PROGRAM

FUNKCJONALNO – UŻYTKOWY

Nazwa nadana zamówieniu przez Zamawiającego:

Regionalna Platforma Cyfrowa Dorzecza Wieprzy i Grabowej II –

Infrastruktura Szerokopasmowej Sieci Teleinformatycznej

Adres obiektu budowlanego, którego dotyczy program funkcjonalno-użytkowy:

Obiekty Jednostek Samorządu Terytorialnego należące do miasta Sławno, powiatu Sławno oraz gmin Sławno, Postomino i Malechowo zgodnie z tabelą: Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej.

Nazwy i kody grup robót:

32510000-1 Bezprzewodowy system telekomunikacyjny

32420000-3 Urządzenia sieciowe

71320000-7 Usługi inżynieryjne w zakresie projektowania

45232300-5 Roboty budowlane i pomocnicze w zakresie budowy linii telefonicznych i ciągów (tele)komunikacyjnych

Nazwa Zamawiającego oraz jego adres:

GMINA MIASTO SŁAWNO
ul. M. C. Skłodowskiej 9
76-100 Sławno

Imiona i nazwiska osób opracowujących program funkcjonalno-użytkowy:

Dariusz Jankowski
PRODAR
Al. Niepodległości 797/1
81-810 Sopot

Spis zawartości programu funkcjonalno-użytkowego:

I. CZĘŚĆ OPISOWA PROGRAMU FUNKCJONALNO-UŻYTKOWEGO

1. OPIS OGÓLNY PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest Program funkcjonalno-użytkowy dla zadania: „Regionalna Platforma Cyfrowa Dorzecza Wieprzy i Grabowej II – Infrastruktura Szerokopasmowej Sieci Teleinformatycznej”.

Przedmiotem niniejszego przedsięwzięcia jest realizacja powiatowej światłowodowo-radiowej sieci szerokopasmowej WAN. Podstawowym zadaniem w ramach projektu jest budowa systemu okablowania światłowodowego i systemu łączności radiowej. Dodatkowo wybudowany będzie system transmisyjny powiatowej sieci szerokopasmowej, której podstawowym zadaniem będzie świadczenie usług transmisji danych i dostępu do Internetu.

Strategicznym celem przedsięwzięcia jest pobudzenie rozwoju gospodarczego regionu dzięki wykorzystaniu technologii informacyjnych, których dostępność zapewni sieć szerokopasmowa. W ramach projektu do jednolitej sieci teleinformatycznej zostaną podłączone urzędy i podległe jednostki organizacyjne sektora publicznego oraz będzie realizowany cel projektu, jakim jest upowszechnienie dostępu do Internetu szerokopasmowego na terenach wykluczonych cyfrowo.

Całość sieci lub jej część transmisyjna będzie mogła być wydzielona i zarządzana przez specjalne do tego celu powołanego Operatora Infrastruktury.

Podstawowym celem budowy niniejszej sieci jest stworzenie warunków dla Jednostek Samorządu Terytorialnego do realizacji zadań własnych z uwzględnieniem poprawy dostępu do szerokorozumianych usług internetowych, w tym w obszarach zagrożonych wykluczeniem cyfrowym. Wybudowana sieć będzie siecią opartą w znacznej części o łącza światłowodowe, wobec czego jej rozwój w kierunku zwiększana pasma i świadczenia nowych usług (np. transmisja głosu, obrazu) praktycznie nie będzie ograniczony.

W ramach części transmisyjnej projektu zostanie zrealizowany jeden węzeł główny, w którym możliwe będzie uruchomienie minimum jednego punktu styku do operatorów dostarczających usługę dostępu do globalnego internetu, w celu dostarczenia tej usługi do Jednostek Samorządu Terytorialnego. Dla zabezpieczania usługobiorców systemu transmisyjnego sieci powiatowej wybudowany zostanie system bezpieczeństwa IT.

Dla realizacji przyjętych założeń zostanie wybudowana infrastruktura pasywna tj. rurociągi teletechniczne, maszty sieci radiowej oraz sieć kabli światłowodowych i przęseł transmisji radiowej opartych o nielicencjonowane częstotliwości.

Topologię sieci wyznaczają punkty adresowe zlokalizowane w pobliżu obiektów wymienionych w tabeli: Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej zamieszczonej w rozdziale 1.1.

W ramach projektu będą dostarczone i zainstalowane urządzenia szkieletowe sieci i urządzenia dostępowe, które będą wykorzystywane dla świadczenia usług transmisyjnych dla wybranych miejskich, powiatowych i gminnych jednostek organizacyjnych oraz przyłączenia ich do sieci Internet. Urządzenia szkieletowe sieci WAN i urządzenia zapewniające styk z operatorami zapewniającymi usługę dostępu do Internetu i innych sieci zewnętrznych (router peeringowy) dla całej sieci zostanie zlokalizowany w serwerowni wyznaczonej przez Zamawiającego. Przyjęto założenie, że serwerownia, w której będzie zainstalowany sprzęt będzie wyposażona w kompletną infrastrukturę: klimatyzację, kontrolę dostępu, systemy ochrony mienia. Dostawca zapewni realizację systemu awaryjnego podtrzymania zasilania.

Wyposażenie serwerowni nie jest przedmiotem niniejszego projektu.

Urządzenia szkieletowe sieci zostaną zlokalizowane w Serwerowni Urzędu Miejskiego w Sławnie.

Projekt będzie realizowany na terenie powiatu Sławno. W projekcie biorą udział:

- Miasto Sławno
- Powiat Sławno
- Gmina Sławno

- Gmina Postomino
- Gmina Malechowo

Do projektu nie przystąpiła gmina Darłowo.

Powstała w ramach projektu sieć będzie strukturą niezależną od istniejących sieci operatorów działających obecnie na rynku. Do sieci tej planowane jest podłączenie takich instytucji publicznych jak: Urzędy Miasta, Urzędy Gminy, szkoły średnie i podstawowe, przedszkola, szpitale, jednostki policji, biblioteki publiczne oraz inne ważne instytucje. Planowane jest uruchomienie czterech węzłów dystrybucyjnych w jednostkach gminnych. Na terenach gmin planuje się budowę infrastruktury dostępowej na potrzeby jednostek. Docelowa liczba jednostek i węzłów na potrzeby projektu została przedstawiona w tabeli: Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej zamieszczonej w rozdziale 1.1.

Przedmiotowa infrastruktura teleinformatyczna wybudowana będzie w celu:

- dostarczenie usług szerokopasmowych dla instytucji miejskich,
- dostarczenie usług szerokopasmowych dla operatorów „ostatniej mili”

W przyszłości sieć może być również wykorzystana do realizacji:

- systemu monitoringu gmin;
- systemu informacji turystycznej (multimedialne punkty informacyjne dla turystów);
- systemu ostrzegania przed zagrożeniami (system sygnalizacji pożarowej, powodziowej);
- systemu kontroli medycznej (monitorowanie ruchu karetek, pacjentów itp.);
- systemu automatycznego odczytywania liczników (wodociągowych, gazowych, itp.);
- systemu monitorowania pojazdów użyteczności społecznej (autobusy, taxi);
- systemu zdalnego pobierania opłat parkingowych;
- systemów dedykowanych dla sieci instytucji publicznych (np. biblioteki, szkoły);
- systemu informacji przystankowej;
- zintegrowanego systemu kontroli dostępu (sygnalizacja włamania).

Planowana sieć szerokopasmowa będzie siecią, która w swoich założeniach ma umożliwić operatorom „ostatniej mili” (operatorzy ISP) dostęp do usług oraz oferowanie klientom końcowym - instytucjom publicznym na obszarze projektu, wielu usług realizowanych poprzez wydajną sieć szerokopasmową. Aby zaprojektować efektywną sieć otwartą dla innych operatorów należy wybrać odpowiednią architekturę, która umożliwi realizację założeń projektu.

Jako najkorzystniejsze rozwiązanie dla planowanej sieci szerokopasmowej planuje się budowę sieci trójwarstwową:

- warstwę szkieletową,
- warstwę dystrybucyjną,
- warstwę dostępową.

Rozwiązanie takie daje łatwiejsze utrzymanie sieci, uproszczone zarządzanie, zmniejsza czas potrzebny na zlokalizowanie awarii, zmniejsza ogólne koszty utrzymania sieci.

1.1 Charakterystyczne parametry określające wielkość obiektu lub zakres robót budowlanych

Projekt sieci szerokopasmowej obejmie obiekty przedstawione w poniższej tabeli:

Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej

L.p.	Symbol	Nazwa	Dokładny adres	Nr działki	Charakter miejsca (szkoła/ świetlica/ itp.)	Rodzaj dostępu (światłowód/radio)
1	SM01	Urząd Miejski w Sławnie	M.C. Skłodowskiej 9	585 obr.2	Instytucja publiczna	światłowód
2	SM01A	Urząd Gminy Sławno	M.C. Skłodowskiej 9	585 obr.2	Instytucja publiczna	światłowód
3	SM02	Szkoła podstawowa nr 3	Stefanii Sempołowskiej 3	77 i 78 obr.2	szkoła	światłowód
4	SM03	MKRPA (Miejska Komisja Rozwiązywania Problemów Alkoholowych)	Rapackiego 10	293 obr.2	Instytucja publiczna	światłowód
5	SM04	SDK (Sławieński Dom Kultury) + lokalizacja kamery	Cieszkowskiego 2	972 obr.2	dom kultury	światłowód
6	SM05	Przedszkole Miejskie nr 4	Cieszkowskiego 1	230 obr.2	przedszkole	światłowód
7	SM06	Przedszkole Miejskie nr 1	Wojska Polskiego 2	583 obr. 2	przedszkole	światłowód
8	SM07	Szkoła podstawowa nr 1	Kossaka 31	636 obr. 3	szkoła	światłowód
9	SM08	Przedszkole Miejskie nr 3	Filtrowa 1	642 obr. 3	przedszkole	światłowód
10	SM09	MPGKIM (lokalizacja kamery - monitoring)	Polanowska 43	242/2 obr. 3	kamera	światłowód
11	SM10	GKI (Wydział Gospodarki Komunalnej i Inwestycji - UM w Sławnie)	Polanowska 41	240/3 obr. 3	Instytucja publiczna	światłowód
12	SM11	Gimnazjum Miejskie	Plac Sportowy 1	977/5 obr. 2	szkoła	światłowód
13	SM12	Ośrodek Sportu i Rekreacji	Plac Sportowy 1	977/5 obr. 2	Instytucja publiczna	światłowód
14	SM13	Miejski Ośrodek Pomocy Społecznej	Mielczarskiego 1	279/2 obr. 2	Instytucja publiczna	światłowód
15	SM14	Przedszkole Miejskie nr 2	Jedności Narodowej 22	872/4 obr. 2	przedszkole	światłowód
16	SM15	Sklep (lokalizacja kamery - monitoring)	M.C. Skłodowskiej	239 obr. 2	kamera	światłowód
17	SM16	Komenda Policji (dyżurka monitoring)	Gdańska 2	235 obr. 2	policja - monitoring	światłowód
18	SM17	LUX (lokalizacja kamery – monitoring)	Wyszyńskiego	331/1 obr. 2	kamera	światłowód
19	SM18	Hotele W Starym Kinie (lokalizacja kamery – monitoring)	Jedności Narodowej 20	871 obr. 2	kamera	światłowód
20	SM19	SDH (lokalizacja kamery – monitoring)	Wyszyńskiego	681 obr. 2	kamera	światłowód
21	SM20	Budynek mieszkalny (lokalizacja kamery – monitoring)	Racibora 6	1367 obr. 2	kamera	światłowód
22	SM21	Targowisko miejskie – lokalizacja kamery – monitoring)	Mickiewicza 24	627/8 obr 2.	kamera	światłowód
23	SM22	Budynek mieszkalny (lokalizacja kamery – monitoring)	Dworcowa 2	21/22 obr. 3	kamera	światłowód
24	SM23	Latarnia ślimak obwodnicy (lokalizacja kamery – monitoring)		115/5 obr. 3	kamera	światłowód
25	SM24	MiniLUX (lokalizacja kamery – monitoring)	Skrzyżowanie Prusa – Moniuszki	493 obr. 3	kamera	światłowód
26	SM25	Budynek mieszkalny (lokalizacja kamery – monitoring)	Witosa 6	1371/1 obr. 2	kamera	światłowód
27	SM26	Latarnia przy Gimnazjum (lokalizacja	Plac Sportowy 1	969 obr. 2	kamera	światłowód

		kamery – monitoring)				
28	SM00	Maszt Energa GPZ Sławno	Koszalińska 43	638 i 639 obr. 3	maszt	światłowód
29	SP00	Starostwo Powiatowe w Sławnie	76-100 Sławno, ul. Sempołowskiej	357/13 obr.2	Instytucja publiczna	światłowód
30	SP01	Powiatowa Poradnia Psychologiczno - Pedagogiczna w Sławnie	76-100 Sławno, ul. Kopernika 9	914 obr. 2	poradnia	światłowód
31	SP02	Wielofunkcyjna Placówka Opiekuńczo-Wychowawcza w Sławnie	76-100 Sławno, ul. Cieszkowskiego 4B	202/4 obr. 2	szkoła	światłowód
32	SP03	Szpital Powiatowy w Sławnie	76-100 Sławno, ul. I Pułku Ułanów 9	54/2 obr.2	szpital	światłowód
33	SP04	Specjalny Ośrodek Szkolno - Wychowawczy dla Dzieci i Młodzieży Niepełnosprawnej im. Marii Grzegorzewskiej w Sławnie	76-100 Sławno, ul. Kopernika 9	914 obr. 2	szkoła	światłowód
34	SP05	Zespół Szkół Zawodowych w Sławnie	76-100 Sławno, ul. I-go Pułku Ułanów 11	335 obr.2	szkoła	światłowód
35	SP06	Zespół Szkół Agrotechnicznych w Sławnie	76-100 Sławno, ul. Sempołowskiej 2	357/16 obr.2	szkoła	światłowód
36	SP07	Zespół Szkół im. Jana Henryka Dąbrowskiego w Sławnie	76-100 Sławno, ul. Cieszkowskiego 4B	202/5 obr.2	szkoła	światłowód
37	DP01	Dom Dziecka im. J. Korczaka w Darłowie	76-150 Darłowo, ul. Morska 78	58/2 obr.10	dom dziecka	radio
38	DP02	Zespół Szkół Morskich w Darłowie	76-150 Darłowo, ul. Szpitalna 1	143 obr.13	szkoła	radio
39	DP03	Muzeum - Zamek Książąt Pomorskich w Darłowie	76-150 Darłowo, ul. Zamkowa 4	512	muzeum	radio
40	SG01	Gimnazjum w Sławsku	Sławsko 97	427/7	szkoła	światłowód
41	SG02	Gimnazjum we Wrześnicy	Wrześnica 19A	259	szkoła	radio
42	SG03	SP Żukowo	Żukowo 65	116/4	szkoła	radio
43	SG04	SP Boleszewo	Boleszewo 61	199	szkoła	radio
44	SG05	SP Bobrowice	Bobrowice 22-23	67,68	szkoła	radio
45	SG06	SP Gwiazdowo	Gwiazdowo 43	209	szkoła	radio
46	SG07	SP Warszkowo	Warszkowo 33a	794/4	szkoła	radio
47	SG08	Świetlica Kwasowo	Kwasowo 1a	194/16	świetlica	światłowód
48	SG09	Świetlica Smardzewo	Smardzewo 35a	320	świetlica	radio
49	SG10	OSP Stary Kraków	Stary Kraków 35a	174	remiza OSP	światłowód
50	SG11	Świetlica Radosław	Radosław 9	213	świetlica	radio
51	SG12	Świetlica Tychowo	Tychowo 23a	272	świetlica	radio
52	SG13	Świetlica Janiewice	Janiewice 64a	698	świetlica	radio
53	SG14	Świetlica Brzeście	Brzeście 23a	98	świetlica	radio
54	SG15	Świetlica Łętowo	Łętowo 40/1	211/2	świetlica	radio
55	SG16	Świetlica Warszkówko	Warszkówko 26	31/2	świetlica	radio
56	SG17	Świetlica Noskowo	Noskowo 40b	15/2	świetlica	radio
57	SG18	Świetlica Rzyszczewo	Rzyszczewo 28c	92/5	świetlica	radio
58	SG19	Świetlica Bobrowiczki	Bobrowiczki 26c	349/2	świetlica	radio
59	PG01	Urząd Gminy Postomino	76-113 Postomino 30	253	Instytucja publiczna	światłowód
60	PG02	GOPS Postomino	76-113 Postomino 30	253	Instytucja publiczna	światłowód
61	PG03	ZS Jarosławiec	76-107 Jarosławiec, Bałtycka 65b	164/1, 378/9	zespół szkół	światłowód
62	PG04	ZS Postomino	76-113 Postomino 15c	246/5, 146	zespół szkół	światłowód
63	PG05	ZS Pieszcz	76-113 Postomino, Pieszcz 46	76/3	zespół szkół	radio
64	PG06	SP Staniewice	76-113 Postomino, Staniewice 61	164/2	szkoła	światłowód
65	PG07	ZSS Korlino	76-113 Postomino, Korlino 4a	337/3	zespół szkół	radio
66	PG08	Biblioteka Postomino	76-113 Postomino 30	253	biblioteka	światłowód

67	PG09	Centrum Kultury i Sportu Postomino	76-113 Postomino 97	159/1	Instytucja publiczna	światłowód
68	PG10	Agencja Mienia Gminnego i Spraw Publicznych	76-113 Postomino 94	59	Instytucja publiczna	światłowód
69	PG12	Punkt Informacji Turystycznej Jarosławiec	76-107 Jarosławiec, Nadmorska 30	259/4	Instytucja publiczna	światłowód
70	PG13	Centrum Aktywności Społecznej Postomino	76-113 Postomino 85a	286/2	Instytucja publiczna	światłowód
71	PG14	Świetlica Kanin	76-113 Postomino, Kanin	199	świetlica	światłowód
72	PG15	Świetlica Nacmierz	76-113 Postomino, Nacmierz	310/2	świetlica	światłowód
73	PG16	Świetlica Rusinowo	76-113 Postomino, Rusinowo	428/2	świetlica	radio
74	PG17	Świetlica Królewo	76-113 Postomino, Królewo	100/2	świetlica	radio
75	PG18	Świetlica Łącko	76-113 Postomino, Łącko	163/1	świetlica	radio
76	PG19	Świetlica Chudaczewo	76-113 Postomino, Chudaczewo	194/1	świetlica	światłowód
77	PG20	Świetlica Masłowice	76-113 Postomino, Masłowice	99/1	świetlica	światłowód
78	PG21	Świetlica Pałowo	76-113 Postomino, Pałowo	117	świetlica	radio
79	PG22	Świetlica Pałówko	76-113 Postomino, Pałówko	21	świetlica	radio
80	PG23	Świetlica Nosalin	76-113 Postomino, Nosalin	246	świetlica	radio
81	PG24	Świetlica Staniewice	76-113 Postomino, Staniewice	320	świetlica	światłowód
82	PG25	Świetlica Wilkowice	76-113 Postomino, Wilkowice	50/1	świetlica	radio
83	PG26	Świetlica Marszewo	76-113 Postomino, Marszewo	130/2	świetlica	radio
84	PG27	Świetlica Pieszcz	76-113 Postomino, Pieszcz	190/2	świetlica	radio
85	PG28	Świetlica Karsino	76-113 Postomino, Karsino	54	świetlica	radio
86	PG29	Świetlica Mazów	76-113 Postomino, Mazów 8	20	świetlica	radio
87	MG01	Urząd Gminy Malechowo	76-142 Malechowo 22A	425/2	Instytucja publiczna	światłowód
88	MG02	Gminny Ośrodek Pomocy Społecznej w Malechowie	76-142 Malechowo 22A	425/2	Instytucja publiczna	światłowód
89	MG03	Zespół Ekonomiczno Administracyjny w Malechowie	76-142 Malechowo 22A	425/2	Instytucja publiczna	światłowód
90	MG06	Gminna Biblioteka Publiczna w Malechowie	76-142 Malechowo 55	492	Instytucja publiczna	światłowód
91	MG07	Gimnazjum w Malechowie	76-142 Malechowo 65B	179 i 180	Szkoła	światłowód
92	MG08	Straż Gminna w Malechowie	76-142 Malechowo 67B	476/3	Instytucja publiczna	światłowód
93	MG09	Gminna Biblioteka Publiczna Filia w Niemicy	76-142 Malechowo, Niemica 31	256/16	Instytucja publiczna	radio
94	MG10	Szkoła Podstawowa w Niemicy	76-142 Malechowo, Niemica 31	256/16	Szkoła	radio
95	MG11	Gminna Biblioteka Publiczna Filia w Lejkowie	76-142 Malechowo, Lejkowo	150/8	Instytucja publiczna	radio
96	MG12	Szkoła Podstawowa w Lejkowie	76-142 Malechowo, Lejkowo 11	150/10	Szkoła	radio
97	MG14	Zespół Szkół w Ostrowcu	76-129 Ostrowiec 61	198/6	Szkoła	światłowód
98	MG15	Gminna Biblioteka Publiczna Filia w Ostrowcu	76-129 Ostrowiec 61	198/6	Instytucja publiczna	światłowód
99	MG17	ŚOW w Przystawach	76-142 Malechowo, Przystawy 5	179/2	Świetlica	radio
100	MG18	ŚOW w Laskach	76-142 Malechowo, Laski 15	36/236	Świetlica	radio
101	MG19	ŚOW w Święcianowie	76-142 Malechowo,	219	Świetlica	światłowód

			Święcianowo 41			
102	MG20	ŚOW w Sulechowie	76-142 Malechowo, Sulechowo 56A	282/4 i 282/5	Świetlica	radio
103	MG21	ŚOW w Kosierzewie	76-129 Ostrowiec, Kosierzewo 11	25/58	Świetlica	światłowód
104	MG22	ŚOW w Pękaninie	76-142 Malechowo, Pękanino 7	41/4	Świetlica	radio
105	MG23	ŚOW w Kusicach	76-142 Malechowo, Kusice 4	25/7	Świetlica	radio
106	MG24	ŚOW w Karwicach	76-142 Malechowo, Karwice 20A	76/3 i 76/4	Świetlica	radio
107	MG25	ŚOW w Ostrowcu	76-129 Ostrowiec, Ostrowiec 15	126/5	Świetlica	światłowód
108	MG26	ŚOW w Podgórkach	76-129 Ostrowiec, Podgórki 29A	189/51	Świetlica	światłowód
109	MG28	Gminna Biblioteka Publiczna Filia w Pękaninie	76-142 Malechowo, Pękanino	41/4	Instytucja publiczna	radio

Tabela 2. Lokalizacje węzłów szkieletowych szerokopasmowej sieci teleinformatycznej

L.p.	Symbol	Nazwa	Dokładny adres	Typ węzła
1	SM01	Urząd Miejski w Sławnie	M.C. Skłodowskiej 9	węzeł główny
2	MG01	Urząd Gminy Malechowo	76-142 Malechowo 22A	węzeł
3	MG21	ŚOW w Kosierzewie	76-129 Ostrowiec, Kosierzewo 11	węzeł
4	PG01	Urząd Gminy Postomino	76-113 Postomino 30	węzeł
5	PG14	Świetlica Kanin	76-113 Postomino, Kanin	węzeł

Tabela 3. Lokalizacje masztów telekomunikacyjnych szerokopasmowej sieci teleinformatycznej

L.p.	Symbol	Nazwa	Dokładny adres	Nr działki	Wysokość masztu [m]
1	SM00	Maszt Energa GPZ Sławno - istniejący	Koszalińska 43	638 i 639 obr. 3	50
2	DP01	Dom Dziecka im. J. Korczaka w Darłowie	76-150 Darłowo, ul. Morska 78	58/2 obr.10	5-35
3	DP02	Zespół Szkół Morskich w Darłowie	76-150 Darłowo, ul. Szpitalna 1	143 obr.13	5-35
4	DP03	Muzeum - Zamek Książąt Pomorskich w Darłowie	76-150 Darłowo, ul. Zamkowa 4	512	5-35
5	SG01	Gimnazjum w Sławsku	Sławsko 97	427/7	5-35
6	SG02	Gimnazjum we Wrześnicy	Wrześnica 19A	259	5-35
7	SG03	SP Zukowo	Żukowo 65	116/4	5-35
8	SG04	SP Boleszewo	Boleszewo 61	199	5-35
9	SG05	SP Bobrowice	Bobrowice 22-23	67,68	5-35
10	SG06	SP Gwiazdowo	Gwiazdowo 43	209	5-35
11	SG07	SP Warszkowo	Warszkowo 33a	794/4	5-35
12	SG09	Świetlica Smardzewo	Smardzewo 35a	320	5-35
13	SG10	OSP Stary Kraków	Stary Kraków 35a	174	5-35
14	SG11	Świetlica Radosław	Radosław 9	213	5-35
15	SG12	Świetlica Tychowo	Tychowo 23a	272	5-35
16	SG13	Świetlica Janiewice	Janiewice 64a	698	5-35
17	SG14	Świetlica Brzeście	Brzeście 23a	98	5-35
18	SG15	Świetlica Łętowo	Łętowo 40/1	211/2	5-35
19	SG16	Świetlica Warszkówko	Warszkówko 26	31/2	5-35
20	SG17	Świetlica Noskowo	Noskowo 40b	15/2	5-35
21	SG18	Świetlica Rzyszczewo	Rzyszczewo 28c	92/5	5-35
22	SG19	Świetlica Bobrowiczki	Bobrowiczki 26c	349/2	5-35
23	PG01	Urząd Gminy Postomino	76-113 Postomino 30	253	5-35
24	PG05	ZS Pieszcz	76-113 Postomino, Pieszcz 46	76/3	5-35
25	PG06	SP Staniewice	76-113 Postomino, Staniewice 61	164/2	5-35
26	PG07	ZSS Korlino	76-113 Postomino, Korlino 4a	337/3	5-35
27	PG14	Świetlica Kanin	76-113 Postomino, Kanin	199	5-35
28	PG15	Świetlica Naćmierz	76-113 Postomino, Nacmierz	310/2	5-35
29	PG16	Świetlica Rusinowo	76-113 Postomino, Rusinowo	428/2	5-35
30	PG17	Świetlica Królewo	76-113 Postomino, Królewo	100/2	5-35
31	PG18	Świetlica Łącko	76-113 Postomino, Łącko	163/1	5-35
32	PG21	Świetlica Pałowo	76-113 Postomino, Pałowo	117	5-35
33	PG22	Świetlica Pałówko	76-113 Postomino, Pałówko	21	5-35
34	PG23	Świetlica Nosalin	76-113 Postomino, Nosalin	246	5-35
35	PG25	Świetlica Wilkowice	76-113 Postomino, Wilkowice	50/1	5-35
36	PG26	Świetlica Marszewo	76-113 Postomino, Marszewo	130/2	5-35
37	PG27	Świetlica Pieszcz	76-113 Postomino,	190/2	5-35

			Pieszcz		
38	PG28	Świetlica Karsino	76-113 Postomino, Karsino	54	5-35
39	PG29	Świetlica Mazów	76-113 Postomino, Mazów 8	20	5-35
40	MG01	Urząd Gminy Malechowo	76-142 Malechowo 22A	425/2	5-35
41	MG09	Gminna Biblioteka Publiczna Filia w Niemicy	76-142 Malechowo, Niemica 31	256/16	5-35
42	MG10	Szkoła Podstawowa w Niemicy	76-142 Malechowo, Niemica 31	256/16	5-35
43	MG11	Gminna Biblioteka Publiczna Filia w Lejkowie	76-142 Malechowo, Lejkowo	150/8	5-35
44	MG12	Szkoła Podstawowa w Lejkowie	76-142 Malechowo, Lejkowo 11	150/10	5-35
45	MG17	ŚOW w Przystawach	76-142 Malechowo, Przystawy 5	179/2	5-35
46	MG18	ŚOW w Laskach	76-142 Malechowo, Laski 15	36/23	5-35
47	MG19	ŚOW w Święcianowie	76-142 Malechowo, Święcianowo 41	219	5-35
48	MG20	ŚOW w Sulechowie	76-142 Malechowo, Sulechowo 56A	282/4 i 282/5	5-35
49	MG21	ŚOW w Kosierzewie	76-129 Ostrowiec, Kosierzewo 11	25/58	5-35
50	MG22	ŚOW w Pękaninie	76-142 Malechowo, Pękanino 7	41/4	5-35
51	MG23	ŚOW w Kusicach	76-142 Malechowo, Kusice 4	25/7	5-35
52	MG24	ŚOW w Karwicach	76-142 Malechowo, Karwice 20A	76/3 i 76/4	5-35
53	MG26	ŚOW w Podgórkach	76-129 Ostrowiec, Podgórki 29A	189/51	5-35
54	MG28	Gminna Biblioteka Publiczna Filia w Pękaninie	76-142 Malechowo, Pękanino	41/4	5-35

1.1.1 Kablowa sieć światłowodowa

Przedmiotem opracowania jest budowa Powiatowej Sieci Szerokopasmowej na terenie większej części Powiatu Sławieńskiego. Część kablowa tej sieci przebiega przez tereny miasta Sławno oraz gmin Sławno, Postomino i Malechowo. Opracowanie swoim zakresem obejmuje prace projektowe i prace wykonawcze dotyczące wykorzystania budowy nowych ciągów światłowodowych (kabli optotelekomunikacyjnych). Ponadto niniejsze opracowanie odnosi się do wdrożenia sieci IP/MPLS oraz urządzeń dostępowych na potrzeby realizacji połączeń i świadczenia usług wyłącznie na potrzeby własne Powiatu oraz zapewnienia bezpieczeństwa sieci IT dla obiektów w tabeli: Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej.

Do wymienionych w powyższej tabeli obiektów lub w ich pobliżu należy wybudować kable światłowodowe jednomodowe o pojemności 72 włókien. Biorąc pod uwagę ewentualne przyszłe rozbudowy systemu Inwestor może wymagać zwiększenia ilości włókien na poszczególnych odcinkach sieci. W takich przypadkach pojemność i ilość kabli światłowodowych będzie ograniczona jedynie ilością i przekrojem rur zastosowanych do budowy rurociągów teletechnicznych. Długość trasowa sieci światłowodowej przeznaczonej do realizacji w ramach niniejszego zadania wynosi 70 km, w tym 51,5 km sieci światłowodowej szkieletowej i 18,5 km sieci światłowodowej dostępowej.

Zakończenia części pasywnej sieci światłowodowej, takie jak przełącznice światłowodowe, półki zapasu, itp. oraz urządzenia aktywne (routery, przełączniki, urządzenia bezpieczeństwa sieci IT), wraz z dodatkowym osprzętem, zasilaczami awaryjnymi (UPS) i odpowiednim systemem chłodzenia zostaną zainstalowane w szafach 19 calowych o wysokości 45U lub 42U i wymiarach 800 x 800 mm w dedykowanych pomieszczeniach technicznych podłączanych obiektów lub w specjalnych szafach zewnętrznych.

Kable światłowodowe wybudowane w ramach niniejszego projektu należy zakończyć:

- na przełącznicy światłowodowej zlokalizowanej wewnątrz budynku w dedykowanym do tego celu pomieszczeniu lub
- na przełącznicy światłowodowej zlokalizowanej w specjalnej szafie zainstalowanej na zewnątrz budynku najlepiej w pasie drogowym w bezpośrednim sąsiedztwie studni kablowej.

Decyzja o zakończeniu sieci światłowodowej wewnątrz budynku lub w szafce na zewnątrz budynku zapadnie na etapie opracowywania projektu budowlanego sieci światłowodowej.

W Powiatowej Sieci Szerokopasmowej rurociągi teletechniczne wykonane będą w postaci zestandaryzowanych rurociągów kablowych HDPE układanych bezpośrednio w ziemi, równolegle w wiązkach 3 rur. Rury na całej długości rurociągu kablowego nie powinny krzyżować się w żadnym miejscu lub zamieniać miejscami z rurami sąsiednimi. Przewiduje się zastosowanie ciągów wykorzystujących standardowe rury HDPE 40/3,7mm. Na terenie miasta Sławno założono wykonanie rurociągów z dwóch rur HDPE 40/3,7 i jednej rury mikrokanalizacji. Dla potrzeb realizacji sieci dostępowej na terenach miejskich wskazane jest wykorzystanie istniejącej infrastruktury Inwestora, a także dopuszcza się wykorzystanie istniejącej infrastruktury obcych operatorów (pierwotna kanalizacja teletechniczna, rurociągi kablowe). W przypadku wykorzystania pierwotnej kanalizacji teletechnicznej obcego operatora należy wybudować w niej kanalizację wtórną złożoną wyłącznie z 1 rury mikrokanalizacji.

Uwaga:

Na odcinkach skrzyżowań z ciekami wodnymi i innymi szczególnymi przeszkodami terenowymi, gdzie niezbędne jest wykonanie przewiertu sterowanego rurociąg kablowy należy wybudować w rurze osłonowej HDPE Ø140.

1.1.2 Łącza radioliniowe

W punkcie tym opisano zakres prac związanych z wybudowaniem łączy radioliniowych. Opracowanie obejmuje swoim zakresem prace projektowe i wykonawcze dotyczące wykorzystania istniejącej infrastruktury budowlanej oraz budowy nowej infrastruktury telekomunikacyjnej na potrzeby realizacji sieci połączeń radioliniowej.

Łączna długość radiolinii przeznaczona do realizacji w ramach niniejszego zadania wynosi ok. 129 km. Łączna liczba łączy radioliniowych punkt-punkt wyniesie 45 łączy. Łączna liczba masztów telekomunikacyjnych lub konstrukcji wsporczych radiolinii do wybudowania wyniesie 53 szt.

Wyposażenie pojedynczego węzła radioliniowego powinno składać się z:

- Masztu,
- Urządzenia zewnętrznego ODU wraz z anteną,
- Urządzenia wewnętrznego IDU
- Szafy telekomunikacyjnej 19”
- Klimatyzacji (jeśli niezbędna).

W lokalizacjach wskazanych w tabeli: Tabela 3. Lokalizacje masztów telekomunikacyjnych szerokopasmowej sieci teleinformatycznej należy wybudować maszty telekomunikacyjne o wysokości od 5 do 35m n.p.t. w zależności od lokalizacji, tak aby przyszłe łącza radioliniowe zrealizowane pomiędzy poszczególnymi lokalizacjami miały bezpośrednią widoczność optyczną LOS (Line of Sight) oraz zapewniały przynajmniej 60% wolnej strefy Fresnela. Spełni to podstawowe wymaganie przy projektowaniu łączy radioliniowych.

Zakończenia aktywne urządzeń radioliniowych należy umieścić w 19” szafach sprzętowych o wymiarach 600 x 800 mm zainstalowanych w pomieszczeniach wewnątrz budynków. Jeśli jest to możliwe szafy te powinny być instalowane w specjalnie przygotowanych do tego celu pomieszczeniach (serwerownie).

Transmisja danych poprzez urządzenia radioliniowe obywać się będzie w paśmie nielicencjonowanym, które nie wymaga uzyskania stosownych pozwoleń radiowych i jest pasmem wolnym od opłat administracyjnych.

1.1.3 Główny węzeł szkieletowy

Główny węzeł szkieletowy będzie wyposażony w następujące komponenty:

- Główny przełącznik szkieletowy
- Centralny Firewall
- System podtrzymania zasilania – UPS

W głównym węźle szkieletowym będą podłączone następujące usługi i systemy:

- Centrum Zarządzania Bezpieczeństwem Sieci
- Operatorzy oferujący usługę dostępu do globalnego Internetu

Główny węzeł szkieletowy będzie połączony z węzłami szkieletowymi łączem MetroEthernet 1 Gb/s.

Lista obiektów, w których będą ulokowane węzły szkieletowe jest przedstawiona w tabeli: Tabela 2. Lokalizacje węzłów szkieletowych szerokopasmowej sieci teleinformatycznej na stronie 9.

1.1.4 Węzły szkieletowe

Węzły szkieletowe będą połączone z Głównym węzłem szkieletowym łączem MetroEthernet 1 Gb/s. Punkty dostępowe i przełączniki tranzytowe będą podłączone do węzłów szkieletowych łączami MetroEthernet 1Gb/s. Węzły szkieletowe będą wyposażone w:

- Przełącznik szkieletowy
- System podtrzymania zasilania – UPS (min 3 godziny)

Lista obiektów, w których będą ulokowane węzły szkieletowe jest przedstawiona w tabeli: Tabela 2. Lokalizacje węzłów szkieletowych szerokopasmowej sieci teleinformatycznej na stronie 9.

1.1.5 Punkty dostępowe

Punkty dostępowe będą zlokalizowane w obiektach, do których będą dostarczane usługi dla użytkowników sieci. Punkty dostępowe zapewnią możliwość bezpiecznego dostępu oraz kontrolę dostępu do sieci.

Punkty dostępowe będą podłączane do sieci szkieletowej lub do przełączników tranzytowych łączem światłowodowym MetroEthernet 1Gb/s lub radiowym o przepływności zagregowanej łącza minimum 25 Mb/s i przepływności dostępnej do punktu dostępowego w przypadku agregacji połączeń w ramach kaskady linków radiowych minimum 5 Mb/s.

Punkt dostępowy będzie składał się z Bramy Usługowej punktu dostępowego wyposażonej w urządzenia zapewniające podłączenie do sieci poprzez WiFi. Planuje się stosowanie pojedynczego punktu dostępowego WiFi w wykonaniu wewnątrz budynkowym w ramach lokalizacji (planuje się wykonanie 95 punktów dostępowych).

Projekt umożliwia podłączenie istniejących sieci lokalnych w poszczególnych lokalizacjach do systemu dostępowego z wykorzystaniem łączy ethernet o przepływności 100Mb/s. Projekt nie obejmuje budowy sieci lokalnych LAN (switchy lokalnych, okablowania) ani dostawy terminali końcowych (komputerów stacjonarnych, laptopów, MDA, drukarek, serwerów, itp.).

1.1.6 Przełączniki tranzytowe

Opcjonalne przełączniki tranzytowe będą stosowane, wtedy gdy topologia sieci światłowodowej w obszarze podłączenia do węzłów szkieletowych będzie inna niż gwiazda (kaskada lub pierścień). Przełączniki tranzytowe będą podłączone do przełączników szkieletowych (lub innych przełączników tranzytowych) łączem MetroEthernet 1Gb/s. Nie przewiduje się systemu podtrzymania zasilania w lokalizacjach przełączników tranzytowych.

1.1.7 Centrum Zarządzania i Bezpieczeństwa Sieci

Centrum Zarządzania i Bezpieczeństwa Sieci będzie realizowało funkcje kontroli i monitoringu wszystkich elementów sieci oraz z świadczonych przez tą sieć usług. Użytkownicy korzystający z usług sieci będą podlegali procesowi autentykacji, autoryzacji i weryfikacji.

Centrum zarządzania będzie wyposażone w następujące urządzenia:

- System Monitoringu i Zarządzania Siecią
- Centralny System Zarządzania Bezpieczeństwem sieci
- System Kontroli Dostępu do Sieci
- System Autoryzacji, Autentykacji i Weryfikacji
- System podtrzymania zasilania UPS – 3 godziny
- 1 stację roboczą i 5 laptopów

1.2 Aktualne uwarunkowania wykonania przedmiotu zamówienia

1.2.1 Ogólne uwarunkowania dotyczące całości sieci szerokopasmowej

Topologia sieci światłowodowych i radiowych implikuje w głównej mierze strukturę fizyczną projektowanej sieci, lecz również ma istotny wpływ na jej architekturę logiczną. Brak znajomości rzeczywistych przebiegów sieci uniemożliwia dokładne określenie zakresu sieci światłowodowej i radiowej w projekcie, dlatego na tym etapie konieczne było przyjęcie pewnych założeń (określonych wcześniej).

Na etapie projektowania sieci światłowodowej i radiowej, po określeniu rzeczywistej długości sieci będzie konieczna rewizja przyjętych założeń projektowych i ponowne zaprojektowanie sieci z uwzględnieniem aktualnych uwarunkowań technicznych i budżetowych.

Budowa i eksploatacja sieci telekomunikacyjnych przez jednostki samorządu terytorialnego lub ich związki podlegają przepisom prawnym regulującym działalność samorządów w tym zakresie. Dlatego też stworzenie infrastruktury telekomunikacyjnej i sposób eksploatacji utworzonej sieci szerokopasmowej muszą być zgodne z obowiązującymi: ustawą o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz.U. 2010 nr 106 poz. 675) i ustawą Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800), wraz z rozporządzeniami wydanymi na podstawie ww. ustaw.

1.2.2 Kablowa sieć światłowodowa

Przed przystąpieniem do prac budowlanych należy sporządzić projekt budowlano-wykonawczy oraz uzyskać niezbędne pozwolenia i uzgodnienia.

Do budowy sieci szkieletowej i dostępowej należy zastosować kable światłowodowe. Powodami, dla których w tego typu rozwiązaniach stosuje się kable światłowodowe są m.in.:

- mała tłumienność przesyłanych sygnałów co daje możliwość budowy długich odcinków bez konieczności regeneracji przesyłanego sygnału;
- odporność na zakłócenia;
- bardzo duża trwałość;

- możliwość uzyskiwania bardzo dużych prędkości transmisji;
- praktycznie nieograniczona przepustowość uzależniona wyłącznie od zewnętrznych ograniczeń technologicznych;
- niski stopień awaryjności;
- wysoka niezawodność i jakość transmisji;
- mała waga;
- małe wymiary.

Jedyne praktycznie wady sieci światłowodowej wynikają nie z zastosowania kabli światłowodowych lecz z technologii procesu budowlanego i są to;

- stosunkowo wysoki koszt budowy;
- długi okres budowy.

Reasumując zalety kabli światłowodowych i możliwości, jakie oferują sieci wykonane z ich zastosowaniem zdecydowanie przemawiają za wyborem tego rozwiązania.

Budowę sieci światłowodowej można realizować na kilka sposobów:

1. Układanie kabli bezpośrednio w ziemi

- wymaga stosowania droższych kabli przystosowanych do tego rodzaju technologii;
- daje małą elastyczność wybudowanej w ten sposób sieci – każdorazowe „wejście w kabel” wymaga prowadzenia robót ziemnych.

2. Układanie kabli w rurze osłonowej

- umożliwia stosunkowo łatwy dostęp do kabla w przypadku konieczności jego wymiany spowodowanej uszkodzeniem;
- zdecydowanie większe bezpieczeństwo kabla w związku z zastosowaniem rury osłonowej;
- daje małą elastyczność wybudowanej w ten sposób sieci – każdorazowe „wejście w kabel” wymaga prowadzenia robót ziemnych

- zastosowanie głównie na obszarach pozamiejskich.

3. Budowa kabli w kanalizacji teletechnicznej w dodatkowej rurze osłonowej lub w mikrokanalizacji

- bardzo duże bezpieczeństwo dla wybudowanej w tej technologii sieci
- najczęściej stosowane przez operatorów sieci telekomunikacyjnych na terenach miejskich i zurbanizowanych
- duża elastyczność budowanej sieci w kontekście jej rozbudowy, usuwania awarii
- umożliwia lokalizację złączy w studniach kablowych bez konieczności stosowania specjalnych zasobników.

1.2.3 Łącza radioliniowe

Wykonanie dokumentacji projektowej wraz z uzgodnieniami wymaganymi przepisami prawa budowlanego oraz budowa na podstawie tej dokumentacji, zatwierdzonej przez Zamawiającego.

Kompletna dokumentacja projektowa winna zawierać:

- Projekt i dokumentacja sieci,
- Projekt radiowo-technologiczny,
- Projekt drogi kablowej,
- Projekt konstrukcyjno-budowlany – zależnie od specyfikacji danej lokalizacji,
- Projekt propagacji sygnału radiowego (planowanie radiowe),
- Specjalistyczne obliczenia obciążeń masztu - zależnie od specyfikacji danej lokalizacji

1.2.4 Aktywne urządzenia sieciowe

Przed przystąpieniem do prac budowlanych należy sporządzić projekt budowlano-wykonawczy oraz uzyskać niezbędne pozwolenia i uzgodnienia.

Podstawowe założenia dla projektu aktywnych urządzeń sieciowych muszą uwzględnić projekty sieci światłowodowej i radiowej. Specyfikacja zastosowanych elementów sieciowych, ilość i rodzaj interfejsów sieciowych musi odpowiadać

rzeczywiście zaprojektowanym rodzajom łączy, interfejsów fizycznych. Należy zwrócić szczególną uwagą na dobór rodzaju i ilości wkładek SFP co bezpośrednio przełoży się na budżet projektu.

Minimalne wymagane przepływności w relacjach światłowodowych to 1Gb/s. Minimalne wymagane przepływności zagregowane dla łącza radiowego to 25 Mb/s w normalnych warunkach pracy.

Wymagane jest optymalne dobranie wielkości szaf na urządzenia sieciowe (42U lub 9U) i dobranie zasilania awaryjnego zapewniającego podtrzymanie zasilania w lokalizacjach węzłowych przez minimum 3 godziny.

Urządzenia sieciowe muszą być łatwe w utrzymaniu, zarządzaniu. Powinna być możliwość ich rozbudowy a szczególnie zwiększenia przepływności projektowanego systemu w przyszłości do minimum 10Gb/s.

Zaleca się w miarę możliwości stosowanie urządzeń sieciowych, aplikacji, systemów zarządzania jednego producenta.

1.3 Ogólne właściwości funkcjonalno-użytkowe

Przedstawiony w niniejszym opracowaniu system będzie składał się kilku podstawowych komponentów:

- Systemu kabli światłowodowych oraz radiolinii zwanych warstwą fizyczną sieci lub w dalszej części siecią dystrybucyjną. Sieć dystrybucyjna będzie zakończona
    - na przełącznicy światłowodowej zlokalizowanej wewnątrz budynku w dedykowanym do tego celu pomieszczeniu lub
    - na przełącznicy światłowodowej zlokalizowanej w specjalnej szafie zainstalowanej na zewnątrz budynku najlepiej w pasie drogowym w bezpośrednim sąsiedztwie studni kablowej.

Decyzja o zakończeniu sieci światłowodowej wewnątrz budynku lub w szafce na zewnątrz budynku zapadnie na etapie opracowywania projektu budowlanego sieci światłowodowej.

- Urządzeń transmisyjnych sieci WAN składających się z:
    - Sieci szkieletowej, która obejmuje przełączniki szkieletowe i routery do sieci zewnętrznych zlokalizowane w węźle głównym
    - Urządzeń dostępowych – zlokalizowanych w obiektach wg tabeli Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej
    - Systemu zarządzania siecią WAN - zlokalizowanego w węźle głównym

Planowana sieć szerokopasmowa dla projektu „Regionalna Platforma Cyfrowa Dorzecza Wieprzy i Grabowej II – Infrastruktura Szerokopasmowej Sieci Teleinformatycznej” powinna umożliwiać użytkownikom korzystanie z takich usług jak dostęp do globalnego Internetu i innych usług oferowanych przez systemy istniejące w powiecie Sławno. Sieć będzie posiadała własny nowoczesny system zapewnienia bezpieczeństwa, możliwość autoryzacji, autentykacji i weryfikacji użytkowników oraz kontroli dostępu do sieci. Administratorzy będą mogli z jednej konsoli zarządzać wszystkimi elementami sieci.

1.3.1 Warstwa fizyczna sieci – sieć światłowodowa

Zadaniem warstwy fizycznej sieci jest połączenie kablami światłowodowymi lub radioliniami wszystkich obiektów sieci (patrz: Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej).

Kable światłowodowe są w obecnej chwili najlepszym medium transmisyjnym wykorzystywany przy budowie tego typu systemów, jednak ze względu na koszty realizacji zostało w niniejszym opracowaniu połączone z systemem radiolinii służącymi do podłączenia obiektów bardziej oddalonych lub o niskich wymogach transmisyjnych.

Do budowy sieci światłowodowych należy zastosować:

- tradycyjne kable światłowodowe szczególnie na obszarach o mniejszej intensywności zabudowy oraz na długich odcinkach, na których nie przewiduje się większej ilości potencjalnych użytkowników sieci (mniejsza ilość wyprowadzeń – odpięć z głównego kabla)
- mikrokanalizację i mikrokable światłowodowe na obszarach o intensywnej i bardzo intensywnej zabudowie z dużą ilością potencjalnych użytkowników i o dużym potencjale rozwojowym sieci (teren miasta Sławna).

Taki mieszany sposób budowy kanalizacji teletechnicznej i sieci kabli światłowodowych pozwala na uzyskanie:

- bardzo dużej elastyczności sieci;
- możliwości łatwej rozbudowy sieci;
- możliwości łatwego dostosowywanie konfiguracji sieci w zależności od pojawiających się nowych użytkowników lub spełniania potrzeb istniejących i nowych użytkowników sieci;
- optymalizację kosztów budowy sieci poprzez stworzenie warunków do łatwego i szybkiego, a przez to stosunkowo taniego reagowania na potrzeby użytkowników;
- możliwości wykorzystania istniejących, nie wykorzystanych lub wykorzystywanych w niewielkim zakresie, rurociągów kablowych;

- budowę jednej sieci światłowodowej, którą będzie można wykorzystywać dla realizacji usług dla jej użytkowników, jak i dla potrzeb planowanego intensywnie rozbudowywanego monitoringu wizyjnego (kamery).

Najkorzystniejszą technologią budowy sieci światłowodowej na terenie powiatu Sławno jest budowa sieci w rurociągu teletechnicznym wybudowanym z rur o średnicy ϕ40 – budowanych jako wiązki 3 rur – wraz z zastosowaniem zasobników (na terenach niezabudowanych) i studni kablowych tradycyjnych (betonowych) lub z tworzywa HDPE (na terenach zabudowanych i w pasach drogowych poza terenami zabudowanymi).

Podczas budowy rurociągów kablowych wszystkie przejścia przez ulice należy bezwzględnie zabezpieczać rurą osłonową grubościenną np. HDPE ϕ140. Podobnie należy zabezpieczać skrzyżowania projektowanego rurociągu z obcym uzbrojeniem podziemnym (np. z wodociągami i gazociągami). Przejścia przez drogi krajowe i wojewódzkie oraz przez cieki podstawowe i szczegółowe należy wykonywać metodami bezwykopowymi (przecisk prosty, przewiert sterowany), przy wykorzystaniu rury osłonowej grubościennej typu HDPE (np. HDPE ϕ140).

1.3.2 Warstwa fizyczna sieci – Łącza radioliniowe

Bezprzewodowa sieć łączy radioliniowych ma zapewnić dostęp do usług intranetowych i internetowych dla jednostek podległych jednostkom samorządowym wymienionym w tabeli Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej.

Celem nadrzędnym planowanej sieci jest stworzenie warunków do rozwoju społeczeństwa informacyjnego na terenie poszczególnych gmin powiatu Sławno. Łączność radiowa powinna zostać zrealizowana w nielicencjonowanym paśmie częstotliwości 5,4 GHz. Zakłada się, że sumaryczna (uplink + downlink) przepływność do pojedynczego obiektu podłączonego drogą radiową będzie nie mniejsza niż 5Mbit/s.

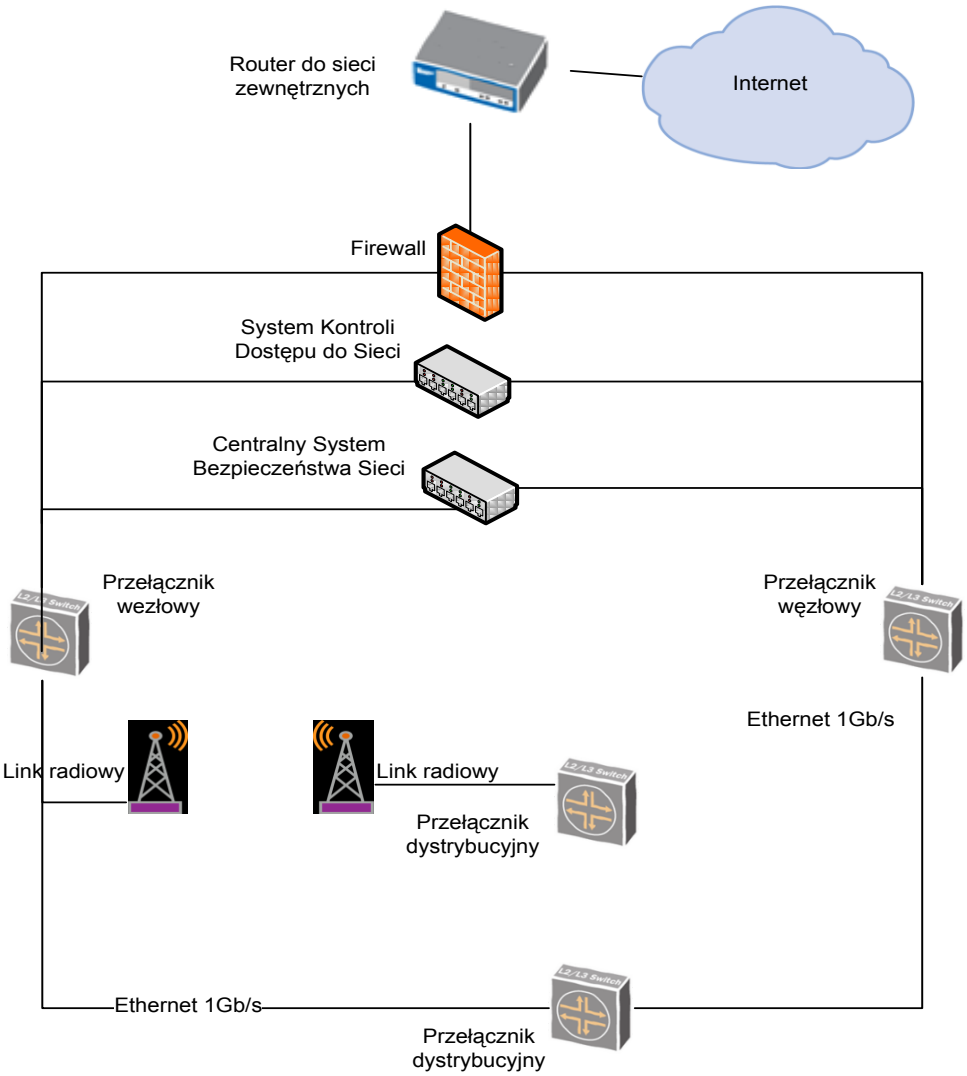
Sieć radioliniowa powinna być tak zaprojektowana, aby w przyszłości, jeśli zajdzie taka potrzeba, zwiększenie przepływności mogło być realizowane na zasadzie aktywacji odpowiednich kluczy programowych.

1.3.3 Architektura sieci

1.3.3.1 Architektura logiczna

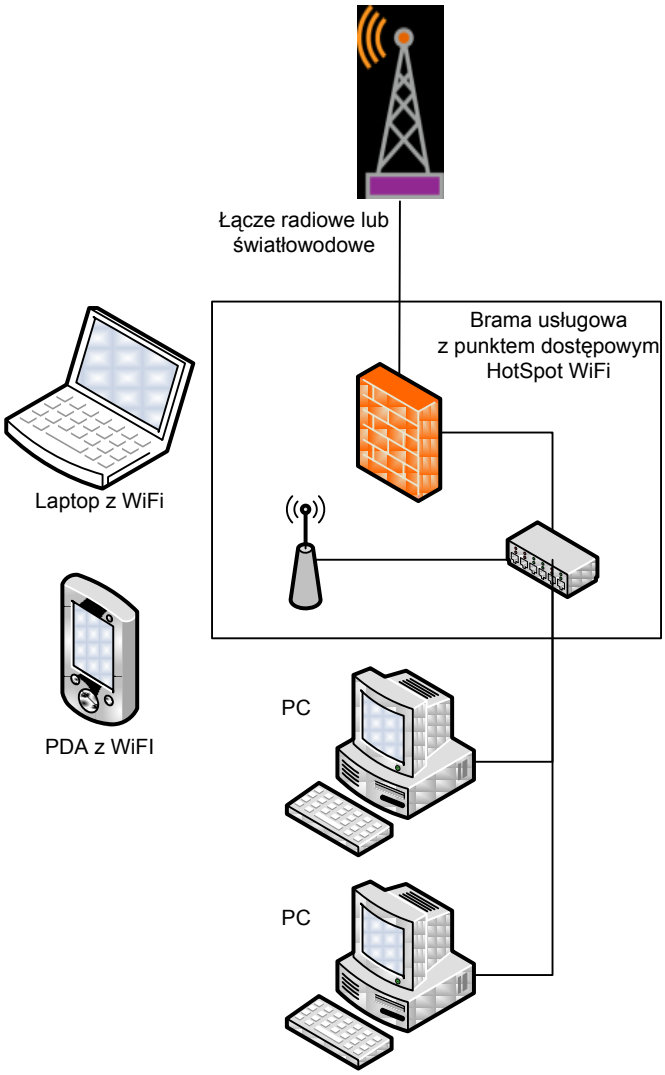
Topologia szkieletu sieci jest przedstawiona na rysunku poniżej:

Topologia szkieletu sieci



Rysunek nr 1: Topologia szkieletu sieci

Topologia Stacji Klienckiej



Rysunek nr 2: Architektura Punktu Dostępowego

1.3.3.2 Przełącznik szkieletowy

W systemie będą występowały dwa rodzaje przełączników, główne przełączniki szkieletowe i przełączniki szkieletowe.

Główne przełączniki szkieletowe będą umożliwiały podłączenie do sieci usług dostępnych dla wszystkich użytkowników sieci, infrastruktury współdzielonej przez użytkowników sieci oraz systemów zarządzania umożliwiających pełną kontrolę elementów sieci i realizację założonej polityki bezpieczeństwa. Do Głównego przełącznika Szkieletowego Będzie podłączony:

- Centralny Firewall
- Centrum Zarządzania Bezpieczeństwem Sieci (w jednej lokalizacji)

Przełączniki szkieletowe będą połączone łączami światłowodowymi pracującymi w standardzie MetroEthernet z prędkością 1 Gb/s.

Do Przełączników Szkieletowych będą podłączone Przełączniki Tranzytowe (gdzie potrzeba) oraz Bramy Usługowe (łącze MetroEthernet 1Gb/s w przypadku światłowodu i minimum 25 Mb/s w przypadku łączy radiowych).

1.3.3.3 Przełącznik tranzytowy

Przełączniki tranzytowe będą niezbędne w przypadkach, gdy architektura sieci światłowodowej lub radiowej w obszarze połączenia do węzła szkieletowego będzie inna niż gwiazda (kaskada lub pierścień). Przełączniki tranzytowe będą podłączone do przełączników szkieletowych (lub innych przełączników tranzytowych) łączem światłowodowym MetroEthernet 1Gb/s. Nie przewiduje się podtrzymania zasilania dla przełączników tranzytowych. Do każdego przełącznika tranzytowego będzie za pośrednictwem światłowodowego łącza MetroEthernet 1Gb/s lub radiowego łącza 25 Mb/s, dołączona Brama Usługowa Punktu Dostępowego.

1.3.3.4 Centralny Firewall

Firewall jest to system sprzętowej i programowej ochrony przed niepowołanym dostępem do sieci. System firewall powinien oferować zintegrowane zaawansowane mechanizmy switchingu, routingu i bezpieczeństwa. System powinny charakteryzować następujące cechy:

- interfejsy Gigabit Ethernet, możliwość rozbudowy o porty optyczne i typowe porty WAN,
- mechanizm Intrusion Prevention
- antywirus,
- antyspam,
- filtrowanie stron WWW,
- content filtering (rozszerzenia plików, MIME),
- sprzętowa akceleracja IPS i AV,
- możliwość rozbudowy o wieloportowe moduły z PoE
- pełny zakres protokołów routingu dynamicznego (RIP, OSPF, IS-IS, BGP, protokoły multicast), MPLS,
- klient VPN w sposób automatyczny instalowany na stacjach użytkowników.

Urządzenie to będzie podłączone do Głównych Przełączników Szkieletowych. Sposób podłączenia, prędkość portów Ethernet, rodzaj adapterów, powinien być określony na etapie projektu wykonawczego.

1.3.3.5 Centralny System Zarządzania Bezpieczeństwem Sieci

Centralny System Bezpieczeństwa sieci powinien umożliwiać zarządzanie bezpieczeństwem sieci. System powinien realizować funkcje: Security Information and Events Management (SIEM) i Network Behavior Anomalny Detection (NBAD) oraz utrzymywać centralne repozytorium logów. Centralny System Zarządzania Bezpieczeństwem Sieci musi umożliwiać zarządzanie bezpieczeństwem na wszystkich elementach sieci.

1.3.3.6 Aplikacja zarządzania i monitorowania sieci

Aplikacja zarządzania i monitorowania sieci powinna umożliwiać scentralizowane zarządzanie eksploatacją następujących urządzeń:

- Główny Przełącznik Szkieletowy
- Przełączniki Szkieletowe
- Przełączniki Tranzytowe
- Firewall

- Centralny System Bezpieczeństwa sieci
- Bramy Usługowe Punktu Dostępowego
- Punkt dostępowy HotSpot WiFi

Aplikacja powinna dawać możliwość dokładnego konfigurowania polityk bezpieczeństwa oraz kompleksowe narzędzia monitoringu, sygnalizacji i analiz ich przestrzegania na wszystkich elementach sieci.

1.3.4 Aplikacja Serwera Weryfikacji i Autentykacji

Zadaniem tej aplikacji jest wysłanie zapytania do użytkownika próbującego zalogować się do sieci. Użytkownik jest proszony o wpisanie identyfikatora i hasła. Aplikacja będzie stanowiła sobą bazę istniejących użytkowników wraz z hasłami i odpowiednią polityką zarządzania hasłami. Aplikacja będzie współpracować z Systemem Kontroli Dostępu do Sieci.

1.3.5 System Kontroli Dostępu do Sieci

System powinien zarządzać procesem dostępu do zasobów sieciowych przez cały okres jego trwania poczynając od procesu logowania. Urządzenie działa we współpracy z Aplikacją Serwera Autentykacji i Weryfikacji, przełącznikami szkieletowymi i dystrybucyjnymi oraz Bramami Usługowymi.

1.3.6 Brama Usługowa Punktu Dostępowego

Brama Usługowa powinna oferować zintegrowane zaawansowane mechanizmy switchingu, routingu i bezpieczeństwa, które pozwolą użytkownikom podłączyć się za jej pośrednictwem do sieci.

Urządzenie to będzie zainstalowane w węźle klienckim sieci i podłączone do szkieletu sieci.

Funkcjonalność bramy usługowej musi umożliwiać zorganizowanie kilku niezależnych sieci lokalnych LAN z dowolną adresacją IP jednocześnie zapewniając separacją poszczególnych sieci (np. Intranet UM, LAN szkolny, sieć publiczna). Dodatkowo powinna być możliwość autentykacji wszystkich użytkowników sieci oraz kontrola dostępu. Urządzenie musi posiadać funkcjonalność firewall i zgodnie z ustaloną

polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa).

Zaawansowana funkcjonalność Bramy Usługowej wynika z potrzeby zrealizowania sieci lokalnych w lokalizacjach klienckich, zapewnienia bezpieczeństwa tym sieciom oraz uniemożliwienia zakłócenia pracy sieci dostępowej i szkieletowej przez nieuprawnione działania użytkowników.

Brama Usługowa będzie zarządzana za pośrednictwem Aplikacji Zarządzania i Monitorowania Sieci. Do urządzenia może być podłączone jedno lub więcej urządzeń Access Point WiFi Urządzenie to utworzy HotSpot, do którego przez radio będą mogły logować się urządzenia pracujące w obiekcie.

1.3.6.1 Punkt dostępowy HotSpot WiFi

Urządzenie będzie umożliwiać podłączenie do sieci za pośrednictwem urządzeń WiFi pracujących w standardzie 802.11a/b/g/n. Urządzenie powinno być wyposażone w podwójny dwupasmowy odbiornik i być w pełni zarządzane z systemów zarządzania elementami sieci i jej bezpieczeństwem poprzez Bramę Usługową stacji klienckiej.

1.4 Szczegółowe właściwości funkcjonalno-użytkowe

Szczegóły programu funkcjonalno-użytkowego będą omówione z wykonawcą wyłonionym w wyniku postępowania przetargowego. Dla skrócenia procesu realizacji zadania zakłada się zasadę „zaprojektuj i wybuduj”.

System sieci szerokopasmowej opisanej w niniejszym dokumencie będzie spełniał następujące założenia techniczno eksploatacyjne:

1. Planowana jest realizacja szkieletu optycznego o przepływności minimum 1 Gb/s, łącząca 5 węzłów szkieletowych (zgodnie z tabelą Tabela 2. Lokalizacje węzłów szkieletowych szerokopasmowej sieci teleinformatycznej).
2. Wszystkie pozostałe lokalizacje (zgodnie z tabelą Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej), podłączone będą łączami optycznymi 1Gb/s lub radiowymi o przepływności zagregowanej przęsła radiowego minimum 25 Mb/s.
3. Wszelkie relacje światłowodowe, zgodnie z wymaganiami projektu będą realizowane jako para światłowodowych włókien jednomodowych, które będą wybudowane od końca do końca, z zakończeniem na przełącznicach optycznych we wskazanych w tabeli lokalizacjach.
4. Wszystkie relacje radiowe będą wybudowane zgodnie z wymaganiami projektu i będą to łącza typu punkt-punkt zrealizowane przy wykorzystaniu nielicencjonowanych, otwartych częstotliwości radiowych. Minimalna zagregowana przepływność pojedynczego łącza nie powinna być mniejsza niż 25 Mb/s w normalnych warunkach pracy. Minimalna przepływność do Bramy Dostępowej, wynikająca z połączenia kaskadowego linków radiowych nie powinna być mniejsza niż 5 Mb/s.
5. Łącze dostępu do Internetu wraz z firewall będzie zrealizowane w lokalizacjach Urząd Miasta Sławno.
6. Planowana Główna Lokalizacja węzłowa (z zaawansowanym routingiem, BGP) z możliwym połączeniem do Data Center i Internetu w Urzędzie Miasta Sławno.
7. Zastosowanie węzłów tranzytowych zależy od topologii sieci dostępowej i jest niezbędne w przypadku gdy na danym terenie zostanie wybudowana

infrastruktura optyczna i/lub radiowa w topologii pierścienia lub kaskady. Dla topologii gwiazdy przełączniki tranzytowe nie będą koniecznie.

8. We wszystkich lokalizacjach należy zapewnić możliwość organizacji wielu sieci lokalnych oraz dostęp WiFi (wymagany routing, NAT, serwer DHCP, firewall) wraz z kontrolą dostępu, autentykacją, zarządzaniem pasmem.
9. Centrum zarządzania NOC zlokalizowany będzie w UM Sławno. Wymagane funkcje: zarządzanie i monitorowanie całości systemu, w tym kontrola dostępu, pasma, zarządzanie użytkownikami. Zastosowane rozwiązania NAC, UTM, System zarządzania sieci, Radius. Aplikacje systemów bezpieczeństwa powinny być zainstalowane na serwerach zalecanych przez producenta aplikacji.
10. System podtrzymania zasilana na 3 godz. powinien być zrealizowany w lokalizacjach węzłowych. Nie przewiduje się podtrzymania zasilania w lokalizacjach tranzytowych.
11. Cały system powinien wspierać VLAN, QoS.

2. OPIS WYMAGAŃ ZAMAWIAJĄCEGO W STOSUNKU DO PRZEDMIOTU ZAMÓWIENIA

2.1 Cechy obiektu dotyczące rozwiązań budowlano-konstrukcyjnych i wskaźników ekonomicznych – Wymagania dotyczące sieci światłowodowych

Realizacja niniejszego przedsięwzięcia obejmuje prace projektowe i budowlane niezbędne do wybudowania rurociągów kablowych z rur typu HDPE Ø40 oraz rur osłonowych typu HDPE Ø110 lub HDPE Ø140, a następnie ułożenie w nich kabli światłowodowych oraz uruchomienie radiolinii. Projektowany przebieg trasowy rurociągów oznaczono na mapach linią niebieską (sieć szkieletowa) i różową (sieć dostępowa) – patrz załącznik nr 1 do PFU.

Biorąc pod uwagę wymiary prefabrykowanych studni i silne uzbrojenie innymi urządzeniami podziemnymi na terenie miasta, zaprojektować studnie typu SKR-1 lub studnie z tworzywa HDPE. W uzasadnionych przypadkach, lecz dopiero po odkryciu urządzeń obcych w rejonie projektowanych studni, dopuszcza się możliwość wymurowania z bloczków betonowych studni nietypowych, dopasowanych do lokalnie zastanych warunków - w takim przypadku należy każdorazowo powiadamiać Zamawiającego. Na terenach niezabudowanych, poza pasem drogowym, projektować zasobniki kablowe betonowe.

2.1.1 Studnie SKR-1 lub z tworzywa HDPE obok obiektów kubaturowych

W ramach zamówienia podstawowego należy zaprojektować i wybudować odpowiednią ilość studni, w miejscach właściwych, szczególnie na odgałęzieniach kabli światłowodowych, przy ścianach obiektów kubaturowych lub zewnętrznych szaf dostępowych oraz na wszystkich załamaniach kanalizacji pod kątem prostym.

Studnie należy wykonać zgodnie z warunkami wykonania i odbioru robót budowlanych dla przyłączy do Punktów Dostępowych i Dystrybucyjnych. Odstępstwem

od tej reguły jest węzeł główny, gdzie jako studnie przyobiektowe / stacyjne można zastosować większą studnię, magistralne typu SKMXX-3.

2.1.2 Budowa i oznakowanie rurociągu

Rurociąg wykonać z rur wewnętrznie-rowkowanych HDPE ϕ40 układając je na całym przebiegu wszystkich nowoprojektowanych kabli.

Na prostych odcinkach należy dążyć do możliwie długich odcinków rury bez jej przecinania. Ze względu na standardowe długości fabrykacyjne rur HDPE40 równe 150m lub 250m oraz na to, że większość trasy przebiega po terenach niezabudowanych, należy zamówić odcinki o długościach minimum 500m.

Dla zapewnienia długotrwałej sprawności i funkcjonalności rurociąg kablowy powinien być szczelny w każdym punkcie, niedostępny dla zanieczyszczeń stałych i płynnych zarówno w czasie budowy, jak i eksploatacji. Wybudowane sekcje (pomiędzy projektowanymi lokalizacjami zapasów kabla światłowodowego) rurociągu kablowego po wybudowaniu należy poddać próbom kalibracyjno-ciśnieniowym.

We wszystkich studniach kablowych oraz zasobnikach rury należy oznakować przywieszką identyfikacyjną danej linii, oraz napisem „UWAGA! KABEL ŚWIATŁOWODOWY” i symbolem lasera – zgodnie z obowiązującymi zasadami oznakowania kabli optotelekomunikacyjnych.

2.1.3 Kable optotelekomunikacyjne

Zgodnie z założeniami technicznymi, zalecana linia optotelekomunikacyjna winna być: dielektryczna, zdolna do efektywnego i szybkiego zwiększenia przepustowości, podziemnie-kanałowa z odgałęzieniami do obiektów kubaturowych, w których zlokalizowane będą Punkty Dostępowe Szerokopasmowej Sieci Światłowodowej.

Mając na uwadze bardzo szybki rozwój nowych technologii oraz zwiększające się zapotrzebowanie na pasmo, projektowana linia będzie już teraz przygotowana na zwiększenie swojej przepustowości, przez zastosowanie odpowiedniej ilości tub zależnie od pojemności kabla.

Do budowy sieci światłowodowej należy zastosować kable zewnętrzne, przeznaczone do układania w rurociągach i kanalizacji teletechnicznej. O ile to będzie możliwe przyłącza kablowe do budynków Punktów Dostępowych należy wykonać kablami np. typu ZW-NOTKtsd. Są to kable uniwersalne (ZW-), z powłoką z tworzywa bezhalogenowego (N), optotelekomunikacyjne (OTK), tubowe (luźna tuba) z suchym uszczelnieniem ośrodka (ts), całkowicie dielektryczne (d).

Kable liniowe należy zaciągnąć do rurociągu metodą pneumatyczną strumieniową (najmniej obciążającą dla kabla spośród rozpowszechnionych obecnie metod montażu kabli optycznych) lub mechaniczną z zachowaniem dopuszczalnej (określonej w normach) siły ciągu. Szczegółowe zalecenia dotyczące zaciągania kabli zawarte są np. w normach zakładowych ZN-96/TP S.A.-002 oraz ZN-96/TP S.A.-013.

Projektowane zapasy złączowe winny mieć długości wynikające z obowiązujących norm dotyczących montażu kabli światłowodowych.

Zapasy złączowe kabli liniowych instalowane w studniach teletechnicznych lub zasobnikach należy nawinąć na prefabrykowane-gotowe stelaże zapasów kabla. Zastosowane stelaże (zwijaki) powinny posiadać regulowane wymiary z możliwością dostosowania do wielkości studni kablowej i długości zapasów kabli optycznych.

Wszystkie zapasy kablowe należy przymocować do stelaży opaskami zaciskowymi z tworzyw sztucznych i oznaczyć przywieszką identyfikacyjną linii z każdej strony zwijaka.

2.1.4 Prowadzenie i oznakowanie kabli w obiektach

Ze studni przyobiektowej kable należy wprowadzić do wnętrza budynku w uniepalnionej rurze HDPEt Ø40 mm, którą należy zakończyć tuż po przekroczeniu ściany, ale po uprzednim unieruchomieniu jej na drabince kablowej lub wsporniku kablowym. Tak zamocowaną rurkę należy obustronnie uszczelnić (zarówno w studni jak i w budynku) za pomocą uszczelek rozporowych do rur z kablami światłowodowymi (np. produkcji Jackmoon - typ FIBER OPTIC SIMPLEX). Wszystkie te zabiegi związane są z zabezpieczeniem przed przenoszeniem ognia, gazów i płynów do wnętrza budynku.

Od miejsca, w którym rurę HDPEt Ø40 z kablem uszczelniono uszczelką (np. Jackmoon), kabel należy ułożyć w bezhalogenowym wężu ochronnym (rurze peszla), do zapasu stacyjnego i dalej do rozdzielacza kabla przy przełącznicy ODF.

Całość przebiegu trasowego kabla, należy czytelnie oznakować przywieszkami identyfikacyjnymi linii.

2.1.5 Montaż złączy światłowodowych

Montaż złączy będzie odbywał się w samochodzie pomiarowo-montażowym. Złącza kabli międzywęzłowych należy zorganizować wewnątrz projektowanych muf światłowodowych, umożliwiających jednotorową organizacje włókien (po 2wł.) na kasetach spawów i pojemności, co najmniej 192 takich torów. Ponadto uszczelnienie główne głowicy z pokrywą powinno być mechaniczne czyli rozbieralne (wielokrotnego użytku).

W przypadku złączy optycznych na kablach dostępowych, instalowanych w studniach teletechnicznych należy zastosować liniowe osłony złączowe, przelotowo-rozgałęźne o mniejszej maksymalnej pojemności spawów. Zewnętrzna osłona takich muf powinna być wykonana jest z polietylenu wysokiej gęstości HDPE, zaś głowica mufy musi posiadać, co najmniej trzy wejścia okrągłe dla kabli o średnicy od 8 do 16 mm oraz gardziel owalną dla dwóch kabli o średnicy od 8 do 20mm i wyposażona w termokurczliwe uszczelnienia wejść kablowych. Instalowane wewnątrz kasety powinny umożliwić zmagazynowanie do 144 spawanych włókien czy innych elementów biernych (rozgałęźniki i multipleksery optyczne).

Przy montażu kablowych złączy odgałęźnych w celu minimalizacji liczby spawów przypadających na włókno/tor transmisyjny, należy dążyć do tego by przecinana była tylko tuba/tuby kabla głównego, zawierająca odgałęziane włókna optyczne.

Ze względu na możliwą rozbudowę Powiatowej Sieci Szerokopasmowej w instalowanych złączach kablowych należy zespolić tylko te włókna światłowodowe, które będą wykorzystywane do transmisji.

Poprawność instalacji pozostałych (ciemnych) włókien zostanie wykazana na podstawie analizy jednostronnych pomiarów reflektometrycznych danego odcinka, tylko w trzecim lub w czwartym oknie transmisyjnym.

Wszystkie kable wchodzące do osłony złączowej, muszą być oznaczone przywieszką identyfikacyjną danej linii.

2.1.6 Montaż stacyjny

Zakończenia kablowe, zależnie od rodzaju obiektu (patrz Tabela 1. Lista obiektów szerokopasmowej sieci teleinformatycznej), należy projektować w szafkach kablowych lub w pomieszczeniach technicznych w szafach teleinformatycznych 19 calowych o wysokości 45U lub 42U i wymiarach 800 x 800 mm. Kabel optotelekomunikacyjny wprowadzany do szafy w bezhalogenowym wężu ochronnym (w peszlu), ma być rozszyty w rozdzielaczu kabla liniowego. Rozdzielacz taki powinien charakteryzować się następującymi cechami:

- zabezpieczeniem przed przesuwaniem kabla wzdłuż osi (mocowanie elementu centralnego kabla),
- zabezpieczeniem przed ruchem skrętnym kabla (kabel powinien być przymocowany do obudowy rozdzielacza za pomocą metalowej opaski),
- tuby rozszytego kabla powinny być prowadzone do przełącznicy ODF w specjalnej rurze (tzw. tubie transportowej),
- tuby transportowe wychodzące z rozdzielacza (osłaniające tuby z kabla) powinny być mocowane do paneli przełącznic w uchwytach z zatrzaskiem (szybkozłączach) i oznaczone przywieszkami identyfikacyjnymi danej linii optotelekomunikacyjnej

Projektowane 19-calowe przełącznice światłowodowe w wykonaniu perforowanym powinny posiadać wymienione poniżej cechy:

- budowę modułową – z możliwością całkowitego wyjmowania modułu z tackami spawów
- wykonanie zapasu tub kabla liniowego pod modułem z kasetami na spawy,
- kasety zapewniające promień gięcia włókien powyżej 40mm,

- kasety na spawy dla 24 spawów każda
- magazynki dla 12 termokurczliwych osłon spawów
- tuby z kabla mocowane w kasetach uchwytem do tub lub opaskami
- wprowadzenie tub kabla do przełącznicy w peszli, mocowanej do przełącznicy w szybkozłączce,
- moduły z tackami prowadzone na plastikowych szynach z zatrzaskami,
- możliwość regulacji mocowania na odpowiedniej głębokości (przełącznice mają być wyposażone w przesuwne prowadnice („uszy”) po bokach przełącznicy, które pozwalają przesuwać i mocować półkę na odpowiedniej głębokości stojaka).

2.1.7 Znakowanie elementów traktów optotelekomunikacyjnych

Przewieszki identyfikacyjne kabli światłowodowych i złączy kabli światłowodowych powinny być wykonane w sposób trwały i estetyczny oraz powinny być odporne na działanie warunków panujących w studniach kablowych. Przewieszki powinny być wydrukowane na papierze koloru żółtego, a następnie hermetycznie zafoliowane. Otwory w przewieszkach służące do ich mocowania na rurze, kablu lub złączu światłowodowym powinny być wykonane poza obszarem papieru w sposób zabezpieczający wydrukowaną przewieszkę przed przenikaniem wody i wilgoci. Przewieszki należy umieszczać:

- w każdej studni kablowej, w komorach kablowych, w korytach kablowych i tunelach kablowych (co 3m),
- na kablach po obu stronach złączy,
- na złączach światłowodowych,
- oraz przy wyprowadzeniu kabla na przełącznicę światłowodową.

2.1.8 Pomiary montażowe i końcowe

1) Po wykonaniu wszystkich połączeń na danym odcinku linii, należy wykonać pomiary reflektometryczne z obydwu stron zmontowanego odcinka, dla dwóch długości fal (1310nm i 1550nm). Dopiero po stwierdzeniu poprawności montażu można ostatecznie zamknąć mufę złączową.

Na tym etapie należy również wykonać jednostronne pomiary dla fali 1550mn wszystkich włókien ciemnych.

2) Po całkowitym zmontowaniu odcinka i docelowym zamocowaniu muf (w studniach itp.), należy wykonać końcowe obustronne pomiary reflektometryczne, dla dwóch długości fal (1310nm i 1550nm) dla włókien zakończonych obustronnie złączkami mechanicznymi (dla włókien jednostronnie zakończonych złączkami wykonać pomiar jednostronny).
3) Pomiary tłumienności wtrąceniowej metodą transmisyjną wykonać dla wszystkich włókien zakończonych obustronnie złączkami mechanicznymi.
4) Pomiary reflektancji złączek mechanicznych, należy wykonać osobno dla każdej z zainstalowanych złączek światłowodowych.
5) Po wykonaniu wszystkich połączeń na danym odcinku linii, należy wykonać pomiary reflektometryczne z obydwu stron zmontowanego odcinka, dla dwóch długości fal (1310nm i 1550nm). Dopiero po stwierdzeniu poprawności montażu można ostatecznie zamknąć mufę złączową.
6) Na tym etapie należy również wykonać jednostronne pomiary dla fali 1550mn wszystkich włókien ciemnych.
7) Po całkowitym zmontowaniu odcinka i docelowym zamocowaniu muf (w studniach itp.), należy wykonać końcowe obustronne pomiary reflektometryczne, dla dwóch długości fal (1310nm i 1550nm) dla włókien zakończonych obustronnie złączkami mechanicznymi (dla włókien jednostronnie zakończonych złączkami wykonać pomiar jednostronny).
8) Pomiary tłumienności wtrąceniowej metodą transmisyjną wykonać dla wszystkich włókien zakończonych obustronnie złączkami mechanicznymi.
9) Pomiary reflektancji złączek mechanicznych, należy wykonać osobno dla każdej z zainstalowanych złączek E2000/APC/0,1dB RANDOM.

2.2 Cechy obiektu dotyczące rozwiązań budowlano-konstrukcyjnych i wskaźników ekonomicznych – Wymagania dotyczące łączy radioliniowych

2.2.1 Wymagania urządzeń radioliniowych

- praca w paśmie częstotliwości 5,4 GHz,
- musi posiadać możliwość pracy w kanałach 5 MHz, 10 MHz lub 15 MHz
- obsługa modulacji uplink/downlink: BPSK, QPSK, 16QAM, 64QAM
- anteny dwupolaryzacyjne (polaryzacja H i V)
- technika MIMO,
- adaptacyjna modulacja OFDM,
- przepływność w podstawowej konfiguracji 20Mbit/s, z możliwością programowego zwiększenia do 50Mbit/s lub 100Mbit/s,
- możliwość dynamicznej zmiany podziału pasma uplink/down link,
- dostępność wersji sprzętowej ODU z anteną zintegrowaną oraz w wersji z anteną zewnętrzną,
- wbudowany zabezpieczenie ochronne przed wyładowaniami atmosferycznymi w module ODU,
- korekcja błędów (FEC),
- obsługa 802.1q, 802.1p,
- wbudowany analizator widma,
- interfejs urządzenia wewnętrznego IDU 100BaseT lub 100/1000BaseT z obsługą auto MDI/MDIX,
- obsługa minimum 4 poziomów priorytetów ruchu,
- zarządzania i konfiguracja poprzez wbudowany serwer WWW, SNMP (w wersji co najmniej 2c) oraz dedykowany system zarządzania NMS
- podłączenie urządzenie zewnętrznego ODU poprzez jeden kabel sieciowy kat. 5 przenoszący zasilanie (PoE),
- maksymalny pobór mocy nie większy niż 60 Watt,
- zasilanie modułu wewnętrznego IDU z napięcia ~230V lub =48V,
- temperatura pracy urządzeń ODU (-40° C to +55° C)
- zgodność z wymogami zasadniczymi CE

2.2.2 Wymagania dla Systemu Zarządzania

Wymagania dla systemu zarządzania:

- możliwość definiowania kilku kont administratora,
- możliwość personalizacji ustawień graficznych konsoli administratora,
- zbieranie oraz monitorowanie parametrów jakościowych urządzeń, statystyk ruchowych, alarmów, zdarzeń,
- możliwość generowania wykresów parametrów radiowych urządzeń,
- tworzenie wzorów konfiguracyjnych z możliwością wprowadzania ich do wyselekcjonowanej grupy urządzeń,
- możliwość wyświetlania wszystkich elementów wybudowanej sieci radioliniowej na podkładach map satelitarnych,
- możliwość generowania profili terenowych,
- filtracja widoków m.in. poprzez typ urządzenia, stan urządzenia oraz stan łącza,
- możliwość aktualizacji oprogramowania zarządzanych urządzeń,
- możliwość integracji z systemami zarządzania wyższego poziomu poprzez SNMP.

2.3 Cechy obiektu dotyczące rozwiązań budowlano-konstrukcyjnych i wskaźników ekonomicznych – Wymagania dotyczące urządzeń aktywnych sieci

2.3.1 Ogólna charakterystyka urządzeń

Przedstawione w tym rozdziale wymagania co do rozlokowania poszczególnych urządzeń w poszczególnych obiektach i ich głównych parametrów związanych z prędkością i rodzajem portów transmisyjnych określają podstawowe warunki współpracy tych urządzeń w ramach sieci opisanej w niniejszym dokumencie.

Na etapie projektu wykonawczego powinna być opracowana szczegółowa charakterystyka każdego komponentu sieci rozumiana jako uszczegółowienie wymagań określonych w rozdziale 2.

2.3.1.1 Główny węzeł szkieletowy

Przewidziano jeden Główny Węzeł Szkieletowy w lokalizacji Urząd Miejski w Sławnie, który będzie wyposażony w następujące komponenty:

- Główny router i przełączniki szkieletowe (1 szt.)
  - Router 20x1GE SFP (1szt.)
  - Switch 24x1GE SFP (1szt.)
  - Switch 2x1GE SFP, 24x1GE (1 szt)
- Centralny Firewall z zaawansowanym systemem ochrony sieci – UTM
- System podtrzymania zasilania – UPS (3 godziny)
- Szafa Teletechniczna 19” 42U

2.3.1.2 Węzeł szkieletowy

- Przełącznik szkieletowy (4szt)
  - Switch 24x1GE SFP (4 szt) lub
  - Switch 2x1GE SFP, 24x1GE (4 szt)

- System podtrzymania zasilania UPS min 3 godziny (4szt.)
- Szafa Teletechniczna 19” 9U

Lista obiektów, w których będą ulokowane węzły szkieletowe jest przedstawiona w tabeli: Tabela 2. Lokalizacje węzłów szkieletowych szerokopasmowej sieci teleinformatycznej na stronie 9.

2.3.1.3 Punkt dostępowy

Punkty dostępowe będą zlokalizowane w obiektach, do których będą dostarczane usługi dla użytkowników sieci. Ogółem liczba dostępowych Bram Usługowych wyniesie 102 szt. W punktach dostępowych będą zainstalowane Bramy Usługowe w jednej z dwóch konfiguracji (w zależności od rodzaju łącza radiowe lub światłowodowe):

- 2 x 1 GE (1000BaseT) lub
- 2 x 1 GE SFP

We wszystkich lokalizacjach Brama Usługowa będzie rozbudowana o moduł bezprzewodowego dostępu do sieci WiFi.

Opcjonalnie Punkt Dostępowy może być wyposażony w przełącznik tranzytowy, co będzie miało miejsce, wtedy gdy topologia sieci światłowodowej lub radiowej w obszarze podłączenia do węzłów szkieletowych będzie inna niż gwiazda (kaskada lub pierścień). Przełączniki tranzytowe będą zainstalowane w konfiguracji portowej :

- 24x1000BaseT, 4x1GE SFP lub
- 24x1000BaseT

Nie przewiduje się zabezpieczenia tych przełączników systemem podtrzymania zasilania.

Urządzenia transmisyjne będą montowane w szafie teletechnicznej 19” 9U.

2.3.2 Centrum Zarządzania i Bezpieczeństwa Sieci

Centrum Zarządzania Bezpieczeństwem Sieci będzie realizowało funkcje kontroli i monitoringu wszystkich elementów sieci oraz z świadczonych przez tą sieć usług. Użytkownicy korzystający z usług sieci będą podlegali procesowi autentykacji, autoryzacji i weryfikacji.

Centrum Zarządzania Sieci będzie wyposażone w następujące urządzenia:

- System Monitoringu i Zarządzania Siecią
- Centralny System Zarządzania Bezpieczeństwa sieci
- System Kontroli Dostępu do Sieci
- System Autoryzacji, Autentykacji i Weryfikacji
- System podtrzymania zasilania UPS – 3 godziny (wspólny z Głównym Węzłem szkieletowym)
- Stanowisko administratorów - 3 stacje robocze PC z Monitorem 24”
- Przełącznik lokalnej sieci NOC w konfiguracji:
  - 48x1GE
- Szafa teletechniczna 19” 42U (wspólna z Głównym Węzłem szkieletowym)

2.3.3 Wymagania na podstawowe komponenty

2.3.3.1 Główny Przełącznik Szkieletowy

- Router musi być dedykowanym urządzeniem sieciowym o wysokości 2U przystosowanym do montowania w szafie rack 19 cali o głębokości 80 cm, wyposażonym w wymienny zasilacz oraz wentylatory. Ruter musi być wyposażony w zasilacze dostosowane do napięcia 220-230V, w ilości umożliwiającej poprawną pracę routera w pełnej konfiguracji przy obsadzeniu wszystkich dostępnych slotów modułami z interfejsami.
- Router musi posiadać możliwość wyposażenia w nadmiarowe zasilacze w celu uzyskania redundancji zasilania 1:1.
- Zarządzanie i konfiguracja routera przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny routera musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać ze sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez router nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony w co najmniej 2 GB pamięci RAM, pamięć Flash, port konsoli oraz interfejs Ethernet służący do zarządzania out-of-band. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu

operacyjnego routera z nośnika danych podłączonego do slotu USB na module kontrolnym.

- System operacyjny rutera musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo.
- Router mieć przepustowość nie mniejszą niż 60 Gbps full duplex oraz obsługiwać nie mniej niż 55 milionów pakietów na sekundę.
- Router musi obsługiwać interfejsy 10 Gigabit Ethernet zgodne z IEEE 802.3ae. Ruter musi być dostarczony z min. 4 interfejsami 10 Gigabit Ethernet XFP. Interfejsy 10 GbE muszą współpracować z modułami XFP pochodzącymi od innych producentów. Urządzenie musi umożliwiać rozbudowę do 8 interfejsów 10 Gigabit Ethernet.
- Router musi obsługiwać interfejsy 1 Gigabit Ethernet SFP. Musi być dostępny moduł z 20 interfejsami Gigabit Ethernet SFP. Urządzenia musi obsługiwać moduły SFP o prędkościach 1 Gb/s i 100 Mb/s. Interfejsy GbE muszą współpracować z modułami SFP pochodzącymi od innych producentów. Urządzenie musi umożliwiać rozbudowę do 40 interfejsów Gigabit Ethernet.
- Router musi obsługiwać ramki Jumbo o wielkości 9 KB.
- Porty GbE i 10 GbE urządzenia muszą obsługiwać mechanizm Digital Optical Monitoring (DOM).
- Urządzenie musi obsługiwać w sprzęcie routing IPv4, IPv6 oraz MPLS.
- Urządzenie musi obsługiwać routing statyczny IPv4 oraz ruting dynamiczny IPv4 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.
- Urządzenie musi obsługiwać routing statyczny IPv6 oraz ruting dynamiczny IPv6 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.

- Router jednocześnie musi obsługiwać nie mniej niż 900 tysięcy wpisów w tablicy routingu IPv4, 900 tysięcy wpisów w tablicy VPN IPv4, 700 tysięcy wpisów w tablicy routingu IPv6 oraz 128 tysięcy adresów MAC.
- Router musi obsługiwać mechanizm tworzenia wirtualnych ruterów (kontekstów, routerów logicznych) umożliwiający ruting pakietów w oparciu o niezależne tablice routingu – musi m.in. umożliwiać uruchomienie nie mniej niż 5 instancji routingu BGP dla różnych numerów systemów autonomicznych. Ponadto ruter musi obsługiwać sprzętowo 3 pełne tablice BGP dla IPv4 dla 3 różnych numerów systemów autonomicznych (przy założeniu, że w pełnej tablicy BGP znajduje się 300 tysięcy prefiksów). Router musi obsługiwać nie mniej niż 500 sesji BGP.
- Router musi obsługiwać protokół redundancji VRRP.
- Mechanizm BFD musi być obsługiwany dla IPv4, IPv6 oraz MPLS LSP.
- Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów. Filtrowanie ruchu musi odbywać się co najmniej na podstawie adresów MAC, IPv4 i IPv6. Router musi obsługiwać nie mniej niż 10 000 reguł filtrowania ruchu. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.
- Router musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Router musi udostępniać za pomocą protokołu SNMP co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach tranzytowych. Ponadto po SNMP muszą być dostępne liczniki pakietów i bajtów przechwyconych przez poszczególne filtry ruchu (ACL).
- Router musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wyjściowego i wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL) oraz dla poszczególnych sieci VLAN.

- Router musi posiadać mechanizmy klasyfikowania ruchu, jego filtrowanie oraz znakowanie w oparciu co najmniej 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN. Dodatkowo klasyfikacja pakietów musi się również odbywać o dane z protokołu BGP – nie mniej niż Community i AS Path. Znakowanie pakietów musi być wykonywane również przez tri-colored policer.
- Urządzenie musi wykonywać shaping lub policing ruchu per port.
- Router musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego. Urządzenie musi posiadać możliwość buforowania do 100 ms na wszystkich portach tranzytowych. Router musi obsługiwać mechanizm WRED.
- Router musi mieć zaimplementowane tunelowanie GRE oraz IP-IP bezpośrednio na karcie liniowej o wydajności przynajmniej 1Gbps.
- Router musi obsługiwać ruch IP multicast – w zakresie co najmniej protokołów IGMP (wersje 1, 2, 3) oraz PIM-SM.
- Na wszystkich interfejsach przeznaczonych do obsługi ruchu tranzytowego urządzenia musi obsługiwać usługi MPLS – nie mniej niż L2 VPN, VPLS (oparte o LDP i BGP) oraz BGP/MPLS VPN (L3 VPN).
- Router musi obsługiwać nie mniej niż 2000 sieci VPLS.
- Dla L2 VPN oraz VPLS musi być obsługiwany multihoming.
- Router musi obsługiwać protokół sygnalizacji RSVP-TE z mechanizmem Fast Reroute (node protection oraz link protection).
- Router musi posiadać możliwość uruchomienia mechanizmu DiffServ Traffic Engineering w celu przekierowania ruchu należącego do różnych klas obsługi ruchu na różne ścieżki MPLS.
- Router musi obsługiwać ruch multicast w IPVPN według draft-rosen-vpn-mcast-08.txt.
- W ramach IPVPN ruch multicast musi być obsługiwany wykorzystując sygnalizację BGP oraz w zakresie transportu MPLS point-to-multipoint według draft-ietf-l3vpn-2547bis-mcast-bgp-03.txt, draft draft-ietf-l3vpn-2547bis-mcast-02.txt, Requirements for Multicast in Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs) RFC4834 oraz draft-ietf-l3vpn-mvpn-considerations-01

- Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 4094 sieci VLAN jednocześnie.
- Urządzenie musi obsługiwać mechanizm Q-in-Q włącznie z funkcją terminowania wewnętrznych sieci VLAN na interfejsach warstwy trzeciej.
- Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s.
- Ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone przez urządzenie również w trybie MPLS/VPLS.
- Urządzenie musi obsługiwać pracę w architekturze pierścienia z możliwością przerwania pierścienia w różnych miejscach dla różnych sieci wirtualnych (np. z wykorzystaniem Per VLAN Spanning Tree Protocol). Urządzenie musi umożliwiać szybkie przywrócenie (nie dłużej niż 1 sekunda) komunikacji w pierścieniu składającym się z co najmniej 100 urządzeń.
- Router musi obsługiwać mechanizm monitorowania i próbkowania ruchu w warstwach 3 i 4 dla ruchu IPv4 przy pomocy protokołu sFlow lub równoważnego. Router musi obsługiwać protokół Netflow v9 zgodnie z RFC 3954 z pełną wydajnością.
- Router musi być zarządzany poprzez tekstowy interfejs linii komend (CLI) dostępny po porcie konsoli, oraz protokół Telnet i SSH dostępny przez interfejs do zarządzania out-of-band oraz dowolny interfejs tranzytowy. Router musi posiadać funkcję współpracy z zewnętrznymi serwerami AAA RADIUS (RFC 2138, RFC 2139) oraz TACACS+ (RFC 1492).
- Router musi posiadać funkcję limitowania pasma dla usług, których działania jest niezbędne do prawidłowego działania urządzenia, a które mogą stać się celem ataku Denial of Service.
- Urządzenia musi mieć domyślnie zaimplementowane zabezpieczenia przed atakami na poziomie protokołu ARP – minimalny wymagany poziom zabezpieczeń to limitowanie ruchu ARP.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej

przez okres jednego roku.

- Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, przez producenta oraz polskiego dystrybutora sprzętu,
- wymianę uszkodzonego sprzętu (wysyłka sprzętu: producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania, dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych

2.3.3.2 Przełącznik węzłowy 24xSFP

Switch stackowalny o następującej konfiguracji:

- obudowa rackowa 19” o wysokoci 1U
- co najmniej 24 sloty SFP 100BASE-FX/1000-BASE-X akceptujące interfejsy SFP dowolnego producenta
- możliwość instalacji co najmniej 2 slotów 10 GbE typu XFP, akceptujące interfejsy XFP dowolnego producenta lub 4 sloty 1 GbE typu SFP akceptujące interfejsy SFP dowolnego producenta
- możliwość stackowania co najmniej 10 switchy z przepływnością stacka co najmniej 128 Gbit na sekundę
- obsługa co najmniej 24000 adresów MAC
- obsługa co najmniej 4096 VLANów
- obsługa co najmniej 10000 Ipv4 prefixów
- obsługa co najmnie 2000 grup multicastowych
- obsługa multicastów z pełną przepustowością interfejsu
- obsługa 8 kolejek QoS per port oraz kolejki strict priority
- maksymalna przepustowość switcha co najmniej 65 milionów pakietów na sekundę
- dwa w pełni redundantne zasilacze AC
- obsługa następujących protokołów sieciowych: RSTP, MSTP, 802.1Q, GVRP, LACP, OSPF, IS-IS, BGP, VRRP
- obsługa protokołów IPv6: RIP, OSPF, ISIS, BGP
- obsługa protokołów IGMP v1,2,3 oraz PIM
- wsparcie dla mechanizmu QinQ

- wsparcie dla “private VLAN”
- dostęp po protokole SSH z możliwością uwierzytelniania za pomocą protokołu RADIUS
- wsparcie dla 802.1X
- możliwość edycji konfiguracji na urządzeniu bez jej jednoczesnego aplikowania (aplikowanie konfiguracji na żądanie)
- możliwość powrócenia do uprzednio zapisanej konfiguracji w wypadku utraty połączenia z urządzeniem.
- Urządzenie musi być objęte wsparciem w okresie jednego roku:
    - Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu,
    - Wymiana uszkodzonego sprzętu (producent wysyła sprzęt następnego dnia roboczego),
    - Dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.3.3.3 Przełącznik węzłowy 24xGE

- Przełącznik musi być dedykowanym urządzeniem sieciowym o głębokości nie większej niż 30 cm, wysokości 1U i przystosowanym do montowania w szafie rack 19’’ oraz posiadać oprzyrządowanie niezbędne do zamocowania w takiej szafie.
- Przełącznik musi posiadać 24 porty dostępowe Ethernet 10/100/1000 Auto-MDI/MDIX.
- Przełącznik musi być wyposażony w nie mniej niż 4 wbudowane porty uplink Gigabit Ethernet SFP– (obsługiwane co najmniej TX, SX, LX, LH, a także FX i BX)
- Przełącznik musi posiadać zasilacz AC oraz moduł wentylacji.
- Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
- Przełącznik musi być wyposażony w nie mniej niż 1 GB pamięci Flash oraz 512 MB pamięci DRAM. Przełącznik musi posiadać slot USB pozwalający na podłączenie zewnętrznego nośnika danych. Przełącznik musi umożliwiać uruchomienie systemu operacyjnego z zewnętrznego nośnika danych umieszczonego w slocie USB.
- Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.

- Przełącznik musi posiadać architekturę non-blocking. Wydajność przełączania w warstwie 2 nie może być niższa niż 56 Gb/s i 40 milionów pakietów na sekundę. Przełącznik nie może obsługiwać mniej niż 8 000 adresów MAC.
- Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
- Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1Q w ilości nie mniejszej niż 1024. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based).
- Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3AD - nie mniej niż 32 grupy LAG, po nie mniej niż 8 portów.
- Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP).
- Switch powinien posiadać opcję definiowania zapasowego portu dla portu podstawowego, tzn. tylko jeden z dwóch interfejsów jest aktywny w danej
- Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
- Urządzenie musi obsługiwać ruting między sieciami VLAN – ruting statyczny oraz protokół rutingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 6 000.
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wchodzącego i wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1P), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
- Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 1500 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
- Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
- Przełącznik musi posiadać funkcjonalność IGMP (v2, v3) snooping i wysyłać ramki multicastowe tylko do nasłuchujących klientów.

- Urządzenie musi posiadać możliwość diagnostyki kabla, TDR (Time Domain Reflectometer) na wszystkich portach 10/100/1000BASE-T.
- Przełącznik musi obsługiwać IEEE 802.1X zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
- Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
- Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem.
- Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 40 poprzednich, kompletnych konfiguracji.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres jednego roku.
    - Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, przez producenta oraz polskiego dystrybutora sprzętu,
    - wymianę uszkodzonego sprzętu (wysyłka sprzętu: producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania,
    - dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych

2.3.3.4 Centralny Firewall

Wymagania na Firewall:

- System zabezpieczeń musi realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz aplikacji Urządzenie musi realizować zarządzanie pasmem sieci (QoS) oraz musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site.
- Urządzenie zabezpieczeń musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI (IPS) wspieranego sprzętowo. Aktualizacja bazy sygnatur ataków (IPS) powinna odbywać się na żądanie, bądź automatycznie zgodnie z ustalonym w konfiguracji harmonogramem.
- Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu kontroli antywirusowej kontrolującego pocztę elektronicznej (SMTP, POP3, IMAP, FTP oraz HTTP. Włączenie kontroli antywirusowej nie wymaga dodatkowego serwera.
- Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu kontroli antyspamowej działającego w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie wymaga dodatkowego serwera.
- Urządzenie zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie wymaga dodatkowego serwera.
- System zabezpieczeń musi być dostarczany jako dedykowane urządzenie sieciowe nie posiadające wrażliwych na awarie elementów sprzętowych (np. twardego dysku). Całość sprzętu i oprogramowania musi być dostarczana i supportowana przez jednego producenta.
- System zabezpieczeń nie może posiadać ograniczeń na liczbę chronionych komputerów w sieci wewnętrznej.
- System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki definiowane są pomiędzy dowolnymi strefami bezpieczeństwa. Urządzenie musi obsługiwać nie mniej niż 30 stref bezpieczeństwa.
- Urządzenie zabezpieczeń musi być sterowane przez opracowany przez producenta zabezpieczeń dedykowany system operacyjny.
- Urządzenie zabezpieczeń musi posiadać przepływność firewall nie mniej niż 1Gbps (dla dużych pakietów) i nie mniej niż 500 Mb/s dla ruchu dla ruchu IMIX; nie mniejszą niż 250 Mb/s dla IPSec VPN (3DES/AES) i obsługiwać nie mniej niż 4000 polityk bezpieczeństwa.

- Urządzenie zabezpieczeń musi być wyposażone w 16 portów Gigabit Ethernet 10/100/1000 Base-T oraz posiadać 4 sloty na dodatkowe moduły interfejsów. Wbudowane interfejsy muszą umożliwić dowolne definiowanie trybu pracy – jako interfejs L3, czy też grupowanie interfejsów w grupę L2 (Bridge Group)
- W urządzeniu musi istnieć możliwość uruchomienia następujących interfejsów sieciowych: E1, Serial, ISDN BRI, ADSL2, oraz Ethernet 1000 Mbps SFP.
- Urządzenie musi zapewniać obsługę 512 sieci VLAN
- Urządzenie musi posiadać minimum 1 GB pamięci operacyjnej (DRAM).
- Urządzenie musi oferować wsparcie dla 802.1X
- Sieci VPN tworzone przez system zabezpieczeń muszą działać poprawnie w środowiskach sieciowych, gdzie na drodze VPN wykonywana jest translacja adresów NAT. System zabezpieczeń musi posiadać zaimplementowany mechanizm IPSec NAT Traversal dla konfiguracji VPN client-to-site oraz site-to-site.
- System zabezpieczeń musi posiadać zaimplementowane mechanizmy monitorowania stanu tuneli VPN i stałego utrzymywania ich aktywności (tzn. po wykryciu nieaktywności tunelu automatycznie następuje negocjacja IKE).
- Konfiguracja VPN musi odbywać się w oparciu o reguły polityki bezpieczeństwa (Policy-based VPN) oraz ustawienia rutingu (Routing-based VPN).
- Urządzenie musi obsługiwać nie mniej niż 20 wirtualnych ruterów posiadających odrębne tabele rutingu, umożliwiające podłączenie do urządzenia sieci o tej samej adresacji IP. Urządzenie musi obsługiwać protokoły rutingu RIP, OSPF i BGP.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (m.in. pasma gwarantowane i maksymalne, priorytety, oznaczenia DiffServ).
- Zarządzanie funkcjami zabezpieczeń w pełnym zakresie musi odbywać się z linii poleceń (CLI), graficznej konsoli GUI, oraz scentralizowanego systemu zarządzania. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Administratorzy mogą być uwierzytelniani za pomocą haseł statycznych oraz haseł dynamicznych (RADIUS).

- System zabezpieczeń musi posiadać mechanizmy uwierzytelniania tożsamości użytkowników za pomocą haseł statycznych i dynamicznych. Użytkownicy definiowani są w bazie lokalnej (tzn. bazie utrzymywanej na urządzeniu) oraz na zewnętrznych serwerach LDAP, RADIUS lub SecurID (ACE/Server).
- System zabezpieczeń musi współpracować z wiodącymi urzędami certyfikacji (m.in. Verisign, Entrust, Microsoft) i musi wspierać standardy PKI (PKCS 7, PKCS 10) oraz protokół SCEP
- System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT umożliwiają m.in. dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet. Udostępnianie w Internecie usług wielu serwerów musi odbywać się z użyciem tylko jednego publicznego adresu IP.
- System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim.

Wraz z produktem wymagane jest dostarczenie opieki technicznej oraz subskrypcji na funkcję IPS (AV, AS etc) ważnej przez okres 1 roku. Opieka powinna zawierać:

- wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora zabezpieczeń,
- wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania,
- aktualizację bazy ataków IPS,
- definicji wirusów,
- blacklist antyspamowych
- bazy kategorii stron WWW,
- dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.3.3.5 System Monitoringu i Zarządzania Sieci

Własności centralnego systemu zarządzania urządzeniami sieciowymi i urządzeniami zabezpieczeń

- Centralny system zarządzania powinien posiadać funkcje monitorowania i konfigurowania wszystkich aktywnych urządzeń sieciowych zastosowanych w projekcie.
- Centralny system zarządzania musi składać się z serwera zarządzania zainstalowanego na serwerze oraz konsoli GUI zainstalowanej na stacjach roboczych. Serwer zarządzania musi zawierać bazę polityk bezpieczeństwa oraz konfiguracje i logi ze wszystkich zarządzanych urządzeń. W sieci można zainstalować wiele konsol GUI.
- System zarządzania musi pozwalać na zarządzanie co najmniej 200 urządzeniami, z możliwością zwiększenia tej liczby.
- System zarządzania z jednej konsoli GUI musi pozwalać na konfigurację urządzeń firewall/VPN w zakresie systemu operacyjnego (m.in. adresacja i ruting IP) oraz zabezpieczeń (m.in. firewall, VPN i QoS).
- System zarządzania musi pozwalać na skonfigurowanie całości urządzenia zabezpieczeń firewall/VPN bez dostępu do urządzenia, a następnie wyeksportowanie konfiguracji do zabezpieczonego kryptograficznie pliku (zaszyfrowanego). Urządzenie zabezpieczeń powinno umożliwiać załadowanie tak stworzonej konfiguracji.
- System zarządzania musi odczytywać konfigurację istniejącą na urządzeniu zabezpieczeń oraz musi wprowadzać na urządzenie nową konfigurację.
- System zarządzania musi posiadać funkcjonalność stworzenia 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 systemu zabezpieczeń musi składać 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 musi umożliwiać wykonywanie scentralizowanej aktualizacji oprogramowania urządzeń zabezpieczeń oraz wykonywania backup-ów konfiguracji urządzeń.
- System zarządzania musi pozwalać na scentralizowane aktualizowanie bazy sygnatur ataków na wielu urządzeniach zabezpieczeń, zlokalizowanych w różnych miejscach w sieci.
- System zarządzania musi śledzić wszystkie czynności wykonywane na nim przez administratorów zabezpieczeń.
- System zarządzania musi zawierać narzędzia korelujące zdarzenia związane z bezpieczeństwem (m.in. przedstawia zestawienia komputerów wykonujących ataki, komputerów na które zostały wykonane ataki oraz rodzaje przeprowadzonych ataków).
- System zarządzania musi umożliwiać zdefiniowane wielu poziomów uprawnień administratorów (minimum 50 różnych uprawnień).
- System zarządzania musi monitorować stan tuneli VPN (tzn. przedstawiać graficzną prezentację aktualnego stanu tuneli VPN oraz wynegocjowanych parametrów IPSec i IKE).
- System zarządzania musi pozwalać na przeglądanie i selekcjonowanie rejestrowanych zdarzeń.
- System zarządzania musi generować raporty graficzne i tekstowe na postawie rejestrowanych zdarzeń.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres jednego roku.
    - Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, przez producenta oraz polskiego dystrybutora sprzętu,

- wymianę uszkodzonego sprzętu (wysyłka sprzętu: producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania,
- dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.3.3.6 Centralny System Zarządzania Bezpieczeństwem Sieci

Scentralizowany, zintegrowany system zarządzania bezpieczeństwem SIEM i NBAD

- System zarządzania bezpieczeństwem musi utrzymywać centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizować funkcje Security Information and Event Management (SIEM) i Network Behavior Anomalny Detection (NBAD).
- Moduł SIEM musi pobierać logi z wielu różnych elementów systemu informatycznego, poddawać je korelacji i na tej podstawie przedstawiać administratorom wiarygodne informacje na temat stanu bezpieczeństwa i wykrytych incydentów.
- Moduł NBAD na podstawie statystyk i opisu ruchu (NetFlow, itp.) pobieranych bezpośrednio z urządzeń sieciowych (ruterów, przełączników) musi dokonywać analizy stanu i efektywności pracy sieci, w tym wykrywania sytuacji nieprawidłowych (anomalii).
- Moduł NBAD musi dokonywać wykrywania anomalii w systemie informatycznym za pomocą analizy behawioralnej. W tym celu muszą być na bieżąco budowane profile normalnego stanu i zachowania sieci oraz identyfikowane odchylenia (m.in. zmiany stanu, nagłe zwiększenia lub zmniejszenia natężenia ruchu i przekroczenie wartości progowych).
- Moduł NBAD musi posiadać możliwość wykrywania nowych obiektów w systemie informatycznym (hostów, aplikacji, protokołów, itd.). Moduł NBAD musi także posiadać możliwość wykrywania awarii systemów, m.in. zablokowanych lub uszkodzonych serwerów i aplikacji.
- System zarządzania musi być dostarczony jest jako jedno, gotowe do użycia urządzenia Appliance. Nie jest dopuszczalne oprogramowanie instalowane na sprzęcie ogólnego przeznaczenia.
- Urządzenie Appliance musi posiadać minimum 8 GB pamięci RAM oraz 2 dyski o pojemności co najmniej 500 GB funkcjonujące w konfiguracji RAID 1.

- Urządzenie Appliance musi posiadać wydajność co najmniej 250 zdarzeń na sekundę oraz 15000 strumieni (Flows) na minutę.
- Urządzenie Appliance musi działać na bazie dostrojonego przez producenta systemu operacyjnego klasy Linux. Nie jest dopuszczalne zastosowanie do tego celu systemu operacyjnego Microsoft Windows.
- Urządzenie Appliance musi umożliwiać integrację z zewnętrznymi repozytoriami danych, co najmniej i SCSI SAN i NAS.
- Wszystkie funkcje systemu (SIEM, NBAD) muszą być dostępne są w ramach jednego urządzenia Appliance.
- Moduły SIEM i NBAD muszą być zintegrowane ze sobą tak, aby informacje o naruszeniach bezpieczeństwa były przedstawiane na podstawie analiz obu tych modułów.
- Obsługa incydentów bezpieczeństwa musi odbywać się na podstawie wielu źródeł informacji, nie mniej niż:
    - zdarzenia i logi z systemów zabezpieczeń (firewall, VPN, IPS, AV, itd.), systemów operacyjnych (Unix, Microsoft Windows, itd.) oraz aplikacji i baz danych,
    - statystyki i opis ruchu sieciowego odbierane z urządzeń za pomocą NetFlow, J-Flow, S-Flow i Packeteer oraz odczytywane bezpośrednio z sieci (span port),
- System zarządzania musi umożliwiać pobieranie logów z innych systemów za pomocą wielu metod, nie mniej niż Syslog (standardowy format logów, protokoły TCP i UDP), SNMP (wiadomości o zdarzeniach przesyłane poprzez SNMP Trap), a także Security Device Event Exchange (SDEE) i Java Database Connectivity API (JDBC).
- System zarządzania musi umożliwiać odczytywanie logów z systemów operacyjnych Microsoft Windows i Unix, nie mniej niż Redhat Linux, IBM AIX i SUN Solaris.
- System zarządzania w zakresie odczytu logów musi umożliwiać integrację z innymi systemami zarządzania zabezpieczeń, nie mniej niż Juniper Security Manager, IBM ISS SiteProtector i Check Point SmartCenter.
- Administratorzy bezpieczeństwa muszą mieć do dyspozycji dedykowane, graficzne narzędzia, uruchamiane z wykorzystaniem standardowej przeglądarki Web. Nie jest dopuszczalne instalowanie do tego celu dodatkowych aplikacji.
- System zarządzania musi posiadać możliwość powiadamiania administratorów o zdarzeniach za pomocą co najmniej email, SNMP oraz Syslog. System zarządzania

musi posiadać możliwość nawiązania połączenia z urządzeniami zabezpieczeń sieci w celu zablokowania niedozwolonej komunikacji.

- System zarządzania musi umożliwiać przypisywanie zidentyfikowanych incydentów bezpieczeństwa do obsługi określonym administratorom.
- System zarządzania musi umożliwiać wdrożenie w architekturze scentralizowanej (wszystkie funkcje na jednym Appliance) oraz rozproszonej, złożonej z wielu urządzeń. Struktura rozproszona budowana jest w celu zwiększenia wydajności systemu. W przypadku rozproszonej struktury zarządzanie całości systemu musi odbywać się z jednej konsoli. W przypadku rozproszonej struktury musi być możliwość kryptograficznej ochrony (szyfrowanie) komunikacji sieciowej pomiędzy komponentami systemu.
- System zarządzania musi umożliwiać definiowanie precyzyjnych uprawnień administratorów w zakresie monitorowanego obszaru systemu informatycznego oraz dostępnych operacji w systemie zarządzania. Tożsamość administratorów musi być weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania - co najmniej RADIUS, LDAP i Active Directory.
- System zarządzania do celów obsługi zdarzeń musi utrzymywać centralne repozytorium logów z możliwością ich przeglądania w formie rzeczywistej (raw) oraz znormalizowanej. Dla logów system musi utrzymywać wskaźniki czasu (time stamp). Starsze logi muszą być poddawane kompresji.
- System zarządzania musi składować informacje w bazie danych zaprojektowanej do tego celu przez producenta. Nie jest dopuszczalne użycie do tego celu bazy danych ogólnego przeznaczania.
- Składowane w systemie zarządzania informacje muszą być zabezpieczone kryptograficznie za pomocą sum kontrolnych - dostępne są minimum funkcje MD2, MD5, SHA-1 oraz SHA-2 (NIST FIPS 180-2).
- System zarządzania musi mieć możliwość wykonywania operacji backup i restore, uruchamianych z graficznej konsoli. System zarządzania musi mieć możliwość wykonywania archiwizacji informacji do zewnętrznych repozytoriów danych – nie mniej niż iSCSI SAN i NAS.
- System zarządzania musi posiadać możliwość tworzenia wielu typów raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów oraz na podstawie predefiniowanych wzorców (raportów). Raporty muszą być tworzone są

w wielu formatach - minimum PDF, HTML, CSV, RTF i XML.

- System zarządzania musi posiadać co najmniej 200 predefiniowanych raportów. W celu sprawnego przeszukiwania predefiniowanych raportów muszą być one pogrupowane – co najmniej według typu urządzeń i zdarzeń bezpieczeństwa. W systemie muszą być dostępne predefiniowane raporty na zgodność ze standardami bezpieczeństwa - minimum dla PCI i SOX.
- System zarządzania musi utrzymywać szczegółowy log audytowy rejestrujący co najmniej następujące operacje administratorów - login/logoff i zmiany konfiguracji systemu.
- System zarządzania musi posiadać możliwości weryfikacji poprawności swojego działania i powiadamiania administratorów o nieprawidłowościach - co najmniej za pomocą wpisu do logów systemowych oraz SNMP Trap.

2.3.3.7 Brama Usługowa z punktem dostępowym HotSpot WiFi

Wymagania na bramę usługową

- Firewall musi być dostarczony jako dedykowane urządzenie sieciowe o wysokości 1U.
- Urządzenie musi być wyposażone w co najmniej 1 GB pamięci RAM, pamięć Flash 1 GB oraz port konsoli. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym.
- System operacyjny firewalla musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.
- Urządzenie musi być wyposażone w nie mniej niż 2 wbudowanych interfejsy Ethernet

10/100/1000 oraz 6 wbudowanych interfejsów Fast Ethernet 10/100 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji).

- Urządzenie musi być wyposażone w 1 slot na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: ADSL 2/2+, Serial, E1, Gigabit Ethernet (SFP). Ponadto urządzenie musi posiadać slot na podłączenie karty 3G ExpressCard z modemem HSDPA.
- Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 12 strefami bezpieczeństwa z wydajnością nie mniejszą niż 250 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 80 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 32 000 równoległych sesji oraz zestawić nie mniej niż 2 000 nowych połączeń/sekundę.
- Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 250 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 75 Mb/s. Urządzenie musi posiadać możliwość udostępniania użytkownikom wbudowanego klienta IPSec VPN za pośrednictwem strony WWW.
- Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 500 reguł polityki bezpieczeństwa.
- Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.
- Urządzenie zabezpieczeń musi mieć możliwość rozbudowy funkcjonalności (poprzez zakup licencji bez konieczności wymiany/rozbudowy sprzętu) o:
    - moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać

dodatkowego serwera Kontrola antywirusowa musi być realizowana sprzętowo z wydajnością nie mniejszą niż 30 Mb/s dla ruchu HTTP. Musi istnieć możliwość wyboru działania mechanizmu kontroli antywirusowej w trybie sprzętowym i programowym.

- moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera.
- moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera.

- Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 3 wirtualnych ruterów.
- Urządzenie musi oferować wsparcie dla 802.1X
  - Urządzenie powinno współpracować z Punktem Dostępowym WiFi spełniającym wymagania: IEEE Standard: EEE 802.11a/b/g, IEEE 802.11n draft 2.0, IEEE 802.11h, IEEE 802.11d, IEEE 802.11e
  - Security:802.11i, Wi-Fi Protected Access 2 (WPA2), WPA, 802.1X, Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)
  - Zarządzania z Aplikacji zarządzania I Monitorowania Sieci za pośrednictwem Bramy Usługowej opisanej w tym punkcie
- Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.
- Urządzenie musi obsługiwać co najmniej 16 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet.
- Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
- Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować

w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.

- Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta.
- Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
- Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres jednego roku.
    - Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, przez producenta oraz polskiego dystrybutora sprzętu,
    - wymianę uszkodzonego sprzętu (wysyłka sprzętu: producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania,
    - dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

2.3.4 Aplikacja Serwera Weryfikacji i Autentykacji

Jako aplikacja serwera weryfikacji i autentykacji powinno być zainstalowane oprogramowanie freeRADIUS.

2.3.5 System Kontroli Dostępu do Sieci

Wymagania na system kontroli dostępu:

- Urządzenie musi być oparte o specjalizowaną platformę sprzętową oraz zapewniać obsługę co najmniej 2000 jednoczesnych użytkowników.

- Rozwiązanie musi umożliwiać tworzenie i wymuszanie szczegółowych polityk kontroli dostępu użytkowników do zasobów sieciowych. Polityki tworzone są w oparciu o tożsamość użytkownika, stan bezpieczeństwa jego urządzenia dostępowego, lokalizację sieciową lub dowolną kombinację powyższych kryteriów.
- Wymuszanie polityk dostępu do sieci musi być możliwe w warstwie 2 modelu ISO/OSI z wykorzystaniem standardu 802.1X w celu zapewnienia funkcji NAC (ang. Network Access Control) w sieci oraz w warstwie 3 modelu ISO/OSI w celu zapewnienia kontroli dostępu na poziomie zasobu.
- Urządzenie musi umożliwiać budowanie infrastruktury NAC we współpracy z:
    - rozwiązaniami sieciowymi dowolnego dostawcy spełniającymi standard 802.1x/EAP,
    - urządzeniami kontroli dostępu (firewall),
    - dowolną kombinacją powyższych
- Rozwiązanie musi zawierać wbudowany serwer RADIUS umożliwiający uwierzytelnienie w warstwie 2 sieci w oparciu o standard 802.1x bez konieczności stosowania rozwiązań trzecich.
- Rozwiązanie musi umożliwiać autentykację użytkowników w oparciu o:
    - serwery RADIUS,
    - usługi katalogowe LDAP, Microsoft Active Directory, Novell NDS/eDirectory,
    - natywną, lokalna baza danych użytkowników,
    - system RSA SecurID,
    - certyfikaty X.509,
    - serwery NIS
- Urządzenie musi umożliwiać uwierzytelnienie dwuskładnikowe (hasło statyczne plus certyfikat, hasło dynamiczne plus certyfikat). Musi istnieć możliwość rozdzielenia serwera autentykacji użytkowników od serwera autoryzacji dostępu do zasobów.
- 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.
- 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,
  - integracji z systemami weryfikacji stanu bezpieczeństwa firm trzecich,

- Urządzenie musi umożliwiać budowanie konfiguracji odpornych na awarię w trybie Aktywny/Aktywny oraz Aktywny/Pasywny.
- System musi umożliwiać spójne zarządzanie z jednej konsoli administracyjnej wieloma urządzeniami w przypadku budowania konfiguracji nadmiarowych.
- Urządzenie musi posiadać min 2 porty 10/100 Base-TX.
- Urządzenie musi być zarządzane poprzez przeglądarkę Web
- Urządzenie musi umożliwiać wykonywanie lokalnych kopi zapasowych konfiguracji lub na zewnętrznym serwerze FTP oraz SCP.
- Urządzenie musi umożliwiać integrację z zewnętrznymi serwerami SNMP v.2 oraz SYSLOG
- Urządzenie musi przechowywać dwie wersje oprogramowania oraz umożliwiać reset do wersji fabrycznej.
- Urządzenie musi zapewniać możliwość współpracy z rozwiązaniem klasy SSL VPN 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.
- Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres jednego roku.
  - Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną, przez producenta oraz polskiego dystrybutora sprzętu,
  - wymianę uszkodzonego sprzętu (wysyłka sprzętu: producent wysyła sprzęt następnego dnia roboczego), dostęp do nowych wersji oprogramowania,

2.3.6 Stanowisko Administratorów Sieci

Stanowisko będzie wyposażone w

- Stację Robocze – 1 szt. (wg specyfikacji jak poniżej)

- Komputery przenośne laptop – 5 szt. (wg specyfikacji poniżej)

2.3.7 Stacja Robocza

Stacja robocza powinna być nie gorsza niż:

HP Z200 Xeon X3430 2.4GHz 3x1GB ECC 320GB DVD+/-RW Win7_32+WXPPL

O specyfikacji:

Typ obudowy komputera	Mini Tower
Nazwa rodziny produktów	HP Z200
Ilość zainstalowanych procesorów	1 szt.
Maksymalna ilość procesorów	1 szt.
Typ zainstalowanego procesora	Intel Xeon /Quad-Core/Kod procesoraX3430
Częstotliwość procesora	2,4 GHz
Częstotliwość szyny QPI/DMI	2,5 GT/s
Pojemność pamięci cache [L2]	8 MB
Ilość zainstalowanych dysków	1 szt.
Maksymalna ilość dysków	3 szt.
Pojemność zainstalowanego dysku	320 GB
Typ zainstalowanego dysku	SATA II
Zainstalowane sterowniki dysków	6 x SATA
Pojemność zainstalowanej pamięci	3072 MB
Maksymalna pojemność pamięci	16384 MB
Rodzaj zainstalowanej pamięci	DDR3
Typ pamięci	Non-ECC
Częstotliwość szyny pamięci	1333 MHz
Ilość banków pamięci	4 szt.
Ilość wolnych banków pamięci	1 szt.
Producent chipsetu zainstalowanej płyty głównej	Intel
Typ zainstalowanego chipsetu	3450
Zintegrowana karta graficzna	Nie
Zintegrowana karta dźwiękowa	tak
Typ zintegrowanej karty dźwiękowej	Zintegrowana
Zintegrowana karta sieciowa	tak
Typ zintegrowanej karty sieciowej	10/100/1000 Mbit/s

Bezprzewodowa karta sieciowa	Nie
Bluetooth	Nie
Ilość slotów PCI	3 szt.
Ilość wolnych slotów PCI	3 szt.
Ilość slotów PCI-E	1x1 szt.
Ilość wolnych slotów PCI-E	1x1 szt.
Ilość slotów PCI-E	4x1 szt.
Ilość slotów PCI-E	16x2 szt.
Ilość wolnych slotów PCI-E	16x2 szt.

- Dodatkowe informacje n/t slotów PCI
- 3 x slot PCI (standard)
- 1 x slot PCI-E 16x (standard)
- 1 x slot PCI-E 16x (standard) [16x mechanicznie, 4x elektrycznie]
- 1 x slot PCI-E 4x (standard)
- 1 x slot PCI-E 1x (standard)

Ilość wolnych kieszeni 3,5 (zewnętrznych)	0 szt.
Ilość wolnych kieszeni 3,5 (wewnętrznych)	2 szt.
Ilość wolnych kieszeni 5,25 (zewnętrznych)	2 szt.

Interfejsy:

- 1 x 15-stykowe D-Sub (wyjście na monitor)
- 13 x USB 2.0
- 1 x RJ-45 (LAN)
- PS/2 (klawiatura)
- PS/2 (mysz)
- 1 x wejście liniowe
- 1 x wyjście liniowe
- 1 x wejście na mikrofon
- 1 x wejście na mikrofon (na froncie obudowy)
- 1 x wyjście słuchawkowe (na froncie obudowy)

Dodatkowe informacje o portach USB 2.0/3.0

- 6 x USB 2.0 (tylny panel)
- 2 x USB 2.0 (przedni panel)
- 5 x USB 2.0 (opcja)

Napędy wbudowane (zainstalowane): DVD±RW Super Multi (+ DVD-RAM) Dual Layer

Moc zasilacza (zasilaczy):320 Wat

System operacyjny

- Microsoft Windows 7 Professional PL 32-bit
- Microsoft Windows XP Professional PL

Dołączone wyposażenie: mysz

Dodatkowe informacje: Fabryczny downgrade do Windows XP Professional

Stacja robocza powinna być wyposażona w monitor 24” o specyfikacji nie gorszej niż:

HP LP2475w o specyfikacji:

Parametry

Wielkość przekątnej ekranu (cale)	24
Rozdzielczość maksymalna (piksele)	1920x1200
Wielkość plamki (mm)	0
Rodzaj źródła światła (CCFL/LED)	CCFL
Typ podświetlenia (krawędziowe/matrycowe)	Krawędziowe
Jasność (cd/m2)	400
Kontrast (x:1)	1000
Kąt widzenia w pionie/poziomie (stopnie)	178/178
Czas reakcji (ms)	6

Regulacje obrazu

Regulacja temperatury barwowej	tak
Modyfikacja podstawowych barw składowych	tak

Ergonomia

Obracanie na boki	tak
Obracanie góra-dół	tak
Pivot	tak
Regulacje wejść wideo	tak
Przełącznik: DVI/D-Sub (przycisk wyboru źródła)	nie
Sprzętowe obracanie obrazu do pozycji pionowej	nie

Multimedia

Głośniki	nie

Subwoofer	nie
Mikrofon	nie
Wyjście audio	nie
Tuner TV	nie
Kamerka internetowa	nie
Czytnik kart pamięci	nie

Złącza

D-Sub (liczba)	Tak
DVI (liczba)	Tak
HDMI (liczba)	Tak
DisplayPort (liczba)	Nie
HDCP	tak
Hub USB (liczba)	Tak (5)
Komozytowe	tak
S-Video	tak
Euroscart	Nie
Komponentowe	tak

Wyposażenie dodatkowe

Pilot zdalnego sterowania	nie
Kabel DVI lub HDMI	tak
Kabel USB	tak
Kabel audio	nie
Oprogramowanie	nie
Kalibrator	nie

2.3.8 Komputer przenośny

Komputery przenośne (5 szt.) typu laptop powinny być nie gorsze niż:

HP EliteBook 8440p (VQ667EA)

O specyfikacji:

Właściwości systemowe

Typ procesora

Procesor Intel® Core™ i7-620M (2,66 GHz, 4 MB pamięci podręcznej L3)

Zainstalowany system operacyjny

Oryginalny Windows® 7 Professional 32

Zestaw układów

Mobile Intel® QM57 Express

Wymiary i waga

Waga produktu

Od 2,12 kg

Wymiary (szer. x głęb. x wys.)

33,6 x 23,6 x 3,1 cm

Pamięć

Standardowa pamięć

4 GB pamięci DDR3 SDRAM 1333 MHz

Gniazda pamięci

2 gniazda SODIMM z obsługą pamięci dwukanałowej

Archiwizacja danych

Napędy wewnętrzne

Dysk SATA II 500 GB, 7200 obr./min

Napędy optyczne

Blu-ray ROM DVD+/-RW SuperMulti DL LightScribe

Grafika

Wyświetlacz

Wyświetlacz LED HD+ o przekątnej 35,6 cm (14"), rozdzielczość 1600x900, z powłoką antyrefleksyjną

Grafika

Karta graficzna NVIDIA NVS 3100 z 512 MB wydzielonej pamięci wideo

Funkcje rozszerzeń

Porty

3 porty USB 2.0

1 wejście VGA

1 złącze DisplayPort

1 wejście mikrofonu stereo

1 wyjście słuchawek stereo/wyjście sygnałowe audio

1 port 1394a

1 gniazdo zasilania

1 złącze RJ-11 (wybrane modele)

1 port RJ-45

1 złącze dokowania

1 złącze akumulatora dodatkowego

Sloty

1 gniazdo kart Express Card/54

1 czytnik kart procesorowych

1 karta secure digital/MultiMedia

Karta dźwiękowa

Technologia HP Premier Sound™, głośniki stereo, wyjście słuchawek stereo/wyjście sygnałowe audio, wejście mikrofonu stereo, zintegrowany zespół dwóch mikrofonów, dotykowe sterowanie głośnością i wyciszeniem

Wbudowany aparat fotograficzny

Kamera internetowa 2 MP

Klawiatura

Klawiatura z otworami odpływowymi odporna na zalanie

Zawartość opakowania

Tabliczka dotykowa z przewijaniem z dwoma przyciskami wyboru, wskaźnik z dwoma dodatkowymi przyciskami wyboru

Komunikacja

Interfejs sieciowy

karta sieciowa Intel 10/100/1000 Gigabit

Technologie bezprzewodowe

Intel 802.11a/b/g/n, Bluetooth 2.1, moduł szerokopasmowy HP un2420 Mobile Broadband EV-DO/HSPA (wymaga usług operatora sieci telefonii komórkowej)

Wymagania dotyczące zasilania i eksploatacji

Zasilanie

Zasilacz zewnętrzny HP Smart 90 W, technologia HP Fast Charge

Typ akumulatora

6-ogniwowy akumulator litowy (51 Wh)

Zasilanie

6-ogniwowy akumulator litowy (51 Wh)

Zakres temperatur podczas eksploatacji

5-35°C

Zarządzanie bezpieczeństwem

Zarządzanie bezpieczeństwem

McAfee Security Solution, HP ProtectTools Security Manager, Enhanced Pre-Boot Security, HP SpareKey, One-Step Logon, Setup Password, DriveLock Password, TPM 1.2 Embedded Security Chip, TPM Enhanced DriveLock, HP Disk Sanitizer, gniazdo blokady Kensington, obsługa Computrace LoJack Pro dla narzędzi HP ProtectTools, opcj. czytnik linii papilarnych HP, opcj. filtr ekranowy HP Privacy Filter, opcj. obsługa Computrace LoJack Pro Premium dla narzędzi HP ProtectTools z funkcją monitoringu GPS

W zestawie

Dołączone oprogramowanie

HP Recovery Manager (tylko w systemach Windows 7 i Vista), HP QuickLook, HP QuickWeb, HP Power Assistant, HP Client Manager Software

Gwarancja

3-letnia gwarancja z naprawą w punkcie serwisowym, w niektórych krajach z odbiorem i zwrotem do klienta (dostępne są rozszerzenia gwarancji sprzedawane oddzielnie), roczna gwarancja na akumulator podstawowy lub 3-letnia gwarancja na akumulator HP Long Life

2.4 Warunki wykonania i odbioru robót budowlanych odpowiadających zawartości specyfikacji technicznych wykonania i odbioru robót budowlanych

2.4.1 Wymagania na Wykonawcę

Wykonawca przedsięwzięcia powinien posiadać kompetencje w zakresie wszystkich stosowanych w przedmiotowym przedsięwzięciu technologii i stosowanych urządzeń i rozwiązań technicznych.

Wykonawca przedsięwzięcia powinien udokumentować zdolności integracji różnych technologii telekomunikacyjnych oraz zarządzania projektami o porównywalnej skali i zakresie rzeczowym. Na dowód tego Wykonawca powinien przedstawić odpowiednie referencje.

W postępowaniu o udzielenie zamówienia mogą wziąć udział Wykonawcy nie podlegający wykluczeniu na podstawie art. 24 ust. 1 i 2 ustawy Prawo zamówień publicznych i spełniający warunki art. 22 ust. 1 tj. Wykonawcy, którzy:

1. posiadają uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień;
2. posiadają niezbędną wiedzę i doświadczenie oraz dysponują potencjałem technicznym i osobami zdolnymi do wykonania zamówienia lub przedstawią pisemne zobowiązanie innych podmiotów do udostępnienia potencjału technicznego i osób zdolnych do wykonania zamówienia;
3. w zakresie sieci bezprzewodowych (łączy radioliniowych punkt-punkt w paśmie nielicencjonowanym 5,4 GHz) są autoryzowanym partnerem producenta proponowanej technologii i posiadają pisemne potwierdzenie tego faktu (autoryzację) wystawione przez przedstawiciela producenta;
4. w zakresie urządzeń aktywnych sieci szkieletowej i dostępowej są autoryzowanym partnerem producenta proponowanej technologii i posiadają pisemne potwierdzenie tego faktu (autoryzację) wystawione przez przedstawiciela producenta;

5. w zakresie bezpieczeństwa sieci IT są autoryzowanym partnerem producenta proponowanej technologii i posiadają świadectwo/certyfikat potwierdzający autoryzację.

Warunkiem udziału w postępowaniu jest:

1. Wykonanie przez Wykonawcę w sposób należyty w okresie ostatnich 5 lat (dla projektów 3 lat) przed dniem wszczęcia postępowania o udzielenie zamówienia, a jeżeli okres prowadzenia działalności jest krótszy, to w tym w okresie projektów i robót budowlanych, odpowiadających swoim rodzajem projektom i robotom budowlanym stanowiącym przedmiot zamówienia, tj. wykonanie:
    a. co najmniej 2 projektów budowlanych polegających na zaprojektowaniu kanalizacji teletechnicznej lub rurociągów kablowych oraz linii optotelekomunikacyjnej

       o łącznym zakresie minimum 100 000 m kanalizacji teletechnicznej lub rurociągów kablowych oraz minimum 100 000 m linii optotelekomunikacyjnej, w tym co najmniej 1 projektu o zakresie minimum 70 000 m kanalizacji teletechnicznej lub rurociągów kablowych oraz minimum 70 000 m linii optotelekomunikacyjnej, w tym co najmniej 5 000 m linii optotelekomunikacyjnej na terenie miejskim w ułożonej w mikrokanalizacji;
    b. co najmniej 2 robót budowlanych polegających na budowie kanalizacji teletechnicznej lub rurociągów kablowych o łącznej długości minimum 70 000 m, w tym łącznie co najmniej 5 000 m na terenie miejskim;
    c. co najmniej 2 robót budowlanych polegających na budowie linii optotelekomunikacyjnej o długości łącznej minimum 70 000 m, w tym co najmniej 1 roboty budowlanej polegającej na wybudowaniu linii optotelekomunikacyjnej o długości co najmniej 10 000 m w jednej relacji;
    d. co najmniej 2 robót budowlanych polegających na budowie na terenie miejskim linii optotelekomunikacyjnej ułożonej w mikrokanalizacji o długości łącznej minimum 5 000 m, w tym co najmniej 1 linii optotelekomunikacyjnej o długości co najmniej 3 000 m ułożonej w jednej relacji;
    e. co najmniej 1 roboty budowlanej polegającej na budowie, przebudowie lub remoncie nawierzchni bitumicznej o powierzchni co najmniej 1000 m^2 każda;

f. co najmniej 1 przedsięwzięcia polegającego na zaprojektowaniu i wybudowaniu w ramach jednego zlecenia gminnej sieci szerokopasmowej obejmującej przynajmniej 20 miejscowości, w tym przynajmniej 1 miasto;
g. co najmniej 2 przedsięwzięć polegających na zaprojektowaniu i wybudowaniu jednorodnej sieci łączy radioliniowych punkt-punkt, w tym co najmniej jednej sieci bezprzewodowej o łącznej liczbie co najmniej 40 łączy radioliniowych punkt-punkt;
h. przynajmniej 2 przedsięwzięć (projektów realizacyjnych) o wartości co najmniej 8 000 000 PLN brutto obejmujących swoim zakresem dostawy wdrożenia i integracji co najmniej trzech z wymienionych technologii: sieci światłowodowe, transmisja danych IP, bezpieczeństwo danych, transmisja radiowa.

2. Wykonanie przez Wykonawcę w sposób należyty w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie minimum dwie usługi polegające na dostawie urządzeń aktywnych sieci na rzecz jednego odbiorcy o całkowitej wartości dostaw co najmniej 1 000 000 zł każda.

3. Wykonanie przez Wykonawcę w sposób należyty w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie minimum jednej usługi polegającej na dostawie i wdrożeniu systemu urządzeń klasy UTM/NBAD/SIEM lub NAC w min. 2 lokalizacjach połączonych ze sobą siecią MAN/WAN, na kwotę min. 100.000 zł netto, w technologii zgodnej z przedmiotem niniejszego zamówienia

4. Dysponowanie osobami posiadającymi następujące kompetencje, doświadczenie zawodowe i uprawnienia:
   a. dla stanowiska Kierownik Kontraktu Wykonawca powinien udokumentować, że dysponuje lub będzie dysponować minimum 1 osobą posiadającą wykształcenie wyższe techniczne, udokumentowaną wiedzę w zakresie zarządzania projektami potwierdzoną certyfikatem PRINCE2 lub równoważnym certyfikatem innej organizacji, posiada aktualne uprawnienia budowlane do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności telekomunikacyjnej w zakresie telekomunikacji przewodowej wraz z infrastrukturą

towarzyszącą (udokumentowane co najmniej 5-letnie doświadczenie zawodowe) oraz wykazać aktualną przynależność do właściwej izby samorządu zawodowego, zgodnie z art. 12 ust. 7 Ustawy Prawo budowlane (Dz. U. z 2006r. Nr 156, poz. 1118 z późn. zm.) i posiadać wymagane ubezpieczenie od odpowiedzialności cywilnej. Wskazana osoba winna udokumentować zrealizowanie w charakterze Kierownika Projektu, nie mniej niż trzy projekty w specjalności telekomunikacyjnej obejmujących swoim zakresem integrację co najmniej trzech z wymienionych technologii: sieci światłowodowe, transmisja danych IP, bezpieczeństwo danych, transmisja radiowa.

b. dla stanowiska Główny Inżynier Wykonawca powinien udokumentować, że dysponuje lub będzie dysponować minimum 1 osobą posiadającą wykształcenie wyższe techniczne oraz uprawnienia wymagane przepisami Prawa budowlanego do pełnienia samodzielnych funkcji technicznych w budownictwie. Wskazana osoba winna posiadać aktualne uprawnienia budowlane do projektowania i kierowania robotami budowlanymi bez ograniczeń w specjalności telekomunikacyjnej w zakresie telekomunikacji przewodowej wraz z infrastrukturą towarzyszącą (udokumentowane co najmniej 3-letnie doświadczenie zawodowe) oraz wykazać aktualną przynależność do właściwej izby samorządu zawodowego, zgodnie z art. 12 ust. 7 Ustawy Prawo budowlane (Dz. U. z 2006r. Nr 156, poz. 1118 z późn. zm.) i posiadać wymagane ubezpieczenie od odpowiedzialności cywilnej.

c. W zakresie sieci bezprzewodowych:
    i. minimum dwoma inżynierami, którzy przeszli odpowiednie szkolenie i uzyskali certyfikację producenta oferowanego sprzętu potwierdzającą zdanie egzaminów w zakresie wdrożenia i utrzymania oferowanych rozwiązań, zgodnych z przedmiotem zamówienia.

d. W zakresie urządzeń aktywnych sieci:
    i. minimum dwoma inżynierami, którzy przeszli odpowiednie szkolenie i uzyskali certyfikację producenta oferowanego sprzętu potwierdzającą zdanie egzaminów w zakresie wdrożenia i utrzymania oferowanych rozwiązań, zgodnych z przedmiotem zamówienia.

e. W zakresie bezpieczeństwa sieci IT:
    i. minimum dwoma inżynierami, posiadającymi certyfikat producenta, potwierdzający zdanie egzaminów w zakresie implementacji i konfiguracji

oferowanych rozwiązań klasy UTM/NBAD/SIEM, zgodnych z przedmiotem zamówienia.

ii. minimum jednym inżynierem, posiadającym certyfikat producenta potwierdzający zdanie egzaminów w zakresie implementacji i konfiguracji oferowanych rozwiązań NAC, zgodnych z przedmiotem zamówienia

5. Znajdowanie się Wykonawcy w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia;

Potwierdzeniem sytuacji ekonomicznej i finansowej Wykonawcy zapewniającej wykonanie zamówienia i będącej warunkiem udziału w postępowaniu jest:

a. osiągnięcie średniorocznego przychodu za ostatnie 3 lata obrotowe, a jeżeli okres prowadzenia działalności jest krótszy – za ten okres (na podstawie „Rachunku zysków i strat” poz. „przychód netto ze sprzedaży produktów, towarów i materiałów” lub „przychód netto ze sprzedaży i zrównane z nimi”, a w przypadku Wykonawców niezobowiązanych do sporządzania sprawozdania finansowego innych dokumentów określających obroty) w wysokości nie mniejszej niż 10 000 000,00 PLN;
b. posiadanie środków finansowych lub zdolności kredytowej w wysokości co najmniej 1 000 000,00 PLN;
c. posiadanie ubezpieczenia od odpowiedzialności cywilnej w zakresie prowadzonej działalności, o wysokości sumy ubezpieczenia (określonej w PLN) nie mniejszej niż 1.500.000,00 PLN;

2.4.2 Warunki wykonania i odbioru - sieć światłowodowa

2.4.2.1 Rurociąg teletechniczny i mikrokanalizacja – wymagania projektowe dla elementów

Ogólne wytyczne dotyczące rurociągów kablowych

Podstawową funkcją sieci rurociągów kablowych jest stworzenie podziemnej infrastruktury liniowej służącej do prowadzenia kabli światłowodowych spełniających funkcję medium transmisyjnego dla Powiatowej Sieci Szerokopasmowej.

Elementy sieci oraz instalacje powinny zapewniać trwałość i funkcjonalność sieci przez okres 30 lat. Taki okres funkcjonowania sieci w normalnym trybie eksploatacji może zapewnić przyjęty w niniejszym opracowaniu wariant budowy sieci rurociągów kablowych wraz z zastosowanymi kablami światłowodowymi oraz fakt, że wybudowana sieć światłowodowa będzie siecią nowej generacji.

Zaprojektowana sieć rurociągów powinna umożliwiać instalacje i deinstalacje kabli światłowodowych z rurociągów przez cały okres eksploatacji. Dla zapewnienia długotrwałej sprawności i funkcjonalności rurociągi kablowe powinny być szczelne w każdym punkcie, niedostępne dla zanieczyszczeń stałych i płynnych zarówno w czasie budowy, jak i eksploatacji. Dotyczy to zarówno ciągów zajętych przez kable, jak i ciągów pustych. W Powiatowej Sieci Szerokopasmowej rurociągi kablowe wykonane będą w postaci zestandaryzowanych ciągów z rur HDPE układanych równolegle bezpośrednio w ziemi. Rury na całej długości rurociągu kablowego nie powinny w żadnym miejscu krzyżować się lub zamieniać miejscami z rurami sąsiednimi. Rozwiązanie przewiduje zastosowanie (na terenie miasta Sławno) ciągów mieszanych wykorzystujących standardowe rury HDPE 40/3,7mm oraz prefabrykowane rury z mikrokanalizacją w postaci wiązek mikrorur 5x10/8mm lub 10x7/5,5mm. Przyjęto zasadę – dwie standardowe rury HDPE 40 i jedna rura mikrokanalizacji. Dobór odpowiedniej konfiguracji zależny jest od miejsca w strukturze sieci.

Identyfikacja rur ciągów

Ciągi rur standardowych powinny być rozróżnialne przez stosowanie rur RHDPE40 koloru czarnego z oznakowaniem w postaci pasków: niebieskiego i czerwonego na zewnętrznej powierzchni oraz stosowanie przywieszek identyfikacyjnych w studniach i komorach kablowych. Rury z mikrokanalizacją powinny być wyróżnione w ramach ciągu kolorem pomarańczowym zewnętrznej powłoki. Wiązki z mikrorurkami powinny być różnokolorowe w celu zapewnienia identyfikacji pojedynczej mikrorury.

Studnie kablowe i zasobniki – wymagania ogólne

W Powiatowej Sieci Szerokopasmowej jako uzupełnienie rurociągów kablowych w zakresie miejsc łączenia, rozgałęziania i innych czynności ułatwiających eksploatacje wybudowanej sieci kanalizacji dopuszcza się zastosowanie następujących elementów:

- Betonowe studnie kablowe optymalne typu SKO-xx; (SKO);
- Studnie kablowe z tworzywa HDPE typu ROMOLD będące funkcjonalnymi odpowiednikami studni betonowych (SKPE);
- Zasobniki zapasu kabla (ZZK) i zasobniki złączowe (ZZ) z tworzywa HDPE;
- Akcesoria rozdzielcze i połączeniowe rur prefabrykowanych (typy Y, P, T, H) systemu mikrokanalizacji;
- Szafy kablowe zewnętrzne (SKZ) wyposażonych w niezbędny osprzęt dodatkowy.

Betonowe studnie kablowe

Zalecane studnie betonowe typu SKR przeznaczone są do budowy telekomunikacyjnej kanalizacji kablowej pierwotnej od 1-4 otworowej oraz kanalizacji teletechnicznej. Kształty i wymiary oraz wykonanie studni kablowych typu SKO uwzględniają wymagania dotyczące warunków instalowania współczesnych kabli telekomunikacyjnych, kabli optotelekomunikacyjnych (światłowodowych) oraz zapewniają wystarczająco dużo miejsca na posadowienie akcesoriów rozdzielczych i połączeniowych rur prefabrykowanych (typy Y, P, T, H). Dla ułatwienia prac montażowych projektować należy w miarę możliwości studnie dwudzielne.

Studnie kablowe z tworzywa HDPE

Zamiennikami studni betonowych są studnie kablowe z tworzywa HDPE zalecane do stosowania wszędzie tam gdzie występują tereny podmokłe, w centrum miasta, na zabytkowej Starówce oraz wszędzie tam gdzie trudno poruszać się ciężkim sprzętem budowlanym lub zabudowa studni spowodowałaby spore utrudnienia w ruchu.

Szafy kablowe

Rozdział tras kanalizacji i podział tras kabla światłowodowego dopuszcza się wykonywać również w specjalnych szafach zewnętrznych i wewnętrznych. W miarę możliwości należy unikać projektowania szaf zewnętrznych wybierając na miejsca podziału kabla pomieszczenia i szafy w budynku będącym własnością Zamawiającego.

Zastosowanie szaf kablowych zewnętrznych w powiatowej sieci szerokopasmowej powinno ograniczyć się do wykonywania pasywnych połączeń niewymagających instalacji sprzętu aktywnego wewnątrz szafy.

Każda szafa powinna posiadać:

- korpus wyposażony w drzwi z zamkiem;
- konstrukcję wsporczą i/lub elementy do mocowania osłon złączowych i ewentualnie innych elementów przewidzianych do umieszczenia w szafie;
- urządzenia do mocowania i uszczelniania wprowadzanych kabli;
- listwę zaciskową lub zacisk do uziemiania;
- opcjonalny osprzęt służący do zapewnienia odpowiednich warunków klimatycznych w szafie;
- ewentualnie inne części składowe - wg normy szczegółowej lub dokumentacji producenta.

Mikrokanalizacja światłowodowa – wymagania ogólne

Mikrokanalizacja jest rodzajem wielootworowej kanalizacji teletechnicznej o zmniejszonych średnicach podstawowych rur (otworów) przeznaczonych do instalacji mikrokabli światłowodowych. Podstawowym elementem systemu jest mikrorurka (mikrotuba) wykonana z HDPE będąca odpowiednikiem funkcjonalnym rur wtórnych typu

RHDPE w kanalizacji standardowej. Do mikrorurki wdmuchiwane są specjalne mikrokable światłowodowe o materiale powłoki i średnicach dobranych do średnicy mikrorurki.

Elementami składowymi systemów mikrokanalizacji są:

- **mikrorury** o średnicach zewnętrznych od 4 do 15 mm otwierające nowe możliwości w zakresie projektowania i budowy kanalizacji telekomunikacyjnej. Mikrorury są wykorzystywane do zwielokrotnienia liczby otworów rurociągu w ramach istniejącej kanalizacji wtórnej poprzez wdmuchiwanie lub zaciąganie mechaniczne nawet do kilkudziesięciu mikrorur o różnych średnicach. Szeroka gama średnic pozwala na łatwe dostosowanie do wymaganej pojemności i przyszłych zastosowań budowanej kanalizacji. Wiązki mikrorurek mogą być również instalowane w istniejącej kanalizacji teletechnicznej przy użyciu metod mechanicznych (zaciąganie) lub pneumatycznych.

- **rury prefabrykowane z wiązkami** zawierające do kilkunastu standardowych konfiguracji mikrorur o różnych średnicach. Wybór odpowiedniej konfiguracji zależy od miejsca zabudowy w strukturze sieci światłowodowej (rury szkieletowe, rury dla sieci dystrybucyjnych, rury w warstwie dostępowej, etc.).

- **akcesoria połączeniowe mikrorur** przeznaczone do wodoszczelnego (opcjonalnie gazoszczelnego) połączenia mikrorurek, wykonywania redukcji średnicy oraz zaślepiania niewykorzystywanych tub.

- **akcesoria połączeniowe rur** prefabrykowanych i standardowych potrzebnych do wykonywania szczelnych połączeń lub rozgałęzień rurociągu kablowego z mikrokanalizacją.

- **uszczelnienia rur** prefabrykowanych i wiązek mikrorur, uszczelnienia kabla i mikrorury oraz zatyczki dla końcówek rur

- **mikrokable** światłowodowe o średnicach i materiale powłoki odpowiednio dobranymi do zastosowania w poszczególnych typach mikrorur Dostępne są mikrokable z zakresu od włókien FTTH o średnicach od 1,2mm do 2,5mm przez kable o pojemności 72/96 włókien i średnicy max. 5,8 mm/7,2 mm aż do kabli o pojemnościach 144 i 192 włókna przy średnicy max.9,5mm

Mikrokanalizacja powinna zapewniać:

- łatwość wdmuchiwania mikrokabli światłowodowych na odcinkach do 2 km;
- ochronę sieci kablowej przed zagrożeniami mechanicznymi, chemicznymi i innymi, w tym przed uszkodzeniami mechanicznymi z powodu złego oznakowania (budowana bezpośrednio w ziemi),
- szybką rozbudowę równoległą i szeregową sieci światłowodowej bez wykonywania robót ziemnych,
- wykonywanie odgałęzień mikrokanalizacji w studniach kablowych, szafach ulicznych, pomieszczeniach technicznych lub bezpośrednio w ziemi,
- wodoszczelność na poziomie mikrorurek i mułoszczelność na poziomie rur z mikrorurkami, tzn. zabezpieczenie mikrokanalizacji przed przenikaniem wody do wnętrza mikrorurek i wnikaniem mułu i zanieczyszczeń stałych do wnętrza prefabrykowanych rur mikrokanalizacji niezależnie czy są one puste czy wypełnione mikrorurkami.

Do budowy mikrokanalizacji można wykorzystywać:

- istniejącą infrastrukturę kanalizacji teletechnicznej własnej Zamawiającego;
- istniejącą infrastrukturę innych operatorów telekomunikacyjnych;
- w szczególnych przypadkach wszelkie instalacje rurowe.

2.4.2.2 Kable optotelekomunikacyjne – wymagania ogólne

Wymagania dotyczące kabli światłowodowych liniowych i magistralnych

Do budowy linii światłowodowych na odcinkach odgałęzień zewnętrznych i magistralnych można używać zarówno mikrokabli światłowodowych o średnicy maksymalnej 6 mm, jak i kabli kanałowych układanych w kanalizacji standardowej. W odgałęzieniach zewnętrznych i relacjach punkt-punkt, dla których nie przewiduje się budowy ikrokanalizacji można stosować kable kanałowe do kanalizacji standardowej.

Wymagania dotyczące kabli światłowodowych warstwy dystrybucji

W warstwach niższych do budowy połączeń światłowodowych mogą być projektowane zarówno wymienione powyżej kable kanałowe wielotubowe, z tubą

centralną oraz mikrokable. Liczba włókien kabli stosowanych w tej warstwie wynosić będzie najczęściej od 4 do 48 włókien. Z uwagi na przyjętą minimalną ilość włókien doprowadzanych do budynku wynoszącą 4 włókna, optymalnym rozkładem włókien w kablach będą konstrukcje n x 4. W pozostałych przypadkach konstrukcja kabla może być inna i powinna odpowiadać aktualnym potrzebom i zamierzeniom rozwojowym.

Wymagania dotyczące kabli światłowodowych wewnątrz budynkowych

Kable do zastosowania wewnątrz budynków powinny mieć powłokę z materiału nierozprzestrzeniającego płomieni. Światłowody w kablu budynkowym powinny mieć włókna tego samego rodzaju, co w kablu liniowym. Przebiegający w budynku kabel liniowy prowadzi się w osłonie z rury z materiału trudnopalnego.

Wymagania dotyczące mikrokabli światłowodowych

Wymagania ogólne dotyczące kabli stosowanych w mikrokanalizacji zawiera norma europejska IEC60794-5.

W mikrokanalizacji budowanej na potrzeby Powiatowej Sieci Szerokopasmowej zalecane są mikrokable o parametrach zgodnych z wymienioną normą oraz spełniające dodatkowe, następujące wymagania:

- powłoki mikrokabli powinny być wykonane z materiałów zapewniających niski współczynnik tarcia w kontakcie z mikrorurkami;
- mikrokable powinny być dostosowane do instalacji w mikrokanalizacji metodą pneumatyczną strumieniową;
- średnice zewnętrzne mikrokabli powinny być dobrane do średnic wewnętrznych mikrorurek i powinny zapewniać projektowe zasięgi wdmuchiwania.

2.4.2.3 Osprzęt światłowodowy – standardy podstawowe

Osłony złączowe (mufy światłowodowe)

Osłony złączowe powinny być dostosowane do konstrukcji kabla oraz powinna umożliwiać wprowadzenie mikrorurek z możliwością doszczelnienia wykonanego w podobny sposób jak dla kabli światłowodowych. Odcinki instalacyjne kabli powinny być tak ułożone, aby złącza kabli światłowodowych były zlokalizowane w miarę możności w miejscach łatwo dostępnych.

Złącza kabli światłowodowych powinny być umieszczane w studniach kablowych, w zasobnikach złączowych (rurociągi kablowe), w szafach kablowych.

Przełącznice światłowodowe

Przełącznica światłowodowa powinna umożliwiać zakończenie różnych rodzajów linii optotelekomunikacyjnych, niezależnie od ich przeznaczenia, liczby i rodzaju światłowodów. Przełącznica światłowodowa jest przeznaczona do przyłączenia i odłączenia traktów światłowodowych od urządzeń stacyjnych oraz do dogodnego wykonania przełączeń torów światłowodowych między polami jednej przełącznicy.

2.4.2.4 Rurociąg teletechniczny i mikrokanalizacja – wytyczne wykonawczo-projektowe

Projektowanie trasy przebiegu rurociągów kablowych

Przebieg rurociągów powinien uwzględniać przebieg ulic ze szczególnym uwzględnieniem ulic remontowanych i modernizowanych przez Zarząd Dróg Miejskich. Z uwagi na wysokie koszta odtworzenia nawierzchni instalacja rurociągów przy wspólnych inwestycjach może przynieść Zamawiającemu 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.

Zalecane jest projektowanie tras rurociągów kablowych przez obszary w jak największym stopniu wykorzystujące zasoby miejskie, tj.:

- w istniejącej kanalizacji teletechnicznej będącej zasobem miasta;
- w chodniku;
- w trawniku;
- w pasie rozdzielającym drogi dwujezdniowe ;
- w pasie drogowym;
- w polu i terenach zielonych miasta;
- na mostach, przejściach schodowych, tunelach będących zasobem miasta.

Przepusty i skrzyżowania z przeszkodami terenowymi

Liczba zbliżeń i skrzyżowań rurociągu kablowego z innymi urządzeniami uzbrojenia terenowego, wodami powierzchniowymi, miejscami narażonymi na uszkodzenia mechaniczne, chemiczne, itp. powinna być możliwie mała.

Sposób realizowania zbliżeń i skrzyżowań podczas budowy rurociągu kablowego powinien być jednoznacznie określony w zatwierdzonym projekcie technicznym (projekcie budowlanym i wykonawczym) uzgodnionym z właścicielem uzbrojenia terenowego, do którego zbliża się projektowany rurociąg.

Przy skrzyżowaniach linii światłowodowych z przeszkodami wodnymi, jezdniami o nawierzchni utwardzonej, torowiskami, rurociągami itp. należy przewidzieć obiektowe rury przepustowe o średnicy, co najmniej 110 mm.

W każdym wypadku przy projektowaniu przejść pod dużymi obiektami wodnymi, drogami krajowymi, torami kolejowymi lub tramwajowymi należy zaprojektować większą liczbę rur niż to wynika z potrzeb.

Odgałęzienia rurociągu kablowego i kabli światłowodowych

Wszelkie odgałęzienia i zmiany tras przebiegu kabli w rurociągach kablowych w warstwie magistralnej oraz odgałęziania kabli światłowodowych (z zastosowaniem osłon złączowych) należy wykonywać w studniach, zasobnikach, szafach kablowych lub komorach kablowych budynków należących do Zamawiającego. Punkty styku miejskich rurociągów kablowych z sieciami innych operatorów należy lokalizować w studniach kablowych lub w szafach dostępowych przystosowanych do tego celu.

Wymagania dotyczące procesu projektowania mikrokanalizacji

Wybór metody wykonania mikrokanalizacji światłowodowej w warstwie dostępowej sieci należy dokonywać uwzględniając kilka czynników ekonomicznych i technicznych takich jak:

- miejsce instalacji mikrokanalizacji w strukturze sieci miejskiej uwzględniające ogólne wymagania, co do minimalnej ilości otworów kanalizacji w danej warstwie sieci światłowodowej i projektowanej pojemności sieci światłowodowej;

- rodzaj istniejącej kanalizacji teletechnicznej i możliwości techniczne jej wykorzystania pod rozbudowę o nowo instalowane wiązki mikrorurek;
- odległości pomiędzy studniami, które określają wybór metody instalacji mikrokanalizacji

Dobór średnic mikrorurek

Rozmiar mikrorurek należy dobierać odpowiednio do miejsca w strukturze sieci światłowodowej. Typowy zakres średnic zewnętrznych mikrorur wynosi: 4, 5, 7, 10, 12 i 15 [mm].

W warstwie dystrybucyjnej powinny być stosowane wiązki lub rury prefabrykowane z mikrorurkami o średnicach 12/10mm,10/8mm lub 7/5.5mm. W warstwie dystrybucyjnej średnice mikrorurek będą mniejsze, a zalecanymi średnicami będą: 10/8mm, 7/5.5mm, 5/3.8mm.

Dobór ilości mikrorurek (ilości otworów mikrokanalizacji)

Ilość otworów mikrokanalizacji będzie silnie zależna od docelowej pojemności systemu światłowodowego w danym miejscu. Na ogół ilość ta będzie silnie zależna od takich czynników jak:

- miejsce w strukturze sieci,
- docelowa pojemność systemu, pojemność pojedynczych kabli, które będą instalowane w każdej mikrorurce,
- ilość planowanych użytkowników mikrokanalizacji,
- współczynnik nadmiarowości.

Dla celów projektowych należy uzależnić ilość otworów od miejsca w strukturze projektu.

2.4.2.5 Wymagania dla dokumentacji projektowo-wykonawczej

Format i zawartość dokumentacji technicznej

Dokumentacją powiatowej sieci szerokopasmowej dla powiatu Sławno będą w szczególności:

1. projekt techniczny (projekt budowlany i projekt wykonawczy),
2. dokumentacje kosztorysowe,
3. dokumentacja powykonawcza.

Wymagania ogólne i zasady podstawowe dla dokumentacji technicznej

a) W dokumentacji projektowej musi znajdować się odniesienie do danych wyjściowych (formalnoprawnych oraz technicznych) stanowiących podstawę do opracowania i uzasadniających projektowane rozwiązania techniczne.

b) Dokumentacja projektowa musi być sporządzona w sposób umożliwiający jej sprawdzenie i weryfikację przyjętych rozwiązań technicznych.

c) Wszystkie rysunki muszą być wykonane przejrzyście, z naniesionymi czytelnie danymi, ponumerowane i podpisane przez autora (autorów) i sprawdzającego (w przypadku takiego wymogu ustalonego w odpowiednich przepisach prawnych).

d) Wszystkie rysunki, które nie są wykonane na mapach geodezyjnych, należy wykonać w programie AutoCad lub kompatybilnym i należy dostarczyć je również w wersji elektronicznej (w pliku edytowalnym).

e) Wszystkie tablice i zestawienia należy wykonać w programie Excel lub kompatybilnym i dostarczyć je w wersji elektronicznej (w pliku edytowalnym).

f) Dokumentację projektową należy przekazać Zamawiającemu. Zakres informacji zawartych w dokumentacji projektowej musi umożliwić uzyskanie pozwolenia na budowę lub skutecznego zgłoszenia, sporządzenie specyfikacji materiałowej, realizację budowy, prowadzenie nadzoru budowy i sporządzenie dokumentacji powykonawczej po zakończeniu budowy.

Zawartość projektu budowlanego

Projekt budowlany powinien zawierać:

a) stronę tytułową wg wzoru;
b) informację o podstawie prawnej opracowania (nr zlecenia, nr umowy, data zlecenia i umowy);
c) decyzję o warunkach zabudowy i zagospodarowania terenu (lub wypis z planu zagospodarowania przestrzennego);
d) uzgodnienia branżowe wraz z protokołami ZUDP;
e) pozwolenie na budowę (lub potwierdzenie skutecznego zgłoszenia);
f) ogólny przebieg projektowanej sieci telekomunikacyjnej,
g) przebieg sieci telekomunikacyjnej i przyłączy energetycznych na mapach geodezyjnych dopuszczonych na danym terenie do projektowania wraz z wszystkimi elementami sieci naniesionymi w wymaganej skali.
h) każdy rysunek powinien być zaopatrzony w tabelkę
i) trasę linii (sieci) telekomunikacyjnej stanowiącą przedmiot inwestycji na mapach ewidencji gruntów potwierdzonych przez właściwy urząd;
j) wypisy z ewidencji gruntów działek, przez które przebiega projektowana linia (sieć), potwierdzone przez właściwy urząd, a na kopiach za zgodność z oryginałem;
k) dokumenty stwierdzające prawo Zamawiającego do dysponowania terenem na czas prowadzenia budowy potwierdzone na kopiach za zgodność z oryginałem;
l) charakterystykę techniczną opracowania;
m) wykaz norm i dokumentów odniesienia, zgodnie z którymi wykonano projekt;
n) symbolikę i oznaczenia wykorzystane w projekcie budowlanym;
o) spis rysunków i schematów zawartych w projekcie budowlanym;
p) uwagi końcowe.

Zawartość projektu wykonawczego

Projekt wykonawczy powinien składać się z odpowiedniej liczby tomów (zgodnie z zakresem zadania).

Nazwa zadania podana w tytule powinna być zgodna z zapisem w umowie. Projekt wykonawczy (lub poszczególne jego części (zależnie od zakresu zadania) powinien zawierać:

a) stronę tytułową wg wzoru
b) informację o podstawie prawnej opracowania (nr zlecenia, nr umowy, data zlecenia i umowy);
c) rysunek ogólnego przebiegu projektowanej sieci telekomunikacyjnej;
d) projekt sieci rurociągów kablowych;
e) lokalizacje posadowienia szaf kablowych;
f) projekt sieci światłowodowej;
g) bilans mocy poszczególnych odcinków światłowodów (liczony dla fal 1310 i 1550);
h) wydruk przedmiarów dla projektowanego zakresu wraz z wersją elektroniczną w programie kosztorysowania określonym przez Zamawiającego;
i) charakterystykę techniczną opracowania;
j) wykaz norm i dokumentów odniesienia, zgodnie z którymi wykonano projekt;
k) symbolikę i oznaczenia wykorzystane w projekcie;
l) spis wykonanych rysunków i schematów;
m) tabele z danymi projektowymi;
n) uwagi końcowe.

Wymagania dla rysunków projektowych

Plan sytuacyjny sieci telekomunikacyjnej

Ogólny przebieg trasowy sieci telekomunikacyjnej należy przedstawić na jednym rysunku w skali nie mniejszej niż 1:10 000. Zakres informacji, która powinna być możliwa do uzyskania z map ogólnego przebiegu trasowego to przede wszystkim szybki przegląd trasy, ocena jej konfiguracji, lokalizacja punktów charakterystycznych (poszczególnych węzłów sieci miejskiej wraz z określeniem ich rodzaju, lokalizacja szaf kablowych, złączy światłowodowych, skrzyżowanie sieci z rzekami, torami kolejowymi itp.).

Przebieg trasowy rurociągów kablowych.

Przebieg rurociągu należy nanieść na dopuszczone do projektowania mapy geodezyjne (sytuacyjno– wysokościowe) w skali 1:500. Przebieg wyróżnić wg przyjętej metodyki.

Niezbędne jest również naniesienie na mapę:

a) lokalizacji studni kablowych;
b) lokalizacje obudów liniowych i odgałęzień mikrokanalizacji umieszczonych w studniach lub bezpośrednio w ziemi;
c) wszystkich rur ochronnych (obiektowych) przez podanie ich liczby, typu i długości;
d) lokalizacji zasobników i zapasów kabla światłowodowego;
e) lokalizacji złączy (należy podać numer złącza i jego typ);
f) długości trasowej i optycznej w miejscach charakterystycznych (szafy kablowe, studnie, złącza, zapasy, przejście przez rzeki, drogi);
g) lokalizacji szaf kablowych wraz z opisem;
h) przebiegu przyłączy energetycznych dla szaf kablowych.

Schemat rozwinięty rurociągów kablowych

Schemat rozwinięty kanalizacji kablowej należy wykonać w programie AutoCad lub kompatybilnym, umożliwiającym ich przeglądanie. Format schematów: A3 lub większy (wg ISO), złożony do A4. Schemat powinien pozwolić prześledzić trasę kabla

światłowodowego łączącego poszczególne warstwy sieci. Na schemacie koniecznie należy przedstawić:

a) przebieg rurociągów (z zachowaniem proporcji przy rysowaniu długości poszczególnych odcinków);
b) numerację studni;
c) długości przelotów między studniami;
d) liczbę rur rurociągu (profil);
e) liczbę mikrorur w wiązce (profil);
f) przebieg kabli (na profilach wskazać otwór zajmowany przez kabel);
g) lokalizację złączy;
h) sposób rozszycia kabli na przełącznicy w szafach optycznych;
i) opis kabli, złączy, zapasów;
j) godła geodezyjne i numery map, na których można znaleźć przedstawiony odcinek kanalizacji;
k) długości trasowe i optyczne kabli w miejscach charakterystycznych (złącza, zapasy, przełącznice w szafach optycznych)
l) podać adres lokalizacji szaf kablowych i szaf optycznych poszczególnych punktów węzłowych sieci;
m) zaznaczyć symbolicznie przebieg ulic ułatwiający zlokalizowanie poszczególnych elementów sieci.

Schemat rozpływu włókien światłowodowych

Schemat rozpływu włókien należy wykonać w programie AutoCad lub kompatybilnym. Format schematów: A3 lub większy (wg ISO), złożony do A4. Schemat powinien pozwolić prześledzić trasę włókien światłowodowych łączących poszczególne warstwy sieci.

Na schemacie należy przedstawić:

a) schemat rozszycia kabli na przełącznicach z uwzględnieniem numeracji:
   - stojaka przełącznicy i listwy na tym stojaku,
   - numeru pola na przełącznicy,
   - numeru włókna kabla głównego,

- numeru włókna kabla odgałęźnego
- nazwy kabla głównego i odgałęźnego;

b) lokalizację złączy (nr złącza, długość trasowa, długość optyczna, numer studni);
c) lokalizację zapasów (długość trasowa, długość optyczna, numer studni);
d) odpowiednie oznaczenie włókien (numer tuby, kolor osłony włókna);
e) dokładne informacje o kablu (typ, długość trasową i optyczną poszczególnych odcinków oraz całego kabla, nr odcinka fabrykacyjnego).

Rysunki obiektowe

Na kolejnych arkuszach (osobne rysunki) należy uwidocznić w skali 1:50 lub 1:100 wszelkie sytuacje kolizyjne, nieczytelne na mapach w skali 1:500. Sytuacje szczególne, kiedy niezbędne jest wykorzystanie do realizacji metody bezrozkopowej (przecisk lub przewiert sterowany), należy uwidocznić jako przekrój poprzeczny przez przeszkodę w skali 1:100 lub w skali 1:500/1:100 (dla przewiertów powyżej 100m).

Rysunek przebiegu wewnątrzbudynkowego

Schemat należy wykonać w skali 1:50 lub1:100 w programie AutoCad lub kompatybilnym. Format schematów: A3 lub większy (wg ISO), złożony do A4. Należy zwrócić szczególną uwagę na przedstawienie graficzne:

- miejsca wprowadzania kabli;
- sposobu ich prowadzenia (po drabinkach, w korytkach, po ścianie, po suficie, w rurce osłonowej);
- lokalizacji przełącznicy optycznej;
- długości projektowanych kabli i osłon rurowych oraz typu zastosowanego osprzętu.

Tabele w projekcie wykonawczym

W projekcie techniczno-wykonawczym (tom I) należy zamieścić tabele zawierające podsumowanie ilościowe kanalizacji warstwy magistralnej w formie zestawienia:

a) zakresu rzeczowego projektowanej kanalizacji i sieci światłowodowej;
b) długości kanalizacji;
c) ilości obiektów;
d) typów studni;
e) długości kabla światłowodowego;
f) projektowanych złączy i skrzynek zapasu kabla światłowodowego;
g) tabeli przedmiarów robót:

- rozbiórka i naprawa nawierzchni,
- budowa rurociągu kablowego i mikrokanalizacji,
- budowa i montaż sieci światłowodowej, itd

h) asortymentu i ilości materiałów;
i) zajmowanych odcinków pasa drogowego;

Zestawienie zbiorcze

Zestawienie zbiorcze zamieszczane dokumentacji wykonawczej powinno zawierać następujące dane:

a) zakres rzeczowy dla całej zaprojektowanej sieci;
b) zbiorcze zestawienie długości kanalizacji dla całej sieci;
c) zbiorcze zestawienie studni;
d) zestawienie kabli światłowodowych;
e) zbiorcze zestawienie projektowanych złączy i skrzynek zapasu kabla światłowodowego;
f) zbiorcze zestawienie zakończeń kablowych;
g) zbiorcze zestawienie ważniejszych materiałów użytych do budowy sieci;
h) zbiorcze zestawienie przedmiarów z podziałem na elementy:

- budowa sieci magistralnej dla wszystkich obszarów łącznie (rozbiórka i naprawa nawierzchni, budowa kanalizacji i mikrokanalizacji, budowa i montaż sieci światłowodowej itp.),
- budowa sieci dystrybucyjnej dla wszystkich obszarów łącznie (rozbiórka i naprawa nawierzchni, budowa kanalizacji, budowa i montaż sieci, itp.),
- budowa sieci dostępowej dla wszystkich obszarów łącznie (rozbiórka i naprawa nawierzchni, budowa rurociągu, budowa i montaż sieci dostępowej itp.)
- budowa sieci wewnątrzbudynkowych dla wszystkich obszarów łącznie (budowa pionów, budowa i montaż sieci wewnątrzbudynkowych itp.).

2.4.2.6 Wymagania dla dokumentacji powykonawczej

Dokumentacja powykonawcza wybudowanej linii optotelekomunikacyjnej powinna zawierać wszystkie składniki określone prawem budowlanym. Dokumentacja dostarczana jest Zamawiającemu po zakończeniu budowy linii przez firmy wykonawcze oraz przez firmy geodezyjne dokonujące inwentaryzacji wybudowanych rurociągów kablowych.

Część trasową dokumentacji powykonawczej stanowi odrębna dokumentacja powykonawcza niezależna od poprawionej dokumentacji projektowej wykonywana na bieżąco, w miarę postępu budowy linii, przez uprawnionego geodetę pod nadzorem wykonawcy i inspektora nadzoru inwestorskiego. Fakt ten powinien znaleźć odzwierciedlenie w postaci odpowiedniego zapisu w dzienniku budowy.

Załącznikami do dokumentacji powykonawczej powinny być:

- protokoły przekazania użytkownikom terenu czasowo zajętego dla potrzeb budowy linii oraz odpowiednie protokoły stwierdzające prawidłowość wykonania zbliżeń i skrzyżowań linii z innymi obiektami uzbrojenia terenowego;
- schemat wyprostowany linii, uwzględniający złącza, zapasy, przebieg w kanalizacji z podaniem odległości pomiędzy tymi elementami;
- schemat rozpływu włókien;
- geodezyjna dokumentacja powykonawcza;
- protokoły zawierające wyniki pomiarów.

Na komplet dokumentacji składają się mapy i wersja elektroniczna na płycie CD-R (DVD-R). Wszystkie dostarczane Zamawiającemu pliki należy zapisać na płycie CD–R lub DVD-R w postaci naturalnej, tj. nie w archiwach skompresowanych.

Wykonawca budujący sieć światłowodową zobowiązany jest dostarczyć:

a) projekt z naniesionymi wszystkimi zmianami, które miały miejsce podczas budowy, potwierdzony przez projektanta, inspektora nadzoru i kierownika budowy,
b) przekroje poprzeczne przejść przez przeszkody terenowe (drogi, cieki wodne, linie kolejowe itp.)
c) wyniki pomiarów kabli światłowodowych;
d) schemat rozwinięty kanalizacji, wraz ze schematem wyprostowanym kabli światłowodowych;
e) schemat rozpływu włókien z naniesionymi zmianami

Geodeta inwentaryzujący sieć światłowodową zobowiązany jest dostarczyć:

a) 2 egzemplarze potwierdzonych przez Ośrodek Dokumentacji Geodezyjnej i Kartograficznej kopii map zasadniczych z naniesioną i wyróżnioną kolorem trasą zinwentaryzowanych urządzeń;
b) komplet kserokopii szkiców polowych z inwentaryzacji;
c) przebieg ogólny (orientacja) sieci telekomunikacyjnej w skali umożliwiającej naniesienie rysunku na formacie nie większym niż A-3;
d) przebieg szczegółowy sieci wykonany na dodatkowym, trzecim komplecie kopii map zasadniczych z naniesionymi informacjami dodatkowymi (domiary trasowe do charakterystycznych punktów kanalizacji kablowej, kabli ziemnych, rurociągów kablowych, obiektów ochronnych) itp.
e) skany map zasadniczych z naniesioną i wyróżnioną kolorem trasą zinwentaryzowanych urządzeń;
f) zestaw współrzędnych zinwentaryzowanych urządzeń
g) komplet odbitek map (mogą być bez potwierdzenia Ośrodka) z dodatkowymi informacjami dotyczącymi przebiegu sieci telekomunikacyjnej.

Po uzgodnieniu z Zamawiającym zalecane jest wykorzystywanie map numerycznych w formacie zaakceptowanym przez Zamawiającego w miejsce

poszczególnych map i odbitek map zasadniczych. Poszczególne przebiegi i urządzenia powinny znaleźć się w różnych warstwach mapy numerycznej.

Przy sporządzaniu dokumentacji powykonawczej sieci telekomunikacyjnej należy stosować symbole i oznaczenia identyczne jak w projektach budowlanym i wykonawczym.

Projekt i budowa rurociągu kablowego

Projekt i ułożenie światłowodu w rurociągu powinny być wykonane zgodnie z ogólnymi warunkami do projektowania i budowy kanalizacji teletechnicznej na potrzeby Powiatowej Sieci Szerokopasmowej.

1) Projektując kanalizację należy przede wszystkim zwracać uwagę na:

   a) Studnie kablowe powinny spełniać następujące wymagania określone normą ZN-96/TPSA-023. Studnie wykorzystane do budowy kanalizacji teletechnicznej na potrzeby sieci światłowodowej powinny mieć wymiary nie mniejsze niż studnie typu SKR-1 lud z tworzywa HDPE.
   b) Studnie mogą posiadać zabezpieczenie przed ingerencją osób nieuprawnionych w postaci zamka z układem zasuwowo-ryglowym zaś pokrywy powinny mieć wywietrznik z czytelnym logo sieci
   c) Prostoliniowość przebiegu kanalizacji**.** Kanalizacja kablowa powinna na odcinkach między sąsiednimi studniami kanalizacji deszczowej przebiegać prostoliniowo. W uzasadnionych technicznie wypadkach, rury kanalizacji mogą odchylać się od przebiegu prostoliniowego. Przebieg ten powinien być na tyle prostoliniowy, aby możliwe było przeciągnięcie przez nią kalibru wykonanego z materiału nieulegającego odkształceniu o długości 1 m i średnicy równej połowie średnicy wewnętrznej rury, o krawędziach zaokrąglonych (promień zaokrąglenia 5 mm).
   d) Przyłącza do obiektów kubaturowych. Jako studnie przyobiektowe dla Punktów Dostępowych i Dystrybucyjnych Szerokopasmowej Sieci Światłowodowej należy stosować studnie typu SKR-1 lub z tworzywa HDPE. Dla Punktów Węzłowych jako studnie przyobiektowe/stacyjne można zastosować studnie magistralne typu SKMXX-3.

Ze studni przyobiektowej należy wykonać przepusty rurowe do właściwego budynku. Przebieg trasowy w budynku zaczyna się od przekroczenia ściany zewnętrznej, które należy wykonać rurą typu HDPE

Należy bezwzględnie zastosować rurę przepustową ze względu na konieczność zastosowania w przyszłości odpowiednich uszczelek mechanicznych do rur z kablami np.: Jackmoon.

Badania linii optotelekomunikacyjnych oddawanych do eksploatacji

Do każdej wybudowanej linii optotelekomunikacyjnej powinna być sporządzona dokumentacja powykonawcza zgodna ze stanem rzeczywistym wykonania, uwzględniająca zmiany przeprowadzone w czasie budowy w stosunku do dokumentacji projektowej. Powinna być ona uzupełniona wynikami badań parametrów technicznych.

Wykaz badań przy odbiorze linii optotelekomunikacyjnej

Sprawdzenie wykonania linii optotelekomunikacyjnej

Wybudowana linia optotelekomunikacyjna powinna być sprawdzona pod kątem zgodności z powykonawczą dokumentacją projektu optycznego i trasowego. W czasie budowy powinny być przestrzegane zasady budowy linii optotelekomunikacyjnych zawarte w ZN 93ITPSA-O01, ZN 93ITPSA-O02. Sprawdzenie zasad budowy i realizacji wykonania polega na sprawdzeniu zgodnie z przedstawionymi poniżej punktami.

- Oględziny.
- Sprawdzenie materiałów stosowanych do budowy.
- Sprawdzenie rodzaju zastosowanych kabli.
- Sprawdzenie dokumentów homologacji,
- Sprawdzenie zasad wyboru trasy linii.
- Sprawdzenie przebiegu linii w terenie i obiektach.
- Sprawdzenie usytuowania linii.
- Sprawdzenie prawidłowości realizacji przejść rokadowych.
- Sprawdzenie poprawności oznakowania linii.
- Sprawdzenie poprawności wprowadzenia kabli do budynków.
- Sprawdzenie poprawności prowadzenia kabli na przejściach przez rzeki.

- Sprawdzenie poprawności prowadzenia kabli na terenach szkód górniczych.
- Sprawdzenie poprawności prowadzenia kabli w przejściach obiektowych.
- Sprawdzenie kierunków linii i numeracji linii.
- Sprawdzenie sposobu ułożenia kabla w kanalizacji.
- Sprawdzenie prawidłowości montażu kabli nadziemnych.
- Sprawdzenie prawidłowości montażu kabli stacyjnych.
- Sprawdzenie poprawności wykonania skrzyżowań i zbliżeń.
- Sprawdzenie poprawności doboru i instalacji rur polietylenowych kanalizacji wtórnej.
- Sprawdzenie poprawności doboru zasobników złączowych oraz sposobu zamocowania mufy kablowej i zapasów kabla w zasobniku.
- Sprawdzenie poprawności doboru i montażu muf kablowych.
- Sprawdzenie długości zapasów kabla w zasobniku złączowym.
- Sprawdzenie poprawności montażu przełącznic światłowodowych.
- Sprawdzenie poprawności połączeń światłowodów oraz ułożenia zapasów światłowodów w mufach i przełącznicy.
- Sprawdzenie zgodności z projektem połączeń włókien optycznych kabli liniowych, stacyjnych i złączy optycznych w przełącznicy,
- Sprawdzenie poprawności oznaczeń ostrzegających przy złączach światłowodowych urządzeń nadawczych z laserem półprzewodnikowym,

Wykaz badań optycznych

Na zbudowanej linii optotelekomunikacyjnej przed oddaniem do eksploatacji należy przeprowadzić zestaw pomiarów zgodnie z punktem 2.1.8.

Opis badań przy odbiorze linii optotelekomunikacyjnej

Linia optotelekomunikacyjna powinna być budowana zgodnie z zasadami budowy, opisanymi w ZN 96/TPSA-001, ZN 96/TPSA-002. Należy kontrolować zarówno stosowane materiały, przeprowadzanie pomiarów kontrolnych odcinków kabla wciąganych do kanalizacji, itp. Szczególną uwagę należy zwrócić na sytuacje opisane poniżej.

- **oględziny**

Należy sprawdzić, czy wybudowana linia i jej elementy składowe odpowiadają tym wymaganiom, które mogą być sprawdzone bez użycia specjalnych narzędzi czy przyrządów pomiarowych i bez demontażu. Dopuszcza się wykonanie wykopów kontrolnych. Przy oględzinach należy:

1. dokonać starannego przeglądu jakości wykonania elementów konstrukcyjnych, jakości montażu konstrukcji, mocowania, itd.
2. sprawdzić zabezpieczenia przed samo odkręceniem połączeń gwintowanych, zabezpieczenie przed korozją elementów z powłokami galwanicznymi i malarskimi,
3. sprawdzić ułożenie kabli w kanalizacji, na mostach, wiaduktach, w tunelach,
4. sprawdzić wykonanie odbudowy nawierzchni i uporządkowania terenu,
5. sprawdzić czytelność napisów i oznaczeń oraz ich estetykę,
6. sprawdzić zgodność wykonania i zgodność zastosowanych materiałów i elementów składowych z powykonawczą dokumentacją techniczną.

- **sprawdzenie materiałów stosowanych do budowy**

Optotelekomunikacyjna linia kablowa powinna być wykonana z kabli o właściwościach zgodnych z projektem technicznym. Rury polietylenowe do budowy kanalizacji wtórnej, mufy kablowe, przełącznice światłowodowe, szafki kablowe i stosowany osprzęt powinny posiadać świadectwa homologacji. Na całej długości linii optotelekomunikacyjnej rury polietylenowe kanalizacji wtórnej powinny posiadać ten sam kolor lub powinny być identycznie kolorowane. Wprowadzenie do budynku powinno być wykonane kablem niepalnym lub kablem palnym w rurach osłonowych bezhalogenowych.

- **sprawdzenie poprawności doboru i montażu muf kablowych**

Mufy dla kabli światłowodowych powinny być uszczelniane opaskami termokurczliwymi z klejem termotopliwym. Poszczególne połączone włókna światłowodowe powinny być starannie ułożone i umocowane, przy czym promień gięcia włókien powinien być większy niż 55 mm.

- **sprawdzenie poprawności wykonania skrzyżowań i zbliżeń**

Skrzyżowanie kabla z gazociągiem powinno być wykonane z zachowaniem odległości w płaszczyźnie pionowej co najmniej 0,15 m od zewnętrznej ścianki

gazociągu. Kabel powinien być zabezpieczony rurą z tworzywa sztucznego na długości co najmniej 1,5 m od osi skrzyżowania.

- **sprawdzenie lokalizacji trasy przebiegu kabla**

Zastosowana technologia budowy linii powinna umożliwiać lokalizację trasy kabla, a wykonawca powinien podać sposób lokalizacji trasy z dokładnością nie gorszą niż 20cm w stosunku do osi kabla.

- **sprawdzenie zgodności numeracji włókien optycznych kabli liniowych, stacyjnych i złączy optycznych w przełącznicy**

Awaria kabla światłowodowego może polegać na uszkodzeniu (przecięciu) całego kabla lub tylko pojedynczego włókna optycznego. Jeśli uszkodzeniu ulegnie tylko jedno włókno optyczne, to możliwa jest naprawa bez przerywania transmisji na pozostałych światłowodach. W tym przypadku bardzo istotne jest zachowanie zgodności połączeń kolejnych włókien optycznych ze schematem optycznym linii, aby w czasie usuwania awarii nie zaszło omyłkowe przerwanie pracującego toru lub nie wystąpiło porażenie światłem pracującego lasera. Stąd należy zwracać szczególną uwagę na zgodność realizacji połączenia z projektem. W przypadku przypuszczenia występującej pomyłki, np. gdy numer włókna nie zgadza się z numerem złącza w przełącznicy, należy sprawdzić zgodność połączeń ze schematem optycznym. Sprawdzenie zgodności polega na wizualnym obejrzeniu wszystkich połączeń w mufie lub przeprowadzeniu pomiaru.

- **pomiar zgodności połączeń**

Do złącza badanego toru w przełącznicy światłowodowej należy podłączyć reflektometr lub do złączy w przeciwległych przełącznicach podłączyć zestaw do pomiaru tłumienności metodą transmisyjną. Korzystając ze schematu optycznego należy odczytać numery światłowodów, które powinny być połączone z badanym złączem w określonej mufie. Następnie należy otworzyć badaną mufę kablową i nawinąć około 10 zwojów światłowodu na cylinder o średnicy 25 mm i obserwować efekt zmiany tłumienności badanego toru. Jeżeli po nawinięciu nie wystąpi efekt zmiany tłumienności (odczytywany na końcu linii), to wtedy jest brak zgodności połączeń. Jeśli jest brak zgodności połączeń,

to wtedy należy sprawdzić wszystkie połączenia w mufie kablowej, a jeśli trzeba to na całym odcinku linii.

2.4.3 Warunki wykonania i odbioru – Łącza radioliniowe

Wykonawca zobowiązany jest do opracowania dokumentacji projektowej (budowlanej i wykonawczej) zgodnie z obowiązującym na dzień jej wykonania Prawem budowlanym oraz zasadami wiedzy technicznej.

Do zadań Wykonawcy należy w szczególności:

- uzyskanie niezbędnych uzgodnień branżowych, opinii, ekspertyz itp.
- opracowanie projektów budowlanych wraz z uzyskaniem pozwolenia na budowę
- opracowanie projektów wykonawczych
- opracowanie kosztorysów inwestorskich
- opracowanie przedmiarów robót
- opracowanie specyfikacje technicznych wykonania i odbioru robót budowlanych

Szczegółowe uzgodnienia w sprawie umieszczenia urządzeń i infrastruktury łączy radioliniowych w budynkach należy przeprowadzić bezpośrednio z administratorami poszczególnych obiektów oraz z przedstawicielem Zamawiającego.

Dokumentacje projektowe należy przekazać w następującej ilości:

- projekt budowlany……..... 4 egz.
- projekt wykonawczy……..... 5 egz.
- przedmiar robót……..... 5 egz.
- kosztorys inwestorski…….. 2 egz.
- specyfikacja techniczna wykonania i odbioru robót budowlanych..... 5 egz.
- wersja elektroniczna wszystkich dokumentacji (pliki .pdf/.doc i .dwg)…. 2 szt.

Dokumentacja projektowa powinna zostać wykonana zgodnie z Rozporządzeniem Ministra Infrastruktury z dn. 2 września 2004 r. 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. zmianami.

Kosztorys inwestorski powinien być opracowany zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 18 maja 2004 r. w sprawie określania metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac

projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz. U. Nr 130 poz. 1389 z 2004 r.).

Przedmiary robót powinny zawierać dane wyszczególnione w Rozporządzeniu Ministra Infrastruktury z dn. 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego.

Specyfikacje techniczne wykonania i odbioru robót budowlanych powinny zawierać wszystkie dane wyszczególnione w Rozporządzeniu Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego.

Wytyczne instalacyjne:

- Wymiary szafy teletechnicznej powinny być tak dobrane, aby zapewnić swobodny przepływ powietrza, określony w dokumentacji instalacyjnej urządzeń. Rekomendowany standard – wymiary szafy: 42U, 800 x 600 mm
- Szafa powinna zapewniać swobodny dostęp do urządzeń od frontu i od tyłu
- Szafa powinna zapewniać swobodne ułożenie okablowania zasilającego oraz transmisyjnego
- Szafa powinna być wyposażona w otwory górne i dolne do wprowadzania okablowania
- Szafa oraz jej części składowe powinny być uziemione
- Wszystkie urządzenia instalowane w szafie powinny być niezależnie uziemione
- Okablowanie powinno być prowadzone pod podłogą techniczną, lub w przypadku jej braku, w drabinkach i/lub korytach kablowych
- W przypadku stosowania zasilania redundantnego obwody zasilające powinny być podłączone do osobnych zabezpieczeń
- Okablowanie transmisyjne powinno być zwinięte w szafie w pętli oraz zamocowane w sposób uniemożliwiający jego przypadkowe uszkodzenie
- Wszystkie kable, zarówno zasilające, jak i transmisyjne powinny być w szafie opisane w sposób umożliwiający bezbłędną identyfikację

- Szafy powinny być opisane w celu identyfikacji
- W przypadku konieczności instalacji urządzeń montowanych od frontu, których głębokość i masa jest znaczna należy również przewidzieć ewentualną instalację półek podtrzymujących urządzenia
- Szafa powinna zostać wyposażona w listwy zasilające 230V, z gniazdami w ilości zapewniającej dalszą ewentualną instalację urządzeń dodatkowych, opisane w sposób, który wskazuje na podłączenie ich do osobnych obwodów zasilających (redundancja).

Węzeł radioliniowy

Wyposażenie węzła radioliniowego powinno składać się z:

- maszt (wysokość w zależności od wymagań)
- moduł zewnętrzny ODU
- szafy telekomunikacyjnej,
- systemu zasilania gwarantowanego w okresie 3 godzin
- układu zabezpieczeń odbiorów,
- przełącznika dystrybucyjnego
- urządzenia wewnętrznego IDU,
- System sygnalizacji włamania i napadu
- System czujników alarmu pożarowego
- System klimatyzacji i wentylacji pomieszczeń (jeżeli niezbędny) zapewniający odpowiednie warunki klimatyczne pracy zainstalowanych urządzeń

Urządzenia i instalacje zewnętrzne

W przypadku instalacji urządzeń zewnętrznych, w zależności od warunków możemy wyróżnić trzy typy instalacji:

1. **Instalacja anten i ODU na istniejących masztach.**

Najprostszy typ wymagający tylko projektu technologicznego radiowego.

2. **Instalacja anten i ODU na nowych masztach do 3m**.

Podejście wymagające projektu konstrukcji (bez uzyskiwania pozwolenia na budowę) oraz projektu technologicznego radiowego (podstawa prawna Prawo Budowlane, art. 30, ust. 1 pkt 3 lit. b).

3. **Instalacja anten i ODU na masztach powyżej 3m.**

Najdłuższy w realizacji typ instalacji wymagający całej ścieżki uzyskania pozwolenia na budowę oraz projektu technologicznego radiowego. Czas realizacji tego typu instalacji może trwać rok i dłużej.

Na urządzenia i instalacje zewnętrzne składają się:

- maszty,
- instalacja uziemiająca,
- urządzenia radioliniowe,
    - część ODU, anteny
    - urządzenia wewnętrzne IDU,
    - okablowanie.

Specyfikacja dla konstrukcji masztowej i instalacji uziemiającej jest uzależniona od wyboru producenta sprzętu urządzeń radioliniowych ponieważ wymiary, waga oraz połączenia pomiędzy urządzeniami są specyficzne dla każdego producenta. Dlatego najlepiej dopiero po wyborze sprzętu wykonywać specyfikację do projektu technologicznego radiowego oraz konstrukcyjnego. Każdy producent sprzętu dostarcza specyfikację techniczną w której dokładnie określone są wszystkie potrzebne parametry i zalecenia instalacyjne.

Urządzenia i instalacje wewnętrzne

Na urządzenia i instalacje wewnętrzne składają się:

- szafa telekomunikacyjna,
- urządzenia wewnętrzne IDU,
- okablowanie,

Połączenie urządzeń zewnętrznych (ODU) z wewnętrznymi (IDU).

W zależności od producenta urządzeń radioliniowych, pomiędzy urządzeniami zewnętrznymi (ODU) a wewnętrznymi (IDU) komunikacja oraz zasilanie odbywa się poprzez kabel sieciowy z zasilaniem PoE

W projekcie trzeba ująć drogę kablową pomiędzy ODU a IDU. Będzie ona wynikała z miejsc montażu masztów oraz miejsca instalacji szafy z urządzeniami.

System Zarządzania

System Zarządzania urządzeniami radioliniowymi powinien zostać zainstalowany w głównej siedzibie Zamawiającego, skąd zapewniona będzie łączność ze wszystkimi komponentami systemu.

2.4.4 Warunki wykonania i odbioru – Urządzenia aktywne sieci

2.4.4.1 Dokumentacja projektowa i wykonawcza

Wykonawca zobowiązany jest do opracowania dokumentacji projektowej (wykonawczej) zgodnie z obowiązującym na dzień jej wykonania Prawem budowlanym oraz zasadami wiedzy technicznej.

Do zadań Wykonawcy należy w szczególności:

- uzyskanie niezbędnych uzgodnień branżowych, opinii, ekspertyz itp.
- opracowanie projektów wykonawczych
- opracowanie kosztorysów inwestorskich

Dokumentacje projektowe należy przekazać w następującej ilości:

- projekt wykonawczy…….. 5 egz.
- kosztorys inwestorski……. 2 egz.
- wersja elektroniczna wszystkich dokumentacji (pliki .pdf/.doc i .dwg) 2 szt.

Dokumentacja projektowa powinna zostać wykonana zgodnie z Rozporządzeniem Ministra Infrastruktury z dn. 2 września 2004 r. 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. zmianami.

Kosztorys inwestorski powinien być opracowany zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 18 maja 2004 r. w sprawie określania metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz. U. Nr 130 poz. 1389 z 2004 r.).

Specyfikacje techniczne wykonania i odbioru robót budowlanych powinny zawierać wszystkie dane wyszczególnione w Rozporządzeniu Ministra Infrastruktury z dnia 2 września 2004 r. w sprawie szczegółowego zakresu i formy dokumentacji

projektowej, specyfikacji technicznych wykonania i odbioru robót budowlanych oraz programu funkcjonalno-użytkowego.

2.4.4.2 Wytyczne i wymagania instalacyjne

2.4.4.2.1 Główny Węzeł Szkieletowy

Ogółem przewidziano jeden Główny Węzeł Szkieletowy będzie wyposażony w następujące komponenty:

- Główny przełącznik szkieletowy (1 szt.)
- Centralny Firewall z zaawansowanym systemem ochrony sieci – UTM
- System podtrzymania zasilania – UPS (3 godziny)
- Szafa Teletechniczna 19” 42U

Wytyczne instalacyjne:

- Wymiary szafy teletechnicznej powinny być tak dobrane, aby zapewnić swobodny przepływ powietrza, określony w dokumentacji instalacyjnej urządzeń. Rekomendowany standard – wymiary szafy: 42U, 800 x 100 mm
- Szafa powinna zapewniać swobodny dostęp do urządzeń od frontu i od tyłu
- Szafa powinna zapewniać swobodne ułożenie okablowania zasilającego oraz transmisyjnego
- Szafa powinna być wyposażona w otwory górne i dolne do wprowadzania okablowania
- Szafa oraz jej części składowe powinny być uziemione
- Wszystkie kable, zarówno zasilające, jak i transmisyjne, powinny być zabezpieczone rurą typu „peszel” o średnicy dobranej do stosowanego okablowania. Wyjątek stanowi okablowanie uziemiające
- Wszystkie urządzenia instalowane w szafie powinny być niezależnie uziemione
- Okablowanie powinno być prowadzone pod podłogą techniczną, lub w przypadku jej braku, w drabinkach i/lub korytach kablowych
- W przypadku stosowania zasilania redundantnego obwody zasilające powinny być podłączone do osobnych zabezpieczeń

- Sugeruję się doprowadzenie kabla światłowodowego od przełącznicy światłowodowej do szafy teletechnicznej i zakończenie go na patchpanelu
- Okablowanie transmisyjne do połączeń urządzeń aktywnych z punktem dystrybucyjnym powinno mieć nadmiarową długość określoną jako podwójna wysokość szafy, co umożliwi ewentualną zmianę konfiguracji instalacyjnej urządzeń w szafie
- Okablowanie transmisyjne powinno być zwinięte w szafie w pętli oraz zamocowane w sposób uniemożliwiający jego przypadkowe uszkodzenie
- Szafa powinna zostać oznaczona znakami ostrzegawczymi informującymi o pracy urządzeń laserowych
- Szafa powinna być wyposażona w urządzenie typu KVF, umożliwiający lokalną pracę na serwerze administratorom systemu
- Wszystkie kable, zarówno zasilające, jak i transmisyjne powinny być w szafie opisane w sposób umożliwiający bezbłędną identyfikację
- Szafy powinny być opisane w celu identyfikacji
- W przypadku konieczności instalacji urządzeń montowanych od frontu, których głębokość i masa jest znaczna należy również przewidzieć ewentualną instalację półek podtrzymujących urządzenia
- Szafa powinna zostać wyposażona w listwy zasilające 230V, z gniazdami w ilości zapewniającej dalszą ewentualną instalację urządzeń dodatkowych, opisane w sposób, który wskazuje na podłączenie ich do osobnych obwodów zasilających (redundancja).

2.4.4.2.2 Węzeł szkieletowy

W Węzłach Szkieletowych będą instalowane:

- Przełączniki Szkieletowe
- Zasilacz awaryjny UPS gwarantujący podtrzymanie zasilani na czas 3 godzin

Wymagane wyposażenie punktów dostępowych:

- Przełącznice światłowodowe panelowe o ilości wymaganej ilością połączeń

- Szafa dwudzielna min. 9U 500mm głębokości dla paneli kablowych i urządzeń (rozmiar szafy powinien być zweryfikowany na etapie projektu wykonawczego) wyposażona w:
    - Patchpanele do krosowania połączeń pomiędzy urządzeniami
    - Organizatory kabli instalowanych wewnątrz szafy
    - Listwy zasilające o ilości gniazd o 100% przekraczającej ilość wymaganą przez urządzenia
- Szafa powinna być zabezpieczona przed nieuprawnionym dostępem.
- Podstawowa adaptacja budowlana punktu dostępowego (matowanie, szpachlowanie, itp).

Założenia:

- Urządzenia transmisyjne będą zarządzane z odpowiedniego stanowiska zarządzającego sieci.
- Sugeruje się doprowadzenie okablowania strukturalnego do szafy i rozszycie go na patchpanelach.
- Szafa powinna być wyposażona w prowadnice kabli.

2.4.4.2.3 Punkty Dostępowe

W Punktach Dostępowych będą instalowane:

- Bramy Usługowe z Punktem Dostępowym WiFi

W uzasadnionych topologią sieci światłowodowej lub radiowej przypadkach w Punktach Dostępowych będzie instalowany:

- Przełącznik Tranzytowy

Wymagane wyposażenie punktów dostępowych:

- Przełącznice światłowodowe panelowe o ilości wymaganej ilością połączeń
- Szafa dwudzielna min. 9U 500mm głębokości dla paneli kablowych i urządzeń (rozmiar szafy powinien być zweryfikowany na etapie projektu wykonawczego) wyposażona w:

  - Patchpanele do krosowania połączeń pomiędzy urządzeniami
  - Organizatory kabli instalowanych wewnątrz szafy
  - Listwy zasilające o ilości gniazd o 100% przekraczającej ilość wymaganą przez urządzenia
- Szafa powinna być zabezpieczona przed nieuprawnionym dostępem.
- Podstawowa adaptacja budowlana punktu dostępowego (matowanie, szpachlowanie, itp).

Założenia:

- Urządzenia transmisyjne będą zarządzane z odpowiedniego stanowiska zarządzającego sieci.
- Sugeruje się doprowadzenie okablowania strukturalnego do szafy i rozszycie go na patchpanelach.
- Szafa powinna być wyposażona w prowadnice kabli.

2.4.4.2.4 Centrum Zarządzania i Bezpieczeństwa Sieci

Centrum Zarządzania i Bezpieczeństwa Sieci będzie wyposażone w następujące urządzenia:

- System Monitoringu i Zarządzania Siecią
- Centralny System Zarządzania Bezpieczeństwa sieci
- System Kontroli Dostępu do Sieci
- System Autoryzacji, Autentykacji i Weryfikacji
- System podtrzymania zasilania UPS – 3 godziny
- Stanowiska administratorów
- Przełącznik lokalnej sieci NOC
- Szafa teletechniczna serwerowa 19” 42U
  - Patchpanele do krosowania połączeń pomiędzy urządzeniami
  - Organizatory kabli instalowanych wewnątrz szafy
  - Panele wentylacji
  - Listwy zasilające o ilości gniazd o 100% przekraczającej ilość wymaganą przez urządzenia

Wytyczne instalacyjne:

- Szafa teletechniczna umożliwiająca instalację wszystkich opisanych powyżej urządzeń powinna być dostarczona wraz z urządzeniami.
- Wymiary szafy teletechnicznej powinny być tak dobrane, aby zapewnić swobodny przepływ powietrza, określony w dokumentacji instalacyjnej urządzeń. Rekomendowany standard – wymiary szafy: 42U, 800 x 100 mm
- Szafa powinna zapewniać swobodny dostęp do urządzeń od frontu i od tyłu
- Szafa powinna zapewniać swobodne ułożenie okablowania zasilającego oraz transmisyjnego
- Szafa powinna być wyposażona w otwory górne i dolne do wprowadzania okablowania
- Szafa oraz jej części składowe powinny być uziemione
- Wszystkie kable, zarówno zasilające, jak i transmisyjne, powinny być zabezpieczone rurą typu „peszel” o średnicy dobranej do stosowanego okablowania. Wyjątek stanowi okablowanie uziemiające
- Wszystkie urządzenia instalowane w szafie powinny być niezależnie uziemione
- Okablowanie powinno być prowadzone pod podłogą techniczną, lub w przypadku jej braku, w drabinkach i/lub korytach kablowych
- W przypadku stosowania zasilania redundantnego obwody zasilające powinny być podłączone do osobnych zabezpieczeń
- Sugeruję się doprowadzenie kabla światłowodowego od przełącznicy światłowodowej do szafy teletechnicznej i zakończenie go na patchpanelu
- Okablowanie światłowodowe do połączeń urządzeń aktywnych z punktem dystrybucyjnym powinno mieć nadmiarową długość określoną jako podwójna wysokość szafy, co umożliwi ewentualną zmianę konfiguracji instalacyjnej urządzeń w szafie
- Okablowanie światłowodowe powinno być zwinięte w szafie w pętli oraz zamocowane w sposób uniemożliwiający jego przypadkowe uszkodzenie
- Szafa powinna zostać oznaczona znakami ostrzegawczymi informującymi o pracy urządzeń laserowych
- Wszystkie kable, zarówno zasilające, jak i transmisyjne powinny być w szafie opisane w sposób umożliwiający bezbłędną identyfikację

- Szafy powinny być opisane w celu identyfikacji
- W przypadku konieczności instalacji urządzeń montowanych od frontu, których głębokość i masa jest znaczna należy również przewidzieć ewentualną instalację półek podtrzymujących urządzenia
- Szafa powinna zostać wyposażona w listwy zasilające 230V, z gniazdami w ilości zapewniającej dalszą ewentualną instalację urządzeń dodatkowych, opisane w sposób, który wskazuje na podłączenie ich do osobnych obwodów zasilających (redundancja).

2.4.4.2.5 Urządzenia szkieletu sieci i przełączniki tranzytowe

- Urządzenia powinny zostać zamontowane w szafach teletechnicznych w sposób opisany w ich dokumentacji instalacyjnej, ze szczególnym zwróceniem uwagi na swobodny dostęp do tych urządzeń z przodu i/lub z tyłu oraz na swobodny przepływ powietrza.
- Urządzenia szkieletowe powinny być oznaczone w sposób jednoznaczny, umożliwiający ich bezbłędną identyfikację.
- Urządzenia szkieletowe powinny być skonfigurowane dla połączeń do odpowiadających im urządzeń sieci a w szczególności do Systemu Zarządzania i Monitorowania Sieci

Urządzenia powinny mieć zapewniony zdalny bezpieczny dostęp do celów konfiguracji, administracji, serwisu

2.4.4.2.6 Brama usługowa z punktem dostępowym HotSpot WiFi

- Urządzenia dostępowe powinny zostać zamontowane w szafach teletechnicznych w sposób opisany w ich dokumentacji instalacyjnej, ze szczególnym zwróceniem uwagi na swobodny dostęp do tych urządzeń z przodu i/lub z tyłu oraz na swobodny przepływ powietrza.
- Urządzenia dostępowe powinny być oznaczone w sposób jednoznaczny, umożliwiający ich bezbłędną identyfikację.
- Skonfigurowane dla zarządzania za pomocą Aplikacji Zarządzania i Monitorowania Sieci

2.4.4.2.7 Aplikacja zarządzania i Monitorowania Sieci

Aplikacja powinna mieć łączność z urządzeniami :

- Główny Przełącznik Szkieletowy
- Przełączniki Szkieletowe
- Centralny Firewall
- Centralny System Zarządzania Bezpieczeństwem Sieci
- System Kontroli Dostępu do Sieci
- Brama Usługowa z Punktami Dostępowymi

2.4.4.2.8 Aplikacja Serwera Weryfikacji i Autentykacji

Konfiguracja Aplikacji powinna być określona na etapie projektu wykonawczego.

2.4.4.2.9 System Kontroli Dostępu do Sieci

System Kontroli Dostępu do Sieci powinien być zainstalowany na zasadach podobnych jak urządzenia szkieletu sieci.

Opracowanie i implementacja polityk dostępu do sieci powinno być przedmiotem Projektu Wykonawczego.

2.4.4.2.10 Centralny System Zarządzania Bezpieczeństwem Sieci

Zakres prac instalacyjnych dotyczących obu systemów obejmuje:

- Opracowanie uzgodnionej z Zamawiającym polityki bezpieczeństwa w oparciu o oferowane rozwiązanie
- Instalację urządzeń i odpowiedniego okablowania
- Wykonanie aktualizacji firmware’u urządzenia
- Konfiguracja interfejsów i routingu, oraz pozostałych elementów ustawień sieciowych
- Uruchomienie i zaktualizowanie subskrypcji dostępnych modułów, oraz wykonanie wszelkich aktualizacji
- Konfiguracja kont administratorów, oraz profili dostępu
- Utworzenie grup, oraz zakresów adresacji dla nich, a także nazw hostów istniejących w sieci i przypisanie im adresów

- Konfiguracja poszczególnych profili dla modułów AntiVirus, Intrusion Protection, Web Filter i AntySpam - zgodnie z opracowaną polityką i po zatwierdzeniu przez zamawiającego
- Konfiguracja profili bezpieczeństwa
- Stworzenie profili dla użytkowników i skonfigurowanie sposobu autentykacji - integracja z Active Directory
- Stworzenie polityk bezpieczeństwa
- Stworzenie tuneli VPN wraz z odpowiadającą mu polityką
- Weryfikacja działania polityk i "troubleshooting"
- Konfiguracja logowania i raportowania do urządzenia centralnego
- Konfiguracja zarządzania w urządzeniu centralnym
- Konsultacje w zakresie tuningu systemu
- Opracowanie dokumentacji powykonawczej
- Urządzenie powinno mieć zapewniony zdalny bezpieczny dostęp do celów konfiguracji, administracji, serwisu

2.4.4.3 Wsparcie techniczne i utrzymanie

Wykonawca sieci szerokopasmowej powinien oferować wsparcie w okresie 1 roku przy założeniu, że awaria krytyczna będzie usunięta w następnym dniu roboczym

Zakres wymaganego wsparcia technicznego producentów został opisany dla każdego komponentu oddzielnie w rozdziale 2.

Odpowiedzialność gwarancyjna Wykonawcy powinna zostać określona na etapie tworzenia SIWZ.

Wykonawca powinien zadbać o stworzenie zdalnego bezpiecznego łącza VPN za pomocą, którego możliwa będzie zdalna pomoc techniczna świadczona przez Wykonawcę lub producenta urządzeń.

Inwestor powinien zadbać o utrzymywanie w/w łącz VPN w ciągłej gotowości w okresie eksploatacji.

2.4.4.4 Szkolenia

Wymagane jest zapewnienie autoryzowanego szkolenia z zakresu utrzymania wszystkich urządzeń. Szkolenie powinno być przeprowadzone dla 5 osób w języku polskim w ośrodku szkolenia dostawcy lub producenta przez certyfikowanych inżynierów lub trenerów.

Ostateczna liczba szkolonych osób i zakres szkolenia będzie określona na etapie projektu wykonawczego.

II. CZĘŚĆ INFORMACYJNA PROGRAMU FUNKCJONALNO-UŻYTKOWEGO

1. DOKUMENTY POTWIERDZAJĄCE ZGODNOŚĆ ZAMIERZENIA BUDOWLANEGO Z WYMAGANIAMI WYNIKAJĄCYMI Z ODRĘBNYCH PRZEPISÓW

Budowa telekomunikacyjnych linii kablowych wymaga zgłoszenia budowy (art. 29 Prawa Budowlanego – Dz.U. 207, 2003r., poz. 2016 z późn. zmianami – tekst jednolity).

Dla budowy przyłączy do budynków i telekomunikacyjnych linii kablowych nie jest wymagane pozwolenie na budowę (art. 29 ust. 1 ppkt. 20 i 20a Prawa Budowlanego j.w.), dla budowy przyłączy nie wymagane jest też zgłoszenie w związku z art. 29a tego samego prawa.

Na obszarach objętych Miejscowymi Planami Zagospodarowania Przestrzennego nie są wymagane decyzje o warunkach zabudowy - art. 4 Ustawy o planowaniu i zagospodarowaniu przestrzennym (Dz.U. 80 poz. 717 z 10.05.2003 z późn. zmianami).

Dla prac w budynkach zabytkowych oraz na terenach objętych ochroną konserwatorską wymagane jest zezwolenie konserwatora – Wojewódzkiego Urzędu Ochrony Zabytków, jednakże dopiero na etapie opracowywania dokumentacji technicznej i pozwolenia na budowę/zgłoszenia (zezwolenie jest wymagane dla przeprowadzenia prac remontowych w pomieszczeniach). Na obecnym etapie takie pozwolenie nie jest wymagane.

Dla prac związanych z przekraczaniem cieków podstawowych wymagane jest uzyskanie pozwolenia wodno-prawnego od Starosty, jednakże dopiero na etapie opracowywania dokumentacji technicznej i pozwolenia na budowę/zgłoszenia. Na obecnym etapie takie pozwolenie nie jest wymagane.

Dla prac związanych z przekraczaniem torów kolejowych i terenów zamkniętych wymagane jest uzyskanie pozwolenia na budowę/zgłoszenia od Marszałka, a dla prac

związanych z układaniem rurociągów równolegle do torów w odległości mniejszej lub dopuszczona w ustawie „kolejowej” wymagane jest uzyskanie zgody na odstępstwo od zakazu układania infrastruktury podziemnej niezwiązanej z ruchem kolejowym w odległości mniejszej niż 10m od granicy pasa kolejowego lub 20m od toru, zawartego w tej ustawie od Starosty, jednakże dopiero na etapie opracowywania dokumentacji technicznej i pozwolenia na budowę/zgłoszenia. Na obecnym etapie takie pozwolenie lub odstępstwo nie są wymagane.

Dla prac na terenach pasa nadmorskiego wymagane jest uzyskanie pozwolenia od Urzędu Morskiego oraz (jeśli wymagane) odstępstwo od art. 82 ustawy Prawo Wodne od Marszałka Województwa, jednakże dopiero na etapie opracowywania dokumentacji technicznej i pozwolenia na budowę/zgłoszenia. Na obecnym etapie takie pozwolenie nie jest wymagane.

2. OŚWIADCZENIE ZAMAWIAJĄCEGO STWIERDZAJĄCE JEGO PRAWO DO DYSPONOWANIA NIERUCHOMOŚCIĄ NA CELE BUDOWLANE

Ze względu na to, że dokładne wytyczenie trasy nastąpi dopiero na etapie projektu budowlanego oświadczenia Zamawiającego potwierdzające jego prawo do dysponowania nieruchomościami na cele budowlane uzyska Wykonawca na etapie wykonywania projektu budowlanego.

3. PRZEPISY PRAWNE I NORMY ZWIĄZANE Z PROJEKTOWANIEM I WYKONANIEM ZAMIERZENIA BUDOWLANEGO

Wszystkie roboty należy wykonywać zgodnie z obowiązującymi normami i przepisami. Prace należy prowadzić zgodnie z obowiązującymi przepisami BHP i PPOŻ.

Wykonawca bezwzględnie winien stosować się do uwag zawartych w uzgodnieniach branżowych i innych.

Urządzenia, osprzęt oraz kable telekomunikacyjne zastosowane przy budowie winny mieć certyfikat ze znakiem B.

Podczas prac należy stosować się do norm zakładowych TP S.A.:

1. ZN-96/TPSA-002 Telekomunikacyjne linie kablowe dalekosiężne. Linie optotelekomunikacyjne. Ogólne wymagania techniczne,
2. ZN 96/TPSA-004 Zbliżenia i skrzyżowania z innymi urządzeniami uzbrojenia terenowego. Ogólne wymagania i badania,
3. ZN 96/TPSA-005. Kable optotelekomunikacyjne. Wymagania i badania,
4. ZN 96/TPSA-006. Złącza spajane światłowodów jednomodowych. Wymagania i badania,
5. ZN 96/TPSA-007. Złączki światłowodowe i kable stacyjne. Wymagania i badania,
6. ZN 96/TPSA-009. Przełącznice światłowodowe. Wymagania i badania,
7. ZN-96/TPSA-013. Kanalizacja wtórna i rurociągi kablowe. Wymagania i badania.
8. ZN-96/TPSA-014. Rury z polichlorku winylu (RPCW). Wymagania i badania.
9. ZN-96/TPSA-016. Rury polietylenowe karbowane dwuwarstwowe (RHDPEk). Wymagania i badania.
10. ZN-96/TPSA-017. Rury kanalizacji wtórnej i rurociągu kablowego (RHDPE). Wymagania i badania.
11. ZN-96/TPSA-018. Rury polietylenowe (RHDPEp) przepustowe. Wymagania i badania.
12. ZN-96/TPSA-020. Złączki rur kanalizacji kablowej. Wymagania i badania.
13. ZN-96/TPSA-021. Uszczelki końców rur kanalizacji kablowej. Wymagania i badania.
14. ZN-96/TPSA-022. Przywieszka identyfikacyjna. Wymagania i badania.
15. ZN-96/TPSA-023. Studnie kablowe. Wymagania i badania.
16. ZN-96/TPSA-041. Zabezpieczone pokrywy studni kablowych, dodatkowe (wewnętrzne). Wymagania i badania.
17. PN-91/M-34501 Gazociągi i instalacje gazownicze. Skrzyżowania gazociągów z przeszkodami terenowymi. Wymagania.
18. PN-76/E-05125 Elektroenergetyczne i sygnalizacyjne linie kablowe. Projektowanie i budowa.
19. PN-75/E-05100 Elektroenergetyczne linie napowietrzne. Projektowanie i budowa.

oraz norm, instrukcji i zaleceń w nich przywołanych.

Ustawy i Rozporządzenia

1. Zarządzenie Ministra Łączności Ministra dnia 28.02.1986 wprowadzające Wytyczne Ministra ochronie linii urządzeń telekomunikacyjnych przed szkodliwym oddziaływaniem linii energetycznych i trakcji elektrycznej prądu stałego;
2. Ustawa z dnia 23.12.1990 o łączności (dziennik Ustaw Nr 86 poz.504) z późniejszymi zmianami;
3. Zarządzenie Ministra Łączności z dnia 02.09.1997 w sprawie warunków, jakim powinny odpowiadać linie i urządzenia telekomunikacyjne, oraz urządzenia do przesyłania płynów i gazów razie zbliżenia się do skrzyżowania (Mon. Pol. Nr 59 poz. 567);
4. Zarządzenie Ministra Łączności z dnia 12.03.1992 w sprawie zasad i warunków budowy linii telekomunikacyjnych wzdłuż dróg publicznych, wodnych, kanałów, oraz w pobliżu lotnisk i w miejscowościach, a także ustalenia warunków, jakim te linie powinny odpowiadać (Mon. Pol. Nr 13 poz. 95);
5. Rozporządzenie Ministra Łączności z dnia 31.05.1993 w sprawie określenia systemów telekomunikacyjnych, zakładanych i używanych na terytorium Rzeczpospolitej Polskiej (Dz. Ustaw. Nr 63 poz. 302);
6. Rozporządzenie Ministra Łączności z dnia 16.06.1993 r w sprawie wymagań technicznych i eksploatacyjnych oraz warunków wzajemnej współpracy urządzeń, linii i sieci telekomunikacyjnych zakładanych i używanych na terytorium Rzeczpospolitej Polskiej (Dz. Ustaw. Nr 70 poz. 340);

    - Załącznik nr 2. Podstawowe wymagania techniczne i eksploatacyjne dla sieci telekomunikacyjnych.
    - Załącznik nr 11. Wymagania techniczne i eksploatacyjne dla kabli i linii światłowodowych.
    - Załącznik nr 13. Wymagania techniczne i eksploatacyjne dla światłowodowej przełącznicy kabli jednomodowych.

7. Rozporządzenie Ministra Łączności z dnia 16.03.1994 w sprawie wprowadzenia obowiązku stosowania Polskich Norm i norm branżowych z dziedziny łączności (Dz. U. Nr 40 poz. 151);

8. Ustawa z dnia 7.07.1994. Prawo budowlane (Dz. U. Nr 89 poz. 414) z późniejszymi zmianami;
9. Ustawa z dnia 12.05.1995. O zmianie ustawy o łączności, oraz niektórych innych ustaw (Dz. U. Nr 60 poz. 310);
10. Ustawa z dnia 27.04.2001 Prawo Ochrony Środowiska wraz z rozporządzeniami wykonawczymi
11. Ustawa z dnia 07.05.2010 o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. Nr 106 poz. 675)
12. Ustawa z dnia 16.07.2004 Prawo Telekomunikacyjne (Dz. U. Nr 171 poz. 1800)
13. Ustawa z dnia 03.10.2008 O udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz. U. Nr 199 poz. 1227)
14. Rozporządzenie Ministra Transportu z dnia 03.07.2007 w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego (Dz. U. Nr 24 poz. 195 i 196).

Normy Branżowe

1. BN-80/6775-03.00. Prefabrykaty budowlane z betonu. Elementy nawierzchni dróg, ulic, parkingów i torowisk tramwajowych. Wymagania i badania.
2. BN-80/6775-03.01. Prefabrykaty budowlane z betonu. Elementy nawierzchni dróg, ulic, parkingów i torowisk tramwajowych. Płyty betonowe.
3. BN-73/8984-08. Kanalizacja kablowa. Ogólne wymagania i badania.
2. BN-82/3233-25. Osprzęt linii telekomunikacyjnych. Kanalizacja kablowa. Tablica orientacyjna do oznaczania studni kablowych.
3. BN-85/8984-01. Telekomunikacyjne sieci miejscowe. Studnie kablowe. Klasyfikacja i normy.
4. BN-88/8984-19. Telekomunikacyjne sieci przewodowe wewnątrz zakładowe. Linie kablowe. Ogólne wymagania i badania.
5. BN-89/8984-10-17/03 Telekomunikacyjne sieci miejscowe. Linie kablowe. Wymagania i badania

Polskie Normy

1. PN/T-01001. Słownictwo telekomunikacyjne. Pojęcia podstawowe.

2. PN/T-01002. Nazwy i określenia.
3. PN/T-01003. Słownictwo telekomunikacyjne. Telefonia. Nazwy i określenia.
4. PN-63B-06251 Roboty betonowe i żelbetonowe. Wymagania techniczne.
5. PN-91/M-34501. Gazociągi i instalacje gazownicze. Skrzyżowania gazociągów z przeszkodami terenowymi. Wymagania.
6. PN-91/T-06700. Bezpieczeństwo pracy przy promieniowaniu emitowanym przez urządzenia laserowe. Klasyfikacja sprzętu. Wymagania i wytyczne dla użytkownika.

4. INNE POSIADANE INFORMACJE I DOKUMENTY NIEZBĘDNE DLA ZAPROJEKTOWANIA ROBÓT BUDOWLANYCH

Wykonawca uzyska na etapie projektu budowlanego wszystkie dokumenty niezbędne do zaprojektowania robót budowlanych, a w szczególności:

- kopię mapy zasadniczej
- wyniki wszystkich wymaganych prawem badań
- porozumienia, zgody lub pozwolenia oraz warunki techniczne i realizacyjne

- związane z przyłączeniem do istniejących sieci teletechnicznych
- pozostałe wymagane dokumenty

4.1 Kopia mapy zasadniczej

Kopia mapy zasadniczej zostanie uzyskana przez Wykonawcę na etapie wykonywania projektu budowlanego.

4.2 Wyniki badań gruntowo – wodnych na terenie budowy dla potrzeb posadowienia obiektów

Nie przewiduje się badań gruntowo – wodnych.

4.3 Zalecenia konserwatorskie konserwatora zabytków

Wykonawca zobowiązany będzie do uzyskania zezwolenie konserwatora – Wojewódzkiego Urzędu Ochrony Zabytków na prace adaptacyjne w budynkach zabytkowych na etapie opracowywania dokumentacji technicznej.

4.4 Inwentaryzacja zieleni

Projektowanie kanalizacji teletechnicznej na miejskich terenach zielonych powinno być uzgodnione z właściwymi organami zarządzającymi tymi terenami.

4.5 Dane dotyczące zanieczyszczeń atmosfery do analizy ochrony powietrza oraz posiadane raporty, opinie lub ekspertyzy z zakresu ochrony środowiska

Zgodnie z Dyrektywą Rady Unii Europejskiej Nr 85/337/EWG (ze zmianami wprowadzonymi Dyrektywą Rady Unii Europejskiej Nr 97/11/EW wraz z aneksami II i III) oraz na podstawie Rozporządzenia Rady Ministrów z dnia 24 września 2002 r. w sprawie określenia rodzajów przedsięwzięć mogących znacząco oddziaływać na środowisko oraz szczegółowych kryteriów związanych z kwalifikowaniem przedsięwzięć do sporządzania raportu o oddziaływaniu na środowisko (Dz.U. 2002 nr 179 poz. 1490), ocena oddziaływania planowanego przedsięwzięcia na stan środowiska naturalnego nie jest wymagana.

4.6 Pomiary ruchu drogowego, hałasu i innych uciążliwości

Projektowana inwestycja nie jest związana z ruchem drogowym, nie wytwarza hałasu i nie powoduje innych uciążliwości.

4.7 Inwentaryzacja lub dokumentacja obiektów budowlanych

Wszystkie węzły sieci powstaną w pomieszczeniach technicznych jednostek Urzędów Miast i Gmin nie podlegających przebudowie, odbudowie, rozbudowie, nadbudowie lub remontom w zakresie architektury, konstrukcji, instalacji i urządzeń technologicznych.

Nie przewiduje się rozbiórki obiektów budowlanych.

Instalacja urządzeń aktywnych nie zmienia dotychczasowych funkcji pomieszczeń.

4.8 Porozumienia, zgody lub pozwolenia oraz warunki techniczne i realizacyjne związane z przyłączeniem obiektu do istniejących sieci oraz dróg

Porozumienia, zgody lub pozwolenia oraz warunki techniczne i realizacyjne związane z przyłączeniem obiektu do istniejących sieci oraz dróg zawierane będą w zależności od potrzeb na etapie projektowania.

4.9 Dodatkowe wytyczne inwestorskie i uwarunkowania związane z budową i jej przeprowadzeniem

Budowa i eksploatacja sieci telekomunikacyjnych przez jednostki samorządu terytorialnego lub ich związki podlegają przepisom prawnym regulującym działalność samorządów w tym zakresie. Dlatego też stworzenie infrastruktury telekomunikacyjnej i sposób eksploatacji utworzonej sieci szerokopasmowej muszą być zgodne z obowiązującymi: ustawą o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz.U. 2010 nr 106 poz. 675) i ustawą Prawo telekomunikacyjne (Dz.U. 2004 nr 171 poz. 1800), wraz z rozporządzeniami wydanymi na podstawie ww. ustaw.

5. ZAŁĄCZNIKI

5.1 Załącznik Nr 1 – Mapa planowanego przebiegu kabla światłowodowego oraz planowanych łączy radioliniowych

Arkusz Nr 1 – Powiat Sławno

Arkusz Nr 2 – Miasto Sławno

5.2 Załącznik Nr 2 – Wykaz działek dla sieci światłowodowej

5.3 Załącznik Nr 3 – Harmonogram realizacji

III. SŁOWNIK POJĘĆ I SKRÓTÓW

3G (Telefonia komórkowa trzeciej generacji) - jest telefoniczną siecią cyfrową telefonii komórkowej bazującą na rozwiniętych w stosunku do 2.5G standardach i technologii trzeciej generacji z rodziny standardów IMT-2000. Dzięki poszerzonej pojemności sieci umożliwia ona wprowadzenie dodatkowych usług wykorzystujących transmisję wideo oraz transmisję pakietową (komutacje pakietów). System telefonii trzeciej generacji (3G) umożliwia nieograniczony dostęp radiowy do globalnej infrastruktury telekomunikacyjnej za pośrednictwem segmentu naziemnego, zarówno dla użytkowników stacjonarnych jak i ruchomych. Jest systemem integrującym w zamierzeniu wszystkie systemy telekomunikacyjne (teleinformatyczne, radiowe i telewizyjne). W odróżnieniu od systemu telefonii drugiej generacji GSM, w których dominującą usługą miała być usługa głosowa, a następnie rozwinięte o transmisję pakietową w oparciu o standardy GPRS oraz EDGE (zwane też systemem 2.5G) w systemach 3G od momentu rozpoczęcia projektowania zakładano „równoprawne” świadczenia różnych usług jak transmisja dźwięku, wideo i transmisji danych (pakietowa). Telefonia 3G bazuje na standardzie UMTS (ang. Universal Mobile Telecommunications System, pol. Uniwersalny System Telekomunikacji Ruchomej).

4G (Telefonia komórkowa czwartej generacji) - termin używany dla określenia standardów telefonii komórkowej, które mają być następcą systemu 3G. Wspólną cechą systemów określanych jako 4G jest przesyłanie głosu i danych za pomocą komutacji pakietów opartej na protokole IP, uproszczona architektura sieci szkieletowej oraz polepszona przepływność w sieci radiowej (w stosunku do obecnie wykorzystywanych standardów).

AV AntyVirus.

ATM (Asynchronous Transfer Mode) - technika asynchronicznego przesyłu danych zaakceptowana przez ITU-T jako docelowa technika komutacyjna dla sieci szerokopasmowej B-ISDN (Broadband Integrated Services Digital Network). Szerokopasmowa technologia komunikacyjna, dzięki której możliwe jest przesyłanie danych interakcyjnych, różnej wielkości plików, sygnału wizyjnego,

a także możliwa jest transmisja głosu. Jest to standard, który obecnie może być stosowany w sieciach lokalnych LAN, miejskich MAN, a nawet rozległych WAN. Informacja w tym standardzie przesyłana jest w postaci krótkich pakietów zaopatrzonych w nagłówek o minimalnej wielkości: 48 bajtów informacji + 5 bajtów nagłówka.

BGP (Border Gateway Protocol) - zewnętrzny protokół routingu służący do wymiany informacji o dostępnych sieciach IP pomiędzy systemami autonomicznymi, może być stosowany jako wewnętrzny protokół routingu (iBGP) do wymiany informacji o dostępnych sieciach np. w sieci MPLS.

BSA (Bitstream Access) - termin określający dostęp do lokalnej pętli abonenckiej na potrzeby sprzedaży usług szerokopasmowej transmisji danych.

CoS (Class of Services) - CoS jest formą priorytowego kolejkowania, która jest używana w protokołach sieciowych. To jest droga do klasyfikacji i priorytowania pakietów, bazując na typie aplikacji (głos, obraz, transmisja plików, typie użytkownika i innych ustawień). CoS jest dziedziną kolejkowania, podczas gdy QoS zawiera szerszy zakres technologii w zarządzaniu zasobami sieciowymi.

CPE (Customer Provided Equipment) - urządzenie sieciowe klienta (w odróżnieniu od urządzenia sieciowego operatora).

CLEC (Competitive Local Exchange Carier) - lokalny dostawca usług telekomunikacyjnych, konkurencyjny do operatora / operatorów dominujących.

DHCP (Dynamic Host Configuration Protocol) - standardowy protokół przypisujący adres IP komputerom w sieci lokalnej. Serwer DHCP tworzy przypisanie, a komputer klienta wywołuje komputer serwera, aby otrzymać żądany adres.

DoS (Denial of Service - odmowa usługi) - atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów.

EoMPLS (Ethernet over MPLS) - przesyłanie ramek protokołu sieci lokalnej Ethernet przez sieć MPLS, tunelowanie.

Falowanie kabla - zjawisko, któremu ulega kabel ułożony w kanalizacji teletechnicznej. Ze względu na giętkość kabel wprowadzony do rury nie będzie ułożony prosto, lecz będzie pofalowany. W celu obliczenia długości instalacyjnej kabla w celu jego zakupu należy pomnożyć długość poszczególnych odcinków kanalizacji przez odpowiedni współczynnik większy od 1.

FE, Fast Ethernet (znany również jako 100Base-T) - to standard szybkiej sieci lokalnej oparty na modyfikacji dotychczas funkcjonującego standardu Ethernet, o prędkości przesyłu danych – 100 Mb/s.

Firewall - zapora sieciowa (firewall – zapora przeciwogniowa). Jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz tzn. sieci publicznych, np. Internetu.

GE, Gigabit Ethernet (GbE lub 1 GigE) jest terminem określającym wiele standardów transmisji ramek Ethernetowych z szybkością 1 Gbit/s. Sygnał sieci Gigabit Ethernet może być przesyłany przez wiele różnych typów medium transmisyjnych jak np. światłowód (1000BASE-X), skrętka (1000BASE-T) lub kabel koncentryczny (1000BASE-CX). Standard IEEE 802.3z zawiera 1000BASE-SX dla transmisji przez światłowód wielomodowy, 1000BASE-LX dla transmisji światłowodem jednomodowym i praktycznie wycofany z użycia 1000BASE-CX, który używa kabla koncentrycznego.

HDPE (High Density PE) - polietylen wysokiej gęstości stosowany jako materiał do produkcji m.in. rur kanalizacji teletechnicznej.

IDS, IPS (Intrusion Detection System, Intrusion Prevention System) – systemy wykrywania i zapobiegania włamaniom) – urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym.

IGP (Interior Gateway Protocols) – rodzina protokołów trasowania danych wewnątrz systemu autonomicznego. Protokoły IGP:

- Protokoły RIP i RIPv2 (ang. Routing Information Protocol),
- Protokół IGRP (ang. Interior Gateway Routing Protocol),
- Protokół EIGRP (ang. Enhanced Interior Gateway Routing Protocol),
- Protokół OSPF (ang. Open Shortest Path First),
- Protokół IS-IS (ang. Intermediate System-to-Intermediate System).

IMS (IP Multimedia Subsystem) - ramowa architektura opracowana przez 3GPP. Umożliwia zintegrowane przesyłanie danych i głosu w sieciach IP. Architektura IMS oparta jest o protokoły SIP, Diameter i H.248. Obecnie, w ETSI TISPAN, trwają prace nad adaptacją architektury IMS do sieci o dostępie stacjonarnym.

IP (Internet Protocol) - protokół komunikacyjny warstwy sieciowej modelu OSI (warstwy internet w modelu TCP/IP). Używany powszechnie w Internecie i sieciach lokalnych. Dane w sieciach IP są wysyłane w formie bloków określanych mianem pakietów. W przypadku protokołu IP, przed rozpoczęciem transmisji nie jest zestawiana wirtualna sesja komunikacyjna pomiędzy dwoma hostami, które nie komunikowały się ze sobą wcześniej. Protokół IP jest protokołem zawodnym – nie gwarantuje, że pakiety dotrą do adresata, nie zostaną pofragmentowane, czy też zdublowane, a ponadto mogą dotrzeć do odbiorcy w innej kolejności niż zostały nadane. Niezawodność transmisji danych jest zapewniana przez protokoły warstw wyższych (np. TCP), znajdujących się w hierarchii powyżej warstwy sieciowej. Obecnie występuje w wersji pokołu 4 (IPv4) lub 6 (IPv6).

IPv4 (Internet Protocol version 4) – czwarta wersja protokołu komunikacyjnego IP przeznaczonego dla Internetu. Identyfikacja hostów w IPv4 opiera się na adresach IP. Dane przesyłane są w postaci standardowych datagramów. Wykorzystanie IPv4 jest możliwe niezależnie od technologii łączącej urządzenia sieciowe – sieć telefoniczna, kablowa, radiowa, itp. IPv4 znajduje się obecnie w powszechnym użyciu. Dostępna jest również nowsza wersja – IPv6. Dokładny opis czwartej wersji protokołu IP znajduje się w RFC 791. W modelu TCP/IP protokół IPv4 znajduje się w warstwie sieciowej.

IPv6 / IPNG (Internet Protocol version 6 / Internet Protocol Next Generation) – najnowsza wersja protokołu IP, będąca następcą IPv4, do którego stworzenia przyczynił się w głównej mierze problem małej, kończącej się ilości adresów IPv4. Dodatkowymi zamierzeniami było udoskonalenie protokołu IP: eliminacja wad starszej wersji, wprowadzenie nowych rozszerzeń (uwierzytelnienie, zlikwidowanie konieczności stosowania translacji adresów i adresów prywatnych w wielu sieciach, kompresja i inne), zminimalizowanie czynności wymaganych do podłączenia nowego węzła do Internetu (autokonfiguracja). IPv6 stanowi tylko jedną warstwę w modelu OSI – nie ingeruje on w inne warstwy, np. aplikacyjną, co pozwala działać istniejącym już protokołom zasadniczo bez problemów. IPv6 opisują dokumenty RFC 1883 i RFC 1884.

ISDN (Integrated Services Digital Network) - sieć cyfrowa z integracją usług. Technologia sieci telekomunikacyjnych mająca na celu wykorzystanie infrastruktury PSTN do bezpośredniego udostępnienia usług cyfrowych użytkownikom końcowym (bez pośrednictwa urządzeń analogowych) (end-to-end circuit-switched digital services). Połączenia ISDN zalicza się do grupy połączeń wdzwanianych (komutowanych). Wyróżnia się 2 rodzaje dostępu do ISDN: BRI (2B + D) oraz PRI (30B+D). Kanał B o przepływności 64kbps i kanał D do zarządzania połączeniem w przypadku BRI posiada 16kbps, a w przypadku PRI 64kbps.

IS-IS, **ISIS** (Intermediate System to Intermediate System) – protokół trasowania typu stanu łącza (link-state) oparty na otwartych standardach. IS-IS jest protokołem wewnętrznej bramy – IGP (ang. Interior Gateway Protocol), czyli używany jest wewnątrz systemu autonomicznego. Opisany jest w dokumencie RFC 1142. Używa algorytmu Dijkstry, by znaleźć najlepszą ścieżkę w sieci.

ISO-OSI, model OSI (Open System Interconnection) - standard zdefiniowany przez ISO oraz ITU-T, o pełnej nazwie ISO OSI RM, opisujący strukturę komunikacji sieciowej. Model ISO OSI RM (ISO OSI Reference Model) (model odniesienia łączenia systemów otwartych) jest traktowany jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Podstawowym założeniem modelu jest podział systemów sieciowych na 7 warstw (layers) współpracujących

ze sobą w ściśle określony sposób. Dla Internetu sformułowano uproszczony Model DoD, który ma tylko 4 warstwy.

ISP (Internet Service Provider) – dostawca usług internetowych, dostawca usługi dostępu do internetu.

LAN (Local Area Network) - sieć lokalna lub wewnętrzna, najmniej rozległa postać sieci komputerowej, zazwyczaj ogranicza się do jednego biura lub budynku.

LLU dostęp do lokalnej pętli abonenckiej - oznacza, zgodnie z określeniem zawartym w prawie telekomunikacyjnym, korzystanie z lokalnej pętli abonenckiej lub lokalnej podpętli abonenckiej pozwalające na korzystanie z pełnego pasma częstotliwości pętli abonenckiej (pełny dostęp do lokalnej pętli abonenckiej) lub niegłosowego pasma częstotliwości pętli abonenckiej przy zachowaniu możliwości korzystania z lokalnej pętli abonenckiej przez jej operatora do świadczenia usług telefonicznych (współdzielony dostęp do lokalnej pętli abonenckiej).

MAN (Metropolitan Area Network) - duża sieć komputerowa, której zasięg obejmuje aglomerację lub miasto. Tego typu sieci używają najczęściej połączeń światłowodowych do komunikacji pomiędzy wchodzącymi w jej skład rozrzuconymi sieciami LAN. Sieci miejskie są budowane przede wszystkim przez duże organizacje samorządowe, edukacyjne lub prywatne, które potrzebują szybkiej i pewnej wymiany danych pomiędzy punktami w ramach miejscowości bez udziału stron trzecich. Do technologii używanych przy budowaniu takich sieci należą ATM, FDDI, SMDS oraz Gigabit Ethernet. Tam gdzie niemożliwe jest użycie połączeń światłowodowych często stosuje się bezprzewodowe połączenia radiowe, laserowe lub podczerwone.

MIB (Management Information Base) - baza danych opisująca sprzęt komputerowy, na którym działa klient SNMP.

MPLS (Multiprotocol Label Switching) - technologia stosowana przez routery/przełączniki, w której routing (trasowanie) pakietów został zastąpiony przez tzw. przełączanie etykiet. Na brzegu sieci z protokołem MPLS do pakietu dołączana jest dodatkowa informacja zwana etykietą (Label). Router po odebraniu pakietu z etykietą (jest to z punktu widzenia danego routera etykieta wejściowa) używa jej jako indeksu do

wewnętrznej tablicy etykiet, w której znajduję się następny punkt sieciowy (next hop) oraz nowa etykieta (etykieta wyjściowa). Etykieta wejściowa jest zastępowana wyjściową i pakiet jest wysyłany do następnego punktu sieciowego (np. do następnego routera). Jeżeli następny router nie obsługuje protokołu MPLS etykieta jest usuwana i pakiet kierowany jest dalej wg. standardowej tablicy routingu. Pomimo, że teoretycznie istnieje możliwość zastosowania MPLS do przełączania pakietów dowolnego protokołu rutowalnego (na co wskazuje słowo Multiprotocol w nazwie), praktyczne zastosowania dotyczą jedynie protokołu IP.

MPLS pozwala na realizację między innymi następujących usług:

- MPLS IP VPN-y
- TE (Traffic Engineering Tunnels)
- AToM (ang. Any Transport over MPLS)
- VPLS (ang. Virtual Private LAN Services)

Multicast - rodzaj transmisji, w której dokładnie jeden punkt wysyła pakiety do wielu punktów (ale nie do wszystkich – broadcast). Istnieje tylko jeden nadawca i wielu odbiorców. Przykładem takiej transmisji może być transmisja sygnału radia internetowego z wykorzystaniem multicast.

NAC (Network Access Control) - Kontroler dostępu do sieci. Funkcjonalność NAC łączy ze sobą zdolność zabezpieczenia różnorodnych sieci w jedno spójne rozwiązanie realizując uwierzytelnianie oraz ocenę/weryfikację zabezpieczeń dla systemów operacyjnych typu Microsoft, Linux, Solaris, AIX, MacOS, FreeBSD. Każde podłączenie urządzenia do sieci podlega cyklowi NAC opartemu o autentykację, wykrywanie, ocenę, kwarantannę, rekultywację oraz autoryzację. System przy pomocy NAC Gateway tworzy pewnego rodzaju Proxy z udziałem serwera Radius dla 802.1x i/lub autentykacji typu web-based, wspiera również lokalną autoryzację w oparciu o adresację MAC. Proces ten może również być realizowany na dwa sposoby: w czasie przyłączania i po przyłączeniu, przy czym druga funkcja na bieżąco bada kondycję systemu końcowego (Wymagany IDS). Dzięki temu może realizować ciągłą analizę zagrożeń oraz zapobiegać i kontrolować.

NAT (Network Address Translation), nazywany też w jednej ze swych odmian maskaradą (z ang. masquerade). Technika translacji adresów sieciowych stosowana, gdy sieć lokalna używa adresów prywatnych IP lub w celu zabezpieczenia sieci lokalnej przez atakami z zewnątrz. Technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (tak IP jak i TCP/UDP), aby potwierdzić wprowadzone zmiany. Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do internetu przy wykorzystaniu pojedynczego publicznego adresu IP.

NPE (Network Provided Edge) - punkt w sieci MetroEthernet, gdzie terminowane są usługi sieciowe realizowane w warstwie 2 modelu ISO-OSI, a zaczynają być realizowane usługi warstwy trzeciej – typowe usługi rdzenia sieci.

ODF (Optical Distribution Frame) – przełącznica światłowodowa.

OSPF (Open Shortest Path First) - w wolnym tłumaczeniu "pierwszeństwo ma najkrótsza ścieżka". Jest to wewnętrzny protokół routingu typu stanu łącza (Link State). Opisany jest w dokumentach RFC 2328. Jest zalecanym protokołem wśród protokołów niezależnych (np. RIP, ang. Routing Information Protocol). W przeciwieństwie do protokołu RIP, OSPF charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek i brakiem ograniczenia skoków powyżej 15, przyspieszoną zbieżnością. Przeznaczony jest dla sieci posiadających do 50 routerów w wyznaczonym obszarze routingu. Cechami protokołu OSPF są: routing wielościeżkowy, routing najmniejszym kosztem i równoważne obciążenia.

Q-in-Q rozszerzenia do 802.1ad Provider Bridge również znane jako stackowane VLANy.

QoS (Quality of Service) - jakość usług. Wymagania nałożone na połączenie komunikacyjne, realizowane przez daną sieć telekomunikacyjną. Aby zapewnić QoS, stosowane są następujące mechanizmy:

- kształtowanie i ograniczanie przepustowości

- zapewnienie sprawiedliwego dostępu do zasobów
- nadawanie odpowiednich priorytetów poszczególnym pakietom wędrującym przez sieć
- zarządzanie opóźnieniami w przesyłaniu danych
- zarządzanie buforowaniem nadmiarowych pakietów: DRR, WFQ, WRR
- określenie charakterystyki gubienia pakietów
- unikanie przeciążeń: Connection Admission Control (CAC), Usage Parameter Control (UPC)

PE (Provider Edge) - brzeg sieci operatora, do urządzeń PE włączane są urządzenia klienta (CPE).

Peering - wymiana ruchu pomiędzy dostawcami usług internetowych (ISP) na zasadach partnerskich. Peering składa się z trzech elementów:

- fizycznego połączenia pomiędzy sieciami,
- protokołu umożliwiającego wymianę ruchu między sieciami,
- umowy peeringowej

Dostawcy usług internetowych łączą swoje sieci za pomocą punktów połączeń (peering point), następnie zawierają umowę peeringową, która dokładnie precyzuje zasady wymiany przez nich ruchu. Dzięki peeringowi informacja w Internecie może wędrować krótszą drogą, a co za tym idzie szybciej. Zmniejsza to obciążenie łączy i umożliwia efektywniejsze ich wykorzystanie.

Peszel, rura peszla - karbowana rura osłonowa na kable teletechniczne: elektryczne, telefoniczne, światłowody lub rury sanitarne (wodociągowe, centralnego ogrzewania, kanalizacyjne, itp.). Karby umożliwiają łatwiejsze tworzenie łuków i jednocześnie pozytywnie wpływają na trwałość mechaniczną osłony. Peszel umożliwia fizyczny rozdział kabli np. w szachtach teletechnicznych. Peszel można również układać w bruzdach w ścianie przed otynkowaniem lub w podłogach przed wykonaniem wylewek, w celu późniejszego zaciągnięcia okablowania.

PSTN (Public Switched Telephone Network - Publiczna Komutowana Sieć Telefoniczna) - oznacza tradycyjną sieć telefoniczną Jej funkcjonowanie polega na łączeniu

(komutowaniu) abonentów poprzez ustanowienie bezpośredniego połączenia (kanału) między nimi przy użyciu sieci kablowej i central telefonicznych. PSTN to tradycyjne telefony stacjonarne i sieci telefonów komórkowych. Obecnie PSTN coraz częściej wykorzystuje technologie cyfrowe, więc różnica pomiędzy VoIP a PSTN zaciera się coraz bardziej.

RIP (Routing Information Protocol) - Protokół Informowania o Trasach należący do grupy protokołów bram wewnętrznych (IGP), oparty jest na zestawie algorytmów wektorowych, służących do obliczania najlepszej trasy do celu.

SDH (Synchronous Digital Hierarchy) - Synchroniczna Hierarchia Systemów Cyfrowych, jest to technologia sieci transportu informacji, charakteryzująca się tym, że wszystkie urządzenia działające w sieci SDH, pracujące w trybie bezawaryjnym, są zsynchronizowane zarówno do nadrzędnego zegara (PRC) jak i do siebie nawzajem (w odróżnieniu od takich technologii jak, np. ATM). Ważną cechą jest również to, że podstawowa jednostka transportowa STM-N (Synchronous Transport Module - Synchroniczny Moduł Transportowy), w czasie zwielokrotniania ma przepływność, będącą N-tą wielokrotnością STM-1 (155,52 Mbit/s). Ta właściwość nie występuje np. w technologii PDH. Sieci SDH charakteryzują się o wiele większą niezawodnością od innych oraz mniejszą podatnością na uszkodzenia wynikającą z budowy m.in. struktur pierścieniowych. Dzięki temu mają możliwość automatycznej rekonfiguracji w czasie krótszym niż 50 ms.

Stosuje się następujące wielokrotności:

- STM-1 (155,52 Mbit/s),
- STM-4 (622,08 Mbit/s),
- STM-16 (2488,32 Mbit/s),
- STM-64 (9953,28 Mbit/s),
- STM-256 (39813,12 Mbit/s).

SIEM (Security Information and Event Management) – zarządzanie bezpieczeństwem informacji i zdarzeniami.

SLA (Service Level Agreement) - umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług informatycznych poprzez stały cykl obejmujący:

- uzgodnienia,
- monitorowanie usługi informatycznej,
- raportowanie,
- przegląd osiąganych wyników.

SNMP (Simple Network Management Protocol) z ang. Prosty Protokół Zarządzania Siecią - standard protokołu używanego do nadzoru i zarządzania różnymi elementami sieci telekomunikacyjnych, takimi jak routery, przełączniki, komputery czy centrale telefoniczne. Istnieją obecnie trzy wersje protokołu SNMP:

- pierwsza (SNMPv1),
- druga (SNMPv2),
- trzecia (SNMPv3).

STP (Spanning-Tree Protocol) - protokół komunikacyjny, sporządzony przez IEEE (Institute of Electrical and Electronics Engineers) opisany w dokumencie IEEE 802.1d. Jest to protokół wykorzystywany przez sieci komputerowe (np. LAN) w drugiej warstwie modelu sieciowego ISO/OSI. STP obsługiwany jest przez przełączniki (network switch) i mostki sieciowe (network bridge). Stworzony dla zwiększenia niezawodności środowisk sieciowych. Umożliwia on konfigurację tych urządzeń w sposób zapobiegający powstawaniu pętli. Protokół ten tworzy graf bez pętli w kształcie drzewa i ustala zapasowe łącza. W trakcie normalnej pracy sieci blokuje je, tak by nie przekazywały one żadnych danych. Wykorzystywana jest tylko jedna ścieżka, po której może odbywać się komunikacja. Na szczycie grafu znajduje się główny przełącznik tzw. korzeń (root) zarządzający siecią. Korzeniem zostaje przełącznik na podstawie identyfikatora. W momencie gdy STP wykryje problem np. zerwany link, to rekonfiguruje sieć uaktywniając łącze zapasowe, potrzebuje na to ok. 30 do 60 sekund.

Poprawkami do STP są protokoły:

- RSTP (ang. Rapid Spanning Tree Protocol, IEEE 802.1w) zapewnia krótszy czas przywracania sprawności połączeń po awarii.
- MSTP (ang. Multiple Spanning Tree Protocol, IEEE 802.1s) umożliwia równoważenie obciążenia i zwiększa odporność sieci na błędy dzięki zapewnieniu wielu ścieżek przekazywania ruchu danych.

TCP/IP (Transmission Control Protocol / Internet Protocol) - pakiet najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. Najczęściej obecnie wykorzystywany standard sieciowy, stanowiący podstawę współczesnego Internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: TCP oraz IP.

TDM (Time Division Multiplexing) - technika przesyłu sygnałów cyfrowych polegając na zwielokrotnianiu w dziedzinie czasu. Przesyłane sygnały dzielone są na części, którym później przypisywane są czasy transmisji. Najpierw przesyłana jest pierwsza część pierwszego sygnału potem pierwsza część drugiego sygnału itd. Gdy zostaną przesłane wszystkie pierwsze części, do głosu dochodzą drugie części sygnału. Podstawowym sygnałem używanym w telekomunikacji z komutacją kanałów jest strumień E1 (30 kanałów 64 kbps). Sygnał najczęściej fizycznie jest wyprowadzany stykiem G.703 lub V.35.

UPE (User Provided Edge), Jest to styk stanowiący punkt, w którym kończy się sieć zarządzana przez operatora, a zaczyna się sieć klienta.

UNI (User-Network Interface) - styk pomiędzy siecią a użytkownikiem realizuje urządzenie UNI. Najbardziej popularnym UNI jest karta sieciowa Ethernet.

Unicast - rodzaj transmisji, w której dokładnie jeden punkt wysyła pakiety do dokładnie jednego punktu - istnieje tylko jeden nadawca i tylko jeden odbiorca. Wszystkie karty Ethernet posiadają zaimplementowany ten rodzaj transmisji. Oparte na nim są podstawowe protokoły takie jak TCP, HTTP SMTP, FTP i telnet i częściowo ARP, który pierwsze żądanie wysyła zawsze korzystając z transmisji broadcast.

UTM (Unified Threat Management) - zunifikowane (zintegrowane) zarządzanie zagrożeniami. Wielofunkcyjne zapóry ogniowe oferujące:

- ochronę antyspamową (filtrowanie e-poczty)
- ochronę antywirusową,
- wykrywanie intruzów,
- zapobieganie wtargnięciu intruzów,
- filtrowanie treści internetowych,
- standardowe usługi zapór ogniowych, jak np. translacja adresów (NAT).

Urządzenia UTM zdobywają rynek kosztem dotychczasowych rozwiązań firewall/VPN oraz innych zabezpieczeń realizowanych punktowo. Zapory klasy UTM są doskonałym rozwiązaniem dla małych i średnich firm, a także dla oddziałów większych przedsiębiorstw, gdzie brak odpowiedniego zaplecza finansowego oraz technicznego do zarządzania kompleksowym systemem zabezpieczeń sieciowych jest barierą nie do przeskoczenia. Posiadają one wiele wbudowanych modułów ochrony, a ich instalacja, konfiguracja i zarządzanie ogranicza koszty wdrożenia i utrzymania się.

VLAN (Virtual Local Area Network), sieć wirtualna jest siecią komputerową wydzieloną logicznie w ramach innej, większej sieci fizycznej. Do tworzenia VLAN-ów wykorzystuje się konfigurowalne switche, umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych, poprzez separację ruchu pomiędzy określonymi grupami portów. Komunikacja między VLAN-ami jest możliwa tylko wtedy, gdy w VLAN-ach tych partycypuje port należący do routera. W przełącznikach zarządzalnych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (tagowanie) poprzez doklejenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (trunking).

VPLS MPLS pozwala na realizację między innymi następujących usług:

- MPLS IP VPN-y
- TE (Traffic Engineering Tunnels)
- AToM (Any Transport over MPLS)
- VPLS (Virtual Private LAN Services)

VoIP (Voice over Internet Protocol) - technologia cyfrowa umożliwiająca przesyłanie dźwięków mowy za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP, popularnie nazywana "telefonią internetową". Dane przesyłane są przy użyciu protokołu IP, co pozwala wykluczyć niepotrzebne "połączenie ciągłe" i np. wymianę informacji, gdy rozmówcy milczą.

VPN (Virtual Private Network) - wirtualna sieć prywatna. Można ją opisać jako "tunel", przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej, jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Taki kanał może opcjonalnie kompresować lub szyfrować w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa przesyłanych danych.

VRF (VPN Routing and Forwarding) - routing i przekazywanie dla VPN.

WiMAX (Worldwide Interoperability for Microwave Access) - technologia bezprzewodowej, radiowej transmisji danych. Została oparta na standardach IEEE 802.16 i ETSI HiperMAN. Standardy te stworzono dla szerokopasmowego, radiowego dostępu na dużych obszarach. Standardy te określają informacje dotyczące konfiguracji sprzętu tak, aby urządzenia różnych dostawców pracowały na tych samych konfiguracjach, tj. aby wzajemnie ze sobą współgrały. WiMAX jest technologią umożliwiającą budowę bezprzewodowych miejskich sieci komputerowych (MAN), a także rozległych obszarów usługowych, wykorzystywanych na przykład do świadczenia usług szerokopasmowego, bezprzewodowego dostępu do Internetu dla klientów indywidualnych i biznesowych. Standard ten zapewnia mobilność w wersji 802.16e.