


Wykonawca:	<b>KONSORCJUM</b>			
	<b>WASKO S.A.</b> ul. Berbeckiego 6 44-100 Gliwice	<b>FONBUD Sp. z o.o.</b> ul. Redycka 71 51-169 Wrocław	<b>J. Dudek TELNET S.K.A.</b> ul. Obr. Poczty Gdańskiej 13A 52-504 Wrocław	
Jednostka projektowa:			<b>Wasko S.A.</b> 44-100 Gliwice ul. Berbeckiego 6	tel. +48 32 33 25 500 fax +48 32 33 25 505 <a href="mailto:wasko@wasko.pl">wasko@wasko.pl</a> <a href="http://www.wasko.pl">www.wasko.pl</a>
Stadium:	<b>PROJEKT WYKONAWCZY</b>			
Temat opracowania:	<b>Likwidacja obszarów wykluczenia informacyjnego i budowa dolnośląskiej sieci szkieletowej</b> Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. Urządzenia teletransmisyjne.			
Obiekt:	<b>Sieć kablowa. Urządzenia teletransmisyjne</b>			
Branża:	<b>Teletechniczna</b>			
Inwestor:	<b>Województwo Dolnośląskie</b> 50-411 Wrocław, ul. Wybrzeże Słowackiego 12-14			
	Nr archiwalny:	<b>DT-W/658/12-97-PW</b>		
	Wersja:	<b>1.2</b>		
	Tom:	<b>1/5</b>		
	Egzemplarz:	<b>/5</b>		

<b>Funkcja Imię i nazwisko</b>	<b>Uprawnienia/ specjalność</b>	<b>Numer uprawnień</b>	<b>Data</b>	<b>Podpis</b>
Projektował : Michał Olempa	telekomunikacyjna	SLK/0978/PWOT/05	14.05.2013	
Opracował : Marek Plaza	telekomunikacyjna	-----	14.05.2013	
Sprawił : Ryszard Śpitalniak	telekomunikacyjna	DT-WBT/02428/03/U	14.05.2013	



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



## SPIS TREŚCI

1	Część ogólna .....	8
1.1	Przedmiot opracowania .....	8
1.2	Podstawa opracowania projektu .....	10
1.3	Opis ogólny i zakres rzeczowy inwestycji.....	10
1.3.1	Opis ogólny .....	10
1.3.2	Zakres rzeczowy .....	11
2	Oświadczenie projektanta .....	13
3	Normy i dokumenty odniesienia .....	14
3.1	Wykaz norm i dokumentów odniesienia .....	14
3.2	Symbolika i oznaczenia wykorzystane w projekcie.....	16
4	Charakterystyka techniczna opracowania.....	17
4.1	Standard nazewnictwa i numeracji elementów sieci.....	17
4.2	Topologia i organizacja logiczna sieci.....	18
4.3	Wymagania w zakresie separacji transmisji danych.....	19
4.4	Założenia techniczne.....	19
4.5	Wymagania ogólne dla urządzeń sieciowych podlegających dostawie.....	23
4.5.1	Wymagania w zakresie zarządzania i monitorowania urządzeń sieciowych .....	24
4.5.2	Wymagania ogólne dla urządzeń szkieletu sieci.....	25
4.5.3	Wymagania ogólne dla urządzeń warstwy dystrybucyjnej.....	26

4.5.4	Wymagania ogólne dla sieci i przełączników sieci zarządzającej PSZ .....	27
4.5.5	Wymagania ogólne dla infrastruktury punktów wymiany ruchu IXP .....	28
4.5.6	Wymagania ogólne dla Węzłów Wymiany Ruchu WWR .....	29
4.5.7	Wymagania ogólne dla systemu DWDM .....	30
4.5.8	Wymagania ogólne dla infrastruktury CZS i zCSZ .....	32
4.5.8.1	Wymagania w zakresie niezawodności i wydajności CZS i zCSZ .....	34
4.5.8.2	Wymagania w zakresie zarządzania i bezpieczeństwa CZS i zCSZ .....	35
4.6	Infrastruktura węzłów dolnośląskiej sieci szerokopasmowej .....	35
4.6.1	Infrastruktura Węzła Szkieletowego i CZS Wrocław WS_C3_10/CZS .....	42
4.6.2	Infrastruktura Węzła Szkieletowego Legnica WS_C3_5 .....	45
4.6.3	Infrastruktura Węzła Szkieletowego Wałbrzych WS_C3_9 .....	46
4.6.4	Infrastruktura Węzła Szkieletowego Rudna WS_C2_8 .....	47
4.6.5	Infrastruktura Węzła Szkieletowego Strzelin WS_C2_7 .....	47
4.6.6	Infrastruktura Węzła Szkieletowego Kłodzko WS_C2_4 .....	48
4.6.7	Infrastruktura Węzła Szkieletowego Jelenia Góra WS_C2_3 .....	49
4.6.8	Infrastruktura Węzła Szkieletowego Bolesławiec WS_C1_1 .....	49
4.6.9	Infrastruktura Węzła Szkieletowego Lubań WS_C2_6 .....	50
4.6.10	Infrastruktura Węzła Dystrybucyjnego klasy „F” Oleśnica WD_F_47 .....	51
4.6.11	Infrastruktura Węzłów Dystrybucyjnych klasy „E” Góra, Ścinawa, Łagiewniki WD_E_16, WD_E_59, WD_E_34 .....	52
4.6.12	Wymagania ogólne dla infrastruktury węzłów dystrybucyjnych klasy „D” WD_D_x .....	52
4.6.13	Infrastruktura zCSZ Świdnica .....	53
4.6.14	Punkty dostępu do Internetu (IPX) .....	55



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



4.6.15	Rozbudowa węzłów sieci DSS .....	56
4.7	Organizacja połączeń międzywęzłowych .....	57
4.8	Charakterystyka techniczna urządzeń przeznaczonych do wybudowania sieci .....	58
4.8.1	Szczegółowe wymagania dla routerów szkieletowych .....	58
4.8.2	Szczegółowe wymagania dla routerów dystrybucyjnych .....	60
4.8.3	Szczegółowe wymagania dla routerów punktów wymiany ruchu (IXP) .....	62
4.8.4	Szczegółowe wymagania dla Przełączników Sieci Zarządzającej PSZ .....	63
4.8.5	Szczegółowe wymagania dla urządzeń i systemów Centrów Zarządzania Siecią .....	66
4.8.5.1	Szczegółowe wymagania dla Przełącznika CZS .....	67
4.8.5.2	Szczegółowe wymagania dla Firewall z IDS/IPS .....	68
4.8.5.3	Szczegółowe wymagania dla Systemu Zarządzania Siecią .....	69
4.8.5.4	Wymagania dla Systemu Prezentacji Stanu Sieci.....	72
4.8.6	Szczegółowe wymagania dla urządzeń systemu DWDM .....	73
4.8.7	Wymagania dotyczące patchcordów .....	77
4.9	Opis czynności uruchomieniowych i wstępnej konfiguracji sieci .....	78
4.9.1	Przygotowanie Planu Wdrożenia .....	78
4.9.2	Opracowanie polityki bezpieczeństwa.....	81
4.9.3	Ramowe wymagania odnośnie konfiguracji urządzeń.....	82
4.9.3.1	Węzeł szkieletowy.....	82
4.9.3.2	Węzeł dystrybucyjny .....	83
4.9.3.3	Węzeł IXP .....	83
4.9.3.4	Węzeł CZS i zCZS.....	84
4.10	Testy akceptacyjne, odbiór i gwarancja .....	85



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



4.10.1	Testy akceptacyjne systemów IP oraz SZS i SPSS .....	86
4.10.2	Testy akceptacyjne systemu DWDM.....	88
4.10.2.1	Test redundancji zasilania .....	89
4.10.2.2	Poziom sygnału nadawanego Tx interfejsu klienckiego.....	89
4.10.2.3	Czułość interfejsu klienckiego – minimalny poziom sygnału odbieranego.....	91
4.10.2.4	Przesterowanie interfejsu klienckiego – maksymalny poziom sygnału .....	93
4.10.2.5	Poziom sygnału nadawanego Tx interfejsu liniowego .....	95
4.10.2.6	Czułość interfejsu liniowego .....	96
4.10.2.7	Przesterowanie interfejsu liniowego .....	97
4.10.2.8	Widmo sygnału liniowego transpondera.....	99
4.10.2.9	Moc wyjściowa optycznego kanału nadzoru OSC (Optical Supervision Channel) .	102
4.10.2.10	Czułość wejściowa kanału nadzoru.....	103
4.10.2.11	Sprawdzenie parametrów wzmacniaczy oraz weryfikacja OSNR (Optical Signal-To-Noise Ratio) .....	104
4.10.2.12	Zachowanie wzmacniacza w przypadku zmiany liczby kanałów optycznych .....	105
4.10.2.13	Sprawdzenie poprawności alarmowania elementów sieciowych .....	106
4.10.2.14	48h test BER dla uruchamianych serwisów .....	106
4.10.2.15	Wykonanie testów RFC 2544 dla serwisów Ethernet .....	107
4.10.2.16	Zmiana wersji oprogramowania węzła DWDM .....	108
4.10.3	Odbiór .....	108
4.10.4	Gwarancja .....	109
4.11	Wymagania w zakresie szkoleń.....	110
5	Spis dokumentów związanych.....	115



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



6	Spis tabel .....	116
6.1	Lista węzłów sieciowych .....	116
6.2	Zestawienie montowanych urządzeń wg lokalizacji węzłów .....	120
6.3	Lista urządzeń podlegających dostawie .....	121
6.4	Lista czynności do wykonania .....	122
6.5	Tabela orientacyjnych* długości relacji międzywęzłowych .....	123
6.6	Tabela orientacyjnych wartości dyspersji chromatycznej dla relacji .....	123
6.7	Tabela orientacyjnych wartości tłumienności dla relacji .....	124
6.8	Macierz przepływności łączy DWDM .....	125
6.9	Macierz zajętości włókien w szkielecie sieci .....	125
6.10	Tabela dodatkowych wymagań dla routerów szkieletowych RS_C1-3 .....	127
6.11	Tabela dodatkowych wymagań dla routerów dystrybucyjnych model E .....	128
6.12	Lista testów do wykonania dla routerów szkieletowych i dystrybucyjnych .....	128
6.13	Maksymalne dopuszczalne wartości opóźnień i strat pakietów w zależności od klasy ruchu 130	
7	Uwagi końcowe .....	131
8	Informacja BIOZ .....	131
8.1	Lista urządzeń podlegających dostawie .....	131
8.2	Zakres stosowania .....	131
8.3	Zakres wykonywania robót .....	131
8.4	Przewidywane zagrożenia .....	132
8.4.1	Wykaz elementów – potencjalnych źródeł zagrożenia .....	132
8.4.2	Wykaz zagrożeń i ryzyk .....	132



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



8.5	Środki zapobiegania niebezpieczeństwom .....	132
9	Załączniki .....	134
1.	Blokowy schemat rozptywu włókien	
2.	Topologia geograficzna połączeń tras światłowodowych DSS	
3.	Schemat organizacji połączeń sieci IP w rdzeniu sieci DSS	
4.	Schemat organizacji połączeń sieci DWDM w DSS	
5.	Schemat ogólny połączeń w sieci DSS	
6.	Schemat logiczny organizacji podłączeń routerów IXP do szkieletu sieci DSS	
7.	Schemat logiczny organizacji połączeń w zCZS Świdnica w DSS	
8.	Schemat logiczny organizacji połączeń w CZS Wrocław w DSS	
9.	Symboliczny schemat połączeń między Przełącznikami Sieci Zarządzającej	
9A.	Schemat połączeń między Przełącznikami Sieci Zarządzającej	
10.	Rozmieszczenie urządzeń w szafach w węźle szkieletowym i CZS Wrocław	
11.	Rozmieszczenie urządzeń w szafach we wszystkich węzłach szkieletowych oprócz Wrocławia	
12.	Rozmieszczenie urządzeń w szafie zewnętrznej dla węzła dystrybucyjnego klasy F (Oleśnica)	
13.	Rozmieszczenie urządzeń w szafie zewnętrznej dla węzła dystrybucyjnego klasy E (Góra, Ścinawa, Łagiewniki)	
14.	Rozmieszczenie urządzeń w szafie zewnętrznej dla węzłów dystrybucyjnych klasy D	
15.	Rozmieszczenie urządzeń w szafach kontenera oraz budynku dworca zCZS Świdnica	



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



# 1 Część ogólna

## 1.1 Przedmiot opracowania

Niniejsze opracowanie jest częścią dokumentu pn. „Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci”, zawierającego projekty wykonawcze, specyfikacje techniczne wykonania i odbioru, instrukcje BIOZ oraz przedmiary i kosztorysy prac dla elementów części aktywnej Dolnośląskiej Sieci Szkieletowej (DSS). W/w dokument jest częścią projektu pn. "Likwidacja obszarów wykluczenia informacyjnego i budowa dolnośląskiej sieci szkieletowej", realizowanego przez Województwo Dolnośląskie (Inwestor).

**Podstawowym założeniem przyjętym przy projektowaniu części aktywnej Dolnośląskiej Sieci Szkieletowej było stworzenie sieci neutralnej technologicznie na bazie której świadczone będą usługi klasy Operator-dla-Operatora (ang. CsC, Carrier supporting Carrier), spełniającej wymagania dla tzw. sieci następnej generacji (ang. NGN - Next-Generation Networks), jak również efektywnej finansowo zarówno w zakresie nakładów inwestycyjnych jak i kosztów eksploatacyjnych.**

W zaprojektowanym modelu odbiorcami usług nie są klienci indywidualni, lecz podmioty świadczące usługi telekomunikacyjne, to jest operatorzy telekomunikacyjni, czy też Jednostki Samorządu Terytorialnego zgłoszone w rejestrze UKE.

W zgodzie z dokumentem *Studium wykonalności dla projektu pn.: „Likwidacja obszarów wykluczenia informacyjnego i budowa dolnośląskiej sieci szkieletowej”*, w ramach aktywności Dolnośląskiej Sieci Szkieletowej założono przygotowanie sieci do świadczenia następujących usług:

1. Dzierżawa infrastruktury pasywnej sieci:
  - a) dzierżawa kanalizacji teletechnicznej;
  - b) dzierżawa ciemnych włókien światłowodowych;
  - c) usługa kolokacji.
2. Usługi teletransmisyjne:



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





a) Usługi transmisji optycznej:

- optyczne lambdy dla klienta,
- usługi transmisji punkt-punkt dla dowolnego protokołu,

b) Usługi Ethernet:

- Ethernet Line (Eth LL), Ethernet Virtual Line(VLL), Ethernet LAN (VPLS), Ethernet Virtual LAN (VPLS),
- Carrier of carriers - Metro Ethernet,

c) Routing IP:

- IP Leased Lines,
- IP-VPN,

d) Internet access:

- Carrier of IP carriers,
- Quality Internet,
- Enhanced Bussines Services.

Zaprojektowana do realizacji wyżej wskazanych usług sieć szkieletowa posiada szereg cech użytkowych wymienionych poniżej:

1. przyjmuje ruch o zadeklarowanej przepustowości w jednym z węzłów i przesyła ten ruch do innych węzłów,
2. różnicuje poziom usługi, poprzez przypisanie do przesyłanego ruchu zdefiniowanego priorytetu, decydującego o metodzie reakcji w sytuacji degradacji,
3. zapewnia stałe, i możliwie niskie opóźnienia i zmienność opóźnienia przesyłanego ruchu,
4. monitoruje stan sieci, urządzeń, usług i połączeń,
5. monitoruje stan informacji ruchowych (przepustowości),
6. umożliwia rozbudowę w przypadku konieczności zwiększenia przepustowości, dodania węzła, czy zwiększenia liczby połączeń końcowych.

Przedmiotem niniejszego opracowania jest określenie szczegółowych rozwiązań technicznych, niezbędnych do wybudowania i uruchomienia infrastruktury urządzeń aktywnych sieci optycznej oraz systemu monitorowania i prezentacji stanu sieci.

Dokumentem ściśle powiązaniem z niniejszym opracowaniem sieci jest dokument "Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II". Dokument ten zawiera szereg wytycznych projektowych i wymagań co do architektury i technologii budowy sieci uwzględnionych finalnie w Projekcie.

## 1.2 Podstawa opracowania projektu

Podstawę do wykonania niniejszego opracowania stanowi umowa nr Nr DT-W/658/12 z dnia 28.02.2012r, zawarta pomiędzy **Inwestorem**:

**Województwem Dolnośląskim**, z siedzibą we Wrocławiu, ul. Wybrzeże Słowackiego 12-14, 50-411 Wrocław

oraz **Wykonawcą projektu, konsorcjum firm**:

**Wasko S.A.** z siedzibą w Gliwicach, ul. Berbeckiego 6, 44-100 Gliwice (lider konsorcjum), **FONBUD Sp. z o.o.** z siedzibą we Wrocławiu, ul. Redycka 71, 51-169 Wrocław (uczestnik konsorcjum), **Jerzy Dudek TELNET S.K.A.** z siedzibą we Wrocławiu, ul. Obrońców Poczty Gdańskiej 13A, 52-204 Wrocław (uczestnik konsorcjum).

Nadto, projekt został wykonany w oparciu o:

1. uzgodnienia robocze i formalno-prawne dokonane przez projektanta,
2. normy i przepisy obowiązujące w budownictwie łączności.

## 1.3 Opis ogólny i zakres rzeczowy inwestycji

### 1.3.1 Opis ogólny

Ze względu na specyfikę funkcjonowania sieci typu CsC w warstwie transportowej zaprojektowano system DWDM (ang. dense wavelength division multiplexing), którego urządzenia umiejscowiono w 9 węzłach szkieletowych oraz w 1 węźle dystrybucyjnym (Oleśnica).



Zaprojektowana topologia sieci DSS jest topologią:

1. kratową w warstwie szkieletowej sieci – krata niepełna (pseudo-mesh),
2. warstwa agregująca sieci w topologii gwiazdy z redundancją łączy.

W wyniku przeprowadzenia analizy ruchowej przypisano węzłom szkieletowym funkcje agregujące czyli połączono funkcjonalności P (ang. Provider router) oraz PE (ang. Provider Edge router) w szkieletowych urządzeniach IP (routerach).

Nadto, w wyniku analiz zapotrzebowania na usługi oraz przewidywanego wstępnie ruchu w sieci, zaprojektowano wyposażenie w sprzęt aktywny IP dla 5 węzłów dystrybucyjnych. Pozostałe węzły dystrybucyjne skonfigurowano tak, aby były one gotowe w każdej chwili do przyjęcia sprzętu aktywnego w zależności od potrzeb biznesowych przyszłego operatora sieci DSS oraz zgłaszanego zapotrzebowanie na usługi ze strony operatorów trzecich.

W wyniku analiz zapotrzebowania na usługi oraz w uzgodnieniu z Zamawiającym, dokonano przesunięcia urządzeń aktywnych planowanych wstępnie dla węzła dystrybucyjnego w Sobótce, tym samym zCZS Świdnica uzyskał cechy węzła dystrybucyjnego, z przeznaczeniem do obsługi obszarów przyległych (w szczególności gminy Sobótka).

Projekt przygotowano w taki sposób, aby możliwa była realokacja sprzętu aktywnego (urządzeń lub wyposażenia) pomiędzy poszczególnymi węzłami DSS, zarówno szkieletowymi jak i dystrybucyjnymi. Ostateczną decyzję o alokacji zaprojektowanych w niniejszej dokumentacji urządzeń aktywnych, w lokalizacjach poszczególnych węzłów DSS, pozostawia się Operatorowi Infrastruktury, stosownie do jego potrzeb. Zakłada się, że decyzje takie Operator Infrastruktury będzie podejmował w okresie eksploatacji, informując o tym Właściciela sieci poprzez wprowadzanie odpowiednich zapisów do udostępnionego systemu paszportyzacji DSS.

Szczegółowy opis przeprowadzonej analizy ruchu zawarto w odrębnym dokumencie.

### 1.3.2 Zakres rzeczowy

Opracowanie zawiera projekt części aktywnej Dolnośląskiej Sieci Szkieletowej, tj. Regionalnej Sieci Szerokopasmowej Województwa Dolnośląskiego. W projekcie opisano wyposażenie punktów sieci w sprzęt aktywny, sposób ich połączenia oraz opis wymagań stawianych tym urządzeniom. Zakres rzeczowy projektu obejmuje wyposażenie:

1. 9 Węzłów Szkieletowych,

2. 82 Węzłów Dystrybucyjnych,
3. 1 Centrum Zarządzania Siecią i 1 Zapasowego Centrum Zarządzania Siecią
4. 2 punktów wymiany ruchu IXP.

Spis węzłów wraz z realizowanymi funkcjami zawiera Tabela 6.1.

W ramach realizacji niniejszego projektu Wykonawca (Operator Infrastruktury) musi:

1. Dostarczyć, zamontować we właściwych lokalizacjach i uruchomić urządzenia aktywne wymienione w tabeli 6.3 (wraz z oprogramowaniem i licencjami niezbędnymi do uzyskania opisanej w projekcie funkcjonalności), zgodnie z opisem technicznym zamieszczonym w punkcie 4,
2. Wykonać niezbędne połączenia pomiędzy portami urządzeń oraz przełącznic, realizując topologię sieci opisaną w punkcie 4.7. Kompletną, szczegółową listę połączeń powinien przygotować Operator Infrastruktury, na podstawie schematu rozwiniętego przebiegu włókien oraz znajomości charakterystyk konkretnych wybranych przez siebie implementacji urządzeń sieciowych.
3. Opracować zasady polityki bezpieczeństwa dla Dolnośląskiej Sieci Szerokopasmowej, uwzględniające specyfikę zaoferowanej implementacji sprzętowej, zgodnie z wymaganiami opisanymi w punkcie 4.9.2,
4. Opracować Plan Wdrożenia oraz dokonać konfiguracji urządzeń, zgodnie z wymaganiami zamieszczonymi w punktach 4.9.2 i 4.9.3,
5. Przeprowadzić testy akceptacyjne potwierdzające spełnienie opisanych wymagań przez poszczególne urządzenia oraz osiągnięcie zaplanowanych funkcjonalności przez całą sieć, zgodnie z opisem zamieszczonym w punkcie 4.10,
6. Przeprowadzić szkolenia personelu, zgodnie z opisem zamieszczonym w punkcie 4.11.

Szczegółowe zestawienie prac objętych niniejszym projektem, wraz z podaniem zakresu wymagań dla tych prac, zostało ujęte w tabeli 6.4.

## 2 Oświadczenie projektanta

### O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust. 4 Prawa Budowlanego (Dz. Nr 207 z 2003 r. Poz. 2016 z późniejszymi zmianami)

**oświadczam jako projektant**

że projekt:

*DT-W/658/12-97-PW **Projekt wykonawczy. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. TOM1. Urządzenia teletransmisyjne**, realizowany w ramach zadania „Likwidacja obszarów wykluczenia informacyjnego i budowa dolnośląskiej sieci szkieletowej”*

sporządzono zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej oraz że jest on kompletny, z punktu widzenia celu jakiemu ma służyć.

.....  
(podpis)



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



### 3 Normy i dokumenty odniesienia

#### 3.1 Wykaz norm i dokumentów odniesienia

Wszystkie prace należy wykonać według opisów ogólnych i szczegółowych zawartych w projekcie, zgodnie z właściwymi przepisami branżowymi oraz podanymi poniżej normami i dokumentami odniesienia:

1. PN-91/E-05009, Instalacje elektryczne w obiektach budowlanych
2. PN-EN 60950-1, Urządzenia techniki informatycznej. Bezpieczeństwo. Część 1: Wymagania podstawowe
3. Zalecenie ITU-T M.3010 Principles for a telecommunications management network,
4. Zalecenie ITU-T M.3400 TMN management functions,
5. dZalecenie ITU-T Y.2401/M.3060: Principles for the Management of Next Generation Networks
6. Zalecenie ITU-T Y.2201: Requirements and capabilities for ITU-T NGN
7. Zalecenie ITU-T Y.2601: Fundamental characteristics and requirements of future packet based networks
8. Zalecenie ITU-T Y.2615: Routing mechanisms in public packet telecommunication data networks
9. Zalecenie ITU-T Y.140.1 (2004), Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services.
10. Zalecenie ITU-T Y.2611: High-level architecture of future packet-based networks
11. Zalecenie ITU-T Y.2704: Security mechanisms and procedures for NGN
12. Zalecenie ITU-T G.652 Characteristics of a single-mode optical fibre cable
13. Zalecenie ITU-T G.709 Network Node Interface for the Optical Transport Network (OTN). OTU interfaces

14. Zalecenie ITU-T G.872 Architecture of Optical Transport Networks (OTN)
15. Zalecenie ITU-T G.873.1 Optical Transport Network (OTN): Linear protection
16. Zalecenie ITU-T G.8251 The control of jitter and wander within the optical transport network (OTN)
17. Zalecenie ITU-T G.8201 Error performance parameters and objectives for multi-operator international paths within the Optical Transport Network (OTN)
18. Zalecenie ITU-T G.798 Characteristics of Optical Transport Network Hierarchy Equipment
19. Functional Blocks.
20. Zalecenie ITU-T G.694.1 Spectral grids for WDM applications: DWDM frequency grid
21. Zalecenie ITU-T G.692 Optical interfaces for multichannel systems with optical amplifiers
22. Zalecenie ETS 300 019-1-2 Class 2.3 Public transportation, no special precautions are required
23. Zalecenie ETS 300 019-1-3 Class 3.1E Partly temperature controlled locations
24. Zalecenie ETS 300 119-2 Engineering requirements for racks and cabinets
25. Zalecenie ETS 300 119-4 Engineering requirements for shelves in miscellaneous racks and cabinets
26. Norma EN 300 386 Telecommunication network equipment; EMC Test requirements, Electrostatic discharge
27. Standard IEEE 802.3 – podstawowy zestaw standardów definiujących technologię Ethernet, w tym podstawowy schemat ramki i metody transmisji
28. PN-EN 60825-2:2005 + A1:2007 Bezpieczeństwo urządzeń laserowych - Część 2: Bezpieczeństwo światłowodowych systemów telekomunikacyjnych
29. PN-EN 61300-3-29:2008 "Światłowodowe złącza i elementy bierne -- Podstawowe procedury badań i pomiarów -- Część 3-29: Badania i pomiary - Technika pomiaru do określania transmitancji widmowej elementów DWDM."

### 3.2 Symbolika i oznaczenia wykorzystane w projekcie



Router Szkieletowy



Router dystrybucyjny



Przełącznik sieciowy



Firewall / Zapora Ogniowa z IPS/IDS



Urządzenie system DWDM



Elementy Systemu ZSN



Serwer



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





## 4 Charakterystyka techniczna opracowania

### 4.1 Standard nazewnictwa i numeracji elementów sieci

WS\_x – Węzeł Szkieletowy, gdzie „x” oznacza numer danego węzła szkieletowego,

WD\_x – Węzeł Dystrybucyjny, gdzie „x” oznacza numer danego węzła dystrybucyjnego,

WS\_C1\_x – Węzeł Szkieletowy klasy C1, gdzie „x” oznacza numer danego węzła szkieletowego,

WS\_C2\_x – Węzeł Szkieletowy klasy C2, gdzie „x” oznacza numer danego węzła szkieletowego,

WS\_C3\_x – Węzeł Szkieletowy klasy C3, gdzie „x” oznacza numer danego węzła szkieletowego,

WD\_D\_x – Węzeł Dystrybucyjny klasy D, gdzie „x” oznacza numer danego węzła dystrybucyjnego,

WD\_E\_x – Węzeł Dystrybucyjny klasy E, gdzie „x” oznacza numer danego węzła dystrybucyjnego,

WD\_F\_x – Węzeł Dystrybucyjny klasy F, gdzie „x” oznacza numer danego węzła dystrybucyjnego,

IXP\_x – Węzeł Wymiany Ruchu z Internetem, gdzie „x” oznacza numer danego węzła IXP,

CZS – Centrum Zarządzania Siecią we Wrocławiu

zCZS – Zapasowe Centrum Zarządzania Siecią w Świdnicy,

WWR-W\_x – Wojewódzki Węzeł Wymiany Ruchu, gdzie „x” oznacza numer danego węzła WR-W,

PPS – Pasywny Punkt Styku

RS\_C1\_x – Router Szkieletowy model C1, gdzie „x” oznacza numer danego węzła szkieletowego,

RS\_C2\_x – Router Szkieletowy model C2, gdzie „x” oznacza numer danego węzła szkieletowego,

RS\_C3\_x – Router Szkieletowy model C3, gdzie „x” oznacza numer danego węzła szkieletowego,

RD\_E\_x – Router Dystrybucyjny model E, gdzie „x” oznacza numer danego węzła dystrybucyjnego,

DWDM\_x – Urządzenie DWDM, gdzie „x” oznacza numer danego węzła szkieletowego lub dystrybucyjnego,

PSZ\_x – Przełącznik Sieci Zarządzającej, gdzie „x” oznacza numer danego węzła szkieletowego lub dystrybucyjnego,

FW\_CZS\_x – Firewall CZS/zCZS, gdzie „x” oznacza numer danego FW

PCZS\_x – Przełącznik Sieciowy CZS

SZS – System Zarządzania Siecią

SPSS – System Prezentacji Stanu Sieci

WWR-M – Międzynarodowy Węzeł Wymiany Ruchu

ZSN – Zintegrowany System Nadzoru

ODF – ang. Optical Distribution Frame

## 4.2 Topologia i organizacja logiczna sieci

Architektura zaprojektowanej sieci wynika przede wszystkim z fizycznych uwarunkowań sieci oraz z logicznego podziału na funkcjonalności poszczególnych węzłów. Blokowy schemat rozptywu włókien przedstawiono na rysunku numer 1, natomiast topologię geograficzną połączeń tras światłowodowych DSS ukazano na rysunku numer 2.

System DWDM służy jako transport dla warstwy usługowej IP. W jego ramach zaprojektowano połączenie ze sobą węzłów szkieletowych (WS) i węzła dystrybucyjnego (WD) w Oleśnicy. Projekt systemu DWDM wyskalowano tak, aby możliwe były zarówno: dzierżawienie długości fali („ $\lambda$ ”) tylko w oparciu o DWDM (tzn. bez angażowania urządzeń IP), jak i przenoszenie ruchu IP klientów oraz ruchu własnego IP Operatora. W wyniku przeprowadzonych analiz przyjęto, że inicjalnie jedynie 5 węzłów dystrybucyjnych sieci DSS zostanie wyposażone w sprzęt aktywny IP umożliwiające podłączenie klientów końcowych. W pozostałych węzłach dystrybucyjnych jedynym zaprojektowanym sieciowym urządzeniem aktywnym będzie przełącznik sieci zarządzającej.

Rysunek 3 przedstawia schemat zaprojektowanej sieci IP w warstwie szkieletowo – dystrybucyjnej.

Rysunek 4 prezentuje schemat zaprojektowanej sieci transportowej DWDM.

Rysunek 5 przedstawia schemat ogólnej struktury sieci.

### 4.3 Wymagania w zakresie separacji transmisji danych

W warstwie IP wymaga się zastosowania technologii opartej na połączeniach wirtualnych (VPN) zestawianych w warstwie drugiej lub trzeciej modelu OSI wraz z odpowiednimi mechanizmami konwergencji, odpowiednio na bazie protokołów VLAN lub IP MPLS. Takie rozwiązanie gwarantuje odpowiednią niezawodność, skalowalność, szybkość procesu przywrócenia usługi po awarii światłowodu oraz elastyczność zarządzania rozległą siecią szkieletową.

### 4.4 Założenia techniczne

Celem projektu jest zbudowanie wysokowydajnej i redundantnej sieci szkieletowo - dystrybucyjnej opartej na transmisji 10 i 100 Gb/s. W projekcie przyjęto, iż system DWDM służy do połączenia ze sobą relacji między węzłami szkieletowymi (WS) i węzłem dystrybucyjnym (WD) w Oleśnicy.

Połączenia fizyczne zostały tak zaprojektowane, aby o ile to możliwe, żadne połączenie między dwoma węzłami szkieletowymi nie wykorzystywało tej samej trasy kablowej. Ich liczba została zminimalizowana tylko do takich przypadków, które łączą bezpośrednio dwa węzły fizycznym medium bez przebiegania przez inny węzeł szkieletowy, z zastrzeżeniem, że na niektórych odcinkach włókna biegą tą samą drogą fizyczną (w tym samym kablu, zgodnie z rysunkiem 1).

Połączenia węzłów dystrybucyjnych zaprojektowano w taki sposób, aby każdy węzeł dystrybucyjny połączony był do dwóch różnych węzłów szkieletowych lub do węzła szkieletowego i węzła dystrybucyjnego lub do jednego WS lub WD ale dwoma parami włókien.

Ruch generowany z Pasywnych Punktów Styku (PPS) oraz z połączeń bezpośrednio w WD będzie agregowany w lokalizacjach węzłów dystrybucyjnych (WD) i wymieniany z węzłami szkieletowymi (WS), które również będą posiadały funkcję agregacji.

Agregacja odbywać się będzie poprzez podłączenie urządzenia IP klienta, wyposażonego w interfejs optyczny, bezpośrednio do routera dystrybucyjnego (lub szkieletowego) znajdującego się w jednej z 14 lokalizacji umieszczonych w tabeli 6.1 (węzły klasy Cx, D, E, F, zCZS).

Fizyczne połączenie włókien światłowodowych nastąpi w sposób pasywny w PPS lub poprzez krosowanie połączeń między urządzeniem klienta a urządzeniem sieci DSS które zostanie wykonane w WD lub WS.

System DWDM ma zapewnić transport dla połączeń IP o przepływności i topologii wynikających z przeprowadzonej analizy, jak również możliwość zestawienia kanału optycznego pomiędzy dwoma

dowolnymi lokalizacjami sieci DSS, w których zaplanowano urządzenia DWDW (wszystkie WS i WD Oleśnica).

W węzłach szkieletowych sieci IP założono łączenie funkcji P i PE w jednym urządzeniu.

W wyniku przeprowadzonej symulacji przyporządkowano poszczególnym węzłom, gdzie umieszczony zostanie sprzęt aktywny kategorii ze względu na ich rodzaje i wielkości, z zachowaniem poniższych zasad:

1. węzeł szkieletowy kategorii C 1-3: „obsadzony infrastrukturą pasywną optyczną poszerzony o elementy systemu xWDM (DWDM) oraz elementy realizujące funkcje IP”,
2. węzeł dystrybucyjny kategorii D: „obsadzony infrastrukturą pasywną optyczną, poszerzony o elementy sieci zarządzającej”,
3. węzeł dystrybucyjny kategorii E: „obsadzony infrastrukturą pasywną optyczną, poszerzony o elementy systemu IP/Ethernet”,
4. węzeł dystrybucyjny kategorii F: „obsadzony infrastrukturą pasywną optyczną, poszerzony o elementy systemu xWDM (DWDM) i poszerzony o elementy systemu IP/Ethernet”.

Gdzie: 1-węzeł mały, 2 - węzeł średni, 3 – węzeł duży.

Tabela 6.1 zawiera listę węzłów wyposażonych w sprzęt aktywny umożliwiający podłączanie klientów, wraz z przyporządkowaną im kategorią.

Zarówno w szkielecie, jak i dystrybucji sieci IP rekomendowana jest separacja ruchu klientów za pomocą L2 i L3 VPN lub równoważny w zależności od potrzeb biznesowych i uwarunkowań klientów.

W zakresie doboru urządzeń aktywnych rekomenduje się, żeby sieć DSS była oparta na konfiguracji sprzętowej zapewniającej bardzo dużą dostępność sieci.

W sieci DSS konieczna i wymagana jest implementacja sprzętu klasy operatorskiej. Urządzenia klasy operatorskiej posiadają pasywną szynę danych, a wszystkie moduły są redundantne i wymienne w czasie pracy urządzenia. Dzięki temu w urządzeniach tych nie występują element SPOF (ang. single point of failure). Rekomenduje się by sieć zbudowana w oparciu o taki sprzęt zapewniała niezawodność sięgającą poziomu 99,999%. Aby zapewnić dużą dostępność całej architektury sieci szkieletowej DSS należy zastosować szereg równoległych mechanizmów niezawodnościowych. Projekt wymusza zastosowanie niżej wymienionych mechanizmów w ten sposób obniżając perspektywę strat ruchu, skrócenie przerwy w dostępności usług oraz podwyższenia parametry SLA. Na

urządzeniach szkieletowych i o ile to możliwe, również na dystrybucyjnych, należy zadbać o uruchomienie poniższych funkcjonalności i zastosować się do poniższych wskazówek:

1. Redundancja zasilaczy – Wszystkie urządzenia aktywne sieci szkieletowej: routery IP w węzłach dystrybucyjnych i szkieletowych oraz urządzenia DWDM muszą posiadać redundantne zasilacze mogące pracować przy wykorzystaniu różnych obwodów zasilania.
2. Redundancja modułów liniowych – w przypadku, gdy węzły szkieletowe podłączone są między sobą zagregowanym łączem (np. 2x10 Gb/s), Wymagane jest by każde z łącz kończyło się na różnych kartach liniowych. Pozwala to uniknąć przerwy w przypadku awarii jednej z nich.
3. Szybka zbieżność protokołów routingu (ang. Fast Convergence) – routery typowych sieci NGN umożliwiają uzyskanie zbieżności protokołu routingu, (czyli odnalezienie i zainstalowanie nowych ścieżek po awarii) w czasie poniżej jednej sekundy. Należy włączyć mechanizmy Fast Convergence, dla użytych w konfiguracji sieci protokołów IP (rekomendowany IS-IS. Dalsze obniżenie czasu zbieżności powinno być zrealizowane przy pomocy protokołu BFD (ang. Bidirectional Forwarding Detection).
4. Szybkie przekierowanie ruchu, FRR (ang. Fast Re-Route) – w ramach protokołu MPLS należy skorzystać z mechanizmu szybkiego przekierowania ruchu (ang. Fast ReRoute), który umożliwia przeniesienie ruchu na predefiniowaną zapasową ścieżkę natychmiast po wykryciu awarii. Daje to czasy odtworzenia usługi ok. 50ms.
5. Mechanizmy odtworzenia stanu protokołów, GR (ang. Graceful Restart) – wiele protokołów posiada funkcjonalność szybkiego odtworzenia stanu, gdy sąsiedzi wspomagają taki proces np. po przełączeniu urządzenia na zapasowy moduł sterujący. Funkcjonalność taka jest nazywana Graceful Restart (GR). Jest ona wykorzystywana jednocześnie z funkcjonalnością Non-Stop Forwarding (NSF), czyli podtrzymania przełączania ruchu na podstawie starych informacji jeszcze zanim zostanie odtworzony nowy stan protokołów.
6. Mechanizmy zachowania stanu protokołów, NSR (ang. Non Stop Routing) – należy włączyć mechanizm zachowania stanu wewnątrz urządzenia, co pozwala na płynne przejęcia obsługi protokołów routingu przez zapasowy moduł sterujący.
7. Redukcja czasu uaktualniania oprogramowania, ISSU (ang. In-Service Software Upgrade) – mechanizmy uaktualniania oprogramowania różnią się zakresem w zależności od implementacji rozwiązania przez danego producenta, począwszy od instalowania łatek (ang. patch), poprzez dodawanie/usuwanie całych modułów, małą zmianę wersji systemu (np. 6.1 - > 6.2), aż po kompletną wymianę wersji (np. 6.x -> 7.x). Tym niemniej wymusza się w urządzeniach IP sieci DSS mechanizmów wspomagających aktualizacje pozwalającą na



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



znaczącą redukcję czasu trwania okien serwisowych, oraz ewentualnych przerw w świadczeniu usług.

Dodatkowo wymaga się:

1. Wyposażenia każdej klasy węzłów sieci DSS w sprzęt modularny, modele z jednej rodziny sprzętowej wybranego przez Operatora producenta urządzeń IP i DWDM. Modularność urządzeń DWDM i IP zapewnia Operatorowi możliwość zmiany pojemności i przepustowości sieci w oparciu o aktualne zasoby sprzętowe, jedynie poprzez np. manipulację obsadzeniem kartami liniowymi urządzeń IP czy elementów systemu DWDM.
2. W zależności od lokalizacji logicznej węzła szkieletowego i stawianych mu wymagań, co do liczby interfejsów koniecznych do obsługi połączeń szkieletowych i dystrybucyjnych, dokonano podziału węzłów klasy C na podklasy: C1, C2 i C3 (od najmniejszego do największego). Dotyczy to zarówno wyposażenia węzłów w sprzęt DWDM, jak i klasy IP. Zaprojektowany podział służył określeniu czy w związku z niejednorodnym obsadzeniem kartami liniowymi poszczególnych węzłów szkieletowych nie może zaproponować w mniejszych węzłach mniejszych gabarytowo modeli urządzeń transmisyjnych. Również węzły dystrybucyjne wyposażone w mniejszą liczbę kart liniowych, będą mogły w ten naturalny sposób być zamontowane w mniejszej gabarytowo obudowie, tzw. chassis z mniejszą liczbą dostępnych slotów. W związku z powyższymi założeniami wymaga się, aby urządzenia pochodziły z jednej rodziny modeli sprzętowych w celu umożliwienia przenoszenia modułów pomiędzy lokalizacjami w zależności od potrzeb przyszłych operatora sieci DSS.

W zakresie sieci transportowej, system DWDM musi wykorzystywać 1 łącze 100 Gb/s w głównym pierścieniu Wałbrzych – Wrocław - Legnica i od 2-4 łącz 10 Gb/s na pozostałych relacjach. Dodatkowo system powinien być tak wyposażony, by umożliwić zestawienie 1 lub 2 dowolnych łącz (oprócz 100G) między dwoma dowolnymi węzłami szkieletowymi zgodnie z opisem na rysunku 4 bez ponoszenia dodatkowych kosztów, co w skalowaniu ujęto jako kolejne interfejsy po stronie klientckiej i odpowiednio rozbudowaną stronę liniową w każdym z 10 węzłów w których stanie sprzęt DWDM.

W zakresie bezpieczeństwa i kontroli dostępu do urządzeń sieciowych, dostęp zdalny musi być zabezpieczony poprzez:

1. wykorzystanie wyłącznie bezpiecznych, szyfrowanych protokołów dostępowych do interfejsów administracyjnych urządzeń (np. SSH dla CLI, HTTPS dla GUI),
2. dostęp do interfejsów zarządzania będzie zabezpieczony osobistymi kontami administratorów w CZS i zCZS,
3. rejestrowane w systemie wszelkich działań administratorów,



4. zsynchronizowanie zegarów wszystkich urządzeń z tym samym serwerem NTP.

W sieci DSS zostanie zbudowana wydzielona sieć zarządzająca na potrzeby zarządzania infrastrukturą aktywną oraz na potrzeby Zintegrowanego Sytemu Nadzoru, obejmującego podsystemy:

1. kontroli dostępu,
2. monitoringu CCTV,
3. sygnalizacji przeciwpożarowej,
4. systemu sygnalizacji włamania i napadu.

Zgodnie z wymaganiami Unii Europejskiej, niniejszy projekt nie obejmuje szczegółów implementacyjnych i konfiguracyjnych urządzeń (szablonów konfiguracji) ze względu na konieczność zachowania neutralności technologicznej i umożliwienia wyboru najlepszego rozwiązania spośród rozwiązań różnych producentów. Szczegółowe elementy implementacyjne powinny zostać opracowane w ramach Planu Wdrożenia, po wyborze konkretnego rozwiązania i dostawcy. Dodatkową zaletą takiego podejścia jest to, że wybór urządzeń spełniających opisane wymagania dokona się bezpośrednio przed rozpoczęciem fazy wykonawczej projektu, co zagwarantuje ich możliwie najwyższą aktualność technologiczną.

## 4.5 Wymagania ogólne dla urządzeń sieciowych podlegających dostawie

Wymagania ogólne dotyczące urządzeń:

1. całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży danego producenta,
2. dostarczone urządzenia muszą być nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem), nieużywane, (przy czym dopuszcza się, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, (w takim przypadku Wykonawca będzie zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem),
3. całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów, której wymiar będzie podlegać ustaleniom wynikającym z Umowy między Wykonawcą a Zamawiającym,

4. zamawiający może zażądać testów poszczególnych funkcjonalności przed wyborem oferty,
5. dostarczone oprogramowanie musi być w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 3 miesiące) na dzień poprzedzający dzień składania ofert,
6. oferowane urządzenia w dniu składania ofert nie mogą być wytypowane przez producenta do wycofania z produkcji lub sprzedaży,
7. dostarczane urządzenia powinny być kompletne pod kątem wymagań im stawianym oraz celu, któremu mają służyć. Urządzenie kompletne oznacza urządzenie spełniające wszystkie wymagania wskazane w niniejszym projekcie wraz z pełnym okablowaniem (np. kable zasilające) i akcesoriami (np. wkładki SFP), niezbędnymi do jego uruchomienia.

Szczegółowe zestawienie montowanych urządzeń wg lokalizacji węzłów zamieszczono w tabeli 6.2, natomiast szczegółowe zbiorcze zestawienie urządzeń aktywnych zamieszczono w tabeli 6.3.

#### 4.5.1 Wymagania w zakresie zarządzania i monitorowania urządzeń sieciowych

Sieć DSS do prawidłowego działania musi posiadać mechanizmy zapewniające sprawną i szybką reakcję na zaistniałe problemy, pozwalające szybko ocenić stan sieci, bez konieczności przeglądania stanu każdego urządzenia z osobna. Również zmiany konfiguracji urządzeń, szczególnie związanych z zapewnieniem, uzgodnionego z klientem w kontrakcie SLA (ang. Service Level Agreement), poziomu usług, wymaga narzędzi pozwalających przeprowadzać je globalnie dla dużej liczby urządzeń jednocześnie z poziomu Centrum Zarządzania Siecią.

Wymagania stawiane urządzeniom sieciowym w zakresie zarządzania są następujące:

1. Urządzenia muszą wspierać standardowe mechanizmy monitoringu stanu połączeń takie jak:
  - a) 802.1ag - wykrywanie usterek w łączności (ang. CFM, Connectivity Fault Management),
  - b) 802.3ah – obsługa zagnieżdżonych nagłówków Ethernet (ang. Provider Backbone Bridges, PBB).
2. Urządzenia muszą być zarządzane poprzez:
  - a) interfejs CLI (konsolę).
  - b) SNMP v1, SNMP v2, SNMP v3 lub inny otwarty protokół.



3. Urządzenia IP powinny mieć możliwość tworzenia i przywracania kopii zapasowych konfiguracji z pamięci lokalnej urządzenia lub serwera, import i export wersji tekstowej z i na komputer typu PC
4. Plik konfiguracyjny urządzenia powinien być zabezpieczony przed niepożądanym dostępem oraz zmianami – tylko osoby uwierzytelnione powinny posiadać dostęp do pliku konfiguracyjnego.

#### 4.5.2 Wymagania ogólne dla urządzeń szkieletu sieci

Wymagania ogólne stawiane routerom szkieletowym zostały zawarte w punkcie 3.3.3 "Węzły szkieletowe" dokumentu "Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II". Należy pamiętać, iż w sieci DSS role węzłów agregacyjnych pełnią także routery szkieletowe, co ma swoje odzwierciedlenie w szczegółowych wymaganiach technicznych dla routerów szkieletowych. Można, zatem wyróżnić następujące wymagania:

1. wydajność, pozwalająca na przesyłanie zagregowanych strumieni ruchu,
2. przepustowość rzędu kilkuset Gb/s. Oznacza to kilkanaście portów 10 Gb/s przeznaczonych na łączność między węzłami szkieletowymi lub porty 100 Gb/s oraz kilkanaście do kilkudziesięciu portów 10 Gb/s przeznaczonych do podłączenia innych typów węzłów. Dodatkowo kilkanaście do kilkudziesięciu portów 1 Gb/s na połączenia klienckie,
3. sprawne zarządzanie ruchem i rozwiązywanie problemów, – co oznacza dostępność mechanizmów typu inżynieria ruchu, oraz narzędzi wspomagających sprawdzanie działania usług i łącz,
4. skalowalność, czyli możliwości rozbudowy. Modularność i zapas przepustowości pozwalają to osiągnąć,
5. obsługę ruchu multicastowego zgodnie z przyjętą polityką i świadczonymi usługami,
6. generowanie statystyk ruchowych w celu usprawnienia inżynierii sieci, projektowania rozwoju łącz oraz kontroli przepustowości i parametrów ruchowych dla poszczególnych usług,
7. nawiązywanie i terminowanie połączeń usługowych, w tym VPN warstwy trzeciej oraz drugiej, tranzyt ruchu IPv4/v6,
8. gwarancje jakości usług na poziomie zagregowanym, na podstawie klas ruchowych,
9. urządzenia szkieletowe powinny być w pełni modularne i zapewniać redundancję głównych elementów: zasilania, modułów sterujących, matrycy przełączającej bez konieczności wyłączania urządzenia; rekomenduje się by również moduły wentylacji zapewniały

redundancję bez konieczności wyłączania urządzenia, jakkolwiek ostateczną decyzję w zakresie uwzględnienia rekomendacji pozostawia się Operatorowi Infrastruktury,

10. urządzenia powinny mieć możliwość rozbudowy o kolejne porty 100 Gb/s na potrzeby przewidywanego rozwoju usług i ruchu w sieci.

#### 4.5.3 Wymagania ogólne dla urządzeń warstwy dystrybucyjnej

Wymagania ogólne stawiane routerom dystrybucyjnym zostały zawarte w punkcie 3.3.4 "Węzły agregacyjne" dokumentu "Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II". Typowa funkcjonalność oczekiwana od urządzeń warstwy dystrybucyjnej to:

1. przynależność do z tej samej rodziny modeli sprzętowych, co routery szkieletowe,
2. wydajność, rzędu kilkudziesięciu do kilkuset Gb/s, w zależności od wielkości danego węzła i liczby obsługiwanych klientów. Oznacza to kilkanaście portów 10 Gb/s przeznaczonych na łączność do węzłów szkieletowych oraz kilkanaście do kilkudziesięciu portów 1 Gb/s na połączenia klienckie,
3. implementacja brzegowej polityki bezpieczeństwa, zapewniającej blokowanie ruchu, który nie jest zgodny z przyjętymi zasadami, (np. adresy źródłowe spoza zakresu klienta, lub docelowe z sieci operatorskiej),
4. implementacja brzegowej polityki gwarancji jakości usług, zapewniającej przyjmowanie ruchu jedynie w ramach kontraktów oraz jego znakowanie w celu prawidłowego przetwarzania w ramach kolejnych węzłów,
5. obsługa ruchu multicastowego zgodnie z przyjętą polityką i świadczonymi usługami,
6. generowanie statystyk ruchowych w celu usprawnienia inżynierii sieci, projektowania rozwoju łączy oraz kontroli przepustowości i parametrów ruchowych dla poszczególnych usług,
7. nawiązywanie i terminowanie połączeń usługowych, w tym połączeń wirtualnych – L2/L3 VPN a także tranzyt ruchu IPv4/v6.

Urządzenia agregujące mają zwykle architekturę modułarną i w pełni redundantną. Wyjątkiem bywają tu węzły małe, gdzie możliwości techniczne i koszty zapewnienia pełnej redundancji są nadmierne. Stosuje się wówczas urządzenia o architekturze stałej, z redundancją zasilania, lecz z pojedynczymi modułami sterującymi.

#### 4.5.4 Wymagania ogólne dla sieci i przełączników sieci zarządzającej PSZ

Sieć zarządzania DSS oparta zostanie o przełączniki sieci zarządzającej PSZ, które połączone będą ze sobą siecią niezależną od sieci produkcyjnej DSS. Sieć zarządzania zestawiona będzie w oparciu o parę włókien (duplex), w relacjach punkt-punkt pomiędzy poszczególnymi lokalizacjami WD i WS. Niezależnie od tych połączeń, osobne łącza (VLAN) dla sieci zarządzającej i ZSN należy zaaranżować na łączach szkieletowych i dystrybucyjnych, wykorzystując połączenia między urządzeniami szkieletowymi i dystrybucyjnymi. Dla zapewnienia bezpieczeństwa transmisji i jej odseparowania od ruchu produkcyjnego sieć zarządzania będzie wydzielona w warstwie logicznej – poprzez osobne VLANy oraz dedykowaną adresację. PSZ powinny być wyposażone w interfejsy 1 Gb/s. Do PSZ podłączyć należy interfejsy zarządzania urządzeń transmisyjnych i IP oraz elementów podsystemów ZSN:

1. kamer cctv,
2. centralek alarmowych (sygnalizacji włamania i p.poż),
3. kontrolerów systemu kontroli dostępu.

Symboliczny, jak i właściwy schemat połączeń pomiędzy przełącznikami PSZ znajdują się na rysunkach 9 i 9A.

Wymagania ogólne dla przełącznika sieciowego IP sieci zarządzającej:

1. dla wszystkich węzłów szkieletowych (w tym w WS/CZS we Wrocławiu) oraz dla węzła dystrybucyjnego w Oleśnicy należy przewidzieć co najwyżej 2 urządzenia typu Przełącznik Sieci Zarządzającej (PSZ).
  - a. pierwszy PSZ będzie pełnił rolę agregatora optycznego dla sieci zarządzającej oraz Zintegrowanego Systemu Nadzoru zgodnego z rodziną standardów 1000BASE-X (tj. zapewniającego wsparcie dla minimum LX, SX, ZX), wyposażonego w wymaganą w danym węźle liczbę wkładek optycznych typu ZX. Będzie on kierował informacje z poszczególnych elementów systemu ZSN, poprzez węzły szkieletowe do Centrów Zarządzania Siecią (CZS/zCZS).
  - b. drugi PSZ będzie pełnił rolę przełącznika sieciowego pracującego w standardzie co najmniej 100BASE-T z obsługą standardu IEEE 802.3at (PoE+). Będzie on kierował informacje z poszczególnych elementów systemu ZSN za pośrednictwem agregatora optycznego (pierwszy PSZ), do którego będzie bezpośrednio, lokalnie podłączony, poprzez węzły szkieletowe do Centrów Zarządzania Siecią (CZS/zCZS),

2. dla wszystkich węzłów dystrybucyjnych (oprócz węzła dystrybucyjnego w Oleśnicy) PSZ będzie pełnił rolę zarówno agregatora optycznego jak i przełącznika sieciowego; wymaga się zgodności z rodziną standardów 1000BASE-X (tj. zapewnienia wsparcia dla minimum SX, LX, ZX), wyposażenia w odpowiednią dla danego węzła liczbę wkładek optycznych typu ZX oraz w porty w standardzie co najmniej 100BASE-T z obsługą standardu IEEE 802.3at (PoE+). Będzie on kierował informacje z poszczególnych elementów systemu ZSN zlokalizowanych w danym WD, za pośrednictwem zespólnego agregatora optycznego poprzez węzły szkieletowe do Centrów Zarządzania Siecią (CZS/zCZS).

#### 4.5.5 Wymagania ogólne dla infrastruktury punktów wymiany ruchu IXP

Wymiana ruchu z operatorami lokalnymi odbywa się w węzłach dystrybucyjnych lub szkieletowych, zaś w ustalonych węzłach wymiany ruchu (ang. IXP, Internet eXchange Point) oraz punktach styku możliwa jest wymiana ruchu z ogólnopolskimi, europejskimi lub światowymi operatorami telekomunikacyjnymi. .

Urządzenia dedykowane do obsługi punktów wymiany ruchu to przede wszystkim skalowalne routery IP umożliwiające zaawansowane przetwarzanie ruchu pod względem filtrowania na zgodność z politykami oraz przetwarzanie informacji routingu.

Punkt styku IXP powinien między innymi zapewniać dostęp do światowych zasobów sieciowych. Protokołem routingu wymaganym do użycia na styku z dostawcami łączy do sieci Internet jest BGP. Ze względu na olbrzymią liczbę operacji w pamięci RAM urządzenia (wpisy do tablicy routingu BGP), styk zapewniać musi odpowiednią skalowalność i oraz mechanizmy umożliwiające świadczenie w sposób niezawodny i bezpieczny usługi o wysokich parametrach jakościowych.

W przypadku routerów dedykowanych do obsługi punktów styku IXP istotnymi, wymaganymi właściwościami są:

1. wysoka niezawodność i ciągłość świadczenia usług osiągnięta przez redundancję połączeń, urządzeń, modułów lub oprogramowania zarządzającego routerami,
2. wysoka wydajność umożliwiająca realizację wymaganych usług (peering BGP, Quality of Service,
3. zaawansowanie mechanizmy Quality of Service umożliwiające elastyczną konfigurację wielu usług i polityk,
4. wsparcie dla protokołów sieciowych uruchomionych na routerach szkieletowych, w celu elastycznej współpracy w ramach całej sieci,
5. wsparcie dla protokołu IP w wersji 6.

Punkt styku do każdego z operatorów telekomunikacyjnych powinien charakteryzować się redundancją na poziomie fizycznym tj., połączeniem dwoma różnymi torami do różnych urządzeń brzegowych, czyli w sposób zdublowany do szkieletu sieci. Takie rozwiązanie pozwala na rozłożenie obciążenia związanego z obsługą ruchu, a w przypadku awarii jednego z nich zapewnia ciągłość działania usługi dostępu do Internetu. Dwa punkty styku zapewniają również ciągłość działania sieci nawet w sytuacji awarii jednego z węzłów.

Wymagania oraz ograniczenia technologiczne wyłonionych w przetargu operatorów, udostępniających łącza telekomunikacyjne, mogą być zróżnicowane. Opisane w tej części ogólne wymagania dotyczące urządzeń zapewniają dużą elastyczność i możliwość spełnienia tych najbardziej typowych. Ze względu na brak konieczności stosowania dodatkowych urządzeń do konwersji sygnałów, jako najtańszą inwestycyjnie opcję przewidziano wykonanie styku do operatora w technologii 1 Gb/s, a połączenia między węzłami wymiany ruchu i połączenia do węzłów szkieletowych łączami o prędkości 10 Gb/s. Router musi mieć możliwość rozszerzenia o kolejne porty 10 Gb/s w przypadku konieczności zastosowania takiego połączenia również z innym operatorem.

#### 4.5.6 Wymagania ogólne dla Węzłów Wymiany Ruchu WWR

Węzły Wymiany Ruchu – (wojewódzkie i międzynarodowe) są to węzły, których zadaniem jest zapewnienie punkt styku do wymiany ruchu między sieciami przyległymi geograficznie do sieci DSS np. sieciami szkieletowymi innych województw czy nawet regionów innych państw.

W ramach projektu sieci DSS zaprojektowano dwa Węzły Wymiany Ruchu z Wielkopolską Siecią Szerokopasmową (WSS). Wybudowane punkty styku będą miały charakter pasywny. Fizyczne połączenie sieci będzie zrealizowane w dwóch miejscach: w Węźle Dystrybucyjnym Cieszków oraz w miejscowości Syców (w mufie kablowej). Połączenia fizycznie należy zakończyć na routerze WS Wrocław i/lub WD Oleśnica. O rodzaju interfejsów optycznych zdecydują Operatorzy Infrastruktury DSS i WSS Preferowane są interfejsy dalekiego zasięgu 1 Gb/s lub 10 Gb/s Ethernet. Możliwe jest również połączenie na bazie systemów DWDM, dzięki zastosowaniu funkcjonalności „przenoszenia obcej lambdy”, co również umożliwiłoby terminację połączeń w WD Oleśnica lub WS Wrocław.

Oprócz ww. zaprojektowanych dwóch Węzłów Wymiany Ruchu z Wielkopolską Siecią Szerokopasmową możliwe są inne punkty styku do wymiany ruchu między sieciami przyległymi geograficznie do sieci DSS, które wystąpić mogą w następujących węzłach:

1. styk z projektami lokalnymi (4 węzły): WS\_8 Rudna, WD\_14 Głogów, WD\_17 Grębocice, WD\_22 Jerzmanowa,

2. styk wojewódzki (9 węzłów): WD\_2 Bierutów, WD\_4 Brzeg Głogowski, WD\_13 Dziadowa Kłoda, WD\_16 Góra Śląska, WD\_43 Niechlów, WD\_61 Sarby, WD\_75 Wiązów, WD\_76 Wierzbo, WD\_83 Ziębice,
3. styk międzynarodowy (5 węzłów): WD\_29 Kudowa Zdrój (Czechy), WD\_39 Międzylesie (Czechy), WD\_52 Pieńsk (Niemcy), WD\_67 Szklarska Poręba (Czechy), WD\_82 Zgorzelec (Niemcy).

Ze względu na możliwość zaistnienia konieczności realizacji któregoś z ww. punktów styku projektant powinien uwzględnić miejsce na rozszycie wszystkich włókien, które będzie wymagało zaangażowania 2 półek przełącznic, każda o wysokości 3U oraz 2 półek na zapasy patchcordów (każda o wysokości 3U).

#### 4.5.7 Wymagania ogólne dla systemu DWDM

System DWDM musi umożliwiać budowę traktów i węzłów transmisyjnych optycznej sieci transportowej, umożliwiając transmisję sygnałów optycznych o różnej strukturze ramkowania (np. SDH, Ethernet). System DWDM musi gwarantować interoperacyjność usług. Trakty transmisyjne DWDM będą zestawiane z wykorzystaniem par włókien światłowodowych (po jednym włóknie dla każdego kierunku transmisji).

Urządzenia systemu DWDM muszą być skalowalne - powinna być możliwa ich stopniowa rozbudowa. Przy projektowaniu warstwy transportowej sieci w oparciu o DWDM należy uwzględnić:

1. jednolitość technologiczną zastosowanego rozwiązania,
2. maksymalny zasięg użyteczny,
3. rodzaj kanałów GigabitEthernet wymaganych do transportu.

Urządzenia DWDM muszą spełniać aktualne standardy ITU-T i ETSI z zakresie struktury, realizowanych funkcji, wymagań środowiskowych i klimatycznych, kompatybilności elektromagnetycznej, zasilania i uziemiania tj.:

1. urządzenia DWDM nie powinny stanowić jakiegokolwiek niebezpieczeństwa dla personelu w trakcie instalacji, eksploatacji i utrzymania,
2. bloki i moduły mogące stanowić zagrożenie (np. nadajniki laserowe) muszą mieć stałe oznakowanie ostrzegawcze,
3. wszystkie laserowe źródła światła powinny być automatycznie wyłączane (ang. ALS – Automatic Laser Shutdown lub APSD – ang. Automatic Power ShutDown) w przypadku zaniku



sygnału optycznego (np. przerwanie światłowodu, rozłączenie złącza optycznego) w jakiegokolwiek części drogi optycznej.

Budowa urządzeń DWDM musi być modularna, dając możliwość szybkiej wymiany pojedynczych podzespołów oraz elastyczną rozbudowę systemu. Preferowane jest by obudowa urządzeń instalowanych w węzłach sieci, umożliwiała wykonywanie wszelkich czynności eksploatacyjnych i utrzymaniowych od strony frontowej np. wymianę modułów, interfejsów, połączeń kablowych itd. Urządzenia DWDM muszą umożliwiać instalację w standardowych stojakach 19”.

W zakresie zasilania system DWDM musi spełniać następujące wymagania:

1. urządzenia muszą być wyposażone w zaciski ochronne w celu ich uziemienia,
2. urządzenia muszą być przystosowane do zasilania z dwóch niezależnych źródeł prądu przemiennego o napięciu znamionowym 230V,
3. urządzenia muszą działać poprawnie w przypadku uszkodzenia jednego z obwodów zasilania. Uszkodzenie to nie może powodować przerwy w pracy dowolnego elementu systemu DWDM, a w szczególności nie może mieć wpływu na serwisy przenoszone przez sieć. Urządzenia muszą poprawnie pracować w przypadku zasilania tylko z jednego układu,
4. urządzenia powinny posiadać mechanizm automatycznego wyłączenia systemu, nie powodujący uszkodzeń, przy spadku napięcia zasilającego, poniżej określonej wartości progowej – np. przy osiągnięciu wartości granicznych układów zasilania, podczas pracy baterijnej,
5. po awarii układu zasilania i ponownym włączeniu napięcia zasilającego, system musi automatycznie odtworzyć konfigurację i wszystkie przenoszone usługi sprzed awarii. Poprawna transmisja wszystkich serwisów musi być przywrócona w czasie nie dłuższym niż kilka minut od momentu przywrócenia zasilania,
6. Dostawca systemu musi dostarczyć niezbędne okablowanie umożliwiające podłączenie urządzenia do źródeł zasilania.

W zakresie warunków klimatycznych i środowiskowych:

1. urządzenia powinny spełniać normy przechowywania zgodne z zaleceniem „ETSI ETS 300 019-2-1 T 1.2 Specification of Environmental test: Storage”,
2. urządzenia powinny spełniać normy transportu zgodnie z zaleceniem „ETSI ETS 300 019-2-2 T 2.3 Specification of Environmental test: Transportation”,
3. urządzenia DWDM powinny spełniać warunki kompatybilności elektromagnetycznej (ang. EMC - Electromagnetic Compatibility) zgodnie z zaleceniem „EN 300 386-2:V1.1.3, 1997-12”.

Rekomenduje się by rozwiązanie sprzętowe DWDM było otwarte na wprowadzenie mechanizmów GMPLS i zintegrowanie ich z odpowiednikami funkcjonalnymi po stronie pakietowych urządzeń przełączających (router'y i switch'e).

Rozwiązanie sprzętowe DWDM powinno być otwarte na zastosowanie techniki OTN (zgodnie z Rekomendacją ITU-T G.709) posiadającej zintegrowane przełącznice elektroniczne z realizacją:

1. szybkiego przełączania ruchu w celu zestawiania ścieżek oraz ich zabezpieczania, bez ograniczeń występujących w wersji czysto optycznej,
2. agregacji strumieni o niższej przepustowości w strumieniu zbiorcze w celu optymalizowania sposobu zagospodarowania poszczególnych kanałów optycznych.

Orientacyjne długości relacji pomiędzy poszczególnymi węzłami systemu DWDM, wyliczone wartości dyspersji chromatycznej i tłumienności konieczne do zaprojektowania systemu znajdują się odpowiednio w tabelach 6.5, 6.6 i 6.7. Wartości te muszą zostać zweryfikowane przez Wykonawcę z dokładniejszymi (określonymi ostatecznie w projektach budowlanych i wykonawczych DSS) parametrami relacji światłowodowych, przed przystąpieniem do wyboru systemu DWDM.

#### 4.5.8 Wymagania ogólne dla infrastruktury CZS i zCSZ

Centrum Zarządzania Siecią (ang. Network Operating Center, NOC) to miejsce, zespół zasobów ludzkich i środków infrastrukturalnych, w którym agregowana jest informacja o parametrach oraz stanie, urządzeń, łączy i usług, a także skąd wykonywane są operacje takie jak zmiany konfiguracji, uaktualnianie oprogramowania urządzeń oraz wdrażanie nowych usług i podłączanie nowych klientów.

Dlatego też w projekcie przewidziano istnienie Centrum Zarządzania Siecią (Wrocław) i zapasowego Centrum Zarządzania Siecią (Świdnica), jak i zaplanowano wyposażenie go w niezbędny sprzęt oraz dedykowane oprogramowanie, które będzie pełniło funkcje takie jak:

1. automatyczne zbieranie informacji z urządzeń sieciowych,
2. wykrywanie błędów i problemów w czasie rzeczywistym,
3. wykrywanie urządzeń i połączeń, szczegółowy podgląd topologii, analiza połączeń warstwy drugiej i trzeciej modelu OSI,
4. narzędzia do zarządzania listą urządzeń, oprogramowaniem i ich konfiguracją,
5. diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,



6. generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji,
7. monitorowanie i ewentualnie autoryzowanie urządzeń przyłączających się do sieci,
8. przetwarzanie zebranych informacji poprzez inteligentne filtrowanie oraz ich korelowanie by wykryć te szczególnie istotne i zaprezentować je w czytelnej formie zespołowi utrzymania sieci,
9. monitorowanie i zbieranie informacji na temat wydarzeń związanych z naruszaniem polityki bezpieczeństwa, atakami oraz anomaliami i podejmowanie skutecznych działań zapobiegawczych,
10. konfigurowanie poszczególnych urządzeń zarówno z poziomu CLI jak i graficznego interfejsu użytkownika.

Platforma Zarządzania urządzeniami sieciowymi (IP i DWDM) eksploatowana w ramach DSS musi posiadać grupę cech umożliwiających zarówno zarządzanie zaimplementowanymi urządzeniami, usługami i technologiami, jak i przewidywanymi do wdrożenia w przyszłości. To oznacza, iż zaprojektowana platforma musi być:

1. modularna i skalowalna – rozmiar sieci, jej konfiguracja oraz stosowane technologie ulegają ciągłym zmianom. Platforma zarządzania musi umożliwiać dostosowanie do zmian dokonanych w sieci,
2. zorientowana geograficznie - sieci telekomunikacyjne mają strukturę hierarchiczną i sposób zarządzania poszczególnymi jej elementami często zależy od ich rzeczywistej lokalizacji. Platforma powinna, więc odzwierciedlać nie tylko logiczną, ale i geograficzną strukturę sieci,
3. niezawodna – w miejscach krytycznych dla platformy i systemu zarządzania szczególnie narażonych na utratę danych i funkcjonalności, muszą być zaimplementowane sprzętowe i programowe mechanizmy gwarantujące zachowanie danych i funkcji systemu,
4. otwarta – oprócz rozwoju systemów telekomunikacyjnych występuje ewolucja otoczenia i systemów wspomagających zarządzanie przedsiębiorstwem. Stąd też zastosowana platforma musi posiadać mechanizmy umożliwiające współpracę z każdym stosowanym powszechnie standardem wymiany informacji funkcjonującym w tym zakresie w technologiach IT,
5. bezpieczna – system zarządzania ze względu na charakter informacji przez niego generowanej i przepływającej, powinien posiadać wbudowane mechanizmy kontroli i stopniowania dostępu do zasobów i wykonywanych operacji. Ponadto informacja przenoszona pomiędzy poszczególnymi węzłami systemu powinna być zabezpieczona przed niepożądanym dostępem.

Realizacja powyższych obszarów stanowi minimum, które powinien udostępniać operatorom sieci system (lub systemy) zarządzania. System winien być rozszerzony o dodatkowe możliwości:

1. wizualizacji topologii łączy i urządzeń, w tym inwentaryzacji automatycznej wraz z możliwością eksportu do systemu ewidencji (paszportyzacji) (np. jako moduł w ramach systemu zarządzania konfiguracjami, lub awariami),
2. wprowadzania usług (ang. provisioning) tj. podłączania kolejnych klientów i usług w sposób zautomatyzowany i dostosowany do procesów operatora sieci.

W ramach projektów wykonawczych części pasywnej CZS (nr projektu: DT-W/658/12) i zCZS (nr projektu: DT-W/658/12-ZCZS-PW) dla systemu zarządzania zaprojektowana zostanie lokalna sieć LAN (część pasywna) łącząca:

1. serwery działające pod jego kontrolą i przyjmujące dane pochodzące z urządzeń,
2. wszystkie elementy centrum zarządzania,
3. niezbędne zabezpieczenia (firewall) zapobiegające atakom na centrum.

Konfiguracja urządzeń CZS i zCZS leży w gestii Operatora Infrastruktury – Projektant nie narzuca tutaj szczegółowej konfiguracji.

Urządzenia potrzebują także dodatkowych informacji pochodzących z rozmaitych elementów systemu zarządzania, na przykład informacji o autoryzacji i uprawnieniach użytkowników, przesyłane zwykle za pomocą takich protokołów jak: RADIUS, TACACS+ lub LDAP. System musi zapewnić interoperacyjność w tym zakresie.

#### 4.5.8.1 Wymagania w zakresie niezawodności i wydajności CZS i zCZS

Ze względu na krytyczne znaczenie centrum zarządzania siecią dla operatora, oraz dla klientów usług, centrum zduplikowano dla uzyskania niezbędnej redundancji geograficznej. Centrum podstawowe (CZS) będzie zlokalizowane przy WS Wrocław, zaś centrum zapasowe (zCZS) - w Świdnicy.

Informacje o sieci i usługach będą przesyłane przez urządzenia w sposób aktywny (alarmy SNMP, syslog czy też statystyki ruchowe typu Netflow/cflow), oraz pasywny (uzyskiwane przez odpytywanie SNMP, zdalne wykonywanie komend poprzez interfejs CLI lub XML). Funkcjonalność typu Netflow/cflow, aby miała użyteczną wartość, powinna być realizowana sprzętowo i w sposób rozproszony (na poszczególnych kartach liniowych).

#### 4.5.8.2 Wymagania w zakresie zarządzania i bezpieczeństwa CZS i zCZS

Zasoby CZS muszą być w odpowiedni sposób chronione przez nieautoryzowanym dostępem osób trzecich (ochrona przed niszczeniem, modyfikacją, przechwytywaniem danych, blokowaniem usług i serwerów, wykonywaniem nieautoryzowanych transakcji). Dlatego koniecznym jest zastosowanie urządzenia zabezpieczającego typu Firewall (ściany ogniowej), które zapewni możliwość przepuszczania/filtrowania ruchu tych użytkowników do poszczególnych urządzeń CZS, z dokładnością do określonych usług udostępnianych przez serwery.

Dodatkowo, zaplanowana infrastruktura sieciowa zawiera urządzenie zabezpieczające sieć, realizujące funkcjonalność IPS – (ang. Intrusion Prevention System). Funkcjonalność ta polega na:

1. analizowaniu ruchu pod kątem znanych i zdefiniowanych rodzajów (tzw. sygnatur) ataków, i w razie wykrycia ataku podejmowania określonych, skonfigurowanych działań,
2. wykrywaniu nadużyć związanych z nieprawidłowym wykorzystaniem protokołów ,
3. wykrywanie anomalii związanych z ruchem sieciowym.

W Centrum Zarządzania Siecią muszą zostać przygotowane odpowiednie warunki do monitorowania, wprowadzania zmian oraz reagowania na zdarzenia w sieci. Zarządzanie obejmuje następujące obszary:

1. utrzymanie i monitorowanie sieci DSS,
2. zarządzanie usługami oraz definiowanie nowych usług i ich wdrażanie,
3. rozwój sieci, w tym rozbudowa sieci, dołączenia nowych klientów, testy i odbiory,
4. zarządzania bezpieczeństwem w sieci,
5. przygotowywanie raportów na temat stanu sieci, poziomu bezpieczeństwa.

### 4.6 Infrastruktura węzłów dolnośląskiej sieci szerokopasmowej

Węzły sieci DSS zostaną wyposażone w infrastrukturę pasywną pozwalającą na zapewnienie wymaganej docelowej pojemności połączeń. Połączenia pomiędzy urządzeniami aktywnymi a przełącznikami światłowodowymi należy wykonać patchcord-ami SC/APC. Długość patchcordów należy dobrać tak, aby zapewnić wygodne połączenie między przełącznicą a urządzeniami, w sposób gwarantujący jego bezpieczeństwo. Dokładny opis pasywnej infrastruktury światłowodowej każdego węzła znajduje się w projektach wykonawczych opisujących infrastrukturę pasywną węzłów.

Sprzęt aktywny w węzłach będą stanowiły modułarne urządzenia DWDM oraz IP (wymagania stawiane tym urządzeniom opisano w punkcie 4.8 niniejszego projektu).

Sprzęt aktywny zostanie umieszczony w następujących miejscach:

1. CZS Wrocław i WS Wrocław - w serwerowni UMWD realizowanej w ramach projektu MIT (Modernizacja Infrastruktury Teleinformatycznej), w budynku przy ul. Mazowieckiej 15 we Wrocławiu,
2. węzły szkieletowe, zCZS w Świdnicy - w kontenerach telekomunikacyjnych,
3. węzły dystrybucyjne w zewnętrznych szafach telekomunikacyjnych (z zapewnieniem podtrzymania zasilania oraz właściwego chłodzenia).

Dla zapewnienia wystarczającej ilości miejsca na urządzenia aktywne w Węzłach Szkieletowych, CZS i zCZS przewidziano zastosowanie szaf serwerowych o gabarytach 800x1000 mm i wysokości 42U, przy czym w CZS zastosowane zostaną również szafy 45U 800x800 mm. Szafy te powinny charakteryzować się nośnością minimum 600kg i umożliwić zamontowanie ciężkich urządzeń przykręconych do profili montażowych i podpartych osprzętem mocującym. Dostawa, montaż oraz szczegółowy opis wymagań dotyczących szaf będą przedmiotem właściwych projektów wykonawczych opisujących infrastrukturę pasywną każdego węzła.

Szafy w kontenerach WS i zCZS oraz szafy w CZS powinny zostać ustawione tak, aby zapewnić strefy serwisowe zarówno z przodu jak i z tyłu. Z przodu szaf przestrzeń serwisowa obejmuje pas o szerokości minimum 0,75m, z tyłu szaf – minimum 0,60m. Szafy można łączyć bokami po dwie tak, żeby odległość między parami szaf oraz między daną parą szafy a ścianą kontenera (lub UPS-em) była nie mniejsza niż 0,60m.

W lokalizacjach Węzłów Dystrybucyjnych klasy D i E zastosowane zostaną szafy zewnętrzne o minimalnych wymiarach wewnętrznych 850/1730/2300 mm (głębokość/wysokość/szerokość). Każda szafa składać się będzie z trzech niezależnych w zakresie dostępu komór: komory na urządzenia węzła WD DSS (komora urządzeń aktywnych), komory na sprzęt kolokowany (komora urządzeń kolokowanych) oraz komory elektrycznej. W komorze urządzeń aktywnych oraz w komorze urządzeń kolokowanych zostanie przewidziany osobny przedział na urządzenia podtrzymania energetycznego (przedział na baterie zewnętrzne UPS). W komorze na urządzenia węzła WD będą dostępne dwa stelaże 19" o wysokości 22U i głębokości 0,80m. W komorze urządzeń kolokowanych jeden stelaż 19" o wysokości 22U i głębokości 0,80m. Drzwi boczne komory elektrycznej należy wyposażać w wizjer licznika energii elektrycznej oraz specjalny przepust służący do tymczasowego wprowadzenia kabla z agregatu zasilania zewnętrznego do gniazda zasilania awaryjnego z zaciskiem uziemiającym dla agregatu zlokalizowanego wewnątrz przedziału elektrycznego na szynie DIN.

W lokalizacji Węzła Dystrybucyjnego klasy F w Oleśnicy zastosowana zostanie szafa zewnętrzna o minimalnych wymiarach wewnętrznych 850/1730/3000 mm (głębokość/wysokość/szerokość). Szafa składać się będzie z trzech niezależnych w zakresie dostępu komór: komory na urządzenia

węzła WD DSS (komora urządzeń aktywnych), komory na sprzęt kolokowany (komora urządzeń kolokowanych) oraz komory elektrycznej. W komorze urządzeń aktywnych oraz w komorze urządzeń kolokowanych zostanie przewidziany osobny przedział na urządzenia podtrzymania energetycznego (przedział na baterie zewnętrzne UPS). W komorze na urządzenia węzła WD będą dostępne trzy stelaże 19" o wysokości 22U i głębokości 0,80m. W komorze urządzeń kolokowanych jeden stelaż 19" o wysokości 22U i głębokości 0,80m. Drzwi boczne komory elektrycznej należy wyposażyć w wizjer licznika energii elektrycznej oraz specjalny przepust służący do tymczasowego wprowadzenia kabla z agregatu zasilania zewnętrznego do gniazda zasilania awaryjnego z zaciskiem uziemiającym dla agregatu zlokalizowanego wewnątrz przedziału elektrycznego na szynie DIN.

Dodatkowe wyposażenie szaf w węzłach szkieletowych i dystrybucyjnych będą stanowić następujące elementy pasywne (nie wchodzące w zakres części aktywnej i zdefiniowane w projektach wykonawczych węzłów):

1. szuflady zapasu patchcordów / multipatchcordów,
2. patchcordy lub multipatchcordy,
3. listwy zasilające,
4. panele wentylacyjne,
5. przełącznice optyczne (wraz z ich dodatkowym wyposażeniem),
6. poziome organizery kablowe dla patchcordów,
7. pionowe organizery kablowe dla patchcordów,
8. patch-panele z gniazdami RJ-45,
9. zakończenia kabli liniowych operatorów zewnętrznych (opcjonalnie),
10. wymienniki wody lodowej dla klimatyzacji szaf (tylko w CZS).

Wyposażenie szaf w węzłach w pozostałe (aktywne) elementy zostało opisane w punktach od 4.6.1 do 4.6.13 dotyczących infrastruktury poszczególnych węzłów.

Poniżej zamieszczono szczegółowe wymagania minimalne, dotyczące ww. elementów pasywnych wchodzących w skład wyposażenia szaf (uszczegółowienie wymagań w stosunku do „Wymagań technicznych DSS”):

1. szuflady (półki) zapasu patchcordów przeznaczone do magazynowania zapasów długości aktywnych patchcordów, zainstalowanych w przełącznicy światłowodowej nie posiadającej systemu zarządzania sznurami optycznymi, lub gdy wykorzystanie takiego systemu jest w danym przypadku niemożliwe lub niecelowe; szuflady muszą spełniać następujące wymagania:

- a) możliwość instalowania w szafach i stojakach na 19" profilach montażowych,
  - b) możliwość indywidualnego magazynowania patchcordów (wraz ze złączami) w otwieranych kasetach,
  - c) gęstość upakowania: co najmniej 6 patchcordów 2J o długości do 3 m i średnicy 2,4 mm każdy (lub co najmniej 1 multipatchcord 12J o długości do 3 m) w przeliczeniu na 1U zajętej przez szufladę/półkę przestrzeni,
  - d) wysokość maksymalna: 3U (w zależności od liczby planowanych patchcordów, wraz z odpowiednią rezerwą przestrzenną), z możliwością płynnej regulacji głębokości montażu szuflady w stojaku łącznie z możliwością montażu na tylnych belkach,
  - e) wyposażone w owalne wycięcia lub specjalne przepusty do bocznego wprowadzania patchcordów,
  - f) możliwość wprowadzania patchcordów na półkę od lewej bądź od prawej strony i ich wyprowadzania w ten sam sposób lub przez górną część półki.
2. szuflady (półki) zapasu multipatchcordów przeznaczone do magazynowania zapasów długości multipatchcordów, zainstalowanych w przełącznicy światłowodowej nie posiadającej systemu zarządzania sznurami optycznymi, lub gdy wykorzystanie takiego systemu jest w danym przypadku niemożliwe lub niecelowe; szuflady muszą spełniać następujące wymagania:
- a) możliwość instalowania w szafach i stojakach na 19" profilach montażowych,
  - b) możliwość indywidualnego magazynowania patchcordów (wraz ze złączami) w otwieranych kasetach,
  - c) gęstość upakowania: co najmniej co najmniej 1 multipatchcord 12J o długości do 3 m w przeliczeniu na 1U zajętej przez szufladę/półkę przestrzeni,
  - d) wysokość maksymalna: 1U z możliwością płynnej regulacji głębokości montażu szuflady w stojaku łącznie z możliwością montażu na tylnych belkach,
  - e) możliwość wprowadzania patchcordów na półkę z tyłu,
  - f) półka zapasu multipatchcordów musi posiadać moduł zapewniający bezpieczne parkowanie pojedynczych wtyków multipatchcordu.
3. patchcordsy i multipatchcordsy muszą spełniać następujące minimalne wymagania:
- a) pojemność 2-12 włókien SM, 9/125, zakończonych wtykiem SC/APC,
  - b) kabel w powłoce typu LSZH.
  - c) tłumienność całkowita nie większa niż 0,3 dB,
  - d) tłumienność odbicia (reflektancja) nie mniejsza niż 60dB.
4. listwy zasilająca muszą spełniać następujące minimalne wymagania:
- a) wysokość 1 lub 2 U,



- b) montaż na tylnej belce,
- c) wyposażenie w minimum 6 gniazd DIN 49440, 16 A, 250 V,
- d) wyposażenie w moduł przepięciowy z filtrem przeciwzakłóceń,
- e) wyposażenie w podświetlany włącznik.

5. panele wentylacyjne muszą spełniać następujące wymagania:

- a) wysokość maksymalnie 1U,
- b) montaż w podstawach dachów oraz na 19" profilach montażowych szaf,
- c) minimalna ilość wentylatorów w panelu – 4 szt.,
- d) wyposażenie w termostat z możliwością regulacji temperatury w przedziale od 0 °C do 60 °C.

Dopuszcza się rozwiązanie z panelem wentylacyjnym umieszczonym w dachu szafy.

6. przełącznica optyczna musi posiadać następujące właściwości i realizować następujące funkcje:

- a) w zależności od typu węzła musi realizować funkcje przełączeniowe lub przełączeniowo-połączeniowe, przy czym funkcja przełączeniowo - połączeniowa może być zrealizowana poprzez zastosowanie półek wielofunkcyjnych (przełączeniowo - połączeniowych) lub odrębnych półek jednofunkcyjnych (półek połączeniowych i półek przełączeniowych):
  - funkcje przełączeniowo - połączeniowe - spawania włókien kabla z luźnymi tubami, nie zakończonych złączami wielowłóknowego kabla stacyjnego (kabel IFC - włókna w ścisłych tubach) lub nie zakończonych złączami kabla wielopigtajlowego (kabel break-out) z pigtailami i przełączanie tych pigtaili na patchcordy; funkcja uwzględnia możliwość lokowania połączeń spawanych niektórych włókien (na tackach) równolegle z przełączaniem w pozostałych włókien,
  - funkcje przełączeniowe – przy użyciu patchcordów – zakończonych złączami kabla wielopigtajlowego (kabel break-out) lub zakończonych złączami wielowłóknowego kabla stacyjnego (kabel IFC - włókna w ścisłych tubach),
  - funkcje połączeniowe - magazynowania spawów kabla zewnętrznego z innym kablem zewnętrznym bądź z kablem wewnątrz-budynkowym; magazynowania spawów kabla zewnętrznego lub kabla wewnątrz-budynkowego z pigtailami; magazynowania spawów kabla zewnętrznego lub kabla wewnątrz-budynkowego z zakończonymi złączami kablem wielowłóknowym typu IFC (włókna w półścisłych tubach); magazynowania wzajemnych spawów pigtaili,
- b) organizacja przełączania w kasetach (wykluczone przełączanie przednie) pozwalająca na:
  - zarządzanie patchcordami (w płaszczyźnie poziomej),
  - uzyskanie pełnego dostępu do obu stron złącza rozłączalnego,



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



- uniknięcie niekontrolowanych zapasów długości patchcordów przy przełączaniu do innych złączy w obrębie tej samej kasety lub półki,
  - instalację różnych typów adapterów złączy rozłączalnych, w szczególności SC/APC i LC/APC,
  - prowadzenie i ochronę sznurów optycznych za pomocą elementów zapewniających kontrolowane promienie gięcia włókien,
- c) możliwość przełączania na jednej kasecie i pomiędzy kasetami tej samej półki,
- d) pojemność złączy: nie mniej niż 48 pól przełączeniowych lub spawów w przeliczeniu na każde zajęte 1U,
- e) możliwość instalowania w szafach i stojakach na 19" profilach montażowych,
- f) przystosowanie do prowadzenia kabli stacyjnych i liniowych oraz patchcordów w systemie bocznym (ang. side-access),
- g) obudowa przełącznicy musi być wyposażony w owalne otwory w bokach korpusu do bezpiecznego prowadzenia kabli liniowych i stacyjnych (pełne przecięcia z boku półek i w lejkowych wlotach sznurów optycznych, ułatwiające przełączanie patchcordów wewnątrz szafy / stojaka),
- h) możliwość zakańczania kabli z boku lub z tyłu półki,
- i) możliwość spawania wstążek włókien,
- j) możliwość integracji rozgałęźników optycznych,
- k) możliwość opcjonalnego magazynowania zapasów długości patchcordów,
- l) wyposażona fabrycznie instalowane w półce tuby prowadzące włókna i elementy do kontroli promienia gięcia włókien pozwalające na uzyskanie łatwego i jednocześnie kontrolowanego dostępu do włókien i spawów,
- m) wyposażona w niezbędną (zależną od liczby kabli) liczbę rozdzielaczy tub, stelaży zapasów tub, oraz złączy SC/APC (wraz z uwzględnieniem niezbędnych rezerw opisanych w Wymaganiach technicznych DSS).
7. poziome organizery kablów muszą spełniać następujące wymagania:
- a) wysokość 1U,
  - b) funkcja poprzecznej organizacji patchcordów,
  - c) montaż na 19" profilach montażowych szaf.
8. pionowe organizery kablów muszą spełniać następujące wymagania:
- a) wysokość 42U,
  - b) wymiary:
    - szerokość 90÷100 mm,



- głębokość 90÷100 mm,
- c) funkcja pionowej organizacji patchcordów,
- d) montaż na bocznej powierzchni 19" profilów montażowych szaf (przód szafy).

9. patch-panel RJ-45 musi spełniać następujące wymagania:

- a) wysokość 1U,
- b) montaż na 19" profilach montażowych szaf,
- c) rodzaj gniazda - RJ45 kat. 6, ekranowane,
- d) minimalna ilość portów - 24 .

10. wymagania dla zakończeń kabla liniowego operatora zewnętrznego określi Operator Infrastruktury.

W każdym kontenerze (węzłów szkieletowych oraz zCZS) zamontowane zostaną co najmniej: dwie szafy węzłowe, jedna szafa kolokacji oraz jedna szafa ODF (dla zakończeń kabli liniowych). W każdej z dwóch szaf węzłowych i w szafie kolokacji (19" o wymiarach 42U 800x1000mm) zamontowane będą co najmniej następujące elementy:

1. panel wentylacyjny (1 szt.),
2. listwa zasilająca (1 szt.),
3. szuflada zapasu multipatchcord (4 sztuki na każdą z szaf, montaż na przedniej i tylnej części 19" profilów montażowych szaf),
4. organizery kablów (3 sztuki na każdą z szaf, montaż na przedniej i tylnej części 19" profilów montażowych szaf),
5. pionowy organizator kablów (1 szt.),
6. zamek jednopunktowy w drzwiach (1 szt.).

W kontenerze będzie również zainstalowana szafa ODF spełniająca poniższe wymagania:

1. wysokość 42U,
2. wymiary 1200 x 600 mm,
3. drzwi przednie szklane,
4. 2 wydzielone przedziały kabli krosowych o szerokości 200 ± 250 mm każdy, wyposażone w pionowe organizery kablów oraz w boczny i tylny moduł zarządzania patchcordami, umożliwiając ich zamocowanie za pomocą opaski rzepowej,
5. rozdzielacz tub.

Szafa ODF powinna zawierać następujące elementy wyposażenia:

1. 4 przełącznice optyczne (3 + 1 jako rezerwa),
2. półki zapasu multipatchcordów (wymiały i liczba dostosowane do planowanej liczby pól komutacyjnych + rezerwa).

Z uwagi na zapewnienie ciągłości działania sieci, wszystkie węzły ulokowane w kontenerach (tj. wszystkie WS oprócz WS\_Wrocław) muszą zostać wyposażone w zasilacz awaryjny (UPS) oraz agregat prądotwórczy. WS\_Wrocław korzystać będzie z infrastruktury serwerowni projektu (MIT).

W każdej szafie zewnętrznej węzłów dystrybucyjnych zamontowane będą co najmniej następujące elementy pasywne:

1. panel wentylacyjny – na każdy rack 1 szt. (za wyjątkiem węzłów klasy E i F),
2. listwa zasilająca – na każdy rack 1 szt.,
3. organizator kablowy poziomy – na każdy rack 2 szt.,
4. przełącznica optyczna - 1 szt. w jednej komorze węzłowej (za wyjątkiem węzła klasy F w Oleśnicy – 2 szt.),
5. szuflada zapasu multipatchcordów (2 szt. - jedna w komorze węzłowej, druga w komorze kolokacji),
6. szuflada zapasu patchcordów (1 szt. na każdy rack w komorze węzłowej).

W wybranych WD alokowane zostaną 2 UPS-y. Niezależnie przewidziano przewoźne agregaty prądotwórcze rozlokowane po całym regionie, których zadaniem będzie umożliwienie utrzymania zasilania WD w energię elektryczną w razie awarii.

Szczegółowe projekty wykonawcze dla części elektrycznej w zakresie UPS, agregatów, jak również klimatyzacji i chłodzenia w WS i WD zawierają dokumenty związane:

1. DT-W/658/12-97 Projekt wykonawczy. Część elektryczna i sanitarna WS,
2. DT-W/658/12-97 STWiOR. Część elektryczna i sanitarna WS,
3. DT-W/658/12-97 Projekt wykonawczy. Część elektryczna i sanitarna WD,
4. DT-W/658/12-97 STWiOR. Część elektryczna i sanitarna WD.

#### 4.6.1 Infrastruktura Węzła Szkieletowego i CZS Wrocław WS\_C3\_10/CZS

Węzeł szkieletowy WS\_Wrocław i CZS Wrocław zlokalizowane będą w budynku przy ulicy Mazowieckiej 15 we Wrocławiu, w serwerowni na 1 piętrze oraz na parterze w pomieszczeniach 14

i 15. W serwerowni wybudowanej w ramach projektu Modernizacji Infrastruktury Teleinformatycznej (MIT) Urzędu Marszałkowskiego Województwa Dolnośląskiego, na potrzeby umieszczenia urządzeń aktywnych projektu DSS, udostępnione zostaną 3 szafy serwerowe. W pomieszczeniach nr 14 i 15 na parterze zaplanowano szafy kolokacyjne na potrzeby operatorów zewnętrznych: odpowiednio 2 szafy 19" 45U oraz jedną szafę 42U.

W każdej z pięciu szaf serwerowych w serwerowni MIT (19", o wymiarach 42U i 800x1000mm), zamontowane zostaną następujące elementy pasywne:

1. szuflada zapasu multipatchcord (4 sztuki na każdą z szaf, montaż na przedniej i tylnej części 19" profilów montażowych szaf),
2. poziomy organizator kablowy (3 sztuki na każdą z szaf, montaż na przedniej i tylnej części 19" profilów montażowych szaf),
3. pionowy organizator kablowy (1 szt.),

Dodatkowo szafę nr 16 należy wyposażyć w patch-panel RJ-45 (1 szt.).

W szafach węzła (serwerownia MIT) należy zamontować następujące urządzenia aktywne:

1. listwa zasilająca,
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcords) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Wrocław.
3. przełącznik sieci zarządzającej Typ 4,
4. przełącznik sieci zarządzającej Typ 3 (2 szt.),
5. zaporę ogniową w konfiguracji klastra (HA),
6. przełącznik sieciowy CZS,
7. serwer systemu zarządzania siecią i prezentacji stanu sieci,
8. serwery Zintegrowanego Systemu Nadzoru (ZSN).

Szafy zlokalizowane w CZS Wrocław w pomieszczeniach nr 14 i 15 będą wyposażone w następujący osprzęt:

1. w pomieszczeniu nr 14 (każda z dwóch szaf 19" o wymiarach 45U 800x800mm):
  - a) panel wentylacyjny,

b) przedziały urządzeń teletransmisyjnych kolokowanych (każdy łącznie 6U), przeznaczone na kolokację:

- zakończenia kabla liniowego operatora zewnętrznego,
- urządzenia aktywnego o nominalnym poborze mocy nie większym niż 400 W,
- opcjonalnego organizera kablowego,
- listwy zasilającej,

c) wymiennik ciepła (instalacja wody lodowej) dla klimatyzacji szafy,

2. pomieszczenie 15:

a) szafa ODF spełniająca poniższe wymagania:

- wysokość 45U,
- wymiary 1200 x 600 mm,
- drzwi przednie szklane,
- 2 wydzielone przedziały kabli krosowych o szerokości 200 ÷ 250 mm każdy, wyposażone w pionowe organizery kablowe oraz w boczny i tylny moduł zarządzania patchcordami, umożliwiające ich zamocowanie za pomocą opaski rzepowej,
- rozdzielacz tub.

Szafa ODF powinna zawierać następujące elementy wyposażenia:

- przełącznica optyczna - strona liniowa (5 sztuk),
- przełącznica optyczna - strona stacyjna (pole komutacyjne) - (3 sztuki),
- przełącznica optyczna - strona stacyjna (pole komutacyjne) - rezerwa (1 sztuka),

b) szafa kolokacyjna urządzeń Operatora Infrastruktury z bocznym wymiennikiem ciepła typu „side cooler (szafa 19” o wymiarach 42U 1100x800mm):

- listwa zasilająca (1 szt.),
- szuflada zapasu multipatchcord (4 szt.),
- poziomy organizator kablowy (2 szt.),
- pionowy organizator kablowy (1 szt.),
- patch-panel RJ-45 (2 szt.),
- przełącznik sieci zarządzającej Typ 4 (1 szt.),
- przedział na urządzenia teletransmisyjne,
- zamek jednopunktowy w drzwiach,

- boczny wymiennik ciepła (instalacja wody lodowej) typu „side cooler” o wymiarze 42U 300x800mm,

Dopuszczalne jest zastosowanie bocznego wymiennika ciepła w formie dostawianego urządzenia zewnętrznego lub zespolonego z szafą.

Wymagania dla szaf kolokacyjnych (szafy węzłowe 1 i 2 na rysunku 10) przedstawiają się następująco:

1. drzwi przednie i tylne o wysokości 6 U z blachy pełnej,
2. osłony pełne z boku szafy,
3. zamki jednopunktowe dla drzwi każdego przedziału,
4. odrębne drzwi dla każdego przedziału, poszczególne przedziały wewnątrz szafy oddzielone są za pomocą poziomych przegród perforowanych (rekomendowana siatka) z otworami bocznymi umożliwiającymi niezakłóconą cyrkulację pionową powietrza w szafie.

**Roźmieszczenie urządzeń w szafach w węźle szkieletowym i CZS Wrocław przedstawia rysunek 10. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w Węźle Szkieletowym/CZS Wrocław (w szafach serwerowni MIT) nie może przekroczyć 10kW na szafę, tj. sumarycznie 30 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.2 Infrastruktura Węzła Szkieletowego Legnica WS\_C3\_5

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C3 wraz z wymaganą optyką i okablowaniem (patchordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Legnica,

3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

**Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych klasy WS\_Cx\_x, w tym w Legnicy, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Legnica nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### **4.6.3 Infrastruktura Węzła Szkieletowego Wałbrzych WS\_C3\_9**

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C3 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Wałbrzych,
3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

**Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach, w tym w Wałbrzychu, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Wałbrzych nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.4 Infrastruktura Węzła Szkieletowego Rudna WS\_C2\_8

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C2 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Rudna,
3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

**Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ułożonych w kontenerach w tym w Rudnej przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Rudna nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.5 Infrastruktura Węzła Szkieletowego Strzelin WS\_C2\_7

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C2 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Strzelin,



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach, w tym w Strzelinie, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.

Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Strzelin nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.6 Infrastruktura Węzła Szkieletowego Kłodzko WS\_C2\_4

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C2 wraz z wymaganą optyką i okablowaniem (patchcody),
2. system DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcody) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Kłodzko,
3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach, w tym w Kłodzku, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.

Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Kłodzko nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.7 Infrastruktura Węzła Szkieletowego Jelenia Góra WS\_C2\_3

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C2 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Jelenia Góra,
3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach w tym w Jeleniej Górze przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.

Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Jelenia Góra nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.8 Infrastruktura Węzła Szkieletowego Bolesławiec WS\_C1\_1

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C1 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie

zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Bolesławiec,

3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

**Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach, w tym w Bolesławcu, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Bolesławiec nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### **4.6.9 Infrastruktura Węzła Szkieletowego Lubań WS\_C2\_6**

W kontenerze węzła szkieletowego zamontować należy:

1. router szkieletowy w konfiguracji dedykowanej dla modelu C1 wraz z wymaganą optyką i okablowaniem (patchcordy),
2. urządzenie systemu DWDM wyposażone w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Lubań,
3. przełącznik sieci zarządzającej Typ 3 (1 szt.),
4. przełącznik sieci zarządzającej Typ 4 (1 szt.).

**Rozmieszczenie urządzeń w szafach 8 węzłów szkieletowych ulokowanych w kontenerach, w tym w Lubaniu, przedstawia rysunek 11. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafach (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach Węzła Szkieletowego Lubań nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.10 Infrastruktura Węzła Dystrybucyjnego klasy „F” Oleśnica WD\_F\_47

W szafie zewnętrznej węzła dystrybucyjnego Oleśnica należy zamontować:

1. router dystrybucyjny w konfiguracji dedykowanej dla modelu E wraz z wymaganą optyką i okablowaniem (patchcordy) - 1 szt.,
2. urządzenie systemu DWDM wyposażony w panele dystrybucji zasilania, okablowanie interfejsów elektrycznych i optycznych (patchcordy) oraz niezbędne wyposażenie zapewniające uruchomienie transmisji w kierunkach zgodnych z tabelą 0 dla węzła Oleśnica 1 szt.,
3. przełącznik sieci zarządzającej Typ 3 (1 szt. w jednej komorze węzłowej),
4. przełącznik sieci zarządzającej Typ 4 (1 szt. w jednej komorze węzłowej).

Szafę telekomunikacyjną węzła dystrybucyjnego klasy F należy zaprojektować z właściwym stopniem ochrony – minimum IP54 + stosowanie filtrów przeciwpyłowych (zgodnie z Normą PN92/E-08106).

**Rozmieszczenie urządzeń w szafie zewnętrznej dla węzła dystrybucyjnego klasy F Oleśnica przedstawia rysunek 12. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafie (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy wszystkich urządzeń transmisyjnych (IP i DWDM) dostarczonych przez Wykonawcę i zamontowanych w szafie Węzła Dystrybucyjnego Oleśnica nie może przekroczyć 10kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### **4.6.11 Infrastruktura Węzłów Dystrybucyjnych klasy „E” Góra, Ścinawa, Łagiewniki WD\_E\_16, WD\_E\_59, WD\_E\_34**

W szafie zewnętrznej węzłów dystrybucyjnych Góra, Ścinawa, Łagiewniki należy zamontować następujące urządzenia:

1. router szkieletowy w konfiguracji dedykowanej dla modelu E wraz z wymaganą optyką i okablowaniem (patchordy) - 1 szt. w jednej komorze węzłowej,
2. przełącznik sieci zarządzającej Typ 1 - 1 szt. w jednej komorze węzłowej.

Szafy telekomunikacyjne węzłów dystrybucyjnych klasy E należy zaprojektować z właściwym stopniem ochrony – minimum IP54 + stosowanie filtrów przeciwpyłowych (zgodnie z Normą PN92/E-08106).

Rozmieszczenie urządzeń w szafie zewnętrznej dla węzłów dystrybucyjnych klasy E przedstawia rysunek 13. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafie (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.

Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie zewnętrznej nie może przekroczyć 300 kg na każdy stelaż 19”.

**Maksymalny pobór mocy wszystkich urządzeń transmisyjnych dostarczonych przez Wykonawcę i zamontowanych w szafie Węzła Dystrybucyjnego WD\_E\_x nie może przekroczyć 8kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### **4.6.12 Wymagania ogólne dla infrastruktury węzłów dystrybucyjnych klasy „D” WD\_D\_x**

Inicjalnie są to węzły bez sprzętu aktywnego do podłączenia klientów końcowych (wszystkie WD oprócz WD Ścinawa, Góra, Łagiewniki, Oleśnica, zCZS Świdnica). Wyposażenie węzłów dystrybucyjnych klasy D w zakresie urządzeń sieciowych będzie składać się tylko z przełącznika sieciowego sieci zarządzającej PSZ. Pełnić on będzie rolę urządzenia dostępowego dla kamer systemu CCTV opartego o kamery IP, sygnalizacji przeciwpożarowej oraz systemu sygnalizacji włamania i napadu, systemu kontroli dostępu. W przyszłości będzie możliwe przyłączenie do niego interfejsów zarządzających urządzeniami aktywnymi, dostawionych do węzła w skutek prawdopodobnej rozbudowy czy zmiany organizacyjnej sieci.

Rozbudowa sprzętu aktywnego w tych węzłach będzie możliwa staraniem Operatora Infrastruktury, stosownie do potrzeb, bądź poprzez nowe inwestycje, bądź poprzez przemieszczenie niewykorzystywanego sprzętu z innych węzłów.

W szafie zewnętrznej węzłów dystrybucyjnych klasy D należy zamontować przełącznik sieci zarządzającej Typ 1 lub 2 zgodnie z Tabelą 4.1 - 1 szt. w jednej komorze węzłowej.

Szafy telekomunikacyjne węzłów dystrybucyjnych klasy D należy zaprojektować z właściwym stopniem ochrony – minimum IP54 + stosowanie filtrów przeciwpyłowych (zgodnie z Normą PN92/E-08106).

**Rozmieszczenie urządzeń w szafie zewnętrznej dla węzłów dystrybucyjnych klasy D przedstawia rysunek 14. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafie (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie zewnętrznej nie może przekroczyć 300 kg na każdy stelaż 19”.**

**Maksymalny pobór mocy wszystkich urządzeń transmisyjnych dostarczonych przez Wykonawcę i zamontowanych w szafie Węzła Dystrybucyjnego WD D x nie może przekroczyć 6 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.13 Infrastruktura zCSZ Świdnica

Pomieszczenia operatorów zapasowego Centrum Zarządzania Siecią węzła zCZS Świdnica znajdzie się w budynku dworca PKP Świdnica, natomiast część serwerowa w kontenerze stojącym ok. 30m od budynku.

W budynku znajdzie się przełącznik sieci zarządzającej do którego wpięte będą stanowiska operatorów zCZS Świdnica oraz infrastruktura budynkowa Zintegrowanego Sytemu Nadzoru ZSN. W szafie telekomunikacyjnej 19" o wysokości 12U i wymiarach od min. 550 mm x 450 mm do max. 600 mm x 500 mm znajdującej się w ww. budynku należy zamontować następujące urządzenia:

1. panel wentylacyjny (1 szt.),
2. listwa zasilająca (1 szt.),
3. przełącznica optyczna (1 szt.),

4. organizator kablowy (2 szt.),
5. patch-panel kat. 6, 24xRJ45 (1 szt.),
6. szuflada zapasu patchcordów (1 szt.),
7. przełącznik sieci zarządzającej Typ 1 (1 szt.).

W kontenerze węzła zCZS Świdnica zamontowane będą 2 szafy węzłowe, 1 szafa kolokacji oraz 1 szafa ODF, wszystkie wyposażone w osprzęt pasywny zdefiniowany identycznie jak dla szaf w kontenerach węzłów szkieletowych. W kontenerze zCZS należy zamontować:

1. router dystrybucyjny w konfiguracji dedykowanej dla klasy węzła E wraz z wymaganą optyką i okablowaniem (patchordy) - w jednej szafie węzłowej,
2. przełącznik sieci zarządzającej Typ 2 – 1 szt. w jednej szafie węzłowej,
3. zapora ogniowa w konfiguracji klastra (HA),
4. przełącznik sieciowy CZS,
5. serwer systemu zarządzania siecią i systemu prezentacji stanu sieci - w jednej szafie węzłowej,
6. serwery Zintegrowanego Systemu Nadzoru ZSN - w jednej szafie węzłowej.

**Rozmieszczenie urządzeń w szafach kontenera oraz budynku dworca zCZS Świdnica przedstawia rysunek 15. Sumaryczny wymiar wszystkich urządzeń zamontowanych w szafie (liczba zajętych „U”) nie może przekroczyć wymiarów określonych na tym rysunku.**

**Maksymalna waga urządzeń zainstalowanych w pojedynczej szafie serwerowej nie może przekroczyć 500 kg.**

**Maksymalny pobór mocy urządzeń dostarczonych przez Wykonawcę i zamontowanych w szafach zCZS Świdnica nie może przekroczyć 18,2 kW.**

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.



#### 4.6.14 Punkty dostępu do Internetu (IPX)

Urządzenia pełniące funkcję routerów wymiany ruchu (IXP), przyłączone będą do szkieletu sieci za pomocą dwóch łączy w standardzie 10 Gb/s, podłączonych do dwóch różnych węzłów szkieletowych: Wrocław, Legnica.

Z uwagi na bezpieczeństwo urządzeń oraz potrzebę zapewnienia nieprzerwanej pracy połączenia projektowanej sieci szkieletowej z siecią Internet, zaprojektowano użycie dwóch urządzeń do obsługi oddzielonych geograficznie lokalizacji:

1. IXP\_1 Wrocław, ul. Joannitów 13 – kolokacja TK Telekom,
2. IXP\_2 Wrocław, ul. Bernardyńska 4 – kolokacja TP S.A.

Łączność pomiędzy nimi w oparciu o protokół BGP odbywać się będzie w za pomocą łączy w standardzie 10 Gb/s

Ze względu na niemożność określenia specyfiki teletransmisyjnej łączy operatorów zewnętrznych, dostępnych w chwili uruchamiania sieci w punktach IXP, możliwy jest jedynie ich ogólny opis. Wstępnie założono, że możliwe będzie nawiązanie połączeń w standardzie Gigabit Ethernet z użyciem modułów światłowodowych SFP/XFP. Szczegóły operatorskiego punktu styku zawierać powinien Plan Wdrożenia.

Schemat logiczny podłączenia routerów IXP z siecią szkieletową zawiera rysunek 6.

Routerzy wymiany ruchu, przeznaczone do obsługi połączeń z IXP\_1 i IXP\_2 można zainstalować w szafach węzła szkieletowego Wrocław lub w lokalizacjach Punktów Wymiany Ruchu (do decyzji Operatora infrastruktury). Do obydwu lokalizacji IXP doprowadzone zostaną kable 72J z WS Wrocław, które zostaną rozszyte obustronnie na przełącznicach optycznych.

Po stronie Operatora Infrastruktury pozostanie ustalenie ewentualnych warunków kolokacji sprzętu aktywnego w w/w lokalizacjach IXP\_1 i IXP\_2 (w przypadku jeśli podejmie on decyzję o umieszczeniu tam routerów).

Wykonawca zobowiązany jest do dostarczenia wszystkich kabli (krosowych miedzianych i światłowodowych oraz kabli zasilających) niezbędnych do podłączenia i uruchomienia wszystkich dostarczonych urządzeń.

#### 4.6.15 Rozbudowa węzłów sieci DSS

W przyszłości będzie możliwa rozbudowa przepustowości szkieletu sieci poprzez agregację dodatkowych połączeń 10 Gb/s lub 100 Gb/s, ponieważ zaprojektowane urządzenia posiadają możliwość rozbudowy o kolejne porty 10 Gb/s lub 100 Gb/s oraz zapewniona jest niezbędna rezerwa eksploatacyjna włókien w relacjach WS-WS oraz WS-WD.

Ewentualna dalsza rozbudowa sieci powinna być realizowana poprzez rozbudowę kart urządzeń szkieletowych i dystrybucyjnych (zwiększanie gęstości portów oraz wydajności urządzenia), oraz zwiększenie liczby urządzeń dostępowych.

Rozbudowa sieci DSS poprzez dodawanie kolejnych kanałów powinna odbywać się bezprzerwowo, czyli bez wpływu na ruch już przenoszony.

Dla węzłów klasy „D” rozbudowę stanowić będzie dodanie i instalacja w nich urządzeń dystrybucyjnych do którym będą mogli być podłączani klienci. Tym samym węzły te zmienią kategorię na E lub F.

W przypadku rozbudowy danego kierunku transmisji DWDM o kolejne kanały optyczne (przepływności) należy najpierw doposażyć w karty, „półkę” (obudowę) dedykowaną do tego kierunku transmisji. W przypadku braku miejsca, należy zainstalować kolejną „półkę”.

W przypadku rozbudowy węzła DWDM poprzez dodanie nowego kierunku transmisji zaleca się aby dokładane karty liniowe i transpondery (muxpondery) zainstalować w nowej dedykowanej na ten kierunek „półce”. Ma to na celu zapobieżenie sytuacji, w której uszkodzenie kontrolera, chłodzenia (wentylatorów) czy zasilania obudowy wpłynęłoby na awarię więcej niż jednego kierunku transmisji.

Nowo dodawany węzeł musi być w pełni kompatybilny z istniejącą siecią, szczególnie pod względem interfejsów liniowych, klienckich oraz systemu zarządzania.

Ze względów utrzymaniowo-eksploatacyjnych zaleca się rozbudowę sieci szkieletowej sprzętem tej samej serii. Przykładem korzyści z tego wynikających może być brak konieczności wprowadzania nowych modułów do magazynu części zapasowych, czy też możliwość przenoszenia części pomiędzy węzłami w przypadku zmiany struktury sieci szkieletowej.

## 4.7 Organizacja połączeń międzywęzłowych

W głównym pierścieniu sieci, tj. między węzłami szkieletowymi Wrocław – Wałbrzych – Legnica zastosowano połączenie w technologii 1x100 Gb/s. Pozostałe połączenia międzywęzłowe tworzą pierścienie ze zagregowanych łączy o przepustowości Nx10 Gb/s. Inicjalna konfiguracja połączeń sieci powinna być zgodna ze schematami zawartymi na rysunkach 3-9A.

Topologia ta zapewnia ciągłość transmisji w przypadku awarii jednego lub dwóch łączy w tej samej relacji lub nawet kilku łączy w całej sieci szkieletowej. Również całkowita awaria jednego z węzłów szkieletowych nie przerwie poprawnego funkcjonowania sieci. Dodatkowo w przyszłości będzie możliwe dalsze skalowanie sieci szkieletowej, poprzez uruchomienie kolejnych połączeń np. 10 Gb/s. Na niezawodność wpływać będzie również stosowanie mechanizmów agregacji łączy (np. z zastosowaniem protokołu LACP bądź ECMP).

Zalecanymi mechanizmami zapewniającym wykrycie awarii łącza i przełączenie ruchu na łącza alternatywne są:

1. protokół routingu dynamicznego np. IS-IS wraz z rozszerzeniem BFD
2. protokół MPLS Fast Reroute oraz mechanizmy MPLS TE (Traffic Engineering)

Zaprojektowano schemat połączeń kablowych zapewniających optymalny poziom niezawodności w warstwie fizycznej na wypadek uszkodzenia kabla światłowodowego dla całego obszaru sieci DSS. Z wszystkich dostępnych 72 włókien światłowodowych w kablu szkieletowym OTK 72J 24 włókna zarezerwowano dla warstwy szkieletowej (połączenia pomiędzy WS i ciemne włókna do ewentualnej dzierżawy), 24 włókna dla warstwy dystrybucyjnej (dołączenie WD do WS i łączenie WD między sobą), zaś 24 włókna dla warstwy dostępowej (dołączenie pasywnych punktów styku (PPS) do WD). Schemat docelowych przepustowości i zajętości włókien światłowodowych zawarto w tabeli 6.9.

## 4.8 Charakterystyka techniczna urządzeń przeznaczonych do wybudowania sieci

### 4.8.1 Szczegółowe wymagania dla routerów szkieletowych

Wymagania na routery szkieletowe zostały szeroko zdefiniowane w punktach 3.3.3 oraz 3.6 dokumentu „Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II”, i są wiążące dla Wykonawcy - Operatora Infrastruktury w fazie wyboru inicjalnego kompletu urządzeń, finansowanego przez Województwo Dolnośląskie. Poniżej zdefiniowano dodatkowe wymagania jakościowe i ilościowe jakimi powinien charakteryzować się router szkieletowy wykorzystany w sieci DSS. Wymagania dla routerów szkieletowych poszczególnych modeli C1-3 zawarto poniżej:

1. router musi być dedykowanym urządzeniem sieciowym przystosowanym do montażu w szafie typu rack 19”,
2. router musi być urządzeniem z rozdzieloną realizacją funkcji kontrolnych od przełączania pakietów (tzw. sprzętowe przełączanie pakietów),
3. router musi mieć budowę modułową, tzn. pozwalać na wyjmowanie modułów kart liniowych, zasilaczy, modułów odpowiedzialnych za funkcje kontrolne i przełączanie pakietów,
4. router musi być wyposażony w redundantne zasilacze obsługujące napięcie zmienne 230V,
5. router musi być dostarczony z kompletnym okablowaniem, niezbędnym do jego uruchomienia,
6. zastosowane w routerze implementacje protokołów i funkcjonalności muszą być zgodne z wymienionymi w punkcie 3.6 "Kluczowe cechy routerów P i PE" dokumentu "Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II" oraz w dokumentach normatywnych.

Dodatkowo w zakresie obsługiwanych protokołów router musi:

1. obsługiwać w pełni protokół BGP wraz z funkcjonalnością Route Reflektorów,
2. obsługiwać protokoły multicastowe: PIM-SM, PIM-SSM, IGMPv2/v3, MSDP dla IPv4 i PIM-SM, MLDv1/v2 dla IPv6,
3. obsługiwać ramki Ethernet o wielkości co najmniej 9 kB,
4. być zgodnym ze standardami Ethernet OAM (IEEE 802.3ag, 802.3ah, ITU-T Y.1731) , MPLS OAM,

5. obsługiwać tagowanie 802.1Q; wsparcie dla co najmniej 4094 VLAN ID,
6. obsługiwać autoryzację administratorów za pośrednictwem serwerów autoryzacji RADIUS,
7. obsługiwać zarządzanie za pomocą szyfrowanego tekstowego interfejsu konfiguracyjnego (CLI), poprzez protokół SSH,
8. spełniać wymagania zawarte w tabeli 6.10,

Rekomenduje się, aby router obsługiwał ruch multicastowy na bazie MPLS P2MP (RSVP-TE) i w ramach IP VPN (MVPN).

W zakresie interfejsów router szkieletowy musi:

1. Dla węzła klasy C1:
  - a) posiadać co najmniej 8 interfejsów 10 Gb/s Ethernet SFP+ lub XFP (obsadzone modułami typu Single Mode) oraz co najmniej 40 interfejsów 1 Gb/s Ethernet SFP (w tym co najmniej 39 obsadzone modułami typu Single Mode Long Range oraz jeden 1000BASE-T do dodatkowego połączenia z Przełącznikami Sieci Zarządzającej),
  - b) posiadać minimum 3 sloty do obsługi kart liniowych,
  - c) oferować możliwość instalacji co najmniej 128 portów 1 Gb/s i 32 porty 10Gb/s na urządzenie,
  - d) umożliwiać instalację kart liniowych umożliwiających kształtowania ruchu w kierunku zarówno od jak i do klienta,
  - e) posiadać dedykowany interfejs zarządzania typu Ethernet RJ-45.
2. Dla węzła klasy C2 i C3:
  - a) posiadać co najmniej 12 interfejsów 10 Gb/s Ethernet SFP+ lub XFP (obsadzone modułami typu Single Mode) oraz co najmniej 40 interfejsów 1 Gb/s Ethernet SFP (w tym co najmniej 39 obsadzone modułami typu Single Mode Long Range oraz jeden 1000BASE-T do dodatkowego połączenia z Przełącznikami Sieci Zarządzającej),
  - b) posiadać minimum 5 slotów do obsługi kart liniowych,
  - c) oferować możliwość instalacji co najmniej 128 portów 1 Gb/s i 32 portów 10 Gb/s na urządzenie,
  - d) umożliwiać instalację kart liniowych umożliwiających kształtowania ruchu w kierunku zarówno od jak i do klienta,
  - e) posiadać dedykowany interfejs zarządzania typu Ethernet RJ-45.
3. Dodatkowo dla węzła klasy C3:

- a) posiadać co najmniej 2 interfejsy 100 Gb/s.

Wymaga się, aby zastosowane karty liniowe mogły być dowolnie relokowane pomiędzy routerami klasy C1, C2 i C3.

Dodatkowo rekomenduje się by węzły klas C1-C3 obsługiwały interfejsy typu Synchroniczny Ethernet (do decyzji Operatora Infrastruktury).

#### 4.8.2 Szczegółowe wymagania dla routerów dystrybucyjnych

W dziewięciu lokalizacjach routery szkieletowe pełnią również role routerów dystrybucyjnych - funkcjonalnie routery P i PE zunifikowano w jedno urządzenie, uzupełniając wymaganie o porty „klienckie”.

W pozostałych przypadkach routery dystrybucyjne muszą wypełniać założenia zdefiniowane w punktach 3.3.4 oraz 3.6 dokumentu „Wymagana techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II”, które są wiążące dla Wykonawcy - Operatora Infrastruktury w fazie wyboru inicjalnego kompletu urządzeń, finansowanego przez Województwo Dolnośląskie.

Urządzenia pełniące role routerów dystrybucyjnych powinny być urządzeniami pochodzącymi z tej samej rodziny modeli co routery szkieletowe lub też role routerów dystrybucyjnych mogą pełnić karty/moduły wyniesione routerów szkieletowych.

W tym drugim przypadku wymaganiem dodatkowym jest konieczność zainstalowania w węźle dystrybucyjnym dwóch modułów (lub kart) wyniesionych, każdego połączonych z innym routerem szkieletowym, w celu zwiększenia dostępności sieci w przypadku awarii jednego z tych routerów. Parametry wydajnościowe kart/modułów wyniesionych i liczba dostępnych interfejsów musi spełniać wymagania identyczne jak dla dedykowanych routerów dystrybucyjnych.

W przypadku niezależnego routera modularnego możliwe będzie przenoszenie kart liniowych pomiędzy urządzeniami tworzącym sieć szkieletowo-dystrybucyjną, dając przyszłemu Operatorowi Infrastruktury większą elastyczność w zarządzaniu zasobami sprzętowymi sieci DSS.

W przypadku zastosowania dedykowanych routerów w węzłach klasy E i F ich wymagane parametry określono poniżej:

1. router musi być dedykowanym urządzeniem sieciowym przystosowanym do montażu w szafie typu rack 19". Wysokość urządzenia nie może przekraczać 5RU,

2. router musi być urządzeniem z rozdzieloną realizacją funkcji kontrolnych od przełączania pakietów (tzw. sprzętowe przełączanie pakietów),
3. router musi mieć możliwość wymiany modułów kart liniowych i zasilaczy (w przypadku urządzeń modularnych).
4. router musi być wyposażony w redundantne zasilacze obsługujące napięcie zmienne 230V.

W zakresie interfejsów router musi:

1. posiadać co najmniej 4 interfejsy 10 Gb/s Ethernet SFP + lub XFP (obsadzone modułami typu Single Mode) oraz co najmniej 20 interfejsów 1 Gb/s Ethernet SFP (w tym co najmniej 19 obsadzone modułami typu Single Mode Long Range oraz jeden 1000BASE-T do dodatkowego połączenia z Przełącznikami Sieci Zarządzającej),
2. oferować możliwość instalacji co najmniej 40 portów 1 Gb/s i 6 portów 10 Gb/s na urządzenie,
3. posiadać dedykowany interfejs zarządzania typu Ethernet RJ-45.

Dodatkowo rekomenduje się by routery w węzłach dystrybucyjnych obsługiwały interfejsy typu Synchroniczny Ethernet (do decyzji Operatora Infrastruktury).

Router musi być dostarczony z kompletnym okablowaniem, niezbędnym do jego uruchomienia. Wymaga się, aby implementacje protokołów i funkcjonalności zastosowane w routerze były zgodne z wymienionymi w punkcie 3.6 "Kluczowe cechy routerów P i PE" dokumentu *"Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II"* z dokumentami normatywnymi. Z uwagi na rozwój technologii sieciowych dopuszcza się implementację w urządzeniu nowszych standardów niż (lub zastępujących) tam wymienione.

Dodatkowo w zakresie obsługiwanych protokołów router musi:

1. w pełni obsługiwać protokół BGP wraz z funkcjonalnością Route Reflektorów,
2. obsługiwać protokoły multicastowe: PIM-SM, PIM-SSM, IGMPv2/v3, MSDP dla IPv4 i PIM-SM, MLDv1/v2 dla IPv6,
3. obsługiwać ramki Ethernet o wielkości co najmniej 9 kB,
4. być zgodnym z Ethernet OAM (IEEE 802.3ag, 802.3ah, ITU-T Y.1731) oraz (w przypadku stosowania technologii MPLS) MPLS OAM,
5. obsługiwać tagowanie 802.1Q i zapewniać wsparcie dla co najmniej 4094 VLAN ID.
6. obsługiwać autoryzację administratorów za pośrednictwem serwerów autoryzacji RADIUS,



7. obsługiwać zarządzanie za pomocą szyfrowanego tekstowego interfejsu konfiguracyjnego (CLI), na przykład poprzez protokół SSH,
8. posiadać funkcjonalność tworzenia i przywracania kopii zapasowych konfiguracji z pamięci lokalnej urządzenia lub serwera, import i export wersji tekstowej z i na komputer typu PC
9. spełniać wymagania ilościowe dla parametrów zawartych w tabeli 6.11.

Rekomenduje się, aby router obsługiwał ruch multicastowy na bazie MPLS P2MP (RSVP-TE) i w ramach IP VPN (MVPN).

#### 4.8.3 Szczegółowe wymagania dla routerów punktów wymiany ruchu (IXP)

Dla punktów wymiany ruchu zastosowano dedykowane urządzenia, co pozwala odizolować sieć szkieletową od ewentualnych zaburzeń pochodzących z sieci innych operatorów, na przykład poprzez protokół BGP, które tym samym mogłyby przenosić się także na inne usługi realizowane przez to samo urządzenie (wymagania na liczbę wpisów w tablicach routingu (RIB) i forwardingu (FIB) zostały ustalone na bazie aktualnej liczby prefiksów „Globalnej tablicy BGP” dla protokołu IPv4 i IPv6 lub jako ich wielokrotność).

Poniżej zestawiono wymagania dla routerów pełniących funkcję punktów wymiany ruchu i dostępu do Internetu

Router IPX musi:

1. być dedykowanym urządzeniem sieciowym przystosowanym do montażu w szafie typu rack 19". Wysokość urządzenia nie może przekraczać 5RU.
2. być urządzeniem z rozdzieloną realizacją funkcji kontrolnych od przełączania pakietów (tzw. sprzętowe przełączanie pakietów),
3. mieć budowę modułarną, tzn. pozwalać na wyjmowanie modułów kart liniowych i zasilaczy.
4. być wyposażony w redundantne zasilacze obsługujące napięcie zmienne 230V; w przypadku zasilaczy napięcia stałego 48V należy dostarczyć osobno właściwy konwerter AC/DC o maksymalnej wysokości 3RU.

W zakresie interfejsów router musi:

1. posiadać co najmniej 4 interfejsy 10 Gb/s Ethernet SFP + lub XFP oraz co najmniej 10 interfejsów 1 Gb/s Ethernet SFP (wszystkie z optyką typu Single Mode),
2. oferować możliwość instalacji co najmniej 40 portów 1 Gb/s i 6 portów 10Gb/s na urządzenie,
3. w zakresie wydajności router musi:
  - a) przełączać pakiety co najmniej na poziomie 50Mpps,

- b) dysponować przepustowością na poziomie co najmniej 60 Gb/s,
  - c) obsługiwać liczbę co najmniej 900k wpisów w tablicy routingu dla IPv4,
  - d) obsługiwać liczbę co najmniej 900k wpisów w tablicy routingu dla IPv4 VPN,
  - e) obsługiwać liczbę co najmniej 700k wpisów w tablicy routingu dla IPv6,
  - f) obsługiwać liczbę co najmniej 64k adresów MAC,
  - g) oferować pojemność tablicy RIB na poziomie co najmniej 4mln wpisów,
  - h) oferować pojemność tablicy FIB na poziomie co najmniej 1mln wpisów.
- 4. posiadać dedykowany interfejs zarządzania typu Ethernet RJ-45,
  - 5. posiadać funkcjonalność tworzenia i przywracania kopii zapasowych konfiguracji z pamięci lokalnej urządzenia lub serwera, import i export wersji tekstowej z i na komputer typu PC,
  - 6. być dostarczony z kompletnym okablowaniem, niezbędnym do jego uruchomienia.
  - 7. w zakresie obsługiwanych protokołów router musi:
    - a) obsługiwać w pełni protokół BGP z opcją Route Reflektorów,
    - b) obsługiwać protokoły multicastowe: PIM-SM, PIM-SSM, IGMPv2/v3, MSDP dla IPv4 i PIM-SM, MLDv1/v2 dla IPv6,
  - 8. obsługiwać ramki Ethernet o wielkości co najmniej 9 kB,
  - 9. być zgodnym z Ethernet OAM (IEEE 802.3ag, 802.3ah, ITU-T Y.1731) oraz (w przypadku stosowania technologii MPLS) MPLS OAM,
  - 10. obsługiwać tagowanie 802.1Q dla co najmniej 4094 VLAN ID,
  - 11. obsługiwać autoryzację administratorów za pośrednictwem serwerów autoryzacji RADIUS,
  - 12. obsługiwać zarządzanie za pomocą szyfrowanego tekstowego interfejsu konfiguracyjnego (CLI) na przykład poprzez protokół i SSH.

#### 4.8.4 Szczegółowe wymagania dla Przełączników Sieci Zarządzającej PSZ

Wymagania na przełączniki sieciowe użyte do budowy Sieci Zarządzającej (OoB – ang. Out of Band) sformułowano poniżej.

Przełącznik musi mieć :

- 1. możliwość montażu w szafie 19",
- 2. zasilanie napięciem zmiennym 230V,
- 3. posiadać dedykowany interfejs zarządzania typu Ethernet RJ-45,



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



4. możliwość obsługi protokołów warstwy 3 i zgodność ze standardami:
  - a) IPv4: RIP, OSPF, IS-IS,
  - b) IPv6: RIPng, OSPFv3, IS-IS,
  - c) Obsługa VRRP lub odpowiednika,
  - d) Obsługa standardów IEEE 802.1Q, IEEE802.1ad, IEEE802.3ad,
5. możliwość obsługi protokołów warstwy 2 i zgodność ze standardami:
  - a) musi obsługiwać protokół STP, RSTP, MSTP,
  - b) musi obsługiwać VLAN 802.1q,
6. umożliwiać wsparcie następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
  - a) klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  - b) implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi,
  - c) implementacja algorytmu Round Robin lub podobnego dla obsługi tych kolejek,
  - d) możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  - e) obsługa IP Precedence i DSCP,
7. funkcjonalność bezpieczeństwa sieciowego:
  - a) listy kontroli dostępu (ACL) L2 i L3 (IPv4 i IPv6),
  - b) Unicast Reverse Path Forwarding (uRPF),
  - c) DHCP snooping, DHCP relay,
  - d) mechanizmy ochrony przed sztormami ruchu (ang. broadcast/multicast storm),
  - e) obsługa autoryzacji administratorów/użytkowników za pośrednictwem RADIUS,
8. wymagania dotyczące zarządzania urządzeniem:
  - a) możliwość definicji uprawnień poszczególnych administratorów urządzenia,
  - b) możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej, jak i import na urządzenie,
  - c) możliwość synchronizacji zegara czasu za pomocą protokołu NTP,
  - d) możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń regularnych,

- e) zarządzanie przez CLI (konsola szeregową, SSHv2), SNMPv3,
- f) syslog,
- g) obsługa tworzenia i przywracania kopii zapasowych konfiguracji z lokalnej pamięci urządzenia lub serwera.

Niezależnie od sformułowanych powyżej wymagań ustalono wymagania dodatkowe dla określonych poniżej typów Przełączników Sieci Zarządzającej (PSZ):

1. Typ 1

Przełącznik sieciowy o wysokości 1U posiadający minimum 8 portów w standardzie co najmniej 100BASE-T z obsługą standardu IEEE 802.3at (PoE+) oraz 2 porty zgodne z rodziną standardów 1000BASE-X (minimum SX, LX, ZX), wyposażony w 1 lub 2 wkładki SFP typu ZX (w węzłach zgodnie z Tabelą 4.1).

2. Typ 2

Przełącznik sieciowy o wysokości 1U posiadający minimum 8 portów w standardzie co najmniej 100BASE-T z obsługą standardu IEEE 802.3at (PoE+) oraz minimum 4 porty zgodne z rodziną standardów 1000BASE-X (minimum SX, LX, ZX), wyposażony w 3 lub 4 wkładki SFP typu ZX (w węzłach zgodnie z Tabelą 4.1).

3. Typ 3

Przełącznik sieciowy o wysokości 1U posiadający minimum 2 porty w standardzie co najmniej 100BASE-T oraz minimum 8 portów (rekomendowana liczba portów – 12) zgodnych z rodziną standardów 1000BASE-X (minimum SX, LX, ZX), wyposażony w odpowiednią liczbę wkładek SFP typu ZX (w węzłach zgodnie z Tabelą 4.1). W przypadku użycia PSZ Typ 3 o łącznej liczbie portów optycznych mniejszą niż 16, wymagana jest możliwość zestawiania w stos.

4. Typ 4

Przełącznik sieciowy o wysokości 1U posiadający minimum 24 porty w standardzie co najmniej 100BASE-T, z obsługą standardu IEEE 802.3at (PoE+) dla minimum 8 portów.

Tabela 4.1 Wykaz węzłów z przydziałem poszczególnych typów przełączników

Klasa przełącznika	Min. liczba portów opt.	Min. liczba portów el.	Węzły	Sumaryczna liczba przełączników w klasie	Liczba portów optycznych obsadzonych wkładkami (w przełączniku lub stosie)
Typ 1	2	8	Dziadowa Kłoda, Bierutów, Prochowice, Warta Bolesławiecka, Leśna, Wleń, Kowary, Szklarska Poręba, Łagiewniki Dzierżoniowskie, Świdnica (budynek)	10	1
			wszystkie pozostałe węzły dystrybucyjne z wyłączeniem Oleśnicy	65	2
Typ 2	4	8	Cieszków, Niechlów, Jawor, Zgorzelec, Nowa Ruda, Kudowa Zdrój, Jemna	7	3
			Świdnica (kontener)	1	4
Typ 3	8	0	Wrocław	2*	16
			Strzelin	2*	15
			Legnica	2*	12
			Kłodzko	2*	11
			Rudna	2*	10
			Oleśnica	2*	9
			Lubań	2*	9
			Jelenia Góra	1	8
			Wałbrzych	1	8
			Bolesławiec	1	5
			wszystkie węzły szkieletowe (w tym 2x Wrocław) oraz Oleśnica	11	24

\* - wymagana liczba przełączników w przypadku połączenia w stos przełączników o 8 portach optycznych (dopuszcza się zastosowanie 1 przełącznika o odpowiednio większej liczbie portów optycznych – patrz wariant rekomendowany dla PSZ Typ 3).

Schemat organizacji połączeń sieci zarządzającej ukazano na rysunku 9 i 9A.

#### 4.8.5 Szczegółowe wymagania dla urządzeń i systemów Centrów Zarządzania Siecią

Zaprojektowany schemat połączeń elementów systemu CZS z siecią szkieletową i zarządzającą prezentuje rysunek numer 7 i 8.

#### 4.8.5.1 Szczegółowe wymagania dla Przełącznika CZS

Przy specyfikacji wymagań funkcjonalnych dla przełącznika sieciowego CZS wzięto pod uwagę możliwość zastosowania urządzenia modularnego lub pary urządzeń tworzących stos. Dla przełącznika sieciowego CZS ustala się następujące wymagania:

Dla urządzenia modularnego:

1. obsługa kart wieloportowych w różnych standardach portów elektrycznych i światłowodowych,
2. obsługa portów o prędkości 1 Gb/s i 10 Gb/s,
3. redundancja krytycznych elementów urządzenia (karty zarządzające, matryca przełączająca, zasilacze),
4. obsługa portów o prędkości 1 Gb/s i 10 Gb/s dla urządzenia tworzącego stos,
5. dedykowane interfejsy o przepustowości co najmniej 32 Gb/s na potrzeby łączenia urządzeń w stos.

Pozostałe wymagania dla przełącznika CZS:

1. możliwość montażu w szafie 19",
2. zasilanie napięciem zmiennym 230V,
3. obsługa protokołów warstwy trzeciej modelu OSI i zgodność ze standardami:
  - a) IPv4: RIP, OSPF, IS-IS, PIM-SM/SSM, IGMP,
  - b) IPv6: RIPng, OSPFv3, IS-IS, PIM-SM/SSM,
  - c) VRRP lub odpowiednika,
  - d) IEEE 802.1Q, IEEE802.1ad, IEEE802.3ad,
4. funkcjonalności bezpieczeństwa sieciowego:
  - a) listy kontroli dostępu (ACL) dla warstw L2 i L3 (IPv4 i IPv6),
  - b) Unicast Reverse Path Forwarding (uRPF),
  - c) DHCP snooping, DHCP relay,
  - d) mechanizmy ochrony przed sztormami ruchu (ang. broadcast/multicast storm),
  - e) obsługa autoryzacji administratorów/użytkowników za pośrednictwem RADIUS,
5. wymagania w zakresie zarządzania urządzeniem:
  - a) definiowanie uprawnień poszczególnych administratorów urządzenia,
  - b) możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej, jak i import na urządzenie,
  - c) możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń regularnych,
  - d) zarządzanie przez CLI (konsola szeregową, SSHv2), SNMPv3,

- e) funkcja syslog,
- f) obsługa tworzenia i przywracania kopii zapasowych konfiguracji z lokalnej pamięci urządzenia lub serwera,

Przełącznik sieciowy CZS musi posiadać co najmniej 48 portów w standardzie 100/1000BASE-T oraz co najmniej 4 porty w standardzie 1000BASE-X.

Maksymalna wysokość przełącznika sieciowego CZS (pracującego w klastrze lub jako urządzenie modułowe) nie może przekraczać 4U.

#### 4.8.5.2 Szczegółowe wymagania dla Firewall z IDS/IPS

Urządzenie firewall z sondami IDS/IPS musi spełniać poniższe wymagania:

- 5. montaż w szafie 19",
- 6. zasilanie napięciem zmiennym 230V,
- 7. klasa Enterprise lub Campus,
- 8. praca w trybie wysokiej dostępności (HA) – klastr,
- 9. ściana ogniowa śledząca stan połączeń z funkcją weryfikacji informacji charakterystycznej dla warstwy aplikacji,
- 10. obsługa lub wsparcie dla protokołów i usług: DHCP (klient i serwer), listy dostępowe ACL, OSPF, 802.1Q, NAT, NetFlow lub równoważny, OSPF, PIM, IGMP, SNMP, LLDP, VRRP, GRE, IS-IS, RADIUS, TACACS+, obsługę protokołu IPv6;
- 11. sprzętowe wsparcie szyfrowania połączeń IPsec (DES, 3DES, AES 128, AES 192 oraz AES256),
- 12. wydajność w trybie firewall co najmniej 2 Gb/s dla obsługi typowego ruchu IPv4,
- 13. wydajność w trybie IPS wynosząca co najmniej 0,5 Gb/s dla obsługi typowego ruchu IPv4,
- 14. obsługa co najmniej 20 000 połączeń na sekundę,
- 15. obsługę co najmniej 250 000 jednoczesnych sesji połączeniowych,
- 16. filtrowanie alarmów,
- 17. działanie w oparciu o wzorce ataków oraz możliwość definiowania wzorców przez użytkownika,
- 18. działanie w oparciu o analizę anomalii ruchu,
- 19. aktualizacja bazy sygnatur winna odbywać się ręcznie i automatycznie,
- 20. wykrywanie i blokowanie technik i ataków (m.in. IP Spoofing, DDoS, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów,



21. zarządzanie z poziomu aplikacji z interfejsem graficznym oraz przez linię komend za pomocą szyfrowanego połączenia (protokoły SSH, HTTPS),
22. powiadamianie o zdarzeniach do systemu prezentacji stanu sieci,
23. wykrywanie ataków ukrytych w wielu następujących po sobie pakietach,
24. ograniczanie ruchu (ang. rate limiting),
25. inspekcja protokołów IP, ICMP, TCP, UDP,
26. brak ograniczeń na liczbę jednocześnie pracujących użytkowników w sieci chronionej,
27. obsługa wirtualnych interfejsów VLAN,
28. inspekcja aplikacyjna protokołów TCP/UDP,
29. wykrywanie ataków w warstwie 2 modelu OSI,
30. dedykowany port do zarządzania,
31. redundantny zasilacz.

Zgodnie ze schematem zaprojektowanego połączenia elementów CZS/zCZS, urządzenie Firewall z IDS/IPS musi dysponować co najmniej 4 interfejsami 10/100/1000BASE-T i oferować możliwość instalacji modułów rozszerzających z portami w standardzie 1000BASE-X lub 100/1000BASE-T.

Maksymalna wysokość Firewall z IDS/IPS nie może przekraczać 4U.

#### 4.8.5.3 Szczegółowe wymagania dla Systemu Zarządzania Siecią

System Zarządzania Siecią powinien stanowić pakiet oprogramowania lub oddzielne dedykowane urządzenie lub urządzenia, zgodnie z wymaganiami zapisanymi w dokumencie *"Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej część II"*. W przypadku, gdy system nie stanowi dedykowanego urządzenia wraz z oprogramowaniem musi być dostarczony serwer, który spełni wymagania aplikacji o parametrach określonych poniżej.

Dostarczony kompletny System Zarządzania Siecią musi być kompatybilny z wszystkimi aktywnymi urządzeniami sieciowymi wykorzystanymi w projekcie sieci DSS.

W zakresie funkcjonalnym dopuszcza się następujące rozwiązania:

1. jeden wspólny System Zarządzania siecią IP i DWDM,
2. jeden System Zarządzania siecią IP i oddzielny jeden System Zarządzania siecią DWDM,

W zakresie sprzętowym dopuszcza się następujące rozwiązania:

1. jedno dedykowane urządzenie dla obu systemów,

2. dwa dedykowane urządzenia dla każdego systemu z osobna - działające w środowisku wirtualnym.

Oprogramowanie lub dedykowane rozwiązanie powinno spełniać następujące wymagania:

1. Oprogramowanie do zarządzania urządzeniami sieci musi stanowić zintegrowany pakiet aplikacji do konfiguracji, administracji, monitoringu i diagnozowania sieci (dopuszczalna jest modułowa budowa rozwiązania).
2. Powyżej wymienione aplikacje/moduły muszą być dostępne poprzez graficzny interfejs użytkownika lub przeglądarkę stron WWW.
3. Oprogramowanie musi umożliwiać definiowanie spersonalizowanego interfejsu prezentującego informacje o sieci. Dostosowywanie odpowiednich widoków GUI musi być dostępne z poziomu użytkownika aplikacji/modułu.
4. System musi udostępniać standardowy interfejs, którego specyfikacja musi zostać opisana w dokumentacji w sposób umożliwiający integracje z systemami:
  - a) paszportyzacji,
  - b) „umbrella” NMS,
  - c) Fault Management,
  - d) Trouble Ticketing.
5. System musi udostępniać aktualne dane o nadzorowanych urządzeniach w postaci plików XML zawierających kompletny zrzut struktury urządzeń (drzewa) wraz z informacją o stanie urządzenia, zależnościach urządzeń oraz ze wszystkimi parametrami urządzenia. Każde urządzenie musi posiadać unikalny identyfikator, niezmienny w całym okresie istnienia urządzenia w systemie. Dane powinny być udostępniane zarówno na żądanie, jak i automatycznie z określoną częstotliwością. Częstotliwość oraz lokalizacja udostępniania danych musi być możliwa do ustalenia konfiguracyjnie.
6. W przypadku zdarzeń związanych z urządzeniami w sieci (np. wykrycia nowego urządzenia lub zmiany, wykrycia awarii) system zapewni wywołanie odpowiednich usług WebService systemu paszportyzacji z przekazaniem wszelkich danych dotyczących zdarzenia (np. wszystkie parametry i pełna struktura zmodyfikowanego urządzenia).
7. Oprogramowanie musi integrować się z oprogramowaniem klasy „umbrella” NMS (np. typu HP-OV),
8. Wymagany zakres funkcjonalności:

- a) wykrywanie błędów i problemów w czasie rzeczywistym (współpraca z serwerami NTP),
  - b) wykrywanie urządzeń i połączeń, szczegółowy podgląd topologii, śledzenie urządzeń końcowych, analiza połączeń warstwy drugiej i trzeciej,
  - c) narzędzia do zarządzania listą urządzeń (ang. inventory management), oprogramowaniem urządzeń i ich konfiguracją,
  - d) narzędzie automatycznej identyfikacji urządzeń instalowanych w sieci,
  - e) narzędzie graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia,
  - f) narzędzie identyfikujące „wąskie gardła” sieci, określanie czasów odpowiedzi urządzeń oraz czasu opóźnienia,
  - g) diagnozowanie stanu, wydajności i dostępności sieci, raportowanie w czasie rzeczywistym oraz w oparciu o dane historyczne,
  - h) generowanie szczegółowego opisu użytkowanych urządzeń i ich konfiguracji.
  - i) zbieranie statystyk co najmniej z wykorzystaniem SNMP lub RMON,
  - j) harmonogramowanie akwizycji danych z urządzeń,
  - k) harmonogramowanie wymiany danych z innymi systemami (w szczególności z systemem Paszportyzacji)
  - l) zbieranie alarmów o stanie urządzeń (np. stanie portów, wykorzystaniu procesora, nieprawidłowej pracy wentylatorów, przekroczeniu temperatury).
9. Oprogramowanie musi być dostarczone wraz z niezbędnymi licencjami pozwalającymi na objęcie monitoringiem wszystkich urządzeń i typów urządzeń zainstalowanych w sieci DSS w momencie zakończenia Projektu oraz umożliwiać dalsze skalowanie, o obsługę minimum 1 000 urządzeń sieciowych (zakup dodatkowych licencji realizowany będzie w ramach ewentualnej rozbudowy sieci),
10. W przypadku, gdy system nie stanowi dedykowanego urządzenia wraz z oprogramowaniem musi być dostarczony serwer o parametrach:
- a) umożliwiających montaż w szafie 19”, o wysokości nie większej niż 2U,
  - b) zasilany napięciem 230V (wraz z przewodami zasilającymi),
  - c) umożliwiających skalowanie rozwiązania o obsługę min. 1 000 dodatkowych urządzeń sieciowych (procesor, pamięć, dyski twarde),
  - d) zapewniających wsparcie dla środowiska wirtualnego (wraz z dostarczeniem wymaganych licencji).



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



#### 4.8.5.4 Wymagania dla Systemu Prezentacji Stanu Sieci

Przeznaczony dla Centrum Zarządzania Siecią System Prezentacji Stanu Sieci w warstwie funkcjonalnej musi:

1. komunikować się z panelami LCD, które stanowią będą ścianę graficzną (videowall) prezentującą stan sieci w danym momencie,
2. stanowić dedykowane urządzenie lub pakiet oprogramowania (dopuszczalna jest modułowa budowa rozwiązania) wraz z serwerem o odpowiednich parametrach,
3. współpracować z serwerami czasu NTP,
4. współpracować z Systemem Zarządzania Siecią oraz system klasy „umbrella NMS”,
5. prezentować i sygnalizować stan funkcjonowania wszystkich urządzeń (w sposób graficzny oraz posiadać możliwość uruchomienia i odpowiedniego przypisania sygnalizacji dźwiękowej),
6. prezentować i sygnalizować stan funkcjonowania wszystkich serwisów (np. DNS, DHCP, SYSLOG, RADIUS, LDAP, BGP),
7. prezentować i sygnalizować stan połączeń wewnętrznych w sieci DSS,
8. prezentować i sygnalizować stan połączeń do operatorów zewnętrznych,
9. prezentować i sygnalizować stan wykorzystania (użytkowania) zasobów sprzętowych (np. CPU, RAM, HDD) dla serwerów z zainstalowanym systemem operacyjnym Linux lub Windows,

Przeznaczony dla Centrum Zarządzania Siecią System Prezentacji Stanu Sieci w warstwie sprzętowej musi:

1. w przypadku dostarczenia dedykowanego urządzenia zapewnić:
  - a) obsługę interfejsów 1 GE,
  - b) możliwość instalacji w szafie 19” o wysokości nie większej niż 2U.
2. w przypadku, gdy system nie stanowi dedykowanego urządzenia wraz z oprogramowaniem musi być dostarczony serwer o parametrach:
  - a) umożliwiających prawidłową obsługę wszystkich funkcjonalności z wydajnością zapewniającą komfort użytkownika (czas odpowiedzi/wyświetlenia informacji) w (procesor, pamięć, dyski twarde),
  - b) zapewniających wsparcie dla środowiska wirtualnego (wraz z dostarczeniem wymaganych licencji).



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



#### 4.8.6 Szczegółowe wymagania dla urządzeń systemu DWDM

System DWDM dla sieci DSS musi być zaimplementowany, uruchomiony i przetestowany zgodnie z macierzą łączy, przedstawioną w tabeli 6.8. *Macierz przepustowości łączy DWDM.*

Urządzenia systemu DWDM muszą spełniać od strony klienckiej następujące wymagania:

1. transpondery i muxpondery dla sygnałów klienckich muszą być wyposażone w interfejsy, w postaci wymiennych optycznych modułów SFP/SFP+/XFP/CFP, w celu elastycznej zmiany typu i szybkości interfejsu,
2. interfejsy klienckie muszą umożliwiać współpracę z optycznymi interfejsami „kolorowymi”, w tym o długości fali z zakresu CWDM (ang. Coarse Wavelength Division Multiplexing), przy czym dopuszcza się moduły o stałej długości fali lub przestrajalne,
3. transpondery i muxpondery systemu DWDM powinny obsługiwać sygnały klienckie o przepływności 10 GbE i 100 GbE,
4. ponieważ oferta usługowa DSS powinna obejmować interoperacyjność z szeregiem innych interfejsów stosowanych w strukturach operatorskich, stąd transpondery i muxpondery systemu DWDM muszą umożliwiać współpracę z następującymi sygnałami klienckimi:
  - a) STM-1, STM-4, STM-16, STM-64,
  - b) 1 GbE (optyczny i elektryczny), 10 GbE LAN, 10 GbE WAN,
  - c) OTU-1, OTU-2, OTU-3, OTU-4,
  - d) FC (ang. Fiber Chanel) 2 Gb/s, FC 4 Gb/s, FC 8 Gb/s,
5. system DWDM musi zapewniać otwartość technologiczną, poprzez wspieranie standardu transmisji tzw. „obcej długości fali”, opisanego w ITU-T G.698.2 (ang. alien wavelength transmission).

System DWDM od strony liniowej musi zapewniać:

1. urządzenia powinny współpracować ze światłowodami o parametrach wg zaleceń ITU-T G.652 oraz G.655 w trzecim oknie transmisyjnym,
2. system DWDM powinien pracować w oparciu o siatkę częstotliwościową zgodną ze standardem ITU-T G.694.1; wymaga się żeby system bazował na odstępach międzykanałowym 50 GHz lub 100 GHz; należy zaimplementować system o następujących liczbach kanałów:
  - a) dla siatki 50 GHz – minimum 80 kanałów,
  - b) dla siatki 100 GHz – minimum 40 kanałów,



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



przy czym należy:

- c) zastosować rozwiązania, które stosują ten sam typ urządzeń do obsługi odstępu międzykanałowego 50 GHz i 100 GHz,
- d) przejście pomiędzy oboma trybami pracy powinno odbywać się na zasadzie dodania multipleksa pracującego z siatką 100 GHz, ale częstotliwościami środkowymi przesuniętymi o 50 GHz,
3. system powinien działać w oparciu o wzmacniacze optyczne EDFA, pracujące w trzecim oknie transmisyjnym na światłowodach jednomodowych,
4. ze względu na parametry systemów DWDM oraz strukturę sieci regionalnej należy założyć, iż system DWDM pracujący w paśmie może działać bez wzmacniaczy optycznych, przy czym musi gwarantować:
  - a) zapas mocy dla przęsła DWDM przyjęty w DSS,
  - b) możliwość tworzenia długodystansowych kanałów optycznych bez regeneracji 3R (odtworzenia kształtu, amplitudy i zegara sygnału),
5. w szczególnych przypadkach dopuszcza się przedłużenie zasięgu pojedynczego skoku optycznego poprzez zastosowanie wzmacniaczy Ramana; ze względu na wysoki koszt i niedogodności eksploatacyjne rozwiązanie takie może być stosowane jedynie w uzasadnionych przypadkach i tylko na najdłuższych trasach takich jak Wałbrzych-Wrocław i Wałbrzych – Strzelin.
6. transpondery i muxpondery muszą posiadać przestrajalne lasery w zakresie pasma C, długości fali od 1530 nm do 1565 nm zgodnie z siatką ITU-T G.694.1,
7. system DWDM powinien zapewniać transmisję sygnałów optycznych bez regeneracji 3R (odtworzenia kształtu, amplitudy i zegara sygnału) na dystansie do 2000 km; wartość ta wynika z łącznej długości włókien w sieci szkieletowej,
8. system DWDM powinien pozwalać na konfigurowanie węzłów do pracy w charakterze:
  - a) terminala końcowego TM (ang. Terminal Multiplexer),
  - b) optycznej krotnicy transferowej OADM (ang. Optical AddDrop Multiplexer) lub ewentualnie ROADM (ang. ReConfigurable Optical AddDrop Multiplexer),
  - c) wzmacniacza optycznego (ang. Optical Amplifier),
9. węzeł typu OADM lub ROADM powinien umożliwiać transmisję co najmniej w pięciu kierunkach, wymaga tego topologia połączeń fizycznych DSS np. WS Wrocław czy WS Legnica,
10. w przypadku zastosowania węzłów typu ROADM, muszą być one w pełni konfigurowalne z systemu nadzoru,



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



11. w przypadku zastosowania ROADM powinny one umożliwiać zamianę sygnału optycznego o dowolnej długości fali na inną oraz pozwalać na skierowanie sygnału liniowego z danego transpondera w węźle na każdy kierunek transmisji,
12. w przypadku zastosowaniu w systemie DWDM przepływności większej niż 10 Gb/s po stronie liniowej, konieczne jest zastosowanie koherentnej modulacji o dużej tolerancji na dyspersję chromatyczną, tak aby wyeliminować konieczność stosowania zewnętrznych modułów kompensujących w przypadku stosowania w sieci DWDM wyłącznie koherentnej modulacji,
13. system powinien być skalowalny, co oznacza, że każdy węzeł DWDM powinien umożliwiać rekonfigurację, bez wymiany znaczących części systemu (takich jak wzmacniacze, multiplexery i kontrolery) w przypadku zmiany:
  - a) liczby obsługiwanych kanałów optycznych w danym kierunku,
  - b) przepływności kanału optycznego po stronie liniowej, np. przejściu od systemu 10 Gb/s do 100 Gb/s,
14. w zakresie jakości transmisji wymaga się, aby stopa błędów przy transmisji sygnału 10 Gigabit Ethernet (IEEE 802.3ae LAN PHY i WAN PHY), 100 Gigabit Ethernet (IEEE 802.3ba) oraz sygnału SDH STM-64 (ITU-T G.707) była nie większa niż 10-12 dla każdego kanału optycznego; na wejściu każdego transpondera/muxpondera wymagany jest poziom OSNR gwarantujący, w zależności od prędkości transmisji i rodzaju modulacji, stopę błędów dla przenoszonych serwisów na poziomie 10-12 lub niższym,
15. system DWDM dla transmisji Ethernet musi gwarantować parametry zgodnie z RFC 2544,
16. dla sygnałów SDH wymaga się transparentnego przenoszenia sygnałów zegara,
17. system musi realizować korekcję błędów FEC (Forward Error Correction) zgodnie z zaleceniami ITU-T G.709.

Należy zastosować rozwiązanie DWDM na wysokim poziomie bezawaryjności; W odniesieniu do urządzeń DWDM należy założyć stosowanie mechanizmów zabezpieczających przed awariami sprzętowymi:

1. wszystkie stosowane urządzenia DWDM muszą posiadać podwójne obwody zasilania,
2. ze względu na imperatyw obniżania tłumienności oraz niski poziom awaryjności optycznych elementów transmisyjnych (np. multiplexery, wzmacniacze) nie przewiduje się ich dublowania,
3. przy budowie węzłów DWDM rekomenduje się dedykowanie każdemu kierunkowi transmisji oddzielnej półki (obudowy) i instalację w niej kart liniowych, transponderów (muxponderów) obsługujących tylko ten kierunek; ma to na celu zapobieżenie sytuacji, w której uszkodzenie



- kontrolera, chłodzenia (wentylatorów) czy zasilania obudowy wpłynęłoby na awarię więcej niż jednego kierunku transmisji w węźle,
4. należy przewidzieć mechanizm protekcji ruchu, który powinien gwarantować ciągłość transmisji w przypadku wystąpienia awarii, poprzez zastosowanie rezerwowych możliwości transmisyjnych tj:
    - a) w wariancie minimalnym: protekcja ścieżek, gdzie elementem przełączającym jest urządzenie klienckie (krotnica SDH, router IP itp.),
    - b) protekcja ścieżek w trybie 1+1 (sygnał dociera do odbiornika ścieżką roboczą i protekcyjną), bez dublowania transponderów/muxponderów, gdzie przełączanie odbywa się na poziomie sieci DWDM (przełączenie ruchu musi się odbyć w czasie mniejszym niż 50 ms),
    - c) w wariancie zaawansowanym dopuszcza się zaawansowane rozwiązania techniczne, rozszerzające zdefiniowane powyżej wymagania np. w oparciu o elektroniczne matryce przełączające OTN i funkcjonalności GMPLS.
  5. w przypadku zastosowania węzłów typu ROADM dopuszcza się zabezpieczanie ruchu poprzez restorację, czyli dynamiczne ustalenie rezerwowej drogi transmisji na podstawie aktualnego obciążenia sieci, po wystąpieniu awarii; podobnie jak w przypadku protekcji ruchu minimalnym rozwiązaniem jest protekcja ścieżek.
  6. w przypadku wyboru serwisów sieci DWDM do zabezpieczenia przez restorację należy pamiętać, że czas zestawienia rezerwowej drogi transmisji po wystąpieniu awarii może trwać nawet kilka minut i uwzględnić ten fakt przy kształtowaniu SLA,

System DWDM i jego elementy powinny być zarządzane zgodnie z zasadami ITU TMN (Telecommunication Management Network) oraz ISO FCAPS. System musi gwarantować zarządzanie centralne typu NMS (ang. Network Management System) oraz lokalne poprzez interfejs Ethernet. NMS powinien posiadać nowoczesny i wygodny w użyciu graficzny interfejs użytkownika (GUI). Nadto system zarządzania urządzeniami DWDM musi spełniać następujące wymagania:

1. dostęp do zarządzania lokalnego i centralnego powinien być zabezpieczony przed niepożądanym dostępem osób trzecich,
2. system zarządzania powinien umożliwiać zdalną aktualizację oprogramowania elementów sieciowych; procedura aktualizacji powinna być odporna na błędy transmisji oprogramowania do urządzeń systemu,.
3. system zarządzania musi udostępniać co najmniej następujące informacje:
  - a) moc optyczna sygnału wejściowego i wyjściowego na wzmacniaczach optycznych i transponderach,

- b) statystyki mechanizmu FEC o skorygowanych i nieskorygowanych błędach, zgodnie ze standardem ITU-T G.826,
  - c) moduły zainstalowane w urządzeniach wraz z numerami seryjnymi i numerami produktu,
  - d) wartości temperatury aktywnych modułów,
  - e) informacje o logowaniach na urządzenia,
  - f) informacje o logowaniach do NMS.
4. centralny system zarządzania NMS oraz nadzór lokalny systemu DWDM musi alarmować o:
- a) uszkodzeniu układu zasilającego,
  - b) zaniku napięcia w obwodzie zasilania,
  - c) uruchomieniu urządzenia po zaniku zasilania,
  - d) uszkodzeniu układu chłodzenia (wentylator),
  - e) zaniku sygnału optycznego po stronie liniowej na wzmacniaczu lub transponderze,
  - f) zaniku sygnału optycznego na interfejsie klienckim,
  - g) przekroczeniu zdefiniowanych progów wartości poziomów mocy odbieranych sygnałów,
  - h) przekroczeniu zdefiniowanych progów wartości temperatury,
  - i) przekroczeniu zdefiniowanych progów błędów transmisji po stronie liniowej lub klienckiej.

#### 4.8.7 Wymagania dotyczące patchcordów

Dostarczane i montowane patchcordeny muszą spełniać następujące wymagania:

1. typ duplex, tj. kabel stacyjny z dwoma włóknami jednomodowymi,
2. jednakowe zakończenia na urządzeniach (standardem zakończeń wybranym w DSS dla przełącznic jest SC/APC); rekomenduje się zastosowanie w urządzeniach sieciowych tego samego standardu, w przeciwnym przypadku tj. wyboru dla urządzeń standardu LC/APC wykonawca musi zapewnić patchcordeny o odpowiednich zakończeniach,
3. tłumienność wsteczna (reflektancja) większa od 60dB,
4. patchcordeny elektryczne muszą być zgodne z ISO/IEC 11801 i ANSI/TIA/EIA 568-B.2.

Patchcordeny należy dostarczyć w liczbie koniecznej do wykonania wszystkich krosowań wymaganych dla uzyskania sieci o opisanej topologii i przepustowości.

## 4.9 Opis czynności uruchomieniowych i wstępnej konfiguracji sieci

### 4.9.1 Przygotowanie Planu Wdrożenia

W celu uzyskania przez sieć DSS właściwej funkcjonalności oraz możliwości wykonania testów odbiorczych niezbędne jest uruchomienie i wstępne skonfigurowanie dostarczonych urządzeń aktywnych. Tryb i szczegółowy zakres konfiguracji zależy w istotny sposób od konkretnej implementacji produktowej (producenta urządzeń), która zostanie ostatecznie wybrana w postępowaniu przetargowym. Dostępne na rynku urządzenia różnych producentów, spełniające wymagania opisane w niniejszej dokumentacji, różnią się silnie pod tym względem.

W związku z powyższym niniejsze opracowanie, jako neutralne technologicznie, definiuje jedynie istotne elementy procesu uruchomienia i konfiguracji (zwanego dalej procesem wdrożenia), które muszą zostać wykonane, niezależnie od ostatecznego wyboru implementacji (producenta urządzeń). Przyjmuje się zatem, że tryb i szczegółowy zakres tych czynności zostanie zaproponowany przez Wykonawcę prac (Dostawcę urządzeń) w niezależnym dokumencie pn. Plan Wdrożenia, stanowiącym integralną część implementacji systemowej (implementacji zespołu urządzeń i oprogramowania).

Plan Wdrożenia musi zostać sporządzony przez Wykonawcę przed przystąpieniem do realizacji projektu zgodnie z wymaganiami niniejszej dokumentacji, oraz dostarczony Zamawiającemu (Inwestorowi) w terminie nie późniejszym niż 4 tygodnie od daty podpisania umowy i zarazem na co najmniej 6 tygodni przed planowaną datą rozpoczęcia prac wdrożeniowych przez Wykonawcę. Z uwagi na konieczność zaangażowania służb Zamawiającego w proces wdrożenia, Plan Wdrożenia podlega sprawdzeniu i akceptacji przez Zamawiającego, który w terminie do 2 tygodni przed planowaną datą rozpoczęcia prac wdrożeniowych może wnieść do niego swoje zastrzeżenia, uwagi lub propozycje korekt. Plan Wdrożenia musi zawierać:

1. proponowany harmonogram wdrożenia,
2. zdefiniowanie usług świadczonych w sieci DSS,
3. schemat przydzielania adresów IP dla urządzeń sieciowych (sposób adresacji węzłów i urządzeń w CZS) i użytkowników sieci (przydział adresów z puli prywatnych i publicznych),
4. konwencje nazywania urządzeń sieciowych i urządzeń w CZS,
5. szczegóły konfiguracji Punków Wymiany Ruchu IXP,
6. opis protokołów routingu używanych w sieci i sposobu ich konfiguracji,
7. opis parametrów i konfiguracji sieci zarządzającej,

8. określenie globalnych parametrów QoS (jak będzie obsługiwany ruch w zależności od kodów DSCP, CoS, EXP), propozycję podziału procentowego całego pasma na klasy ruchu,
9. określenie jak zdefiniowane powyżej usługi będą mapowane na usługi realizowane przez sieć, ze szczególnym uwzględnieniem sposobu ich konfiguracji,
10. określenie globalnych parametrów dla ruchu typu multicast,
11. opis mechanizmów równoważenia łącz,
12. określenie globalnej polityki bezpieczeństwa,
13. opis wszelkich czynności i szczegółów implementacyjnych pozwalających na osiągnięcie przez oferowany zespół urządzeń funkcjonalności opisanej w niniejszej dokumentacji (w tym treść proponowanych skryptów konfiguracyjnych),
14. zestawienie parametrów niezbędnych w procesie wdrożenia, których wartości winny być określone przez Zamawiającego przed rozpoczęciem wdrożenia,
15. zestawienie i szczegółowy opis testów akceptacyjnych, właściwych dla instalowanych urządzeń, które udokumentują spełnienie przez cały system wymagań odnośnie konfiguracji opisanej w punkcie 4.9.3 oraz jego poszczególne części, dla których wymagania określono w niniejszej dokumentacji w punkcie 4.8,
16. wykaz procedur operacyjnych dla administratorów.

Ustala się są następujące wymagania związane z wdrożeniem i uruchomieniem urządzeń aktywnych sieci DSS:

1. Proces wdrożenia winien obejmować następujące etapy:
  - a) Przedstawienie harmonogramu prac, zaakceptowanego przez Zamawiającego,
  - b) Przeprowadzenia szkoleń pracowników Zamawiającego,
  - c) Opracowanie Planu Wdrożenia, w porozumieniu z Zamawiającym, zakończone podpisaniem protokołu akceptacji/odbioru Planu. Odbiór Planu Wdrożenia będzie niezbędnym warunkiem rozpoczęcia prac konfiguracyjnych.
  - d) Dostawa i instalacja komponentów całego systemu.
  - e) Właściwa konfiguracja i uruchomienie całego systemu - przełączenie ruchu produkcyjnego na nową infrastrukturę - wg. Planu Wdrożenia sporządzonego zgodnie z wymaganiami Zamawiającego i przez niego zaakceptowanego,
  - f) Przeprowadzenie testów akceptacyjnych - walidacja rozwiązania (audyt konfiguracji) oraz testów odbiorczych – niezawodnościowych i funkcjonalnych (wymagane dostarczenie

zestawienia w postaci tabeli szczegółowo opisującej poszczególne testy wraz z wynikiem pozytywny/negatywny),

- g) Opracowanie dokumentacji powykonawczej i zaleceń powdrożeniowych, obejmującej:
- szczegółowy wykaz komponentów będących przedmiotem zamówienia oraz miejsca i sposobu ich instalacji,
  - szczegółowy schemat połączeń poszczególnych urządzeń,
  - szczegółową konfigurację poszczególnych urządzeń,
  - konfigurację usług,
  - procedury operacyjne dla administratorów,
  - instrukcje z zadaniami administracyjnymi z wydzieleniem prac codziennych, cotygodniowych, comiesięcznych i ew. innych,
  - procedury archiwizacji danych i awaryjne (ratunkowe),
  - wskazanie szczegółowego sposobu rozbudowy poszczególnych urządzeń,
  - inne istotne informacje mające wpływ na użytkowanie dostarczonych urządzeń.

2. Zamawiający wymaga, aby wszystkie prace, które mogą spowodować przestoje w pracy sieci produkcyjnej, były przeprowadzane w godzinach 16.30 – 7.30. Zamawiający dopuszcza prowadzenie prac wdrożeniowych w dni wolne od pracy po wcześniejszym uzgodnieniu terminu. Szczegółowe informacje o zakresie integracji z istniejącymi sieciami zostaną ustalone z Wykonawcą po podpisaniu umowy.

3. Ogólny opis wdrożenia

- a) Instalacja, wdrożenie i uruchomienie routerów szkieletowych i dystrybucyjnych zgodnie z wymaganiami ustalonymi z Zamawiającym.
- b) Instalacja, wdrożenie i uruchomienie urządzeń DWDM w węzłach szkieletowych i dystrybucyjnych realizujących funkcjonalności zgodnie z wymaganiami ustalonymi z Zamawiającym.
- c) Instalacja, wdrożenie i uruchomienie przełączników, urządzeń zapory ogniowej w CZS i ZCZS oraz rozwiązań bezpieczeństwa zgodnie z wymaganiami ustalonymi z Zamawiającym.
- d) Instalacja, wdrożenie i uruchomienie przełączników sieci zarządzającej, zgodnie z wymaganiami ustalonymi z Zamawiającym.
- e) Instalacja, wdrożenie i uruchomienie systemu zarządzania urządzeniami sieci DSS, systemu monitorującego sieć (w tym: korelacja zdarzeń w sieci, wykrywanie incydentów oraz informowanie zespołu administratorów o zdarzeniach) oraz systemu zarządzania dostępem do urządzeń sieciowych zgodnie z wymaganiami ustalonymi z Zamawiającym



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



- f) Instalacja, wdrożenie i uruchomienie routerów IXP, zgodnie z wymaganiami ustalonymi z Zamawiającym.
- g) Instalacja i konfiguracja wszystkich dostarczonych serwerów wraz z systemem operacyjnym i wymaganymi licencjami, jak również środowisk wirtualnych wraz z wymaganymi licencjami jeśli takie zostaną zastosowane podczas realizacji projektu.
- h) Integracja systemu zarządzania urządzeniami sieci DSS z systemem paszportyzacji DSS.

#### 4.9.2 Opracowanie polityki bezpieczeństwa

Wykonawca opracuje politykę bezpieczeństwa dla DSS. Polityka bezpieczeństwa musi być dostosowana do specyfiki działań i organizacji oraz uwzględniać możliwości wdrażanej implementacji sprzętowo-programowej. Dokument Polityki bezpieczeństwa powinien obejmować w szczególności:

1. Deklarację Zamawiającego w odniesieniu do bezpieczeństwa informacji;
2. Zakres Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
3. Deklarację Stosowania;
4. Raporty z analizy ryzyka;
5. Procedury, instrukcje i formularze niezbędne do poprawnego funkcjonowania SZBI:
  - a) procedurę reagowania na incydenty związane z bezpieczeństwem informacji;
  - b) procedurę tworzenia i zarządzania kopiami zapasowymi;
  - c) wytyczne dot. zabezpieczenia komunikacji;
  - d) wytyczne dot. zabezpieczenia przed kodem złośliwym;
  - e) wytyczne dot. ochrony przed nieuprawnionym fizycznym dostępem do aktywów (cała struktura sieci pasywa, aktywa);
  - f) wytyczne dot. ochrony przed nieuprawnionym logicznym dostępem do danych i aplikacji;
  - g) regulamin ochrony danych osobowych;
  - h) regulamin użytkownika systemu (aplikacje do zarządzania siecią);
  - i) politykę bezpieczeństwa danych osobowych ze wskazaniem na:
    - wykaz zbiorów danych osobowych przetwarzanych (pomoc z zgłoszeniu do GIODO);
    - opis przepływów danych między systemami jeśli wystąpią - to jakie, jeśli nie wystąpią - należy wyraźnie to zaznaczyć;

- określenie środków technicznych i organizacyjnych służących zabezpieczeniu sieci przed nieuprawnionym dostępem;
- wskazanie obszaru przetwarzania danych;
- opis struktury zbiorów (dostarcza wykonawca oprogramowania);
- stworzenie i podpisanie stosownych umów serwisowych oraz umowy o pomocy w zakresie nadzoru i doskonalenia SZBI.

### 4.9.3 Ramowe wymagania odnośnie konfiguracji urządzeń

Minimalne niezbędne wymagania dla skonfigurowanych funkcjonalności i parametrów Dolnośląskiej Sieci Szkieletowej w początkowym okresie jej użytkowania zostały określone poniżej.

Wykonawca jest zobowiązany wykonać szereg czynności uruchomieniowych przygotowujących dostarczoną infrastrukturę do celów operacyjnych. W skład listy czynności oprócz instalacji fizycznej urządzeń w węzłach aktywnych dochodzą minimalne czynności konfiguracyjne zapewniające możliwość rozpoczęcia świadczenia działań biznesowych.

#### 4.9.3.1 Węzeł szkieletowy

1. Dla urządzeń IP:
  - a) Konfiguracja przykładowych usług transportowych opartych o IP w tym : L2/L3 VPN, VPLS, zgodnie z Planem Wdrożenia,
  - b) Konfiguracja mechanizmów niezawodnościowych LACP, MPLS FRR, OSPF BFD i innych zgodnie z Planem Wdrożenia,
  - c) Konfiguracja Quality of Service w szkielecie sieci zgodnie z Planem Wdrożenia,
  - d) Konfiguracja funkcjonalności multicast w szkielecie sieci zgodnie z Planem Wdrożenia,
  - e) Konfiguracja przełącznika sieci Zarządzającej,
  - f) Konfiguracja funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczanie ruchu określonego typu, uwierzytelnianie protokołów routingu, szyfrowane sesje SSH i inne),
  - g) Definicja dostępu administracyjnego (zarówno w oparciu o protokół Radius jak i dostęp lokalny),
  - h) Konfiguracja i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP,



- i) Konfiguracja mechanizmów OAM.
- 2. Dla urządzeń DWDM:
  - a) Konfiguracja urządzeń DWDM zgodnie z topologią przewidzianą dla danego węzła szkieletowego.

#### 4.9.3.2 Węzeł dystrybucyjny

- 1. Dla urządzeń IP:
  - a) Konfiguracja przykładowych usług transportowych opartych o IP, w tym :L2/L3 VPN, VPLS, zgodnie z Planem Wdrożenia,
  - b) Konfiguracja mechanizmów niezawodnościowych LACP, MPLS FRR, OSPF BFD i innych zgodnie z Planem Wdrożenia,
  - c) Konfiguracja Quality of Service rdzenia sieci zgodnie z Planem Wdrożenia,
  - d) Konfiguracja funkcjonalności multicast zgodnie z Planem Wdrożenia,
  - e) Konfiguracja przełącznika sieci Zarządzającej,
  - f) Konfiguracja funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczanie ruchu określonego typu, uwierzytelnianie protokołów routingu, szyfrowane sesje SSH i inne),
  - g) Definicja dostępu administracyjnego (zarówno w oparciu o protokół Radius jak i dostęp lokalny),
  - h) Konfiguracja i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP,
  - i) Konfiguracja mechanizmów OAM.
- 2. Dla urządzeń DWDM:
  - a) Konfiguracja krotnicy DWDM zgodnie z topologią przewidzianą dla danego węzła dystrybucyjnego.

#### 4.9.3.3 Węzeł IXP

- 1. Konfiguracja protokołów routingu,
- 2. Konfiguracja protokołu BGP między węzłami IXP,

3. Konfiguracja protokołu BGP z operatorami wraz z politykami umożliwiającymi elastyczne i efektywne wykorzystywanie łącz do różnych operatorów,
4. Konfiguracja polityk QoS związanych z dostępem do Internetu stosownie z wymaganiami usług zdefiniowanych w Planie Wdrożenia,
5. Konfiguracja list kontroli dostępu filtrujących niepożądanych ruch w ramach poszczególnych usług,
6. Konfiguracja funkcjonalności związanych z bezpieczeństwem (uRPF, ograniczanie ruchu określonego typu, uwierzytelnianie protokołów rutingu, SSH i inne),
7. Definicja dostępu administracyjnego ,
8. Skonfigurowanie i zabezpieczenie dostępu do urządzenia poprzez CLI, SSH, SNMP.

#### 4.9.3.4 Węzeł CZS i zCZS

1. Konfiguracja sytemu dwóch przełączników lub przełącznika modularnego do pracy, celem uzyskania niezbędnej niezawodności i wydajności, w szczególności poprzez:
  - a) odpowiednie zaprojektowanie połączeń pomiędzy przełącznikami oraz przełącznikami a serwerami,
  - b) skonfigurowanie odpowiednich protokołów umożliwiających poprawną pracę serwerów nawet w przypadku całkowitej awarii jednego z przełączników,
2. Konfiguracja systemu zabezpieczeń opartego o zaporę ogniową w trybie HA oraz system proaktywnej ochrony przed atakami:
  - a) wdrożenie polityk bezpieczeństwa zgodnie z Planem Wdrożenia,
  - b) wdrożenie wirtualnych kontekstów,
3. Konfiguracja systemu autoryzacji dostępu do urządzeń sieciowych.
4. Konfiguracja systemu zarządzania urządzeniami sieciowymi:
  - a) skonfigurowanie możliwości diagnozowania stanu, wydajności i dostępności sieci, wraz z raportowaniem w czasie rzeczywistym oraz w oparciu o dane historyczne,
  - b) skonfigurowanie wykrywanie błędów i problemów w czasie rzeczywistym,
  - c) przygotowanie szablonu raportu generowanego przez system listującego użytkowane urządzenia oraz szczegółowe opisy ich konfiguracji.
5. Konfiguracja systemu prezentacji stanu sieci:

- a) Poprawne wprowadzenie wszystkich urządzeń (w tym integracja z systemem paszportyzacji) oraz wizualizacja topologii,
  - b) Konfiguracja monitoringu zdarzeń na wszystkich urządzeniach,
  - c) Konfiguracja reguł korelacji i filtracji zdarzeń zgodnie z polityką bezpieczeństwa,
  - d) Konfiguracja sposobu powiadamiania administratorów o istotnych incydentach,
  - e) Przygotowanie szablonów raportów dla administratorów oraz jednostki zarządzającej siecią DSS o zdarzeniach z ostatniego dnia/tygodnia/miesiąca,
  - f) Konfiguracja interfejsu graficznego (np. w postaci strony WWW) umożliwiającego podgląd sytuacji w sieci (graficzny i ilościowy).
6. Konfiguracja usługi NTP na serwerze Systemu Zarządzania Siecią.
7. Konfiguracja usług DNS i DHCP na serwerze Systemu Zarządzania Siecią.

#### 4.10 Testy akceptacyjne, odbiór i gwarancja

Na potrzeby sprawdzenia wybranych parametrów dostarczonego sprzętu i jego zgodności z założonymi funkcjonalnościami należy przeprowadzić testy odbiorcze. Testy obligatoryjnie należy przeprowadzić na sprzęcie dostarczonym do Zamawiającego.

W zależności od architektury, funkcjonalności i parametrów, testy dla urządzeń sieciowych mogą być zmieniane i dobrane tak, aby uzyskać wyniki wiarygodne dla Zamawiającego. Testy powinny zostać wykonane przy użyciu specjalistycznych mierników sieciowych, np.: IXIA lub Agilent. Zamawiający zastrzega sobie prawo do weryfikacji jakości przeprowadzonych testów i interpretacji wyników przez upoważnioną stronę trzecią (np. Inżyniera Kontraktu). Testy te mają na celu zweryfikowanie poprawności wdrożenia i wykazanie spełnienia wszystkich wymagań zawartych w niniejszym projekcie przez dostarczone urządzenia i oprogramowanie. Testy akceptacyjne i wydajnościowe powinny obejmować urządzenia odpowiedzialne za niezawodność oraz ciągłą dostępność urządzeń usług. Należy także przeprowadzić weryfikację zgodności elementów systemu z normami technicznymi w zakresie bezpieczeństwa informatycznego (PN-EN 60950-1:2007).

Testy platformy IP i DWDM oraz systemów SZS i SPSS należy przeprowadzić na w pełni uruchomionej sieci DSS.

#### 4.10.1 Testy akceptacyjne systemów IP oraz SZS i SPSS

W ramach testów odbiorczych należy także sprawdzić poprawność wykonania czynności wdrożeniowych oraz konfiguracji urządzeń i usług.

W szczególności należy sprawdzić poprawność konfiguracji i działania oprogramowania do monitoringu i analizy zdarzeń w sieci w zakresie:

1. otrzymywanych logów;
2. wysyłania alarmów;
3. możliwości obserwacji zdarzeń;
4. tworzenia raportów związanych z bezpieczeństwem oraz zdarzeniami w sieci;
5. analizy danych - przeszukiwanie logów pod kątem określonych zdarzeń;
6. wizualizacji graficznej zdarzeń związanych z bezpieczeństwem.

Konieczne jest również sprawdzenie poprawności konfiguracji i działania systemu autentykacji i autoryzacji w zakresie możliwości konfiguracji mechanizmów uwierzytelniania użytkownika, w tym m.in. sprawdzanie, możliwości definiowania kont dla użytkowników z różnymi uprawnieniami (np. Administrator, Operator).

Celem testów jest sprawdzenie, czy wszystkie lokalizacje/urządzenia w sieci są dostępne, oraz czy komunikacja i wymiana danych pomiędzy tymi lokalizacjami/urządzeniami jest poprawnie realizowana (drożność systemu) oraz sprawdzenie, czy deklarowane usługi pomiędzy poszczególnymi lokalizacjami/urządzeniami są realizowane z wymaganym poziomem jakości. W ramach testów jakości usług powinny zostać zmierzone następujące parametry kluczowe dla poszczególnych usług:

1. maksymalne opóźnienie przesyłania pakietów dla danego punktu,
2. maksymalne wahanie wartości opóźnienia przesyłania pakietów,
3. maksymalna wartość współczynnika straty pakietów,
4. średnie opóźnienie przesyłania pakietów dla poszczególnych grup/punktów,
5. średnia przepustowość pomiędzy punktami referencyjnymi.

Testy te należy przeprowadzić przy użyciu generatorów ruchu, symulatorów stacji roboczych oraz oprogramowania badającego opóźnienia i straty pakietów. Spodziewane wyniki opóźnień i strat pakietów powinny być zgodne z danymi referencyjnymi zawartymi w tabeli 6.13

W ramach testów akceptacyjnych należy także sprawdzić zachowanie się urządzeń w czasie awarii oraz czas odtwarzania świadczenia usług po awarii. Celem tych testów jest sprawdzenie czasu, jaki jest wymagany przez urządzenie na odtworzenie oferowanych przez niego usług w przypadku, gdy wystąpiła awaria któregoś, z jego komponentów. Zakres testów wymaga zatem, aby zasymulować różnego rodzaju awarie poszczególnych komponentów urządzenia, następnie przywrócić działanie danego komponentu i oszacować niezbędny czas, jaki jest potrzebny, aby dana funkcjonalność urządzenia została w pełni przywrócona. Następnie należy zweryfikować czy nastąpiło pełne przywrócenie funkcjonalności.

Weryfikacja funkcjonalności poszczególnych elementów sieci będzie polegała na zaakceptowaniu przez Zamawiającego każdego z przeprowadzonych testów. Z każdego takiego testu powinien zostać sporządzony protokół zawierający wyniki przeprowadzonych procedur testowych z oceną testu: pozytywną lub negatywną. W przypadku negatywnego wyniku testu protokół powinien zawierać dane dotyczące analizy danego problemu oraz informację o działaniach jakie należy przeprowadzić w celu wyeliminowania zdiagnozowanych problemów. W takim wypadku testy weryfikacyjne po przeprowadzeniu działań naprawczych zostaną przez Operatora powtórzone w celu weryfikacji skutecznego usunięcia nieprawidłowości. Pozytywny wynik testów jest warunkiem koniecznym podpisania przez Zamawiającego protokołu odbioru.

W czasie testów akceptacyjnych należy także sprawdzić poziom zabezpieczeń w CSZ i ZCSZ oraz ciągłości dostępu do sieci Internet w Punktach Wymiany Ruchu.

W zakresie specyficznych testów sprzętu IP, testy powinny zawierać:

Testy redundancji dla routerów szkieletowych muszą obejmować:

1. Pracę routera z jednym modułem kontrolnym, drugi wyciągany „na gorąco”,
2. Pracę routera z jednym modułem przełączającym, drugi wyciągany „na gorąco”,
3. Pracę routera z jednym zasilaczem,
4. Możliwość zmiany oprogramowania bez restartu urządzenia.

Ponadto należy wykonać testy funkcjonalności powiązanych bezpośrednio z technologiami i usługami, które będą wykorzystywane w sieci DSS, zgodnie ze spisem zawartym w tabeli 6.12.

#### 4.10.2 Testy akceptacyjne systemu DWDM

Celem testów jest ocena poprawności działania systemu DWDM, jako całości i w rozbiciu na poszczególne elementy składowe. Wartościami referencyjnymi dla wyników testów są dane katalogowe dostawcy systemu, zgodne ze standardami telekomunikacyjnymi jak również założone wartości parametrów charakterystycznych systemu DWDM, zgodnie z niniejszym projektem.

Wszystkie wyniki testów uruchomieniowych systemu w postaci tabel, wykresów (widma sygnałów) czy raportów muszą zostać poprawnie oznaczone i zarchiwizowane. Dostęp do nich należy zapewnić służbom eksploatacyjno-utrzymaniowym. Mają one służyć, jako wartości referencyjne w przypadku identyfikacji problemów związanych z niewłaściwą pracą systemu DWDM.

W czasie wykonywania testów oraz docelowych połączeń modułów optycznych systemu DWDM należy zadbać o czystość złączy światłowodowych, kierując się następującymi zasadami:

1. każde podłączane złącze musi być sprawdzone pod względem czystości
2. złącza nieposiadające automatycznych zatrzaskowych kłapek, nie powinny być odkładane bez ochronnej zatyczki
3. złącza dostępne tylko poprzez adapter także powinno być sprawdzone,
4. w przypadku stwierdzenia zabrudzenia, złącza muszą być w odpowiedni sposób wyczyszczone i ponownie sprawdzone,

**Wykonując testy należy pamiętać o zasadach bezpiecznej pracy z urządzeniami laserowymi podanymi w Polskiej Normie PN-EN 60825-2: 2009 Bezpieczeństwo urządzeń laserowych - Część 2: Bezpieczeństwo światłowodowych systemów telekomunikacyjnych**

Wykaz wymaganego sprzętu pomiarowego:

1. Tester Ethernet
2. Miernik mocy optycznej
3. Optyczny tłumik regulowany
4. Analizator widma optycznego z funkcją pomiaru długości fali
5. Zestaw patchcordów pomiarowych
6. Mikroskop do inspekcji złączy światłowodowych
7. Urządzenia do czyszczenia złączy światłowodowych (np. Taśma do czyszczenia czół ferrul światłowodowych)

#### 4.10.2.1 Test redundancji zasilania

Zakresem niniejszego testu jest sprawdzenie działania mechanizmu przełączania na protekcyjne źródło zasilanie.

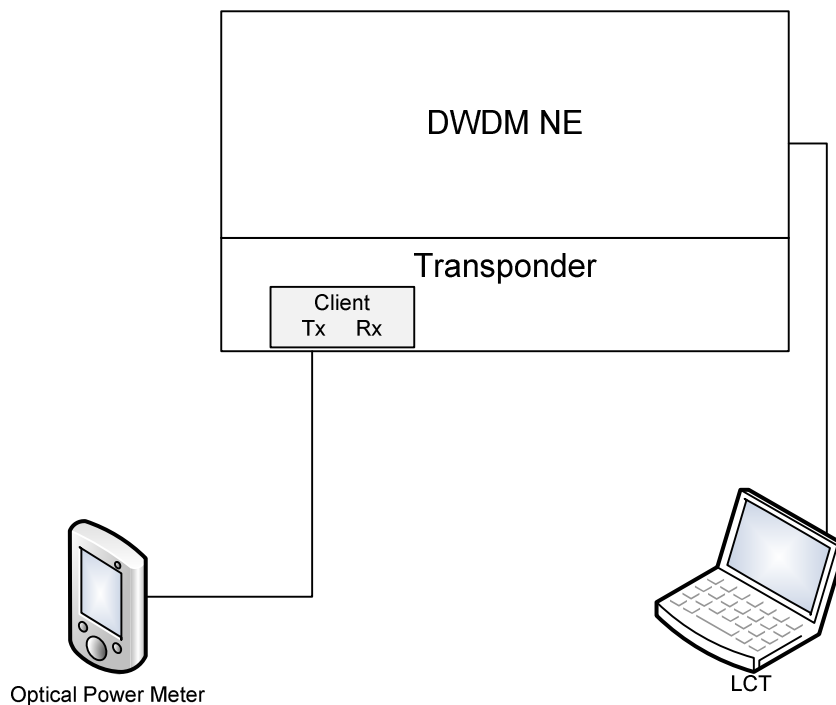
1. Sprzęt pomiarowy - Tester Ethernet.
2. Procedura testu:
  - a) Podłączyć tester Ethernet do portu klienckiego transpondera, wykonać pętlę na drugim końcu serwisu i wystartować pomiar BER,
  - b) Wyłączyć podstawowe źródło zasilania,
  - c) Sprawdzić poprawność wyników pomiaru,
  - d) Załączyć podstawowe źródło napięcia zasilania,
  - e) Wyłączyć protekcyjne źródło napięcia zasilania.
3. Kryterium akceptacji wyniku testu - Poprawność wyników pomiaru, stopa błędów nie powinna przekroczyć wartości 10-12

#### 4.10.2.2 Poziom sygnału nadawanego Tx interfejsu klienckiego

Zakresem niniejszego testu jest określenie poziomu mocy lasera interfejsów klienckich transpondera. Pomiary należy wykonać dla wszystkich typów interfejsów uruchamianych w danym węźle.

1. Sprzęt pomiarowy - Miernik mocy optycznej z patchcordami





Schemat pomiarowy

2. Procedura testu:
  - a) Podłączyć miernik mocy optycznej do portu Tx na interfejsie klienckim transpondera
  - b) Wyłączyć ALS (ang. Automatic laser shutdown) na interfejsie klienckim transpondera i włączyć laser
  - c) Odczytać wartość poziomu mocy z miernika mocy
  - d) Wyłączyć laser i załączyć ALS
3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta, które powinny być zgodne ze standardami ITU-T oraz IEEE przedstawionymi w poniższych tabelach 4.2 i 4.3.

Tabela 4.2 Poziomy mocy sygnałów nadawanych – interfejs XFP

XFP type	Range	Client Launch Power
STM-64 I-64.1	2km	-6 dBm to -1 dBm
OC-192 SR-1	2km	-6 dBm to -1 dBm
10 GbE-LR/LW	2km	-6,2 dBm to +0,5 dBm
STM-64 S-64.2b	40km	-1 dBm to +2 dBm

OC-192 IR-2b	40km	-1 dBm to +2 dBm
10 GbE-ER/EW	40km	-4,7 dBm to +4 dBm

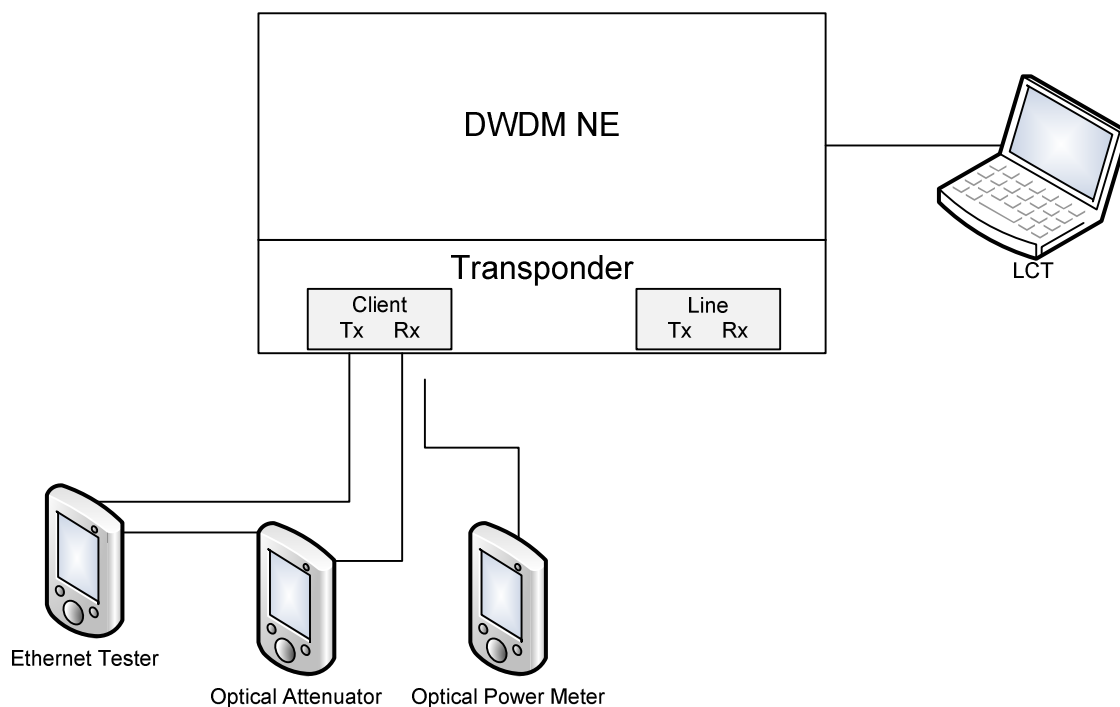
Tabela 4.3. Poziomy mocy sygnałów nadawanych – interfejs SFP

SFP type	Range	Client Launch Power
STM-16 I-16	2km	-10 dBm to -3 dBm
OC-48 SR	2km	-10 dBm to -3 dBm
STM-16 S-16.1	15km	-5 dBm to 0 dBm
OC-48 IR-1	15km	-5 dBm to 0 dBm
STM-16 L-16.1	40km	-2 dBm to +3 dBm
OC-48 LR-1	40km	-2 dBm to +3 dBm
GbE 1000BASE-LX	10km	-11 dBm to -3 dBm
GbE 1000BASE-ZX	80km	0 dBm to +5 dBm

#### 4.10.2.3 Czulość interfejsu klienckiego – minimalny poziom sygnału odbieranego

Celem niniejszego testu jest określenie minimalnego poziomu mocy sygnału odbieranego przez interfejs kliencki transpondera, przy którym nie występują błędy transmisyjne. Pomiary należy wykonać dla wszystkich typów interfejsów uruchamianych w danym węźle

1. Sprzęt pomiarowy:
  - a) Miernik mocy optycznej
  - b) Optyczny tłumik regulowany
  - c) Tester Ethernet



**Schemat pomiarowy**

**2. Procedura testu:**

- a) Podłączyć tłumik regulowany oraz tester Ethernet do portu klienckiego transpondera zgodnie z powyższym schematem
- b) Wykonać pętlę logiczną na porcie klienckim transpondera w celu zawrócenia ruchu z testera
- c) Wyłączyć ALS na interfejsie klienckim transpondera i włączyć laser
- d) Włączyć laser na testerze i uruchomić pomiar BER
- e) Tłumikiem regulowanym ustawić minimalną wartość mocy optycznej na Rx portu transpondera, przy której nie występują błędy na testerze (przez okres nie krótszy niż kilkanaście minut)
- f) Odłączyć tłumik regulowany od Rx portu liniowego transpondera i podłączyć do miernika poziomu mocy, odczytać poziom mocy sygnału
- g) Wyłączyć laser na porcie klienckim transpondera i załączyć ALS

**3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi być równa lub mniejsza od minimalnego dopuszczalnego poziomu mocy na interfejsie według danych katalogowych**

producenta, które powinny być zgodne ze standardami ITU-T oraz IEEE przedstawionymi w tabeli 4.3 i 4.4 poniżej.

Tabela 4.3. Poziomy czułości interfejsów XFP

XFP type	Range	Client Receive Power
STM-64 I-64.1	2km	-1 dBm to -11 dBm
OC-192 SR-1	2km	-1 dBm to -11 dBm
10 GbE-LR/LW	2km	+0,5 dBm to -12,6 dBm
STM-64 S-64.2b	40km	-1 dBm to -14 dBm
OC-192 IR-2b	40km	-1 dBm to -14 dBm
10 GbE-ER/EW	40km	-1 dBm to -14,1 dBm

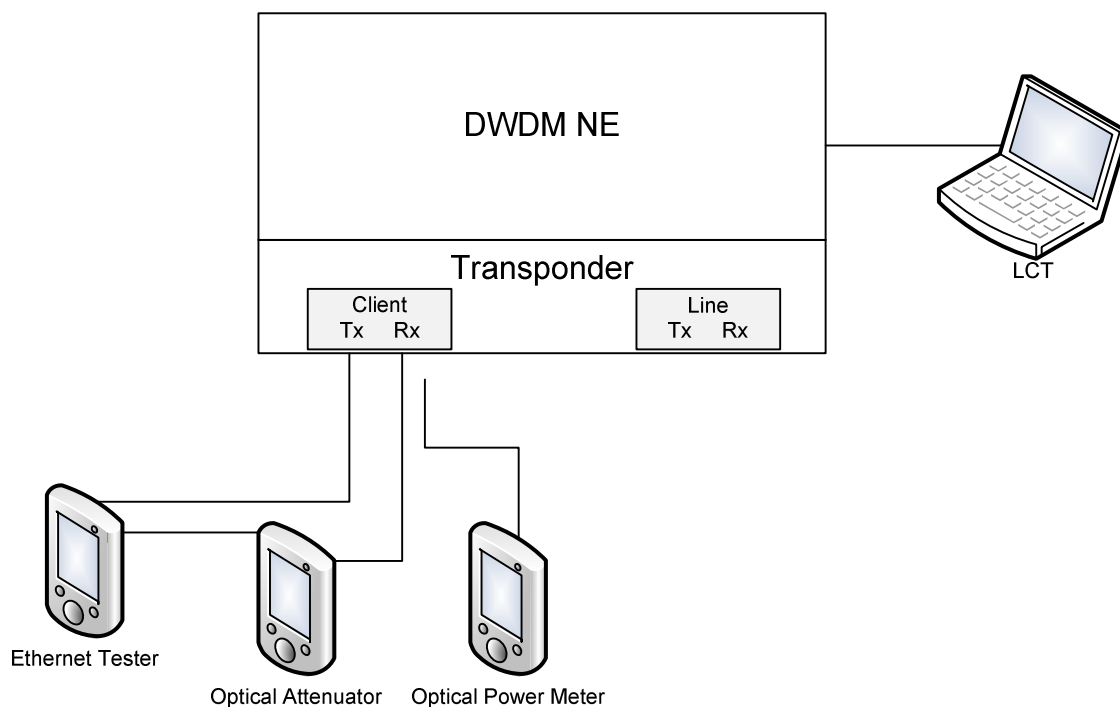
Tabela 4.4. Poziomy czułości interfejsów SFP

SFP type	Range	Client Receive Power
STM-16 I-16	2km	-3 dBm to -18 dBm
OC-48 SR	2km	-3 dBm to -18 dBm
STM-16 S-16.1	15km	0 dBm to -18 dBm
OC-48 IR-1	15km	0 dBm to -18 dBm
STM-16 L-16.1	40km	-9 dBm to -27 dBm
OC-48 LR-1	40km	-9 dBm to -27 dBm
GbE 1000BASE-LX	10km	-3 dBm to -19 dBm
GbE 1000BASE-ZX	80km	-3 dBm to -23 dBm

#### 4.10.2.4 Przesterowanie interfejsu klienckiego – maksymalny poziom sygnału

Celem niniejszego testu jest określenie maksymalnego poziomu mocy sygnału odbieranego przez interfejs kliencki transpondera, przy którym nie występują błędy transmisyjne. Pomiaru należy wykonać dla wszystkich typów interfejsów uruchamianych w danym węźle

1. Sprzęt pomiarowy:
  - a) Miernik mocy optycznej
  - b) Optyczny tłumik regulowany
  - c) Tester Ethernet
  - d) Zestaw patchcordów pomiarowych



**Schemat pomiarowy**

**2. Procedura testu:**

- a) Podłączyć tłumik regulowany oraz tester Ethernet do portu klienckiego transpondera zgodnie z powyższym schematem
- b) Wykonać pętlę logiczną na porcie klienckim transpondera w celu zawrócenia ruchu z testera
- c) Wyłączyć ALS na interfejsie klienckim transpondera i włączyć laser
- d) Włączyć laser na testerze i uruchomić pomiar BER
- e) Tłumikiem regulowanym ustawić maksymalną wartość mocy optycznej na Rx portu transpondera, przy której nie występują błędy na testerze (przez okres nie krótszy niż kilkanaście minut)
- f) Odłączyć tłumik regulowany od Rx portu liniowego transpondera i podłączyć do miernika poziomu mocy, odczytać poziom mocy sygnału
- g) Wyłączyć laser na porcie klienckim transpondera i załączyć ALS

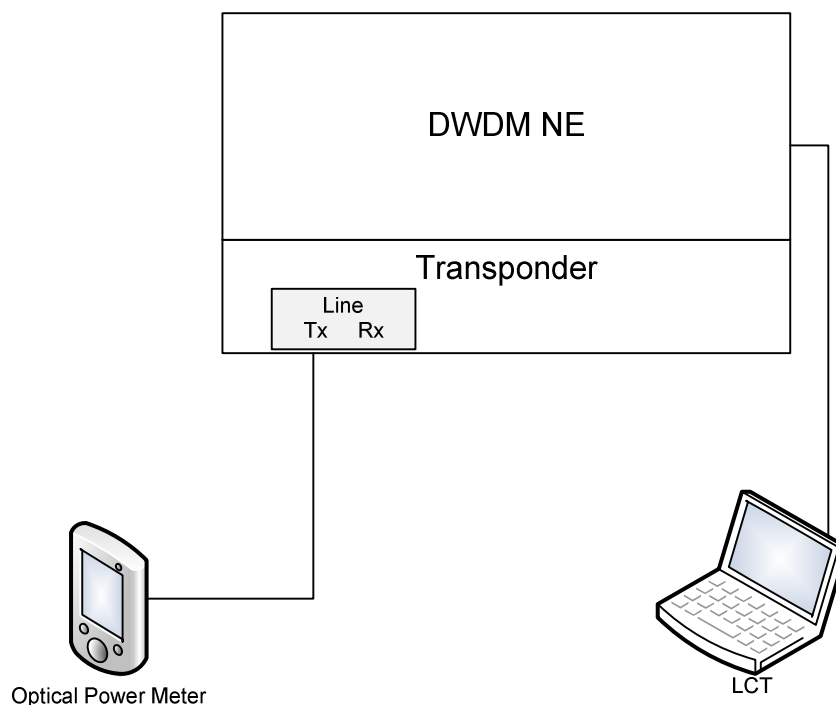
**3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi być równa lub większa od maksymalnego dopuszczalnego poziomu mocy na interfejsie według danych katalogowych**

producenta, które powinny być zgodne ze standardami ITU-T oraz IEEE przedstawionymi w powyższych tabelach 4.3 i 4.4.

#### 4.10.2.5 Poziom sygnał nadawanego Tx interfejsu liniowego

Zakresem niniejszego testu jest określenie poziomu mocy lasera transpondera po stronie liniowej.

1. Sprzęt pomiarowy - miernik mocy optycznej z patchcordami.



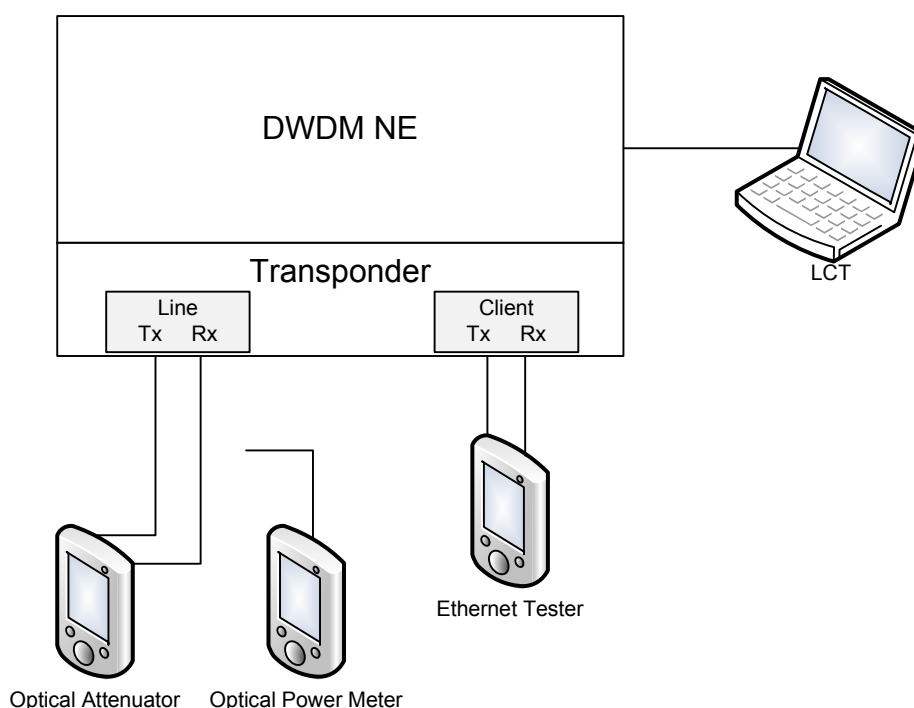
**Schemat pomiarowy**

2. Procedura testu:
  - a) Podłączyć miernik mocy optycznej do portu Tx transpondera
  - b) Wyłączyć ALS na interfejsie liniowym transpondera i włączyć laser
  - c) Odczytać wartość poziomu mocy z miernika mocy
  - d) Wyłączyć laser i załączyć ALS
3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta.

#### 4.10.2.6 Czułość interfejsu liniowego

Celem niniejszego testu jest określenie minimalnego poziomu mocy sygnału odbieranego przez interfejs liniowy transpondera, przy którym nie występują błędy transmisyjne.

1. Sprzęt pomiarowy:
  - a) Patchcords światłowodowe jednomodowe
  - b) Miernik mocy optycznej
  - c) Optyczny tłumik regulowany
  - d) Tester Ethernet



**Schemat pomiarowy**

2. Procedura testu:
  - a) Podłączyć tłumik regulowany do portu liniowego transpondera
  - b) Podłączyć tester Ethernet do interfejsu klienckiego i uruchomić pomiar BER
  - c) Wyłączyć ALS na interfejsie liniowym transpondera i włączyć laser

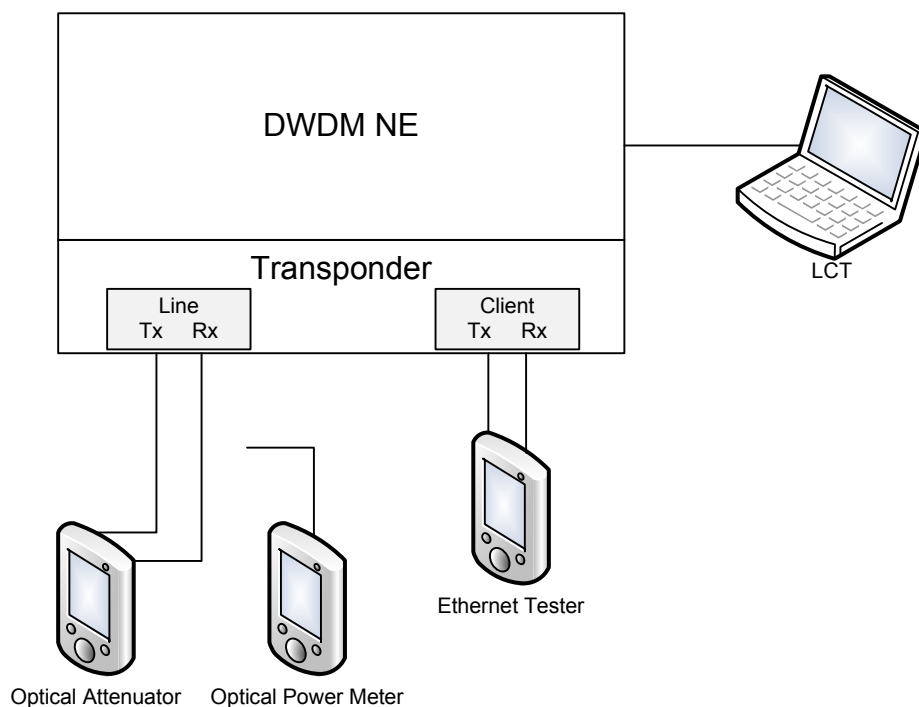


- d) Tłumikiem regulowanym ustawić minimalną wartość mocy optycznej na Rx portu liniowego transpondera, przy której nie występują błędy na testerze (przez okres nie krótszy niż kilkanaście minut)
  - e) Odłączyć tłumik regulowany od Rx portu liniowego transpondera i podłączyć miernik poziomu mocy, odczytać poziom czułości strony liniowej transpondera
  - f) Wyłączyć laser na porcie liniowym transpondera i załączyć ALS
3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta.

#### 4.10.2.7 Przesterowanie interfejsu liniowego

Celem niniejszego testu jest określenie maksymalnej dopuszczalnej wartości mocy na wejściu liniowym transpondera.

1. Sprzęt pomiarowy:
  - a) Patchcordy światłowodowe jednomodowe
  - b) Miernik mocy optycznej
  - c) Optyczny tłumik regulowany
  - d) Tester Ethernet



**Schemat pomiarowy**

**2. Procedura testu:**

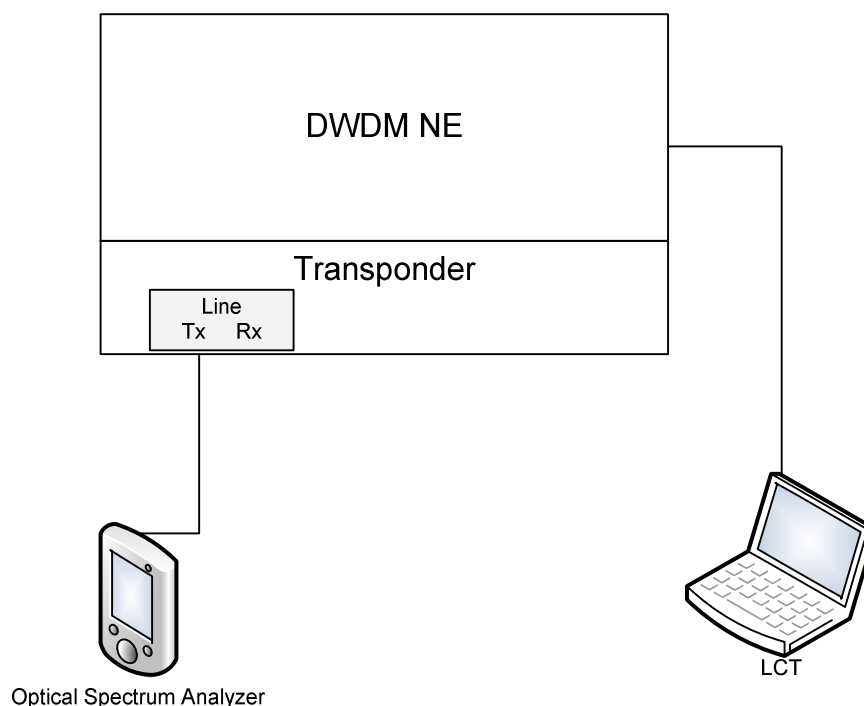
- a) Podłączyć tłumik regulowany do portu liniowego transpondera
- b) Podłączyć tester Ethernet do interfejsu klienckiego i uruchomić pomiar BER
- c) Wyłączyć ALS na interfejsie liniowym transpondera i włączyć laser
- d) Tłumikiem regulowanym ustawić maksymalną wartość mocy optycznej na Rx portu liniowego transpondera, przy której nie ma błędów na testerze (przez okres nie krótszy niż kilkanaście minut)
- e) Odłączyć tłumik regulowany od Rx portu liniowego transpondera i podłączyć z miernikiem poziomu mocy, odczytać poziom sygnału
- f) Wyłączyć laser na porcie liniowym transpondera i załączyć ALS

3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta.

#### 4.10.2.8 Widmo sygnału liniowego transpondera

Celem niniejszego testu jest wyznaczenie widma i odchylenia długości fali optycznej od długości fali nominalnej sygnału liniowego transpondera (zgodnie z ITU-T G.694.1).

1. Sprzęt pomiarowy - analizator widma optycznego z patchcordami pomiarowymi.



**Schemat pomiarowy**

2. Procedura testu:
  - a) Podłączyć analizator widma optycznego z Tx portu liniowego transpondera,
  - b) Wyłączyć ALS na interfejsie liniowym transpondera i włączyć laser,
  - c) Wykonać pomiar widma optycznego sygnału i wyznaczyć długość fali,
  - d) Sprawdzić czy wyznaczona wartość jest zgodna z ITU-T G.957,
  - e) Wyłączyć laser na porcie liniowym transpondera i załączyć ALS.

W przypadku przestrajalnych laserów liniowych transpondera, zmienić nastawę długości fali i powtórzyć test zgodnie z procedurą. Pomiary widma optycznego powinny być wykonane dla skrajnych długości fali oraz zaprojektowanej dla danego transpondera, zgodnie z przyjętą siatką kanałową. Test pozwoli również sprawdzić poprawność przestrajania częstotliwości lasera transpondera.

### 3. Kryterium akceptacji wyniku testu:

- Odchylenie długości fali optycznej od długości fali nominalnej nie powinno przekraczać wartości zdefiniowanej w danych katalogowych producenta,
- Długość fali lasera powinna pokrywać się z siatką zdefiniowaną w ITU-T G.694.1.

Tabela 4.5. Siatka częstotliwości z odstępem 100 GHz

Channel ID	Wavelength (nm)	Frequency (THz)	Channel ID	Wavelength (nm)	Frequency (THz)
1	1563.86	191.70	23	1546.12	193.90
2	1563.05	191.80	24	1545.32	194.00
3	1562.23	191.90	25	1544.53	194.10
4	1561.42	192.00	26	1543.73	194.20
5	1560.61	192.10	27	1542.94	194.30
6	1559.79	192.20	28	1542.14	194.40
7	1558.98	192.30	29	1541.35	194.50
8	1558.17	192.40	30	1540.56	194.60
9	1557.36	192.50	31	1539.77	194.70
10	1556.55	192.60	32	1538.98	194.80
11	1555.76	192.70	33	1538.19	194.90
12	1554.94	192.80	34	1537.40	195.00
13	1554.13	192.90	35	1536.61	195.10
14	1553.33	193.00	36	1535.82	195.20
15	1552.52	193.10	37	1535.04	195.30
16	1551.72	193.20	38	1534.25	195.40
17	1550.92	193.30	39	1533.47	195.50
18	1550.12	193.40	40	1532.68	195.60
19	1549.32	193.50	41	1531.90	195.70
20	1548.51	193.60	42	1531.12	195.80
21	1547.72	193.70	43	1530.33	195.90
22	1546.92	193.80	44	1529.55	196.00

Tabela 4.6. Siatka częstotliwości z odstępem 50 GHz

Channel ID	Wavelength (nm)	Frequency (THz)	Channel ID	Wavelength (nm)	Frequency (THz)
1	1563.86	191.7	45	1563.45	191.75
2	1563.05	191.8	46	1562.64	191.85
3	1562.23	191.9	47	1561.83	191.95
4	1561.42	192.0	48	1561.01	192.05



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Channel ID	Wavelength (nm)	Frequency (THz)	Channel ID	Wavelength (nm)	Frequency (THz)
5	1560.61	192.1	49	1560.20	192.15
6	1559.79	192.2	50	1559.39	192.25
7	1558.98	192.3	51	1558.58	192.35
8	1558.17	192.4	52	1557.77	192.45
9	1557.36	192.5	53	1556.96	192.55
10	1556.55	192.6	54	1556.15	192.65
11	1555.75	192.7	55	1555.34	192.75
12	1554.94	192.8	56	1554.54	192.85
13	1554.13	192.9	57	1553.73	192.95
14	1553.33	193.0	58	1552.93	193.05
15	1552.52	193.1	59	1552.12	193.15
16	1551.72	193.2	60	1551.32	193.25
17	1550.92	193.3	61	1550.52	193.35
18	1550.12	193.4	62	1549.72	193.45
19	1549.32	193.5	63	1548.91	193.55
20	1548.51	193.6	64	1548.11	193.65
21	1547.72	193.7	65	1547.32	193.75
22	1546.92	193.8	66	1546.52	193.85
23	1546.12	193.9	67	1545.72	193.95
24	1545.32	194.0	68	1544.92	194.05
25	1544.53	194.1	69	1544.13	194.15
26	1543.73	194.2	70	1543.33	194.25
27	1542.94	194.3	71	1542.54	194.35
28	1542.14	194.4	72	1541.75	194.45
29	1541.35	194.5	73	1540.95	194.55
30	1540.56	194.6	74	1540.16	194.65
31	1539.77	194.7	75	1539.37	194.75
32	1538.98	194.8	76	1538.58	194.85
33	1538.19	194.9	77	1537.79	194.95
34	1537.40	195.0	78	1537.00	195.05
35	1536.61	195.1	79	1536.22	195.15
36	1535.82	195.2	80	1535.43	195.25
37	1535.04	195.3	81	1534.64	195.35
38	1534.25	195.4	82	1533.86	195.45
39	1533.47	195.5	83	1533.07	195.55
40	1532.68	195.6	84	1532.29	195.65



**PROGRAM REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO

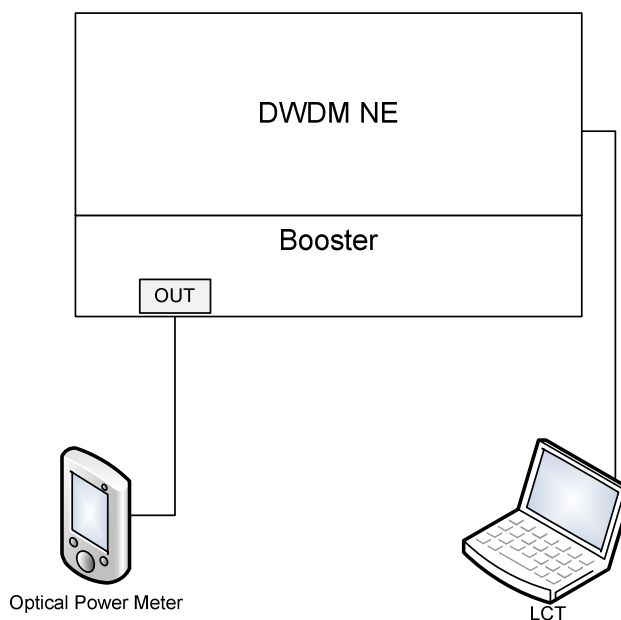


Channel ID	Wavelength (nm)	Frequency (THz)	Channel ID	Wavelength (nm)	Frequency (THz)
41	1531.90	195.7	85	1531.51	195.75
42	1531.12	195.8	86	1530.72	195.85
43	1530.33	195.9	87	1529.94	195.95
44	1529.55	196.0	88	1529.16	196.05

#### 4.10.2.9 Moc wyjściowa optycznego kanału nadzoru OSC (Optical Supervision Channel)

Celem tego testu jest sprawdzenie czy moc wyjściowa OSC mieści się w określonym zakresie.

1. Sprzęt pomiarowy - miernik mocy optycznej z patchcordami.



**Schemat pomiarowy**

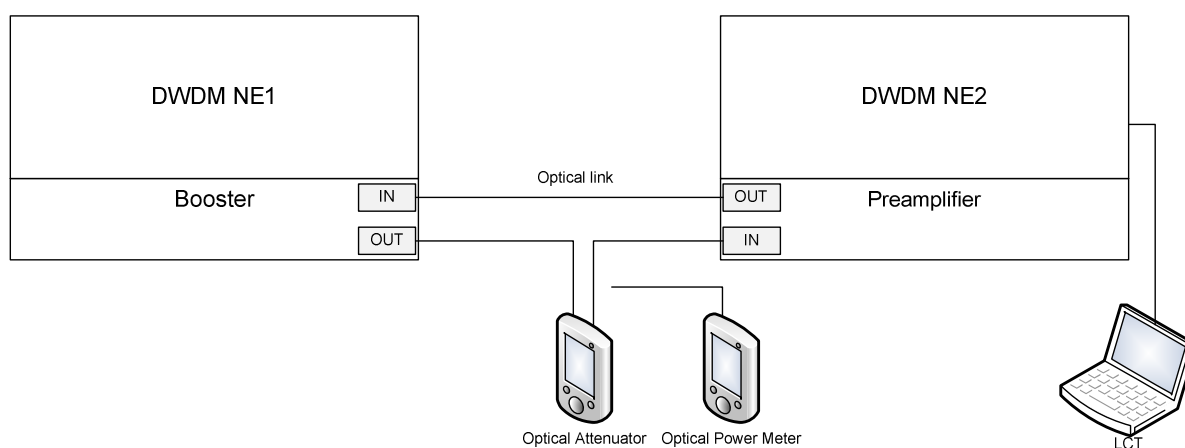
2. Procedura testu:
  - a) Upewnić się czy ALS na interfejsie liniowym transpondera jest załączony, jeśli nie to należy załączyć ALS
  - b) Odłączyć linię optyczną z portu IN przedwzmacniacza (ang. preamplifier)
  - c) Podłączyć miernik mocy optycznej do portu OUT wzmacniacza (ang. booster)

- d) Odczytać wartość poziomu mocy z miernika
3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta.

#### 4.10.2.10 Czułość wejściowa kanału nadzoru

Celem tego testu jest sprawdzenie minimalnego poziomu sygnału kanału nadzoru, przy którym działa poprawnie sieć zarządzania.

1. Sprzęt pomiarowy:
  - a) Patchcody światłowodowe jednomodowe
  - b) Miernik mocy optycznej
  - c) Optyczny tłumik regulowany



**Schemat pomiarowy**

2. Procedura testu:
  - a) Wyłączyć lasery na interfejsach liniowych transponderów
  - b) Linie optyczne połączyć za pośrednictwem tłumika regulowanego z portem IN przedwzmacniacza elementu DWDM NE2
  - c) Zwiększać tłumienie linku optycznego do czasu wystąpienia alarmu o degradacji sygnału OSC
  - d) Minimalnie zmniejszać nastawę tłumika regulowanego do czasu ustąpienia alarmu

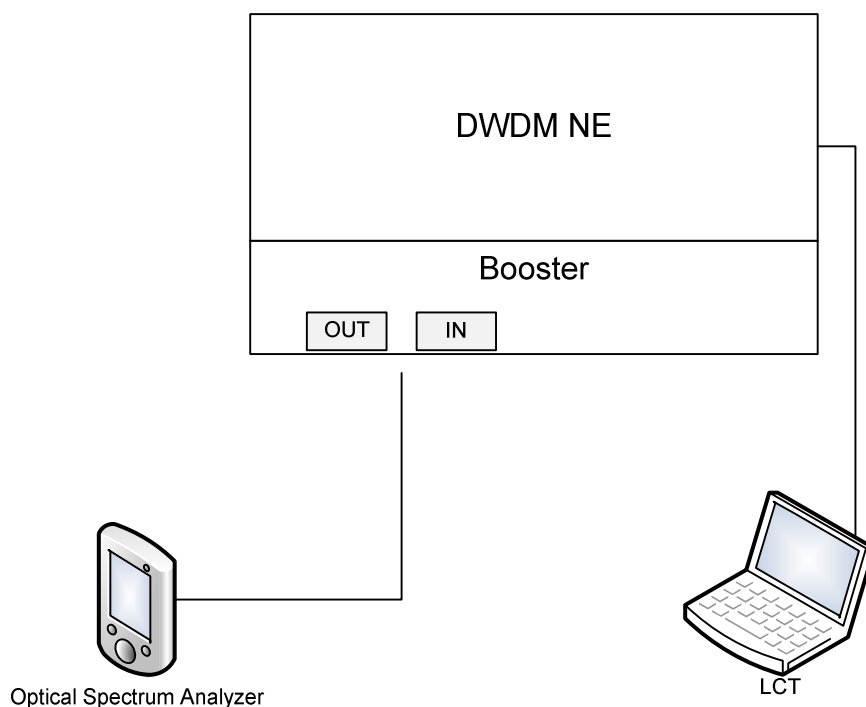


- e) Sprawdzić poprawność komunikacji pomiędzy elementami DWDM
- f) Odłączyć tłumik regulowany od portu IN przedwzmacniacza elementu DWDM NE2 i podłączyć z miernikiem poziomu mocy, odczytać poziom sygnału
3. Kryterium akceptacji wyniku testu - wartość poziomu mocy musi znajdować się w przedziale zdefiniowanym w danych katalogowych producenta.

#### 4.10.2.11 Sprawdzenie parametrów wzmacniaczy oraz weryfikacja OSNR (Optical Signal-To-Noise Ratio)

Celem tego testu jest wyznaczenie wzmocnienia stosowanych wzmacniaczy, określenie współczynnika szumów wprowadzanych przez dany wzmacniacz. Podczas pomiarów widma sygnałów należy dokonać weryfikacji wartości OSNR, szczególnie za wzmacniaczami stanowiącym ostatni punkt wzmocnienia ścieżki optycznej (koniec serwisu – spodziewana najmniejsza wartość OSNR).

1. Sprzęt pomiarowy - analizator widma optycznego z patchcordami pomiarowymi.



**Schemat pomiarowy**

2. Procedura testu:

- a) Upewnić się, że wszystkie kanały optyczne przewidywane do pracy na danym kierunku (wzmacniaczu) są uruchomione,
  - b) Wykonać pomiar widma sygnału na wejściu wzmacniacza,
  - c) Wykonać pomiar widma sygnału na wyjściu wzmacniacza,
  - d) Za pomocą analizatora widma wyznaczyć wartość wzmocnienia i współczynnika szumów dla każdego z kanałów optycznych.
3. Kryterium akceptacji wyniku testu:
- a) Wartość wzmocnienia danego wzmacniacza oraz współczynnika szumów powinna być zgodna z danymi katalogowymi producenta,
  - b) Wartość OSNR powinna być większa bądź równa wartości minimalnej podawanej przez producenta, dla utrzymania stopy błędów dla serwisów na poziomie 10-12.

#### **4.10.2.12 Zachowanie wzmacniacza w przypadku zmiany liczby kanałów optycznych**

Zakresem niniejszego testu jest sprawdzenie, że wzmocnienie wzmacniacza i OSNR dla danego kanału optycznego nie ulegnie znacznej zmianie w przypadku utraty jednego z pozostałych kanałów.

1. Sprzęt i schemat pomiarowy jak w poprzednim teście.
2. Procedura testu:
  - a) Upewnić się, że wszystkie kanały optyczne przewidywane do pracy na danym kierunku (wzmacniaczu) są uruchomione,
  - b) Wykonać pomiar widma sygnału na wyjściu wzmacniacza,
  - c) Zmniejszyć liczbę kanałów optycznych np. pozostawiając tylko jeden,
  - d) Wykonać pomiar widma sygnału na wyjściu wzmacniacza,
  - e) Wyznaczyć zmianę poziomu sygnału i OSNR dla pozostawionego kanału optycznego.
3. Kryterium akceptacji wyniku testu - wartość poziomu sygnału i OSNR dla pozostawionego kanału optycznego może ulec zmianie w zakresie określonym w danych katalogowych producenta.

#### 4.10.2.13 Sprawdzenie poprawności alarmowania elementów sieciowych

Celem testu jest sprawdzenie poprawności alarmowania poszczególnych elementów sieciowych w przypadku świadomego wywołania incydentów przedstawionych poniżej:

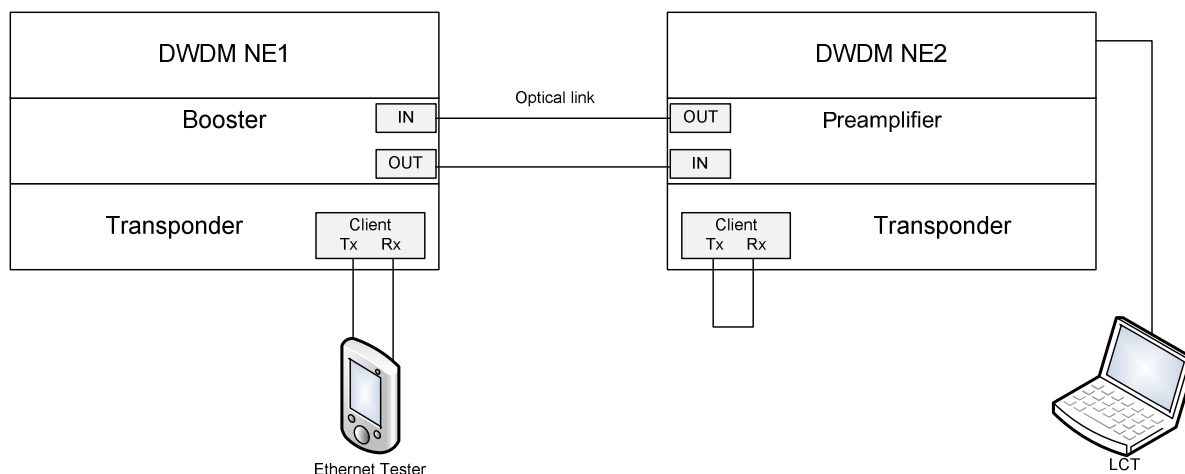
1. Brak jednego z źródeł zasilania
2. Zanik sygnału optycznego w dowolnym miejscu po stronie liniowej
3. Zanik sygnału optycznego po stronie klienckiej
4. Zawyżone tłumienie linku optycznego
5. Wyciągnięcie aktywnego modułu z półki DWDM
6. Wyciągnięcie wentylatora z półki DWDM

Wykonując te testy należy sprawdzić poprawność alarmowania NE w przypadku lokalnego podłączenia do węzła DWDM za pomocą LCT oraz poprawność alarmowania NMS (spływania alarmów z węzłów). Należy również zwrócić uwagę na poprawność alarmowania LED na poszczególnych modułach i kontrolerze.

#### 4.10.2.14 48h test BER dla uruchamianych serwisów

Zakresem niniejszego testu jest ocena poprawności działania poszczególnych serwisów poprzez pomiar bitowej stopy błędów przez okres minimum 48h. W celu skrócenia czasu potrzebnego na testy wszystkich uruchamianych serwisów dopuszcza się ich kaskadowanie.

1. Sprzęt pomiarowy:
  - a) Tester Ethernet,
  - b) Zestaw patchcordów pomiarowych.



**Schemat pomiarowy**

2. Procedura testu:
  - a) Wykonać pętlę fizyczną na interfejsie klienckim (jeden koniec serwisu),
  - b) Podłączyć tester Ethernet do interfejsu klienckiego (drugi koniec serwisu) i uruchomić pomiar BER.
  - c) Zweryfikować poprawność wystartowanego testu i pozostawić pomiar na 48h
3. Kryterium akceptacji wyniku testu - test powinien zakończyć się ze stopą błędów  $10^{-12}$  lub mniejszą.

#### 4.10.2.15 Wykonanie testów RFC 2544 dla serwisów Ethernet

Celem niniejszego testu jest pomiar parametrów łącz Ethernet zgodnie ze standardem RFC 2544.

1. Sprzęt i schemat pomiarowy jak w poprzednim punkcie, dla pomiarów BER.
2. Procedura testu:
  - a) Wykonać pętlę fizyczną na interfejsie klienckim (jeden koniec serwisu),
  - b) Podłączyć tester Ethernet do interfejsu klienckiego (drugi koniec serwisu) i uruchomić pomiar RFC 2544.

#### 4.10.2.16 Zmiana wersji oprogramowania węzła DWDM

Celem testu jest zmiana wersji oprogramowania dla węzła i sprawdzenie braku wpływu na konfigurację i przenoszony ruch.

1. Sprzęt i schemat pomiarowy jak dla pomiarów BER.
2. Procedura testu:
  - a) Wykonać pętlę fizyczną na interfejsie klienckim (jeden koniec serwisu),
  - b) Podłączyć tester Ethernet do interfejsu klienckiego (drugi koniec serwisu) i uruchomić pomiar BER,
  - c) Zmienić wersję oprogramowania dla węzła z poziomu LCT lub NMS.
3. Kryterium akceptacji wyniku testu - brak zmiany w konfiguracji węzła oraz bezbłędny wynik pomiaru po zakończeniu procesu zmiany oprogramowania.

#### 4.10.3 Odbiór

Po pozytywnym zakończeniu testów akceptacyjnych nastąpi odbiór końcowy. Odbiór sieci i systemów będzie przeprowadzony przez komisję techniczną, utworzoną przez wytypowanych przedstawicieli stron. Do protokołu odbioru dołączone powinny być m. in.:

1. dokumentacja opisująca wykonanie testów akceptacyjnych i powdrożeniowych;
2. wykaz urządzeń wraz z numerami seryjnymi;
3. komplet dokumentacji całego systemu w języku polskim oraz procedury eksploatacyjne wraz z instrukcjami;
4. wszystkie wymagane prawem nośniki, licencje i certyfikaty na dostarczony sprzęt i oprogramowanie;
5. wykaz oprogramowania wraz z rodzajem i warunkami licencjonowania;
6. dokumenty potwierdzające przeprowadzenie szkoleń dla pracowników Zamawiającego.

#### 4.10.4 Gwarancja

1. Wykonawca udzieli gwarancji na dostarczone i skonfigurowane komponenty i konfigurację systemu zgodnie z ustaleniami między Wykonawcą a Zamawiającym,
2. Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta
3. Okres gwarancyjny rozpoczyna się z dniem podpisania przez Zamawiającego protokołu odbioru bez uwag.
4. Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednej godziny; tymczasowe usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia lub zaimplementowanie rozwiązania obejściowego skutkującego przewróceniem usług) ma zostać wykonana w przeciągu 6 godzin od momentu przyjęcia zgłoszenia usterki przez Wykonawcę; Finalne usunięcie usterki może nastąpić najpóźniej w przeciągu 21 dni od dnia jej zgłoszenia. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Zamawiającego), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań.
5. W ramach serwisu gwarancyjnego Wykonawca zobowiązuje się do:
  - a) Udzielania drogą telefoniczną, przez pracownika posiadającego certyfikat producenta, nielimitowanych konsultacji w zakresie sprzętu, oprogramowania i eksploatacji systemu, w godzinach pracy Zamawiającego;
  - b) Nieodpłatnej aktualizacji oprogramowania w ramach posiadanych wersji w porozumieniu z Zamawiającym o ile aktualizacja ta nie wymaga zakupów dodatkowych licencji;
  - c) Usuwania usterek funkcjonalnych sprzętu i oprogramowania wynikających z wad powstałych podczas integracji lub implementacji oraz aktualizacji tego oprogramowania;
  - d) W przypadku awarii dostarczonych urządzeń Wykonawca zobowiązuje się do bezpłatnej naprawy lub wymiany najpóźniej w ciągu 7 dni roboczych od dnia zgłoszenia;
  - e) Jeżeli charakter naprawy wymaga przetransportowania sprzętu do Wykonawcy, Wykonawca przetransportuje ten sprzęt we własnym zakresie. Dotyczy to również zwrotu sprzętu po naprawie;

6. W przypadku awarii, wymagającej wizyty serwisu Wykonawcy, przedstawiciel serwisu Wykonawcy ustali z upoważnionym przedstawicielem Zamawiającego szczegóły wizyty serwisowej a w szczególności godzinę rozpoczęcia prac oraz wejścia do budynków.
7. W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki.

## 4.11 Wymagania w zakresie szkoleń

Wykonawca (Operator Infrastruktury) zobowiązany jest do przeprowadzenia szkoleń i warsztatów dla osób będących pełnić funkcje administratorów sieci DSS, pracowników CZS i zCZS. Szkolenia muszą zostać przeprowadzone z ramienia Inwestora lub przez wskazane przez niego podmioty trzecie, z zakresu i technologii wybranych do realizacji sieci DSS. Wymiar i zakres szkolenia należy skonsultować z Zamawiającym, lecz narzuca się wymagania konieczne do spełnienia w tym zakresie:

1. Szkolenia należy przeprowadzić w małych grupach (maksymalnie po 6 osób),
2. Szkolenia powinny zawierać się w minimalnym wymiarze 5 dni po 8 godzin zegarowych dla każdej grupy, dla każdego zakresu materiału,
3. Szkolenia muszą być przeprowadzone w różnych terminach dla każdej z grup,
4. Każdy z uczestników musi mieć własne stanowisko laboratoryjne,
5. Wszystkie osoby z grupy szkoleniowej muszą mieć możliwość jednoczesnego i aktywnego konfigurowania urządzeń laboratoryjnych (używanych do celów szkolenia),
6. Zamawiający dopuszcza w uzasadnionych przypadkach zdalny dostęp do sieci laboratoryjnej,
7. Szkolenie musi odbywać się na terenie Rzeczypospolitej Polskiej i być prowadzone w języku polskim,
8. Jeśli Szkolenia muszą zostać przeprowadzone w ośrodku szkoleniowym, koszt transportu i noclegów osób szkolonych pokryć musi Wykonawca,
9. Szkolenia muszą przeprowadzać osoby certyfikowane do prowadzenia szkoleń z zakresu i technologii zastosowanych do realizacji sieci DSS.

Minimalny zakres tematyki szkolenia powinien obejmować procedury instalacyjne i utrzymaniowe sprzętu wybranego przez Operatora, w tym mechanizmy wysokiej dostępności HA oraz obejmować



tematykę kreowania, utrzymania i diagnozowania usług bazujących na usługach potencjalnie wykorzystywanych w pracy sieci DSS. Szkolenia muszą dostarczyć umiejętności w zakresie:

1. instalacji i uruchamiania poszczególnych elementów sieci DSS,
2. konfiguracji poszczególnych elementów sieci DSS
3. administrowania poszczególnymi elementami sieci DSS,
4. konfiguracji sieci DSS,
5. administrowania Siecią DSS,
6. konfiguracji usług sieci DSS,
7. administrowania siecią DSS,
8. monitorowania i zarządzania ruchem w sieci DSS,
9. zarządzania usługami sieci (z uwzględnieniem zarządzania elementami sieci, menadżerami sieci, itp.) na potrzeby realizacji celów strategicznych sieci.

Wymagania minimalne do osób przystępujących do szkolenia:

1. wykształcenie wyższe techniczne kierunkowe (telekomunikacja, elektronika, informatyka). W przypadku wykształcenia średniego dodatkowo co najmniej rok doświadczenia w eksploatacji sieci telekomunikacyjnych;
2. Ogólna znajomości sieci telekomunikacyjnych opartych o protokół IP: podstawy routingu i przełączania.
3. Ogólna znajomość w zakresie technologii xWDM.

**W ramach dostarczenia urządzeń i uruchomienia sieci DSS Wykonawca zobowiązany jest do zapewnienia/przeprowadzenia następujących szkoleń i warsztatów dla systemów IP oraz SZS i SPSS:**

1. Autoryzowane szkolenia przez producenta wdrażanego rozwiązania, przygotowujące do administracji i obsługi sieci DSS dla grupy 4 pracowników Zamawiającego przeprowadzone w autoryzowanym centrum szkoleniowym i zakończone stosownym certyfikatem z zakresem obejmującym:
  - a) zaawansowaną konfigurację przełączników i protokołów routingu - wymagany czas trwania szkolenia co najmniej 5 dni (5 x 8 godzin):
    - konfiguracja przełączania L2 i L3
    - protokoły STP, RSTP, MST
    - konfiguracja mechanizmów bezpieczeństwa na przełącznikach
    - konfiguracja mechanizmów redundancji (np. VRRP)



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



- konfiguracja i weryfikacja działania RIP, OSPF
  - podstawy działania i konfiguracji BGP,
  - zaawansowana konfiguracja i weryfikacja działania IS-IS,
  - wymiana informacji pomiędzy różnymi protokołami routingu,
  - filtracja routingu,
  - determinacja i modyfikacja wyboru tras,
  - podstawy IPv6,
  - podstawy multicast;
- b) protokół BGP i (opcjonalnie - w przypadku wyboru tej technologii przez Operatora) MPLS - wymagany czas trwania szkolenia co najmniej 5 dni (5 x 8 godzin):
- równoczesna implementacja niezależnych usług w oparciu o wirtualne tablice routingu,
  - konfiguracja i weryfikacja działania protokołu BGP,
  - modyfikacja atrybutów BGP do realizacji polityk dla ruchu przychodzącego i wychodzącego,
  - filtrowanie routingu,
  - optymalizacja BGP (skalowalność i stabilność działania),
  - konfederacje i route reflektor,
  - konfiguracja MP-BGP,
  - konfiguracja i weryfikacja działania MPLS,
  - konfiguracja MPLS VPN,
  - wprowadzenie do MPLS TE;
- c) zarządzanie bezpieczeństwem sieci i konfiguracja urządzeń pod kątem zapewnienia jakości usług (Quality of Service) - wymagany czas trwania szkolenia co najmniej 5 dni (5 x 8 godzin):
- zarządzanie i konfiguracja systemu zapory ogniowej
  - zarządzanie i konfiguracja systemu proaktywnej ochrony przed atakami;
  - znaczenie i planowanie polityk QoS
  - konfiguracja i weryfikacja QoS
  - znakowanie i klasyfikacja pakietów
  - kolejkovanie i zarządzanie kolejkami
  - policing oraz shaping ruchu
  - dobre praktyki w konfiguracji QoS



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



2. Dedykowane warsztaty szkoleniowe dla grupy 6 pracowników Zamawiającego przeprowadzone w centrum szkoleniowym Wykonawcy, obejmujące:
  - a) podstawy konfiguracji urządzeń sieciowych oraz zarządzanie urządzeniami sieciowymi, dostępem do urządzeń sieciowych oraz monitoringiem i korelacją zdarzeń - wymagany czas trwania szkolenia co najmniej 5 dni (5 x 8 godzin):
    - podstawy teoretyczne przełączania i routingu
    - podstawy konfiguracji protokołów routingu
    - podstawy konfiguracji przełączania
    - adresacja IP, planowanie, implementacja
    - podstawy bezpieczeństwa w sieciach IP oraz filtracja ruchu
    - NAT/PAT
    - zarządzanie konfiguracją urządzeń
    - zarządzanie inwentaryzacją
    - zarządzanie awariami
    - tworzenie raportów;
    - zarządzanie systemem monitoringu i korelacji zdarzeń

**W ramach dostarczenia urządzeń i uruchomienia sieci DSS Wykonawca zobowiązany jest do przeprowadzenia następujących szkoleń i warsztatów dla systemu DWDM:**

Autoryzowane szkolenia przez producenta wdrażanego rozwiązania, przygotowujące do administracji i obsługi sieci DSS dla grupy 4 pracowników Zamawiającego przeprowadzone w autoryzowanym centrum szkoleniowym i zakończone stosownym certyfikatem z zakresem obejmującym:

1. Optyczne sieci transportowe
  - a) Podstawy technologii DWDM
  - b) Podstawy budowy OTN
  - c) Hierarchia tworzenia sygnałów w sieciach optycznych, struktura OTM
2. Funkcjonalność systemu DWDM
  - a) Architektura systemu
  - b) Funkcjonalność modułów
  - c) Konfiguracja różnych elementów sieciowych
  - d) System kontroli mocy



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA 

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



3. Obsługa i konfiguracja
  - a) Interfejs użytkownika aplikacji zarządzających
  - b) Konfiguracja sieci zarządzania
  - c) Konfiguracja elementów sieciowych i modułów
  - d) Konfiguracja serwisów
  - e) Wykonywanie kopii zapasowych konfiguracji NE
  - f) Usuwanie awarii
4. Nadzór nad systemem DWDM
  - a) Monitorowanie poprawności działania systemu DWDM
  - b) Alarmy i ich znaczenie
  - c) Konfiguracja systemu alarmowania – logowanie zdarzeń
  - d) Monitorowanie wydajności systemu
5. Administracja serwerem NMS
  - a) Zarządzanie kontami użytkowników
  - b) Procedura wykonywania i przywracania kopii zapasowych
  - c) Zarządzanie plikami logowania

Wymagany czas trwania szkolenia co najmniej 10 dni (2 x 5 dni x 8 godzin).

Zamawiający wymaga wystawienia certyfikatu potwierdzającego uczestniczenie w dedykowanych szkoleniach i warsztatach szkoleniowych.

## 5 Spis dokumentów związanych

1. DT-W/658/12-97-ST **STWiOR**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM1. Urządzenia teletransmisyjne.**
2. DT-W/658/12-97-PR **Przedmiar**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM1. Urządzenia teletransmisyjne.**
3. DT-W/658/12-97-KS **Kosztorys**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM1. Urządzenia teletransmisyjne.**

Projekty wykonawcze związane:

1. DT-W/658/12-97-PW **Projekt Wykonawczy**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM 2. Zintegrowany System Nadzoru.**
2. DT-W/658/12-97-PW **Projekt Wykonawczy**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM 3. Urządzenia zabezpieczenia energetycznego i klimatyzacji w węzłach szkieletowych.**
3. DT-W/658/12-97-PW **Projekt Wykonawczy**. Projekt techniczny części aktywnej DSS oraz projekt techniczny i plan wdrożenia systemów informatycznych zarządzania i monitoringu sieci. **TOM 4. Urządzenia zabezpieczenia energetycznego i klimatyzacji w węzłach dystrybucyjnych i zCZS.**

Inne dokumenty związane:

1. Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej, Część 2: Wymagania dla dokumentacji części aktywnej sieci - opracowane przez Politechnikę Wrocławską, wersja dokumentu 1.2 z 16.04.2012 r.;

## 6 Spis tabel

### 6.1 Lista węzłów sieciowych

Lp	TYP_Nazwa Węzła	Nr węzła	Klasa węzła	Nr logiczny	Lokalizacja węzła
<b>Węzły szkieletowe klasy C1</b>					
1	WS_Bolesławiec	WS_1	C1	WS_C1_1	Działka numer 127 obręb Bolesławiec N-4, arkusz 13, kontener
2	WS_Lubań	WS_6	C1	WS_C1_6	Działka numer 1/5, obręb Lubań 4, arkusz 8, kontener
<b>Węzły szkieletowe klasy C2</b>					
3	WS_Jelenia Góra	WS_3	C2	WS_C2_3	Działka numer 71/3 obręb Jelenia Góra N-24, arkusz 2, kontener
4	WS_Kłodzko	WS_4	C2	WS_C2_4	Działka numer 12/1 obręb Jurandów, arkusz 1, kontener
5	WS_Strzelin	WS_7	C2	WS_C2_7	Działka numer 12/9, obręb Strzelin, arkusz 15, kontener
6	WS_Rudna	WS_8	C2	WS_C2_8	Działka numer: 766, obręb Rudna, arkusz 6, kontener
<b>Węzły szkieletowe klasy C3</b>					
7	WS_Legnica	WS_5	C3	WS_C3_5	Działka numer 201/4, Miasto Legnica obręb Piątnica, arkusz 5, kontener
8	WS_Wałbrzych	WS_9	C3	WS_C3_9	Działka numer 299/14, obręb Stary Zdrój N-19, arkusz 5, kontener
9	WS_Wrocław	WS_10	C3	WS_C3_10	Wrocław, ul. Mazowiecka 15, dz. nr 17, AM-2, obręb Południe, Serwerownia MIT, pomieszczenia 14 i 15
<b>Węzły dystrybucyjne klasy D</b>					
10	WD_Bardo Śląskie	WD_1	D	WD_D_1	Działka numer 175, obręb Bardo, arkusz 4 i 5, szafa zewnętrzna
11	WD_Bierutów	WD_2	D	WD_D_2	Działka numer 4/7, obręb Bierutów, arkusz 14. , szafa zewnętrzna
12	WD_Borek Strzelecki	WD_3	D	WD_D_3	Działka numer 285, obręb Borek Strzelecki, Arkusz 2, szafa zewnętrzna
13	WD_Brzeg Głogowski	WD_4	D	WD_D_4	Działka numer 663, obręb Brzeg Głogowski I, arkusz 2. , szafa zewnętrzna
14	WD_Bukowice Trzebnickie	WD_5	D	WD_D_5	Działka numer 384/1, obręb Bukowice, arkusz 3. , szafa zewnętrzna
15	WD_Chojnów	WD_6	D	WD_D_6	Działka numer: 39/4, obręb Chojnów N-2, arkusz 4, szafa zewnętrzna
16	WD_Ciepłowody	WD_7	D	WD_D_7	Działka numer 293, obręb Ciepłowody, arkusz 1, szafa zewnętrzna
17	WD_Cieszków	WD_8	D	WD_D_8	Działka numer 470/1, obręb Cieszków, arkusz 2. , szafa zewnętrzna
18	WD_Czernica	WD_9	D	WD_D_9	Działka numer 346 obręb Czernica, Arkusz 1, szafa zewnętrzna
19	WD_Długołęka	WD_10	D	WD_D_10	Działka numer 444/4, obręb Długołęka,



**PROGRAM REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Lp	TYP_Nazwa Węzła	Nr węzła	Klasa węzła	Nr logiczny	Lokalizacja węzła
					arkusz 1. , szafa zewnętrzna
20	WD_Dobromierz	WD_11	D	WD_D_11	działka numer: 85/94 obręb Dobromierz arkusz 1, szafa zewnętrzna
21	WD_Dobroszyce	WD_12	D	WD_D_12	Działka numer 459/2, obręb Dobroszyce, arkusz 7, szafa zewnętrzna
22	WD_Dziadowa Kłoda	WD_13	D	WD_D_13	działka numer: 652 obręb Dziadowa Kłoda arkusz 2, szafa zewnętrzna
23	WD_Głogów	WD_14	D	WD_D_14	Działka numer 46/8 obręb Nadodrze, arkusz 17, szafa zewnętrzna
24	WD_Głuszycza	WD_15	D	WD_D_15	Działka numer 255, obręb Głuszycza 1, arkusz 8 i 10. , szafa zewnętrzna
25	WD_Grębocice	WD_17	D	WD_D_17	Działka numer 626/1, obręb Grębocice, arkusz 2, szafa zewnętrzna
26	WD_Gryfów Śląski	WD_18	D	WD_D_18	Działka numer 76, obręb Ubocze, arkusz 3. , szafa zewnętrzna
27	WD_Jawor	WD_19	D	WD_D_19	Działka numer 95/8, obręb Przemysłowy N-6, arkusz 7, szafa zewnętrzna
28	WD_Jemielno	WD_20	D	WD_D_20	działka numer: 399/1 obręb Jemielno arkusz 1, szafa zewnętrzna
29	WD_Jemna	WD_21	D	WD_D_21	Działka numer 42/1, obręb Jemna, arkusz 1. , szafa zewnętrzna
30	WD_Jerzmanowa	WD_22	D	WD_D_22	działka numer: 495/2 obręb Jarzmanowa arkusz 2, szafa zewnętrzna
31	WD_Jordanów Śląski	WD_23	D	WD_D_23	Działka numer 36/4, obręb Jordanów Śląski, arkusz 3,4,5. , szafa zewnętrzna
32	WD_Kondratowice	WD_24	D	WD_D_24	Działka numer 4/4, obręb Kondratowice, arkusz 1. , szafa zewnętrzna
33	WD_Kostomłoty	WD_25	D	WD_D_25	działka numer: 381/1 obręb Kostomłoty arkusz 5, szafa zewnętrzna
34	WD_Kowary	WD_27	D	WD_D_27	Działka numer 19/16, obręb Kowary N-1, arkusz 7. , szafa zewnętrzna
35	WD_Krzeszów	WD_28	D	WD_D_28	Działka numer 646/3, obręb Krzeszów, arkusz 12. , szafa zewnętrzna
36	WD_Kudowa Zdrój	WD_29	D	WD_D_29	Działka numer 17/2, obręb Zakrze, arkusz 3 i 9, szafa zewnętrzna
37	WD_Lądek Zdrój	WD_30	D	WD_D_30	Działka numer 78/7, obręb Zatorze, arkusz 3. , szafa zewnętrzna
38	WD_Legnickie Pole	WD_31	D	WD_D_31	działka numer: 392/2 obręb Legnickie Pole arkusz 1, szafa zewnętrzna
39	WD_Leśna	WD_32	D	WD_D_32	Działka numer 294/4, obręb Leśna, arkusz 1, szafa zewnętrzna
40	WD_Lubomierz	WD_33	D	WD_D_33	Działka numer 12, obręb Lubomierz N-2, arkusz 1, szafa zewnętrzna
41	WD_Malczyce	WD_35	D	WD_D_35	Działka numer: 556/12, obręb Malczyce, arkusz 1, szafa zewnętrzna
42	WD_Marciszów	WD_36	D	WD_D_36	Działka numer 1/13, obręb Marciszów, arkusz 1, szafa zewnętrzna
43	WD_Męcinka	WD_37	D	WD_D_37	działka numer: 713/1 obręb Męcinka arkusz 2, szafa zewnętrzna



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





Lp	TYP_Nazwa Węzła	Nr węzła	Klasa węzła	Nr logiczny	Lokalizacja węzła
44	WD_Mietków	WD_38	D	WD_D_38	działka numer: 176/2 obręb Mietków arkusz 2, szafa zewnętrzna
45	WD_Międzyziesie	WD_39	D	WD_D_39	Działka numer 334/3, obręb Międzyziesie, arkusz 1, szafa zewnętrzna
46	WD_Miękinia	WD_40	D	WD_D_40	Działka numer: 332, obręb Miękinia, arkusz 2, szafa zewnętrzna
47	WD_Miłkowice	WD_41	D	WD_D_41	Działka numer: 466/1, obręb Miłkowice, arkusz 1, szafa zewnętrzna
48	WD_Mirsk	WD_42	D	WD_D_42	Działka numer 402, obręb Mirsk N-1, arkusz 5, szafa zewnętrzna
49	WD_Niechlów	WD_43	D	WD_D_43	Działka numer 733/1, obręb Naratów, arkusz 2, szafa zewnętrzna
50	WD_Niemcza	WD_44	D	WD_D_44	Działka numer 33/7, obręb Stare Miasto, arkusz 5, szafa zewnętrzna
51	WD_Nowa Ruda	WD_45	D	WD_D_45	Działka numer 326/7, obręb Nowa Ruda N-3, arkusz 19, szafa zewnętrzna
52	WD_Nowogrodziec	WD_46	D	WD_D_46	Działka numer 79, obręb Nowogrodziec N- 4, arkusz 5, szafa zewnętrzna
53	WD_Pęgów	WD_49	D	WD_D_49	Działka numer 28/2, obręb Pęgów, arkusz 1, szafa zewnętrzna
54	WD_Piekary Udanin	WD_50	D	WD_D_50	Działka numer 245/2, obręb Udanin, arkusz 1, szafa zewnętrzna
55	WD_Pielgrzymka	WD_51	D	WD_D_51	Działka numer 999, obręb Pielgrzymka, arkusz 2, szafa zewnętrzna
56	WD_Pieńsk	WD_52	D	WD_D_52	Działka numer 161, obręb Pieńsk N-2, arkusz 4, szafa zewnętrzna
57	WD_Piława Górna	WD_53	D	WD_D_53	Działka numer 457/15, obręb Kośmin 3, arkusz 9, szafa zewnętrzna
58	WD_Piskorzyna	WD_54	D	WD_D_54	Działka numer 416, obręb Piskorzyna, arkusz 2, szafa zewnętrzna
59	WD_Platerówka	WD_55	D	WD_D_55	Działka 153/3, obręb Centrum, arkusz 5, szafa zewnętrzna
60	WD_Polanica Zdrój	WD_56	D	WD_D_56	Działka 153/3, obręb Centrum, arkusz 5, szafa zewnętrzna
61	WD_Prochowice	WD_57	D	WD_D_57	Działka numer 23, obręb Prochowice N-1, arkusz 2, szafa zewnętrzna
62	WD_Radków	WD_58	D	WD_D_58	Działka numer 387/2, obręb Radków, szafa zewnętrzna
63	WD_Sarby	WD_61	D	WD_D_61	Działka numer 122, obręb Karnków, arkusz 2, szafa zewnętrzna
64	WD_Skokowa	WD_62	D	WD_D_62	Działka numer 124/4, obręb Skokowa, arkusz 1, szafa zewnętrzna
65	WD_Sobótka	WD_63	D	WD_D_63	Działka numer 1/6, obręb Sobótka, arkusz 18, szafa zewnętrzna
66	WD_Stara Kamienica	WD_64	D	WD_D_64	Działka numer 388/2, obręb Stara Kamienica, arkusz 1, szafa zewnętrzna
67	WD_Sulików	WD_65	D	WD_D_65	Działka numer 54/1, obręb Sulików, arkusz 2, szafa zewnętrzna
68	WD_Szczytna	WD_66	D	WD_D_66	Działka numer 270, obręb Szczytna, arkusz



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Lp	TYP_Nazwa Węzła	Nr węzła	Klasa węzła	Nr logiczny	Lokalizacja węzła
					6, szafa zewnętrzna
69	WD_Szklarska Poręba	WD_67	D	WD_D_67	Działka numer 385/1, obręb Szklarska Poręba N-5, arkusz 6, szafa zewnętrzna
70	WD_Środa Śląska	WD_68	D	WD_D_68	Działka numer: 39/5, obręb Środa Śląska, arkusz 2, szafa zewnętrzna
71	WD_Świerzawa	WD_69	D	WD_D_69	Działka numer 1/4, obręb Świerzawa, arkusz 1, szafa zewnętrzna
72	WD_Trzebnica	WD_70	D	WD_D_70	Działka numer: 43/3, obręb Trzebnica, arkusz 16, szafa zewnętrzna
73	WD_Warta Bolesławiecka	WD_71	D	WD_D_71	Działka numer 526, obręb Warta Bolesławiecka, arkusz 1, szafa zewnętrzna
74	WD_Wądroże Wielkie	WD_72	D	WD_D_72	Działka numer 1, obręb Wądroże Wielkie, arkusz 1, szafa zewnętrzna
75	WD_Wąsosz	WD_73	D	WD_D_73	Działka numer 656, obręb Wąsosz, arkusz 15, szafa zewnętrzna
76	WD_Węglińiec	WD_74	D	WD_D_74	Działka numer 237, obręb Węglińiec N-2, arkusz 1, szafa zewnętrzna
77	WD_Wiązów	WD_75	D	WD_D_75	Działka numer 237/1, obręb Wiązów, arkusz 2, szafa zewnętrzna
78	WD_Wierzchno	WD_76	D	WD_D_76	działka numer: 382/8 obręb Wierzchno arkusz, szafa zewnętrzna
79	WD_Wleń	WD_77	D	WD_D_77	Działka numer 33, Obręb Wleń N-1, arkusz 1, szafa zewnętrzna
80	WD_Wojcieszków	WD_78	D	WD_D_78	Działka numer 238/10, obręb Wojcieszków N-4, arkusz 1, szafa zewnętrzna
81	WD_Zagrodno	WD_79	D	WD_D_79	Działka numer 658, obręb Zagrodno, arkusz 4, szafa zewnętrzna
82	WD_Zawonia	WD_80	D	WD_D_80	Działka numer 130/2, obręb Zawonia, szafa zewnętrzna
83	WD_Zebrzydowa	WD_81	D	WD_D_81	Działka numer: 800, obręb Zebrzydowa, arkusz 1, szafa zewnętrzna
84	WD_Zgorzelec	WD_82	D	WD_D_82	Działka numer 23, obręb Zgorzelec N-7, arkusz 5, szafa zewnętrzna
85	WD_Ziębice	WD_83	D	WD_D_83	Działka numer: 41, obręb Zachód, arkusz 24, szafa zewnętrzna
86	WD_Złoty Stok	WD_84	D	WD_D_84	Działka numer 4, obręb Złoty Stok, arkusz 10, szafa zewnętrzna
87	WD_Żórawina	WD_85	D	WD_D_85	Działka numer 150/6, Żórawina, arkusz 1, szafa zewnętrzna
<b>Węzły dystrybucyjne klasy E</b>					
88	WD_Góra	WD_16	E	WD_E_16	Działka numer 180, obręb Góra, arkusz 7, szafa zewnętrzna
89	WD_Łagiewniki Dzierżoniowskie	WD_34	E	WD_E_34	Działka numer 453/2, obręb Łagiewniki, arkusz 6, szafa zewnętrzna
90	WD_Ścinawa	WD_59	E	WD_E_59	Działka numer: 541/4, obręb Ścinawa N-2, arkusz 23, szafa zewnętrzna
<b>Węzły dystrybucyjne klasy F</b>					
91	WD_Oleśnica	WD_47	F	WD_F_47	Działka numer: 2/1, obręb Oleśnica, arkusz



**PROGRAM REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Lp.	TYP_Nazwa Węzła	Nr węzła	Klasa węzła	Nr logiczny	Lokalizacja węzła
					53, szafa zewnętrzna
<b>Centrum Zarządzania Siecią we Wrocławiu</b>					
92	CZS Wrocław	CZS	CZS	CZS	WS Wrocław, ul. Mazowiecka 15, dz. nr 17, AM-2, obręb Południe, Serwerownia MIT, pomieszczenia 14 i 15
<b>Zapaszowe Centrum Zarządzania Siecią w Świdnicy</b>					
93	ZCZS_Świdnica	zCZS	zCZS	zCZS	działka numer 1/10 obręb Śródmieście N-4, Arkusz 10, kontener oraz pomieszczenia wydzielone w budynku dworca PKP

## 6.2 Zestawienie montowanych urządzeń wg lokalizacji węzłów

Lp.	Nazwa węzła	Numer logiczny węzła	Zestawienie zamontowanych urządzeń *
1.	WS_Bolesławiec	WS_C1_1	Router szkieletowy model C1 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
2.	WS_Jelenia Góra	WS_C2_3	Router szkieletowy model C2 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 2 -kpl.
3.	WS_Kłodzko	WS_C2_4	Router szkieletowy model C2 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
4.	WS_Legnica	WS_C3_5	Router szkieletowy model C3 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 2 -kpl.
5.	WS_Lubań	WS_C1_6	Router szkieletowy model C1 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
6.	WS_Strzelin	WS_C2_7	Router szkieletowy model C2 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
7.	WS_Rudna	WS_C2_8	Router szkieletowy model C2 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
8.	WS_Wałbrzych	WS_C3_9	Router szkieletowy model C3 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
9.	Wrocław (WS i CZS)	WS_C3_10, CZS	Router szkieletowy model C3 - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Zapora ogniowa w konfiguracji klastra (HA) - 1 kpl. Przełącznik sieciowy CZS (modułarny lub stos) - 1 kpl. System zarządzania siecią - 1 kpl. System prezentacji stanu sieci – 1 kpl. Przełącznik sieci zarządzającej - 2 kpl. Router IXP_1 - 1 kpl. Router IXP_2 - 1 kpl.

Lp.	Nazwa węzła	Numer logiczny węzła	Zestawienie zamontowanych urządzeń *
10.	WD_Góra	WD_E_16	Router dystrybucyjny model E - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
11.	WD_Ścinawa	WD_E_59	router dystrybucyjny model E - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
12.	WD_Łagiewniki	WD_E_34	router dystrybucyjny model E - 1 kpl. Przełącznik sieci zarządzającej 1 -kpl.
13.	Świdnica (zCZS)	zCZS	Router dystrybucyjny model E - 1 kpl. Zapora ogniowa w konfiguracji klastra (HA) - 1 kpl. Przełącznik sieciowy CZS (modularny lub stos) - 1 kpl. System zarządzania siecią System Prezentacji stanu sieci - 1 kpl. Przełącznik sieci zarządzającej - 2 kpl.
14.	WD_Oleśnica	WD_F_47	Router dystrybucyjny model E - 1 kpl. Urządzenie systemu DWDM - 1 kpl. Przełącznik sieci zarządzającej – 1 kpl.
15.	Wrocław IXP_1 Joannitów	IXP_1	Opcjonalnie (zamiast w WS_Wrocław) router IXP - 1 kpl.
16.	Wrocław IXP_2 Bernardyńska	IXP_2	Opcjonalnie (zamiast w WS_Wrocław) router IXP - 1 kpl.
17.	Pozostałe niewymienione węzły dystrybucyjne klasy D zgodnie z tabelą 6.1	WD_D_x	Przełącznik sieci zarządzającej - 1 kpl.

\* Wymagania zamontowanych urządzeń zgodnie z danymi zawartymi w tabeli 6.3.

### 6.3 Lista urządzeń podlegających dostawie

Lp.	Nazwa urządzenia	Ilość	Opis wymagań
1	Router szkieletowy model C1	2 kpl. <sup>1)</sup>	Pkt 4.5.2, 4.8.1
2	Router szkieletowy model C2	4 kpl. <sup>1)</sup>	Pkt 4.5.2, 4.8.1
3	Router szkieletowy model C3	3 kpl. <sup>1)</sup>	Pkt 4.5.2, 4.8.1
4	Router dystrybucyjny model E	5 kpl. <sup>1)</sup>	Pkt 4.5.3, 4.8.2
5	Urządzenie systemu DWDM	10 kpl. <sup>1)</sup>	Pkt 4.5.7, 4.8.6
6	Router IXP	2 kpl. <sup>1)</sup>	Pkt 4.5.5, 4.8.3
7	Zapora ogniowa (firewall)	2 kpl. <sup>2)</sup>	Pkt 4.5.8, 4.8.5.2
8	Przełącznik CZS	2 kpl. <sup>3)</sup>	Pkt 4.5.8, 4.8.5.1
9	System zarządzania siecią	2 kpl.	Pkt 4.5.8, 4.8.5.3
10	System prezentacji stanu sieci	2 kpl.	Pkt 4.5.8, 4.8.5.4
11	Przełącznik sieci zarządzającej – Typ 1	75 kpl. <sup>1)</sup>	Pkt 4.5.4, 4.8.4
12	Przełącznik sieci zarządzającej – Typ 2	8 kpl. <sup>1)</sup>	Pkt 4.5.4, 4.8.4
13	Przełącznik sieci zarządzającej – Typ 3	17 kpl. <sup>1) 5)</sup>	Pkt 4.5.4, 4.8.4
14	Przełącznik sieci zarządzającej – Typ 4	11 kpl. <sup>1)</sup>	Pkt 4.5.4, 4.8.4
15	Patchcord kat. 6 – 1m	25 szt. <sup>4)</sup>	Pkt 4.8.5.5
16	Patchcord kat. 6 – 3m	50 szt. <sup>4)</sup>	Pkt 4.8.5.5



**PROGRAM REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Lp.	Nazwa urządzenia	Ilość	Opis wymagań
17	Patchcord kat. 6 – 5m	50 szt. <sup>4)</sup>	Pkt 4.8.5.5
18	Patchcord kat. 6 – 7m	100 szt. <sup>4)</sup>	Pkt 4.8.5.5
19	Patchcord jednomodowy duplexowy – 1m	32 szt. <sup>4)</sup>	Pkt 4.8.5.5
20	Patchcord jednomodowy duplexowy – 3m	64 szt. <sup>4)</sup>	Pkt 4.8.5.5
21	Patchcord jednomodowy duplexowy – 5m	64 szt. <sup>4)</sup>	Pkt 4.8.5.5
22	Patchcord jednomodowy duplexowy – 10m	20 szt. <sup>4)</sup>	Pkt 4.8.5.5
23	Patchcord jednomodowy duplexowy – 1m	64 szt. <sup>4)</sup>	Pkt 4.8.5.5
24	Patchcord jednomodowy duplexowy – 3m	128 szt. <sup>4)</sup>	Pkt 4.8.5.5
25	Patchcord jednomodowy duplexowy – 5m	128 szt. <sup>4)</sup>	Pkt 4.8.5.5
26	Patchcord jednomodowy duplexowy – 10m	20 szt. <sup>4)</sup>	Pkt 4.8.5.5

- <sup>1)</sup> Komplet oznacza urządzenie wraz z kompletnym okablowaniem np. kable zasilające, akcesoriami (np. wkładki SFP) niezbędnymi do jego uruchomienia
- <sup>2)</sup> Komplet stanowi para urządzeń pracujących w klastrze
- <sup>3)</sup> Komplet stanowi para urządzeń tworzących stos lub jedno urządzenie modułowe
- <sup>4)</sup> Wskazane ilości patchcordów są ilościami minimalnymi. Wykonawca zobowiązany jest dostarczyć komplet okablowania, w tym patchcordsy, do dostarczanych urządzeń, tak by zapewnić wszystkie połączenia między dostarczającymi urządzeniami oraz infrastrukturą pasywną węzłów.
- <sup>5)</sup> Liczba przełączników może być mniejsza, jeśli zastosowane zostaną przełączniki o większej niż 8 liczbie portów optycznych.

## 6.4 Lista czynności do wykonania

Lp	Opis czynności	Ilość	Wymagania
1	Dostawa, zamontowanie, uruchomienie i konfiguracja routera szkieletowego	9 kpl.	Pkt 4.5.2, 4.8.1, 4.9.3
2	Dostawa, zamontowanie, uruchomienie i konfiguracja routera dystrybucyjnego	5 kpl.	Pkt 4.5.3, 4.8.2, 4.9.3
3	Dostawa, zamontowanie, uruchomienie i konfiguracja krotnicy DWDM	10 kpl.	Pkt 4.5.7, 4.8.6, 4.9.3
4	Dostawa, zamontowanie, uruchomienie i konfiguracja routera IXP	2 kpl.	Pkt 4.5.5, 4.8.3, 4.9.3
5	Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika sieci zarządzającej	111 kpl.	Pkt 4.5.4, 4.8.4, 4.9.3
6	Dostawa, zamontowanie, uruchomienie i konfiguracja przełącznika CZS	2 kpl.	Pkt 4.5.8, 4.8.5.1, 4.9.3
7	Dostawa, zamontowanie, uruchomienie i konfiguracja systemu Zapory Ogniowej	2 kpl.	Pkt 4.5.8, 4.8.5.2, 4.9.3
8	Dostawa, zamontowanie, uruchomienie i konfiguracja systemu prezentacji stanu sieci	2 kpl.	Pkt 4.5.8, 4.8.5.4, 4.9.3
9	Dostawa, zamontowanie, uruchomienie i konfiguracja systemu zarządzania siecią	2 kpl.	Pkt 4.5.8, 4.8.5.3, 4.9.3
10	Wykonanie krosowania patchcord-em UTP kat.6	225 szt.	Pkt 4.8.5.5
11	Wykonanie krosowania patchcord-em światłowodowym duplexowym	520 szt.	Pkt 4.8.5.5
12	Opracowanie planu wdrożenia	1 szt.	Pkt 4.9.1



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



13	Opracowanie polityki bezpieczeństwa	1 szt.	Pkt 4.9.2
14	Wykonanie testów akceptacyjnych	1 kpl.	Pkt 4.10
15	Przeprowadzenie szkoleń	1 kpl.	Pkt 4.11

## 6.5 Tabela orientacyjnych \* długości relacji międzywęzłowych

Lp	Relacja	Długość włókien [km]
1	WS_Wrocław - WS_Legnica	82,5
2	WS_Legnica - WS_Wałbrzych	92,0
3	WS_Wałbrzych - WS_Wrocław	124,5
4	WS_Wałbrzych - Świdnica_CZS	47,1
5	Świdnica_CZS - WS_Wrocław	77,4
6	WS_Wrocław - WS_Rudna Miasto	82,4
7	WS_Rudna Miasto - WS_Bolesławiec	90,8
8	WS_Bolesławiec - WS_Lubań	51,8
9	WS_Lubań - WS_Jelenia Góra	61,6
10	WS_Jelenia Góra - WS_Wałbrzych	50,3
11	WS_Jelenia Góra - WS_Legnica	86,3
12	WS_Wrocław - WS_Strzelin	44,1
13	WS_Strzelin - WS_Kłodzko	62,0
14	WS_Kłodzko - WS_Wałbrzych	66,7
15	WS_Legnica - WS_Bolesławiec	52,4
16	WS_Rudna Miasto - WS_Legnica	43,4
17	WS_Wałbrzych - WS_Strzelin	154,6
18	WS_Wałbrzych - Świdnica_CZS	47,1
19	Świdnica_CZS - WS_Strzelin	107,5
20	WS_Wrocław - WD_Oleśnica	40,2

\* wartości orientacyjne wyznaczone na podstawie koncepcji; ostateczna weryfikacja długości nastąpi po opracowaniu projektów budowlanych i wykonawczych.

## 6.6 Tabela orientacyjnych wartości dyspersji chromatycznej dla relacji

Lp	Relacja	Długość włókien [km]	Dyspersja chromatyczna [ps/nm]
1	WS_Wrocław - WS_Legnica	82,5	1 402,50
2	WS_Legnica - WS_Wałbrzych	92,0	1 564,00
3	WS_Wałbrzych - WS_Wrocław	124,5	2 116,50
4	WS_Wałbrzych - Świdnica_CZS	47,1	800,70

Lp	Relacja	Długość włókien [km]	Dyspersja chromatyczna [ps/nm]
5	Świdnica_CZS - WS_Wrocław	77,4	1 315,80
6	WS_Wrocław - WS_Rudna Miasto	82,4	1 400,80
7	WS_Rudna Miasto - WS_Bolesławiec	90,8	1 543,60
8	WS_Bolesławiec - WS_Lubań	51,8	880,60
9	WS_Lubań - WS_Jelenia Góra	61,6	1 047,20
10	WS_Jelenia Góra - WS_Wałbrzych	50,3	855,10
11	WS_Jelenia Góra - WS_Legnica	86,3	1 467,10
12	WS_Wrocław - WS_Strzelin	44,1	749,70
13	WS_Strzelin - WS_Kłodzko	62,0	1 054,00
14	WS_Kłodzko - WS_Wałbrzych	66,7	1 133,90
15	WS_Legnica - WS_Bolesławiec	52,4	890,80
16	WS_Rudna Miasto - WS_Legnica	43,4	737,80
17	WS_Wałbrzych - WS_Strzelin	154,6	2 628,20
18	WS_Wałbrzych - Świdnica_CZS	47,1	800,70
19	Świdnica_CZS - WS_Strzelin	107,5	1 827,50
20	WS_Wrocław - WD_Oleśnica	40,2	683,40

## 6.7 Tabela orientacyjnych wartości tłumienności dla relacji

Lp	Relacja	Długość włókien [km]	Tłumienie [dB]	Tłumienie+rezerwa [dB]
1	WS_Wrocław - WS_Legnica	82,5	20,63	25,63
2	WS_Legnica - WS_Wałbrzych	92,0	23,00	28,00
3	WS_Wałbrzych - WS_Wrocław	124,5	31,13	36,13
4	WS_Wałbrzych - Świdnica_CZS	47,1	11,78	16,78
5	Świdnica_CZS - WS_Wrocław	77,4	19,35	24,35
6	WS_Wrocław - WS_Rudna Miasto	82,4	20,60	25,60
7	WS_Rudna Miasto - WS_Bolesławiec	90,8	22,70	27,70
8	WS_Bolesławiec - WS_Lubań	51,8	12,95	17,95
9	WS_Lubań - WS_Jelenia Góra	61,6	15,40	20,40
10	WS_Jelenia Góra - WS_Wałbrzych	50,3	12,58	17,58
11	WS_Jelenia Góra - WS_Legnica	86,3	21,58	26,58
12	WS_Wrocław - WS_Strzelin	44,1	11,03	16,03
13	WS_Strzelin - WS_Kłodzko	62,0	15,50	20,50
14	WS_Kłodzko - WS_Wałbrzych	66,7	16,68	21,68
15	WS_Legnica - WS_Bolesławiec	52,4	13,10	18,10
16	WS_Rudna Miasto - WS_Legnica	43,4	10,85	15,85
17	WS_Wałbrzych - WS_Strzelin	154,6	38,65	43,65



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





18	WS_Wałbrzych - Świdnica_CZS	47,1	11,78	16,78
19	Świdnica_CZS - WS_Strzelin	107,5	26,88	31,88
20	WS_Wrocław - WD_Oleśnica	40,2	10,05	15,05

## 6.8 Macierz przepływności łączy DWDM

		Bolesławiec	Jelenia Góra	Kłodzko	Legnica	Lubań	Strzelin	Rudna	Wałbrzych	Wrocław	Oleśnica
		WS_1	WS_2	WS_3	WS_4	WS_5	WS_6	WS_7	WS_8	WS_9	WD_47
Bolesławiec	WS_1				5 x 10G	4 x 10G		4 x 10G			
Jelenia Góra	WS_2				4 x 10G	4 x 10G			5 x 10G		
Kłodzko	WS_3						6 x 10G		6 x 10G		
Legnica	WS_4								1 x 100G	1 x 100G	
		5 x 10G	4 x 10G					5 x 10G	1 x 10G	1 x 10G	
Lubań	WS_5	4x 10G	4 x 10G								
Strzelin	WS_6			6 x 10G					4 x 10G	6 x 10G	
Rudna	WS_7	4 x 10G			5 x 10G					6 x 10G	
Wałbrzych	WS_8				1 x 100G					1 x 100G	
			5 x 10G	6 x 10G	1 x 10G		4 x 10G			1 x 10G	
Wrocław	WS_9				1 x 100G				1 x 100G		
					1 x 10G		6 x 10G	6 x 10G	1 x 10G		4 x 10G
Oleśnica	WD_47									4 x 10G	

## 6.9 Macierz zajętości włókien w szkieletzie sieci

		Legnica	Lubań	Rudna
7		WS_5	WS_6	WS_8
Bolesławiec	WS_1	3 x 10G	2 x 10G	2 x 10G
		2J	2J	2J

		Lubań	Legnica	Wałbrzych
7		WS_6	WS_5	WS_9
Jelenia Góra	WS_3	2 x 10G	2 x 10G	3 x 10G
		2J	2J	2J

		Wałbrzych	Strzelin
8		WS_9	WS_7
Kłodzko	WS_4	4 x 10G	4 x 10G
		2J	2J



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



<b>8+2</b>		<b>Bolesławiec</b>	<b>Jelenia Góra</b>	<b>Wrocław</b>	<b>Rudna</b>
		WS_1	WS_3	WS_10	WS_8
<b>Legnica</b>	WS_5	3 x 10G	2 x 10G	1x100G	3 x 10G
		2J	2J	2J	2J

<b>4</b>		<b>Bolesławiec</b>	<b>Jelenia Góra</b>
		WS_1	WS_3
<b>Lubań</b>	WS_6	2 x 10G	2 x 10G
		2J	2J

<b>12</b>		<b>Kłodzko</b>	<b>Wrocław</b>	<b>Wałbrzych</b>	<b>Łagiewniki</b>
		WS_4	WS_10	WS_9	WD_34
<b>Strzelin</b>	WS_7	4 x 10G	4 x 10G	4 x 10G	2 x 10G
		2J	2J	2J	4J

<b>11</b>		<b>Legnica</b>	<b>Wrocław</b>	<b>Bolesławiec</b>	<b>Ścinawa</b>	<b>Góra</b>
		WS_5	WS_10	WS_1	WD_59	WD_16
<b>Rudna</b>	WS_8	3 x 10G	4 x 10G	2 x 10G	1 x 10G	1 x 10G
		2J	2J	2J	2J	2J

<b>10+2</b>		<b>Jelenia Góra</b>	<b>Wrocław</b>	<b>Kłodzko</b>	<b>Strzelin</b>	<b>Sobótka</b>
		WS_3	WS_10	WS_4	WS_7	WD_63
<b>Wałbrzych</b>	WS_9	3 x 10G	1 x 100G	4 x 10G	2 x 10G	1 x 10G
		2J	2J	2J	2J	2J

<b>12+2</b>		<b>Rudna</b>	<b>Legnica</b>	<b>Wałbrzych</b>	<b>Strzelin</b>	<b>Sobótka</b>	<b>Oleśnica</b>	<b>Ścinawa</b>
		WS_8	WS_5	WS_9	WS_7	WD_63	WD_47	WD_59
<b>Wrocław</b>	WS_10	4 x 10G	1 x 100G	1 x 100G	4 x 10G	1 x 10G	2 x 10G	1 x 10G
		2J	2J	2J	2J	2J	4J	2J

<b>2</b>		<b>Góra</b>
		WD_16
<b>Ścinawa</b>	WD_59	1 x 10G
		2J

(\*)Dodatkowo zawsze dwa włókna dla każdej lokalizacji WS i WD dla sieci zarządzania

## 6.10 Tabela dodatkowych wymagań dla routerów szkieletowych

### RS\_C1-3

Lp.	Parametr	C1 mały	C2 średni	C3 duży
1	Minimalna przepustowość matrycy przełączającej	400 Gb/s	1 Tb/s	1 Tb/s
2	Ilość Interfejsów Ethernet 1G SFP	40	40	40
3	Ilość Interfejsów Ethernet 10G XFP lub SFP+	8	12	12
4	Ilość Interfejsów Ethernet 100G CFP	n/d	n/d	2
5	Minimalna przepustowość routera per slot	40 Gb/s Full Duplex	100 Gb/s Full Duplex	100 Gb/s Full Duplex
6	Minimalna liczba obsługiwanych prefixów IPv4/IPv6 (w tablicy FIB)	1mln/0,5mln	1mln/0,5mln	1mln/0,5mln
7	minimalna liczba obsługiwanych tras/grup multicastowych	64k/1000	64k/1000	64k/1000
8	minimalna liczba L3 VPN / aktywnych tras na pojedynczy L3 VPN	2000/64k	3000/64k	3000/64k
9	minimalna liczba instancji VPLS / adresów MAC	2000/64k	3000/64k	3000/64k
10	minimalna liczba jednoczesnych sesji BGP	256	256	256
11	minimalna liczba obsługiwanych filtrów dla pakietów (IPv4 i IPv6)	10k	10k	10k

## 6.11 Tabela dodatkowych wymagań dla routerów dystrybucyjnych model E

Lp.	Parametr	Wartość
1	minimalna przepustowość routera	40 Gb/s Full Duplex
2	minimalna ilość Interfejsów Ethernet 1G SFP	20
3	minimalna ilość Interfejsów Ethernet 10G XFP/SFP+	4
4	minimalna liczba interfejsów Ethernet 1G per chassis	40
5	minimalna liczba interfejsów Ethernet 10G per chassis	4
6	minimalna liczba obsługiwanych prefixów IPv4/IPv6 (w tablicy FIB)	1mln/0,5mln
7	minimalna liczba obsługiwanych tras/grup multicastowych	64k/1000
8	minimalna liczba L3 VPN / aktywnych tras na pojedynczy L3 VPN	1000/64k
9	minimalna liczba instancji VPLS / adresów MAC	500/16k
10	minimalna liczba jednoczesnych sesji BGP	256
11	minimalna liczba obsługiwanych filtrów dla pakietów (IPv4 i IPv6)	10k

## 6.12 Lista testów do wykonania dla routerów szkieletowych i dystrybucyjnych

Lp.	Nazwa testu	Wykonywana operacja	Opis konfiguracji Wykonywana operacja	Oczekiwane zachowanie określające poprawne wykonanie testu	Wynik i testu
1	OSPF	Konfiguracja protokołu routingu OSPF	Konfiguracja AREAO pomiędzy 3 urządzeniami WS i 1 WD, ustalenie typu połączenia Point-to-Point	Nawiązanie sąsiedztwa, budowa topologii sieci	
2	IS-IS	Konfiguracja protokołu IS-IS, linki typu L2, test autentykacji linku, test redystrybucji prefiksów statycznych i przyłączeniowych	Konfiguracja protokołu IS-IS, Konfiguracja linku typu Level-2 Autentykacja pakietów LSA i Hello hasłem z hashem md5 Eksport trasy statycznej i przyłączeniowej do protokołu IS-IS	Nawiązanie sąsiedztwa, prawidłowa, redystrybucja trasy statycznej	
3	BGP	Konfiguracja protokołu BGP, ustalenie peeringu pomiędzy routerami DSS i routerem dostępowym Operatora	Uruchomienie protokołu BGP, zestawienie sąsiedztwa pomiędzy routerami DSS i routerem Operatora z pełną tablicą prefiksów BGP,	Ściągnięcie tablicy globalnej routingu	

Lp.	Nazwa testu	Wykonywana operacja	Opis konfiguracji Wykonywana operacja	Oczekiwane zachowanie określające poprawne wykonanie testu	Wynik i testu
4	MPLS <sup>1</sup> (LDP)	Uruchomienie protokołu LDP,	Konfiguracja protokołu LDP, ustawienie ID na adres lo0.	Przypisanie etykiet prefiksom z tablicy routingu	
5	MPLS <sup>1</sup> L3VPN	Zestawienie tunelu L3VPN z pomiędzy routerami szkieletowymi	Zestawienie tunelu L3VPN z wykorzystaniem LDP pomiędzy routerami szkieletowymi, , sprawdzenie tablicy routingu w nowym VRF-ie, sprawdzenie komunikacji między hostami	W tablicy routingu dla VRF-a powinny pojawić się prefiksy sieci prywatnej, nawiązania komunikacji (ICMP) poprzez tunel między dwoma urządzeniami pełniącymi rolę urządzeń CE	
6	MPLS <sup>1</sup> L2VPN (draft-martini)	Zestawienie tunelu L2VPN między routerami szkieletowymi	Konfiguracja tunelu L2VPN przechodzącego przez routery szkieletowe i dystrybucyjny	Test komunikacji z hosta podłączonego przez routerami szkieletowymi wybranymi jako końce tunelu	
7	CoS	Konfiguracja markowania ruchu i na jej podstawie odpowiednie przydzielenie pasma.	Konfiguracja Class-of-Service spełniająca założone warunki, założenie polityki CoS na interfejsy, testy host-to-host	Założony powinien zostać policer na całość ruchu do wartości 1 Mb/s, ruch FTP do 100 kb/s trafiał do klasy X i jest markowany jako EF jeśli wartość została przekroczona trafiał do klasy Y i markowany był innym znacznikiem DSCP	
8	Przełączenie routingu IGP	Dołożyć link bezpośredni między dwoma skrajnymi routerami szkieletowymi	Konfiguracja routerów szkieletowego do obsługi OSPF, MPLS LDP, RSVP, rozłączyć następnie dodatkowy link	Pingowanie z jednego routera hostów umieszczonych za drugim, obserwacja poziomu strat w momencie przełączenia, Oczekiwany czas przełączenia – ok 2sek	
9	Przełączenie ścieżek MPLS <sup>1</sup>	Konfiguracja obsługi MPLS LDP pomiędzy 3 routerami	Rozłączenie połączenia i test przełączenia ścieżek LSP	Pingowanie z hosta za routerem WS końcówkę tunelu L3VPN zestawionego do skrajnego routera WS , obserwacja poziomu strat w momencie przełączenia, Oczekiwany czas przełączenia – 2sek	
10	Wyjęcie modułu kontrolo-przełączającego	Fizyczne wyjęcie modułu	Konfiguracja obsługi synchronizacji tablic routingu pomiędzy modułem podstawowym i backupowym, Fizyczne	Host podłączony do badanego routera generujący ruch ICMP do zdalnego hosta za tunelem L3VPN. Oczekiwana	

<sup>1</sup> W przypadku wyboru i stosowania technologii MPLS przez Operatora Infrastruktury


**PROGRAM REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



Lp.	Nazwa testu	Wykonywana operacja	Opis konfiguracji Wykonywana operacja	Oczekiwane zachowanie określające poprawne wykonanie testu	Wynik i testu
			wyjęcie modułu aktywnego obserwacja ruchu w momencie przełączenia, włożenie z powrotem i wyjęcie modułu będącego pierwotnie modułem backupowym obserwacja ruchu	degradacja ruchu na poziomie braku transmisji kilkun pakietów	
11	Bezprzerwow upgrade oprogramowania routera	Test upgrade-u software-u na jednym z routerów WS	Test ICMP z hosta podłączonego do badanego routera do hosta za tunelem L3VPN	Test ICMP z hosta podłączonego do badanego routera do hosta za tunelem L3VPN, oczekiwana degradacja ruchu na poziomie braku transmisji kilkun pakietów	
12	Multicast	Konfiguracja protokołu PIM – Dense Mode	Ściągnięcie grup multicastowych	Weryfikacja grup multicastowych, sąsiedztwa PIM	
13	Zagregowany interfejs, agregacja interfejsów	Dołożenie linku dodatkowego pomiędzy dwa routery WS i konfiguracja protokołu zgodnego z IEEE 802.3ad (LACP)	Konfiguracja interfejsu zagregowanego pomiędzy dwoma routerami szkieletowymi, wypięcie jednego linku, test ICMP pomiędzy dwoma badanymi routerami	Prawidłowe zestawienie interfejsu zagregowanego, utrata pojedynczych pakietów ICMP (max 1-2)	

### 6.13 Maksymalne dopuszczalne wartości opóźnień i strat pakietów w zależności od klasy ruchu

Kategoria usługi	Usługa	Typ usługi	Pasmo (kb/s)	Opóźnienie (jednokierunkowe typu koniec-koniec)	Fluktuacja (Jitter)	Poziom utraty pakietów
Usługi głosowe	Rozmowa telefoniczna	Dwukierunkowy (konwersacyjny)	4-25	< 150 ms typowo, 400 ms max.	< 1ms	< 3%
	Wideo media	Strumieniowanie	5-128	10 s max.	< 2ms	< 3%
	Wideo wiadomości	Strumieniowanie	4-13	< 1 s playback 2 s max	< 1ms	< 3%
Usługi video	Wideo fonia	Dwukierunkowy (konwersacyjny)	32-384	< 150 ms typowo, 400 ms max. < 100 ms lip-sync	< 10ms	< 3%
	Wideo media	Strumieniowanie	4-25	10 s max.	< 2s	< 2%
Dane 1	Przeglądanie stron	Interaktywny	Określa SLA	< 0,5 s typowo	n/a	0
Dane 2	Pobór danych dla aplikacji mobilnych	W tle	< 1 KB	< 0,5 s typowo	n/a	0
Dane 3	Telemetria	Interaktywny	< 28,8 K	< 0,5 s typowo	n/a	0



**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIĘĆ  
SZKIELETOWA  
DSS

UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



## 7 Uwagi końcowe

Całość prac wykonać zgodnie ze wskazanymi normami oraz przepisami obowiązującymi chwili wykonywania prac. Wszystkie zastosowane urządzenia i materiały muszą posiadać odpowiednie atesty albo/i certyfikaty dopuszczające do obrotu i stosowania. Zaproponowane w niniejszej dokumentacji materiały można zamienić na inne, równoważne technicznie po uzgodnieniu z Inwestorem i Inspektorem Nadzoru, przy aprobacie projektanta. Przed oddaniem systemu do użytkowania należy wykonać wskazane badania, pomiary i testy akceptacyjne. Ich wyniki, zapisane w protokołach, muszą być pozytywne, spełniając określone przepisami (normami) wymagania.

## 8 Informacja BIOZ

### 8.1 Lista urządzeń podlegających dostawie

Informację BIOZ opracowano zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 23. czerwca 2003 r. w sprawie dotyczącej bezpieczeństwa i ochrony zdrowia (Dz. U. Nr 120/2003, poz. 1126). Zgodnie z Rozporządzeniem Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r., w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy, pracodawca jest zobowiązany ocenić oraz określić szczegółowe wymagania bezpieczeństwa i ochrony zdrowia w trakcie realizacji projektu.

### 8.2 Zakres stosowania

Niniejsza informacja dotyczy zagrożeń występujących podczas wykonania robót oraz montażu urządzeń, zgodnie z zakresem rzeczowym niniejszego projektu.

### 8.3 Zakres wykonywania robót

1. roboty instalacyjne w budynku, kontenerze telekomunikacyjnym, szafie zewnętrznej
2. prace montażowe.



## 8.4 Przewidywane zagrożenia

### 8.4.1 Wykaz elementów – potencjalnych źródeł zagrożenia

Niżej wymienione elementy istniejącej infrastruktury mogą stworzyć zagrożenie bezpieczeństwa i zdrowia ludzi:

1. diody laserowe nadajników optycznych,
2. przyłącza kablowe i instalacje elektroenergetyczne nN,
3. przyłącza i instalacje wod-kan,
4. instalacje CO,
5. drogi wewnętrzne komunikacyjne i transportowe w obiektach.

Powyższe elementy należy wziąć pod uwagę przy wykonywaniu prac.

### 8.4.2 Wykaz zagrożeń i ryzyk

Niżej wymienione zagrożenia i ryzyka mogą wystąpić przy wykonywaniu prac:

1. upadek z wysokości (drabiny),
2. uszkodzenie ciała od ręcznego dźwigania zbyt dużych ciężarów lub uderzenia,
3. porażenie prądem w czasie prac instalacyjnych lub montażowych związanych z zasilaniem systemu,
4. niebezpieczeństwo uszkodzenia oka (siatkówki lub rogówki) promieniowaniem lasera.

## 8.5 Środki zapobiegania niebezpieczeństwom

Wymagania dotyczące ogólnych przepisów bezpieczeństwa i higieny pracy określa Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r. w sprawie bezpieczeństwa i higieny pracy: Rozdział 6, ustęp B: Roboty budowlane, rozbiórkowe, remontowe i montażowe prowadzone bez wstrzymywania ruchu zakładu pracy lub jego części, Rozdział 6, ustęp D: Prace przy użyciu materiałów niebezpiecznych.

Przy pracy z urządzeniami laserowymi stosować się do zaleceń: PN-EN 60825-1:2000, PN-91/T-06700 Bezpieczeństwo przy promieniowaniu emitowanym przez urządzenia laserowe. Klasyfikacja

sprzętu. Wymagania i wytyczne dla użytkownika, PN-91/T-06701 Bezpieczeństwo elektryczne urządzeń i instalacji laserowych.

Pracodawca powinien opracować szczegółowe wymagania dla bezpiecznego prowadzenia tych prac, w szczególności:

1. zapewnić nadzór nad tymi pracami,
2. stosować odpowiednie środki zabezpieczające,
3. zastosować imienny podział pracy,
4. ustalić właściwą kolejność wykonywanych zadań,
5. zadbać o odzież ochronną, kaski, rękawice i okulary ochronne.

Pracownicy zatrudnieni na budowie powinni mieć następujące przeszkolenie BHP:

1. wstępne, ogólne,
2. podstawowe lub okresowe,
3. stanowiskowe.

Przed rozpoczęciem robót należy:

1. sprawdzić sprawność sprzętu,
2. pouczyć pracowników o bezpiecznych metodach pracy na określonych stanowiskach,
3. powierzyć obsługę sprzętu wykwalifikowanym pracownikom,
4. odpowiednio zagospodarować i przygotować teren budowy,
5. wykonać odpowiednie ogrodzenie i oznakowanie miejsca pracy,
6. zapewnić urządzenie pomieszczeń higieniczno-sanitarnych,
7. zapewnić łączność alarmową (telefoniczną),
8. wyłączyć i uziemić urządzenia energetyczne – linie zasilające nN,
9. wywiesić tablice ostrzegawcze o treści „nie załączać”,
10. sprawdzić oznaczenie nadajników laserowych etykietami ostrzegawczymi, w przypadku ich braku zamontować dobrze widoczne etykiety o treści „Uwaga – promieniowanie laserowe niewidoczne dla oka, chronić oczy”,
11. sprawdzić poprawność sygnalizacji emisji promieniowania (sygnalizacji załączenia urządzeń).

Przy montażu należy zapewnić przestrzeganie instrukcji montażu poszczególnych urządzeń.

## 9 Załączniki

Z-1. Kopie uprawnień i wpisów do właściwych Izb projektantów i sprawdzających

Z-2. Rysunki

1. Blokowy schemat rozptywu włókien
2. Topologia geograficzna połączeń tras światłowodowych DSS
3. Schemat organizacji połączeń sieci IP w rdzeniu sieci DSS
4. Schemat organizacji połączeń sieci DWDM w DSS
5. Schemat ogólny połączeń w sieci DSS
6. Schemat logiczny organizacji podłączeń routerów IXP do szkieletu sieci DSS
7. Schemat logiczny organizacji połączeń w zCZS Świdnica w DSS
8. Schemat logiczny organizacji połączeń w CZS Wrocław w DSS
9. Symboliczny schemat połączeń między Przełącznikami Sieci Zarządzającej
- 9A. Schemat połączeń między Przełącznikami Sieci Zarządzającej
10. Rozmieszczenie urządzeń w szafach w węźle szkieletowym i CZS Wrocław
11. Rozmieszczenie urządzeń w szafach we wszystkich węzłach szkieletowych oprócz Wrocławia
12. Rozmieszczenie urządzeń w szafie zewnętrznej dla węzła dystrybucyjnego klasy F (Oleśnica)
13. Rozmieszczenie urządzeń w szafie zewnętrznej dla węzła dystrybucyjnego klasy E (Góra, Ścinawa, Łagiewniki)
14. Rozmieszczenie urządzeń w szafie zewnętrznej dla węzłów dystrybucyjnych klasy D
15. Rozmieszczenie urządzeń w szafach kontenera oraz budynku dworca zCZS Świdnica

## **Z-1. Kopie uprawnień i wpisów do właściwych Izb projektantów i sprawdzających**





**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO







**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO





**PROGRAM  
REGIONALNY**  
NARODOWA STRATEGIA SPÓJNOŚCI



**DOLNY  
ŚLĄSK**

DOLNOŚLĄSKA  
SIEĆ  
SZKIELETOWA



UNIA EUROPEJSKA  
EUROPEJSKI FUNDUSZ  
ROZWOJU REGIONALNEGO



## Z-2. Rysunki

