych organów lub ekspertów, którzy na zlecenie Zamawiającego dokonają weryfikacji przedstawionej dokumentacji na okoliczność zgodności z wymaganiami i normami prawnymi.

2.1.2. Wymagania formalne dla dokumentacji projektowej

Dokumentacja projektowa będzie opracowana zgodnie z przepisami:

a) Ustawy z dnia 7 lipca 1994r - Prawo budowlane (Dz.U.z 2006 Nr 156.poz.1118 z pózn.zm) z uwzględnieniem art 20 ust 1 i 2 tej ustawy
b) rozporządzenia Ministra Infrastruktury z dnia 3 Lipca 2003 r w sprawie szczegółowego zakresu i formy projektu budowlanego (Dz.U z 2003 r Nr 120 poz 1133 z pożn.zm)
c) rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 r w sprawie szczegółowego zakresu i formy dokumentacji projektowe) specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno -użytkowego (Dz.U. z 2004 r nr 2020 poz 2072 z póz.zm.).
d) Ustawa z dnia 7 maja 2010 r.o wspieraniu rozwoju usług i sieci telekomunikacyjnych (MegaUstawa) wraz z późniejszymi zmianami
a) obowiązującymi normami zasadami wiedzy technicznej , przepisami BHP ,. itp.

Przedmiary robót opracowane zostaną zgodnie z przepisami *Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004r w sprawie szczegółowego zakresu i formy dokumentacji projektowej. specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz U z 2004 nr 202. poz.2072 z póz.zm)* i zawierać będą w szczególności zestawienie wszystkich przewidywanych do wykonania robót w kolejności technologicznej ich wykonania oraz zestawienie urządzeń i armatury (sporządzone na podstawie dokumentacji projektowej), zgodnie z systematyką robót właściwą dla danego przedsięwzięcia a także zawierające opisy, jednostki oraz ilości wyliczone zgodnie z zasadami ustalonymi w specyfikacjach technicznych

Specyfikacje techniczne wykonania i odbioru robót budowlanych wykonane zostaną zgodnie z przepisami rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego (Dz.U.z 2004 r nr 202 poz 2072 z późn zm)

Informacja dotycząca bezpieczeństwa i ochrony zdrowia ze względu na specyfikę projektowanych obiektów budowlanych opracowana zostanie zgodnie z przepisami ustawy z dnia 7 lipca 1994i Prawo budowlane (Dz U .'2006r Nr 156 poz 1118 z późn zm) - art 20 ust 1 pkt 1b tej ustawy

Kosztorysy inwestorskie wykonane zostaną zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 18 maja 2004r w sprawie określenia metod i podstaw sporządzenia kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowania kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz.U. z 2004 nr 130 poz 1389).

Opracowania projektowe i opisowe objęte zamówieniem a w szczególności, specyfikacje techniczne, przedmiary robót będą wzajemnie spójne i skoordynowane pod względem technicznym dla zapewnienia uwzględnienia zasad bezpieczeństwa i ochrony zdrowia w procesie budowy.

2.1.3. Wymagania odnośnie formy dokumentacji projektowej

Dokumentację projektową należy opracować i dostarczyć w następujących formach i ilościach egzemplarzy (oddzielnie dla każdego tomu opracowania dokumentacji):

a) projekt budowlany i projekt wykonawczy - po 5 egzemplarzy na papierze (w tym 1 egz. nie zszyty), oraz po 1 egzemplarzu na nośniku elektronicznym płyta CD (format PDF lub JPG)
b) informacja dotycząca bezpieczeństwa i ochrony zdrowia (BIOZ) - po 3 egzemplarze na papierze. oraz 1 egzemplarz na nośniku elektronicznym (program WORD)
c) specyfikacje techniczne wykonania i odbioru robót budowlanych - po 3 egzemplarze na papierze oraz 1 egzemplarz na nośniku elektronicznym (program WORD)
d) przedmiary robót (komplet) - po 2 egzemplarze na papierze , oraz 1 egzemplarz na nośniku elektronicznym (program ZUZIA)
e) kosztorysy inwestorskie (komplet) - po 2 egzemplarze na papierze oraz 1 egzemplarz na nośniku elektronicznym (program ZUZIA)

Opracowania projektowe poszczególnych etapów powinny zapewnić spójność funkcjonalną i technologiczną projektowanej sieci (w tym m.in. w zakresie organizacji i wyposażenia węzłów sieci) z istniejącą infrastrukturą telekomunikacyjną Miejska Sieć Szerokopasmowa Żywiec. W celu przejrzystości dokumentacji oraz umożliwienia

Zamawiającemu rozliczanie projektu wymaga się przyjąć podział obszarowy poszczególnych części dokumentacji dotyczącej projektów kanalizacji i okablowania światłowodowego lub innego zatwierdzonego przez Zamawiającego.

Dokumentacja projektowa powinna posiadać :

a) nazwę opracowania i wykaz zawartości.
b) pisemne oświadczenia Wykonawcy, że jest ona wykonana zgodnie z umową, obowiązującymi przepisami techniczno-budowlanymi oraz normami i że zostaje wydana w stanie zupełnym (kompletna z punktu widzenia celu któremu ma służyć).
c) trwale oznaczenia projektu z informacjami o realizacji projektu ze środków unijnych wg wzoru uzgodnionego z Zamawiającym.

Nazwy plików wersji elektronicznej należy wpisać bez użycia polskich znaków.

2.1.4. Pozostałe wymagania

Przed przystąpieniem do realizacji prac projektowych, należy zapoznać się z planami modernizacyjnymi spółek komunalnych, posiadających swoją infrastrukturę na terenie miasta Żywiec. Do przyjętych planów modernizacji, należy dopasować harmonogram prac wykonawczych w ramach tworzenia infrastruktury światłowodowej projektu sieci dla miasta Żywiec.

Przed przystąpieniem do prac projektowych należy przeprowadzić weryfikację stanu istniejącej infrastruktury teletechnicznej. W ramach oceny, należy skupić się w głównej mierze na istniejących rurach przeznaczonych dla okablowania światłowodowego, wymienionych poniżej oraz wybudowanych po dacie zamknięcia prac koncepcyjnych. Należy sprawdzić stan oraz drożność ułożonych rur i ocenić możliwość prowadzenia w nich okablowania światłowodowego oraz wiązek mikrokanalizacji.

Istotnym z punktu widzenia budowy sieci zasobem miasta są drogi, chodniki i tereny zielone będące pod administracyjnym nadzorem Urzędu Miasta. Z uwagi na duża liczbę planowanych modernizacji oraz planowaną budowę nowych dróg, projektowane trasy kanalizacji i harmonogram prac powinny uwzględniać możliwość prowadzenia wspólnych prac ziemnych w jak największym zakresie. Powinno to zredukować wysokie nakłady na odtworzenie nawierzchni. Ma zapobiegać również sytuacji, w której budowa kanalizacji teletechnicznej zmusza do naruszenia nawierzchni świeżo wyremontowanej drogi, chodnika lub terenu zielonego.

Wszelkie wątpliwości lub propozycje Wykonawcy odnośnie formatu dokumentacji muszą zostać uzgodnione z Zamawiającym przed przystąpieniem do wykonywania dokumentacji projektowej. Odstępstwa i wszelkie zmiany od założeń projektowych musza uzyskać pisemną akceptację Zamawiającego.

Akceptacja dokumentacji projektowej przez Zamawiającego nie zwalnia Wykonawcy z odpowiedzialności za kompletność projektu i zakres prac wykonawczych nim objętych. Ewentualne prace dodatkowe nie ujęte na etapie projektu, ale niezbędne do zrealizowania zadania określonego w niniejszym dokumencie zostaną wykonane na koszt Wykonawcy.

2.2. Zadania Wykonawcy związane z budową sieci światłowodowej

Po zakończeniu procedury weryfikacji dokumentacji projektowej złożonej przez Wykonawcę, zatwierdzeniu harmonogramu prac budowlanych i wdrożeniowych i uzyskaniu pisemnej akceptacji Zamawiającego, Wykonawca wybuduje trakty kablowe, przyłącza obiektowe, kanalizację łącznikową oraz sieci stacyjne do Lokalnych Punktów Dostępowych LPD i przyłączy budynkowych do końcowych jednostek samorządowych objętych podłączeniem.

Akceptacja dokumentacji projektowej przez Zamawiającego nie zwalnia Wykonawcy z odpowiedzialności za kompletność projektu i zakres prac wykonawczych nim objętych. Ewentualne prace dodatkowe nie ujęte w ofercie przetargowej a także w projekcie wykonawczym, ale niezbędne do zrealizowania zadania określonego w niniejszym dokumencie zostaną wykonane na koszt Wykonawcy.

W szczególności zakres prac obejmować będzie:

- zainstalowanie wzmacnianych kabli światłowodowych w oparciu o wybraną w projektach i dopuszczoną przez MWPIK Żywiec technologię układania kabli w istniejącej kanalizacji deszczowej i ściekowej wraz z wszelkimi elementami liniowymi (osłony złączowe, stelaże zapasów i wykonanie szczególnych rozwiązań technicznych dla przejść kablami światłowodowymi miejsc charakterystycznych sieci kanalizacji ściekowej i deszczowej tj.

dla wszelkich obiektów technicznych (np. studzienek, komór przelewowych, kanalizacji przełazowej i nieprzełazowej, wejść do budynków, nawiązań między kanalizacją ściekową a deszczową, etc);

- wybudowanie nowych doziemnych ciągów kanalizacji teletechnicznej łącznikowej (łączącej poszczególne rodzaje kanalizacji deszczowej i ściekowej), rurociągów do wybranych węzłów lokalnych LPD oraz kanalizacji przyłączy budynkowych do jednostek organizacyjnych Miasta Żywiec wraz z zabudową studni, odtworzeniem nawierzchni, niezbędnymi przejściami pod drogami, wykonaniem przepustów ściennych etc;
- wybudowanie połączenia światłowodowego relacji Urząd Miejski - Stajnia Pałacowa oraz Stajnia Pałacowa - Straż Miejska w postaci odcinka rurociągu kablowego o długości 622m zawierającego rury prefabrykowane mikrokanalizacji wraz z 12 studniami kablowymi, instalacja mikrokabla 48J wraz z odpowiednim wyposażeniem węzłów kończącym tor światłowodowy. Szczegółowy zakres prac zawiera posiadany przez Zamawiającego projekt budowlano-wykonawczy do zadania p.t. „Budowa teletechnicznej kanalizacji kablowej i kabli światłowodowych relacji Urząd Miejski - Park Zamkowy - Straż Miejska dla potrzeb monitoringu i transmisji danych na terenie miasta Żywiec” stanowiący załącznik F niniejszego dokumentu;
- zinwentaryzowanie, sprawdzenie drożności (kalibracja) i dołączenie istniejących ciągów rurowych z mikrokanalizacją wykonanych przez Urząd Miasta we wcześniejszych etapach prac ziemnych wraz z wykonaniem niezbędnych połączeń i dołożeniem złączek i obudów liniowych mikrokanalizacji, tam gdzie okaże się to niezbędne (połączenia nowej kanalizacji z istniejącą oraz studnie na istniejących przebiegach bez zabudowanych obudów liniowych);
- wdmuchnięcie mikrokabli 24J i 72J do istniejącego toru mikrokanalizacji na relacji Urząd Miasta – Ecoterm oraz kabla 48J do nowej kanalizacji na odcinku Stajnia Pałacowa – Urząd Miasta oraz odcinek łącznikowy kabla/mikrokabla 144J na relacji Urząd Miasta-studnia nr 7;
- zabudowanie nowych, niezbędnych obiektów rozdzielczych jak studnie kablowe, zasobniki, liniowe i odgałęźne obudowy doziemne mikrokanalizacji wraz z niezbędnym osprzętem połączeniowym i uszczelniającym;
- wykonanie wszelkich przepustów, przecisków i przewiertów sterowanych oraz zabezpieczenie występujących kolizji z innymi rodzajami infrastruktury ziemnej rurami osłonowymi zgodnie z normami i wymogami;
- wykonanie wszelkich połączeń i zakończeń torów włókien wg zaprojektowanego rozpływu włókien;
- wykonanie pomiarów kontrolnych i odbiorowych.

Łączna długość trasowa sieci magistralnej do wykonania różnymi metodami szacowana jest na 16 050m, w tym 1342m stanowić będą mikrokable wdmuchnięte do istniejącej mikrokanalizacji wykonywanej w ramach wcześniejszego projektu Urzędu Miasta, 3212m trasy kabli układanych w kanalizacji sanitarnej, 11 495m – w kanalizacji deszczowej różnego rodzaju. Do wykonania należy również przyjąć około 982m w nowobudowanej i nowoprojektowanej kanalizacji ziemnej łącznikowej oraz 22 przyłącza przyobiektowe (łącznie szacuje się ok. 2,5-3km tras przyłączy), a także 622m w kanalizacji ziemnej na trasie Straż Miejska - Stajnia Pałacowa - Urząd Miasta.

Zestawienie szacowanych długości trasowych kabli światłowodowych zawiera **Załącznik C.** Wszystkie podane długości dotyczą długości trasowych, długości kabli powinny uwzględniać nadmiar długości na niezbędne zapasu liniowe, złączowe, przyobiektowe i wynikające z technologii. Wykonawca powinien oszacować prawidłowe wartości we własnym zakresie i na własne ryzyko.

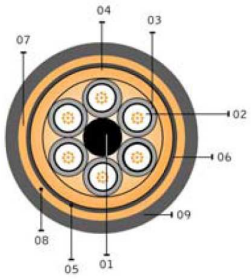
2.2.1. Zakres i wymagania dla prac wykonawczych związanych z budową kabli światłowodowych w istniejącej kanalizacji sanitarnej i deszczowej

W zakres zadania wchodzić będzie budowa nowych kabli światłowodowych w istniejącej kanalizacji deszczowej i ściekowej będącej w zasobach MPWIK Żywiec. Kable wykorzystywane do budowy sieci miejskiej powinny być kablami przeznaczonymi do układania w kanalizacji wodnej, a w szczególności ich konstrukcja powinna charakteryzować się poniższymi parametrami minimalnymi.

Rodzaj kabla przeznaczonego do budowy sieci w kanalizacji deszczowej i ściekowej:

Kabel zewnętrzny wzmacniany w podwójnym płaszczu PE z osłoną z drutów stalowych o taśmy aluminiowej, wielotubowy, tuba żelowana PBT o śr.2.0mm , włókna optyczne w płaszczu lakierowanym 250um, centralny element dielektryczny, wewnętrzne zbrojenie dielektryczne z włókna szklanego, zewnętrzne zbrojenie z plecionki metalowej, odporność na promienie UV, odporny na wnikanie i penetrację wzdłużną wody, zakres temperaturowy -40oC – 70oC, silna osłona przeciw gryzoniom, powłoki PE (opcjonalnie LSZH)

Konstrukcja:



1 – dielektryczny pręt centralny
2 – włókna światłowodowe
3 – luźna tuba wypełniona żelem
4 – wzmocnienie z włókien szklanych
5 – sznurki do rozrywania powłoki
6 – powłoka wewnętrzna z PE wraz z barierą z folii aluminiowej
7 - pancerz z drutów stalowych
8 - powłoka zewnętrzna z PE

Parametry kabla:

Rozkłady włókien:	12J – 2T6F, 24J – 4T6F, 48J – 8T6F, 72J – 6T12F, 144J – 12T12F
Średnica kabla:	12J i 24J - 11.5mm, 48J, 72J, 144J - 15.5mm
Minimalny naciąg stały:	1300N (4-48J), 1800N (48J-144J),
Minimalny naciąg instalacyjny:	3500N (12,24J), 5000N (48J, 72J, 144J)
Odporność na zgniatanie:	min.4000N
Minimalny promień gięcia:	20 x średnic
Zakres temperaturowy pracy:	-40^{o}C do +70^{o}C
Kolor powłoki zewnętrznej:	czarny lub niebieski
Kodowanie kolorystyczne tub i włókien:	wg IEC 60304
Znaczniki na kablu:	oprócz normalnych identyfikatorów i znaczników długości musi znajdować się napis: „MSS ZYWIEC” lub inny wg wskazań Inwestora

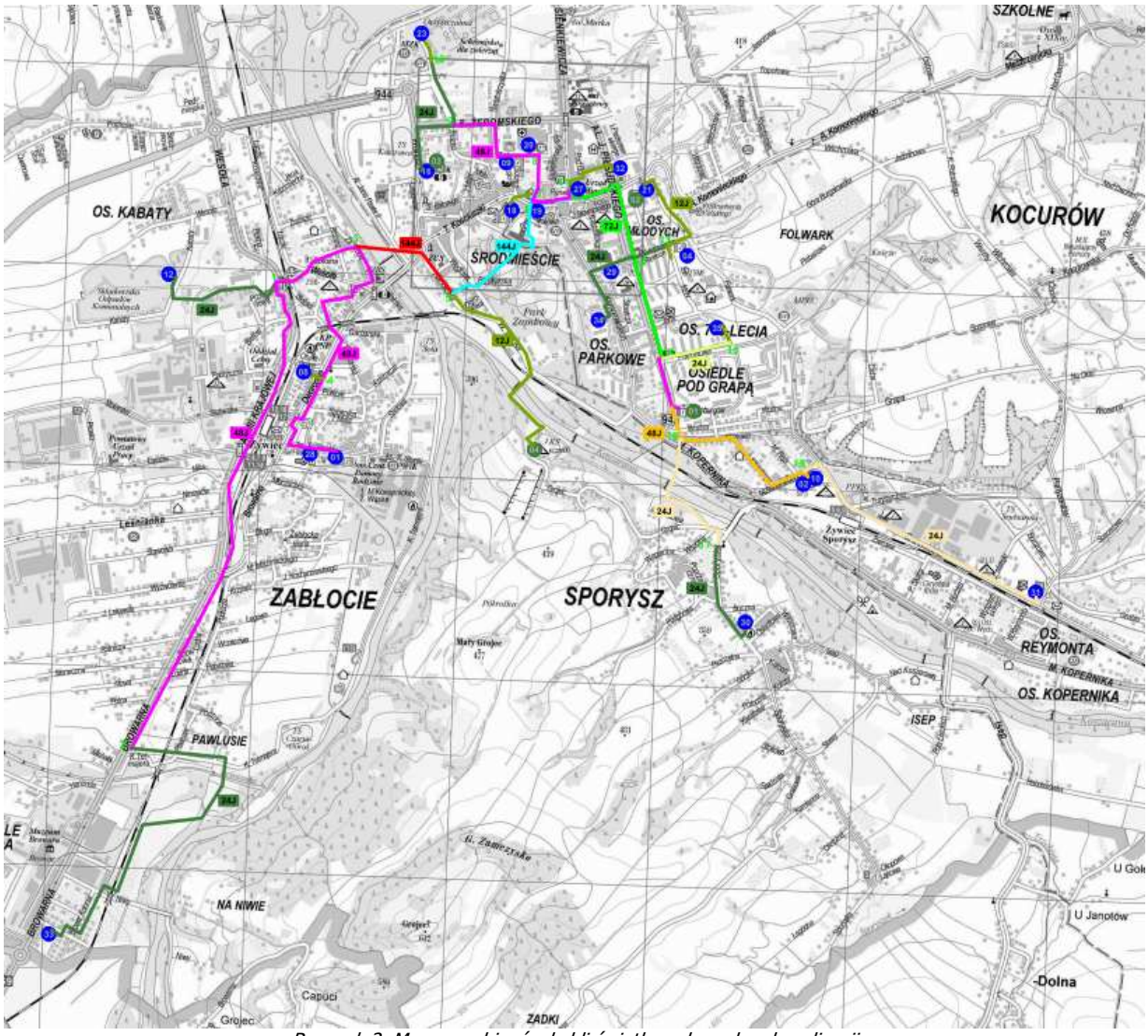
Do prowadzenia kabla przewidziano istniejące kanały przełazowe i nieprzełazowe kanalizacji deszczowej i grawitacyjnej kanalizacji sanitarnej (kanały kamionkowe i betonowe o średnicy Ø 300 i powyżej). Nie przewiduje się wykorzystania kanalizacji tłocznej.

W podstawowej metodzie wykonania przyjęto, że specjalne kable przeznaczone do montażu w kanalizacji ściekowej instalowane będą metodami rozprężnymi i zawieszane pod stropem kanałów nieprzełazowych przy pomocy zawiesi oplotowych dobranych do średnicy kabla i kotwionych w studzienkach kanalizacyjnych. W wyjątkowych sytuacjach dopuszcza się układanie kabli na dole kanału kanalizacji deszczowej lub mocowanych na ścianie bocznej w przypadku kanałów przełazowych przy pomocy kotew i kołków samouszczelniających. W przypadku wybranych fragmentów sieci kanalizacji nieprzełazowej Zamawiający dopuszczać będzie także zastosowanie metod montażu zrobotyzowanego, które nie będą naruszały struktury rurarzu kanałów.

Osprzęt naprężający oraz pozostały osprzęt do montażu kabli powinien być wykonany z metali odpornych na korozję i agresywne środowiska wodne. Uchwyty kablowe systemu zrobotyzowanego powinny umożliwiać montaż kabla w zatrzaskach uchwytu bez dodatkowych elementów mocujących.

Mufy złączowe stosowane do wykonania odgałęzień kabli dystrybucyjnych oraz do wykonania złącz odcinków fabrykacyjnych kabli powinny być jak najbardziej płaskie, odporne na wnikanie wody oraz wykonane z materiałów gwarantujących odporność na środowisko, w którym będą eksploatowane. Przy każdej mufie złączowej powinien zostać zgromadzony zapas złączowy kabla (15 m na każdą stronę) w specjalnych stelażach montowanych w studzience kanalizacyjnej lub na uchwytach ściennych po obwodzie studzienki. W miarę możliwości należy unikać projektowania osłon złączowych w studzienkach kanalizacyjnych, dobierając tak odcinki prefabrykacyjne aby miejsca połączeń wypadały w studzienkach przyobiektowych.

Przewidywany przebieg tras kablowych z zaznaczeniem typu kanalizacji wodnej przedstawiono na poniższym rysunku, a także w większej skali na rysunku nr 2.0 z załącznika.

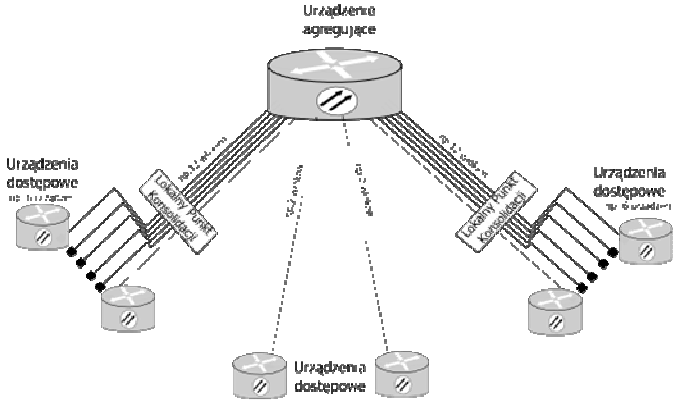


Rysunek 2. Mapa przebiegów kabli światłowodowych w kanalizacji sanitarnej i deszczowej sieci miejskiej w Żywcu

Dla sieci miejskiej w Żywcu struktura magistrali będzie topologią gwiazdy związaną praktycznie bezpośrednio z warstwą dystrybucji. W takim przypadku występować będzie największa liczba urządzeń, a co za tym idzie największa ilość połączeń bezpośrednich pomiędzy punktami. Rozwiązania topologii dla tej warstwy obejmują:

- gwiazda , w której do każdego punktu dostępowego PA dociera dedykowany tor światłowodowych bez pośrednictwa włączenia do Lokalnych Punktów Dystrybucji;

- gwiazda z pośrednictwem pasywnych Lokalnych Punktów Dystrybucji, w której podobnie jak poprzednio, do punktu dostępowego dociera dedykowany tor światłowodowy jednakże rozdział tras torów włókien dokonuje się w szafie zewnętrznej lub przełącznicy wnętrzowej Lokalnego Punktu Dystrybucji (do punktu docierać powinny kable o ilości włókien będącej iloczynem ilości punktów dostępowych i przyjętego standardu 6 włókien/punkt końcowy. Szczególną odmianą tej topologii będą wszystkie technologie zwielokrotnienia falowego WDM zakładające wykorzystanie 1 włókna światłowodowego do transmisji sygnału dla kilku (2-16) abonentów/punktów dostępowych.



Rysunek 3: Zalecana topologia gwiazdy lokalnej w warstwie dostępowej z/bez Lokalnymi Punktami Dystrybucji

Na kablu magistralnym zostaną zbudowane łącza światłowodowe do Lokalnych Punktów Dostępowych LPD oraz połączenia do punktów styku z Operatorami.

Połączenie podstawowe pomiędzy dwoma punktami sieci (punktem GPD a punktami końcowymi) jest realizowane za pomocą 6 włókien jednomodowych, wśród których 2 włókna są podstawowe, natomiast 4 kolejne włókna są połączeniem o przeznaczeniu zapasowym i/lub przyszłościowym. Prędkością docelową transmisji realizowanej we włóknach podstawowych będzie standard 10Gb/s, dla łącz redundantnych dopuszcza się możliwość zastosowania transmisji 1Gb/s.

Z uwagi na spore zapotrzebowanie na włókna warstwy magistralnej oraz konieczność optymalizacji kosztów instalacji kabli przewiduje się zastosowanie kabli o większej liczbie włókien niż wynikająca z zsumowania pojemności połączeń podstawowych. W szczególności minimalną pojemność kabla docierającego do punktów końcowych określono na 12 włókien, a oczekiwany przez Zamawiającego minimalny rozpływ włókien określa załączony **Schemat rozpływu włókien (Rysunek nr 2.0).**

W tym celu Zamawiający przewiduje, że niezbędne będzie zabudowanie wielotubowych kabli światłowodowych 12 elementowych o pojemności do 144 włókien światłowodowych. Zastosowanym włóknem powinno być włókno jednomodowe 9/125 z usuniętym pikiem wodnym standardu ITU-T.G652D.

W celu obliczenia niezbędnych długości kabli należy przewidzieć odpowiedni współczynnik zafalowania, zapasy kabla wynikające z norm telekomunikacyjnych (zapasy złączowe i liniowe, przyobiektowe), wejścia do budynków a także zapasy technologiczne wynikające z technologii układania kabli w kanalizacji ściekowej i sanitarnej. Łączna długość wykorzystanych kabli będzie większa niż długość trasowa.

Włókna kabli magistralnych należy zakańczać w przełącznicach Punktów Dystrybucyjnych wprowadzając i wyprowadzając pełne profile kabli do pomieszczeń PD umożliwiając dokonywanie komutacji w obiektach bez konieczności modyfikacji połączeń w mufach znajdujących się w studzienkach kanalizacyjnych.

W celu wykonania połączeń światłowodowych do obiektów końcowych i węzłowych poprzez wybudowane rurociągi kablowych należy przy użyciu metody pneumatycznej lub zaciągania mechanicznego zainstalować uniwersalne kable światłowodowe w powłokach LSOH o odpowiedniej pojemności. Następnie należy je zakończyć na przełącznicach światłowodowych poprzez spajanie włókien optycznych z kabla światłowodowego z pigtailami w przełącznicach. Końcowym elementem każdego toru optycznego będzie łącznik światłowodowy SC/APC zamontowany w przełącznicy.

Zamawiający wymaga, aby wszystkie punktu rozdziału sieci w miarę możliwości technicznych były lokowane w szafach wnętrzowych w obiektach węzłowych sieci miejskiej. W wyjątkowych przypadkach mogą to być mufy światłowodowe montowane w studniach kablowych przyobiektowych.

Po wybudowaniu każdy odcinek światłowodu pomierzyć przy pomocy reflektometru i miernika strat mocy optycznej. Do każdego wybudowanego odcinka Wykonawca dostarczy dokumentację powykonawczą.

2.2.2. Zakres i wymagania dla prac budowlanych związanych z budową kanalizacji łącznikowej oraz kanalizacji ziemnej przyłączy obiektowych

Przebieg kanalizacji światłowodowej łącznikowej oraz kanalizacji przyłączy obiektowych powinien uwzględniać przebieg ulic i terenów zielonych należących do Urzędu Miasta, a trasy te będą lokowane wyłącznie na działkach będących w gestii samorządu. Z uwagi na wysokie koszta odtworzenia nawierzchni instalacja kanalizacji przy wspólnych inwestycjach może przynieść Inwestorowi znaczące oszczędności. Stąd w projektach powinno kłaść się duży nacisk na koordynacje projektu i harmonogramu prac z ziemnymi pracami i inwestycjami prowadzonymi przez miejskie służby infrastrukturalne.

Zamawiający oczekuje wykonawstwa prac budowlanych w sposób jak najmniej ingerujący w stopień zagęszczenia gruntu, estetykę wykonanych nawierzchni i jakość odtworzenia miejsc objętych wykopami. W szczególności Zamawiający informuje, że Wykonawca powinien spełnić wymagania Referatu d/s Dróg Publicznych i Wydziału Inwestycji Miejskich uzyskane na drodze uzgodnień. Na dzień dzisiejszy wymagania te obejmują konieczność odtwarzania w sposób gwarantujący jednolity współczynnik zagęszczenia gruntu co może skutkować koniecznością odtwarzania np. całej szerokości chodników.

W projekcie sieci miejskiej uwzględniono występowanie miejsc podziału, studni przyobiektowych ułatwiających wykonanie odgałęzień do obiektów oraz dokonywania przejść między poszczególnymi typami kanalizacji wodnej realizowanych w postaci:

- studni kablowych z betonu SK-2, SKR-1, SKO-2, SKR-2, SK-6
- studni i zasobników polietylenowych z HDPE
- szaf kablowych zewnętrznych.

Szacowana liczba punktów, w których wyżej wymienione elementy będą niezbędne wynosi ok. **62 szt.** W oszacowaniu kosztów przyjęto zastosowanie studni betonowych z przyjętego powyżej typoszeregu. Zadaniem projektanta będzie odpowiedni dobór liczby, miejsca zabudowy i wielkości studni/ szafy kablowej w zależności od charakteru miejsca podziału i miejsca w strukturze sieci.

Proponowaną rurą przyłącza obiektowego jest rura osłonowa o średnicy minimum 110mm. Wszystkie rury wprowadzane do obiektów powinny zostać zakończone w studni przyobiektowej i obustronnie uszczelnione gazo i wodoszczelnie (od strony studni i obiektu). Wprowadzenie kabli z kanalizacji wodnej powinno odbywać się z najbliższego dogodnego obiektu kanalizacji wodnej do studni przyobiektowej 2 rurami HDPE40 z obustronnym uszczelnieniem gazo i wodoszczelnym obu końców rur HDPE (od strony studni przyobiektowej i obiektu kanalizacji wodnej). Studnie przyobiektowe powinny być wyposażone w stelaż zapasu kabla z kanalizacji wodnej (zapas złączowy 15m + liniowy 50m) oraz stelaż zapasu kabla przyłącza (zapas złączowy 15m).

Zaprojektowane studnie powinny uwzględniać możliwość wprowadzania kanalizacji kablowej 1-4 otworowej. Kształty i wymiary oraz wykonanie studni kablowych powinno także uwzględniać wymagania dotyczące warunków instalowania współczesnych kabli telekomunikacyjnych kabli optotelekomunikacyjnych (światłowodowych) i mikrokabli światłowodowych oraz muszą zapewnić wystarczająco dużo miejsca na posadowienie akcesoriów rozdzielczych i połączeniowych rur prefabrykowanych. Zaproponowane studnie powinny umożliwić również wykorzystanie studni przelotowo, narożnie, odgałęźnie oraz uzyskanie korzystnych relacji odnośnie do kosztów produkcji i kosztów budowy.

Dla ułatwienia prac montażowych projektować należy w miarę możliwości studnie dwudzielne. Stosowanie studni o większych gabarytach lub innego rodzaju podyktowane względami projektowymi wymaga uzgodnienia z Inwestorem. Projektant musi również rozstrzygnąć konieczność zastosowania osadnika, czyli prefabrykowanego umocnienia zagłębienia w dnie studni, przeznaczonego do odprowadzania wody opadowej. Studnie powinny być wyposażone w pełny osprzęt dodatkowy jak: rury wsporcze i uchwyty pozwalające zamontować rury RHDPE w studni.

Studnie powinny posiadać pokrywy z trwałym oznaczeniem właściciela – Gmina Żywiec. Zamawiający wymaga aby studnie kablowe posiadały elementy żeliwne ram i pokryw. Dobór klasy obciążalności zależeć będzie od miejsca posadowienia studni i zostanie dobrana przez Wykonawcę. Zamawiający zatwierdzi te propozycje po ocenie projektów technicznych. Wszystkie studnie kablowe powinny być zabezpieczone dodatkowymi pokrywami antywłamaniowymi z zamkiem typu Abloy, dopasowanymi do rodzaju studni kablowej. Pokrywy powinny być wykonane z pełnej blachy zabezpieczonej galwanicznie i spełniać wymagania firmy TPSA w zakresie hermetyzacji sieci.

Prace te należy wykonać zgodnie z obowiązującym prawem i normami budowlanymi stosowanymi w telekomunikacji oraz wytycznymi zawartymi w dokumentacjach Zamawiającego. Wykaz tych norm załączono w końcowej części tego opracowania.

2.3. Zadania Wykonawcy związane z modernizacją i budową infrastruktury pomieszczeń węzłowych

Zgodnie z harmonogramem prac zatwierdzonym przez Zamawiającego, Wykonawca przystosuje wybrane obiekty warstwy dystrybucyjnej do pełnienia funkcji sieciowych. W szczególności dostosowanie pomieszczeń dotyczyć będzie:

- 1 obiektu Głównego Punktu Dystrybucji (GPD) zintegrowanego z Centrum Zarządzania Siecią (CZS) i z Operatorskim Punktem Styku Z Internetem (IXC)
- 10 Lokalnych Punktów Dostępowych zintegrowanych z funkcjonalnością końcowych Punktów Abonenckich,
- 9 samodzielnych końcowych Punktów Abonenckich,

Infrastrukturę lokalnego węzła sieciowego lub punktu końcowego stanowić będzie szafa teleinformatyczna, pasywne światłowodowe elementy rozdzielcze umożliwiające zakończenie i rozdział włókien światłowodów sieci miejskiej (przełącznice wraz z patchcordami światłowodowymi), urządzenia aktywne sieci, urządzenia systemu nadzoru zabezpieczenia fizycznego sieci i inne systemy pomocnicze służące niezawodnej pracy urządzeń (instalacja zasilająca, klimatyzacja, wentylacja, zasilanie rezerwowe, oświetlenie, etc – w zależności od zapotrzebowania i charakteru węzła).

2.3.1. Szczegółowe zadania Wykonawcy związane modernizacją infrastruktury pomieszczeń węzłowych

Prace projektowe związane z modernizacją pomieszczeń węzłowych obejmować będą:

- dokonanie wizji lokalnych i uzgodnień posadowienia infrastruktury technicznej węzłów sieci miejskiej w jednostkach samorządowych wg wykazu z Załącznika A.
- uzgodnienie przebiegu tras w obiektach i lokalizacji szaf dla wszystkich lokalizacji węzłowych i końcowych wraz z pozyskaniem zgód zarządców obiektów.
- wykonanie niezbędnych projektów (jeśli będą wymagane prawem) modernizacji pomieszczeń węzłów sieci miejskiej wraz z infrastrukturą towarzyszącą;
- wykonanie projektów branżowych i specjalistycznych których konieczność opracowania może wyniknąć trakcie projektowania
- wykonanie Informacji dotyczącej bezpieczeństwa i ochrony zdrowia podczas prac wykonawczych.
- opracowanie szczegółowych przedmiarów robot i kosztorysów inwestorskich oraz harmonogramu rzeczowo-finansowego prac budowlanych i wdrożeniowych z podziałem na etapy realizacji ze szczególnym uwzględnieniem prac zanikowych lub ulegających zakryciu.
- sporządzenie Specyfikacji Technicznej Wykonania i Odbioru Robót Budowlanych.
- wykonanie dokumentacji powykonawczej wykonanych prac.

Wszystkie projekty należy wykonać zgodnie z obowiązującym prawem budowlanym i normami stosowanymi w telekomunikacji w odniesieniu do sieci wnętrzowych oraz zgodnie z wytycznymi zawartymi w dokumentacjach Zamawiającego. Wykaz tych norm załączono w końcowej części tego opracowania.

Zakres niezbędnych prac i wyposażenie zależne będzie od charakteru węzła i zostanie określone przez projektanta Wykonawcy na etapie projektowania na bazie minimalnych wymagań Zamawiającego. W szczególności Zamawiający oczekuje że Wykonawca:

- dostosuje pomieszczenia jednostek wybranych na węzły sieci do przyjęcia potrzebnej infrastruktury teletechnicznej, zamontuje szafy teleinformatyczne o odpowiedniej pojemności zależnej od charakteru węzła i liczby urządzeń przewidzianych do zamontowania w szafie wraz z niezbędnymi zapasami na rozbudowę.
- wykona odpowiednie remonty i modernizacje stanu technicznego pomieszczenia,
- doprowadzi zasilanie elektryczne do szafy teleinformatycznej z najbliższej rozdzielni budynkowej (w przypadku obiektów użytkowanych na mocy porozumienia, rozdzielnice należy zaopatrzyć w podlicznik zużycia energii elektrycznej) oraz wykona oddzielne zabezpieczenie elektroenergetyczne (nadprądowe, przeciwprzepięciowe) dla danego węzła;
- wykona instalację oświetlenia jeśli pomieszczenie go nie posiada,
- wykona min. 2 tory miedziane kategorii 6 FTP (dla odległości do 90m) lub tor światłowodowy 4 włóknowy 9/125 z kabla stacyjnego (dla odległości ponad 90m) łączące szafy węzła sieci miejskiej z szafą lub pomieszczeniem mieszczącym urządzenia aktywne sieci LAN jednostki organizacyjnej Zamawiającego.

- wykona odpowiednie przepusty ścienne i wnętrzową instalacje osłonową dla kabli światłowodowych (korytka elektroinstalacyjne, rurki RL, mikrorurki bezpośrednio w tynku, etc) i doprowadzi je do szaf teleinformatycznych węzła,
- wykona fizyczne zabezpieczenia dostępu do pomieszczenia lub szafy teletechnicznej, jeśli pomieszczenie będzie użytkowane wspólnie z gospodarzem obiektu,
- zaprojektuje i wykona wszelkie inne instalacje lub modernizacje pozwalające na bezpieczne i pewne użytkowanie pomieszczenia w charakterze węzła telekomunikacyjnego.

Proponowane wyposażenie minimalne poszczególnych węzłów stanowić będą elementy zaproponowane na etapie koncepcji i zamieszczone w *załączniku D – Zestawienie ilości minimalnych elementów wyposażenia węzłów*. Szczegółowe wymagania Zamawiającego odnośnie wyposażenia i elementów węzła zintegrowanego, w tym wymagania minimalne dla systemu zasilania gwarantowanego znajdują się w *Załączniku E - Opis wymagań dla obiektów węzłowych.*

Zadaniem Wykonawcy będzie jednakże zaprojektowanie i wykonanie kompletnej infrastruktury węzła z punktu widzenia funkcji, którą będzie pełnił.

2.3.2. Szczegółowe zadania Wykonawcy związane z modernizacją i budową infrastruktury zintegrowanego węzła głównego (GPD / CZS / IXC)

Szerszy zakres prac niż dla węzłów dystrybucyjnych Wykonawca będzie zobowiązany wykonać w pomieszczeniach przeznaczonych przez Zamawiającego na serwerownie Centrum Zarządzania Siecią. Wynika to z kluczowej roli jaką będzie pełnić ten węzeł w administracji i monitorowaniu sieci miejskiej.

Zakres prac związanych z modernizacja obejmuje przekształcenie wskazanego pomieszczenia w nowoczesną serwerownie wraz z niezbędną infrastrukturą i instalacjami oraz z zapewnieniem możliwości zarządzania siecią przez administratorów z pomieszczeń Biura d/s Informatyki i Telekomunikacji. Celem Wykonawcy jest zbudowanie nowoczesnej serwerowni o odpowiedniej infrastrukturze teleinformatycznych wyposażonej w niezbędne okablowanie światłowodowe i strukturalne wraz z kompletnymi, niezbędnymi instalacjami elektrycznymi, oświetleniowymi, klimatyzacją, wentylacją i instalacjami teletechnicznymi zapewniającymi prawidłowe działanie węzła.

W szczególności do zadań Wykonawcy należeć będzie:

- przeprowadzenie wizji lokalnych w pomieszczeniach istniejącej i nowoprojektowanej serwerowni sieci miejskiej celem szczegółowej weryfikacji zakresu prac, oszacowanie nośności stropów pomieszczenia i przydatności pod kątem planowanego zastosowania,
- wykonanie niezbędnego projektu budowlanego modernizacji pomieszczenia zintegrowanego węzła sieciowego oraz pomieszczenia podpiwniczenia przewidzianego na agregatorownie wraz ze wszystkimi projektami branżowymi i wykonawczymi,
- wykonanie modernizacji istniejących pomieszczeń przeznaczonych przez Zamawiającego na węzeł zintegrowany CZS/GPD/IXC. Wykonawca dokona niezbędnych prac budowlanych, których zakres na etapie koncepcyjnym oszacowano na: zamurowanie okna lub zamontowanie krat zabezpieczających, postawienie nowych przeszklonych i izolowanych termicznie ścianek działowych oddzielających wejście do pomieszczenia od części serwerowej, modernizacja instalacji wodno-ściekowej w obrębie pomieszczenia (jeśli okaże się potrzebna), wykonanie podłogi teletechnicznej oraz wykończenia pomieszczeń w niezbędną stolarkę drzwiową klasy antywłamaniowej z zachowaniem istniejących drzwi ozdobnych od strony korytarza.
- wykonanie modernizacji istniejącego pomieszczenia w podpiwniczeniu z przeznaczeniem na pomieszczenie agregatu prądotwórczego, ewentualnie komory UPS;
- wykonanie niezbędnych zabezpieczeń budowlanych serwerowni (drzwi wejściowe antywłamaniowe z zamkiem szyfrowym, ew. wykorzystanie krat w oknach) i pomieszczenia w podpiwniczeniu (drzwi wejściowe antywłamaniowe) oraz wykonanie zabezpieczeń przed ewentualnym zalaniem, jeśli istnieje takie zagrożenie,
- wykonanie duktów kablowych o odpowiedniej pojemności doprowadzających kable światłowodowe z przyłącza obiektowego do serwerowni. Z uwagi na niewielką powierzchnię serwerowni zaleca się wykonanie w podpiwniczeniu dedykowanego pomieszczenia/miejsca na kablownie, w której zgromadzone zostaną zapasy kabli liniowych oraz niezbędny osprzęt kablowy.

- wyposażenie pomieszczeń CZS w niezbędne dukty kablowe w podłodze lub w systemie duktów kablowych podwieszanych gwarantujące rozprowadzenie kabli po całej serwerowni (także dla szaf zabudowanych w przyszłości);
- zaprojektowanie i zbudowanie systemów nadzoru i monitoringu technicznego pomieszczeń serwerowni i pomieszczenia na agregat prądotwórczy wraz z systemami kontroli dostępu i systemem wykrywania pożarów;
- wykonanie przyłącza instalacji elektrycznej o odpowiedniej mocy i obciążalności z najbliższej dostępnej rozdzielnicy budynkowej, wykonanie przyłącza instalacji zasilania dedykowanego z pomieszczenia agregatu prądotwórczego i komory zasilaczy rezerwowych oraz wykonanie instalacji elektrycznej rozprowadzającej moc po pomieszczeniu serwerowni wraz z doprowadzeniem zasilania do szaf serwerowych, wszystkie instalacje powinny zostać zakończone lokalną rozdzielnicą serwerowni z własnym podlicznikiem, grupującą wszystkie zabezpieczone obwody elektryczne z pomieszczenia serwerowni, obwody zasilania rezerwowego oraz obwody przyłącza budynkowego;
- zabudowa kompletnego układu zasilania rezerwowego, w tym redundantnego układu bezprzerwowych zasilaczy rezerwowych (UPS) o łącznej mocy min. 2x12 kVA i podtrzymaniu bateryjnym min. 8 min wraz z przyłączem do zasilania rezerwowego z agregatu prądotwórczego o mocy szczytowej 40kVA oraz niezbędnymi elementami automatyki autostartu i monitorowania parametrów tych urządzeń. W przypadku agregatu należy przewidzieć urządzenia przeznaczone do montażu w pomieszczeniu podpiwniczenia w pobliżu planowanej serwerowni (wraz z zaplanowaniem odpowiedniego układu wyrzutu spalin. Dla zestawów baterii i UPSów zaleca się wydzielenie małego pomieszczenia na komorę bateryjną lub umiejscowienie jej w pomieszczeniu z agregatem.
- wykonanie łącznikowego połączenia światłowodowego min. 72 włóknowego (9/125) oraz za pomocą min.4 kabli miedzianych FTP kat.6A między starą serwerownią a nową wraz z zakończeniem torów dedykowanymi przełącznicami panelowymi 72xSC/APC i FTP kat.6A.
- zabudowa nowych 3 szaf na sprzęt aktywny oraz szafy systemu optycznego dużej pojemności (ODF) wg wymagań projektu wraz z niezbędnym wyposażeniem umożliwiającym wykonanie podłączeń torów optycznych.
- wykonanie stanowiska nadzoru w pomieszczeniu nowej serwerowni z odpowiednim wyposażeniem w sprzęt jak monitor komputer, umeblowaniem i okablowaniem stanowiska.

Infrastrukturę węzła zintegrowanego uzupełnią **dodatkowe systemy,** wśród których obowiązkiem Wykonawcy będzie wykonanie:

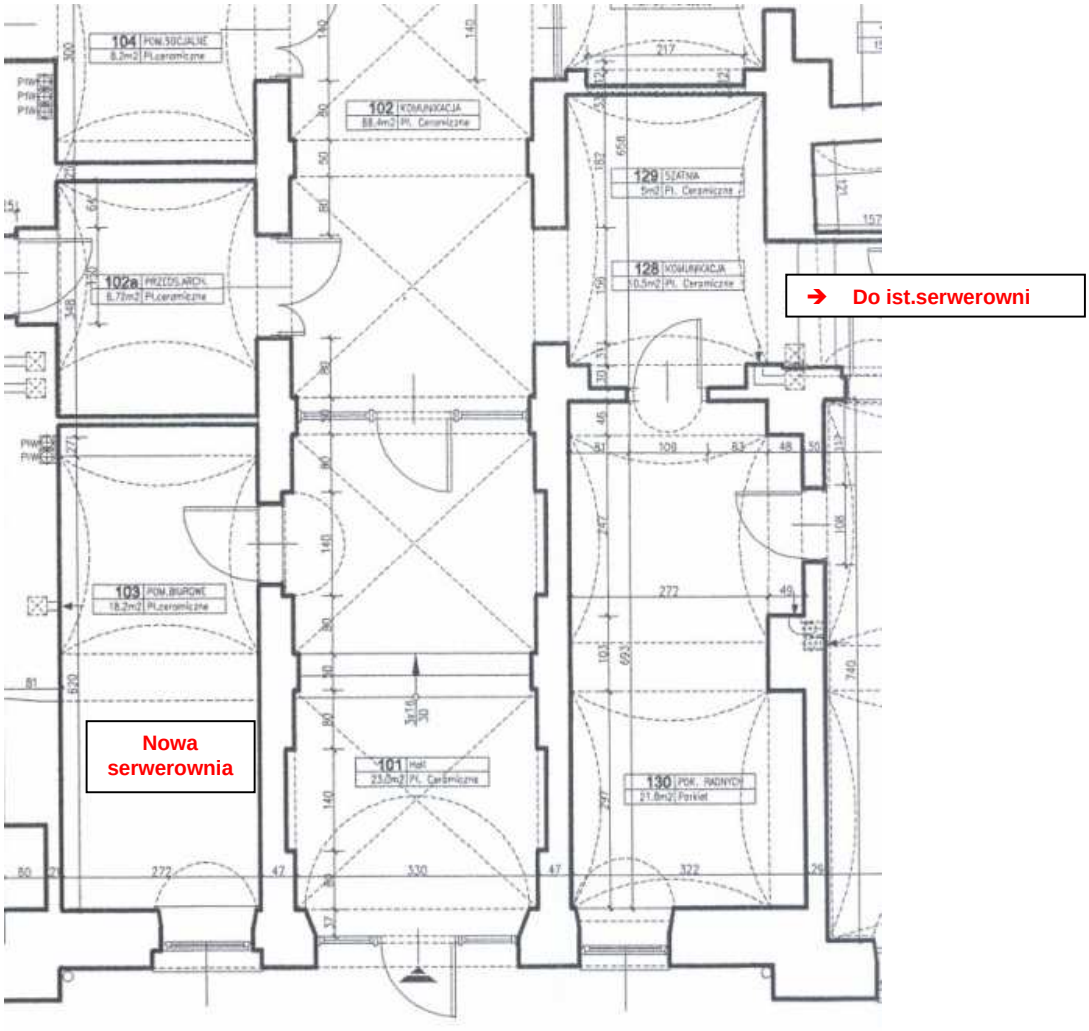
- systemu zasilania gwarantowanego Centrum Zarządzania (obejmuje wykonanie bezprzerwowego zasilania energetycznego, opartego na: wydzielonej wewnętrznej linii zasilającej wyprowadzonej z tablicy głównej budynku wyposażonej w zabezpieczenia przeciwprzepięciowe, agregacie prądotwórczym przejmującym zasilanie w przypadku zaniku napięcia zewnętrznego oraz urządzeniach UPS pracujących w układzie separującym wszelkie zakłócenia pochodzące z instalacji elektroenergetycznej);
- infrastruktury światłowodowej i okablowania strukturalnego pomieszczeń Centrum (max. ok.10 punktów PEL) łączącego poszczególne szafy urządzeń aktywnych oraz pomieszczenia administratorów, starą serwerownie oraz punkty PEL w samej serwerowni;
- nadmiarowego układu klimatyzacji i wentylacji pomieszczeń serwerowni;
- Systemu Kontroli Dostępu (SKD) oraz System Sygnalizacji Włamania i Napadu (SWIN) wraz z instalacja CCTV (3 kamery+rejestrator) obejmującą ochroną pomieszczenia serwerowni i agregatorowni;
- Instalacja Systemu Alarmu Pożarowego (SAP) dla pomieszczenia CZS i pomieszczenia agregatora oraz Instalacja Systemu Układu Gaśniczego (SUG) poszczególnych szaf teleinformatycznych zawierających urządzenia aktywne.

Zadaniem Wykonawcy będzie dobór odpowiednich systemów i urządzeń oraz ich instalacja. Szczegółowe wymagania Zamawiającego odnośnie wyposażenia i elementów węzła zintegrowanego, w tym wymagania minimalne dla systemu zasilania gwarantowanego znajdują się w *Załączniku E - Opis wymagań dla obiektów węzłowych*.

Zamawiający informuje, że na nową serwerownię przeznaczył pomieszczenia nr 001 (103 na rysunku w załączniku) o łącznej powierzchni około 18,2 m^2 i zlokalizowane na parterze budynku Urzędu Miasta przy ul. Rynek 2.

Pomieszczenie te obecnie mają charakter magazynowy i wymagają dostosowania do planowanej funkcjonalności. Wysokość pomieszczeń ponad 3m, nośność stropu wynosi 300kg na 1 m^2, co Wykonawca musi uwzględnić przy planowaniu podłogi technicznej oraz rozmieszczeniu szaf teleinformatycznych.

Gabaryty oraz lokalizacje pomieszczeń przedstawiono na rzucie z rysunku poniżej (bardziej szczegółowy rzut całego piętra na rysunku nr 4.0 z załącznika):



Rysunek 4: Rzut pomieszczeń na planowaną serwerownie z zaznaczeniem istniejącej serwerowni (proszę dosłać rzut parteru budynku)

Zamawiający informuje, że istotnymi utrudnieniami które Wykonawca musi uwzględnić w pracach projektowych i wykonawczych, będą:

- konieczność wykonania łącznika światłowodowego pomiędzy serwerowniami tj. obecną lokalizacją starej serwerowni oraz nowym pomieszczeniem nr 001 z wykorzystaniem podpiwniczenia – brak możliwości przejścia reprezentacyjnym korytarzem wejściowym Urzędu Miasta;
- konieczność wykonania przyłącza energetycznego z rozdzielnicy energetycznej znajdującej się w budynku B Urzędu Miasta w przewiązce miedzy budynkami Urzędu Miasta co wiązać się może z koniecznością wykonania przewiertu / przecisku między budynkami (brak możliwości przejścia korytarzem łącznikowym). Inną możliwością jest wykonanie odrębnego przyłącza energetycznego poprzez zbudowaną kanalizację pierwotną Zamawiającego na odcinku Urząd Miasta – GPZ, jednakże do Wykonawcy w tym przypadku należeć będzie pozyskanie zgody Zakładu Energetycznego oraz wszelkich pozwoleń wraz z poniesieniem kosztów wykonania takiego przyłącza.

- brak zgody na posadowienie jednostek klimatyzatorów na ścianie elewacyjnej i bocznej Urzędu Miasta, co może skutkować koniecznością prowadzenia rurek z cieczą chłodniczą na dużą odległość na tylną elewację budynku lub poprzez dostępne szyby wentylacyjne – na dach budynku.
- mała ilość miejsca na agregat i wąskie korytarze oraz drzwi, które mogą utrudniać montaż urządzenia w pomieszczeniach podpiwniczenia. Istotnym problemem może być również odpowiednie zaprojektowanie i zabezpieczenie prawidłowego układu wentylacji i wyrzutu spalin.
- zabytkowy i reprezentacyjny charakter budynku Urzędu Miasta objętego nadzorem konserwatorskim.

W celu oszacowania wszystkich możliwych zagrożeń Zamawiający oczekuje, że Wykonawca dokona wizji lokalnych przed złożeniem oferty.

Opisane wyżej wymagania, koncepcje i opisy bardziej szczegółowe w Załączniku D i E – stanowią jedynie opis wymagań minimalnych wobec tego węzła sieci. Zadaniem Wykonawcy jest zaprojektowanie i wykonanie kompletnej serwerowni zgodnie z regułami sztuki inżynierskiej.

2.4. Zadania Wykonawcy związane z wdrożeniem warstwy aktywnej sieci miejskiej

W celu realizacji zadań stawianych przed infrastrukturą aktywną i pasywną projektowanej Miejskiej Sieci Szerokopasmowej oraz w oparciu o doświadczenia rynkowe, referencje z wdrożonych podobnych projektów sieci miejskich i analizę dostępnych technologii budowy sieci miejskich należy uznać, iż technologią gwarantującą odpowiednią niezawodność, skalowalność i możliwości zarządzania rozległą siecią miejską będzie technologia **Ethernet.** Stad też zaproponowane urządzenia aktywne oraz zastosowane rozwiązania dla sieci miejskiej w Żywcu powinny bazować na tej technologii.

Zadaniem Wykonawcy będzie wdrożenie i zainstalowanie urządzeń warstwy aktywnej, a w szczególności:

- dostawa urządzeń aktywnych do poszczególnych warstw sieciowych dobranych pod kątem wydajności, ilości i rodzaju portów światłowodowych i miedzianych o odpowiedniej prędkości transmisji;
- instalacja urządzeń w szafach teleinformatycznych jednostek węzłowych;
- wykonanie wszystkich połączeń niezbędnych do utworzenia wymaganej topologii sieci miejskiej i połączeń zgodnie z przyjętym modelem atomowym połączeń oraz z przepustowością przyporządkowaną do danego typu punktu;
- konfiguracja urządzeń aktywnych i przystosowanie ich do scentralizowanego zarządzania poprzez stanowiska administratorów w Centrum Zarządzania Siecią;
- zaprojektowanie i konfiguracja wydzielonych, bezpiecznych sieci VPN obejmujących poszczególne grupy użytkowników sieci miejskiej (szkolnictwo, wydzielone sieci Urzędu Miasta, etc) ze szczególnym naciskiem na zabezpieczenie transmisji systemów przetwarzających dane osobowe i niejawne;
- zaprojektowanie i konfiguracja wydzielonych, bezpiecznych sieci VPN oraz implementacja mechanizmów zapewnienia jakości transmisji QoS dla sieci transmisji pakietów telefonii IP;
- testy wydajnościowe i sprawdzające działanie całego systemu
- przeszkolenie 3 pracowników - przyszłych administratorów sieci wyznaczonych przez Zamawiającego.

2.4.1. Ogólny opis architektury warstwy aktywnej sieci miejskiej

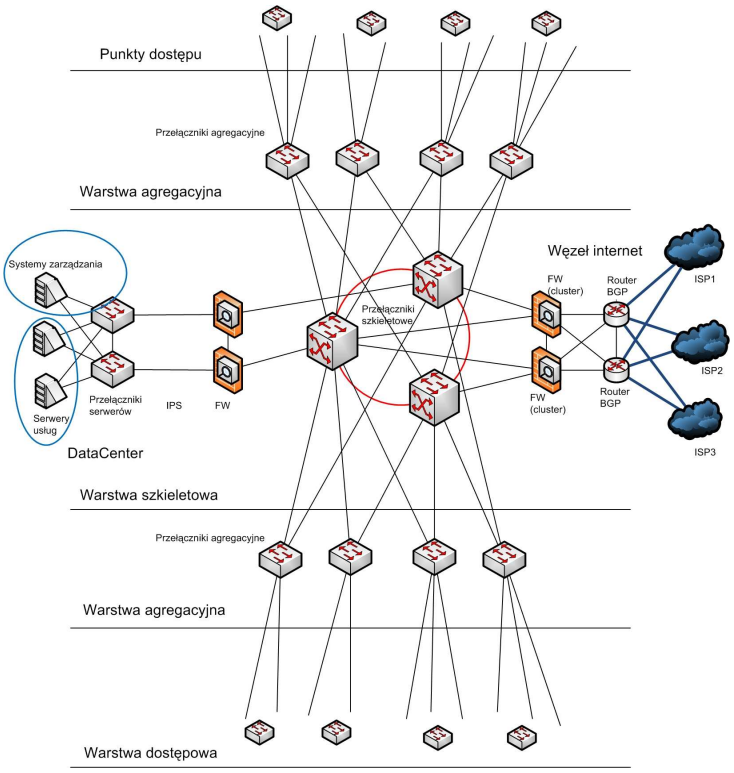
Proponowane rozwiązanie bazuje na podzieleniu sieci na warstwy funkcjonalne aczkolwiek nie wszystkie warstwy będą występowały w bieżącej fazie projektu z uwagi na niedużą liczbę punktów sieci. W sieci o proponowanej strukturze wyodrębnić można punkty charakterystyczne takie jak:

- Węzły rdzeniowe – ich głównym zadaniem jest jak największy, niezawodny i zapewniający właściwą jakość usług transport danych między kluczowymi punktami sieci miejskiej
- Węzły agregujące – mają na celu szybkie i niezawodne przesyłanie danych przy zachowaniu odpowiednich parametrów jakości usług jak również agregacje ruchu z węzłów końcowych. W pierwszej fazie projektu nie przewidziano ich zastosowania, pojawią się w LPD dopiero wraz z rozbudową ilości punktów końcowych przyłączanych do danego punktu LPD.
- Centrum Przetwarzania Danych – będące centralną bazą danych niezbędnych dla efektywnej pracy JST oraz dla aplikacji miejskich (opcja rozbudowy w kolejnych etapach, projekt takiego węzła stanowi działanie komplementarne realizowane np. z Działania 2.2 Rozwój usług elektronicznych)
- Centrum Zarządzania Siecią – będące segmentem, w którym zlokalizowane będą interfejsy zarządzające wykorzystywanych urządzeń, dodatkowo będą zlokalizowane serwery z oprogramowaniem zarządzającym oraz stacje zarządzające, z których to odbywać się będzie zarządzanie i monitorowanie sieci
- Styk z siecią Internet – jego zadaniem jest zapewnić bezpieczny i niezawodny dostęp do sieci Internet, realizowany będzie w postaci min. 2 punktów styku do Internetu (IXS) oraz urządzeń wysokowydajnej bramy dostępu sieci miejskiej do Internetu (IXC).
- Punkty styku z Operatorami – węzły pasywne dostępu do kanalizacji teletechnicznej lub włókien światłowodowych.

Zastosowanie takiego podziału pozwala w prosty i czytelny sposób zorganizować ruch w sieci oraz sprawnie i skutecznie monitorować jej działanie oraz nią zarządzać. Architektura warstwowa, modułowość urządzeń oraz

zastosowane rozwiązania w organizacji segmentu światłowodowego pozwalają na rozbudowę sieci miejskiej w miarę rosnących potrzeb bez zbytniego obciążania budżetu miasta wysokimi nakładami początkowymi.

Polaczenia sieciowe miedzy urządzeniami prowadzone będą siecią światłowodową. Organizacja segmentu światłowodowego i wg schematu rozpływu włókien. Strukturę logiczną sieci w postaci modelu atomowego połączeń międzywęzłowych przedstawiono na powyższym rysunku (jest to schemat docelowy, w obecnej wersji na etapie I budowy sieci występować będzie znaczące uproszczenie do 1 przełącznika szkieletowego).



Rysunek 5: Schemat docelowej struktury aktywnej sieci miejskiej Żywiec

2.4.2. Ogólne założenia dla doboru urządzeń aktywnych do sieci miejskiej

Na etapie doboru urządzeń aktywnych przyjąć należy następujące założenia techniczne:

- Celem projektu jest zbudowanie wysokowydajnej i wysoko redundantnej sieci rdzeniowej i agregacyjnej w technologii Ethernet, w której węzły dystrybucyjne połączone będą łączami o przepustowości 10Gb/s na bazie budowanej obecnie infrastruktury światłowodowej
- Zaplanowano występowanie redundancji połączeń między węzłami
- Przewidziano możliwość podłączenia dużej ilości punktów końcowych łączami 1Gb/s bezpośrednio z węzłów agregacyjnych i rdzeniowych do punktów dostępowych, przy czym występować będzie ograniczenie pasma przypadającego na punkt dostępowy do wartości wynikającej z kategorii użytkownika (jego zapotrzebowania na pasmo).
- Dostęp do Internetu (styk z innymi operatorami) powinien być zabezpieczony poprzez urządzenia firewall typu stateful oraz powinien charakteryzować się redundancją. Urządzenia punktu styku i topologia podłączenia powinny umożliwić rozbudowę przepustowości i możliwość korzystania z wielu operatorów zewnętrznych.
- W jednym z węzłów rdzeniowych powinny być przewidziane urządzenia umożliwiające podłączenie miejskiego Centrum Zarządzania Siecią połączonego z funkcjonalnością Operatorskiego Punktu Styku z Internetem
- Przygotowanie sieci pod realizację aplikacji głosowych w oparciu o technologię VoIP.

- Przygotowanie sieci dla realizacji aplikacji wymagających sieci szerokopasmowych np. e-learning z wykorzystaniem Video, Telemedycyna a także do wykorzystania sieci i jej urządzeń do nowoczesnych technologii rozsyłania telewizji TVoIP z wykorzystaniem multicastów.
- Przygotowanie narzędzi zarządzających dla wdrażanych urządzeń sieciowych.
- Przygotowanie sieci do jednoczesnej obsługi protokołu IPv4 i IPv6 w celu umożliwienia migracji sieci do rozwijanego obecnie standardu IPv6.
- Cała projektowana sieć powinna być w sposób łatwy i spójny zarządzana centralnie przez jednostkę administrującą, co oznacza, że urządzenia będące punktami dostępowymi powinny być również łatwo zarządzane przez operatora. Sieci lokalne istniejące w budynku lub budowane w przyszłości powinny być dołączane przez łącza typu uplink do urządzeń dostępowych sieci.
- Funkcjonalność urządzeń powinna umożliwiać wirtualizację i separację wielu sieci LAN na terenie miasta na współdzielonej infrastrukturze. Dodatkowo urządzenia umożliwią zapewnienie odpowiedniego poziomu bezpieczeństwa (bezpieczne kanały VPN), w szczególności dostępu do usług zarządzanych centralnie (Centrum Danych, Internet, Firewall i inne). Urządzenia użyte do budowy infrastruktury sprzętowej w rdzeniu sieci powinny zapewniać bardzo dużą wydajność i przepustowość, sprzętowo wspierać protokół MPLS i VPLS, oraz umożliwiać dostarczanie poziomów jakości usług (Quality of Service) zarówno w modelu Differentiated Services jak i Integrated Services.

Ponadto przy doborze urządzeń należy kierować się następującymi wskazówkami techniczno-inwestycyjnymi:

- **Unifikacja urządzeń** - należy ograniczyć liczbę rodzajów (rodzin) produktów do niezbędnego minimum w celu ograniczenia kosztów szkolenia kadr i utrzymania sieci.
- **Skalowanie urządzeń -** urządzenia powinny umożliwić zwiększenie przepływności na każdym poziomie hierarchii sieci poprzez dołożenie kolejnych interfejsów lub wymianę interfejsów na szybsze. Uwzględniając typowy współczynnik skalowania na poziomie 15% rocznie w perspektywie 5 lat oznacza podwojenie się zapotrzebowania na obsługiwane pasmo.

Kierowanie się powyższymi zaleceniami jest krytyczne, ponieważ pozwala na uzyskanie znaczących oszczędności w eksploatacji sieci (niższe koszty serwisowania, rekonfiguracji, zarządzania, wdrażania nowych usług etc.).

Połączenia pomiędzy poszczególnymi węzłami sieci charakteryzować się będą różną przepustowością zależną od miejsca węzła w strukturze sieci oraz wymaganej pojemności, przy czym zalecaną przepustowością minimalną przypadającą na węzeł końcowy jest pasmo pozwalające na świadczenie usług NGA/NGN określona na ten moment na 40Mb/s. Za wystarczającą przepustowość dla obiektów o małym zapotrzebowaniu na pasmo przyjęto jednak za wystarczającą przepustowość 10Mb/s.

Zadaniem Wykonawcy będzie wykonanie tych połączeń zgodnie z tabelą zapotrzebowania na pasmo Informacje o oczekiwanej przepływności przyporządkowanej dla poszczególnych punktów zawiera tabela listy wszystkich punków sieci miejskiej (załącznik A).

2.4.3. Wymagania dla urządzeń rdzenia sieci

Podstawową rolą węzłów rdzeniowych jest wysoko niezawodne i bardzo wydajne przełączanie bardzo dużych ilości ruchu przy zapewnieniu odpowiedniego poziomu bezpieczeństwa i jakości usług. Dodatkowo rdzeń sieci będzie także kierował ruch do/z styku z Internetem oraz do/z miejskiego Centrum Zarządzania / Centrum Danych. W początkowym etapie budowy sieci miejskiej przewiduje się zastosowanie **1 urządzenia rdzeniowego** posiadającego w pełni redundantne elementy, ulokowanego w Głównym Punkcie Dystrybucji. Do realizacji ww. redundancji dopuszcza się również wykorzystanie dwóch urządzeń sieciowych w klastrze, które wspólnie będą tworzyły jedno urządzenie logiczne, stanowiące rdzeń sieci.

Obecny projekt obejmuje wdrożenie pojedynczego węzła rdzeniowego oraz zakłada brak węzłów agregacyjnych. Jednak ze względu na planowany, dalszy rozwój sieci, urządzenie rdzeniowe powinno już na tym etapie zapewniać możliwość połączenia z węzłami rdzeniowymi i agregacyjnymi linkami o przepustowości 10 Gb/s, bez potrzeby wymiany lub dokupienia nowych modułów (za wyjątkiem wkładek modułów transmisyjnych).

Dalsza rozbudowa systemu powinna przebiegać poprzez rozbudowę kart urządzeń rdzeniowych (z kontrolą wydajności urządzenia), zwiększenie liczby urządzeń agregujących i dostępowych. Lokalizacja urządzeń na terenie miasta,

odpowiednio pojemna kanalizacja światłowodowa oraz zasięg 10km możliwy do osiągnięcia z standardowo stosowanych modułów światłowodowych typu SFP – powoduje, że zasięgiem sieci może zostać objęte całe miasto.

Po rozbudowie o kolejne dwa urządzenia rdzeniowe, połączenia między urządzeniami rdzeniowymi przyjmą topologię pierścienia, a po dalszym zwiększeniu ilości węzłów powyżej 3 zaleca się zastosowanie topologii „każdy z każdym” (ang.full mesh). Zastosowane urządzenia muszą umożliwiać rozbudowę do tej funkcjonalności.

Warstwa rdzeniowa będzie odpowiadać za transport całości ruchu pomiędzy poszczególnymi fragmentami sieci, oraz za komunikację z Centrum Zarządzania Siecią i Operatorskim Stykiem z Internetem. Kluczowym parametrem, jakim muszą charakteryzować się urządzenia w tej warstwie jest wydajność i wysoka niezawodność.

Urządzenia rdzeniowe poza kryterium gęstości portów, które determinuje zastosowanie określonych grup urządzeń muszą charakteryzować się pewnymi właściwościami. Przyjęto, iż urządzenia sieciowe rdzenia powinny spełniać następujące wymagania:

2.4.3.1. Wymagania ogólne dla urządzeń rdzenia sieci

Wymagania ogólne stawiane węzłom rdzeniowym to:

- Wysoka wydajność potrzebna do obsłużenia połączenia 10 Gb/s i 1 Gb/s w technologii Ethernet, wsparcie dla Quality of Service oraz możliwość kontroli ruchu przy wykorzystaniu list ACL. Oczekiwana wydajność przełącznika rdzeniowego nie może być mniejsza aniżeli sumaryczna prędkość transmisji ze wszystkich węzłów agregacyjnych i dostępowych.
- Wysoka niezawodność i redundancja – awaria któregokolwiek elementu urządzenia rdzeniowego nie może prowadzić do zmniejszenia jego funkcjonalności lub wydajności. Dopuszczalne jest jedynie odcięcie nieredundantnie podłączonych urządzeń agregacyjnych lub dostępowych, jeżeli awarii uległ moduł interfejsów sieciowych.
- Ciągłość działania i dostarczania usług sieciowych poprzez możliwość wymiany modułów w czasie pracy urządzenia (Hot-swap). Dotyczy to zasilaczy, modułów zarządzających, kart liniowych, paneli z wentylatorami etc. W przypadku urządzeń pracujących w systemie wirtualizacji, wymagana jest możliwość wymiany uszkodzonego urządzenia bez przerywania pracy klastra.
- Powinny w znaczący sposób zmniejszać czas konwergencji (odbudowy połączeń logicznych) w przypadku przerwy w transmisji.
- Możliwość wyposażenia w nie mniej niż 8 interfejsów 10Gb/s na kartę liniową lub urządzenie logiczne
- Możliwość wyposażenia w nie mniej niż 24 interfejsy 1Gb/s na kartę liniową lub urządzenie logiczne
- Zapewnienie możliwość rozbudowy o nowe interfejsy, poprzez zwiększenie ilości kart liniowych lub liczby urządzeń w klastrze
- Sieć na poziomie węzłów rdzeniowych powinna umożliwiać wprowadzenie centralnego, jednolitego systemu monitoringu w czasie rzeczywistym i zarządzania.
- Urządzenia powinny wspierać technologię tunelowania ramek Ethernetowych Q-in-Q, która zostanie wykorzystana na połączeniach z przełącznikami dostępowymi.
- Urządzenia powinny wspierać technologie tunelowania MPLS i VPLS, które zostaną wykorzystane w przyszłości, na połączeniach z przełącznikami rdzeniowymi i agregacyjnymi.
- Urządzenie musi mieć możliwość montażu w szafie 19”.

W szczególności minimalne parametry węzła rdzeniowego powinny odpowiadać parametrom przełącznika rutującego, wyposażonego **w 48 portów 1Gb/s SFP oraz 8 portów 10Gb/s SFP+.** Porty przełącznika należy wyposażyć w odpowiednią liczbę modułów SFP oraz SFP+ w liczbie potrzebnej do wykonania połączeń sieciowych przewidzianych w danym węźle rdzeniowym. Urządzenie może składać się z dwóch przełączników fizycznych, tworzących razem jeden przełącznik logiczny stanowiący węzeł rdzeniowy.

Minimalne wymagania przełącznika węzła rdzeniowego (SW-MGR):

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack. 2. Urządzenie musi posiadać redundantny zasilacz. 3. Urządzenie musi obsługiwać minimum 32 tysięcy adresów MAC. 4. Urządzenie musi mieć możliwość obsługi 16 tysięcy adresów IPv4. 5. Urządzenie musi mieć możliwość łączenia w grupę od dwóch do dziewięciu urządzeń, tworzących wspólnie jedno urządzenie logiczne. Z punktu zarządzania i innych urządzeń sieciowych, działające w tym trybie urządzenia mają być widoczne jako jedno urządzenie. Urządzenie musi mieć możliwość wykorzystania portów 10Gb/s w celu utworzenia połączeń miedzy przełącznikami, które mają stanowić jedno urządzenie logiczne lub zastosowanie rozwiązanie równoważnego wykorzystującego przełącznik modularny z min 9 slotami na karty liniowe.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad z możliwością balansowania ruchu ze względu na hash nagłówków L2, L3, L4. Urządzenie musi obsługiwać agregację portów na tym samym lub innym urządzeniu z tego samego virtual chassis. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły i podsieci IP. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP. 3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1d, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad. 6. Urządzenie musi obsługiwać standard 802.3x. 7. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag. 8. Urządzenie musi obsługiwać protokół redundancji dedykowany dla topologii pierścienia. 9. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3, 802.3u, 802.3z, 802.3ab, 802.3ae (technologie 10Base-T, 100Base-T, 1000BASE-X, 1000BaseT, 10Gbase). 10. Urządzenie musi mieć możliwość obsługi technologii Power over Ethernet (IEEE 802.3af). 11. Urządzenie musi obsługiwać ramki Jumbo. 12. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol). 13. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową, multicastową oraz unknown unicast. 14. Urządzenie musi obsługiwać technologie SuperVLAN (VLAN Aggregation). 15. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring). 16. Możliwość automatycznej priorytetyzacji ruchu VoIP.
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać następujące protokoły routingu IPv4: RIPv1/v2, IS-IS, OSPF oraz BGPv4 wraz z obsługą Graceful Restart oraz musi pozwalać na routing oparty o polityki (policy based routing). 2. Urządzenie musi mieć możliwość filtrowania i redystrybucji tras między różnymi protokołami routingu. 3. Konieczna jest obsługa equal-cost route (technologia znana również pod nazwą Equal-cost Multi-path). 4. Urządzenie musi obsługiwać następujące protokoły routingu IPv6: RIPng, OSPFv3, IS-ISv6, MP-BGP. 5. Urządzenie musi obsługiwać protokół VRRP zarówno dla IPv4 jak i IPv6. 6. Urządzenie musi obsługiwać protokół ICMPv6 wraz z ICMPv6 rediretion. 7. Urządzenie musi obsługiwać tunelowanie ruchu IPv6: tunel ręczny (manual) oraz tunel 6to4. Konieczna jest też obsługa translacji adresów ISATAP oraz jednoczesnego korzystania ze stosów IPv4 i IPv6. 8. Urządzenie musi obsługiwać protokół BFD w celu zminimalizowania czasu wykrycia zmiany topologii i przyspieszenia konwergencji protokołów IS-IS, OSPF, BGP. Protokół BFD musi mieć również możliwość współpracy z mechanizmem Fast Reroute dla protokołu MPLS.
IV. Obsługa ruchu multicastowego:
1. Urządzenie musi obsługiwać następujące protokoły routingu multicastowego: PIM-SM, PIM-DM, PIM-SSM, PIM-SMv6, PIM-DMv6, PIM-SSMv6. 2. Urządzenie musi obsługiwać protokoły IGMPv1/v2/v3 wraz z możliwością nasłuchu (IGMPv1/v2/v3 Snooping). 3. Urządzenie musi obsługiwać protokół MLDv2 wraz z możliwością nasłuchu (MLDv2 snooping) – jest to odpowiednik IGMP dla protokołu IPv6. 4. Urządzenie musi obsługiwać protokół MSDP pozwalający na wymianę informacji o źródłach multicastowych między różnymi domenami administracyjnymi oraz wspierać technologię AnyCast-RP.
V. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia. 3. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu). 4. Urządzenie musi mieć możliwość zliczania ruchu (traffic accounting). 5. Interfejsy muszą obsługiwać kolejki typu SP, WRR, WDRR, WFQ, SP+WDRR (lub równoważne) w ilości minimum 8 kolejek na port. Dodatkowo wymagane są mechanizmy ochrony przed przepełnieniem kolejki typu Tail-Drop oraz WRED. 6. Urządzenie musi obsługiwać mechanizmy kształtowania ruchu typu traffic shaping i traffic policing. 7. Urządzenie musi obsługiwać klasyfikację ruchu na podstawie pola ToS nagłówka IPv4 (w standardzie DSCP), portu ingrees, adresu MAC, adresu IP oraz portu TCP/UDP.
VI. Obsługa MPLS i VPLS:
1. Urządzenie musi obsługiwać technologie Layer 3 MPLS VPN oraz Layer 2 MPLS VPN. 2. Urządzenie musi posiadać możliwość jednoczesnego tworzenia połączeń VLL przy użyciu sygnalizacji BGP (draft Kompella) jak i sygnalizacji LDP (draft Martini) na tym samym interfejsie. 3. Urządzenie musi mieć możliwość obsługi protokołów MPLS i LDP na wirtualnych interfejsach VLAN (interfejs VLAN warstwy trzeciej). 4. Urządzenie musi obsługiwać technologie Hierarchial VPLS, również z dostępem typu QinQ (QinQ access). 5. Urządzenie musi obsługiwać technologie MCE (Multi-CE), która pozwala urządzeniu funkcjonować jako urządzenie Customer Edge dla wielu instancji VPN.

6.	Urządzenie musi obsługiwać technologię MPLS Traffic Engineering przy użyciu protokołu RSVP-TE.
VII. Bezpieczeństwo:	
1.	Urządzenie musi obsługiwać standard IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN.
2.	Urządzenie musi mieć możliwość kontroli adresów MAC urządzeń, które mają mieć możliwość komunikacji poprzez dany interfejs.
3.	Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC.
4.	Urządzenie musi zezwalać na autentykację MD5 przynajmniej dla protokołów OSPF, RIPv2 oraz BGP.
5.	Urządzenie musi posiadać mechanizmy ochronne przed atakami typu IP Spoofing oraz ARP Poisoning i obsługiwać technologię uRPF.
VIII. Zarządzanie:	
1.	Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv1.5 lub SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.
2.	Urządzenie musi mieć możliwość pracowania jako klient lub serwer FTP, klient TFPT, oraz obsługiwać protokół XMODEM, YMODEM lub ZMODEM.
3.	Urządzenie musi zezwalać na autentykację użytkowników zarządzających urządzeniem przy użyciu lokalnej bazy danych, serwera Radius oraz serwera TACACS+.
4.	Urządzenie musi mieć możliwość konfiguracji różnych uprawnień dostępu dla różnych użytkowników zarządzających.
5.	Urządzenie musi obsługiwać protokoły SNMPv1, SNMPv2, SNMPv3 oraz RMON.
6.	Urządzenie musi wspierać generowanie statystyk ruchu przy użyciu protokołu NetFlow (lub równoważnego).
7.	Urządzenie musi wspierać protokół NTP.
8.	Urządzenie musi obsługiwać komendy z rodziny trace route dla protokołów IPv4, IPv6, tras multicastowych oraz ścieżek MPLS LSP.
9.	Urządzenie musi obsługiwać technologię hot patching umożliwiającą aktualizację oprogramowania urządzenia bez przerwy w jego funkcjonowaniu.
10.	Urządzenie musi mieć możliwość szczegółowej kontroli pracy urządzenia (debugging), zbierania logów z pracy urządzenia oraz wysyłania ich na zdalny serwer.
11.	Urządzenie musi mieć możliwość przechowywania wielu wersji oprogramowania na przełączniku
12.	Urządzenie musi mieć możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość wysłania i pobrania konfiguracyjnego w postaci tekstowej ze stacji roboczej.

2.4.4. Wymagania dla urządzeń warstw dystrybucji (urządzenia agregujące)

Warstwa dystrybucyjna będzie odpowiadać za transport ruchu z poszczególnych przełączników warstwy dostępowej do szkieletu sieci. Warstwa ta realizuje agregację ruchu pochodzącego od użytkowników końcowych, skierowanego do innych segmentów sieci. Podstawowym zadaniem urządzeń agregujących jest podłączenie od kilkunastu do kilkudziesięciu urządzeń dostępowych do rdzenia sieci. Liczba i rozmieszczenie punktów dystrybucyjnych muszą być dopasowane do przewidywanej ilości użytkowników, którzy będą podłączeni do sieci oraz rozmieszczenia geograficznego skupisk użytkowników.

Na tym etapie realizacji projektu nie przewidziano zastosowania urządzeń agregacji, jednak plany rozwoju sieci przewidują wprowadzenie warstwy dystrybucji. Założenia przewidują podłączenie do urządzeń rdzeniowych przy pomocy światłowodowego łącza o przepustowości 10Gb/s z dodatkowym połączeniem redundantnym do drugiego urządzenia rdzeniowego o przepustowości 1Gb/s.

W przypadku rozbudowy sieci o węzły agregacyjne minimalne parametry urządzenia agregującego powinny odpowiadać parametrom zintegrowanego przełącznika wyposażonego w możliwość zainstalowania 24 x modułów 1Gb/s SFP oraz do 4 opcjonalnych modułów 10Gb/s SFP+

Minimalne wymagania przełącznika węzła agregacyjnego (SW-AGR):

I. Podstawowe parametry urządzenia:	
1.	Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, o wysokości nie większej niż 1U.
2.	Urządzenie musi być wyposażone w redundantne zasilacze.
3.	Urządzenie musi posiadać backplane o wydajności minimum 208Gb/s.
4.	Urządzenie musi być wyposażone w minimum 24 porty 1Gb/s SFP oraz 4 porty 10Gb/s SFP+.
5.	Urządzenie musi posiadać teoretyczną wydajność przełączania minimum 155 Mpps.
6.	Urządzenie musi obsługiwać minimum 32 tysięcy adresów MAC.
7.	Urządzenie musi mieć możliwość obsługi 16 tysięcy adresów IPv4.
8.	Urządzenie musi mieć możliwość łączenia w grupę od dwóch do dziewięciu urządzeń, tworzących wspólnie jedno urządzenie logiczne. Z punktu zarządzania i innych urządzeń sieciowych, działające w tym trybie urządzenia mają być widoczne jako jedno urządzenie. Urządzenie musi mieć możliwość wykorzystania portów 10-gigowych w celu utworzenia połączeń miedzy przełącznikami, które mają stanowić jedno urządzenie logiczne.
9.	Urządzenie musi posiadać slot rozszerzeń pozwalający wyposażyć urządzenie w moduł posiadający 4 porty 10Gb/s SFP+ lub w moduł posiadający 16 portów 1Gb/s SFP.
II. Usługi warstwy drugiej:	
1.	Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad z możliwością balansowania ruchu ze względu na hash nagłówków L2, L3, L4. Urządzenie musi obsługiwać agregację portów na tym samym lub innym urządzeniu z tego samego virtual chassis.
2.	Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły i podsieci IP. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP.
3.	Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p.

4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1d, 802.1w oraz 802.1s.
5. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad.
6. Urządzenie musi obsługiwać standard 802.3x.
7. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag.
8. Urządzenie musi obsługiwać protokół redundancji dedykowany dla topologii pierścienia.
9. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3, 802.3u, 802.3z, 802.3ab, 802.3ae (technologie 10Base-T, 100Base-T, 1000BASE-X, 1000BaseT, 10Gbase).
10. Urządzenie musi mieć możliwość obsługi technologii Power over Ethernet (IEEE 802.3af).
11. Urządzenie musi obsługiwać ramki Jumbo.
12. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol).
13. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową, multicastową oraz unknown unicast.
14. Urządzenie musi obsługiwać technologie SuperVLAN (VLAN Aggregation).
15. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring).
16. Możliwość automatycznej priorytetyzacji ruchu VoIP.

III. Usługi warstwy trzeciej:

1. Urządzenie musi obsługiwać następujące protokoły routingu IPv4: RIPv1/v2, IS-IS, OSPF oraz BGPv4 wraz z obsługą Graceful Restart oraz musi pozwalać na routing oparty o polityki (policy based routing).
2. Urządzenie musi mieć możliwość filtrowania i redystrybucji tras między różnymi protokołami routingu.
3. Konieczna jest obsługa equal-cost route (technologia znana również pod nazwą Equal-cost Multi-path).
4. Urządzenie musi obsługiwać następujące protokoły routingu IPv6: RIPng, OSPFv3, IS-ISv6, MP-BGP.
5. Urządzenie musi obsługiwać protokół VRRP zarówno dla IPv4 jak i IPv6.
6. Urządzenie musi obsługiwać protokół ICMPv6 wraz z ICMPv6 rediretion.
7. Urządzenie musi obsługiwać tunelowanie ruchu IPv6: tunel ręczny (manual) oraz tunel 6to4. Konieczna jest też obsługa translacji adresów ISATAP oraz jednoczesnego korzystania ze stosów IPv4 i IPv6.
8. Urządzenie musi obsługiwać protokół BFD w celu zminimalizowania czasu wykrycia zmiany topologii i przyspieszenia konwergencji protokołów IS-IS, OSPF, BGP. Protokół BFD musi mieć również możliwość współpracy z mechanizmem Fast Reroute dla protokołu MPLS.

IV. Obsługa ruchu multicastowego:

1. Urządzenie musi obsługiwać następujące protokoły routingu multicastowego: PIM-SM, PIM-DM, PIM-SSM, PIM-SMv6, PIM-DMv6, PIM-SSMv6.
2. Urządzenie musi obsługiwać protokoły IGMPv1/v2/v3 wraz z możliwością nasłuchu (IGMPv1/v2/v3 Snooping).
3. Urządzenie musi obsługiwać protokół MLDv2 wraz z możliwością nasłuchu (MLDv2 snooping) – jest to odpowiednik IGMP dla protokołu IPv6.
4. Urządzenie musi obsługiwać protokół MSDP pozwalający na wymianę informacji o źródłach multicastowych między różnymi domenami administracyjnymi oraz wspierać technologię AnyCast-RP.

V. Filtrowanie i kształtowanie ruchu:

1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6.
2. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia.
3. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu).
4. Urządzenie musi mieć możliwość zliczania ruchu (traffic accounting).
5. Interfejsy muszą obsługiwać kolejki typu SP, WRR, WDRR, WFQ, SP+WDRR (lub równoważne) w ilości minimum 8 kolejek na port. Dodatkowo wymagane są mechanizmy ochrony przed przepełnieniem kolejki typu Tail-Drop oraz WRED.
6. Urządzenie musi obsługiwać mechanizmy kształtowania ruchu typu traffic shaping i traffic policing.
7. Urządzenie musi obsługiwać klasyfikację ruchu na podstawie pola ToS nagłówka IPv4 (w standardzie DSCP), portu ingrees, adresu MAC, adresu IP oraz portu TCP/UDP.

VI. Obsługa MPLS i VPLS:

1. Urządzenie musi obsługiwać technologie Layer 3 MPLS VPN oraz Layer 2 MPLS VPN.
2. Urządzenie musi posiadać możliwość jednoczesnego tworzenia połączeń VLL przy użyciu sygnalizacji BGP (draft Kompella) jak i sygnalizacji LDP (draft Martini) na tym samym interfejsie.
3. Urządzenie musi mieć możliwość obsługi protokołów MPLS i LDP na wirtualnych interfejsach VLAN (interfejs VLAN warstwy trzeciej).
4. Urządzenie musi obsługiwać technologie Hierarchial VPLS, również z dostępem typu QinQ (QinQ access).
5. Urządzenie musi obsługiwać technologie MCE (Multi-CE), która pozwala urządzeniu funkcjonować jako urządzenie Customer Edge dla wielu instancji VPN.
6. Urządzenie musi obsługiwać technologię MPLS Traffic Engineering przy użyciu protokołu RSVP-TE.

VII. Bezpieczeństwo:

1. Urządzenie musi obsługiwać standard IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN.
2. Urządzenie musi mieć możliwość kontroli adresów MAC urządzeń, które mają mieć możliwość komunikacji poprzez dany interfejs.
3. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC.
4. Urządzenie musi zezwalać na autentykację MD5 przynajmniej dla protokołów OSPF, RIPv2 oraz BGP.
5. Urządzenie musi posiadać mechanizmy ochronne przed atakami typu IP Spoofing oraz ARP Poisoning i obsługiwać technologię uRPF.

VIII. Zarządzanie:

1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv1.5 lub SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.
2. Urządzenie musi mieć możliwość pracowania jako klient lub serwer FTP, klient TFPT, oraz obsługiwać protokół XMODEM, YMODEM lub ZMODEM.
3. Urządzenie musi zezwalać na autentykację użytkowników zarządzających urządzeniem przy użyciu lokalnej bazy danych, serwera Radius oraz serwera TACACS+.
4. Urządzenie musi mieć możliwość konfiguracji różnych uprawnień dostępu dla różnych użytkowników zarządzających.
5. Urządzenie musi obsługiwać protokoły SNMPv1, SNMPv2, SNMPv3 oraz RMON.
6. Urządzenie musi wspierać generowanie statystyk ruchu przy użyciu protokołu NetFlow (lub równoważnego).
7. Urządzenie musi wspierać protokół NTP.

8.	Urządzenie musi obsługiwać komendy z rodziny trace route dla protokołów IPv4, IPv6, tras multicastowych oraz ścieżek MPLS LSP.
9.	Urządzenie musi obsługiwać technologię hot patching umożliwiającą aktualizację oprogramowania urządzenia bez przerwy w jego funkcjonowaniu.
10.	Urządzenie musi mieć możliwość szczegółowej kontroli pracy urządzenia (debugging), zbierania logów z pracy urządzenia oraz wysyłania ich na zdalny serwer.
11.	Urządzenie musi mieć możliwość przechowywania wielu wersji oprogramowania na przełączniku
12.	Urządzenie musi mieć możliwość przechowywania wielu plików konfiguracyjnych na przełączniku, możliwość wysłania i pobrania konfiguracyjnego w postaci tekstowej ze stacji roboczej.

2.4.5. Wymagania dla urządzeń warstwy dostępowej

Podstawowym zadaniem węzłów końcowych jest podłączenie istniejących w budynkach punktów dostępowych lokalnych sieci komputerowych LAN. Poczyniono założenie, że we wszystkich obiektach objętych zasięgiem warstwy dystrybucyjnej, dostępne będzie okablowanie UTP kategorii, co najmniej piątej rozszerzonej. Takie okablowanie zapewnia możliwości dostarczenia użytkownikom końcowym interfejsu sieciowego w standardzie FastEthernet o przepływności maksymalnie 100Mb/s w jednym kierunku (200Mb/s full-duplex). Przyjęto również założenie, że większość z punktów dostępowych będzie posiadała własne przełączniki i infrastrukturę aktywną, do której zostaną podłączone porty odpowiedniego przełącznika dostępowego sieci miejskiej.

Urządzenia będą lokalizowane w Punktach Abonenckich oraz w Lokalnych Punktach Dostępowych do obsługi jednostki miejskiej, w której mieści się punkt LPD. Z uwagi na wystarczającą liczbę wolnych portów urządzeń rdzeniowych Punkty Abonenckie lub urządzenia warstwy dostępowej znajdujące się Lokalnych Punktach Dostępowych będzie można terminować również bezpośrednio do portów 1GE w urządzeniu rdzeniowym znajdującym się w GPD dzięki wystarczającemu zasięgowi włókien światłowodowych.

Urządzenia warstwy dostępowej będą połączone z urządzeniami warstwy dystrybucyjnej lub rdzeniowej, w oparciu **o topologię gwiazdy** łączami 1 Gb/s realizowanymi na włóknach jednomodowych kabli światłowodowych. Poszczególni użytkownicy sieci podłączani będą z limitem przepustowości przyjętym do stosowania przez Inwestora zależnym od aktualnego zapotrzebowania użytkownika punktu dostępowego oraz charakteru placówki użytkownika. Na etapie prac koncepcyjnych przewidziano zapotrzebowanie na **23 szt. urządzeń końcowych.**

Dobór typu urządzenia powinien uwzględniać przewidzianą przepustowość wymaganą przez użytkowników w danej jednostce oraz potrzebną liczbę portów 10/100Mb/s lub 10/100/1000Mb/s służących do podłączania komputerów użytkowników lub innych urządzeń sieci lokalnych w danej jednostce samorządowej. W szczególności przewidziano wstępnie zastosowanie:

l.p.	Rodzaj jednostki	Typ przełącznika	Szacowana ilość
1	Urzędy, większe jednostki JST w których występują rozległe sieci lokalne i kilka przełączników własnych użytkownika	Zarządzalny warstwy 2 wyposażony w 24 porty 10/100/1000Mb/s RJ45 + 4 porty 1Gb/s SFP, montowany w racku 19” (SWA-A)	**2 kpl**
2	Szkoły, małe urzędy i jednostki JST w których występują sieci lokalne o niewielkiej liczbie użytkowników	Zarządzalny warstwy 2 wyposażony w 24 porty 10/100Mb/s + 2 porty 1Gb/s SFP, montowany w racku 19” (SWA-B)	**7 kpl**
3	Biblioteki, punkty PIAP, przedszkola i żłobki, najmniejsze urzędy o liczbie użytkowników końcowych < 8 lub 16	Zarządzalny warstwy 2 wyposażony w 8 portów 10/100Mb/s + 1 port 1Gb/s SFP, montowany w racku 19” (SWA-C)	**10 kpl**
4	Wyposażenie punktów PIAP	Mediakonwerter WDM 1 x SFP obudowa stand alone (MC-WDM)	**4 kpl**

Tabela 1. Zestawienie urządzeń dostępowych wg typów urządzeń

Zestawienie lokalizacji wszystkich urządzeń aktywnych warstwy sieciowej (bez urządzeń potrzebnych do realizacji innych podsystemów) wraz z przyporządkowaniem pasma zawiera załącznik A.

Węzły te są częścią sieci miejskiej i powinny być zarządzane przez zespół utrzymania sieci miejskiej. Lokalni administratorzy nie powinni mieć dostępu do tych urządzeń. Tylko w ten sposób można jasno podzielić zakres odpowiedzialności i tym samym w niezawodny sposób dostarczyć usługi sieciowe. W przypadku braku właściwej kadry zarządzającej siecią lokalną (problem ten występuje w części JST) można myśleć o rozwiązaniu pośrednim mając przy tym na uwadze skutki tego rozwiązania oraz fakt, iż dodatkowo obciąży ono pracą zespół centralny.

Zarządzanie przełącznikami warstwy dostępowej powinno być odseparowane od ruchu użytkowników. Powinno to być realizowane przez wprowadzenie podziału na porty użytkownika i porty sieciowe. Zarządzenie przełącznikiem powinno być możliwe tylko poprzez port „sieciowy ” (network interface), wszystkie porty użytkowników muszą być

standardowo wyłączone i nie powinny mieć dostępu do warstwy zarządzania przełącznika. Przełączniki powinny blokować możliwość lokalnego dostępu urządzeń klienckich do siebie nawzajem. Dodatkowo oprogramowanie przełącznika powinno wspierać wiele technologii zwiększających bezpieczeństwo: DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, Storm Control, Port Security, ACLs, 802.1x i inne.

2.4.5.1. Wymagania szczegółowe dla urządzeń warstwy dostępowej

Przełączniki dostępowe z portami Gigabit (10/100/1000Mb/s) powinny być niemodularnymi urządzeniami, przeznaczonymi do montażu w szafach teleinformatycznych, o wysokości nie większej niż 1U. Przełączniki powinny posiadać 24 porty 10/100/1000Mb/s RJ45 oraz 4 porty 1Gb/s SFP. Porty przełącznika należy wyposażyć w jeden moduł 1Gb/s SFP LX (LC) w celu podłączenia do sieci miejskiej.

Minimalne wymagania przełącznika dostępowego o 24 portach downlinkowych 10/100/1000Mb/s (SWA-A):

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, wysokość 1U. 2. Urządzenie musi posiadać 24 porty 10/100/1000Mb/s RJ45 oraz posiadać minimum 4 uplinki 1Gb/s SFP. 3. Urządzenie musi posiadać backplane o wydajności minimum 56Gb/s. 4. Urządzenie musi posiadać wydajność przełączania minimum 41,7 Mpps. 5. Urządzenie musi obsługiwać minimum 8 tysięcy adresów MAC. 6. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 32W. 7. Urządzenie musi być przystosowane do pracy w warunkach biurowych w temperaturach 0-45 stopni Celsjusza i wilgotności 10-90%.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły L3. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP. 3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad. 6. Urządzenie musi obsługiwać standard 802.3x. 7. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag. 8. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3i, 802.3u, 802.3z, (technologie 10Base-T, 100Base-X, 1000Base-X). 9. Urządzenie musi obsługiwać ramki Jumbo. 10. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol) oraz LLDP-MED. 11. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową i multicastową. 12. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring).
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać routing statyczny dla protokołów IPv4 i IPv6. Urządzenie musi wspierać protokół BFD dla tras statycznych. 2. Urządzenie musi posiadać wsparcie dla IPv6, w tym IPv6 Neighbor Discovery, IPv6 Stateless Address Auto-configuration, IPv6 DiffServ Architecture oraz ICMPv6. 3. Urządzenie musi obsługiwać funkcje DHCPv6 client, DHCPv6 relay oraz DHCPv6 server. 4. Urządzenie musi obsługiwać podsłuchiwanie ramek IGMPv1/v2/v3 (IGMPv1/v2/v3 Snooping) oraz MLDv1/v2.
IV. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo. 3. Urządzenie musi mieć możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu). 4. Interfejsy muszą obsługiwać kolejki typu SP, WRR oraz SP+WRR (lub równoważne) w ilości minimum 4 kolejek na port. 5. Urządzenie musi obsługiwać mechanizm kształtowania ruchu typu traffic policing. 6. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, adresów MAC oraz portu wejściowego i wyjściowego.
V. Bezpieczeństwo:
1. Urządzenie musi obsługiwać standard IEEE 802.1x. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN 2. Urządzenie musi pozwalać na autentykację na podstawie adresów MAC.
VI. Zarządzanie:
1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.

Przełączniki dostępowe z portami FastEthernet (10/100Mb/s) powinny być niemodularnymi urządzeniami, przeznaczonymi do montażu w szafach teleinformatycznych, o wysokości nie większej niż 1U. Przełączniki powinny być dostępne w konfiguracji 8 i 24 portowej 10/100Mb/s RJ45 z funkcją AUTO-MDIX, a każdy z modeli powinien być dodatkowo wyposażony w 1 lub 2 porty dual-personality 10/100/1000Mb/s RJ45 lub 1Gb/s SFP, pozwalające na

montaż modułów optycznych. Porty przełącznika należy wyposażyć w przynajmniej jeden moduł 1Gb/s SFP o parametrach transmitera dobranych do budżetu mocy zestawionego toru optycznego.

Minimalne wymagania przełącznika dostępowego o 24 portach downlinkowych 10/100Mb/s (SWA-B):

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, wysokość 1U. 2. Urządzenie musi posiadać 24 porty 10/100Mb/s RJ45 oraz posiadać minimum 2 uplinki 1Gb/s SFP. 3. Urządzenie musi posiadać backplane o wydajności minimum 8,8Gb/s. 4. Urządzenie musi posiadać teoretyczną wydajność przełączania minimum 6,5 Mpps. 5. Urządzenie musi obsługiwać minimum 8 tysięcy adresów MAC. 6. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 13W 7. Urządzenie musi być ciche, pozbawione wentylatorów, przystosowane do pracy w warunkach biurowych w temperaturach 0-45 stopni Celsjusza i wilgotności 10-90%.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły L3. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP. 3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad. 6. Urządzenie musi obsługiwać standard 802.3x. 7. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag. 8. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3i, 802.3u, 802.3z, (technologie 10Base-T, 100Base-X, 1000Base-X). 9. Urządzenie musi obsługiwać ramki Jumbo. 10. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol) oraz LLDP-MED. 11. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową i multicastową. 12. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring).
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać routing statyczny dla protokołów IPv4 i IPv6. Urządzenie musi wspierać protokół BFD dla tras statycznych. 2. Urządzenie musi posiadać wsparcie dla IPv6, w tym IPv6 Neighbor Discovery, IPv6 Stateless Address Auto-configuration, IPv6 DiffServ Architecture oraz ICMPv6. 3. Urządzenie musi obsługiwać funkcje DHCPv6 client, DHCPv6 relay oraz DHCPv6 server. 4. Urządzenie musi obsługiwać podsłuchiwanie ramek IGMPv1/v2/v3 (IGMPv1/v2/v3 Snooping) oraz MLDv1/v2.
IV. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo. 3. Urządzenie musi mieć możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu). 4. Interfejsy muszą obsługiwać kolejki typu SP, WRR oraz SP+WRR (lub równoważne) w ilości minimum 8 kolejek na port. 5. Urządzenie musi obsługiwać mechanizmy kształtowania ruchu typu traffic shaping i traffic policing. 6. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, adresów MAC, portu wejściowego oraz VLANu wejściowego.
V. Bezpieczeństwo:
1. Urządzenie musi obsługiwać standard IEEE 802.1x. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN 2. Urządzenie musi pozwalać na autentykację na podstawie adresów MAC oraz przy użyciu mechanizmu Web-based authentication.
VI. Zarządzanie:
1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.

Minimalne wymagania przełącznika dostępowego o 8 portach downlinkowych 10/100Mb/s (SWA-C):

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, wysokość 1U. 2. Urządzenie musi posiadać 8 portów 10/100Mb/s RJ45 oraz posiadać minimum 1 uplink 1Gb/s SFP. 3. Urządzenie musi posiadać backplane o wydajności minimum 3,6Gb/s. 4. Urządzenie musi posiadać teoretyczną wydajność przełączania minimum 2,6 Mpps. 5. Urządzenie musi obsługiwać minimum 8 tysięcy adresów MAC. 6. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 12W 7. Urządzenie musi być ciche, pozbawione wentylatorów, przystosowane do pracy w warunkach biurowych w temperaturach 0-45 stopni Celsjusza i wilgotności 10-90%.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły L3. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP.

3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad. 6. Urządzenie musi obsługiwać standard 802.3x. 7. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag. 8. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3i, 802.3u, 802.3z, (technologie 10Base-T, 100Base-X, 1000Base-X). 9. Urządzenie musi obsługiwać ramki Jumbo. 10. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol) oraz LLDP-MED. 11. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową i multicastową. 12. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring).
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać routing statyczny dla protokołów IPv4 i IPv6. Urządzenie musi wspierać protokół BFD dla tras statycznych. 2. Urządzenie musi posiadać wsparcie dla IPv6, w tym IPv6 Neighbor Discovery, IPv6 Stateless Address Auto-configuration, IPv6 DiffServ Architecture oraz ICMPv6. 3. Urządzenie musi obsługiwać funkcje DHCPv6 client, DHCPv6 relay oraz DHCPv6 server. 4. Urządzenie musi obsługiwać podsłuchiwanie ramek IGMPv1/v2/v3 (IGMPv1/v2/v3 Snooping) oraz MLDv1/v2.
IV. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo. 3. Urządzenie musi mieć możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu). 4. Interfejsy muszą obsługiwać kolejki typu SP, WRR oraz SP+WRR (lub równoważne) w ilości minimum 8 kolejek na port. 5. Urządzenie musi obsługiwać mechanizmy kształtowania ruchu typu traffic shaping i traffic policing. 6. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, adresów MAC, portu wejściowego oraz VLANu wejściowego.
V. Bezpieczeństwo:
1. Urządzenie musi obsługiwać standard IEEE 802.1x. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN 2. Urządzenie musi pozwalać na autentykację na podstawie adresów MAC oraz przy użyciu mechanizmu Web-based authentication.
VI. Zarządzanie:
1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.

2.4.6. Wymagania związane z organizacją przepływu danych

W Miejskiej Sieci Szerokopasmowej Żywiec ważnym elementem bezpieczeństwa oraz zarządzania transmisjami sieciowymi w strukturze całej sieci będą zagadnienia związane z tworzeniem i konfiguracją tuneli grupujących ruch poszczególnych jednostek, przy wykorzystaniu wirtualnych sieci prywatnych (VPN).

Urządzenia warstwy aktywnej Miejskiej Sieci Szerokopasmowej Żywiec w początkowym etapie powinny realizować grupowanie i tunelowanie ruchu oparte o podwójna enkapsulacje 802.1Q (Q-in-Q). Enkapsulacja Q-in-Q pozwala na tworzenie niezależnych, odseparowanych od siebie sieci wirtualnych, współdzielących te same urządzenia aktywne. Za pomocą Q-in-Q dostawcy usług sieciowych mogą separować klientów za pomocą oddzielnych sieci VPN pozwalając im jednocześnie na tworzenie i tunelowanie własnych sieci VLAN poprzez strukturę dostawcy.

Wraz z rozwojem projektu będą powstawały kolejne węzły rdzeniowe i dystrybucyjne, które mają wspólnie powinny utworzyć chmurę MPLS/VPLS. Ruch między urządzeniami dostępowymi a agregującymi będzie wtedy przesyłany w enkapsulacji Q-in-Q, a ruch między urządzeniami agregacyjnymi a rdzeniowymi będzie przesyłany w enkapsulacji MPLS. Rozwiązanie takie pozwoli na tunelowanie ruch klienckiego już na poziomie warstwy dostępowej (Q-in-Q), jednocześnie umożliwiając szybkie i optymalne przesyłania ruchu przez szkielet sieci przy wykorzystaniu najnowszych technologii Metro Ethernet (MPLS/VPLS).

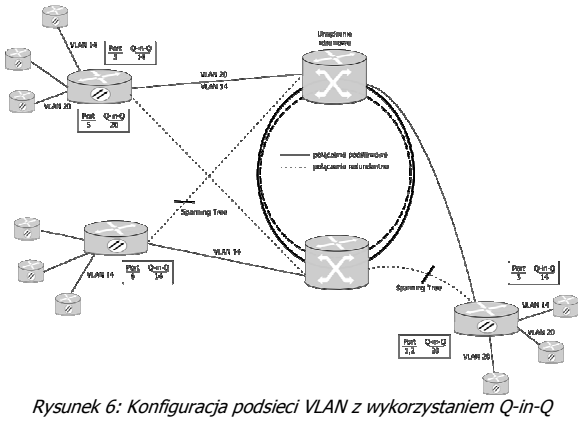
Podczas wdrażania warstwy aktywnej należy przewidzieć i zaimplementować możliwość wydzielenia wirtualnych sieci prywatnych wg określonych usług lub grup użytkowników. W szczególności przewidzieć należy wydzielenie następujących sieci VPN:

- **Sieci wewnętrznych** Jednostek Samorządu Terytorialnego uwzględniając ich strukturę organizacyjną oraz charakter i kierunki wymiany informacji tych Jednostek między sobą. W szczególności może to być kilka sieci VPN, które będą miały możliwość wzajemnej wymiany danych.

- Sieci **„edukacyjnej”** obejmującej placówki oświatowe i edukacyjne znajdujące się na terenie miasta. Wydzielenie powinno ułatwić tworzenie i zarządzanie systemami typu e-Learning oraz powinno umożliwić wdrożenie wydzielonego systemu adresacji IP. Z uwagi na duża ilość obiektów edukacyjnych zaleca się wykonanie kilku sieci VPN lub jednej sieci VPN z podziałem podsieci IP.

- Sieci VPN wydzielonych wg pozostałych **typów użytkowników sieci** wykorzystujących zbudowaną sieć do integracji systemów informatycznych. Przykładem będą szpitale i szpitalne systemy informatyczne oraz szpitale realizujące programy e-Zdrowie. Inną siecią prywatną będą również biblioteki i czytelnie włączane do bibliotecznych systemów bazodanowych i wymiany informacji naukowej. Przykładów może być wiele;

- Wydzielonej sieci VPN obejmującej urządzenia **Publicznego Dostępu do Internetu** (PIAP) z osobną wirtualną siecią prywatną dla urządzeń radiowych typu HOTSPOT.



Rysunek 6: Konfiguracja podsieci VLAN z wykorzystaniem Q-in-Q

- Sieci VPN zakładanych dla poszczególnych **usług sieciowych i bazodanowych** systemów informatycznych takich jak systemy GIS, Centralna Ewidencja Pojazdów, Ewidencja Ludności, Rejestr Gruntów, itp. do których dostęp będzie wymagany przez podmioty różnego typu. Szczególnymi rodzajami takich sieci wirtualnych będą sieci obejmujące zwirtualizowane zasoby serwerów i usług miejskich dostępne po wybudowaniu Centrum Przetwarzania Danych o odpowiedniej funkcjonalności;

- Sieci **monitoringu wizyjnego** miasta łączącego Centrum Nadzoru oraz monitorowane obiekty i system kamer wizyjnych w mieście;

- Systemu **monitoringu skrzyżowań** i obiektów drogowych będący w gestii Miejskiego Zarządu Dróg oraz systemów automatyki i sterowania ruchem w przypadku ich instalacji;

- Sieci wewnętrznych poszczególnych **spółek infrastrukturalnych** miasta posiadających swoje obiekty rozmieszczone na terenie całego miasta, przeznaczonych na przesyłanie danych systemów informatycznych między oddziałami lub obsługę i połączenie systemów telemetrycznych wykorzystywanych przez te spółki na potrzeby rozliczania energii, ciepła, gazu, a nawet do przesyłania sygnałów sterujących urządzeniami;

- Istotne będą również podsieci VLAN związane z **zarządzaniem i monitoringiem** urządzeń aktywnych pracujących w sieci. Porty zarządzające oraz monitorowanie sieci powinno odbywać się w wydzielonych sieciach VLAN, w której będzie również obecne Centrum Zarządzania Siecią.

- Specjalną wersją podsieci będzie również sieć VLAN **dostępu do Internetu** lub przyporządkowanie w ramach powyższych podsieci urządzeń punktu styku z Internetem. Nie wszyscy użytkownicy sieci miejskiej i nie wszystkie usługi publiczne będą wymagały dostępu do Internetu stąd warto tę szczególną sieć poddać segmentacji ze względu na wydajność oraz bezpieczeństwo.

Z uwagi na trudności z określeniem konkretnych ilości wirtualnych sieci prywatnych VPN przypadających na poszczególne obszary wymienione powyżej przyporządkowanie oznaczenia sieci VPN konkretnemu typowi użytkownika powinno być wykonywane w skalowalnym zakresie. Ilość przydzielonych do wykorzystania podsieci powinna odpowiadać zapotrzebowaniu danego użytkownika lub charakterowi usługi i przewidywaniom zapotrzebowania w przyszłości.

Charakterystyczny będzie również dostęp do tej samej stacji, serwera, urządzenia dostępowego z poziomu kliku sieci VPN jednocześnie, w zależności od zakresu wykorzystania zasobów sieci przez dane urządzenie. Dodatkowo komplikuje to kwestie przejrzystości i zarządzania siecią rozległa.

W szczególności wdrożenie warstwy aktywnej sieci powinno przewidywać uzgodnienie ze służbami nadzoru sieci Inwestora oraz z osobami odpowiedzialnymi za systemy informatyczne użytkownika sieci odpowiedzialnego za wdrażany system, w zakresie przynależności poszczególnych elementów systemu do utworzonych wcześniej wirtualnych sieci.

Uzgodnienie to wygodnie będzie przeprowadzić w formie tabelarycznej zaznaczając czy dane urządzenie występuje lub nie w danej podsieci. Przykład fragmentu takiej tabeli poniżej:

VPN	Opis wykorzystania sieci	Przełączniki UM	Stacje końcowe UM	PIAPy	Kamery	Centrum Nadzoru Monitorinu	Centrum Zarządzania Kryzysowego	.....
A	Dostęp do Internetu	**X**	**X**	**X**	--	--	**X**	--
B	Sieć hotspotów	--	--	**X**	--	--	--	--
C	System monitoringu	--	--	--	**X**	**X**	**X**	--
D	System monitoringu skrzyżowań	--	--	--	--	--	**X**	--
E	⋮	--	--	--	--	--	--	--

Tabela 2. Przykładowa tablica sieci VPN dla poszczególnych podsieci w MSS Żywiec

Należy zauważyć, że sieci VPN pozwalają na logiczną separację ruchu, uniemożliwiającą przechwytywanie informacji przez użytkowników różnych sieci prywatnych. Wirtualne sieci prywatne w technologiach Q-in-Q i MPLS nie są jednak odpowiedzialne za szyfrowanie danych wrażliwych. Oznacza to, że w przypadku fizycznej ingerencji w strukturę sieci komputerowej (np. wstawienie transparentnego urządzenia podsłuchującego na trasie światłowodu) może umożliwić dostęp do danych przesyłanych przez urządzenia sieciowe. Ewentualne szyfrowanie informacji poufnych i tajnych nie leży w gestii operatora sieci miejskiej i powinno odbywać się przy wykorzystaniu odpowiedniego oprogramowania lub specjalizowanych urządzeń, zarządzanych przez użytkownika sieci.

2.4.7. Zarządzanie i automatyzacja zarządzania urządzeniami sieciowymi

Zarządzanie jest bardzo ważnym elementem składającym się na działanie sieci, jako całości. Aby duża sieć mogła działać poprawnie i przewidywalnie, musi posiadać mechanizmy zapewniające sprawną i szybką reakcję na zaistniałe problemy oraz pozwalające szybko ocenić stan sieci bez konieczności przeglądania stanu każdego urządzenia z osobna. Również zmiany konfiguracji urządzeń, szczególnie związanych z zapewnieniem, uzgodnionego z klientem w SLA poziomu usług, wymaga narzędzi pozwalających przeprowadzać je globalnie dla dużej liczby urządzeń jednocześnie.

Wymogi nowoczesnych systemów Zarządzania Siecią, konsolidowanych operacyjnie w Centrach Zarządzania, muszą spełniać również przełączniki i urządzenia sieciowe. Optymalne wymagania, jakie powinny spełniać przełączniki to:

- Przełącznik powinien umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu – funkcja SPAN
- Przełącznik powinien umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN – Remote SPAN
- Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem narzędzi zarządzania:
  - powinno umożliwiać zarządzanie poprzez interfejs CLI (konsolę)
  - powinno umożliwiać zarządzanie poprzez SNMP v1, SNMP v2, SNMP v3 non-crypto i SNMP v3 crypto
  - powinno umożliwiać zbieranie i przesyłanie informacji o przesyłanych przez urządzenie strumieniach danych
  - powinno umożliwiać autentykację i autoryzację dostępu do konsoli zarządzania urządzenia przy wykorzystaniu serwera RADIUS lub TACACS
- Plik konfiguracyjny urządzenia powinien mieć możliwość edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nowa konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 10 plików konfiguracyjnych.

- Plik konfiguracyjny urządzenia powinien być zabezpieczony przed niepowołanym dostępem oraz zmianami – tylko osoby z odpowiednimi uprawnieniami powinny posiadać dostęp do pliku konfiguracyjnego.

Zarządzanie urządzeniami odbywać się będzie w wydzielonej podsieci, niedostępnej dla użytkowników sieci miejskiej.

2.5. Zadania Wykonawcy związane z integracją istniejącego segmentu radiowego sieci miejskiej

Segment radiowy Miejskiej Sieci Szerokopasmowej Żywiec jest istniejącym obecnie uzupełnieniem infrastruktury światłowodowej realizującej dostęp do zasobów sieci wszędzie tam, gdzie nie ma możliwości technicznych dla wykonania połączenia światłowodowego (lub są one ekonomicznie nieuzasadnione), wymagany jest radiowy dostęp publiczny oraz wymagane parametry łącza szczególnie w zakresie przepustowości pozwalają na zastosowanie łącz radiowych.

Zadaniem Wykonawcy będzie w szczególności:

- włączenie stacji bazowej WIMAX do sieci miejskiej poprzez łącza światłowodowe w LPD (przy pomocy odpowiednich mediakonwerterów WDM) i 1 włóknem światłowodowym z puli zapasowej do wydzielonego urządzenia (przełącznika sieciowego) agregującego elementy końcowe systemu PIAP znajdującego się w GPD;
- zaprojektowanie i konfiguracja utworzonej wydzielonej warstwy aktywnej sieci w taki sposób aby zapewnić bezpieczny dostęp do zasobów Internetowych dla użytkowników połączeń radiowych WIMAX w warstwie fizycznej oraz aplikacyjnej z uwzględnieniem przyjętej polityki wydzielonych sieci VLAN.

Z uwagi na ogół duże zajętości częstotliwości radiowych wykorzystywanych w telekomunikacji przez operatorów lokalnych (zarówno w częstotliwościach ogólnodostępnych na pasmach 2,4 Ghz i 5GHz oraz na pasmach licencjonowanych) oraz istniejącą radiową sieć miejską w technologii WIMAX dalsze szerokie zastosowanie technologii radiowych w MSS Żywiec może być utrudnione. W szczególności wymagane jest planowanie radiowe dla każdego projektu oraz pozyskanie dostępu do pasm licencjonowanych dostępnych w obszarze miasta i gminy, jeśli takie będą wykorzystywane.

2.5.1. Istniejąca infrastruktura sieci radiowej Zamawiającego

Miasto Żywiec i najbliższe okolice w ramach wcześniejszego projektu zostały objęte systemem radiowej transmisji IP wykorzystujący jako medium transmisyjne standard IEEE 802.16 (wg ustaleń/specyfikacji WiMax Forum). Stacja bazowa systemu radiowego zlokalizowana została na terenie miasta Żywiec w siedzibie Spółki „Ekoterm” z posadowieniem systemów antenowych na kominie przedsiębiorstwa. Jej zadaniem jest agregacja ruchu teleinformatycznego z sieci kilkudziesięciu terminali abonenckich znajdujących się w zasięgu systemu radiowego. Terminale abonenckie są podłączone bezpośrednio do lokalnej sieci komputerowej danej jednostki i tworzą radiowe lokalne punkty dostępu systemu WIMAX (RPA).

W przedmiotowej sieci świadczone są następujące usługi:

- Przesył danych umożliwiających dostęp do sieci Internet;
- Hot-spot bezprzewodowa sieć z dostępem do sieci Internet i portalu informacyjnego;
- Infokioski informacyjne podłączone do sieci Internet oraz do portalu informacyjnego
- Miejska sieć wewnętrzna umożliwiająca uruchomienie elektronicznego obiegu dokumentów;
- Intranetowy portal informacyjny

Zastosowana technologia podlega standaryzacji organizacji IEEE 802.16 – WiMAX. Zgodnie z przyjętymi założeniami w projekcie zastosowano 2 kanały dupleksowe o szerokości 3,5 MHz w paśmie 3,4 – 3,6 GHz. Technologia ta ma zapewnić w realizowanym projekcie cechy systemu radiowego, które charakteryzują technologię WiMAX. Ze wszystkich usług realizowanych przez system radiowy najważniejszymi zadaniami i systemami były:

- **miejska sieć obiegu wewnętrznego dokumentów** (Elektroniczny System Obiegu Dokumentów) to system informatyczny, którego głównym celem jest usprawnienie procesu wymiany informacji w ramach samej organizacji (siedziba główna Urzędu Miasta Żywca oraz rozproszone geograficznie komórki organizacyjne) jak również w kontaktach z innymi jednostkami miejskimi mającymi dostęp do aplikacji. Obejmuje on m.in. archiwizowanie oraz wymianę elektronicznych wersji informacji i dokumentów, które dotychczas miały postać tradycyjną (papierową). Ponadto oprogramowanie zostało wyposażone w mechanizm WorkFlow, czyli automatyzację procesów biznesowych, w całości lub części, podczas której dokumenty, informacje lub zadania są przekazywane od jednego uczestnika do następnego, według odpowiednich procedur zarządczych.

- **intranetowy portal informacyjny** – czyli system zbudowany na bazie serwera www zawierający bazę danych SQL i interfejs użytkownika plus panel administracyjny do zarządzania z poziomu przeglądarki internetowej. System ten jest wykorzystywany do dystrybucji wiadomości publicznych do wszystkich lokalizacji miejskich wraz z infokioskami. Portal został zbudowany pod kątem udostępniania informacji turystycznych, komunikacyjnych, i innych związanych z promocją miasta.

Lokalizacje, które zostały podłączone do radiowej sieci e-Żywiec w systemie WIMAX wraz z usługami i listą urządzeń w poszczególnych lokalizacjach znaleźć można w poniższej tabeli:

l.p.	Symbol	Lokalizacja	Uwagi
1	RPA_1	Miejskie Centrum Kultury (MCK) Al. Wolności 4	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - infokiosk wewnętrzny stojący zgodny z wymogami projektu radiowego i specyfikacją techniczną z dostępem do intranetowego portalu informacyjnego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
2	RPA_2	Miejski Ośrodek Sportu i Rekreacji (MOSiR), ul. Zielona 7	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - infokiosk zewnętrzny wiszący zgodny z wymogami projektu radiowego i specyfikacją techniczną z dostępem do intranetowego portalu informacyjnego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
3	RPA_3	Muzeum Miejskie - Stary Zamek ul. Zamkowa 2	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów
4	RPA_4	Żywiecka Biblioteka Samorządowa ul. Kościuszki 5	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
5	RPA_5	Szkoła Podstawowa Nr. 1 ul. Ks. Słonki 14	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
6	RPA_6	Szkoła Podstawowa Nr. 3 ul. M. Skłodowskiej 2	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów
7	RPA_7	Szkoła Podstawowa Nr. 4 ul. Pod Łyską 36	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
8	RPA_8	Szkoła Podstawowa Nr. 5 ul. Powstańców Śląskich 4	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
9	RPA_9	Szkoła Podstawowa Nr. 9 ul. Podlesie 63	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
10	RPA_10	Zespół Szkolno Przedszkolny Nr. 1 ul. Moszczanicka 26	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
11	RPA_11	Zespół Szkolno Przedszkolny Nr. 2 Żywiec Oczków 101	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
12	RPA_12	Gimnazjum Nr.1	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN

		ul. Dworcowa 26	- router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - infokiosk zewnętrzny wiszący z dostępem do intranetowego portalu informacyjnego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
13	RPA_13	Gimnazjum Nr.1 ul. Zielona 1	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
14	RPA_14	Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. (MPWiK) ul. Ks. Prałata St. Słonki 22	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
15	RPA_15	Miejski Zakład Energetyki Cieplnej „Ekoterm” Sp. z o.o. ul. Folwark 14	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
16	RPA_16	BESKID Sp. z o.o. ul. Kabaty 2	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
17	RPA_17	Przedsiębiorstwo Usług Komunalnych Sp. z o.o. (PUK) – ul. Bracka 51	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
18	RPA_18	Miejski Zakład Komunikacji Miejskiej Sp. z o.o. (MZK) – Al. Wolności 24	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
19	RPA_19	Żywieckie Towarzystwo Budownictwa Społecznego SP. z o.o. (ŻTBS) – Zamkowa 14	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
20	RPA_20	Straż Miejska ul. Zielona 7	- terminal dostępu radiowego oraz urządzenia zasilające i sieci LAN - router zgodny z wymogami specyfikacji technicznej podłączony do sieci LAN i do terminala radiowego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów.
21	RPA_21	Urząd Miejski Żywiec ul. Rynek 2	- terminal dostępu radiowego - urządzenie agregujące ruch z wszystkich lokalizacji - infokiosk wewnętrzny stojący z dostępem do intranetowego portalu informacyjnego - infokiosk zewnętrzny z zadaszeniem, stojący z dostępem do intranetowego portalu informacyjnego - sieć LAN wskazanego obiektu ma dostęp do sieci Internet, intranetowego portalu informacyjnego oraz systemu obiegu dokumentów. - serwer systemu nadzoru systemu radiowej sieci miejskiej - serwer systemu obiegu dokumentów - serwer intranetowego portalu informacyjnego
22	RPA_22	Dworzec PKP (hala główna) ul. Dworcowa	- terminal dostępu radiowego - infokiosk zewnętrzny, stojący, zainstalowany w holu głównym z dostępem do intranetowego portalu informacyjnego.

Tabela 3. Zestawienie istniejących punktów RPA do integracji z siecią MSS ŻYWIEC

2.6. Zadania Wykonawcy związane z wdrożeniem systemu punktów typu PIAP

Budowa systemu punktów **Publicznego Dostępu do Internetu (PIAP)** jest istotnym elementem komunikacji miasta z jego mieszkańcami i służyć powinna propagowaniu idei Społeczeństwa Informacyjnego wśród mieszkańców. Sieć punktów PIAP jest również medium dostępowym dla elektronicznych usług administracji publicznej.

Wdrożenie programu budowy sieci punktów PIAP powinno zostać skorelowane z przygotowanymi przez Inwestora programami aktywizacji środowisk zagrożonych wykluczeniem cyfrowym oraz powinno zakładać również szereg szkoleń z obsługi i wykorzystania zasobów sieciowych. W ślad za programem szkoleniowym powinna zostać przeprowadzona promocja możliwości tych punktów wśród społeczności lokalnej. Możliwości budowy różnych działań aktywizujących bazujących na zbudowanej strukturze telekomunikacyjnej jest bardzo dużo.

Zadaniem Wykonawcy będzie:

- doprowadzenie przyłączy światłowodowych do obiektów w których zlokalizowano punkty PIAP o ile nie przyłączono ich z tytułu innej funkcji obiektu;
- sporządzenie projektu zabudowy urządzeń PIAP wraz z uzyskaniem akceptacji gestora pomieszczeń udostępnianych na PIAP;
- dostarczenie oraz montaż urządzeń systemu PIAP;
- włączenie sprzętu aktywnego do wydzielonej sieci podsystemu punktów PIAP w mieście;
- integracja nowo budowanej sieci łączącej punkty PIAP z dotychczasowymi punktami typu HOTSPOT oraz nowobudowanymi punktami RDP. Lokalizacje punktów istniejących zaznaczono na mapie wszystkich punktów sieciowych.

Infrastrukturą dostępową PIAP do zbudowania podczas bieżącej inwestycji będą 4 nowe Radiowe Punkty Dostępowe (HotSpoty). Zadaniem projektanta będzie również integracja nowo budowanej sieci łączącej punkty PIAP z istniejącymi w mieście HOTSPOTAMI. Lokalizacje punktów istniejących zaznaczono na mapie wszystkich punktów sieciowych. Poniżej określono wymagania techniczne dla poszczególnych typów punktów dostępu publicznego do Internetu.

2.6.1. Radiowe Punkty Dostępowe sieci (hotspoty HTS)

Radiowe Punkty Dostępowe typu Hotspot służą do przekazania sygnału szerokopasmowego z sieci oraz do dystrybuowania go w rejonie stacji bazowej. Z uwagi na bezpieczeństwo danych jednostek samorządowych z sieci powszechnej mogą korzystać jedynie punkty nieprzesyłające danych osobowych, korzystające wyłącznie z dostępu do Internetu.

Połączenie tych punktów należy wykonywać bezpośrednio do punktów rdzeniowych via punkty LPD poprzez redundantne włókna kabli doprowadzanych do obiektów miejskich do wydzielonych przełączników zbierających sygnały radiowe z całego miasta w bezpiecznej podsieci VLAN lub VPN.

Jedynie dla niewielkiej ilości punktów dostępowych będących w zasobach Inwestora podłączanych drogą radiową dopuszcza się podłączenie punktu RPD do urządzenia dostępowego punktu LPD lub urządzenia agregacji przy założeniu, że w sieci działać będzie wydzielona podsieć lub kanał VPN obsługująca ten punkt radiowy.

Lista punktów radiowych typu Hotspot do zbudowania i punktów istniejących, które należy dołączyć do infrastruktury aktywnej sieci miejskiej:

l.p.	Symbol LPD	Symbol HOTSPOT	Proponowana lokalizacja	Uwagi
1	GPD	HTS_1	Spółdzielnia Mieszkaniowa Gronie, ul. Oś. 700-lecia 50	
2	GPD	HTS_2	Pełnomocnik Burmistrza, ul.Powstańców Śląskich 27	
3	LPD_7	HTS_3	Miejskie Centrum Kultury (MCK), ul. Al.Wolności 4	
4	GPD	HTS_4	Amfiteatr pod Groniem	

Tabela 4: Proponowane lokalizacje dla Radiowych Punktów Dostępowych (HTS)

Do realizacji bezprzewodowych punktów dostępu do Internetu we wskazanych obiektach użyteczności publicznej oraz w obszarach zewnętrznych powinny być zainstalowane urządzenia radiowe umożliwiające transmisję radiową w pasmach ogólnodostępnych w standardach 802.11 a/b/g pracujące w pasmie 2,4GHZ. Obszar pokrywany powinien gwarantować dostęp radiowy do RPD z pasmem minimum 54 Mb/s w odległości do 37mb od punktu centralnego. W szczególności dla rozległych obszarów wskazanych przez Inwestora należy zaprojektować kilka punktów radiowych pokrywających zasięgiem zadany obszar.

Rysunek 7: Przykład zestawu stacji bazowej Radiowego Punktu Dostępowego typu Hotspot

Do realizacji dostępu radiowego przewidziano stacje radiowe przeznaczone do środowisk o większym ryzyku uszkodzeń i do zastosowań zewnętrznych, dzięki mocnej konstrukcji obudowy. Urządzenia te powinny oferować między innymi następujące funkcje:

- Podwójne urządzenia radiowe umożliwiają obsługę wielu opcji sieci bezprzewodowych zarówno w paśmie 2,4 GHz, jak i 5 GHz, udostępniając najwyższą wydajność, najlepszy zasięg i obsługę urządzeń klienckich.
- Funkcje zapewniające zasięg nawet w przypadku przeszkód i potencjalnych zakłóceń.
- Łatwa integracja z oprogramowaniem do zarządzania i monitorowania.
- Bezpieczny, blokowany system instalacji w obudowie wzmocnionej
- Obsługa wielu standardów zabezpieczeń do uwierzytelniania tożsamości i ochrony.
- Możliwość zasilania przez sieć Ethernet w celu ułatwienia instalacji.
- Temperatura pracy –20 do 55°C

Urządzenia te powinny również posiadać minimum następujące funkcjonalności:

- zasięgi minimalne na zewnątrz dla 802.11a: od 30 m przy 54 Mb/s do 198 m przy 6 Mb/s i dla 802.11g: od 37 m przy 54 Mb/s do 290 m przy 1 Mb/s
- Bandwidth Management, QoS, Firewall, Port Forwarding, IP Accounting
- obsługę protokoły routingu: RIPv1/2
- obsługę grup VLAN w standardzie 802.1q
- obsługę połączeń PPPoE server, PPtP server,
- funkcjonalność DHCP server dla klientów radiowych, HotSpot
- podstawowe procesy kontroli dostępu: autentykację i autoryzację aktywności użytkowników w sieci w oparciu o protokół RADIUS i współpracę z zewnętrznym serwerem RADIUS,
- możliwość implementowania systemu rozliczania użytkowników korzystających z HotSpota
- bezpieczeństwo i szyfrowanie na radiu: AES-CCMP encryption (WPA2), TKIP (WPA), Cisco TKIP, WPA TKIP, IEEE 802.11 WEP keys 40 bitowe i 128 bitowe
- zdalne zarządzanie i konfiguracji z obsługą protokołów SNMP - przez administratora sieci.

Dla pokrycia obszaru dookoła punktu radiowego przewidziano anteny dookólne o 15 dBi polaryzacji pionowej 360 stopni każda. Polaryzacja pionowa pozwala uniknąć zakłóceń a zwarcie dla prądu stałego chroni karty przed wyładowaniami atmosferycznymi.

Zestaw te powinny umożliwiać użytkownikom Hotspota wyłącznie korzystanie z zasobów sieci Internet w określonym zakresie bez dostępu do zasobów sieciowych komputerów innych użytkowników podłączonych do urządzenia radiowego. Wszystkie urządzenia, a także klienci podłączeni do tych punktów powinni zostać odseparowani od ogólnego ruchu sieciowego poprzez wydzielenia odrębnej grupy VLAN, a nawet odrębnej adresacji IP. Radiowe urządzenia dostępowe powinny być zarządzane wyłącznie od strony portu WAN (Ethernetowego), dostęp administracyjny od strony radiowej powinien zostać zablokowany. Układ sprzętowy realizujący reset urządzenia w przypadku jego niestabilnej pracy (watchdog) powinien samodzielnie resetować urządzenie do ustawień domyślnych gwarantujących poprawną pracę urządzenia z pełnym zakresem zabezpieczeń dostępu.

Zaleca się dołączanie radiowych punktów dostępowych typu HotSpot do wydzielonego, zbiorczego urządzenia agregującego (przełącznika) typu SWA-B, w Głównym Punkcie Dystrybucji. Punkty te należy przyłączyć do przełącznic światłowodowych w LPD (przy pomocy odpowiednich mediakonwerterów) i wolnymi włóknami światłowodowymi przesłać sygnał do urządzenia agregującego w GPD.

Urządzenia zewnętrzne powinny być montowane w obudowach gwarantujących odporność na czynniki zewnętrzne oraz pracę urządzenia w odpowiednim zakresie temperatury. Obudowy, anteny i instalacje antenowe powinny być wykonane w sposób zapewniający odpowiednią ochronę odgromową, wysoką niezawodność oraz zachowanie estetyki miejsca montażu. W miejscach szczególnie reprezentacyjnych oraz zabytkowych sposób montażu powinien zostać uzgodniony z Inwestorem.

Strona logowania oraz strona domyślna wyświetlana jako pierwsza po zalogowaniu powinny posiadać czytelne oznaczenia Inwestora, objaśniać sposób korzystania z systemu radiowego oraz zapewniać jednolity wygląd graficzny z systemem przyjętym dla innych punktów dostępowych typu PIAP w mieście. Obszar zasięgu Hotspota powinien zostać oznaczony odpowiednimi materiałami marketingowymi (naklejki, tablice) w sposób uzgodniony z Inwestorem.

2.6.2. Wymagania dla Publicznych Punktów Dostępowych typu Infomat (INF)

Punktami tego rodzaju powinny być projektowane w mieście w wszelkiego rodzaju infomaty, (infokioski), czyli multimedialne kioski informacyjne (łatwe w obsłudze komputery z ekranem dotykowym), które mają dostarczać obywatelom publicznie dostępnej informacji na wybrany temat. Punkty tego typu są pasywne, gdyż ograniczają się do technicznego zapewnienia połączeń z Internetem lub serwerami wewnętrznymi w celu pozyskania niezbędnych informacji prezentowanych użytkownikowi korzystającemu z punktu. Urządzenia takie powinny, więc być umieszczane w najbardziej dostępnych publicznie miejscach. Mogą być wykorzystywane przez np.: podróżnych, turystów, a także w szpitalach, urzędach administracji publicznej, gminnych ośrodkach kultury, itp.

Zadaniem projektanta będzie integracja istniejących Infomatów z nowo powstającą infrastrukturą sieci i włączenie ich w wydzieloną podsieć oraz jednolity system zarządzania. Decyzją Zamawiającego **nie przewiduje się w I etapie** projektu budowy nowych infomatów w ramach projektu.

l.p.	Symbol LPD	Symbol INFOMAT	Istniejąca lokalizacja	Uwagi
1	GPD	INFO_1	Miejskie Centrum Kultury (MCK) – Al. Wolności 4	infokiosk wewnętrzny stojący
2	GPD	INFO_2	Miejski Ośrodek Sportu i Rekreacji (MOSiR) – ul. Zielona 7	infokiosk zewnętrzny wiszący
3	GPD	INFO_3	Gimnazjum Nr.1 – ul. Dworcowa 26	infokiosk zewnętrzny wiszący
4	GPD	INFO_4 INFO_5	Urząd Miejski Żywiec – Rynek 2	infokiosk wewnętrzny stojący infokiosk zewnętrzny z zadaszeniem
5	GPD	INFO_6	Dworzec PKP (hala główna) – ul. Dworcowa	infokiosk zewnętrzny stojący

Tabela 5: Proponowane lokalizacje istniejących punktów typu Infomat

Podstawową funkcją Infomatów w MSS Żywiec będzie zapewnienie możliwości korzystania z szerokopasmowego dostępu do Internetu, pełnienie funkcji pomocniczej dla HotSpota oraz funkcji informacyjnej w celu dostarczenia obywatelom niezbędnych informacji o sprawach dotyczących życia codziennego. Urządzenia takie powinny, więc być umieszczane w najbardziej dostępnych publicznie miejscach. Mogą być wykorzystywane przez np.: podróżnych, turystów, a także w szpitalach, urzędach administracji publicznej, gminnych ośrodkach kultury. Z uwagi na bezpieczeństwo kiosków zaleca się montować je w punktach objętych monitoringiem wizyjnym miasta.

2.7. Zadania Wykonawcy związane z wdrożeniem wyposażenia Operatorskiego Punktu styku z Internetem

W **Punktach Stykowych z węzłami operatorów zewnętrznych (IXP**) realizowany będzie styk Miejskiej Sieci Szerokopasmowej z dostawcami łącz szerokopasmowych sieci ogólnokrajowej, umożliwiające wymianę ruchu internetowego pomiędzy projektowaną siecią a siecią Internet. Infrastruktura tego punktu powinna zapewniać możliwość redundancji łącz pomiędzy różnymi operatorami lub przewidzieć należy zastosowanie dwóch niezależnych punktów styku IXP z różnymi operatorami. Oprócz nadmiarowości punkty IXP powinny posiadać odpowiednie zabezpieczenia fizyczne i informatyczne, choć na ogół są one zapewnianie przez operatora zewnętrznego.

Zadaniem wykonawcy będzie w szczególności:

- zabudowa infrastruktury pasywnej (przełącznic światłowodowych) w punktach IXP i wykonanie redundantnych połączeń z punktów IXP do węzła centralnego IXC poprzez włókna magistrali sieci;
- zabudowa infrastruktury pasywnej (przełącznic światłowodowych) i aktywnej w punkcie **Operatorskiego Styku z Internetem (IXC)** zlokalizowanym w pomieszczeniu serwerowni Centrum Zarządzania Siecią;
- konfiguracja routerów, firewalla I sondy IDC oraz włączenie do systemu zarządzania tymi urządzeniami z poziomu stanowisk administratorskich;
- określenie reguł filtrowania treści, reguł bezpieczeństwa administracji urządzeniami punktu styku oraz konfiguracja portów otwartych dla regionalnych lub krajowych systemów bazodanowych wymieniających dane z informatycznymi systemami miejskimi (o ile takie będą występowały na etapie wdrożenia);
- określenie Zamawiającemu łącznego zapotrzebowania na pasmo i innych parametrów potrzebnego łącza szerokopasmowego, które umożliwią ogłoszenie przetargu na dostawę łącz dzierżawionych od dostawców szerokopasmowych.

Punkt styku sieci miejskiej z Internetem zostanie zrealizowany w postaci wydzielonego, centralnego aktywnego **Punktu Operatorskiego Styku z Internetem (IXC)** umieszczonego w pomieszczeniach Centrum Zarządzania Siecią zintegrowanego z Głównym Punktem Dystrybucyjnym (serwerownia w budynku Urzędu Miasta) i zawierającego dedykowane bramy sieciowe o odpowiedniej wydajności i funkcjonalności. Połączenia z ogólnokrajowymi dostawcami usług wymiany ruchu szerokopasmowego, umożliwiające wymianę ruchu internetowego pomiędzy projektowaną siecią a siecią Internet realizowane będą poprzez magistralę światłowodową i **Punkty Stykowe z węzłami operatorów zewnętrznych (IXP)**.

Infrastruktura punktu IXP powinna zapewniać możliwość redundancji łącz pomiędzy różnymi operatorami lub przewidzieć należy zastosowanie dwóch niezależnych geograficznie punktów styku IXP z różnymi operatorami.

Połączenia z minimum 2 punktami IXP realizowane będą przez magistralę światłowodową w warstwie szkieletowej w postaci minimum **6 włókien** światłowodowych (2 podstawowe, 2 redundancja i 2 zapasu) i zbiegać się będą w wydzielonym punkcie **Operatorskiego Styku z Internetem (IXC).** Lokalizacja takiego punktu została dobrana pod kątem optymalizacji rozpływu włókien oraz uwzględniając kwestii integracji infrastruktrury. Trasy rozpływu włókien światłowodowych zostały dobrane w sposób gwarantujący pełną niezależność przebiegu trasy i redundancje gwarantującą bezpieczeństwo dostępu do Internetu.

l.p.	Symbol GPD	Symbol	Lokalizacja dostępnych węzłów operatorskich	Uwagi
1	GPD	IXP_01	Urząd Miasta , ul. Rynek 2	Istniejący węzeł sieciowy z zainstalowanymi urządzeniami w dotychczasowej serwerowni
2	GPD	IXP_02	Ul. Wesoła	Nowy możliwy węzeł styku z Operatorem
3	GPD	IXC	Urząd Miasta , ul. Rynek 2	Integracja z CZS i GPD, w nowo projektowanej serwerowni

Tabela 6: Proponowane lokalizacje dostępnych węzłów operatorów oferujących dostęp do sieci Internet

Wybór dostawcy Internetu w podanych wyżej punktach IXP zależy od wyników przetargu na dostawę pasma, które należy przeprowadzić po zakończeniu prac budowlanych i wdrożeniowych sieci miejskiej.

2.7.1. Wymagania dla Infrastruktura Operatorskiego Styku z Internetem (IXC)

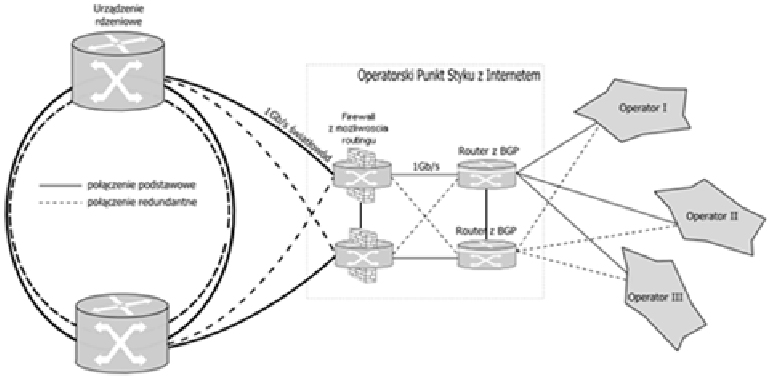
Styk z operatorami zapewniającymi dostęp do Internetu powinien zapewniać redundantny i bezpieczny dostęp do światowych zasobów sieciowych. Protokołem routingowym wymaganym do użycia na styku z dostawcami łączy do

Internetu jest protokół BGP. Ze względu na olbrzymia liczbę wpisów do tablicy rutingu BGP styk z SP należy podzielić na dwie części:

- Dedykowane routery brzegowe zapewniające routing BGP i stanowiące łącze do dwóch lub więcej operatorów
- Routery stanowiące pomost pomiędzy rdzeniem sieci miejskiej a routerami brzegowymi i dostarczające usług bezpieczeństwa dla całej sieci takich jak: **Firewall** (filtracja ruchu, stateful firewall, application proxy itp.) oraz **Aktywne systemy prewencji** (Intrusion Prevention Systems) przeciwko atakom wykorzystującym luki w oprogramowaniu, wraz z możliwością aktualizacji definicji i sygnatur ataków.

W tym celu Wykonawca będzie zobligowany do wdrożenia **2 dedykowanych routerów** pracujących w połączeniu redundantnym oraz **2 dedykowanych urządzeń zabezpieczających** umożliwiających inspekcję stateful firewall oraz Intrusion Prevention System (IPS), pracujących jako klaster niezawodnościowy.

Schemat logiczny podłączenia Operatorskiego Punktu Styku z urządzeniami operatorów zewnętrznych oraz z siecią miejską obrazuje poniższy schemat.



Rysunek 10. Schemat połączeń Operatorskiego Punktu Styku z Internetem i włączenia do GPD

Przyłączenie urządzeń IXC do urządzenia rdzeniowego znajdującego się w tym samym pomieszczeniu Głównego Punktu Dystrybucji powinno zostać wykonane patchcordem światłowodowym pomiędzy portami SFP przełącznika rdzeniowego i firewalla, z redundancją połączenia do drugiego zestawu routerów. Połączenie powinno być zrealizowane z przepustowością 1Gb/s, przy zastosowaniu odpowiednich modułów SFP w obu urządzeniach.

Po rozbudowie sieci miejskiej, gdy pojawi się drugi węzeł rdzeniowy ulokowany w drugim GPD rozbudować należy również połączenia światłowodowe z wykorzystaniem włókien magistrali do odpowiednich portów 1Gb/s przełącznika rdzeniowego w sposób przedstawiony na powyższym rysunku. Zarówno systemy bezpieczeństwa jak i routery brzegowe powinny umożliwiać wykorzystanie interfejsów 10Gb/s, których użycie może się okazać niezbędne wraz z rozwojem sieci komputerowej.

2.7.2. Wymagania dla Infrastruktury Punktów Styku z węzłami operatorów zewnętrznych (IXP).

Przy pomocy włókien magistrali węzły operatorów powinny zostać dołączone do obu routerów brzegowych zlokalizowanych w IXC. Zadaniem wykonawcy z tego powodu będzie w szczególności zabudowa infrastruktury pasywnej sieci miejskiej (w postaci dedykowanych przełącznic światłowodowych) w węzłach operatorów (IXP) i wykonanie redundantnych połączeń z punktów IXP do węzła centralnego IXC poprzez włókna magistrali sieci. Włókna redundantne i zapasu powinny zostać zakończone pigtailami i adapterami na wydzielonych przełącznicach światłowodowych 1U ulokowanych w węźle operatora oraz w zbiorczej przełącznicy 1U 24 port w punkcie IXC.

Oprócz nadmiarowości punkty IXP powinny posiadać odpowiednie zabezpieczenia fizyczne i informatyczne, choć na ogół są one zapewnianie przez operatora zewnętrznego. Z uwagi na kwestię zabezpieczania dostępu do połączeń spawanych w punktach styku IXP przewidziano zastosowanie przełącznic teleskopowych zamykanych na zamek z kluczykiem 1U i 24 porty SC/APC. Na przełącznicy powinno się znaleźć również wyraźne i trwałe oznaczenie Inwestora.

Przyłączenie do urządzeń operatora wymagać będzie odpowiedniego patchcordu światłowodowego. Szczególnym przypadkiem jest węzeł IXP_1 ulokowany w pomieszczeniu serwerowni Urzędu Miejskiego, w którym znajdują się łącza szerokopasmowe różnych operatorów. Podłączenie tego punktu do urządzeń brzegowych znajdujących się w IXC będzie możliwe zwykłym patchcordem lub krótkim kablem światłowodowym łączącym pomieszczenia starej serwerowni i nowego pomieszczenia przeznaczonego na zintegrowany węzeł GPD/IXC/CZS.

2.7.3. Mechanizmy niezawodnościowe i zapewniające dostępność

Dostęp do Internetu jest podstawową usługą, która musi być realizowana przez sieć miejską. Internet otwiera wielkie możliwości, ale korzystanie z niego nie jest pozbawione pewnego ryzyka. W drodze do pełnego wykorzystania Internetu wielką rolę do odegrania mają technologie ochrony danych. Maksymalizacja wydajności zwykle stoi w sprzeczności z chęcią zapewnienia maksymalnego bezpieczeństwa. Odpowiedni dobór urządzeń, takich jak router brzegowy, firewall, sonda IPS pozwala na częściowe rozwiązanie tego dylematu. Wydajność całego rozwiązania styku z Internetem jest taka, jaka jest wydajność jego najsłabszego ogniwa, tak, więc szczególne znaczenie ma poprawne zaprojektowanie całego rozwiązania tak, aby zidentyfikować wszelkie potencjalne wąskie gardła, a następnie je usunąć. W tym celu infrastruktura sieciowa na styku z Internetem powinna zapewniać:

- bezpieczeństwo i skalowalność,
- wydajność umożliwiająca niezakłóconą realizację świadczonych usług,
- niezawodność i wysoką dostępność świadczenia usług dla sieci miejskiej osiągnięta przez redundancję połączeń, urządzeń, modułów zarządzających routerami i innych.

Podłączenie do Internetu należy zrealizować w oparciu o usługi co najmniej dwóch dostawców. Styk do Internetu od każdego z dostawców podłączony dwoma różnymi torami do różnych urządzeń brzegowych zapewni redundancje fizyczną. Całość podłączona zostanie w sposób redundantny dołączona do rdzenia sieci. Zdublowanie routerów brzegowych pozwala na rozłożenie obciążenia związanego z obsługą ruchu Internetowego na dwa lub kilka urządzeń, a w przypadku awarii jednego z nich zapewnia ciągłość działania usługi dostępu do Internetu.

Docelowo wprowadzone rozproszenie routerów na różne lokalizacje dodatkowo zapewni ciągłość działania nawet w sytuacji braku zasilania węzła lub Centrum Zarządzania Siecią. Dla sieci miejskiej Żywiec przyjęto, że integracja z infrastrukturą CZS i GPD wyposażoną w wielostopniową ochronę zasilania będzie wystarczającym zabezpieczeniem i nie ma potrzeby lokowania dodatkowych urządzeń zabezpieczających w pomieszczeniach węzła GPD_1.

2.7.4. Założenia obsługi ruchu wymienianego z globalną siecią internetową

Aby możliwe było podłączenie sieci MAN do kilku dostawców Internetu w celu poprawy bezpieczeństwa działania sieci oraz wydajności konieczne jest złożenie wniosku do RIPE NCC (Réseaux IP Européens Network Cordination Centre) o przydzielenie unikalnego numeru systemu autonomicznego AS i puli adresów IPv4 oraz IPv6. Należy również przeprowadzić negocjacje z dostawcami Internetu w kwestii uruchomienia usługi BGP pomiędzy routerami brzegowymi MAN a routerami brzegowymi dostawców.

Posiadane klasy adresowe IP można wykorzystać wydzielając z niej poszczególne klasy dla grup odbiorców (np. sieć wewnętrzna Jednostek Samorządowych, szkoły osobna, etc). Zalecanym działaniem jest na przykład wyodrębnienie na poziomie adresacji IP podsieci przeznaczonej wyłącznie dla celów edukacyjnych.

Wymagania operatorów wyłonionych w przetargu udostępniających łącza do Internetu dla organizacji technologii podłączenia punktu IXC do ich węzła mogą być różne. Dla zapewnienia realizacji dedykowanych kanałów oraz wymiany różnych usług poprzez sieć operatorską wskazywane są na ogół urządzenia zapewniające możliwość uruchomienia kanałów VLAN (802.1Q). Dla wymiany ruchu urządzenia posiadające wsparcie technologii IPv4, IPv6 oraz BGPv4 oraz obsługę technologii Mulitcast. Łącze światłowodowe powinno wykorzystywać włókna jednomodowe oraz być zakończone w standardzie SC/APC (lub innym wskazanym przez operatora).

Ocenia się, że w początkowym okresie pracy systemu wystarczający będzie styk optyczny o transmisji 60 Mb/s (2 x 30Mb/s) z możliwością rozbudowy w miarę rosnących potrzeb. Ze względu na brak konieczności stosowania dodatkowych urządzeń do konwersji sygnałów jako najtańszą inwestycyjnie opcję podaje się wykonanie styku do operatora w technologii Gigabit Ethernet i moduły światłowodowe SFP.

2.7.5. Wymagania ogólne dla urządzeń brzegowych sieci

Urządzenie pracujące jako router brzegowy musi spełniać poniższe wymogi minimalne:

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, o wysokości maksymalnie 2U. 2. Urządzenie musi posiadać 4 porty 10/100/1000Mb/s RJ45 oraz 6 portów światłowodowych 1Gb/s SFP wyposażonych we wkładki 1Gb/s LX. 3. Urządzenie musi pozwalać na rozbudowę o kolejne interfejsy, minimum 40 portów 10/100/1000Mb/s RJ45 lub 30 portów 1Gb/s SFP. 4. Urządzenie musi pozwalać na routowanie z wydajnością minimum 3.5Gbps i 400Kpps. 5. Urządzenie musi być wyposażone w 2GB pamięci RAM. 6. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 420W. 7. Urządzenie musi być przystosowane do pracy w temperaturach 0-50 stopni Celsjusza i wilgotności 10-90%. 8. Architektura systemu operacyjnego routera powinna posiadać budowę modułową (moduły działają w odseparowanych obszarach pamięci), m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia jest oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. 9. Urządzenie musi pozwalać na konfigurację minimum 60 wirtualnych routerów, pozwalających na logiczną separację interfejsów i tablic routingu.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 256. 3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać podwójne tagowanie ramek Ethernetowych (Q-in-Q). 6. Urządzenie musi obsługiwać interfejsy Ethernet, T1/E1, Synchronous Serial, ISDN, ADSL2 oraz G.SHDSL. 7. Urządzenie musi obsługiwać ramki Jumbo. 8. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring).
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać następujące protokoły routingu IPv4: RIPv1/v2, IS-IS, OSPF oraz BGPv4 wraz z obsługą Graceful Restart oraz musi pozwalać na routing oparty o polityki (policy based routing). 2. Urządzenie musi mieć możliwość filtrowania i redystrybucji tras między różnymi protokołami routingu. 3. Konieczna jest obsługa equal-cost route (technologia znana również pod nazwą Equal-cost Multi-path). 4. Urządzenie musi obsługiwać następujące protokoły routingu IPv6: RIPng, OSPFv3, IS-ISv6, MP-BGP. 5. Urządzenie musi obsługiwać protokół ICMPv6. 6. Urządzenie musi obsługiwać jednoczesne korzystania ze stosów IPv4 i IPv6 (Dual Stack). 7. Urządzenie musi obsługiwać protokół BFD w celu zminimalizowania czasu wykrycia zmiany topologii i przyspieszenia konwergencji protokołów IS-IS, OSPF, BGP. Protokół BFD musi mieć również możliwość współpracy z mechanizmem Fast Reroute dla protokołu MPLS. 8. Urządzenie musi pozwalać na translację adresów NAT i PAT. 9. Urządzenie powinno pozwalać na jednoczesne zestawienie 512 tuneli IPSec VPN.
IV. Obsługa ruchu multicastowego:
1. Urządzenie musi obsługiwać następujące protokoły routingu multicastowego: PIM-SM, PIM-SSM, PIM-SMv6, PIM-SSMv6. 2. Urządzenie musi obsługiwać protokoły IGMPv1/v2/v3 wraz z możliwością nasłuchu (IGMPv1/v2/v3 Snooping). 3. Urządzenie musi obsługiwać protokół MLDv2 wraz z możliwością nasłuchu (MLDv2 snooping) – jest to odpowiednik IGMP dla protokołu IPv6. 4. Urządzenie musi obsługiwać protokół MSDP pozwalający na wymianę informacji o źródłach multicastowych między różnymi domenami administracyjnymi oraz wspierać technologię AnyCast-RP.
V. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo. 3. Interfejsy muszą obsługiwać kolejki typu Priority Queue z jedną kolejką typu Strict Priority (lub równoważne) w ilości minimum 8 kolejek na port. 4. Urządzenie musi obsługiwać mechanizm kształtowania ruchu typu traffic policing i traffic shaping. 5. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, portu wejściowego i wyjściowego, portów TCP/UDP oraz znaczników DSCP, 802.1p oraz EXP.
VI. Obsługa MPLS i VPLS:
1. Urządzenie musi obsługiwać technologie Layer 3 MPLS VPN, Layer 2 MPLS VPN oraz VPLS. 2. Urządzenie musi obsługiwać technologię MPLS Traffic Engineering przy użyciu protokołu RSVP-TE.
VII. Zarządzanie:
1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW. 2. Urządzenie musi pozwalać na zapisanie nie mniej niż 20 poprzednich, kompletnych konfiguracji. 3. Urządzenie musi pozwalać na zdalne zarządzanie przy użyciu API opartego o język XML. 4. Urządzenie musi pozwalać na stopniowanie praw dostępu do poszczególnych gałęzi konfiguracji lub poszczególnych komend dla użytkowników administracyjnych. 5. Urządzenie musi być wyposażone w dwa porty USB, które mogą zostać wykorzystane w celu wykonania kopii zapasowej całego systemu. Urządzenie musi mieć możliwość uruchomienia przy użyciu kopii zapasowej systemu, znajdującej się na urządzeniu USB.

Urządzenie pracujące jako system zabezpieczeń musi spełniać poniższe wymogi minimalne:

I. Podstawowe parametry urządzenia:
1. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, o wysokości maksymalnie 2U. 2. Urządzenie musi posiadać 6 portów 10/100/1000Mb/s RJ45 oraz 4 porty 1Gb/s SFP, wyposażone we wkładki światłowodowe 1Gb/s LX. 3. Urządzenie musi pozwalać na rozbudowę o kolejne interfejsy, minimum 36 portów 10/100/1000Mb/s RJ45 i 4 porty 1Gb/s SFP. 4. Urządzenie musi pozwalać na przesyłanie ruchu z wydajnością minimum 5.5Gbps i 700Kpps, przy włączonym mechanizmie stateful firewall. 5. Urządzenie musi pozwalać na przesyłanie ruchu z wydajnością 800Mbps, przy włączonym mechanizmie Intrusion Prevention System (IPS). 6. Urządzenie musi pozwalać na utrzymywanie minimum 375K sesji oraz tworzenie 27K nowych sesji na sekundę. 7. Urządzenie musi być wyposażone w 2GB pamięci RAM. 8. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 645W. 9. Urządzenie musi być przystosowane do pracy w temperaturach 0-40 stopni Celsjusza i wilgotności 10-90%. 10. Architektura systemu operacyjnego routera powinna posiadać budowę modułową (moduły działają w odseparowanych obszarach pamięci), m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia jest oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. 11. Urządzenie musi pozwalać na konfigurację minimum 48 wirtualnych routerów, pozwalających na logiczną separację interfejsów i tablic routingu. 12. Urządzenie musi pozwalać na pracę w klastrze active/passive lub active/active z drugim urządzeniem tego samego modelu i z tym samym wyposażeniem.
II. Usługi warstwy drugiej:
1. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 2. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 3072. 3. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 4. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 5. Urządzenie musi obsługiwać podwójne tagowanie ramek Ethernetowych (Q-in-Q). 6. Urządzenie musi obsługiwać interfejsy Ethernet, T1/E1, Synchronous Serial, VDSL2, ADSL2 oraz G.SHDSL. 7. Urządzenie musi obsługiwać ramki Jumbo. 8. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring).
III. Usługi warstwy trzeciej:
1. Urządzenie musi obsługiwać następujące protokoły routingu IPv4: RIPv1/v2, IS-IS, OSPF oraz BGPv4 wraz z obsługą Graceful Restart oraz musi pozwalać na routing oparty o polityki (policy based routing). 2. Urządzenie musi mieć możliwość filtrowania i redystrybucji tras między różnymi protokołami routingu. 3. Konieczna jest obsługa equal-cost route (technologia znana również pod nazwą Equal-cost Multi-path). 4. Urządzenie musi obsługiwać następujące protokoły routingu IPv6: RIPng, OSPFv3, IS-ISv6, MP-BGP. 5. Urządzenie musi obsługiwać protokół ICMPv6 wraz z ICMPv6 rediretion. 6. Urządzenie musi obsługiwać jednoczesne korzystania ze stosów IPv4 i IPv6 (Dual Stack). 7. Urządzenie musi obsługiwać protokół BFD w celu zminimalizowania czasu wykrycia zmiany topologii i przyspieszenia konwergencji protokołów IS-IS, OSPF, BGP. Protokół BFD musi mieć również możliwość współpracy z mechanizmem Fast Reroute dla protokołu MPLS. 8. Urządzenie musi pozwalać na translację adresów NAT i PAT.
IV. Obsługa ruchu multicastowego:
1. Urządzenie musi obsługiwać następujące protokoły routingu multicastowego: PIM-SM, PIM-SSM, PIM-SMv6, PIM-SSMv6. 2. Urządzenie musi obsługiwać protokoły IGMPv1/v2/v3 wraz z możliwością nasłuchu (IGMPv1/v2/v3 Snooping). 3. Urządzenie musi obsługiwać protokół MLDv2 wraz z możliwością nasłuchu (MLDv2 snooping) – jest to odpowiednik IGMP dla protokołu IPv6. 4. Urządzenie musi obsługiwać protokół MSDP pozwalający na wymianę informacji o źródłach multicastowych między różnymi domenami administracyjnymi oraz wspierać technologię AnyCast-RP.
V. Filtrowanie i kształtowanie ruchu:
1. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokoły IPv4 i IPv6. 2. Listy ACL muszą być obsługiwane sprzętowo. 3. Interfejsy muszą obsługiwać kolejki typu Priority Queue z jedną kolejką typu Strict Priority (lub równoważne) w ilości minimum 8 kolejek na port. 4. Urządzenie musi obsługiwać mechanizm kształtowania ruchu typu traffic policing i traffic shaping. 5. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, portu wejściowego i wyjściowego, portów TCP/UDP oraz znaczników DSCP, 802.1p oraz EXP.
VI. Obsługa MPLS i VPLS:
1. Urządzenie musi obsługiwać technologie Layer 3 MPLS VPN, Layer 2 MPLS VPN oraz VPLS. 2. Urządzenie musi obsługiwać technologię MPLS Traffic Engineering przy użyciu protokołu RSVP-TE.
VII. Usługi bezpieczeństwa:
1. Urządzenie musi pozwalać na jednoczesne zestawienie 2000 tuneli IPSec VPN. 2. Urządzenie musi pozwalać na szyfrowanie ruchu IPSec VPN z prędkością nie mniejszą niż 1Gbps. 3. Urządzenie musi pozwalać na utworzenie minimum 7000 polityk bezpieczeństwa. 4. Urządzenie musi pozwalać na konfigurację minimum 96 stref bezpieczeństwa. 5. Urządzenie musi pozwalać na konfigurację mechanizmów Antivirus, AntiSpam, Web Filtering oraz IPS po wczytaniu odpowiednich licencji. 6. Urządzenie musi zostać dostarczone wraz z licencją pozwalającą na użytkowanie mechanizmu IPS. 7. Urządzenie musi chronić przed atakami typu Denial of Service.

VIII. Zarządzanie:
1. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.
2. Urządzenie musi pozwalać na zapisanie nie mniej niż 20 poprzednich, kompletnych konfiguracji.
3. Urządzenie musi pozwalać na zdalne zarządzanie przy użyciu API opartego o język XML.
4. Urządzenie musi pozwalać na stopniowanie praw dostępu do poszczególnych gałęzi konfiguracji lub poszczególnych komend dla użytkowników administracyjnych.
5. Urządzenie musi być wyposażone w dwa porty USB, które mogą zostać wykorzystane w celu wykonania kopii zapasowej całego systemu. Urządzenie musi mieć możliwość uruchomienia przy użyciu kopii zapasowej systemu, znajdującej się na urządzeniu USB.

2.8. Zadania Wykonawcy związane z wdrożeniem systemów zarządzania i monitoringu parametrów warstwy aktywnej sieci miejskiej zintegrowanych w pomieszczeniach centrum Zarządzania Siecią

Dla sprawnej administracji i monitoringu sieci miejskiej zakłada się stworzenie Centrum Zarządzania Siecią podłączonego do urządzeń rdzenia sieci. Dlatego też należy stworzyć wydzielone logicznie Centrum Zarządzania Siecią i uwzględnić niezbędny sprzęt oraz dedykowane oprogramowanie, które będzie pełniło funkcje takie jak:

- Automatyczne zbieranie informacji z urządzeń sieciowych
- Monitorowanie parametrów sieciowych w tym pomiary wykorzystania pasma
- Przetwarzanie zebranych informacji z możliwością filtrowania i kategoryzacji
- Efektywny nadzór, diagnostyka i konfiguracja bezpiecznych tuneli IPSec VPN
- Implementacja polityki bezpieczeństwa i wykrywanie działań niezgodny z założonymi politykami
- Inwentaryzacja sprzętu i oprogramowania
- Konfigurowanie poszczególnych urządzeń przy wykorzystaniu graficznego interfejsu użytkownika

Pod pojęciem tym należy rozumieć wydzielone pomieszczenia lub szafy na sprzęt serwerowy, serwery odpowiedniej mocy, stacje obrazowania parametrów sieci oraz stanowiska robocze administratorów. W skład Centrum wchodzić będą również specjalizowane systemy informatyczne, zbierające informacje z urządzeń w całej sieci miejskiej. Proponowanymi lokalizacjami dla wykonania Centrum są:

l.p.	Symbol	Lokalizacja	Uwagi
1	CZS	Urząd Miasta, ul. Rynek 2	Wraz z GPD i IXC

Tabela 7: Proponowana lokalizacja Centrum Zarządzania Siecią

Zadaniem Wykonawcy będzie w szczególności:
- zaprojektowanie i zbudowanie systemów nadzoru i monitoringu technicznego pomieszczeń serwerowni wraz z systemami kontroli dostępu i systemem wykrywania pożarów;
- zaprojektowanie i wdrożenie urządzeń aktywnych i serwerów odpowiedzialnych za monitorowanie parametrów sieci oraz zarządzanie jej poszczególnymi elementami i usługami;
- wdrożenie polityki bezpieczeństwa i reguł zarządzania siecią miejską wraz z systemem nadzoru uprawnień dla administratorów.

2.8.1. Elementy składowe systemu Zarządzania Siecią.

Zarządzanie sieci miejskiej będzie odbywało się przy wykorzystaniu systemów centralnego zarządzania, umożliwiających monitorowanie, raportowanie i rekonfigurację urządzeń sieciowych przy wykorzystaniu uwspólnianiach interfejsów użytkownika.

Na system zarządzania powinny składać się następujące elementy:
a) system zarządzania urządzeniami realizującymi funkcje systemu bezpieczeństwa
b) system zarządzania przełącznikami sieciowymi
c) system silnego uwierzytelniania
d) system archiwizacji danych
e) dwa terminale administratorów sieci (stanowiska operatorskie) oraz serwer terminalowy dla dostępu zdalnego
f) system bezpiecznego dostępu zdalnego
g) urządzenie KVM

Dopuszczalne jest, aby pojedynczy system pełnił więcej niż jedną z wymienionych powyżej funkcjonalności, przy założeniu że spełnia on wszystkie szczegółowe wymagania poszczególnych funkcjonalności. Wymagania te zostały przedstawione w dalszej części rozdziału.

Serwery i urządzenia wchodzące w skład systemu zarządzania powinny zostać włączone w strukturę sieci przy pomocy dedykowanych przełączników dostępowych, gwarantujących wydajne połączenie z rdzeniem sieci miejskiej, oraz między samymi serwerami i urządzeniami.

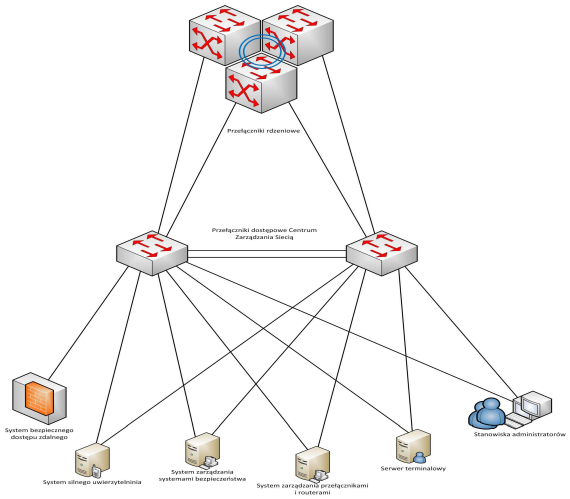
Należy zastosować **2 przełączniki dostępowe**, posiadające minimum 16 portów 10/100/1000Mb/s RJ45 oraz 4 porty 1Gb/s SFP, z których 2 powinny być wyposażone w moduły 1 Gb/s LX (LC). Porty optyczne posłużą do wykonania podłączeń do urządzenia rdzeniowego. Porty miedziane posłużą do podłączenia serwerów i gniazd punktów elektryczno-logicznych (PEL) stanowisk operatorskich i innych znajdujących się na terenie Centrum Zarządzania. Podłączenie do stanowisk operatorskich oraz podłączenie do serwerów powinno zostać zrealizowane za pomocą kabli miedzianych ekranowanych folią kat.6 poprzez panel okablowania strukturalnego kat.6 FTP znajdujący się w tej samej szafie

Minimalne wymagania przełącznika dostępowego o 16 portach downlinkowych 10/100/1000Mb/s (SW-SRV):

I. Podstawowe parametry urządzenia:
8. Urządzenie musi być dedykowanym, urządzeniem sieciowym, przystosowanym do montowania w 19” szafie rack, wysokość 1U. 9. Urządzenie musi posiadać 16 portów 10/100/1000Mb/s RJ45 oraz posiadać minimum 4 uplinki światłowodowe 1Gb/s SFP. 10. Urządzenie musi posiadać backplane o wydajności minimum 40Gb/s. 11. Urządzenie musi posiadać wydajność przełączania minimum 29,8 Mpps. 12. Urządzenie musi obsługiwać minimum 8 tysięcy adresów MAC. 13. Urządzeniu musi być zasilane prądem przemiennym o napięciu 230V i częstotliwości 50Hz. Urządzenie musi pobierać nie więcej niż 23W. 14. Urządzenie musi być przystosowane do pracy w warunkach biurowych w temperaturach 0-45 stopni Celsjusza i wilgotności 10-90%.
II. Usługi warstwy drugiej:
13. Urządzenie musi obsługiwać protokół agregacji łączy 802.3ad. 14. Urządzenie musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 4094. Obsługiwane muszą być sieci VLAN oparte o porty fizyczne, adresy MAC, protokoły L3. W celu automatycznej konfiguracji sieci VLAN, urządzenie musi obsługiwać protokół GVRP. 15. Urządzenie musi wspierać znakowanie ramek zgodnie z protokołem IEEE 802.1p. 16. Urządzenie musi obsługiwać protokół drzewa rozpinającego (Spanning Tree Protocol) w następujących wersjach: IEEE 802.1D, 802.1w oraz 802.1s. 17. Urządzenie musi obsługiwać tagowanie ramek QinQ zgodnie ze standardem IEEE 802.1ad. 18. Urządzenie musi obsługiwać standard 802.3x. 19. Urządzenie musi obsługiwać standardy 802.3ah oraz 802.1ag. 20. Urządzenie musi obsługiwać interfejsy zgodne ze standardami IEEE 802.3i, 802.3u, 802.3z, (technologie 10Base-T, 100Base-X, 1000Base-X). 21. Urządzenie musi obsługiwać ramki Jumbo. 22. Urządzenie musi obsługiwać protokół LLDP (Link Layer Discovery Protocol) oraz LLDP-MED. 23. Urządzenie musi obsługiwać mechanizmy ochrony przed burzą broadcastową i multicastową. 24. Urządzenie musi obsługiwać kopiowanie ruchu między portami (port mirroring) oraz między urządzeniami (remote port mirroring).
III. Usługi warstwy trzeciej:
5. Urządzenie musi obsługiwać routing statyczny dla protokołów IPv4 i IPv6. Urządzenie musi wspierać protokół BFD dla tras statycznych. 6. Urządzenie musi posiadać wsparcie dla IPv6, w tym IPv6 Neighbor Discovery, IPv6 Stateless Address Auto-configuration, IPv6 DiffServ Architecture oraz ICMPv6. 7. Urządzenie musi obsługiwać funkcje DHCPv6 client, DHCPv6 relay oraz DHCPv6 server. 8. Urządzenie musi obsługiwać podsłuchiwanie ramek IGMPv1/v2/v3 (IGMPv1/v2/v3 Snooping) oraz MLDv1/v2.
IV. Filtrowanie i kształtowanie ruchu:
7. Urządzenie musi umożliwiać tworzenie list kontroli dostępu (ACL) w oparciu o protokóły IPv4 i IPv6. 8. Listy ACL muszą być obsługiwane sprzętowo. 9. Urządzenie musi mieć możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu). 10. Interfejsy muszą obsługiwać kolejki typu SP, WRR oraz SP+WRR (lub równoważne) w ilości minimum 4 kolejek na port. 11. Urządzenie musi obsługiwać mechanizm kształtowania ruchu typu traffic policing. 12. Urządzenie musi obsługiwać klasyfikację ruchu QoS na podstawie adresów IPv4 i IPv6, adresów MAC oraz portu wejściowego i wyjściowego.
V. Bezpieczeństwo:
3. Urządzenie musi obsługiwać standard IEEE 802.1x. W przypadku niepowodzenia autentykacji urządzenie musi mieć możliwość umieszczenia suplikanta w odseparowanej sieci VLAN 4. Urządzenie musi pozwalać na autentykację na podstawie adresów MAC.
VI. Zarządzanie:
2. Urządzenie musi mieć możliwość zarządzania przy użyciu interfejsu linii komend za pomocą połączenia SSHv2, jak również konfiguracji za pomocą centralnego systemu zarządzania jak i interfejsu WWW.

Dostęp do zasobów CZS powinien być chroniony przy pomocy redundantnego systemu bezpieczeństwa typu stateful firewall z funkcjonalnością Intrusion Prevention System. Dopuszcza się wykorzystanie w tym celu systemu bezpieczeństwa pracującego w IXP przy zapewnieniu bezpiecznej separacji ruchu (wykorzystanie funkcjonalności wirtualnego routera lub wirtualnego systemu).

W przypadku przekroczenia przepustowości wewnętrznej urządzenia zabezpieczającego przez sumaryczny ruch sieciowy generowany przez serwery aplikacji i zarządzania siecią – przewidzieć należy rozwinięcie struktury Centrum Zarządzania Siecią do struktury przewidzianej dla CPD lub przeniesienie serwerów aplikacji do CPD, jeśli znajdzie się ono w innej lokalizacji.



Rysunek 11. Schemat połączeń między urządzeniami Centrum Zarządzania Siecią

Elementy systemu zarządzania mogą być dedykowanymi urządzeniami lub oprogramowaniem instalowanym na serwerach. Niezależnie od powyższego, należy dostarczyć wszystkie elementy wymagane do jego uruchomienia i poprawnej pracy, w tym wymagany system operacyjny oraz oprogramowanie pomocnicze, takie jak baza danych.
Wszystkie systemy dostarczane w postaci oprogramowania powinny mieć możliwość pracy w środowisku zwirtualizowanym.

W Centrum Zarządzania Siecią zlokalizowane zostaną również serwery aplikacyjne, odpowiedzialne za dostarczanie usług użytkownikom sieci miejskiej, takich jak system Publicznych Punktów Dostępu do Internetu, strony WWW, poczta elektroniczna, serwer DNS, itp.

Wszystkie elementy systemu zarządzania (z wyjątkiem systemu archiwizacji danych oraz systemu silnego uwierzytelniania) nie będące dedykowanymi urządzeniami, oraz wszystkie systemy usługowe, takie jak WWW i poczta, powinny zostać zainstalowane jako wirtualne maszyny na serwerach przeznaczonych pod system wirtualizacyjny.
Serwery pod system wirtualizacyjny powinny korzystać z pamięci masowej zlokalizowanej na macierzy dyskowej, z którą połączone zostaną dwoma dedykowanymi interfejsami Fiber Channel każdy.

Minimalne parametry serwerów oraz macierzy powinny odpowiadać parametrom jak opisano poniżej:

l.p.	Element	Parametry minimalne serwerów
1	Obudowa	Maksymalnie 1U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack)
2	Procesor	Minimum dwa procesory minimum ośmiordzeniowe , x86 - 64 bity, Intel E5-2660 lub równoważne procesory minimum ośmiordzeniowe. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org
3	Liczba procesorów	Minimum 2
4	Pamięć operacyjna	Minimum 64 GB RDIMM DDR3, z możliwością rozbudowy do minimum 768GB. Minimum 24 sloty na pamięć.
5	Sloty rozszerzeń	Minimum 2 sloty PCI-Express Generacji 3, w tym jeden slot x16 (prędkość slotu – bus width) oraz minimum jedno gniazdo pełnej wysokości.
6	Dysk twardy	Możliwość rozbudowy do 10 dysków SFF.
7	Kontroler	Kontroler macierzowy SAS wyposażony w pamięć cache 2GB oraz podtrzymywanie zawartości pamięci typu flash (FBWC) lub równoważne, zapewniający obsługę 10 napędów dyskowych SAS oraz obsługujący poziomy RAID 0/1/1+0/5
8	Karty sieciowe	Minimum 6 portów Ethernet 10/100/1000 Mb/s z funkcją Wake-On-LAN, RJ45
9	Karta Fibre Chanel	Minimum 2 porty 8Gb FC
10	Karta graficzna	Zintegrowana karta graficzna
11	Porty	1 x szeregowy 7 x USB 2.0 (w tym jeden wewnętrzny obsadzony pamięcią USB Flash Media minimum 2GB). VGA Wewnętrzny slot na kartę SD lub port uSSD.
12	Zasilacz	Minimum 2 szt., typ Hot-plug, redundantne

13	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
14	Bezpieczeństwo	Możliwość rozbudowy płyty głównej o moduł szyfrujący TPM.
15	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
16	Gwarancja	3-letnia gwarancja w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Możliwość rozbudowy okresu gwarancyjnego do min. 5 lat (usługa świadczona przez serwis producenta serwera). Producent serwera musi posiadać lokalną organizację serwisową dysponującą certyfikatem ISO 9001.

Tabela 8: Parametry minimalne serwerów z oprogramowaniem do wirtualizacji

l.p.	Element	Parametry minimalne serwera
1	Obudowa	Maksymalnie 1U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack)
2	Procesor	Minimum dwa procesory minimum ośmiordzeniowe , x86 - 64 bity, Intel E5-2660 lub równoważne procesory minimum ośmiordzeniowe. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org
3	Liczba procesorów	Minimum 2
4	Pamięć operacyjna	Minimum 16 GB RDIMM DDR3, z możliwością rozbudowy do minimum 768GB. Minimum 24 sloty na pamięć.
5	Sloty rozszerzeń	Minimum 2 sloty PCI-Express Generacji 3, w tym jeden slot x16 (prędkość slotu – bus width) oraz minimum jedno gniazdo pełnej wysokości.
6	Dysk twardy	2 x dysk 300GB typu Hot-plug SAS, 10000 obr./min., 5 x 600GB typu Hot-plug SAS 10000 obr./min., możliwość rozbudowy do 10 dysków SFF.
7	Kontroler	Kontroler macierzowy SAS wyposażony w pamięć cache 2GB oraz podtrzymywanie zawartości pamięci typu flash (FBWC) lub równoważne, zapewniający obsługę 10 napędów dyskowych SAS oraz obsługujący poziomy RAID 0/1/1+0/5
8	Karty sieciowe	Minimum 4 porty Ethernet 10/100/1000 Mb/s z funkcją Wake-On-LAN, RJ45
9	Karta graficzna	Zintegrowana karta graficzna
10	Porty	1 x szeregowy 7 x USB 2.0 (w tym jeden wewnętrzny). VGA Wewnętrzny slot na kartę SD lub port uSSD.
11	Zasilacz	Minimum 2 szt., typ Hot-plug, redundantne
12	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
13	Bezpieczeństwo	Możliwość rozbudowy płyty głównej o moduł szyfrujący TPM.
14	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
15	Gwarancja	3-letnia gwarancja w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Możliwość rozbudowy okresu gwarancyjnego do min. 5 lat (usługa świadczona przez serwis producenta serwera). Producent serwera musi posiadać lokalną organizację serwisową dysponującą certyfikatem ISO 9001.

Tabela 9: Parametry minimalne serwera systemu archiwizacji danych

l.p.	Element	Parametry minimalne serwera
1	Obudowa	Maksymalnie 1U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania serwera w szafie rack)
2	Procesor	Minimum dwa procesory minimum czterordzeniowe , x86 - 64 bity, Intel E5-2603 lub równoważne procesory minimum czterordzeniowe. W przypadku zaoferowania procesora równoważnego, wynik testu musi być publikowany na stronie www.spec.org
3	Liczba procesorów	Minimum 1
4	Pamięć operacyjna	Minimum 8 GB RDIMM DDR3, z możliwością rozbudowy do minimum 768GB. Minimum 24 sloty na pamięć.
5	Sloty rozszerzeń	Minimum 2 sloty PCI-Express Generacji 3, w tym jeden slot x16 (prędkość slotu – bus width) oraz minimum jedno gniazdo pełnej wysokości.
6	Dysk twardy	3 x dysk 300GB typu Hot-plug SAS, 10000 obr./min., możliwość rozbudowy do 10 SFF.
7	Kontroler	Kontroler macierzowy SAS wyposażony w pamięć cache 512MB oraz podtrzymywanie zawartości pamięci typu flash (FBWC) lub równoważne, zapewniający obsługę 10 napędów dyskowych SAS oraz obsługujący poziomy RAID 0/1/1+0/5
8	Karty sieciowe	Minimum 4 porty Ethernet 10/100/1000 Mb/s z funkcją Wake-On-LAN, RJ45
9	Karta graficzna	Zintegrowana karta graficzna
10	Porty	1 x szeregowy 7 x USB 2.0 (w tym jeden wewnętrzny). VGA

		Wewnętrzny slot na kartę SD lub port uSSD.
11	Zasilacz	Minimum 2 szt., typ Hot-plug, redundantne
12	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
13	Bezpieczeństwo	Możliwość rozbudowy płyty głównej o moduł szyfrujący TPM.
14	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej i graficznej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Możliwość podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
15	Gwarancja	3-letnia gwarancja w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Możliwość rozbudowy okresu gwarancyjnego do min. 5 lat (usługa świadczona przez serwis producenta serwera). Producent serwera musi posiadać lokalną organizację serwisową dysponującą certyfikatem ISO 9001.

Tabela 10: Parametry minimalne serwera systemu silnego uwierzytelniania

l.p.	Element	Parametry minimalne macierzy
1	Obudowa	Maksymalnie 2U RACK 19 cali (wraz ze wszystkimi elementami niezbędnymi do zamontowania w szafie rack)
2	Kontroler	Dwa kontrolery macierzowe pracujące w trybie active-active wyposażone w 2GB mirrorowanej pomiędzy kontrolerami pamięci Cache każdy oraz 2 interfejsy FC 8Gb na kontroler umożliwiające dołączenie do infrastruktury SAN (switch'y FC) lub bezpośrednio do serwerów. Upgrade firmware kontrolerów macierzowych on-line (bez utraty dostępu do dysków logicznych)
3	Dysk	8x 300GB typu Hot-plug SAS 150000 obr./min. Z możliwością rozbudowy do 24 dysków w pojedynczej półce
4	Zasilacze	Minimum 2 zasilacze (system redundantny) w półce
5	Pozostałe funkcje macierzy	Możliwość rozbudowy macierzy do minimum 149 dysków obsługiwanych przez parę kontrolerów macierzowych. Możliwość jednoczesnego umieszczenia w jednej półce dyskowej napędów dyskowych z interfejsem SAS oraz SATA. Funkcja LUN Masking pozwalająca na dołączenie nie mniej niż 64 serwerów do macierzy. Możlwiość utworzenia co najmniej 512 dysków logicznych. Redundantne wentylatory w półce Sprzętowy RAID 0, 1, 3, 5, 6, 10, 50 Wsparcie dla systemów operacyjnych Windows, Linux, VMware Możliwość utworzenia aktywnych dysków zapasowych Oferowana macierz powinna zapewniać możliwość wykonywania szybkich kopi danych typu Snapshot i Clone dysków logicznych na poziomie kontrolerów macierzowych. Oferowana macierz powinna wspierać min. 64 snapshoty i 128 kopii typu clone. Możliwość rozszerzenia liczby snapshot do min. 512 po dokupieniu odpowiednich licencji. Zapewnienie ciągłości dostępu do danych w przypadku uszkodzenia jednej ścieżki dostępu dla wspieranych systemów operacyjnych (Multipathing). Zarządzanie macierzą zdalnie poprzez przeglądarkę i z linii poleceń. Każdy z kontrolerów wyposażony w dwa intefejsy zarządzające: LAN i szeregowy. Obsługa oprogramowania VMware Site Recovery Manager (SRM) 5.0. Oferowana macierz powinna zapewniać możliwość przyrostowej replikacji danych pomiędzy dwoma takimi macierzami. Replikacja wykonywana sprzętowo na poziomie kontrolerów macierzowych. Aktualnie ta funkcjonalność nie jest wymagana. Dla zapewnienia kompatybilności rozwiązania macierz powinna pochodzić od producenta oferowanych serwerów.
6	Gwarancja	3-letnia gwarancja w miejscu instalacji z czasem reakcji w następnym dniu roboczym. Możliwość rozbudowy okresu gwarancyjnego do min. 5 lat (usługa świadczona przez serwis producenta macierzy). Producent macierzy musi posiadać lokalną organizację serwisową dysponującą certyfikatem ISO 9001

Tabela 11: Parametry minimalne macierzy

2.8.1.1. Wymagania dla systemu zarządzania systemami bezpieczeństwa.

Zarządzanie systemami bezpieczeństwa sieci miejskiej zostało przewidziane za pomocą centralnego systemu zarządzania, monitorowania i raportowania, zapewniając możliwość konfiguracji urządzeń i reguł polityki bezpieczeństwa z pojedynczego interfejsu użytkownika. System powinien posiadać narzędzia do monitorowania, raportowania i analizy zdarzeń związanych z funkcjonowaniem sieci i potencjalnych incydentów bezpieczeństwa.

Wymagane cechy:

- spójne monitorowanie systemów bezpieczeństwa i systemu bezpiecznego dostępu zdalnego
- możliwość implementacji globalnej polityki bezpieczeństwa w celu kontroli zagrożeń,
- przechowywanie poprzednich wersji polityk z możliwością ich przywracania,
- szczegółowe dostosowywanie uprawnień administratorów w zależności od ich roli,
- otwarte API XML / SOAP.
- może działać w konfiguracji klastrowej Active – Passive.
- może współpracować z zaawansowanym rozwiązaniem do korelacji zdarzeń i wykrywania zagrożeń (NBAD)

l.p.	Element	Parametry minimalne systemu zarządzania systemami bezpieczeństwa
1	Platforma systemowa	System musi być dostarczony jako dedykowane oprogramowanie umożliwiające instalację na systemie Linux (RHEL) oraz Solaris (SPARC). System zarządzania musi umożliwiać zarządzanie minimum 5 urządzeniami. Centralny system zarządzania ma składać się z serwera zarządzania (dostarczonego jako dedykowane oprogramowanie) oraz konsoli GUI zainstalowanej na stacjach Windows lub Linux. System musi pozwalać na zainstalowanie wielu konsol GUI w sieci.
2	Wymagania funkcjonalne centralnego systemu zarządzania	System ma umożliwiać zarządzanie urządzeniami zabezpieczeń typu IDS/IPS tego samego producenta. System ma umożliwiać zarządzanie urządzeniami zabezpieczeń typu Firewall tego samego producenta. System ma umożliwiać zarządzanie urządzeniami typu SSL VPN tego samego producenta. Składowanie baz polityk zabezpieczeń oraz log’ów ze wszystkich zarządzanych urządzeń typu firewall i IPS. Zarządzanie systemem z konsoli GUI zainstalowanej na stacjach roboczych. Konfiguracja polityk zabezpieczeń dla urządzeń IPS bez dostępu do urządzenia a następnie wyeksportowanie i załadowanie konfiguracji. Możliwość zdefiniowania jednej polityki zabezpieczeń firewall lub IPS w skali wszystkich urządzeń danego typu bądź oddzielnych polityk dla określonych urządzeń. Polityka zabezpieczeń dla urządzeń IPS składa się z reguł. Kolejność reguł określa ich priorytet. Reguły polityki zabezpieczeń dla systemu IPS muszą umożliwiać wprowadzenie następujących ustawień: a). adresy źródłowe i docelowe, b). usługi i protokoły, c). akcja zabezpieczeń, d). opcje logowania, e). opcje alarmowania (Syslog, SNMP), f). urządzenie zabezpieczeń na którym obowiązuje reguła. g). ataki i grupy ataków. h). VLAN. System powinien umożliwiać przeglądanie zawartości pakietów, w których przez system IPS zidentyfikowane zostały ataki. System musi umożliwiać definicję przez użytkownika własnych grup ataków dla systemu IPS. Śledzenie czynności wykonywanych przez administratorów zabezpieczeń. Definiowane wielu poziomów uprawnień administratorów. Przeglądanie i selekcjonowanie rejestrowanych zdarzeń. Generowane raportów na postawie rejestrowanych zdarzeń. Możliwość rozbudowy do pracy w konfiguracji HA odpornej na awarie. System musi umożliwiać powiadamianie poprzez SMTP (e-mail), skrypty użytkownika, SNMP, syslog, Generowanie raportów i monitorowanie systemu. Administratorzy zabezpieczeń powinni mieć do dyspozycji zestaw narzędzi wspomagający ich w zarządzaniu bezpieczeństwem. Korelacja i analiza rejestrowanych zdarzeń oraz prezentacja informacji o wykrywanych naruszeniach bezpieczeństwa powinna odbywać się w czasie rzeczywistym. Konsola zarządzająca powinna prezentować w formie graficznej tworzone w czasie rzeczywistym zestawienia i statystyki (m.in. najczęściej wykonywane ataki, najczęstsze źródła ataków, najczęstsze cele ataków) System zarządzania z jednej konsoli GUI umożliwia całościową konfigurację urządzeń typu firewall/VPN w zakresie systemu operacyjnego (m.in. adresacja i routing IP) oraz zabezpieczeń (m.in. firewall, VPN i QoS). System zarządzania powinien umożliwiać skonfigurowanie całości urządzenia zabezpieczeń firewall/VPN bez dostępu do urządzenia, a następnie wyeksportowanie konfiguracji do pliku. Urządzenie zabezpieczeń powinno umożliwiać załadowanie tak stworzonej konfiguracji. System zarządzania powinien umożliwiać odczyt konfiguracji istniejącej na urządzeniu zabezpieczeń oraz wprowadzenie nowej konfiguracji. System zarządzania umożliwia stworzenie jednej polityki bezpieczeństwa w skali całego przedsiębiorstwa, bądź oddzielnych polityk dla określonych urządzeń zabezpieczeń. Przejście pomiędzy politykami nie wymaga zamykania/otwierania plików polityk (tzn. administrator w jednej konsoli GUI ma jednocześnie dostęp do wielu polityk). Polityka bezpieczeństwa dla systemów zabezpieczeń typu firewall składa się z reguł. Kolejność reguł określa ich priorytet. Reguły polityki bezpieczeństwa powinny umożliwiać wprowadzenie następujących ustawień: - adresy źródłowe i docelowe, - usługi i protokoły, - akcja zabezpieczeń,

		- opcje logowania, - opcje alarmowania (Syslog, SNMP), - zarządzanie pasmem (priorytet, pasmo gwarantowane i maksymalne), - translacja adresów NAT (statyczna, dynamiczna), - uwierzytelnianie użytkowników, - ochrona antywirusowa, - ochrona przed atakami intruzów, - filtracja URL, - czas w którym obowiązuje reguła, - urządzenie zabezpieczeń na którym obowiązuje reguła. System zarządzania umożliwia wykonywanie scentralizowanej aktualizacji oprogramowania urządzeń zabezpieczeń oraz wykonywania backup-ów konfiguracji urządzeń.
3	Gwarancja	Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.8.1.2. Wymagania dla systemu zarządzania przełącznikami sieciowymi.

Powinna być to bezpieczna, zaawansowana platforma do zarządzania urządzeniami sieciowymi, która umożliwi administratorom scentralizowane konfigurowanie, aktualizowanie, monitorowanie i diagnozowanie urządzeń za pomocą łatwych w użyciu, wyświetlających wiele informacji ekranów.
System zarządzania powinien pochodzić od tego samego producenta co przełączniki sieciowe, zapewniając tym samym pełne, jednolite wsparcie i kontrolę nad strukturą sieciową sieci miejskiej.
System musi pozwalać na szczegółową analizę stanu sieci oraz jej poszczególnych elementów wraz z możliwością ich konfiguracji. Do jego zadań będzie należało generowanie obrazu aktualnej topologii, z odrębnymi widokami na warstwę drugą, warstwę trzecią oraz VLANy. System musi pozwalać na przechowywanie i analizę logów urządzeń, wykrywanie wąskich gardeł związanych ze zbyt dużym obciążeniem łączy lub samych urządzeń, oraz powiadamianie administratorów w razie wystąpienia niestabilności sieci, awarii, lub otrzymania określonego typu logu z urządzenia. Oprogramowanie powinno dawać możliwość automatycznego generowania raportów z pracy urządzeń i rozsyłania ich na wybrane adresy e-mail.
Administrator powinien mieć możliwość tworzenia reguł automatycznej reakcji na zdarzenia sieciowe pochodzące z różnych źródeł. System musi umożliwiać aktywną integrację z usługą Active Directory firmy Microsoft, ujednoliconą kontrolę dostępu w sieciach przewodowych i bezprzewodowych oraz łatwe zarządzanie z poziomu przeglądarki WWW.

Szczegółowe wymagania systemu zarządzania siecią:

I. Parametry systemu zarządzania siecią:
1. System musi być zbudowany w architekturze klient – serwer. 2. System musi mieć możliwość implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów. 3. Dostęp do sytemu zarządzania musi być realizowany przez przeglądarkę internetową. 4. System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność. 5. System zarządzania musi pełnić następujące funkcje: • Automatyczne wykrywanie topologii sieci, uwzględniającej urządzenia sieciowe jak i podłączone do przełączników urządzenia, • Monitorowanie stanu urządzeń po protokole SNMP, • Konfiguracja urządzeń po protokole SNMP, • Konfiguracja list dostępu (ACL) na zarządzanych urządzeniach, • Konfiguracja VLANów na zarządzanych urządzeniach, • Zarządzenie konfiguracją urządzeń, tworzenie backupów oraz grupowe implementowanie konfiguracji przechowywanych w systemie zarządzania, • Zarządzenie zdarzeniami, przypisywanie alarmów do różnego rodzaju zdarzeń, • Możliwość wysyłania alarmów np. mailem lub SMS'em, • Generowanie raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta, • Obrazowanie sieci w postaci mapki wraz z wyróżnianiem kolorami występujących alarmów, • Lokalizowanie portu, poprzez który dostępny jest określony adres IP lub MAC, • Możliwość zdefiniowania polityki zmieniającej ustawienia urządzeń sieciowych w przypadku wykrycia ataku sieciowego, • Możliwość utworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym. 6. System musi mieć możliwość instalacji modułów, dostarczanych przez producenta systemu, które pozwolą na rozbudowę systemu o następujące funkcjonalności: • Zarządzanie dostępem użytkowników z wykorzystaniem 802.1x, • Zarządzanie agentami na stacjach roboczych w ramach implementacji technologii Network Access Control, • Zarządzenie infrastrukturą Wi-Fi z wykorzystaniem kontrolerów bezprzewodowych, • Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA,

	• Obsługa informacji przesyłanych z wykorzystaniem NetFlow (lub protokołu równoważnego) z urządzeń sieciowych oraz obrazowanie wyników, • Zarządzenie systemem telefonii IP, • Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS.
7.	Niezbędne jest aby system zarządzania był w stanie podłączyć się i importować dane z Active Directory.
8.	System powinien wspierać dostęp dla gości w przypadku wykorzystywania 802.1x.
9.	System musi mieć możliwość automatycznego tworzenia i rozsyłania raportów.
10.	Wymagana jest możliwość tworzenia kont administratorskich z różnymi poziomami uprawnień, z możliwością przypisywania administratorów do grup urządzeń.
11.	System musi wspierać co najmniej 1400 urządzeń sieciowych różnych producentów w ramach standardowo dostarczanego sytemu.
12.	Dla wszystkich obsługiwanych standardowo urządzeń musi być dostępne nie tylko monitorowanie ale również zarządzanie, czyli możliwość modyfikacji konfiguracji urządzeń.
13.	System musi umożliwiać instalację jako wirtualny serwer działających pod kontrolą oprogramowania wirtualizacyjnego.

2.8.1.3. Wymagania dla systemu silnego uwierzytelniania

System silnego uwierzytelniania będzie zintegrowany z systemem bezpiecznego dostępu zdalnego, w celu podniesienia poziomu bezpieczeństwa. System silnego uwierzytelniania będzie zainstalowany na dedykowanym serwerze wyspecyfikowanym powyżej w tabeli 10.

System silnego uwierzytelniania powinien spełniać poniższe wymagania:

l.p.	Element	Parametry systemu silnego uwierzytelniania
1	Platforma systemowa	Dedykowane oprogramowanie przeznaczone do instalacji na systemie Linux lub FreeBSD
2	Funkcjonalność	Zarzadzanie użytkownikami musi odbywać się w oparciu o jedną bazę użytkowników; Uwierzytelnienie z wykorzystaniem telefonu komórkowego w tym aplikacji wykonanej w technologii Java lub haseł wysyłanych przez sms; Definiowanie budowy haseł jednorazowych w tym: czy maja wykorzystywać czas, czy maja być to hasła numeryczne czy alfanumeryczne, jakiej długości będą hasła oraz jaki będzie czas ich ważności (użyteczności); Możliwość uwierzytelnienie z wykorzystaniem haseł statycznych(integracja wsteczna); Możliwość współpracy z tokenami sprzętowymi firm trzecich lub innych zewnętrznych metod uwierzytelnienia; Obsługa uwierzytelnienia z wykorzystaniem protokołu RADIUS; Centralne zarzadzanie wszystkimi użytkownikami za pomocą interfejsu graficznego wykonanego w technologii WWW oraz linii komend; Zarządzanie z wykorzystaniem użytkowników, grup użytkowników oraz serwisów (kanałów uwierzytelnienia); Możliwość dodawanie dowolnych atrybutów (cech) dla użytkowników; Możliwość dodawania własnych skryptów; Możliwość konfiguracji klastra niezawodnościowego; Logowanie zdarzeń z procesów uwierzytelnień; Blokowanie ilości nieudanych prób logowania (ilość definiowana przez administratora systemu); Zdalna rejestracja w systemie (z wykorzystaniem panelu rejestracyjnego wykonanego w technologii WWW) oraz zdalne przesłanie aplikacji Java na telefon komórkowy;
3	Aplikacja na telefon	Aplikacja powinna być dostępna co najmniej na platformy: Java i iPHONE. W przypadku aplikacji Java wielkość aplikacji poniżej 32 KB co umożliwi instalację na telefonie Nokia 6310i (posiadającym ograniczenia w zakresie wielkości aplikacji Java); Praca całkowicie offline'owa; Możliwość funkcjonalności nieweryfikowalnego PIN-u do aplikacji; Możliwość dodatkowej podpowiedzi do PIN-u do aplikacji; Dowolna zmiana PINu przez użytkownika aplikacji; Możliwość dodania dowolnej liczby profili użytkownika; Obsługa haseł generowanych z wykorzystaniem czasu oraz haseł generowanych bez czasu (generowanych na bazie licznika);
4	Licencja	Licencja dla co najmniej 10 użytkowników
5	Gwarancja	Wsparcie aplikacji przez okres 3 lat
6	Modem	Możliwość instalacji modemu GSM

2.8.1.4. Wymagania dla systemu archiwizacji danych

Z uwagi na zwiększenie niezawodności i szybkości odtworzenia stanu urządzeń CZS należy również zaprojektować **system archiwizacji danych (ang.backup)**. Celem backupu jest zapewnienie bezpieczeństwa danych znajdujących się na nośnikach serwerów w Centrum Zarządzania w aspekcie możliwych awarii lub innych zdarzeń losowych naruszających dostępność danych. W szczególności celem backupu jest zabezpieczenie danych i zapewnienie skrócenia czasu ponownego uruchomienia serwerów/usług oraz udostępnienia danych krytycznych. W

związku z tym należy zaprojektować zastosowanie systemu archiwizującego o odpowiedniej pojemności. Zasady wykonywania archiwizacji danych powinny znaleźć się w Polityce Bezpieczeństwa.

2.8.1.5. Wymagania dla terminali operatorskich i serwera terminalowego

Na przełącznikach znajdujących się w CZS należy przygotować połączenie 1Gb/s do stanowiska operatorskiego dla administratorów. Wymagania minimalne dla urządzenia stanowiska operatorskiego zdefiniowano następująco:

l.p.	Element	Parametry minimalne urządzenia dla stanowiska operatorskiego
1	Typ urządzenia	Komputer przenośny klasy notebook wyposażony w dysk twardy, DVD-ROM, karty sieciowe przewodowe i bezprzewodowe oraz ekran o wymiarach min 15,6” i niezbędne oprogramowanie systemowe
2	Procesor	Intel® Core™ i5-3210M (2,50 GHz, 3 MB pamięci podr. L3, 2 rdzenie) lub równoważny procesor osiągający równoważne lub lepsze wyniki testu wydajności w teście PassMark CPU Mark według wyników opublikowanych na stronie http://cpubenchmark.net
3	Układy głowne	Mobile Intel® HM76 Express
4	Pamięć RAM	4 GB pamięci DDR3 SDRAM 1600 MHz, 2 gniazda SODIMM, możliwość rozbudowy do 16GB
5	Wyświetlacz	Ekran LED HD+ 39,6 cm (15,6"), rozdzielczość 1600x900, z powłoką przeciwodblaskową
6	Napędy dyskowe	Dysk SATA II 500 GB, 7200 obr./min, DVD+/-RW SuperMulti DL
7	Klawiatura	Odporna na zalanie klawiatura z oddzielną częścią numeryczną
8	Touchpad	Tabliczka dotykowa z przewijaniem i obsługą gestów
9	Kamera	Kamera internetowa 720p HD
10	Interfejs sieciowy	Zintegrowana karta sieciowa Intel 82579V Gigabit, Karta sieciowa Broadcom 802.11a/b/g/n Zintegrowany moduł HP z technologią Bluetooth 4.0+ EDR
11	Karta dźwiękowa	SRS Premium Sound wbudowane głośniki stereo Wbudowany mikrofon (zespół dwóch mikrofonów w przypadku instalacji opcjonalnej kamery internetowej) Wyjście słuchawek stereo/wyjście sygnałowe audio Wejście mikrofonu stereo
12	Porty rozszerzeń	2 port USB 3.0 2 porty USB 2.0 1 port DisplayPort 1 port 1394a 1 gniazdo zasilania 1 gniazdo RJ-11 1 gniazdo RJ-45 1 złącze dokowania 1 złącze akumulatora dodatkowego 1 port combo eSATA/USB 2.0 1 port VGA 1 port szeregowy 1 gniazdo kart Express Card/54 1 czytnik kart SD/MMC
13	Zasilanie	Sprawność energetyczna Certyfikat ENERGY STAR® Zasilacz zewnętrzny Smart 65 W; Technologia HP Fast Charge 6-ogniwowy akumulator litowy HP Long Life (55 Wh) Czas pracy baterii: 6-ogniwowy akumulator litowo-jonowy (55 Wh): do 7 godzin 15 min
14	Oprogramowanie	Pakiet Microsoft® Office Starter: niepełne wersje programów Word i Excel® z funkcjami reklamowymi. Brak programów PowerPoint® i Outlook®. Kup pakiet Office 2010, aby w pełni korzystać z wszystkich funkcji Microsoft Security Essentials Adobe® Flash Player PDF Complete Corporate Edition Gotowość do obsługi Skype (wymagany jest dostęp do Internetu) WinZip Basic Preinstalowany oryginalny Windows 7 Profesional Oprogramowanie do zabezpieczenia dysku twardego przed skutkami uderzeń współpracujące z czujnikiem przyśpieszenia Oprogramowanie do usuwania danych z dysków twardych
15	Bezpieczeństwo	Oprogramowanie zabezpieczające klasy Security Manager lub równoważne, czyli elastyczna platforma umożliwiająca zarządzanie funkcjami zabezpieczeń z poziomu pojedynczej konsoli. Moduły oprogramowania zabezpieczającego zapewniają możliwość elastycznego projektowania rozwiązań z zakresu bezpieczeństwa spełniających określonego wymagania i modyfikowania ich, gdy te wymagania się zmienią menadżera danych uwierzytelniających, technologia Computrace Pro, menedżer dostępu do urządzenia, szyfrowanie zawartości dysku, rozpoznawanie twarzy, menedżer prywatności, oprogramowanie Embedded Security. Zwiększone zabezpieczenia komputera przed jego uruchomieniem Wbudowane oprogramowanie umożliwiające dostęp do zablokowanego systemu, np. które umożliwia odpowiedź na 3 osobiste pytania, co pozwala na identyfikację użytkownika i ponowne uzyskanie przez niego dostęp do systemu. Gniazdo blokady zabezpieczającej
16	Gwarancja	Roczna gwarancja podstawowa

2.8.1.6. Wymagania dla systemu bezpiecznego dostępu zdalnego

Zarządzanie siecią powinno odbywać się tylko i wyłącznie z poziomu stacji operatorskich lub serwera terminalowego. Dostęp do serwera terminalowego powinien być możliwie restrykcyjny i realizowany przy wykorzystaniu bezpiecznych, szyfrowanych kanałów opartych o protokół SSL oraz o ile jest to możliwe IPSEC. System powinien sam umożliwić automatyczne przejście z protokołu SSL na IPSEC po wykryciu takiej możliwości.

W zależności od uprawnień użytkowników będzie możliwość przepuszczania/filtrowania ruchu tych użytkowników do poszczególnych urządzeń Centrum Zarządzania z dokładnością do określonych usług udostępnianych przez serwery.

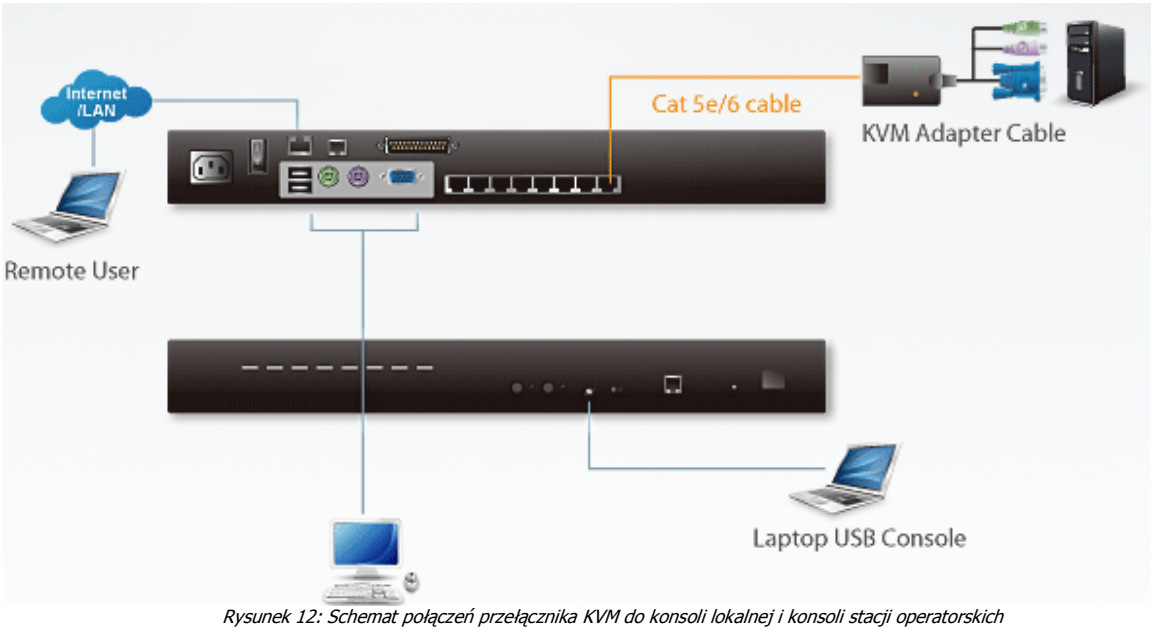
l.p.	Element	Parametry minimalne systemu bezpiecznego dostępu zdalnego
1	Platforma sprzętowa i systemowa.	1 Urządzenie musi być oparte o dedykowaną platformę sprzętową. Musi zapewniać obsługę co najmniej 10 jednoczesnych sesji SSL VPN z możliwością rozbudowy do 100 jednoczesnych sesji 2 Urządzenie typu Appliance Rack Mount. Zasilanie z sieci 230v/50Hz
2	Wymagania funkcjonalne urządzenia	1. Urządzenie musi oferować zróżnicowane metody dostępu do zasobów: • dostęp podstawowy (min. aplikacje Web; standardowe protokoły pocztowe – IMAP, POP3,SMTP; współdzielenie plików – NETBIOS, NFS; usługi terminalowe – telnet, SSH), • dostęp do aplikacji klient-serwer (enkapsulacja dowolnej aplikacji TCP w protokół HTTPS) be konieczności zastosowania dodatkowych licencji, • pełen dostęp sieciowy bez konieczności zastosowania dodatkowych licencji - praca w trybie wysokiej dostępności (SSL) oraz wysokiej wydajności (ESP wraz z kompresją treści). Możliwość automatycznego przełączania z trybu wysokiej wydajności do trybu wysokiej dostępności. 2. Rozwiązanie musi umożliwiać autentykację użytkowników w oparciu o: • serwery RADIUS, • usługi katalogowe LDAP, Microsoft Active Directory, Novell NDS/eDirectory, • lokalna baza danych użytkowników, • system RSA SecurID, • certyfikaty X.509, • serwery NIS 3. Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat, hasło statyczny plus hasło dynamiczne). Musi istnieć możliwość rozdzielenia serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów. 4. Urządzenie musi umożliwiać obsługę CRL poprzez http. 5. Urządzenie musi umożliwiać dynamiczne przyznawanie praw dostępu do zasobów w zależności od: spełnienia określonych warunków przez użytkownika zdalnego, węzeł zdalny, parametry sieci oraz parametry czasowe. 6. Urządzenie musi umożliwiać szczegółową weryfikację stanu bezpieczeństwa węzła zdalnego. Musi istnieć możliwość: • sprawdzenia obecności konkretnego procesu, pliku, wpisu w rejestrze Windows • sprawdzenia czy włączono odpowiednie usługi zabezpieczeń zarówno w momencie logowania jak w trakcie trwania sesji, • sprawdzenia czy wszystkie pobierane pliki pośrednie i pliki tymczasowe instalowane w czasie logowania są usuwane w momencie wylogowania, • sprawdzenia przed zalogowaniem takich atrybutów jak adres IP, typ przeglądarki, certyfikaty cyfrowe, • integracji z systemami weryfikacji stanu bezpieczeństwa firm trzecich, 8. Urządzenie musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny. Musi istnieć możliwość tworzenia konfiguracji nadmiarowej, w której węzły klastra zlokalizowane są w LAN bądź w odległych graficznie sieciach i komunikują się poprzez sieć WAN. 9. System musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku budowania konfiguracji nadmiarowych. 10. Urządzenie musi być zarządzane poprzez przeglądarkę Web 11. Urządzenie musi umożliwiać integrację z zewnętrznymi serwerami SNMP v.2 oraz SYSLOG 12. Urządzenie musi przechowywać dwie wersje oprogramowania oraz umożliwiać reset do wersji fabrycznej. 13. Urządzenie musi zapewniać możliwość współpracy z rozwiązaniem klasy NAC tego samego producenta w zakresie jednokrotnego uwierzytelnienia użytkowników, tj. status uwierzytelnienia użytkownika na urządzeniu dostępowym SSL jest automatycznie i w sposób przezroczysty dla użytkownika przekazywany do urządzenia kontrolującego infrastrukturę NAC.
3	Gwarancja	Wraz z produktem wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta, wysyłkę sprawnego sprzętu w 24h od zgłoszenia awarii, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.8.1.7. Wymagania dla urządzenia KVM

Do obsługi zgromadzonych serwerów w zakresie sterowania myszką i klawiaturą i wyświetlania informacji a monitorze przewiduję się zastosowanie 1 zestawu urządzeń KVM over NET o minimum 8 portach pozwalających na podłączenie, po zastosowaniu odpowiednich adapterów – serwerów z wejściami PC PS/2, USB, MAC, SUN oraz urządzeń wykorzystujących złącze serial i przekazywanie sygnałów (Keyboard, Video, Mouse) do konsoli lokalnej i na konsole komputerów zdalnych (poprzez sieciowy protokół TCP/IP). Przewidziano 1 zestaw łącznie dla systemu serwerów z systemem wirtualizacji, serwera systemu archiwizacji oraz serwera systemu silnego uwierzytelniania., zestaw ten powinien składać się z:

- Rackowy przełącznik KVMoverNET o min. 8 portach dla serwerów i portami konsol zdalnych/lokalnych
- Adaptery KVM-RJ45 do podłączenia serwerów w ilości odpowiedniej do liczby serwerów (min. 4)
- Lokalnej konsoli rackowej 1U wyposażonej w monitor LCD min. 17” i zestaw klawiatura + mysz/trackball/touchpad
- Oprogramowania terminalowego

Każdy serwer znajdujący się w szafie aktywnej zostanie podłączony do portów RJ45 urządzenia KVM zintegrowanym kablem KVM-RJ45 o wejściach odpowiednich dla danego serwera. W przypadku większych odległości między serwerem a KVM możliwe jest również podłączenie adapterem KVM-RJ45 i osobnym kablem budynkowego okablowania strukturalnego UTP (zasięg do 40m).
Urządzenie KVM over NET zostanie podłączone kablem KVM do konsoli znajdującej się w szafie serwerowni i wyposażonej w monitor LCD i zestaw klawiatura + mysz/trackball/touchpad. Monitor i urządzenia wejściowe będą zainstalowane w wersji konsolowej w szafie aktywnej (dostosowany do montażu w rack 19” 1U). Dostęp lokalny administratora jest możliwy także poprzez port lokalnej konsoli Laptop USB. Dostęp zdalny administratorów będzie możliwy poprzez przeglądarkę internetową uruchamianą na stanowiskach operatorskich co wymaga podłączenie urządzenia KVM do portów miedzianych przełączników w CZS.



Rysunek 12: Schemat połączeń przełącznika KVM do konsoli lokalnej i konsoli stacji operatorskich

Dostęp zdalny do konsoli serwerów jak i ustawień przełącznika KVM powinien zostać objęty jednolitą polityką bezpieczeństwa i uzyskiwany regułami dostępu poprzez podsystem dostępu zdalnego. Zadaniem Wykonawcy będzie odpowiednie zaprojektowanie i wykonanie bezpiecznej topologii systemów zarządzających

l.p.	Element	Parametry minimalne
1	Podstawowe parametry urządzeń systemu KVM	Przełącznik KVM over NET w konfiguracji z min. 8 portami RJ45 w obudowie pozwalającej na łatwe zamontowanie w stelażu 19”. Oddzielne gniazdo USB do bezpośredniego podłączenia laptopa i łatwej obsługi konsoli. Osobna magistrala do zdalnego dostępu na zasadzie KVM over IP. Obsługa łączności PS/2, USB, SUN Legacy (13W3), oraz szeregowej (RS-232). Konsola lokalna z obsługą klawiatury i myszy PS/2 oraz USB.

		Obsługa wielu platform: Windows, MAC, Sun i Linux. Wysoka jakość obrazu – do 1600 x 1200 przy 60Hz i przy odległości do 40m oraz 1280 x 1024 przy 75Hz i odległości do 50 m. Możliwość łańcuchowego połączenia do 15 dodatkowych modułów i kontrolowania do 128 komputerów z jednej konsoli. Obudowa 1U 19”.
2	Porty rozszerzeń	Port KVM: 8 x żeńskie złącze RJ-45 do podłączenia serwerów. Klawiatura: 1 x 6-pinowe żeńskie złącze Mini-DIN (fioletowe), 1 x żeńskie złącze USB typu A (białe). Mysz: 1 x 6-pinowe żeńskie złącze Mini-DIN (zielone), 1 x żeńskie złącze USB typu A (białe). Grafika: 1 x żeńskie złącze HDB-15 (niebieskie). Port do połączeń łańcuchowych: 1 x męskie złącze DB-25 (czarne). Port LAN: 1 x żeńskie złącze RJ-45. Uaktualnianie oprogr. Sprzęt.: 1 x żeńskie złącze RJ-11 (czarne). PON: 1 x żeńskie złącze RJ-45. Port Laptop USB: 1 x żeńskie złącze USB Mini typu B (czarne).
3	Zasilanie	Param. Napięcia wej.: 100~240V; 50/60 Hz; 1A. Gniazdo zasilania: 1 x 3-stykowe gniazdo zasilania AC.
4	Zarządzanie	Do 64 kont użytkowników – obsługa 32 użytkoników zalogowanych jednocześnie i kontrolujących systemy. Obsługa kończenia sesji – administrator może zakończyć działającą sesję. Rejestrowanie zdarzeń oraz obsługa windowsowego serwera dziennika zdarzeń. Lokalny dziennik zdarzeń. Identyfikator adaptera – zawiera dane na temat portu i umożliwia administratorowi przeniesienie serwera na inny port bez konieczności zmiany konfiuracji adapterów i przełącznika. Jednoczesny dostęp do serwera przez wielu użytkowników. Możliwość uaktualniania oprogramowania sprzętowego. Obsługa IPv6. Interfejs graficzny: lokalna konsola oparta na przeglądarce oraz AP GUI. Obsługa klientów na różnych platformach (Windows, Mac OS X, Linux, Sun). Obsługa wielu przeglądarek (IE, Mozilla, Firefox, Safari, Opera, Netscape). Interfejs użytkownika oparty na przeglądarce, zbudowany w całości w technikach aplikacji webowych – administrator może wykonywać swoje zadania także z koputerów bez zainstalowanego oprogramowania Java. Rozsyłanie sygnałów z klawiatury – znak wprowadzony z klawiatury może być duplikowany na wszystkie podłączone serwery. Możliwość regulacji jakości sygnału wideo i tolerancji na potrzeby uzyskania optymalnego transferu danych; ustawienie obrazu monochromatycznego; ustwienie progów i szumów oraz kompresji danych w przypadku korzystania z łączy o niskiej przepustowości. Wyświetlanie obrazu na pełnym ekranie lub po przeskalowaniu. Tablica komunikatów umożliwiająca komunikowanie się użytkowników zdalnych. Automatyczna synchronizacja lokalnych i zdalnych ruchów myszy. Klawiatura ekranowa z obsługą wielu języków. Obsługa makr uruchamianych przy kończeniu sesji. Dostęp na pozomie BIOS-u.
5	Zaawansowane zabezpieczenia	Obsługa zdalnego uwierzytelniania: RADIUS, LDAP, LDAPS, oraz MS Active Directory. 128-bitowe szyfrowanie SSL zabezpieczające hasło podczas logowania. Elastyczna infrastruktura szyfrowania – użytkownik może wybrać dowolną kombinację metod 56-bitoego DES, 168-bitowego 3DES, 256-bitoego AES, 128-bitowego RC4 lub losowo – niezależne szyfrowanie komunikacji z klawiaturą/myszą i sygnału wizyjnego. Filtr IP/MAC zapewniający zaawansowaną ochronę. Możliwość konfigurowania uprawnień użytkowników i grup do uzyskania dostępu do serwerów.
6	Konsola lokalna	Typ urządzenia: zintegrowana konsola wysuwana z obudowy 1U z monitorem LCD min. 17” Wyświetlacz LCD min. 17” rozdzielczość 1280 x 1024@75Hz; DDC2B Kompatybilny z przełącznikami KVM z wyjściami PS/2 Może być wyłączony gdy panel LCD jest zgaszony Frontowy panel można schować gdy nie jest używany Dostosować do montaży w rack 19” (1U) Emulacja DDC – ustawienia VGA są autowmatycznie dostosowywane do parametrów wyświetlacza LCD W komplecie jeden kabel 2L-5202P 1,8m do podłączenia komputera PS/2
7	Wymagania gwarancyjne	Roczna gwarancja podstawowa
8	Wyposażenie dodatkowe	Kabel KVM-RJ45 o typie i odpowiedniej długości potrzebnej do podłączenia serwerów Oznaczenia (naklejki) zgodnie z wymogami projektów unijnych

3. Warunki odbioru robót.

Wytyczne dla odbioru poszczególnych prac projektowych i wykonawczych w zakresie wykonawstwa kanalizacji teletechnicznych oraz kabli światłowodowych nie odbiegają szczególnie od ogólnie spotykanych wymagań, co do odbiorów prac projektowych i wykonawczych określanych przez normy branżowe operatorów. W szczególności jednak wytyczne te zdefiniowano i zestandaryzowano w części drugiej dokumentacji koncepcyjnej tj. w Wytycznych projektowo-wykonawczych.

Wykonawca powinien zgłosić Zamawiającemu gotowość do odbioru danego etapu na 3 dni robocze przed planowanym terminem odbioru.

Zamawiający zastrzega sobie prawo do bieżącej kontroli postępu i jakości wykonywanych prac.

3.1. Odbiór dokumentacji projektowej:

Termin odbioru dokumentacji projektowej zgodnie z przyjętym harmonogramem wynosi 6 miesięcy od podpisania umowy o wykonanie zadania. Dokumentacja projektowa może zostać odebrana po dostarczeniu Zamawiającemu wszystkich egzemplarzy wraz z wersją elektroniczną. Przedstawiony projekt musi zawierać wszelkie niezbędne uzgodnienia oraz decyzje administracyjne zgodne z Prawem Budowlanym dla infrastruktury telekomunikacyjnej.

Zamawiający lub Inżynier Kontraktu działający w imieniu Zamawiającego oceni jakość zaproponowanych w projekcie rozwiązań technicznych, kompletność dostarczonej dokumentacji projektowej, jej zgodność z przyjętą przez Zamawiającego Koncepcją techniczną budowy sieci. Sprawdzeniu podlegać będzie również czy Wykonawca dostarczył niezbędne załączniki takie jak kosztorys i harmonogram prac wykonawczych.

Po zatwierdzeniu przez Zamawiającego projektów, kosztorysu oraz harmonogramu dalszych prac Wykonawca może przystąpić do dalszej części wykonywania zadania.

3.2. Odbiór prac związanych z wykonawstwem kanalizacji teletechnicznej i mikrokabli

Odbiory będą przeprowadzane przez upoważnionego przez Zamawiającego Inspektora Nadzoru lub przez pracownika Inżyniera Kontraktu. Zakres odbiorów określają stosowne normy i wytyczne Zamawiającego. Wykonawca będzie zobowiązany w szczególności do informowania Zamawiającego o zakończonych etapach prac, a w szczególności o pracach zanikowych lub ulegających zakryciu. Odbiory będą dokonywane na podstawie formularzy zdawczo-odbiorczych Zamawiającego.

Przed przystąpieniem do instalacji kabli światłowodowych Wykonawca zobowiązany jest do przeprowadzenia próby szczelności wybudowanej kanalizacji.

3.3. Odbiór prac wdrożeniowych poszczególnych systemów i urządzeń

Odbiory będą przeprowadzane przez upoważnionego przez Zamawiającego Inspektora Nadzoru lub przez pracownika Inżyniera Kontraktu. Sprawdzeniu będzie podlegała ocena zgodności wykonanych prac z Koncepcją techniczną sieci oraz zatwierdzonymi przez Zamawiającego projektami dostarczonymi przez Wykonawcę, zgodność parametrów zainstalowanych urządzeń z wymaganiami oraz jakość instalacji. Dokonane również zostanie sprawdzenie funkcjonowania systemu oraz jego funkcjonalność. Dopuszcza się odbiory częściowe zgodnie z przyjętym harmonogramem prac.

3.4. Odbiór dokumentacji powykonawczej oraz odbiór końcowy

Po wykonaniu wszystkich elementów Wykonawca jest zobowiązany do dostarczenia kompletnej dokumentacji powykonawczej, aczkolwiek Zamawiający wymaga, aby dokumentacja powykonawcza dla poszczególnych systemów realizowanych we wcześniejszych etapach dostarczana była w terminie odbioru prac w zakresie pozwalającym na ocenę wykonanych prac. Ostateczny termin oddania kompletnej dokumentacji częściowej danego etapu powinien zamknąć się w terminie do 30 dni od odbioru etapu. Format dokumentacji musi być jednolity i zestandaryzowany umożliwiając identyfikacje każdego etapu.

Dostarczenie kompletnej i jednolitej dokumentacji powykonawczej musi nastąpić w terminie określonym w harmonogramie prac. Ocenie podlegać będzie jej kompletność oraz odwzorowanie rzeczywiście wykonanych prac. Wykonanie zadania zostaje potwierdzone dopiero protokołem zdawczo-odbiorczym odbioru końcowego, na którym zostanie sprawdzona całość wykonanych prac pod kątem zakresu, jakości i terminowości.

II. CZĘŚĆ INFORMACYJNA PROGRAMU FUNKCJONALNO-UŻYTKOWEGO

1. Oświadczenie zamawiającego stwierdzające jego prawo do dysponowania nieruchomością na cele budowlane

Zamawiający informuje, że w trakcie prac koncepcyjnych wytyczając trasę kanalizacji dołożono wszelkich starań, aby jej przebieg lokalizowany był w obiektach lub na terenach, których właścicielem jest miasto lub Skarbu Państwa. W szczególności dotyczy to wykorzystania zasobów kanalizacji wodnej jako medium dla kabli magistralnych.
Zamawiający pozyskał we własnym zakresie zgody właścicieli i zarządców obiektów, w których ulokowane będą elementy węzłów sieci miejskiej na wykonanie w nich prac modernizacyjnych oraz posadowienie infrastruktury sieciowej. W obiektach niebędących w gestii Inwestora a zarządzanych przez podmioty zależne - zgodę na wykorzystanie wskazanych pomieszczeń zawierają stosowne porozumienia zawarte przez Urząd Miasta z tymi jednostkami.

Wszystkie trasy kablowe lub trasy kanalizacji należy lokalizować na terenach będących w gestii miasta lub Skarbu Państwa, tak aby nie zachodziła potrzeba uzyskania zgód od właścicieli prywatnych lub podmiotów prawnych niebędących powiązanych z Beneficjentem. W przypadku zmiany przebiegów trasowych Wykonawca na własny koszt pozyska odpowiednie zgody gestorów terenów.

2. Przepisy prawne i normy związane z projektowaniem i wykonaniem zamierzenia budowlanego

Dokumenty stanowiące ogólne wytyczne odnośnie projektów Społeczeństwa Informacyjnego:

- Strategia kierunkowa rozwoju informatyzacji Polski do roku 2013 oraz perspektywiczna prognoza transformacji społeczeństwa informacyjnego do roku 2020
- Strategia szerokopasmowego dostępu do usług społeczeństwa informacyjnego w Polsce na lata 2007-2013,
- Plan działań na rzecz rozwoju elektronicznej administracji (e-Government) na lata 2005-2006
- Narodowa Strategia Spójności 2007-2013
- i2010 - Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia
- Krajowe Wytyczne dot. kwalifikowania wydatków w ramach Funduszy Strukturalnych i Funduszu Spójności w okresie programowania 2007-2013

Polskie akty prawne powiązane z tematyką miejskich sieci telekomunikacyjnych:

- „Ustawa Prawo telekomunikacyjne z dnia 16 lipca 2004 roku”.
- „Ustawa o świadczeniu usług droga elektroniczna z dnia 18 lipca 2002 roku”
- „Ustawa o dostępie warunkowym”
- „Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym”.
- „Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 roku”.
- Prawo Ochrony Środowiska z dnia 27 kwietnia 2001r., w zakresie zasad ochrony środowiska oraz warunków korzystania z jego zasobów
- Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych1

Ramy prawne Komisji Europejskiej w sektorze komunikacji elektronicznej

- Dyrektywa (2002/19/EC) z dnia 7 marca 2002r. w sprawie dostępu do sieci łączności elektronicznej i urządzeń towarzyszących oraz ich łączenia (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
- Dyrektywa (2002/20/EC) z dnia 7 marca 2002 r. w sprawie zezwoleń na udostępnianie sieci i usługi łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.);
- Dyrektywa (2002/21/EC) z dnia 7 marca 2002r. w sprawie jednolitej struktury regulacji dla sieci i usług komunikacji elektronicznej (DZ. Urz. WE L. 108 z 24 kwietnia 2002r.);
- Dyrektywa (2002/22/EC) z dnia 7 marca 2002r. w sprawie usługi powszechnej i praw użytkowników odnoszących się do sieci i usług łączności elektronicznej (Dz. Urz. WE L. 108 z 24 kwietnia 2002r.) ;
- Dyrektywa (2002/58/EC) z dnia 12 lipca 2002r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. Urz. WE L. 201 z 31 lipca 2002r.);
- Dyrektywa (2002/77/EC) z dnia 16 września 2002r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej (Dz. Urz. WE L. 249 z 17 września 2002r.);
- Rozporządzenie (EC) 2887/2000 o niezależnym dostępie do pętli lokalnych

Normy projektowe Inwestora

- Wymagania techniczno-projektowe dla infrastruktury pasywnej w Miejskiej Sieci Szerokopasmowej

- Wymagania wykonawcze i odbiorowe dla prac wykonywanych w ramach budowy infrastruktury pasywnej Miejskiej Sieci Szerokopasmowej
- Wymagania dla formatu i zawartości dokumentacji projektowej Miejskiej Sieci Szerokopasmowej

Normy projektowe uzupełniające

- Ustawa z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (MegaUstawa)
- Rozporządzenie Ministra Infrastruktury z dnia 26 października 2005 r. w sprawie warunków technicznych, jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie,
- Rozporządzenie Ministra Infrastruktury z dnia 22 czerwca 2010 r. zmieniające rozporządzenie w sprawie warunków technicznych, jakim powinny odpowiadać telekomunikacyjne obiekty budowlane i ich usytuowanie
- Rozporządzenie Ministra Łączności z dnia 21 kwietnia 1995 r. w sprawie warunków technicznych zasilania energią elektryczną obiektów budowlanych łączności. (Dz. U. z dnia 17 maja 1995 r.)
- Normy zakładowe Telefonii DIALOG S.A. ZN-02/TD S.A.-01 – Projektowanie i budowa sieci telekomunikacyjnej - Ogólne zasady projektowania i budowy sieci kablowych
- Normy zakładowe Telefonii DIALOG S.A. ZN-02/TD S.A.-02 - Projektowanie kanalizacji kablowej
- Normy zakładowe Telefonii DIALOG S.A. ZN-02/TD S.A.-02 - Projektowanie sieci optotelekomunikacyjnych
- ZN-96/TPSA-017. Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE). Wymagania i badania.
- ZN-96/TPSA-023. Studnie kablowe. Wymagania i badania.
- ZN-96/TPSA-024. Zasobnik złączowy. Wymagania i badania.
- ZN-96/TPSA-025. Taśmy ostrzegawcze i ostrzegawczo-lokalizacyjne. Wymagania i badania.
- ZN-96/TPSA-026. Słupki oznaczeniowe i oznaczeniowo-pomiarowe. Wymagania i badania.
- ZN-96/TPSA-041 Zabezpieczone pokrywy studni kablowych, dodatkowe (wewnętrzne). Wymagania i badania.
- Normy PN-79/E-08106 – Urządzenia elektroenergetyczne, stopnie ochrony

Przy projektowaniu i budowie segmentu radiowego należy wziąć pod uwagę następujące normy i rekomendacje komitetu ITU:

- Recommendation ITU-R 838, Specific Attenuation Model For Rain For Use In Prediction Methods - [Rekomendacja (zalecenie) ITU-R P.838-3: „Ścisły (specyficzny) model do zastosowania w metodach przewidywania tłumienia przez deszcz”]
- Recommendation ITU-R P.676-3, Attenuation By Atmospheric Gases - [Rekomendacja (zalecenie) ITU-R P676.3: „Tłumienie przez gazy atmosferyczne”]
- Recommendation ITU-R Pn 837-1, Characteristics Of Precipitation For Propagation Modelling - [Rekomendacja (zalecenie) ITU-R PN 837-1: „Charakterystyki opadów atmosferycznych dla modelowania propagacji”] Recommendation ITU-R P.530-7, Propagation Data And Prediction Methods Required For The Design Of Terrestrial Line-Of-Sightsystems - [Rekomendacja (zalecenie) ITU-PN P530-7: „Dane propagacyjne i metody przewidywania wymagane dla projektowania systemów naziemnych z linią bezpośredniej widzialności”

3. Inne posiadane informacje i dokumenty niezbędne do zaprojektowania robót budowlanych

Zamawiający informuje, że nie posiada dla terenów, przez które przebiega planowana kanalizacja teletechniczna łącznikowa oraz przyłącza do obiektów a nie objętych Planem Zagospodarowania Przestrzennego decyzji lokalizacyjnej Inwestycji Celu Publicznego. W przypadku potrzeby zmiany trasy relacji kablowej wykorzystującej kanalizację ściekową lub deszczową spowodowanej przyczynami technicznymi, kolizją z uzbrojeniem terenowym lub innymi kwestiami - zadaniem Wykonawcy będzie uzyskanie tej decyzji na drodze administracyjnej, jeśli okaże się niezbędna. Zakres możliwych zmian i związane z tym koszty Wykonawca musi oszacować we własnym zakresie.

4. Zalecenia konserwatorskie konserwatora zabytków

Zamawiający informuje, że na chwile obecną brak jest szczególnych wytycznych nadzoru konserwatorskiego dla planowanej inwestycji. Szczegółowe informacje zawarte są w Planie Zagospodarowania Przestrzennego, natomiast dla terenów nie objętych planem należy występować po uzgodnienia do Konserwatora Zabytów.

5. Porozumienia, zgody lub pozwolenia związane z realizacją inwestycji

Zamawiający informuje, że na potrzeby prowadzonej inwestycji zawarł następujące porozumienia lub uzgodnienia z podmiotami współpracującymi:

Miejskie Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o w Żywcu – porozumienie w zakresie wykorzystania kanalizacji deszczowej i sanitarnej na potrzeby budowy żywieckiej światłowodowej sieci szerokopasmowej.

Dyrektorzy poszczególnych jednostek samorządowych – uzgodnienia i pozwolenia w zakresie miejsc posadowienia szaf teleinformatycznych stanowiących węzły (GPD, PAG, LPD) i punkty końcowe sieci (PA) oraz infrastrukturę radiowych punktów dostępowych RDP.

Wykonawca będzie działał w oparciu o zgody i pozwolenia, wszelkie trudności i konflikty z jednostkami zarządzającymi obiektami, w których zlokalizowano węzły powstałe związane z wyznaczaniem miejsca na posadowienie infrastruktury w trakcie prac projektowych - Zamawiający zobowiązuje się rozwiązywać wspólnie z Wykonawcą wobec podmiotu wnoszącego sprzeciw.

6. Dodatkowe wytyczne inwestorskie i uwarunkowania związane z budową i jej przeprowadzeniem

Przed przystąpieniem do realizacji prac projektowych, **należy zapoznać się z planami modernizacyjnymi** spółek komunalnych, posiadających swoją infrastrukturę na terenie miasta. Do przyjętych planów modernizacji, należy dopasować harmonogram prac wykonawczych w ramach tworzenia infrastruktury światłowodowej projektu sieci.

Przed przystąpieniem do prac projektowych należy przeprowadzić **weryfikację stanu istniejącej** infrastruktury teletechnicznej. W ramach oceny, należy skupić się w głównej mierze na istniejących rurach przeznaczonych dla okablowania światłowodowego, wymienionych poniżej oraz wybudowanych po dacie zamknięcia prac koncepcyjnych. Należy sprawdzić stan oraz drożność ułożonych rur RHDPE40 i ocenić możliwość prowadzenia w nich okablowania światłowodowego.

III. Załączniki programu funkcjonalno-użytkowego

Rysunek 1.0. Mapa i przebiegu relacji kablowych wg typu kanalizacji
Rysunek 2.0 Wstępny schemat rozpływu kabli optycznych
Rysunek 3.0. Model atomowy połączeń międzywęzłowych sieci miejskiej
Rysunek 4.0 Rzut planowanej serwerowni

Załącznik A. Lista wszystkich punktów węzłowych sieci miejskiej
Załącznik B. Zestawienie szacowanych długości relacji kablowych
Załącznik C. Zestawienie ilościowe materiałów i urządzeń