Jednostka organizacyjna:
Instytut Telekomunikacji, Teleinformatyki i Akustyki

Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej

Część 2:
Wymagania dla dokumentacji części aktywnej sieci
Seria: Wersja 1.5

Autor: Dr inż. Jacek Oko
Dr inż. Rafał Królikowski
Andrzej Maciejewski

Słowa kluczowe:
Infrastruktura teleinformatyczna

Krótkie streszczenie:
Dokument ustanawia standardy i szczegółowe specyfikacje techniczne w zakresie przygotowania wykonawczej i powykonawczej dokumentacji projektowej dotyczącej projektowania i budowy Dolnośląskiej Sieci Szkieletowej (DSS) jako sieci klasy NGN w zakresie części aktywnej sieci

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Metryka dokumentu					
Projekt:	Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej				
Beneficjent:	Województwo Dolnośląskie				
Wykonawca:	Instytut Telekomunikacji, Teleinformatyki i Akustyki Politechnika Wrocławska				
Rodzaj dokumentu:	Dokument standaryzacyjny				
Tytuł dokumentu:	Wymagania techniczne dla wykonawczej i powykonawczej dokumentacji projektowej Część 2: Wymagania dla dokumentacji części aktywnej sieci				
Autor/Autorzy dokumentu:	Zespół projektowy w składzie: Jacek Oko, Rafał Królikowski, Andrzej Maciejewski Korekty od wersji 1.1: Dariusz Balcerzak, Adam Okniński				
Nr wersji:	1.4	**Status:**		**Data**	21.06.2013
Sprawdził:			**Data i Podpis:**		
Zatwierdził:			**Data i Podpis:**		

Historia zmian dokumentu			
Wersja	**Data**	**Osoba/ Osoby**	**Opis**
1.0	17.06.2011	Zespół projektowy	Opracowanie pierwotnej wersji dokumentu
1.1	22.11.2011	Zespół projektowy	Errata pierwotnej wersji dokumentu
1.2	16.04.2012	Beneficjent	Uzupełniono dokument o wymóg wspierania przez urządzenia DWDM standardu ITU-T G.698.2 (alien wavelength transmission)
1.3	25.01.2013	Beneficjent	Zaktualizowano dokument w oparciu o wyniki badania rynku dostawców sprzętu aktywnego. Zmodyfikowano zapisy zagrażające ograniczeniem konkurencji. Usunięto odwołania do nieaktualnych standardów.
1.4	21.06.2013	Beneficjent	Zaktualizowano odwołania do standardów. Zmodyfikowano zapisy zagrażające ograniczeniem konkurencji.
1.5	16.07.2014	Beneficjent	Zaktualizowano dokument w oparciu o pytania i wnioski Kandydatów na Operatora Infrastruktury. Zmodyfikowano zapisy zagrażające ograniczeniem konkurencji.

Wrocław, 16.07.2014

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Spis treści:

Spis ilustracji:

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Spis tabel:

1 Informacje podstawowe i definicje

Rozdział obejmuje informacje podstawowe oraz definicje (wraz ze skrótami) stosowane w niniejszym opracowaniu a w szczególności:

- Słownik,
- Symbolikę i oznaczenia,
- Reguły nazewnictwa i numeracji.

1.1 Ogólne definicje i używane skróty

Na potrzeby niniejszego dokumentu przyjęto grupę definicji:

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

CZS – Centrum Zarządzania Siecią DSS

DHCP - ang. *Dynamic Host Configuration Protocol* – standardowy protokół przypisujący adres IP komputerom w sieci lokalnej. Komputer klienta wywołuje serwer DHCP, aby otrzymać adres IP lub inne informacje konfiguracyjne (np. adresy DNS, WINS, itp.).

DMZ - ang. *DeMilitarised Zone* – strefa zdemilitaryzowana, bądź ograniczonego zaufania, wyodrębniona fizycznie część sieci chroniona częściowo przez zaporę sieciową (ang. *firewall*); jest to wydzielony na zaporze sieciowej firewall obszar sieci komputerowej nie należący ani do sieci wewnętrznej (tj. tej chronionej przez zaporę), ani do sieci zewnętrznej (tej przed zaporą; na ogół jest to Internet). W strefie zdemilitaryzowanej umieszczane są serwery „zwiększonego ryzyka włamania", przede wszystkim świadczące usługi użytkownikom sieci zewnętrznej, którym ze względów bezpieczeństwa nie umożliwia się dostępu do sieci wewnętrznej (najczęściej są to serwery WWW i FTP).

Dostawca – podmiot realizujący dostawy kompletnego systemu mikrokanalizacji i okablowania światowego wraz z osprzętem na zamówienie Inwestora lub Wykonawcy

DSS – Dolnośląska Sieć Szkieletowa, zamiennie do celów promocyjnych używane jest też rozwinięcie „Dolnośląska Sieć Szerokopasmowa",

EoMPLS - ang. *Ethernet over MPLS* – przesyłanie ramek protokołu sieci lokalnej Ethernet przez sieć MPLS, tunelowanie.

Firewall - ang. *firewall* - zapora sieciowa/zapora przeciwogniowa – jeden ze sposobów zabezpieczania sieci i systemów przed intruzami. Termin ten może odnosić się zarówno do dedykowanego sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do sieci lub komputera, które chroni. Pełni zwykle rolę ochrony sieci wewnętrznej LAN przed niepowołanym dostępem z zewnątrz tzn. z sieci publicznej, np. Internetu.

FTP - ang. *Foiled Twisted Pair* – skrętka foliowana.

Inwestor – Województwo Dolnośląskie - Urząd Marszałkowski Województwa Dolnośląskiego

IP - ang. *Internet Protocol* - podstawowy protokół z rodziny protokołów TCP/IP, będącej podstawą komunikacji w Internecie. Oparty jest na komutacji pakietów.

IPS - ang. *Intrusion Prevention System* - systemy wykrywania i zapobiegania włamaniom. Urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie i blokowanie ataków w czasie rzeczywistym.

ISO-OSI - model OSI (ang. *Open System Interconnection*) – standard zdefiniowany przez ISO oraz ITU-T, o pełnej nazwie ISO OSI RM, opisujący strukturę komunikacji sieciowej. Model odniesienia łączenia systemów otwartych ISO OSI RM (ang. *ISO OSI Reference Model*) jest traktowany jako model odniesienia (wzorzec) dla większości rodzin protokołów komunikacyjnych. Podstawowym założeniem modelu jest podział systemów sieciowych na siedem warstw (ang. *layers*) współpracujących ze sobą w ściśle określony sposób. Dla Internetu sformułowano uproszczony Model DoD, który ma tylko cztery warstwy.

IXP - ang. *Internet eXchange Point* – punkt styku sieci różnych dostawców usług internetowych, w którym realizowana jest wymiana ruchu między tymi sieciami.

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

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

MPLS - ang. *Multiprotocol Label Switching* – to technologia stosowana przez routery, w której routing pakietów został zastąpiony przez tzw. przełączanie etykiet. Na brzegu sieci z protokołem MPLS do pakietu dołączana jest dodatkowa informacja zwana etykietą (ang. *label*). Router po odebraniu pakietu z etykietą (jest to z punktu widzenia danego routera etykieta wejściowa) używa jej jako indeksu do wewnętrznej tablicy etykiet, w której zdefiniowane są następne punkty sieciowe (ang. *next hop*) oraz nowa etykieta (etykieta wyjściowa). Etykieta wejściowa jest zastępowana wyjściową i pakiet jest wysyłany do następnego punktu sieciowego (np. do następnego routera). Jeżeli następny router nie obsługuje protokołu MPLS, etykieta jest usuwana i pakiet kierowany jest dalej według standardowej tablicy routingu. Pomimo że teoretycznie istnieje możliwość zastosowania MPLS do przełączania pakietów dowolnego protokołu routowalnego (na co wskazuje słowo multiprotocol w nazwie), praktyczne zastosowania dotyczą jedynie protokołu IP.

Multicast - rodzaj transmisji, w której dokładnie jeden punkt wysyła pakiety do wielu punktów (ale nie do wszystkich tak jak w ramach transmisji rozsiewczej). Istnieje tylko jeden nadawca i wielu odbiorców. Przykładem takiej transmisji może być transmisja sygnału radia internetowego.

Nadsubskrypcja - ang. *Overbooking* – stosunek maksymalnego zapotrzebowania na pasmo do rzeczywistego dostarczanego użytkownikowi. Zwykle mieści się w przedziale 5:1 – 20:1.

NAT - ang. *Network Address Translation* (nazywany też w jednej ze swych odmian maskaradą – ang. *masquerade*) – technika translacji adresów sieciowych stosowana, gdy sieć lokalna używa adresów prywatnych IP lub w celu zabezpieczenia sieci lokalnej przed atakami z zewnątrz.

NGA - ang. *Next Generation Access* - sieć dostępowa następnej generacji, sieć mająca w przyszłości zastąpić dotychczas stosowane rodzaje sieci dostępowych i zapewniająca nieograniczony dostęp do szerokopasmowych usług dla odbiorców końcowych. Jest terminem

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

odnoszącym się do kluczowych zmian w architekturze dostępowyej sieci telekomunikacyjnych, które nastąpią w ciągu następnych 5-10 lat.

NGN - ang. *Next Generation Network* - sieć następnej generacji, sieć pakietowa realizująca usługi telekomunikacyjne i wykorzystująca wiele szerokopasmowych technik transportowych z gwarancją jakości usług (QoS), w której funkcje usługowe są niezależne od wykorzystywanych technik transportowych. Jest to terminem odnoszącym się do kluczowych zmian w architekturze rozległych sieci telekomunikacyjnych, które nastąpią w ciągu następnych 5-10 lat.

Operator Infrastruktury - podmiot wybrany przez Zamawiającego, którego zadaniem będzie zarządzanie i utrzymanie DSS oraz świadczenie usług telekomunikacyjnych z jej wykorzystaniem,

Operatorski Punkt Dostępowy (OPD) – punkt styku (przełącznica światłowodowa) sieci DSS z sieciami innych operatorów

OSPF - ang. *Open Shortest Path First* – w wolnym tłumaczeniu „pierwszeństwo ma najkrótsza ścieżka". Jest to wewnętrzny protokół routingu typu stanu łącza (ang. *link state*), co oznacza, że w ramach pojedynczego obszaru wszystkie routery znają całą jego topologię i wymieniają się między sobą informacjami o stanie łącz, a każdy z nich przelicza trasy samodzielnie (algorytm Dijkstry). Między obszarami OSPF działa jak protokół oparty na wektorach odległości (typu distance-vector), co oznacza że routery brzegowe obszarów wymieniają się między sobą gotowymi trasami. Protokół ten opisany jest w dokumentach RFC 2328 i jest zalecany wśród protokołów niezależnych np. RIP (ang. *Routing Information Protocol*). W przeciwieństwie do protokołu RIP, OSPF charakteryzuje się dobrą skalowalnością, wyborem optymalnych ścieżek i brakiem ograniczenia skoków powyżej 15, a także przyspieszoną zbieżnością. Przeznaczony jest dla sieci posiadających do 50 routerów w wyznaczonym obszarze routingu. Cechami protokołu OSPF są: routing wielościeżkowy, routing najmniejszym kosztem i równoważne obciążenia.

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

Peering - wymiana ruchu pomiędzy dostawcami usług internetowych (ISP) na zasadach partnerskich, zwykle darmowa. Dostawcy usług internetowych łączą swoje sieci za pomocą punktów połączeń (ang. *peering point*), następnie zawierają umowę peeringową, która dokładnie precyzuje zasady wymiany przez nich ruchu.

Q-in-Q - jest opisane w standardzie 802.1Q-in-Q. Rozwiązanie to jest też nazywane składaną na stosie siecią VLAN. Jest to rozszerzenie standardu 802.1Q. Pozwala zachować ustawienia sieci VLAN użytkownika i zagwarantować transparentność jej działania w sieci dostawcy. Dzięki temu dostawca usługi może w ramach jednej sieci VLAN obsługiwać wiele sieci VLAN użytkowników. Formalizując definicje ramek Ethernet dla wielu znaczników VLAN, opracowano rozszerzenie do 802.1ad Provider Bridge na potrzeby „tunelowania" ruchu użytkownika przesyłanego w postaci sieci VLAN.

QoS - ang. *Quality of Service* – jakość obsługi. Do zapewnienia jakości QoS stosowane są następujące mechanizmy:

- kształtowanie i ograniczanie przepustowości;
- zapewnienie sprawiedliwego dostępu do zasobów;
- nadawanie odpowiednich priorytetów poszczególnym pakietom wędrującym przez sieć;
- zarządzanie opóźnieniami w przesyłaniu danych;
- zarządzanie buforowaniem nadmiarowych pakietów: DRR, WFQ, WRR;
- określenie charakterystyki gubienia pakietów;

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- unikanie przeciążeń: Connection Admission Control (CAC), Usage Parameter Control (UPC).

RIP - ang. *Routing Information Protocol*, czyli protokół informowania o trasach, należy do grupy protokołów bram wewnętrznych (IGP). Oparty jest na zestawie algorytmów wektorowych, służących do obliczania najlepszej trasy do celu.

Router - urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI, pełniące rolę węzła komunikacyjnego.

SAN - ang. *Storage Area Network* - sieć pamięci masowej. Rodzaj sieci służący do dostępu do zasobów pamięci masowej przez systemy komputerowe.

Sieć dostępowa - sieć łącząca końcowych odbiorców usług sieciowych z lokalnym dostawcą usług. Punktami styku sieci dostepowych z DSS są węzły dostępowe DSS.

Sieć dystrybucyjna - sieć pośrednicząca w wymianie ruchu między sieciami dostępowymi, a siecią szkieletową.

Sieć szerokopasmowa - rozległa sieć komputerowa, zbudowana z wykorzystaniem infrastruktury szerokopasmowej.

Sieć szkieletowa - wysoko wydajna struktura sieciowa łącząca poszczególne części składowe sieci (np. sieci dystrybucyjne i dostępowe). Urządzenia wchodzące w strukturę sieci szkieletowej z reguły odpowiedzialne są za funkcjonowanie całej sieci na określonym obszarze.

SLA - ang. *Service Level Agreement* - jest to umowa utrzymania i systematycznego poprawiania ustalonego między klientem a usługodawcą poziomu jakości usług informatycznych.

Tranzyt IP - płatna wymiana ruchu, w której operator nadrzędny tranzytuje ruch od podłączonego operatora i jego klientów do wybranych części lub całości sieci Internet wykorzystując do tego własne łącza peeringowe i tranzytowe.

TVoIP - ang. *Television over Internet Protocol* - technologia cyfrowa umożliwiająca przesyłanie sygnału telewizji cyfrowej za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP.

Ustalenia techniczne - należy przez to rozumieć ustalenia podane w normach, aprobatach technicznych i szczegółowych specyfikacjach technicznych,

UPS - ang. *Uninterruptible Power Supply* - zasilacz bezprzerwowy. Urządzenie lub system, którego funkcją jest nieprzerwane zasilanie innych urządzeń elektronicznych.

VoIP - ang. *Voice over Internet Protocol* - technologia cyfrowa umożliwiająca przesyłanie mowy za pomocą łączy internetowych lub dedykowanych sieci wykorzystujących protokół IP.

VPN - ang. *Virtual Private Network* - prywatna sieć wirtualna zbudowana przy użyciu publicznych łączy pomiędzy węzłami. Wiele systemów umożliwia tworzenie sieci za pomocą Internetu. Stosuje się w nich szyfrowanie i inne mechanizmy ochrony, które zapewniają dostęp tylko uprawnionym użytkownikom.

WDM - WDM (ang. *Wavelength Division Multiplexing*) – zwielokrotnianie w dziedzinie długości fali. Systemy wykorzystujące technikę WDM występują w dwu podstawowych odmianach:

- systemy z dużym odstępem międzykanałowym (ang. Coarse Wavelenght Division Multiplexing; CWDM)
- systemy z gęstym podziałem międzykanałowym (ang Dense Wavelenght Division Multiplexing; DWDM).

Węzeł sieci - urządzenie sieciowe (lub zespół urządzeń), zawierające wiele łączy telekomunikacyjnych i kierujące przesyłaniem informacji z łączy wejściowych na odpowiednie łącza wyjściowe. Węzły mogą realizować funkcje: retransmisyjne – wzmocnienia/regeneracji sygnału (węzły

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

szkieletowe), agregacji ruchu telekomunikacyjnego (węzły agregacyjne i szkieletowo-agregacyjne) oraz dostępu do sieci lub styku z innymi sieciami (węzły dostępowe pasywne i aktywne),

WiFi - ang. *Wireless Fidelity* - określa zestaw standardów z rodziny 802.11x stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem WiFi jest budowa sieci lokalnych (LAN) opartych na komunikacji radiowej, czyli WLAN.

Wykonawca DSS – wybrany podmiot realizujący budowę sieci DSS wg zatwierdzonej dokumentacji projektowej.

2 Dokumenty bazowe

Niniejszy rozdział wymienia podstawowe standardy i funkcjonalności związane z budową sieci szkieletowych w podziale na technologie.

Załączony zestaw dokumentów standaryzacyjnych stanowi punkt odniesienia dla prac projektowych uszczegóławiających wykorzystanie poszczególnych technologii. Szereg podstawowych standardów (głównie związanych z IPv4) powszechnie obsługiwanych przez urządzenia sieciowe zostało tu pominiętych. Niektóre ze standardów mogą mieć także nowsze wersje.

2.1 Technologia Ethernet

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- IEEE 802.3 – podstawowy zestaw standardów definiujących technologię Ethernet, w tym podstawowy schemat ramki i metody transmisji
- IEEE 802.3u – transmisja 100BaseTX
- IEEE 802.3z – transmisja 1000BaseX
- IEEE 802.3ab – transmisja 1000BaseT
- IEEE 802.3ae – transmisja 10Gbit/s przez światłowód
- IEEE 802.3ba – transmisja 100Gbit/s
- IEEE 802.3ad – agregacja łączy (łącza równoległe)
- IEEE 802.1 – zestaw standardów związanych z przesyłaniem danych w sieci Ethernet
- IEEE 802.1D – przełączanie (ang. bridging) ramek Ethernet
- IEEE 802.1q – obsługa znaczników wirtualnych sieci LAN (ang. Virtual LAN, VLAN)
- IEEE 802.1ad – obsługa zagnieżdżonych znaczników VLAN (ang. PBB, Provider Backbone Bridges), znana potocznie jako QinQ
- IEEE 802.1ah – obsługa zagnieżdżonych nagłówków Ethernet (ang. Provider Backbone Bridges, PBB)
- IEEE 802.1s – obsługa wielu instancji protokołu drzew rozpinających (ang. MSTP, Multiple Spanning Tree Protocol)
- IEEE 802.1ag – wykrywanie usterek w łączności (ang. CFM, Connectivity Fault Management)
- ITU-T Y.1731 – telekomunikacyjny odpowiednik IEEE 802.1ag
- MEF 16 E-LMI – komunikacja na styku usługowym Ethernet
- IETF RFC 2665 – Etherlike-MIB, baza informacji MIB dla protokołu SNMP

2.2 IPv6

W niniejszym obszarze należy wykorzystać, co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 1981 „Path MTU discovery for IPv6” – długość przenoszonych pakietów

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- RFC 2460 „IPv6 Specification” – podstawowe definicje protokołu
- RFC 2461 „Neighbor Discovery for IPv6” – mechanizm odkrywania sąsiadów/routerów
- RFC 2462 „IPv6 Stateless Address Autoconfiguration” – autokonfiguracja adresów
- RFC 2464 „Transmission of IPv6 over Ethernet Networks” – przenoszenie IPv6 w sieci Ethernet
- RFC 2545 „Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing” – rozszerzenie protokołu BGP do przenoszenia informacji o IPv6
- RFC 2711 „IPv6 Router Alert Option” – rozszerzenie do obsługi protokołów typu RSVP
- RFC 3587 „IPv6 Global Unicast Address Format” – format adresacji IPv6
- RFC 4443 „ICMPv6 (ICMP for IPv6)” – ICMP rozszerzone do obsługi IPv6
- RFC 2710 „Multicast Listener Discovery (MLD) for IPv6” – mechanizm zastępujący IGMP w IPv6
- RFC 3810 „Multicast Listener Discovery Version 2 for IPv6” – nowsza wersja MLD

2.3 Multicast IPv4 i IPv6

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 1112 „Host Extensions for IP Multicasting” – obsługa multicast (w tym IGMP) przez urządzenia końcowe
- RFC 2362 „Protocol Independent Multicast Sparse Mode PIM-SM” – podstawowy protokół routingu multicast
- RFC 2858 „Multiprotocol extensions for BGP4” – rozszerzenia BGP do obsługi multicast
- RFC 3376 „Internet Group Management Protocol Version 3” – najnowsza wersja IGMP
- RFC 3618 „Multicast Source Discovery Protocol” – protokół MSDP przenoszący informacje o źródłach multicast pomiędzy domenami administracyjnymi

2.4 Routing IPv4 i IPv6

2.4.1 OSPF

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 2328 „OSPF Version 2” – aktualna definicja protokołu dla IPv4
- RFC 2370 „OSPF Opaque LSA Option” – obsługa rozszerzeń
- RFC 2740 „OSPF for IPv6” – rozszerzenie protokołu OSPF do przenoszenia informacji o IPv6, czyli OSPFv3
- RFC 3101 „OSPF Not-So-Stubby Area (NSSA)” – rozszerzenie funkcjonalności w specyficznych topologiach
- RFC 3137 „OSPF Stub Router Advertisement” – umożliwia ‘omijanie’ routera przez ruch bez wyłączania go
- RFC 3623 „Graceful OSPF Restart” – rozszerzenia umożliwiające przełączanie się na zapasowy moduł sterujący urządzenia bez utraty sesji, przy współpracy urządzeń sąsiednich

- RFC 4552 „Authentication/Confidentiality for OSPFv3” – zabezpieczenie sesji OSPFv3

2.4.2 IS-IS

W niniejszym obszarze należy wykorzystać, co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 1142 „OSI IS-IS Intra-domain Routing Protocol” – definicja protokołu, zaczerpnięta z norm ISO
- RFC 1195 „Use of OSI IS-IS for routing in TCP/IP and Dual Environments” – zastosowanie IS-IS do sieci IP
- RFC 2973 „IS-IS Mesh Groups” – redukcja ilości rozgłoszeń
- RFC 3373 „Three-Way Handshake for IS-IS” – usprawniony mechanizm nawiązywania sąsiedztwa

2.4.3 BGP

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 1997 „BGP Communities Attribute” – definicje podstawowych elementów protokołu BGP
- RFC 2385 „Protection of BGP Sessions via TCP MD5 Signature Option” – zabezpieczenie sesji BGP szyfrowanym hasłem
- RFC 2439 „BGP Route Flap Dampening” – optymalizacja działania protokołu przy częstych zmianach tras
- RFC 2796 „BGP Route Reflection” – optymalizacja przeliczania BGP dzięki zastosowaniu dedykowanych urządzeń
- RFC 2858 „Multiprotocol Extensions for BGP-4” – rozszerzenia BGP do przenoszenia informacji o protokołach innych niż IPv4
- RFC 2918 „Route Refresh Capability for BGP-4” – odświeżanie informacji bez zrywania sesji z sąsiadem
- RFC 3065 „Autonomous System BGP-4 Confederations” – optymalizacja rozsyłania informacji BGP dla szeregu urządzeń
- RFC 3392 „Capabilities Advertisement with BGP-4” – rozgłaszanie zdolności urządzenia poprzez BGP
- RFC 4271 „Border Gateway Protocol 4 (BGP-4)” – aktualna definicja protokołu
- RFC 4893 „BGP Support for Four-octet AS Number Space” – rozszerzenie o obsługę czterobajtowych numerów AS (rozszerzenie przestrzeni adresowej podobne w pewnym sensie do przejścia z IPv4 na IPv6).

2.5 Technologia MPLS

2.5.1 MPLS

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- RFC 3031 „MPLS Architecture" – podstawowy dokument opisujący technologię MPLS
- RFC 3032 „MPLS Label Stack Encoding" – implementacja stosu etykiet
- RFC 3036 „LDP Specification" – specyfikacja protokołu LDP przenoszącego sygnalizację dla MPLS
- RFC 3270 „MPLS Support of Differentiated Services" – obsługa mechanizmów różnicowania jakości usług przez MPLS

2.5.2 Wirtualne sieci prywatne VPN

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 3107 „Carrying Label Information in BGP-4" – rozszerzenia BGP do przenoszenia informacji o etykietach MPLS
- RFC 4364 „BGP/MPLS IP Virtual Private Networks" – rozszerzenia BGP do przenoszenia informacji o sieciach VPN
- RFC 4448 „Encapsulation Methods for Transport of Ethernet over MPLS Networks" – format ramki do przenoszenia sieci VPN warstwy 2 ISO/OSI przez sieć MPLS
- RFC 4576 „Using LSA Options Bit to Prevent Looping in BGP or MPLS IP VPNs (DN Bit)" – optymalizacja w celu zapobiegania pętlom routingowym w sieci.
- RFC 4577 „OSPF as the PE or CE Protocol in BGP or MPLS IP VPNs" – zastosowanie OSPF jako protokołu między siecia operatora a klientem
- RFC 4762 „Virtual Private LAN Service (VPLS) Using LDP Signaling" – metoda tworzenia emulowanej sieci warstwy drugiej (VPLS) na bazie sieci MPLS
- Certyfikacja MEF (Metro Ethernet Forum) – MEF 9 oraz MEF 14 potwierdzające prawidłową implementację usług L2/L3 VPN

2.5.3 Inżynieria ruchu MPLS-TE

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych:

- RFC 2702 „Requirements for Traffic Engineering over MPLS" – opis inżynierii ruchu MPLS
- RFC 2747 „RSVP Cryptographic Authentication" – uwierzytelnianie sesji protokołu RSVP wykorzystywanego do zestawiania połączeń inżynierii ruchu
- RFC 3209 „RSVP-TE: Extensions to RSVP for LSP Tunnels" – rozszerzenia protokołu RSVP do przenoszenia informacji o inżynierii ruchu
- RFC 3630 „TE Extensions to OSPF v2" – rozszerzenia umożliwiające transport informacji o inżynierii ruchu MPLS za pomocą OSPF
- RFC 3784 „ISIS-TE" – rozszerzenia protokołu IS-IS umożliwiające przenoszenie informacji o inżynierii ruchu
- RFC 4090 „Fast Re-Route for RSVP-TE Extensions" – rozszerzenia umożliwiające sygnalizację szybkiego przekierowania ruchu w przypadku awarii

2.6 Warstwa transmisyjna

W niniejszym obszarze należy wykorzystać co najmniej zestaw dokumentów standaryzacyjnych w zakresie wykorzystania technik WDM.

- ITU-T G.692:1998 Optical interfaces for multichannel systems with optical amplifiers (Corrigendum 1:2000; Corrigendum 2:2002);
- PN-EN 60825-2:2005 + A1:2007 Bezpieczeństwo urządzeń laserowych - Część 2: Bezpieczeństwo światłowodowych systemów telekomunikacyjnych;

a w zakresie mechanizmów pomiaru

- 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.”

2.7 Zarządzanie siecią i jej elementami – Centrum Zarządzania Siecią

W niniejszym obszarze należy wykorzystać, co najmniej zestaw dokumentów standaryzacyjnych:

- Zalecenie ITU-T M.3010 Principles for a telecommunications management network,
- Zalecenie ITU-T M.3400 TMN management functions,
- Standard ISO/IEC 7498-4:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 4: Management framework.

2.8 Zintegrowany Systemu Nadzoru (ZSN)

Dokumentację projektową oraz prace budowlano-montażowe należy wykonać, zgodnie z podanymi poniżej normami i dokumentami odniesienia:

- Ustawa z dnia 07.07.1994 – Prawo Budowlane (Dz. U. 2006.156.1118 z późniejszymi zmianami).
- Rozporządzenie Ministra Infrastruktury z dnia 2.09.2004 w sprawie szczegółowego zakresu i formy dokumentacji projektowej (Dz. U. 2004.202.2072).
- Rozporządzenie Ministra Infrastruktury z dnia 06.02.2003 w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz. U. 2003.47.401).
- PN-91/E-05009 Instalacje elektryczne w obiektach budowlanych.
- PN-E-08390-1:1996 Systemy alarmowe. Terminologia.
- PN-E-08290-3:1998 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania central.
- PN-E-08390-5:2000 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania sygnalizatorów.
- PN-93/E-08390.11 Systemy alarmowe. Wymagania ogólne. Postanowienia ogólne.
- PN-93/E-08390.12 Systemy alarmowe. Wymagania ogólne. Zasilacze - Parametry funkcjonalne i metody badań.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- PN-93/E-08390.13 Systemy alarmowe. Wymagania ogólne. Próby środowiskowe.
- PN-93/E-08390.14 Systemy alarmowe. Wymagania ogólne. Zasady stosowania.
- PN-93/E-08390.22 Systemy alarmowe. Włamaniowe systemy alarmowe. Ogólne wymagania i badania czujek.
- PN-93/E-08390.23 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania aktywnych czujek podczerwieni.
- PN-93/E-08390.24 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania ultradźwiękowych czujek Dopplera.
- PN-93/E-08390.25 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania mikrofalowych czujek Dopplera.
- PN-93/E-08390.26 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania pasywnych czujek podczerwieni.
- PN-93/E-08390.51 Systemy alarmowe. Systemy transmisji alarmu. Ogólne wymagania dotyczące systemów.
- PN-93/E-08390.52 Systemy alarmowe. Systemy transmisji alarmu. Ogólne wymagania dotyczące urządzeń.
- PN-93/E-08390.54 Systemy alarmowe. Systemy transmisji alarmu. Systemy transmisji alarmu wykorzystujące specjalizowane tory transmisji.
- PN-IEC 839-2-7:1996 Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania pasywnych czujek stłuczenia szyby.
- PN-EN 50133-1:2000 Systemy alarmowe. Systemy kontroli dostępu. Wymagania systemowe.
- PN-EN 50133-7:2000 Systemy alarmowe. Systemy kontroli dostępu. Wytyczne stosowania.
- PN-EN 50132-7:2003 Systemy alarmowe. Systemy dozorowe CCTV stosowane w zabezpieczeniach. Część 7: Wytyczne stosowania.
- PN-EN 50132-5:2002 Systemy alarmowe - Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 5: Teletransmisja.
- PN-EN 50132-2-1:2007 Systemy alarmowe - Systemy dozorowe CCTV stosowane w zastosowaniach dotyczących zabezpieczenia – Część 2-1: Kamery telewizji czarno-białej.
- PN-EN 50131-1:2007 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Wymagania systemowe
- PN-EN 50131-2-2:2008 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 2-2: Czujki włamania – Pasywne czujki podczerwieni.
- PN-EN 50131-2-6:2009 Systemy alarmowe – Systemy sygnalizacji włamania i napadu – Część 2-6: Czujki stykowe (magnetyczne).
- PN-EN 50131-6:2000 Systemy alarmowe. Systemy sygnalizacji włamania. Zasilacze.
- PN-EN 50130-4:2002 Systemy alarmowe – Część 4: Kompatybilność elektromagnetyczna – Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych.
- PN-EN 50130-5:2002 Systemy alarmowe – Część 5: Próby środowiskowe.
- PN-EN 54-2:1998 Systemy sygnalizacji pożarowej – Wprowadzenie.
- PN-EN 54-2:2002 Systemy sygnalizacji pożarowej – Część 2: Centrale sygnalizacji pożarowej.

- PN-EN 54-3:2003 Systemy sygnalizacji pożarowej – Część 3: Pożarowe urządzenia alarmowe – Sygnalizatory akustyczne.
- PN-EN 54-4:2001 Systemy sygnalizacji pożarowej – Część 4: Zasilacze.
- PN-EN 54-12:2005 Systemy sygnalizacji pożarowej – Część 12: Czujki dymu – Czujki liniowe działające z wykorzystaniem wiązki światła przechodzącego,
- PN-EN 54-21:2006 Systemy sygnalizacji pożarowej – Część 21: Urządzenia do transmisji sygnałów alarmowych i uszkodzeniowych.
- WBO CNBOP:2006 Wymagania, metody badań i kryteria oceny: Stałe urządzenia gaśnicze – Aerozolowe Generatory Gaśnicze.
- PN-EN 1047-1:1999 Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja i metody badan odporności ogniowej. Urządzenia do przechowywania nośników informacji.
- PN-EN 1143-1:2000 Pomieszczenia i urządzenia do przechowywania wartości. Klasyfikacja i metody badan odporności na włamanie. Szafy, drzwi do pomieszczeń i pomieszczenia.

3 Wymagania i wytyczne dla dokumentacji projektowo-wykonawczej systemów i urządzeń aktywnych

3.1 Wytyczne ogólne do projektowania sieci klasy NGN

Przy projektowaniu nowoczesnych sieci szkieletowych, określanych także Sieciami Następnej Generacji (ang. NGN, Next Generation Network), należy przyjąć metodologię projektową, która sprowadza złożony problem ogólny (wybudować najlepszą sieć, gdzie „najlepsza" jest definiowane wielowymiarowo) do dającego się opisać w przejrzysty sposób zbioru reguł, zasad i standardów, które taka sieć powinna spełniać.

Metodologia taka opracowana przez Wykonawcę winna zostać zatwierdzona przez Zamawiającego.

Metodologia, zwana też inżynierią sieci, jest w przypadku podmiotów komercyjnych często przedmiotem tajemnicy handlowej. Zbiór szczegółowych informacji na ten temat bywa bowiem owocem lat doświadczeń wynikających nie tylko z technologii, ale też zastosowania technologii do celów komercyjnych.

Istnieje jednak szereg zasad wywodzących się zarówno z technologii, jak i obserwacji rozwoju istniejących dużych sieci telekomunikacyjnych, które pozwalają na zaprojektowanie takich sieci w stosunkowo dużym stopniu szczegółowości.

3.1.1 Cel i środki projektowanych sieci klasy NGN

Celem nadrzędnym istnienia szkieletowych sieci operatorskich, w tym Dolnośląskiej Sieci Szkieletowej (DSS) jest zapewnienie świadczenia usług. Należy uwzględnić iż usługi przez DSS mają być świadczone:

- na potrzeby własne (sieci wewnętrzne, firmowe lub instytucjonalne)
- na potrzeby podmiotów trzecich (sieci operatorskie i publiczne).

By określić model projektowy sieci podstawowym zadaniem jest określenie wymaganych usług, oraz uwarunkowań technicznych, które wpływają na ich świadczenie obecnie i w przyszłości: koszty zakupu, koszty operacyjne, czy też koszty rozbudowy.

Środkami, z których korzysta się przy projektowaniu są zasoby pasywne, zwykle w postaci pewnych lokalizacji, w których możliwe jest zainstalowanie urządzeń aktywnych, oraz kabli światłowodowych łączących te lokalizacji w określonych relacjach. Te elementy określają topologię fizyczną, cechy niezawodnościowe (pierścienie, czy zwielokrotnione łącza), a także w pewnym wpływają na wybór urządzeń aktywnych.

3.1.2 Usługi świadczone przez Dolnośląską Sieć Szkieletową

W rozważanym przypadku Dolnośląska Sieć Szkieletową należy projektować jako sieć na bazie której świadczone są usługi klasy Operator-dla-Operatora (ang. CsC, Carrier supporting Carrier). W projektowanym modelu odbiorcami usług nie są klienci indywidualni, lecz podmioty zbiorcze, to jest inni operatorzy, oraz firmy bądź instytucje. Obok podmiotów operatorskich należy przyjąć również, iż Dolnośląska Sieć Szkieletowa będzie realizować usługi dla innych podmiotów, w tym Jednostek Samorządu Terytorialnego.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Stąd na etapie projektowym należy przyjąć następujące założenia usługowe (dla kryterium rodzaj odbiorcy usług), jako zakres podstawowy:

1. Dolnośląska Sieć Szkieletowa świadczy usługi CsC z podziałem na operatorów krajowych (np. TP, Dialog, UPC, Polkomtel, itd.)
2. Dolnośląska Sieć Szkieletowa świadczy usługi dla lokalnych ISP (w tym sieci również JST)
3. Dolnośląska Sieć Szkieletowa świadczy usługi dla klienta wewnętrznego (Urzędy Administracji Publicznej, JST itp.)

3.1.2.1 Usługi sieci szkieletowej

Podstawowymi usługami świadczonymi przez sieć tego typu jest realizacja połączeń punkt-punkt oraz punkt-wielopunkt pomiędzy szeregiem lokalizacji.

Połączenia punkt-punkt są wykorzystywane przykładowo przez lokalnego operatora, który chce uzyskać „dostęp do Internetu", czyli wymieniać ruch z dużymi operatorami szkieletowymi mającymi swój węzeł zwykle w jednym z centralnych punktów regionu. Lokalni operatorzy szukają możliwie taniego, szybkiego i niezawodnego łącza, na którym mogliby świadczyć w sposób przewidywalny biznesowo swoje usługi.

W ramach aktywności Dolnośląskiej Sieci Szkieletowej należy przyjąć dla operatorów możliwość:

1. Dzierżawa infrastruktury pasywnej sieci:
    - dzierżawa kanalizacji teletechnicznej;
    - dzierżawa ciemnych włókien światłowodowych;
    - usługa kolokacji.
2. Usługi teletransmisyjne
    - Usługi transmisji optycznej
        - optyczne lambdy dla klienta,
        - usługi transmisji punkt-punkt dla dowolnego protokołu,
    - Usługi Ethernet
        - Ethernet Line (Eth LL), Ethernet Virtual Line(VLL), Ethernet LAN (VPLS), Ethernet Virtual LAN (VPLS),
        - Carrier of carriers - Metro Ethernet,
    - Routing IP
        - IP Leased Lines,
        - IP-VPN,
    - Internet access
        - Carrier of IP carriers,
        - Quality Internet,
        - Enhanced Bussines Services.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Połączenia punkt-wielopunkt odpowiadają modelowi lokalnego operatora obecnego w więcej niż jednej lokalizacji, ale także firmom i instytucjom budującym na bazie sieci szkieletowej swoje sieci wewnętrzne.

Sieć szkieletowa do realizacji wyżej wskazanych usług powinna posiadać szereg cech użytkowych wymienionych poniżej

- powinna umożliwić przyjęcie ruchu o zadeklarowanej przepustowości w jednym z węzłów i przesłać taki ruch do innego węzła.
- powinna umożliwiać zróżnicowanie poziomu usługi, poprzez przypisanie do przesyłanego ruchu pewnego priorytetu, decydującego o metodzie reakcji w sytuacji degradacji. Przykładowo najwyższy poziom może mieć ruch głosowy (ang. VoIP, Voice over IP) z zapewnionymi ścieżkami zapasowymi, kolejny poziom ruch krytyczny dla klienta, czyli tzw. ruch biznesowy firmy lub instytucji, a poziom najniższy ruch „w ramach możliwości" (ang. best effort).
- powinna zapewniać w miarę stałe, i możliwie niskie opóźnienia i zmienność opóźnienia przesyłanego ruchu.
- powinna umożliwiać monitorowanie stanu sieci, urządzeń, usług i połączeń.
- powinna umożliwiać monitorowanie informacji ruchowych (przepustowości).
- powinna posiadać zdefiniowaną metodykę rozbudowy gdy zaistnieje konieczność zwiększenia przepustowości, dodania węzła, czy zwiększenia liczby podłączeń końcowych.

Podane cechy odpowiadają wymaganiom stosowanym w komercyjnych sieciach operatorskich.

Ze względu na swoją specyfikę sieć szkieletowa tego typu pomija szereg usług dodatkowych, których świadczenie w odniesieniu do strumieni ruchu indywidualnych abonentów mija się z celem – sieć taka rozważa strumienie zagregowane.

W zależności od koncepcji rozwoju i zastosowania w przyszłości sieć winna uwzględniać świadczenie usług dodanych a co najmniej:

- zoptymalizowana transmisja rozsiewcza (ang. multicast) na potrzeby rozsyłania strumieni zwykle powiązanych z transmisją obrazu w czasie rzeczywistym, np. telewizji. Dzięki technice multicast ruch taki jest przesyłany w sposób możliwie mało obciążający łącza szkieletowe, co ma znaczenie zarówno dla operatora sieci szkieletowej (więcej zasobów dostępnych dla innych usług), jak i operatora usługi telewizyjnej (niższy koszt jej świadczenia).
- monitoring parametrów transmitowanych strumieni wideo.

3.1.2.2 Usługi sieci dystrybucyjnej

W ramach aktywności Dolnośląskiej Sieci Szkieletowej należy przyjąć iż na poziomie sieci dystrybucyjnej realizowane będą usługi dla podmiotów zbiorczych lokalnych oraz klientów wewnętrznych (Urzędy Administracji Publicznej ,JST itp.). Głównym rodzajem oferowanych usług będzie dostęp do szeroko rozumianego Internetu (w przypadku klienta wewnętrznego rozszerzona o usługę klasy Intranet).

Sieć dystrybucyjna do realizacji wyżej wskazanych usług powinna posiadać szereg cech użytkowych wymienionych poniżej

- powinna umożliwić przyjęcie ruchu o zadeklarowanej przepustowości w jednym z węzłów przesłać zakontraktowany ruch w „górę" sieci,

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- powinna umożliwiać zróżnicowanie poziomu usługi na styku z klientem wewnętrznym lub podmiotem zbiorczym, poprzez przypisanie do przesyłanego ruchu pewnego priorytetu, decydującego o metodzie reakcji w sytuacji degradacji,
- powinna zapewniać w miarę stałe, i możliwie niskie opóźnienia i zmienność opóźnienia przesyłanego ruchu,
- powinna umożliwiać monitorowanie stanu sieci, urządzeń, usług i połączeń,
- powinna umożliwiać monitorowanie informacji ruchowych (przepustowości),
- powinna posiadać zdefiniowaną metodykę rozbudowy gdy zaistnieje konieczność zwiększenia przepustowości, dodania węzła, czy zwiększenia liczby podłączeń końcowych.

3.1.3 Kontrakty jakości usług (SLA)

Świadczenie usług opiera się, między innymi, o zapewnienie klientowi wymaganych parametrów technicznych, a także o zdolności wykazania że parametry zostały spełnione zgodnie z kontraktem. W tym celu stosuje się zestandaryzowane dla danego operatora kontrakty jakości usług (ang. SLA, Service Level Agreement) opisujące pewne zestawy parametrów. Wymaganymi minimalnymi parametrami wymaganymi/zapewnianymi w ramach Dolnośląskiej Sieci Szkieletowej są:

- dostępność sieci,
- średnie opóźnienie pakietu wewnątrz szkieletu (w ms),
- procent strat pakietów, często różny dla różnych klas ruchu w ramach jednej usługi.

Kontrakt SLA opisuje także metodologię pomiaru, by uniknąć nieporozumień. Parametry są mierzone wg przyjętej metody przez same urządzenia sieciowe, oraz przez dedykowane sondy pomiarowe, a następnie zbierane w systemie zarządzania.

Dostępność sieci jest liczona z wyłączeniem zapowiadanych okien serwisowych, jako procent czasu poprawnego działania sieci dla danego klienta. Awarie dotykające jedynie części klientów (np. jeden port lub jedna karta w urządzeniu) muszą być korelowane z danymi odpowiednich klientów.

Opóźnienia liczone są między urządzeniami szkieletowymi, z wyłączeniem odcinka dostępowego. Ten ostatni odcinek może być także objęty SLA, o ile operator zarządza urządzeniem klienckim – chodzi o ewentualną odpowiedzialność za nieprawidłową konfigurację i podobne kwestie.

Kolejnym krokiem jest udostępnienie klientom raportów, czy to w formie periodycznej (zwykle comiesięcznej), czy też na bieżąco na specjalnym portalu. Generowaniem raportów mogą się zajmować albo dedykowane systemy, albo dodatkowe moduły większych systemów zarządzania siecią.

3.2 Technologie sieciowe

3.2.1 Przegląd technologii operatorskich

Na rynku istnieje szereg technologii umożliwiających budowę sieci szkieletowych. Czas życia technologii jest zmienny, są wśród zarówno takie, które istniały jedynie przez kilka lat (zwykle specjalizowane technologie producenckie) oraz takie, które są wciąż aktywnie rozwijane, mimo że istnieją od ponad 10 lat, a także takie które dopiero zaczynają być dostosowywane do tego typu sieci, mimo że istnieją dłużej.

Można stwierdzić, że niemal 100% ruchu użytkowego przesyłanego w sieciach jest ruchem opartym na protokole IP. W ramach tego ruchu niemal całość to IPv4, a znikomy ułamek to IPv6.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Należy zauważyć, że z powodu skończenia się w 2011 roku dostępnej puli adresów IPv4 wdrażanie technologii IPv6 zdecydowanie przyspieszyło, i nowe sieci muszą być projektowane z uwzględnieniem współistnienia obydwu protokołów (ang. dual stack) i równoprawnego ich traktowania.

O ile zdecydowana większość ruchu to IP, szereg klientów preferuje by ich ruch był przesyłany nie za pomocą routingu, lecz w sposób bardziej przezroczysty, symulując bezpośrednie połączenie między punktami wirtualnym „kabelkiem".

Obserwując rozwój komercyjnych sieci operatorskich nieuniknione jest stwierdzenie, że można wyróżnić dwie technologie, które stały się podstawą świadczenia większości usług.

Pierwsza z nich to MPLS (ang. Multiprotocol Label Switching), która pozwala na jednym, współdzielonym szkielecie realizować zarówno przesyłanie ruchu internetowego IPv4/v6, tworzenie dedykowanych, separowanych, wirtualnych sieci prywatnych IPv4/v6, a także niezależne przesyłanie ruchu innych technologii, w szczególności Ethernet, ATM czy TDM. MPLS stał się więc standardem „de facto", niezbędnym przy projektowaniu sieci klasy operatorskiej.

Drugą technologią jest technologia Ethernet. Była ona początkowo ograniczona do sieci lokalnych, jednak z racji bardzo niskiej ceny tej technologii transmisji w porównaniu z technologiami tradycyjnie wykorzystywanymi na dłuższych odległościach, jak SDH, została ona przez lata rozwijana i wzbogacana w kierunku zastosowań operatorskich. Obecny standard Ethernet jest bardzo różny od tego oryginalnego, poza formatem ramki i podstawowymi definicjami zmieniła się niemal cała logika sterowania i przełączania ruchu. Taka wzbogacona odmiana nazywana jest często „operatorskim Ethernetem" (ang. Carrier Ethernet), i polega na obsłudze szeregu rozszerzeń pozwalających na zastosowaniu jej na wielką skalę ze zwiększoną niezawodnością i możliwościami zarządzania. Ethernet, będąc technologią warstwy drugiej ISO/OSI, nadaje się równie dobrze do przesyłania ruchu IPv4/v6, jak i ruchu Ethernet i może znajdywać zastosowanie w realizacji sieci regionalnych.

Zarówno sieci IP/MPLS jak i Ethernet zapewniają świadczenie usług punkt-punkt i punkt-wielopunkt z rozmaitymi gwarancjami i innymi opisanymi cechami. Obydwie technologie optymalizują koszty świadczenia tych usług dzięki wykorzystaniu multipleksacji statystycznej, gdzie pojedyncze łącze fizyczne jest w stanie przenosić bardzo zmienny ruch pochodzący od wielu klientów takiej sieci bez konieczności manualnych interwencji i absorbowania dodatkowych zasobów.

W tradycyjnym modelu sieci szkieletowych, podobnie jak w sieciach nowej generacji, dodatkowo można wykorzystać warstwę optyczną, zapewniającą stałą komutację połączeń, głównie za pomocą wirtualnych światłowodów tworzonych dzięki technologii multipleksacji długości fal (ang. WDM, Wavelength Division Multiplexing). Warstwa ta umożliwia dwie zasadnicze rzeczy przy ograniczonych zasobach światłowodowych, to jest przy dostępności pojedynczych par włókien. Jedną z nich jest właśnie powielenie i udostępnienie wielu wirtualnych par włókien, by zwiększyć przepustowość. Drugą jest uniezależnienie topologii fizycznej od logicznej oraz osiąganie większych dystansów, powyżej limitu na jeden odcinek (zależnego od konkretnej przepustowości).

Przy budowie sieci od podstaw (dla całości rozwiązania lub szczególnych relacji) należy rozważyć projektowo i dokonać analizy wraz z uzyskaniem zgody Zamawiającego na:

- stosowanie technologii WDM,
- stosowanie technologii Ethernet,
- stosowanie technologii MPLS.

Wszelkie wymagania sformułowane w niniejszym dokumencie, w szczególności dla technologii stosowanych w rozwiązaniach sprzętowych, mają charakter bezwzględnie obowiązujący jedynie w

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

przypadku, gdy zostały zapisane w postaci nakazów lub zakazów (tj. z wykorzystaniem zwrotów typu: „musi", „wymaga się", „powinno", „należy" lub: „nie może", „nie powinno", „nie wolno", „nie dopuszcza się". Pozostałe wymagania, zapisane z wykorzystaniem zwrotów typu: „rekomenduje się" lub:, „nie rekomenduje się" mają charakter rekomendacji tzn. ich zastosowanie pozostawia się do decyzji Operatora infrastruktury, stosownie do wybranego przez niego modelu biznesowego prowadzenia działalności operatorskiej.

3.2.2 Technologie usługowe

Sieć szkieletowa MPLS/IP dostarcza szereg usług dla protokołu IP, opartych o warstwę trzecią modelu ISO/OSI:

- natywne przesyłanie ruchu IPv4 unicast i multicast
- natywny przesyłanie ruchu IPv6 unicast i multicast
- tunelowanie IPv6 przez MPLS: 6PE
- wirtualne sieci prywatne dla IPv4: VPNv4
- wirtualne sieci prywatne dla IPv6: VPNv6 / 6VPE

Oprócz tego dostępne są także usługi tunelowania ruchu warstwy drugiej ISO/OSI w przezroczysty sposób. Najczęściej stosowane są te dla ruchu Ethernet:

- VPWS (ang. Virtual Private Wire Service), czyli emulowane połączenie punkt-punkt przesyłające ramki Ethernet między dwoma zakończeniami usługi,
- VPLS (ang. Virtual Private LAN Service), czyli emulowany przełącznik wielopunktowy, stosujący reguły sieci Ethernet by przesyłać ruch pomiędzy wieloma zakończeniami usługi.
- hierarchiczny VPLS, gdzie część agregacyjna jest oparta na VPWS a szkieletowa na VPLS. Pozwala to zastosować tańsze urządzenia w części agregacyjnej, kosztem potrzeby dociągnięcia większej ilości ruchu do węzłów szkieletowych.

3.2.3 Przepustowości i rozbudowa łączy

Na podstawie obserwacji stanu aktualnego i rozwoju technologii transmisji, można określić kilka powszechnie wykorzystywanych przepustowości, związanych głównie z gradacją przepustowości w technologii Ethernet:

- 1 Gbit/s Ethernet jest powszechnie stosowany we wszystkich miejscach sieci. Ta przepustowość jest uważana też często za minimalną przepustowość portów do których podłączani są znaczący użytkownicy. Nawet, jeśli użytkownik początkowo wykorzystuje mniejszą przepustowość, zwykle stosuje się łącza o przepustowości większej, np. 1Gbit/s, co pozwala płynnie zwiększać przepustowość udostępnianą użytkownikowi bez wymiany urządzeń. Należy przyjąć, że jest to minimalna przepustowość na brzegu sieci służąca do podłączania klientów. Bywa to też często przepustowość wystarczająca do przesyłania ruchu pomiędzy mniejszymi węzłami sieci. Rozbudowa przepustowości odbywa się zwykle przez zwielokrotnienie łączy lub przez migrację do 10Gbit/s gdy jest to uzasadnione wymaganiami technicznymi i kosztami zmian.
- 10 Gbit/s Ethernet jest powszechnie stosowany do połączeń międzywęzłowych. Jest to minimalna przepustowość rozważana obecnie przy budowie nowych sieci ze względu na korzystne ceny portów, jak i charakterystykę zasięgu. W przypadku konieczności zwiększenia

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

przepustowości sieci łącza takie są zwykle zwielokrotniane do Nx 10Gbit/s. W przypadku największych operatorów obserwuje się już także zastosowanie technologii 40Gbit/s oraz obserwacje i testy technologii 100Gbit/s.

- 40Gbit/s POS przez szereg lat było jedyną wyższą przepustowością komercyjnie dostępną na rynku. Była to technologia droga, ponieważ oparta na hierarchii optycznej SDH, a nie transmisji Ethernet, z tego powodu częściej spotyka się łącza zwielokrotnione Nx 10Gbit/s. Tym niemniej pojedyncze łącze 40Gbit/s ma szereg zalet kosztowo-operacyjnych i na dzień dzisiejszy jest najpewniejszą alternatywą. 100Gbit/s jest bardzo nową technologią, która dopiero wchodzi na rynek. W 2011 roku zaledwie kilku producentów ogłosiło dostępność produktów z takimi portami, większość z nich realizuje taką transmisję w nieoptymalny sposób. Należy oczekiwać, że dopiero w ciągu 2-3 lat technologia dojrzeje i stanie się częściej wykorzystywana, a po kolejnych 3-4 latach powszechna. Zaporowe są też ceny, co wynika z bardzo małego popytu, małej dostępności i braku zysków produkcji komponentów optycznych na dużą skalę. W przypadku budowy sieci szkieletowej należy wziąć pod uwagę możliwość rozbudowy do 100Gbit/s w wybranych relacjach międzywęzłowych należących do ścisłego rdzenia.

Łącza mogą także mieć rozmaite topologie fizyczne. Zwykle spotyka się dwie topologie:

- pierścień, gdy szereg węzłów jest połączonych pomiędzy sobą każdy z następnym i poprzednim. Daje to zwykle najniższy koszt wykonania łączy w sposób zapewniający zapasową ścieżkę w przypadku awarii, a przy tym możliwa jest także realizacja innych topologii logicznych, np. gwiazdy, jeżeli będzie to bardziej optymalne z punktu widzenia świadczonych usług.
- drzewo lub gwiazda, gdy węzeł jest podłączony do jednego (lub dwóch w przypadku redundancji) węzła nadrzędnego, oraz (dla drzewa) szeregu mniejszych węzłów kolejnego stopnia sieci. Także tutaj jest możliwość manipulowania topologią logiczną, na przykład na topologii fizycznej drzewa można zrealizować topologię logiczną gwiazdy.

Zwykle sieci są budowane w topologii hybrydowej, gdzie główne węzły znajdują się na pierścieniu, a węzły kolejnych stopni są podłączone do nich w postaci drzew lub gwiazd.

Wybór konkretnej topologii zależy od optymalizacji kabli, ale także odległości między węzłami, wielkości węzłów, przepustowości przełączanego przez nie ruchu.

Maksymalne długości ścieżek optycznych między węzłami w topologii logicznej należy wyliczyć, jako sumy długości światłowodów pomiędzy lokalizacjami z uwzględnieniem odpowiedniego zapasu na dodatkowe straty na stykach czy w miejscach naprawy światłowodów.

Przykładowo dla technologii 10G Ethernet łącza można podzielić na następujące grupy:

- do 10km, optyka LR, łącza lokalne, połączenia między urządzeniami w tym samym węźle
- do 40km, optyka ER, typowe połączenia między urządzeniami. Należy przyjąć, że ścieżka geograficzna może mieć około 30-35km. Pozostawiony zapas do zasięgu maksymalnego pozwala uwzględnić niektóre nieprzewidziane sytuacje oraz dodatkowe spawy wykonywane w szafach telekomunikacyjnych.
- do 80km, optyka ZR, połączenia o największym zasięgu dla tej technologii. Dobrze jest założyć pozostawienie pewnego zapasu i ograniczenie długości ścieżek do ok. 65-75km.
- dla odcinków ponad 80km można wykorzystać wzmacniacze optyczne umieszczone w węzłach pośrednich. Pozwoli to uzyskać dodatkowy zasięg tam, gdzie jest to niezbędne.

3.3 Wytyczne do projektowania urządzeń sieci klasy NGN w sieci DSS

3.3.1 Model warstwowy

Sieci operatorskie należy budować w oparciu o model warstwowy. Warstwy oznaczają tutaj nie warstwy modelu ISO/OSI, czy też warstwę optyczną i routerową, ale funkcje połączeniowe pełnione przez urządzenia w węzłach należących do poszczególnych warstw.

Na potrzeby sieci DSS należy przyjąć następujące warstwy sieci:

- **warstwa dostępu** - urządzenia realizujące dostęp do użytkowników końcowych. Są to zwykle systemy transmisji typu DSL, CATV, radiowe czy FTTX. Warstwa dostępowa jest wyłączona z zakresu omawianej sieci, ponieważ sieć ta ma stanowić z założenia sieć operatorską nadrzędną, czyli operatorską dla operatorów, a nie sieć świadczącą bezpośrednio usługi użytkownikom indywidualnym. W gestii operatorów lokalnych będzie leżało zapewnienie dostępu obsługiwanym przez nich użytkownikom. Z kolei instytucje i firmy pragnące skorzystać z usług sieci będą korzystały albo z pośrednictwa lokalnych operatorów, lub będą się podłączały bezpośrednio do węzłów agregacyjno-dystrybucyjnych.
- **warstwa agregacji (lub dystrybucji) -** węzły zajmujące się agregacją ruchu pochodzącego od wielu klientów (lokalnych operatorów, instytucji) i przesyłaniem go w kierunku docelowym, przeważnie w kierunku rdzenia sieci, łączami zwykle o wyższej przepustowości. Ze względu na konieczność realizacji polityk usługowych dla danych klientów to te węzły będą musiały posiadać odpowiednie zasoby sprzętowe oraz elastyczność w konfiguracji tych usług.
- **Warstwa rdzenia/szkieletu sieci -** główne węzły zajmujące się przede wszystkim efektywnym przesyłaniem dużych przepustowości ruchu pomiędzy sobą oraz do punktów styku z Internetem. W tego typu węzłach najszybciej kończy się przepustowość (będąca ogólnie sumą przepustowości pochodzących z węzłów niższych), więc to tych węzłów będzie dotyczyć często rozbudowa. Stosunkowo ograniczona liczba węzłów szkieletowych umożliwia mimo wszystko efektywną rozbudowę, w porównaniu z modelem bez takiej warstwy.

Dopuszcza się w szczególnych przypadkach żeby węzeł rdzeniowy pełnił jednocześnie funkcje węzła agregacyjnego dla swojej lokalizacji. Oznacza to wykorzystanie urządzenia posiadającego obydwa zestawy funkcji, lub dwóch niezależnych lecz połączonych urządzeń w danej lokalizacji.

W zależności od wielkości sieci i stopnia złożoności liczba i typ węzłów zmienia się. Na etapie projektu jest zwykle niemożliwe by przewidzieć rozkład ruchu w takiej sieci. O ile w przypadku operatora posiadającego indywidualnych klientów końcowych istnieją modele statystyczne pozwalające określić na przykład ile ruchu generuje przeciętnie 10-tysięczne osiedle, o tyle jest to zbyt zróżnicowane w przypadku instytucji, firm i innych operatorów – zwykle zakłada się więc tylko ogólne profile przepustowościowe.

Zastosowanie dodatkowych mechanizmów sterujących rozpływem ruchu, jak na przykład inżynieria ruchu MPLS (ang. Traffic Engineering) pozwala dopasować obserwowany ruch do wybudowanej topologii w przypadku stwierdzenie rozbieżności w miarę wzrastania poziomu ruchu w sieci.

3.3.2 Niezawodność

Sieci operatorskie stosują szereg równoległych mechanizmów niezawodnościowych. Pozwala to obniżyć straty ruchu, skrócić przerwy w dostępności usług, oraz podwyższyć parametry SLA. Przy projektowaniu sieci DSS należy zastosować poniższe zasady ogólne dotyczące niezawodności:

- **Redundancja zasilania** – w miarę możliwości urządzenia powinny być zaopatrzone w zwielokrotnione zasilacze, uzyskując możliwość bezprzerwowej pracy w wypadku awarii jednego z zasilaczy, bądź jednego z obwodów zasilania (jeżeli każda grupa zasilaczy pracuje na osobnym).
- **Redundancja wentylatorów** – zapobiega przegrzewaniu urządzenia w sytuacji awarii jednego z zainstalowanych wentylatorów.
- **Redundancja modułów sterujących** – kluczowe urządzenia powinny być wyposażone w podwójne moduły sterujące (ang. Route Processor, RP) z funkcją przełączenia w biegu na zapasowe (ang. hot standby), co pozwala uniknąć przerw w dostępności usług w przypadku awarii głównego modułu.
- **Redundancja matrycy przełączających** – nowoczesne urządzenia wykorzystują matryce przełączające, które także powinny zapewnić redundancję, to jest zapewnienie działania niezdegradowanych usług w przypadku awarii jednej z matryc lub jej części.
- **Redundancja modułów liniowych** – w przypadku, gdy urządzenie jest podpięte do szkieletu dwoma niezależnymi ścieżkami, wskazane jest zapewnienie by każde z łączy kończyło się na innej karcie. Pozwala to uniknąć przerwy w przypadku awarii jednej z kart. W przypadku pojedynczych łączy może to też umożliwić przepięcie klienta z karty, która uległa awarii na zapasową już zainstalowaną w urządzeniu, skracając czas przywrócenia usługi.
- **Redundancja łączy** – o ile to możliwe, topologia logiczna powinna zapewniać zapasowe łącze w ramach szkieletu sieci, by uniezależnić się od awarii jednego z łączy.
- **Redundancja ścieżek** – w przypadku redundancji łączy należy zapewnić by łącza przebiegały inną ścieżką fizyczną.
- **Szybka zbieżność protokołów routingu** (ang. Fast Convergence) – nowoczesne urządzenia umożliwiają uzyskanie zbieżności protokołu routingu (czyli odnalezienie i zainstalowanie nowych ścieżek po awarii) w czasach grubo poniżej sekundy. Przyjęte rozwiązanie powinno obsługiwać takie mechanizmy.
- **Zbieżność niezależna od liczby prefiksów** (ang. PIC) – odświeżanie stanu w protokołach routingu zwykle trwa proporcjonalnie do liczby prefiksów w tablicy routingu. Pierwszy prefiks jest odświeżony szybko, ostatni dużo później. By przyspieszyć odświeżanie stosuje się hierarchiczne tablice, gdzie wystarczają pojedyncze zmiany by przekierować wiele prefiksów na nową ścieżkę (ang. Prefix Independent Convergence). Mechanizmy takie spotyka się dla protokołów IGP, są jednak bardziej przydatne dla BGP, gdzie kilka specjalizowanych odmian pozwala uzyskać pożądany efekt dla różnych typów awarii.
- **Priorytetyzacja prefiksów do synchronizacji** – w przypadku synchronizacji zwykle najistotniejsze jest odświeżenie najpierw prefiksów pokazujących na kluczowe urządzenia, a nie cały Internet. Z tego powodu stosuje się rozwiązania priorytetyzacji prefiksów, poprawiające zbieżność protokołów routingu po awarii.

- **Szybkie przekierowanie ruchu MPLS** (ang. FRR) – w ramach technologii MPLS istnieje mechanizm szybkiego przekierowania ruchu (ang. Fast ReRoute), który umożliwia przeniesienie ruchu na predefiniowaną zapasową ścieżkę natychmiast po wykryciu awarii. Daje to czasy odtworzenia usługi poniżej 100ms.
- **Mechanizmy odtworzenia stanu protokołów** (ang. GR) – 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.
- **Mechanizmy zachowania stanu protokołów** (ang. NSR) – kolejnym krokiem w stosunku do GR jest zachowanie stanu wewnątrz urządzenia, co pozwala na płynne przejęcia obsługi protokołów routingu przez zapasowy moduł sterujący
- **Redukcja czasu uaktualniania oprogramowania** (ang. ISSU) – mechanizmy uaktualniania oprogramowania (ang. In-Service Software Upgrade) różnią się zakresem, począwszy od instalowania łatek (ang. patch), poprzez dodawanie/usuwanie całych modułów, zmianę mniejszej wersji systemu (np. 6.1 -> 6.2), po kompletną zmianę wersji (np. 6.x -> 7.x). Wbrew zapewnieniom marketingowym nie ma jeszcze rozwiązań pozwalających na bezprzerwową aktualizację niezależnie od zakresu tej aktualizacji. Tym niemniej posiadanie przez urządzenia mechanizmów wspomagających aktualizacje oraz modularną architekturę oprogramowania choćby w pewnym zakresie pozwala na znaczącą redukcję czasu trwania okien serwisowych, oraz ewentualnych przerw w świadczeniu usług.

3.3.3 Węzły szkieletowe

Projektując urządzenia (węzły) warstwy rdzenia sieci należy przewidzieć realizację następujących funkcjonalności:

- duża wydajność, pozwalająca na przesyłanie zagregowanych strumieni ruchu. Obecnie stosowane urządzenia mają przepustowość rzędu kilkuset Gbit/s. Oznacza to zwykle kilkanaście portów 10Gbit/s przeznaczonych na łączność między węzłami szkieletowymi (w postaci łączy równoległych) oraz kilkanaście do kilkudziesięciu portów 10Gbit/s przeznaczonych do podłączenia innych typów węzłów. Czasami urządzenia szkieletowe pełnią jednocześnie funkcje dystrybucyjne/agregacyjne, czasami dla zapewnienia odpowiedniego modelu zarządzania siecią i separacji warstw, podłączenia klientów realizowane są także często na osobnych urządzeniach.
- sprawne zarządzanie ruchem i rozwiązywanie problemów – co oznacza dostępność mechanizmów typu inżynieria ruchu, oraz narzędzi wspomagających sprawdzanie działania usług i łączy.
- skalowalność, czyli możliwości rozbudowy. Modularność i zapas przepustowości pozwalają to osiągnąć.
- gwarancje jakości usług na poziomie zagregowanym, na podstawie klas ruchowych.
- przewidywalność. Sposób działania urządzeń powinien być deterministyczny, szczególnie w sytuacji awarii. Sieć i oparte na niej usługi muszą podlegać odpowiednim regułom, pozwalającym na ich szybkie odtworzenie, lub nawet brak przerwy w działaniu.

W zależności od konkretnych wymagań w projekcie uwzględnia się różne typy węzłów szkieletowych, różnej wielkości, stosownej do przewidywanego poziomu ruchu i liczby podłączeń w danym węźle.

Urządzenia szkieletowe powinny być w pełni modularne i zapewniać redundancję głównych elementów: zasilania, wentylacji, modułów sterujących, matrycy przełączającej.

Biorąc pod uwagę przewidywany rozwój usług i ruchu w sieci, urządzenia powinny także mieć możliwość rozbudowy o porty 40 i/lub 100Gbit/s

3.3.4 Węzły agregacyjne

Typowa funkcjonalność oczekiwana od węzłów agregacyjnych to:

- stosunkowo duża wydajność, rzędu kilkudziesięciu do kilkuset Gbit/s, w zależności od wielkości danego węzła i liczby obsługiwanych przezeń klientów.
- implementacja brzegowej polityki bezpieczeństwa, zapewniającej odrzucanie nadchodzącego ruchu, który jest nie jest zgodny z przyjętymi zasadami, (np. adresy źródłowe spoza zakresu klienta, lub docelowe z sieci operatorskiej).
- implementacja brzegowej polityki gwarancji jakości usług, zapewniającej przyjmowanie ruchu jedynie w ramach kontraktów, oraz jego znakowanie w celu prawidłowego przetwarzania w ramach kolejnych węzłów.
- kontrolę ruchu multicast, zgodnie z przyjętą polityką i świadczonymi usługami.
- generowanie statystyk ruchowych w celu usprawnienia inżynierii sieci, projektowania rozwoju łączy oraz kontroli przepustowości i parametrów ruchowych dla poszczególnych usług.
- nawiązywanie i terminowanie połączeń usługowych, w tym VPN warstwy trzeciej oraz drugiej, tranzyt ruchu IPv4/v6.

Podobnie jak w przypadku węzłów szkieletowych, także węzły agregacyjne mogą występować w różnej wielkości. Na potrzeby sieci DSS przyjmuje się trzy typy węzłów:

- małe, wyposażone w jeden lub dwa porty typu „uplink” 10Gbit/s, przeznaczone do podłączenia w kierunku szkieletu sieci, oraz kilkanaście do 20-40 portów światłowodowych 1 Gbit/s przeznaczonych do podłączania klientów usług w danej lokalizacji, lub najbliższej okolicy (przeważnie do kilku-kilkanastu kilometrów).
- średnie, wyposażone w kilka portów „uplink” pozwalających zwiększyć sumaryczną przepustowość do/ze szkieletu, oraz mieszankę portów 10Gbit/s (kilka) i 1Gbit/s (kilkadziesiąt) do podłączania większej liczby klientów, bądź bardziej wymagających klientów w większych węzłach.
- duże, zbliżone skalą do urządzeń szkieletowych, lecz wyposażone w większą liczbę portów dla klientów. Czasami urządzenia te są jednocześnie urządzeniami szkieletowymi.

Urządzenia agregujące mają zwykle architekturę modularną 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. Wybór rozwiązania zależy od przeprowadzenia analizy „what-if” symulującej wpływ awarii na utratę usług i w efekcie uciążliwość oraz straty biznesowe dla klientów.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

3.3.5 Wymiana ruchu z innymi operatorami (ang. peering)

Oprócz lokalnych operatorów podłączanych w poszczególnych węzłach, sieci operatorskie są wyposażone w węzeł wymiany ruchu (ang. IX, Internet Exchange), gdzie dzięki podłączeniu się do kilku ogólnopolskich, europejskich lub światowych operatorów internetowych.

Urządzenia w punktach wymiany ruchu to przede wszystkim skalowalne routery IP umożliwiające zaawansowane przetwarzanie ruchu pod względem filtrowania na zgodność z politykami, oraz przetwarzanie informacji routingu.

Zastosowanie w tym celu dedykowanych urządzeń pozwala odizolować własną sieć i wymusić odpowiednie polityki wymiany ruchu bez zaburzania jej działania. Dla redukcji kosztów spotyka się także rozwiązania, w których router szkieletowy (odpowiedniej skali i mocy przetwarzania) jest równocześnie urządzeniem peeringowym. Takie rozwiązanie może jednak spowodować, że potencjalne problemy związane z przetwarzaniem informacji pozyskanych od innych operatorów mogą przenosić się także na inne usługi realizowane przez to samo urządzenie.

3.3.6 Przetwarzanie informacji BGP (Route Reflector)

W przypadku sieci operatorskich do przetwarzania informacji routingowych BGP stosuje się zwykle dedykowane routery pozwalające odizolować i uniezależnić pozostałe urządzenia sieci od obciążenia takim przetwarzaniem. Skupienie w jednym miejscu polityki wymiany ruchu pozwala także na łatwiejsze zarządzanie siecią.

Urządzenia typu Route Reflector (RR) przejmują funkcjonalność i dokonują przeliczeń na użytek pozostałych urządzeń. Zwykle stosuje się więcej niż jedno takie urządzenie, by zapewnić niezawodność i/lub rozkład obciążenia w przypadku większych sieci.

3.4 Rozwiązania xWDM (DWDM)

Rozwiązania warstwy transportowej szkieletu regionalnej sieci szerokopasmowej (w tym Dolnośląskiej Sieci Szkieletowej) winny realizować kryterium „neutralności technologicznej" postulowane przez Komisję Europejską.

Standardowym rozwiązaniem zapewniającym najlepsze zagospodarowanie struktury światłowodowej warstwy szkieletowej sieci optycznej jest w chwili obecnej zastosowanie techniki zwielokrotnienia w dziedzinie długości fal (ang. Wavelenght Division Multiplexing; WDM). Wykorzystanie tej metody transportu danych zapewnia szereg funkcjonalności niedostępnych przy zastosowaniu innych technik teletransmisyjnych.

Technika xWDM bazuje na tworzeniu wielu niezależnych kanałów optycznych w pojedynczym włóknie światłowodowym. Każdy z uruchomionych kanałów pracuje, jako odseparowane łącze transmisyjne, co gwarantuje uzyskanie największych przepustowości, elastyczności zastosowań oraz skalowalności kosztowej inwestycji (koszt inwestycji rośnie w miarę doposażenia urządzeń w kolejne moduły kanałowe, inwestycja początkowa ogranicza się jedyni do struktury zwielokratniającej).

Technika xWDM jest rekomendowana do budowy warstwy transportowej Dolnośląskiej Sieci Szkieletowej jako rozwiązanie pierwszego wyboru.

Przy projektowaniu sieci należy dokonać wyboru jednej z odmian systemów wykorzystujących technikę WDM tzn.:

- systemy z dużym odstępem międzykanałowym (ang. Coarse Wavelenght Division Multiplexing; CWDM)

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- systemy z gęstym podziałem międzykanałowym (ang Dense Wavelenght Division Multiplexing; DWDM).

W sieciach o zasięgu regionalnym, gdzie odległości pomiędzy kolejnymi węzłami teletransmisyjnymi zwykle sięgają powyżej kilkudziesięciu kilometrów, rekomenduje się zastosowanie techniki DWDM.

3.4.1 Wymagania ogólne

Urządzenia DWDM powinny umożliwiać budowę traktów i węzłów transmisyjnych w optycznej sieci transportowej umożliwiającej transmisję głosu, danych oraz obrazów, przy wykorzystaniu różnych formatów sygnałów (SDH, IP, ATM, Gigabit Ethernet).

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

- Urządzenia DWDM nie powinny stanowić jakiegokolwiek niebezpieczeństwa dla personelu w trakcie instalacji, eksploatacji i utrzymania:
- Bloki i pakiety mogące stanowić zagrożenie (np. nadajniki laserowe) powinny mieć stałe oznakowanie ostrzegawcze.
- Wszystkie laserowe źródła światła powinny być automatycznie wyłączane lub ich moc powinna być zredukowana w przypadku zaniku sygnału optycznego (np. przerwanie światłowodu, rozłączenie złącza optycznego) w jakiejkolwiek części drogi optycznej.

Urządzenia DWDM powinny pracować prawidłowo w pomieszczeniach zamkniętych, bez potrzeby stosowania klimatyzacji oraz w określonym zakresie wartości parametrów otoczenia:

- zakres roboczych temperatur: +5°C † +40°C
- wilgotność względna: 80% przy temperaturze +20°C

3.4.2 Interoperacyjność

Urządzenia muszą współpracować ze światłowodami o parametrach wg zaleceń ITU-T G.652:2003 oraz G.655:2003 w trzecim oknie transmisyjnym.

W przypadku Dolnośląskiej Sieci Szkieletowej należy założyć:

- bezpośrednie wykorzystanie interfejsów 10 GbE oraz 100 GbE w sieci szkieletowej,
- bezpośrednie wykorzystanie interfejsów 10 GbE w sieci dystrybucyjnej.

Oferta usługowa sieci szkieletowej powinna jednak obejmować szereg innych interfejsów przydatnych w strukturach operatorskich. Urządzenia DWDM powinny umożliwiać współpracę z następującymi urządzeniami:

- urządzeniami SDH STM-64/STM-16/STM-4 z zastosowaniem synchronicznych transponderów optycznych,
- urządzeniami SDH STM-64/STM-16/STM-4 wyposażonymi w optyczne interfejsy („kolorowe),
- innymi urządzeniami (ATM, IP, Gigabit Ethernet) z zastosowaniem asynchronicznych transponderów optycznych o szybkości transmisji w zakresie: od 1 Gbit/s Mbit/s do 100 Gbit/s,
- innymi urządzeniami z zastosowaniem synchronicznych transponderów optycznych o szybkości transmisji od 1 Gbit/s do 10 Gbit/s.

Urządzenia muszą zapewniać otwartość technologiczną poprzez wspieranie standardu transmisji tzw. „obcej długości fali", opisanego w ITU-T G.698.2 (ang. alien wavelength transmission).

Urządzenia systemu DWDM powinny być skalowalne oraz powinna być możliwa ich stopniowa rozbudowa.

Przy projektowaniu warstwy transportowej sieci w oparciu o DWDM należy uwzględnić:

- jednolitość technologiczną zastosowanego rozwiązania,
- maksymalny zasięg użyteczny,
- skalowalność i możliwość rozbudowy systemów DWDM do strumieni i 100 Gbit/s.
- rodzaj kanałów xGbE wymaganych do transportu.

Przy doborze właściwego rozwiązania dla warstwy szkieletowej sieci należy również uwzględnić parametry związane z typami usług, które warstwa szkieletowa będzie musiała świadczyć dla pozostałych segmentów sieci. Założenie konieczności zagospodarowania sieci, jako struktury służącej wielu operatorom lokalnym powoduje, że należy zwrócić uwagę na:

- zakres typów interfejsów klienckich obsługiwanych przez konkretny typ urządzenia teletransmisyjnego uwarunkowujących zakres zastosowań struktury teletransmisyjnej;
- funkcjonalności związane z elastycznością struktury połączeniowej oraz możliwością szybkiego kreowania kanałów transportowych.

W chwili obecnej obserwuje się coraz częstsze wprowadzanie do systemów DWDM dodatkowych funkcjonalności mających na celu zwiększenie elastyczności struktury sieci szkieletowych. Rozwiązania takie idą w dwóch niezależnych kierunkach polegających na:

- zintegrowaniu w węzłach DWDM matryc przełączających bazujących na strukturze zwielokrotnienia zgodnej ze standardem OTN (ang. Optical Transport Network),
- zastosowaniu nowych typów węzłów optycznych – rekonfigurowalnych optycznych krotnic przelotowych (ang. Reconfigurable Optical Add/Drop Multiplekser; ROADM).

Obie z wymienionych funkcjonalności dążą do uproszczenia metod zarządzania warstwą optyczną sieci transportowej. Zastosowanie przełączanych struktur optycznych ma na celu skrócenie czasu potrzebnego na dostarczenie usług do kolejnych klientów, wprowadzenie mechanizmów zabezpieczania ruchu bezpośrednio w warstwie optycznej oraz optymalizację wykorzystania tworzonych struktur.

Przy projektowaniu struktury (i doborze rozwiązania sprzętowego) rekomenduje się możliwość zastosowania (opcjonalnie pojedynczo lub razem):

- matryc przełączających bazujących na strukturze zwielokrotnienia zgodnej ze standardem OTN (ang. Optical Transport Network),
- rekonfigurowalnych optycznych krotnic przelotowych (ang. Reconfigurable Optical Add/Drop Multiplekser; ROADM).

Ostateczną decyzję o wprowadzeniu i zakresie zastosowania technik OTN lub ROADM w dobranym rozwiązaniu sprzętowym podejmie Operator Infrastruktury.

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

Przy planowaniu sieci transportowej w ramach Dolnośląskiej Sieci Szerokopasmowej należy uwzględnić gotowość zastosowanych systemów do wprowadzenia wymienionych wyżej funkcjonalności.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

3.4.3 Zarządzalność

System DWDM i jego elementy powinny być zarządzane zgodnie z zasadami ITU TMN (Telecommunication Management Network) oraz ISO FCAPS.

3.4.4 Parametry

W ramach projektowania struktury transmisyjnej Dolnośląskiej Sieci Szerokopasmowej należy:

- projektować sekcje miedzywzmacniakowe nie dłuższe niż 150 km,
- przyjąć iż maksymalna długość sekcji zwielokrotnienia optycznego nie przekroczy 200km.

W ramach Dolnośląskiej Sieci Szerokopasmowej należy:

- stosować systemy DWDM pracujące w paśmie C (1525–1565 nm)

przy czym:
w szczególnych przypadkach dopuszcza się za każdorazową zgodą Zamawiającego (po przeprowadzeniu analizy ekonomicznej i technicznej) stosowania systemów pracujących w paśmie L (1570– 1610 nm)
Należy przyjąć realizację systemów DWDM w oparciu o siatkę częstotliwościową zgodną ze standardem ITU-T G.694.1. przy czym:

- rekomendowane są systemy bazujące na odstępie międzykanałowym 50 GHz lub 100 GHz.

Należy przyjąć realizację systemu o następujących liczbach kanałów:

- dla siatki 50 GHz – 80 kanałów
- dla siatki 100 GHz – 40 kanałów

przy czym rekomenduje się, aby:

- oprzeć się o rozwiązania, które stosują ten sam typ urządzeń do obsługi siatki 50GHz i 100 GHz

Ze względu na parametry systemów DWDM oraz strukturę sieci regionalnej należy założyć iż projektowane systemy DWDM pracujące w paśmie mogą pracować bez wzmacniaczy optycznych przy czym zgodnie ze standardem powinny gwarantować zasięg od 10 do 40 km (kilka do kilkunastu dB). Dla sieci DSS (do celów projektowych) zaleca się zasięg min. 20 km przy następujących warunkach:

- przyjęciu jednostkowej tłumienności włókna zgodnego ze standardem ITU-T G.652 z przedziału od 0.17 do 0.25 dB/km (zaleca się wyznaczenie wartości typowej 0,2 dB/km),
- uwzględnieniu limitów na starzenie włókna (3dB),
- uwzględnieniu typowego zapasu mocy (max. path los) interfejsów optycznych po stronie liniowej (kolorowych) w transponderach optycznych,
- uwzględnieniu typowych tłumienności multiplekserów i innych elementów optycznych,

W przypadku gdy wymagany zasięg bez zastosowania wzmacniaczy będzie niewystarczający, w celu zwiększenia długości sekcji zwielokrotnienia optycznego, podstawowy system DWDM należy uzupełnić o wzmacniacze optyczne EDFA. W takich przypadkach należy uwzględnić instalacje wzmacniaczy w jednym z trzech miejsc struktury systemu DWDM:

1. na wyjściu multipleksera po stronie nadawczej (tzw. booster) – (rozwiązanie stosowane w pierwszej kolejności).
2. na wyjściu multipleksera po stronie nadawczej (tzw. booster) oraz przed demultiplekserem po stronie odbiorczej (ang. preamplifier) – (rozwiązanie stosowane w następnej kolejności).

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

3. w przebiegu sekcji zwielokrotnienia – należy zastosować tzw. wzmacniaki optyczne i uzyskać zwiększenie zasięgu

Przy projektowaniu tras optycznych należy zatem uwzględnić konieczności wzmocnienia sygnału zbiorczego w odstępach 20 – 25 dB (zwykle jest to 60 – 100km licząc po ścieżce optycznej). Zalecaną wartością dla celów projektowych jest 80 km.

W szczególnych przypadkach dopuszcza się przedłużenie zasięgu pojedynczego skoku optycznego o poprzez zastosowanie wzmacniaczy Ramana. Ze względu na wysoki koszt rozwiązanie takie powinno być stosowane jedynie w uzasadnionych przypadkach.

3.4.5 Niezawodność

W sieci szkieletowej należy przyjąć stosowanie rozwiązań DWDM na wysokim poziomie bezawaryjności.

W przypadku najbardziej obciążonych ruchem urządzeń należy założyć założyć stosowanie mechanizmów zabezpieczających przed awariami sprzętowymi:

- wszystkie projektowane urządzenia DWDM winny posiadać podwojone obwody zasilania,
- zaleca się zabezpieczanie kontrolerów (gdy zastosowane rozwiązanie to umożliwia).

Ze względu na analogowy charakter transmisji (niski poziom awaryjności, imperatyw obniżania tłumienności), nie przewiduje stosuje się dublowania optycznych elementów transmisyjnych (multipleksery, wzmacniacze, couplery itp.).

3.4.6 Mechanizmy zabezpieczenia ruchu w technice DWDM.

W ramach projektowania sieci transportowej Dolnośląskiej Sieci Szkieletowej należy przewidzieć mechanizm protekcji ruchu.

Minimalne rozwiązanie stanowi protekcja ścieżek w trybie 2+0, gdzie elementem przełączającym jest urządzenie klienckie (krotnica SDH, router IP itp.).

Rekomendowanym rozwiązaniem w Dolnośląskiej Sieci Szkieletowej jest zastosowanie techniki OTN (zgodnie z Rekomendacją ITU-T G.709) posiadającej zintegrowane przełącznice elektroniczne z realizacją:

- szybkiego przełączania ruchu w celu zestawiania ścieżek oraz ich zabezpieczania, bez ograniczeń występujących w wersji czysto optycznej;
- agregacji strumieni o niższej przepustowości w strumienie zbiorcze w celu optymalizowania sposobu zagospodarowania poszczególnych kanałów optycznych, niedostępnych w urządzeniach „optycznie przeźroczystych”.

Dopuszcza się w szczególnych przypadkach zastosowanie (po analizie ekonomicznej przedstawić do akceptacji Zamawiającego) techniki OTN czysto optycznej (bez matryc elektronicznych) bazujących wyłącznie na mechanizmach przełączania w warstwie optycznej,

Struktura systemu DWDM

Strukturę i organizacje systemu DWDM należy oprzeć o strukturę połączeń światłowodowych.

W projektowaniu struktury systemu DWDM (w przyjmowaniu schematu rozpływu ruchu w sieci optycznej) należy uwzględnić:

- charakter i typ przenoszonych usług,
- strukturę połączeń Operatorskich.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Należy przyjąć, iż struktura ruchu w sieci DSS składać się będzie ze struktur gwiazdowych dedykowanych dla Operatora (z uwzględnieniem wiodącego typu usług w jego sieci) nakładających się na siebie.

Należy konstruować sieć o strukturze maksymalnie zbliżonej do sieci kratowej z wyraźnym wyróżnieniem:

- węzłów „zbiorczych" (przygotowanych to wyprowadzania dużej ilości kanałów klienckich), węzły „zbiorcze" powinny być lokowane w siedzibach operatorów. Zaleca się by węzeł „zbiorczy" lokalizowany był tożsamo z węzłem szkieletowym sieci DSS,

oraz

- węzłów „dystrybucyjnych" (zakończenia maksymalnie kilku do kilkunastu ścieżek/kanałów), które posadowione są na granicy sieci szkieletowej i dystrybucyjnej.

W przypadku zastosowania techniki DWDM należy zaprojektować system DWDM umożliwiający bezpośrednie przejście pomiędzy siecią dystrybucyjną i szkieletową za pomocą interfejsów optycznych „kolorowych".

3.5 Rozwiązania IP/MPLS

W ujęciu organizacji typowa sieć szkieletowa składa się z trzech warstw: Warstwa IGW, Warstwa P oraz warstwa PE. Warstwa IGW służy do dostępu do Internetu IX (ang. peering). W warstwie tej występują urządzenia wymieniające ruch (zwykle za pomocą protokółu BGP) z dostawcami Internetu, partnerami i dużymi klientami. Po wewnętrznej stronie sieci IGW powinien być połączony do warstwy P. W niektórych przypadkach łączy się ją bezpośrednio z dużą ilością routerów PE. Bezpośrednie połączenie z PE może zredukować ilość potrzebnych portów, ale jednocześnie bardzo komplikuje architekturę sieci. Routery P służą do wymiany w węźle oraz do obsługi ruchu pomiędzy węzłem podrzędnym i nadrzędnym. W większości przypadków zachodzi potrzeba instalacji dwóch routerów w węźle nadrzędnym i po minimum jednym routerze w węźle podrzędnym. Dla warstwy P zaleca się stosowanie topologii „mesh" lub „partial mesh". Również w warstwie PE zaleca się instalację jednej lub więcej par routerów PE dla każdego punktu sieci.

Rozwiązania IP/MPLS (jak również MPLS IP) szkieletu regionalnej sieci szerokopasmowej (w tym Dolnośląskiej Sieci Szkieletowej) winny realizować kryterium „neutralności technologicznej" postulowane przez Komisję Europejską.

3.5.1 Planowanie przepustowości

Sieć zaprojektowana z odpowiednim zapasem pasma (przepustowość > max. ilości ruchu) może zapewnić bark zatorów w sieci i zagwarantować najlepszy QOS (małe opóźnienia, niewielki jitter i niewielką stratę pakietów).

Jednakże sieć przewymiarowana oznacza zbyt duże wydatki w stosunku do dochodów. Podczas projektowania należy prawidłowo przewidzieć początkową ilość ruchu (z podziałem na typy) a następnie wdrożyć procedury planowania wzrostu przepustowości.

3.5.1.1 Planowanie pojemności węzłów

Częsta przebudowa węzłów wiąże się z długimi czasami rozbudowy, testów, wdrożeń i optymalizacji. Prowadzi to do dużych wydatków i przerw w dostarczaniu usług. Dlatego też dobór

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

platformy sprzętowej musi być tak przemyślany, aby zapewnił możliwość płynnej rozbudowy w perspektywie 8~10 lat.

3.5.1.2 Planowanie przepustowości połączeń

Biorąc pod uwagę fakt, że karty liniowe stanowią większość kosztów urządzeń sieciowych należy tak dobrać ich parametry, aby zapewnić możliwość realizacji potrzeb przez 2-3 lata bez konieczności ich wymiany.

3.6 Kluczowe cechy routerów P i PE

Na potrzeby projektu Dolnośląskiej Sieci Szkieletowej ustala się blok kluczowych funkcjonalności w obszarze architektury i wymagań funkcjonalnych.

1) Architektura:
   a) Architektura sprzętowa routera musi być modularna – przez co rozumie się, że funkcje: routowania pakietów, przełączania pakietów oraz obsługi ruchu liniowego nie mogą być realizowane w ramach jednego modułu, a dodatkowo wyodrębniony powinien być moduł zasilania. .
   b) Rekomenduje się, aby architektura oprogramowania routera była modularna – pracująca z wykorzystaniem oddzielnych niezależnych procesów.
   c) Główna matryca przełączania pakietów powinna być w pełni nieblokowalna - tak aby obsłużyć z pełną prędkością wszystkie karty liniowe.
   d) Moduły odpowiedzialne za routowanie (Routing Engine RE) oraz przełączenie pakietów (Switch Fabric SF) powinny być redundantne (niezależnie od wariantu implementacyjnego, tj. od tego czy komponenty są rozdzielone fizycznie, czy też nie).
   e) W przypadku awarii któregoś z modułów RE lub SF praca urządzenia / przełączanie pakietów nie może ulec przerwaniu.
   f) Moduły odpowiedzialne za routing (w warstwie 3 modelu OSI) bądź przełączanie pakietów (w warstwie 2 modułu OSI) powinny zapewnić pełną i bezstratną obsługę ruchu ze wszystkich kart liniowych routera, przy maksymalnej utylizacji poszczególnych ich portów (dla wszystkich protokołów, np. IPv4, IPv6, MPLS).
   g) Architektura modułu przełączania karty liniowej powinna pozwolić na bezproblemową obsługę ruchu unicast i multicast (łącznie ze sprzętową replikacją ruchu multicast).
   h) Karty liniowe muszą być obsługiwane przez matrycę przełączającą w ten sposób, iż nie wystąpi spadek wydajności urządzenia, gdy wszystkie wymagane porty będą pracować z maksymalną prędkością liniową (przy założeniu, że zostaną obciążone ruchem IMIX zgodnie z definicją RFC6985).
   i) Wszystkie moduły architektury łącznie z kartami liniowymi powinny być typu „Hot Swappable”. Wyjęcie / włożenie kart nie może mieć wpływu na pracę pozostałych modułów urządzenia.
   j) Router powinien wspierać możliwość kreowania wirtualnych routerów lub wirtualnych instacji rutingowych (VRF) z separacją na poziomie routingu oraz interfejsów.
   k) Architektura routera musi zapewnić wsparcie dla min. 8 sprzętowych kolejek QoS dla każdego portu fizycznego.
   l) Uruchomienie QoS na karcie/porcie nie może mieć wpływu na liniową wydajność karty/portu.
   m) Wewnątrz sprzętowych kolejek QoS powinna istnieć możliwość budowy kolejek priorytetowych (min. 1)..

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

n) Uruchomienie filtrów skonfigurowanych zgodnie z zaleceniami producenta nie powinno znacząco obniżać wydajności routera oraz nie powinno znacząco wpływać na wydajność kart/portów liniowych.
o) Architektura oprogramowania routera powinna pozwalać na zmianę / cofanie zmian konfiguracji.
p) Router powinien pozwolić na dostęp poprzez tekstowy interfejs typu CLI dla trybu konfiguracji i trybu debug.
q) Router powinien mieć standardowo oferować możliwość bezpiecznego zarządzania (out-of-band) za pomocą dedykowanego portu FE/GE na karcie sterującej urządzenia.
r) Router powinien umożliwić dostęp do tekstowego interfejsu zarządzającego po interfejsie konsolowym .
s) Przepustowość routera musi wynosić 100Gbps (Full Duplex)na slot i powinna być skalowalna do co najmniej 200 Gbps w przyszłości. Dla mniejszych węzłów (dystrybucyjnych) przepustowość routera musi wynosić co najmniej 40Gbps na slot.

2) Wymagania funkcjonalne:
a) Routery muszą mieć możliwość pracy jako routery brzegowe jak i routery szkieletowe MPLS.
b) Rekomenduje się, aby implementacja standardu MPLS wspierała następujące standardy wymienione w tabeli poniżej lub standardy nowsze, zastępujące wymienione poniżej.:

Tabela 1. Standardy MPLS

L.p.	Standard	Tytuł
1.	RFC 2205	Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification
2.	RFC 2702	Requirements for Traffic Engineering Over MPLS
3.	RFC 2747	RSVP Cryptographic Authentication
4.	RFC 2961	RSVP Refresh Overhead Reduction Extensions
5.	RFC 3031	Multiprotocol Label Switching Architecture
6.	RFC 3032	MPLS Label Stack Encoding
7.	RFC 3056	LDP Specification
8.	RFC 3063	MPLS Loop Prevention Mechanism
9.	RFC 3107	Carrying Label Information in BGP-4
10.	RFC 3209	RSVP-TE Extensions to RSVP for LSP Tunnels
11.	RFC 3210	Applicability Statement for Extensions to RSVP for LSP-Tunnels
12.	RFC 3215	LDP State Machine
13.	RFC 3270	Multi-Protocol Label Switching (MPLS) Support of Differentiated Services
14.	RFC 3272	Overview and Principles of Internet Traffic Engineering
15.	RFC 3443	Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
16.	RFC 3469	Framework for Multi-Protocol Label Switching (MPLS)-based Recovery
17.	RFC 3478	Graceful Restart Mechanism for LDP
18.	RFC 3612	Applicability Statement for Restart Mechanisms for the Label Distribution Protocol (LDP)

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

L.p.	Standard	Tytuł
19.	RFC 4090	Fast Reroute Extensions to RSVP-TE for LSP Tunnels
20.	RFC 4124	Protocol Extensions for Support of DS-TE
21.	RFC 4125	Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering
22.	RFC 4182	Removing a Restriction on the use of MPLS Explicit NULL
23.	RFC 4221	Multiprotocol Label Switching (MPLS) Management Overview
24.	RFC 4379	Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
25.	RFC 4446	IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)
26.	RFC 4447	Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
27.	RFC 4448	Encapsulation Methods for Transport of Ethernet over MPLS Networks
28.	RFC4875	Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)
29.	RFC4379	Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

c) Router powinien wspierać następujące metody zestawiania tuneli LSP – statycznie, z wykorzystaniem dynamicznych protokołów LDP i RSVP (RSVP-TE).
d) Tunele RSVP powinny mieć możliwość ustawienia parametrów setup i hold priority.
e) Powinna istnieć możliwość obsługi obiektów ERO (ang. explicite router object) typu „loose" i „stricte" oraz RRO (ang. record route object).
f) Router powinien wspierać tunelowanie LDP over RSVP-TE.
g) Router powinien wspierać funkcjonalność MPLS-TE FRR (ang. Fast ReRoute) w trybie protekcji urządzenia (node protection) oraz ścieżki LSP (link protection). Urządzenie powinno pozwolić na przełączenie na zapasową ścieżkę LSP w czasie max. 50 ms.
h) Router powinien wspierać dynamiczne protokoły ISIS oraz OSPF, z możliwością ich wykorzystania jako IGP w środowisku MPLS (wraz z funkcjonalnością TE).
i) Implementacja protokołów ISIS i OSPF w środowisku MPLS powinna opierać się na następujących standardach:

Tabela 2. Standardy ISIS

L.p.	Standard	Tytuł
1.	ISO 9542	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for the Provision of the Connectionless-mode Network Service
2.	ISO 10589	IS-IS intra-domain routing protocol
3.	RFC 1195	Use of OSI Is-Is for Routing in TCP/IP and Dual Environments
4.	RFC 2763	Dynamic Name-to-system ID mapping support
5.	RFC 2966	Route leak support
6.	RFC 2973	Support IS-IS Mesh Groups

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

L.p.	Standard	Tytuł
7.	RFC 3373	Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
8.	RFC 3567	Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
9.	RFC 3719	Recommendations for Interoperable Networks using IS-IS
10.	RFC 3784	ISIS TE support
11.	RFC 3787	Recommendations for Interoperable IP Networks using IS-IS
12.	RFC 3847	Restart signaling for IS-IS
13.	RFC 4444	Management Information Base for Intermediate System to Intermediate System (IS-IS)

Tabela 3. Standardy OSPF

L.p.	Standard	Tytuł
1.	RFC 1583	OSPF Version 2
2.	RFC 1587 lub 3101	The OSPF NSSA Option
3.	RFC 1765	OSPF Database Overflow
4.	RFC 1850	OSPF Version 2 Management Information Base
5.	RFC 2328	OSPF Version 2
6.	RFC 2370	The OSPF Opaque LSA Option
7.	RFC 2740	OSPF for IPv6 (OSPFv3)
8.	RFC 3137	OSPF Stub Router Advertisement
9.	RFC 3623	OSPF Graceful Restart
10.	RFC 3630	Traffic Engineering Extensions to OSPF

j) W środowisku sieci IP/MPLS router powinien wspierać protokół MP-BGP wraz z funkcjonalnościami BGP Route Reflection i AS Confederations.

k) Router powinien wspierać następujące funkcjonalności:
   i) atrybuty community dla BGP – simple i extended
   ii) sygnatury MD5 dla sesji BGP
   iii) BGP Route Flap Damping
   iv) IS-IS Mesh Groups
   v) kryptograficzna autentykacja w ISIS

l) W routerach powinna być możliwość skonfigurowania dedykowanego interfejsu loopback, wykorzystywanego do uruchamiania i utrzymywania sesji routingowych.

m) Implementacja mechanizmu GR (ang. Graceful Restart) dla protokołów: MP-BGP, ISIS , LDP, RSVP-TE lub mechanizmu Non-Stop_Routing dla protokołów: BGP oraz ISIS
   i) powinien umożliwić wykorzystanie BFD w celu przyspieszenia konwergencji protokołów sygnalizacyjnych (np. LDP, RSVP) czy routingu (np. ISIS).
   ii) Urządzenie powinno wspierać funkcjonalność MPLS OAM
   iii) Router powinien posiadać mechanizmy ochrony Control Plane przed atakami, np. typu DoS.
   iv) Router powinien jednocześnie obsługiwać protokół IPv4 i IPv6, stosy obu protokołów powinny być oddzielne i nie oddziaływać wzajemnie na siebie.

v) Router powinien posiadać możliwość zaadresowania wszystkich interfejsów natywnymi adresami IPv4, IPv6 oraz IPv4 i IPv6 jednocześnie.
vi) Powinna istnieć możliwość tworzenia wirtualnych sieci prywatnych warstwy drugiej MPLS (L2VPN), dla następujących technologii warstwy drugiej: Ethernet (oraz ATM po ewentualnym uzupełnieniu o dodatkowe karty liniowe).
vii) Powinna istnieć możliwość tworzenia sieci VPLS - MPLS VPN L2 typu Point-to-Multipoint i Multipoint-to-Multipoint.
viii) Router powinien wpierać różne warianty połączeń z innym operatorem sieci MPLS (Inter-Provider VPNs) dla usług MPLS VPN L3, MPLS VPN L2, MPLS VPN TE.
ix) Powinna istnieć możliwość transportowania protokołu Ethernet w dwóch wariantach: port-to-port i VLAN-to-VLAN poprzez sieć IP/MPLS za pomocą np. tunelowania MPLS.
x) Router powinien posiadać następujące funkcjonalności QoS dla IPv4 i IPv6 dla kierunków inbound oraz outbound:
   (1) klasyfikacja pakietów do różnych klas usługowych,
   (2) markowanie pól w nagłówkach pakietów typu IP ToS (IP Precedence, DSCP), MPLS EXP, Ethernet CoS,
   (3) obsługa pakietów w oddzielnych klasach usługowych (kolejkach) z wykorzystaniem algorytmów:
      (a) WRR lub WFQ/WRR,
      (b) PQ lub SP,
      (c) WRR wraz z PQ lub SP,
   (4) określenie procentowe / wagowe / bps poziomu pasma per kolejka,
   (5) mechanizm policing w klasach,
   (6) mechanizm kształtowania ruchu (shaping),
   (7) WRED (Weighted Random Early Detection),
   (8) konfigurowanie/sterowanie głębokościami kolejek,
   (9) QoS (typu klasyfikacja, markowanie, kolejkowanie, policing, shaping, WRED), funkcjonalności powinny mieć możliwość zastosowania zarówno na interfejsach fizycznych. np. GE, 10GE, jak i logicznych (podinterfejsach), np. VLAN,
   (10) filtrowanie i modyfikowanie wejściowej i wyjściowej informacji routingowej dla protokołów dynamicznego routingu (BGP, OSPF, ISIS, RIP),
   (11) wsparcie dla MPLS VPN zgodnie z RFC 4364,
xi) Router powinien posiadać redundantne zasilacze.
xii) Rekomenduje się, aby router wspierał:
   (1) pre-klasyfikację pakietów dla protokołu tunelowania pakietów IPSEC,
   (2) LFI Fragmentation and Interleaving (np. poprzez możliwość instalacji dodatkowych kart z odpowiednimi portami),

3.6.1 Logiczna architektura sieci

3.6.1.1 Nazewnictwo

Konwencja nazewnictwa powinna pozwalać na jednoznaczną identyfikację każdego z urządzeń w sieci. Skróty nazw lokalizacji, roli urządzenia jego modelu oraz numeru są powszechnie używane przy nadawaniu nazw.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

3.6.1.2 Planowanie adresacji IP

Routery powinny posiadać publiczne adresy IPv4. Umożliwi to ich prawidłową współpracę z innymi urządzeniami w sieci Internet. W przypadku konieczności użycia prywatnych adresów IPv4 dla urządzeń sieciowych należy przewidzieć urządzenie realizujące funkcję NAT. Da to możliwość tłumaczenia prywatnych adresów IPv4 na publiczne adresy IPv6 i na odwrót.

Zaleca się stosowanie hierarchicznej adresacji IP (według struktury geograficznej lub funkcjonalnej), co umożliwi proste agregowanie adresów oraz bardzo ułatwi zarządzanie.

Użycie podwójnej adresacji IPv4/IPv6 umożliwi łagodną migrację w kierunku IPv6. Adresacja sieci IPv6 powinna być zbliżona do adresacji IPv4.

3.6.1.3 Projektowanie IGP

Protokół IGP jest powszechnie używany do połączeń wewnątrz AS (Autonomous System – systemu autonomicznego). ISIS i OSPF to najczęściej używane do tego celu protokoły.

Oba to protokóły stanu połączenia (link state) używające algorytmu Dijkstra i wspierające architekturę hierarchiczną w celu lepszej skalowalności. W podobny sposób wpierają fast convergence i fast reroute w celu zapewnienia szybkiej zbieżności i wysokiej dostępności sieci. Oba pracują z IPv4/v6 jednakże ISIS ma wygodniej zaimplementowaną obsługę IPv6. Obecnie ISIS jest częściej implementowany w sieciach operatorskich a OSPF w sieciach firmowych.

Rekomendowane jest użycie ISIS.

Obecnie routery posiadają bardzo rozbudowane moduły odpowiedzialne za routowanie pakietów umożliwiające obsługę tysięcy routerów na jednym poziomie lub w obszarze.

Podział sieci szkieletowej na wiele poziomów/arei może spowodować trudności w ustanawianiu międzypoziomowego połączenia MPLS LSP i konieczność konfiguracji przecieków prefiksów 32/ IP pomiędzy L1/L2.

Rekomendowane jest użycie ISIS level-2 lub OSPF „area 0” w szkielecie sieci. W celu zapewnienia stabilności sieci rekomendowane jest umiejscowienie sieci Metro Ethernet w innych obszarach niż sieć szkieletowa.

Konfiguracja metryk ma bardzo duży wpływ na wybór ścieżek. Rekomendujemy użycie standardowych metryk opartych na przepustowości łącz (czym większa przepustowość tym mniejsza metryka).

Ze względów bezpieczeństwa oraz wymogu zapewnienia wysokiej dostępności sieci należy aktywować następujące ustawienia: MD5 session validation, priority based fast convergence, NSF/NSR, IGP/LDP synchronization, BFD for IGP, IGP FRR.

3.6.1.4 Projektowanie BGP

BGP to protokół EGP (ang. Exterior Gateway Protocol) w większości przypadków używany do łączenia różnych systemów autonomicznych. Każdy system autonomiczny powinien mieć unikalny numer ASN przyznany przez organizację typu RIR (ang. Regional Internet Registries).

W projekcie tym BGP będzie używany jedynie do propagacji ścieżek IPv4 (internet) i VPNv4.

Zaleca się użycie BGP tylko na brzegu sieci, co oznacza jego konfigurację tylko i wyłącznie na IGW i PE. Konfiguracja taka zwana „BGP free core solution” eliminuje konieczność propagacji dużych ilości informacji o sieci do routerów P czyniąc sieć bardziej stabilną.

W celu zapewnienia lepszego bezpieczeństwa i dostępności usług należy dla BGP zaimplementować następujące mechanizmy:

- MD5 authentication,
- GTSM (Generic TTL Security Mechanism),
- BFD for BGP,
- priority based IGP convergence,
- BGP FRR (Fast Re-route).

3.6.1.5 Projektowanie MPLS

LDP & RSVP to najbardziej popularne protokóły sygnalizacji MPLS. LDP to skrót od „label distribution protocol", który polega na IGP przy wykrywaniu topologii i wyborze ścieżki. LDP bardzo dobrze nadaje się zarówno dla małych jak i dużych sieci. RSVP z kolei polega na IGP przy wykrywaniu topologii I stanu połączeń następnie może wybrać najlepszą ścieżkę bazując na kombinacji różnych czynników takich jak przepustowości łącza, SRLG itp. W porównaniu z LDP, RSVP posiada większe możliwości w zakresie inżynierii ruchu I lepsze szybsze możliwości przekierowania ruchu w przypadku awarii ale jest mniej skalowalny. Sugerujemy użycie LDP dla potrzeb tego projektu.

3.6.1.6 Projektowanie MPLS/BGP VPN

MPLS/BGP VPN to technologia L3VPN używana do budowy oddzielnych sieci L3na jednej fizycznej sieci w celu zapewnienia prywatności i bezpieczeństwa tych sieci. MPLS/BGP VPN może zapewniać połączenia typu „full mesh" lub „hub-spoken connectivity". MPLS/BGP VPN może również łączyć wiele oddzielnych sieci IP/MPLS posiadających różne numery AS według standardu zdefiniowanego w RFC4364.

3.6.2 Zapewnienia należytej jakości usługi - QoS

3.6.2.1 Wymagania QoS

Standardy 3GPP TS 22.105 V6.2.0 i ITU-T Y.1541 określają sposób zapewnienia QoS dla każdego rodzaju ruchu. Wymagania dla poszczególnych usług przedstawia poniższa tabela.

Tabela 4. Wymagania dla QoS

Kategoria usługi	Usługa	Typ usługi	Pasmo (kbps)	Opóźnienie (jednokierunkowe typu koniec-koniec)	Fuktuacja (Jitter)	Poziom utraty pakietów
Usługi głosowe	Rozmowa telefoniczna	Dwukierunkowy (konwersacyjny)	4-25	< 150 ms typowo, 400 ms max.	< 1ms	< 3%
	Wideomedia	Strumieniowanie	5-128	10 s max.	< 2ms	< 3%
	Wideo wiadomości	Strumieniowanie	4-13	< 1 s playback 2 s max	< 1ms	< 3%
Usługi video	Wideofonia	Dwukierunkowy (konwersacyjny)	32-384	< 150 ms typowo, 400 ms max. < 100 ms lip-sync	< 10ms	< 3%
	Wideomedia	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

Kategoria usługi	Usługa	Typ usługi	Pasmo (kbps)	Opóźnienie (jednokierunkowe typu koniec-koniec)	Fuktuacja (Jitter)	Poziom utraty pakietów
Dane 3	**Telemetria**	**Interaktywny**	**< 28,8 K**	**< 0,5 s typowo**	**n/a**	**0**

3.6.3 IP/MPLS DiffServ

IP/MPLS DiffServ jest sposobem na zagwarantowanie odpowiedniego QoS dla poszczególnych typów ruchu z uwzględnieniem, ruchu zarządzającego.

W standardzie RFC3270 dla MPLS DiffServ zdefiniowano trzy modele: „including pipe model", „uniform model" i „short pipe model". „Pipe model" jest zalecany dla przypadków, w których w MPLS LSP występuje jedna lub więcej domen (ang. DiffServ Domain) z różnymi PHB. „Uniform model" jest zalecany dla przypadków, w których w MPLS LSP występuje jedna lub więcej domen (sng. DiffServ Domain) z tym samym PHB. „Short pipe model" jest bardzo podobny do „pipe model" ale posiada inny PHB na węźle agregującym LSP.

Przed implementacją modelu IP/MPLS DiffServ należy jasno zdefiniować granice zaufania QoS. Ogólnie węzły wewnątrz sieci operatora traktuje się, jako zaufane a węzły zewnętrzne, jako niezaufane. Kwalifikacja ruchu I jego markowanie powinna się odbywać tylko w węzłach zaufanych a następnie to ustawienie powinno być respektowane wewnątrz całej sieci.

Tabel poniżej pokazuje przykładowe przypisanie PHB, DSCP, EXP I 802.1p dla poszczególnych usług.

Tabela 5. Definicja priorytetów dla poszczególnych usług

L.p.	Typ usługi	PHB	DSCP	EXP	802.1p
1.	Network Control	CS6	110000	(6)	6
2.	VoIP	EF	101110	5	5
3.	Signaling	AF4	100xx0	4	4
4.	IPTV	AF3	011xx0	3	3
5.	VPN Gloden	AF2	010xx0	2	2
6.	VPN Silver	AF1	001xx0	1	1
7.	Internet	BE	000000	0	0

Ruch zarządzający (OSPF, ISIS, BGP, LDP, RSVP) jest czystym ruchem IP i nie ma etykiety MPLS w szkielecie sieci. Taki ruch musi być klasyfikowany w oparciu o EXP, ale tylko na DSCP.

3.6.4 Dostępność usług

3.6.4.1 Sprzęt

Konfiguracja sprzętowa a bardzo duży wpływ na dostępność sieci. Dlatego też zalecamy użycie sprzętu klasy operatorskiej, którego niezawodność sięga 99.999%. Urządzenia takie posiadają pasywną szynę danych a wszystkie elementy aktywne są redundantne i wymienialne w czasie pracy urządzenia. Dzięki temu w urządzeniach tych nie występuję SPOF (ang. single point of failure).

3.6.4.2 Sieć

W celu zapewnienia bezprzerwowego działania sieci niezbędne jest wdrożenie technologii zapewniającej pełną redundancje.

3.6.5 Zabezpieczenia na poziomie IP/MPLS

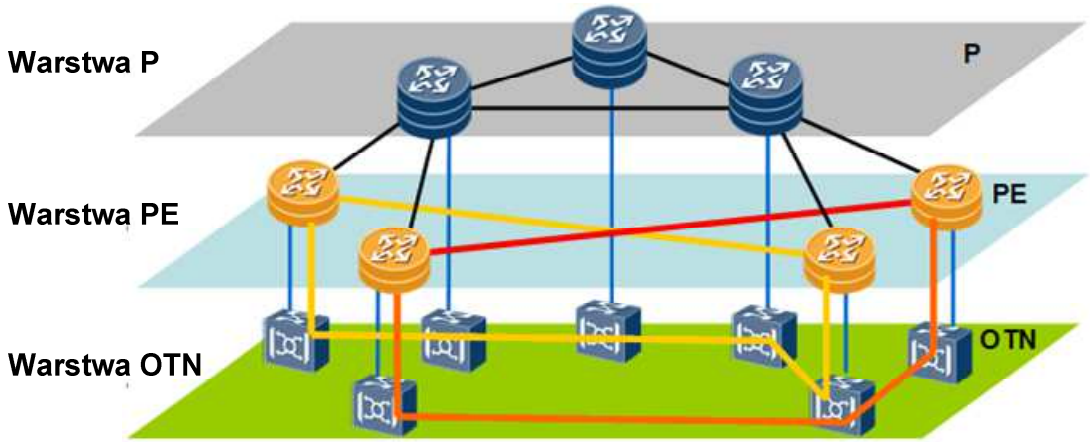
Należy rozważyć użycie następujących funkcjonalności:

- BFD i physical layer OAM dla zapewnienia szybkiej detekcji awarii i szybkiego przełączenia na łączę zapasowe. Implementacja BFD może wykryć awarię w 30ms.
- IGP fast convergence
- BGP fast convergence (np. priority based convergence, next-hop indirection, dynamic update group),
- IGP/LDP synchronization.

3.6.6 Synergia IP & OTN

Warstwa transportowa składa się z warstwy IP/MPLS i DWDM. Sieć powinna być zaprojektowana z uwzględnieniem redundancji obu składników. Nie można dopuścić do sytuacji, gdy łącze podstawowe i backupowe fizycznie realizowane jest tą sama drogą optyczną.

Typowa sieć routowalna zbudowana jest z kilku warstw. Poniższy rysunek pokazuje sieć dwu warstwową z warstwami P i PE. Usługi skonfigurowane na wszystkich routerach w warstwie PE przełączane są przez routery z warstwy P.



Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Rysunek 1. Sieć dwuwarstwowa – szczególny przypadek modelu trójwarstwowego

Linie czerwona i żółta ilustrują przykładowy sposób połączenia routerów P z PE poprzez warstwę OTN (ang. Optical Transport Network).

Synergia ma na celu optymalizację połączeń sieciowych w celu polepszenia wykorzystania przepustowości i zapewnienia braku możliwości wystąpienia pojedynczego punktu awarii na styku sieci MPLS/IP i DWDM.

3.6.6.1 Optymalizacja sieci szkieletowej

W miarę możliwości należy stosować narzędzia do optymalizacji sieci szkieletowej np. „Multi-layer network planning tool" lub równoważne. Jest to system do optymalizacji sieci szkieletowej, który bazuje na synergii informacji otrzymanej z dwóch warstw sieci IP i OTN. Dzięki użyciu informacji pochodzących z dwóch warstw możliwa jest znacząca poprawa wykorzystania zasobów sieci. Rozwiązanie to zabezpiecza sieć przed pokrywaniem się zabezpieczeń w obu warstwach jak również eliminuje SPOF (ang. single point of faliture), które mogą powstać np. w wyniku budowy redundantnych połączeń logicznych na pojedynczym łączu fizycznym.

3.6.6.2 Dynamiczne rozwiązanie SRLG

SRLG to skrót od "shared risk link group". Rożnie rodzaje połączeń między routerowych mogą być oparte na tej samym łączu fizycznym. Jeśli takie łącze ulegnie awarii linki active i standy mogą zostać nią dotknięte. Zadaniem SRLG jest lokalizacji takich zagrożeń i opływane na RSVP-TE w celu ich eliminacji. W ten sposób zapewnia się, że połączenia active i standy nie ulegną awarii jednocześnie.

3.6.6.3 Stosowanie rozwiązań adekwatnych do potrzeb

W niektórych przypadkach stosowanie zaawansowanych rozwiązań xWDM nie ma uzasadnienia ekonomicznego. Jeśli połączeń jest niewiele a ich przepustowość nie będzie rosła lawinowo, dopuszcza się (po uzgodnieniu z Zamawiającym) zastosowanie prostszych rozwiązań.

Warstwę OTN można zrealizować jako szereg bezpośrednich połączeń światłowodowych P2P (ang. point to point) pomiędzy poszczególnymi routerami P i PE. W tym celu należy użyć odpowiednich wkładek optycznych wkładach w routery z obu stron łącza. W przypadku nie wystarczającej ilości światłowodów można użyć technologii pojedynczego włókna (poprzez zastosowanie par odpowiednich wkładek np. WDM TX 1310/RX1550 z jednej strony i WDM TX1550/ RX 1310 po stronie przeciwnej).

3.7 Technika Ethernet

Technika Ethernet jest to rodzina protokołów i technik określonych w zbiorze standardów IEEE 802.3.

Oryginalny standard 802.3 został zatwierdzony w 1983 roku i definiował prędkość transmisji 10Mbps. Obecnie stosowane prędkości transmisji i odpowiadające im standardy to:

- IEEE 802.3u – transmisja 100BaseTX, 100Base-FX
- IEEE 802.3z – transmisja 1000BaseX
- IEEE 802.3ab – transmisja 1000BaseT

- IEEE 802.3ae – transmisja 10Gbit/s przez światłowód (moduły optyczne SR, LR, ER, SW, LW, EW)
- IEEE 802.3ak – transmisja 10Gbit/s – 10GBase-CX4
- IEEE 802.3an - transmisja 10Gbit/s – 10GBase-T
- IEEE 802.3aq transmisja 10Gbit/s – 10Gbase-LRM
- IEEE 802.3ba – transmisja 100Gbit/s

W 2008 roku ukazała się najnowsza wersja 802.3 oznaczona jako 802.3-2008 zawierająca ujednolicone zmiany i wprowadzone wcześniej rozszerzenia. Wraz z poprawką z 2009 roku dotyczącą parametrów czasowych ramki pauzy dla standardu 10G-BASET jest to obecnie obowiązujący standard.

3.7.1 Interfejsy optyczne

W przypadku stosowania interfejsów optycznych należy wykorzystać typowo stosowane interfejsy optyczne, które dzielą się na typy związane z prędkością transmisji danych oraz ze sposobem transmisji danych. Lista stosowanych obecnie typowo interfejsów wraz ze wskazaniem rekomendowanych zawiera poniższa tabela.

Tabela 6. Zestawienie interfejsów optycznych standardu 1Gigabit Ethernet (IEEE 802.3 Clause 34-42)

L.p.	Rodzaj interfejsu optycznego	Opis	Uwagi
1.	1000BASE-SX	do 550m z wykorzystaniem światłowodu wielomodowego	
2.	1000BASE-LX/LH lub LX10	do 10km z wykorzystaniem światłowodu jednomodowego	rekomendowany
3.	1000BASE-ZX	do 70km z wykorzystaniem światłowodu jednomodowego	rekomendowany
4.	1000BASE-BX10	transmisja dwukierunkowa na jednym włóknie, do 10km	
5.	1000BASE-T	do 100m z wykorzystaniem skrętki miedzianej (CAT-5 i wyższe)	

Interfejsy 1Gigabit Ethernet występują także w wersji DWDM, przy czym w typowych rozwiązaniach wspierane jest kilkadziesiąt kanałów zgodnie z siatką ITU.

Tabela 7. Zestawienie interfejsów optycznych standardu 10 Gigabit Ethernet

L.p.	Rodzaj interfejsu optycznego	Opis	Uwagi
1.	10Gbase-SR	(short range) – do 300 metrów z wykorzystaniem światłowodu wielomodowego klasy OM3	
2.	10Gbase-LR	(long reach) – do 10km z wykorzystaniem światłowodu jednomodowego	rekomendowany
3.	10Gbase-LRM	(long reach multimode) – do 260m na światłowodzie wielomodowym OM3 oraz ponad 200m na starszych rodzajach okablowania	
4.	10Gbase-ER	(extended reach) – 40km na światłowodzie jednomodowym	
5.	10Gbase-ZR	nie jest to część oficjalnego standardu – do 80 km na światłowodzie jednomodowym	

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

6.	10GBase-LX4	używa 4 długości fal do przesyłu sygnału 10Gbps z wykorzystaniem starszego okablowania zarówno jedno jak i wielomodowego.	
7.	10Gbase-CX4	15m z wykorzystaniem medium miedzianego	
8.	10Gbase-T	100m z wykorzystaniem skrętki miedzianej CAT6A lub wyższa	

W powyższej tabeli przyjęto Lan PHY - transmisja z prędkością do 10,3125Gbps oraz wskazano rekomendowane standardy modułów optycznych (IEEE 802.3 Clause 48-55). W szczególnych przypadkach dopuszcza się stosowanie interfejsów optycznych nieposiadających rekomendacji, przy czym każdorazowo wymaga to uzasadnienia technicznego (analiza techniczna i uzyskania zgody Zamawiającego.

3.7.2 WAN PHY

WAN PHY (IEEE 802.3 Clause 50) – umożliwia transmisję ramek ethernetowych z wykorzystaniem łączy transmisyjnych SDH/Sonet STM-64/OC-192 (prędkość transmisji jest ograniczana do 9.953 Gbps). Na poziomie warstwy fizycznej WN PHY występuję z odpowiednio 10GBase-SR, 10GBase-LR, 10GBase–ER oraz 10GBase-ZR.

3.7.3 IP poprzez DWDM

W przypadku wyboru rozwiązania klasy IP poprzez DWDM należy zapewnić zgodność interfejsów optycznych z zaleceniem ITU-T G.709. Konstrukcja sieci zgodna z zaleceniem G.709 jest rozwiązaniem umożliwiającym zastosowanie lasera strojonego do siatki określonej przez ITU. W typowych rozwiązaniach wspierane jest kilkadziesiąt kanałów zgodnie z siatką ITU 100GHz lub 50GHz.

3.7.4 Projektowanie łączy warstwy drugiej modelu OSI (Ethernet)

Podstawowym rozwiązaniem w poszczególnych relacjach powinno być łącze oparte o światłowód jednomodowy z optyką dostosowaną do długości łącza.

W przypadku, gdy dysponowana liczba włókien światłowodowych jest niedostateczna, należy przeprowadzić analizę wariantów alternatywnych (analiza techniczna i ekonomiczna) np. zastosować rozwiązania multipleksujące kilka długości fali na jednej parze włókien światłowodowych przypadku wykorzystania infrastruktury transmisyjnej opartej o technologię SDH należy dobrać odpowiednie, kompatybilne moduły optyczne (pamiętając o nieco innej przepływności dla łączy 10GE).

Projektując łącze należy wyznaczyć bilans mocy biorąc pod uwagę

- rodzaj i typ światłowodu,
- jego tłumienność,
- szerokość modalną,
- długość,
- spawy i inne połączenia.

Zaleca się także założyć minimum 10% długości mniej niż wynika to z oficjalnej specyfikacji dla danego typu modułu optycznego (czyli np. 36km a nie 40km), co pozwoli na większą tolerancję dla błędów projektowych oraz dla przyszłych zmian (np. spawanie uszkodzonych światłowodów).

Dla wszystkich łączy o ostatecznym doborze modułów optycznych i rozwiązań transmisyjnych powinny zadecydować pomiary na poszczególnych łączach, które potwierdzą wyniki wyliczeń

teoretycznych oraz zdeterminują czy przy zadanym dystansie i rzeczywistej tłumienności dany rodzaj optyki spełni oczekiwania projektanta.

Dla łączy dłuższych należy dążyć w procesie projektowania do minimalizacji liczby punktów służących do umieszczenia infrastruktury i urządzeń lub o ile nie pozwolą na to możliwości technologiczne rozważyć inne rozwiązania techniki IP poprzez DWDM.

W szczególnych przypadkach po uzyskaniu zgody Zamawiającego dopuszcza się stosowanie optyki z wbudowaną funkcjonalnością zdalnej diagnostyki połączeń optycznych zgodnie z SFF-8472 (Digital Diagnostics Monitoring/Digital Optical Monitoring) Zaleca się wówczas stosowanie Ethernet OAM w cele realizacji funkcji monitoringu stanu łączy oraz ścieżki, diagnozowania jakości usług i podstawowych błędów transmisji i ułatwienia administracji siecią, w szczególności mowa o standardach IEEE 802.3ag oraz IEEE 802.3ah będących obecnie częścią standardu 802.3-2008.

Dla łączy wielokrotnych pomiędzy dwoma lokalizacjami zaleca się:

- stosowanie łączy logicznie zagregowanych,
- terminację połączeń na dwóch różnych modułach liniowych.

Parametry łączy konfigurowane na interfejsach urządzeń powinny umożliwiać realizację usług przewidzianych projektem, w szczególności L2/L3 MPLS VPN oraz powinny optymalizować niezawodność i konwergencję sieci.

W szerszym zakresie projektowym należy pamiętać o:

- unikaniu protokołów STP ze względu na długi czas konwergencji
- zaplanowaniu tunelowania odpowiednich protokołów warstwy drugiej dla odpowiednich usług,
- kontrolowaniu wielkości domen broadcastowych
- zaplanowaniu wykorzystania VLAN ID, w tym translacji i mapowania zgodnie z odpowiednimi usługami.

3.8 Klasy węzłów Dolnośląskiej Sieci Szkieletowej

Na potrzeby projektowania Dolnośląskiej Sieci Szkieletowej dopuszcza się następujące klasy węzłów:

- Węzeł klasy A – obsadzony infrastrukturą pasywną optyczną,
- Węzeł klasy B – Węzeł klasy A poszerzony o elementy systemu xWDM (DWDM),
- Węzeł klasy C – Węzeł klasy B poszerzony o elementy realizujące funkcje IP/MPLS,
- Węzeł klasy D – Węzeł klasy A poszerzony o rozwiązania MPLS posadowione bezpośrednio na infrastrukturze optycznej,
- Węzeł klasy E – Węzeł klasy A poszerzony o elementy systemu Ethernet,
- Węzeł klasy F – Węzeł klasy B poszerzony o elementy systemu Ethernet.

Rodzaj zastosowanego węzła należy przyjąć w uzgodnieniu z Zamawiającym i z zastosowaniem wytycznych dla danej techniki zaimplementowanej w węźle.

3.9 Wytyczne do projektowania miejsc posadowienia aktywnych urządzeń i węzłów sieci klasy NGN w sieci DSS

3.9.1 Wymagania dla szaf telekomunikacyjnych

Szafa kablowa zewnętrzna powinna zostać zainstalowana w miejscu, które nie będzie ograniczać ruchu ulicznego oraz zapewni do niej łatwy dostęp. Szafy kablowe należy ustawiać przy studniach szafkowych mających wielkość dopasowaną do szafek.

Dopuszczalne jest lokalizowanie szafek kablowych we wnękach ścian budynków lub wewnątrz samych budynków. W szafach znajduje się metalowa wsporcza konstrukcja, którą należy uziemić. Umocowanie i ustawienie szafy – szafy kablowe znajdujące się w poszczególnych punktach sieci dystrybucyjnej, należy instalować z uwzględnieniem wytycznych zawartych w projektach budowlanych (lokalizacja) oraz wykończeniowych (montaż, typy szafek).

Instalację szafy telekomunikacyjnej należy wykonać zgodnie z wytycznymi producenta szafy.

Szafy należy wyposażyć w układ ocieplania jak i chłodzenia w celu zapewnienia wewnątrz odpowiednich warunków temperaturowych – zgodnie z normami PN-ETSI EN 300 019-1-4, PN-ETSI EN 300 019-1-3. Elementy grzewcze i chłodzące należy dobrać indywidualnie, na podstawie obliczeń mocy pobieranej przez zamontowane urządzenia oraz warunków atmosferycznych. Szafy zewnętrzne powinny w pełni chronić sprzęt znajdujący się wewnątrz. Obudowy muszą chronić zainstalowane elementy sieci przed negatywnym wpływem czynników pogodowych zewnętrznych np.: opadami deszczu, śniegu, promieniowaniem słonecznym oraz zapyleniem.

Szafa telekomunikacyjna winna mieć wydzielone bloki: blok zasilania zewnętrznego; blok zasilania wewnętrznego UPS; blok pasywny zakończenia kabli światłowodowych; blok aktywny sprzęt teletransmisyjny sieci DSS; blok kolokacji dla sprzętu teletransmisyjnego operatorów lokalnych. Bloki winny mieć wydzielony niezależny dostęp i monitoring.

3.9.2 Wymagania dla kontenerów telekomunikacyjnych

Kontener należy wyposażyć we wszystkie niezbędne systemy w zależności od funkcji jaką będzie pełnił w sieci. Wymiary kontenera umożliwiające zabudowę sprzętu i systemów teletransmisyjnych. Kontener musi być zbudowany na bazie samodzielnej konstrukcji stalowej. Wszystkie elementy muszą być zabezpieczone antykorozyjnie.

W kontenerze węzła sieci powinno zostać stworzone środowisko, w którym wszystkie zainstalowane urządzenia będą wydajnie pracować. Aby zapewnić takie warunki, powinien zostać zainstalowany odpowiedni system ogrzewania, wentylacji i klimatyzacji HVAC (ang. Heating, Ventilation, and Air Conditioning).

Temperatura powietrza wewnątrz pomieszczenia technicznego/kontenera stacji bazowej powinna być utrzymana w przedziale określonym przez producenta urządzeń. Temperatura powietrza odnosi się do temperatury wewnątrz pomieszczenia mierzonej zazwyczaj 60 cm ponad podłogą na środku pomieszczenia. System HVAC powinien zapewniać utrzymanie odpowiedniej temperatury powietrza wewnątrz pomieszczenia.

W celu zmniejszenia kosztów operacyjnych i zapobiegnięciu zamarzaniu sprężarek przy niskich temperaturach zewnętrznych, urządzenia HVAC powinny mieć elementy grzewcze i termostaty umożliwiające chłodzenie lokalizacji przez powietrze z zewnątrz, jeżeli temperatura na zewnątrz spadnie poniżej określonej wartości (tryb wolnego chłodzenia - ang. free-cooling mode).

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Z uwagi na ograniczenia przestrzenne kontenera, system HVAC stosowany w tym rozwiązaniu powinien być klimatyzatorem w obudowie kompaktowej.

W wyliczeniach projektowych zostanie podana wartość zapasu na system HVAC, wymagany na wypadek rozbudowy kontenera o dodatkowe urządzenia.

Kontenery muszą być odporne na szkodliwe działanie zjawisk pogodowych. Kontener musi być wybudowany/postawiony zgodnie z istniejącym prawem budowlanym (i innymi stosującymi się podczas ich budowy/stawiania).

Wymagania środowiskowe:

- system klimatyzacji złożony z 2 klimatyzatorów precyzyjnych (1 pracuje, 1 pozostaje w rezerwie), zapewniając odbiór ciepła od urządzeń; klimatyzatory powinny pracować w układzie "free-cooling", z nawiewem powietrza w przestrzeń podniesionej podłogi; klimatyzatory muszą być przeznaczone dla zastosowań przemysłowych, przystosowane do pracy ciągłej w pomieszczeniach bez stałej obsługi technicznej; wydajność chłodnicza jednostki wewnętrznej musi być dobrana w zależności od pomieszczenia węzła zapewniając temperaturę 20° C ± 2° C i wilgotność 45% ± 20%.;
- urządzenia nie powinny być bezpośrednio wystawione na środowisko powodujące korozję; w przypadkach instalacji kontenera w takich miejscach należy zapewnić odpowiednie filtrowanie powietrza wewnątrz;
- odpowiednie filtrowanie powietrza zapewniające odpowiednią, jakość powietrza wewnątrz (ilość cząsteczek unoszących się w powietrzu nie przekraczająca 90 u.g/m3>;
- minimalna wysokość do sufitu około 2400 mm umożliwiająca swobodny montaż kabli, szaf krosowych i innych urządzeń.

Dodatkowe wymagania:

- Podłoga:
  - wytrzymałość min. 800kg/m²;
  - docieplenie o grubości do uzyskania współczynnika max. k=0,28W/m²;
  - pokryta wykładziną trwałą, antystatyczną;
  - otwór technologiczny do wprowadzenia kabli.
- Ściany:
  - materiał: żelbet ocieplony, warstwowy;
  - docieplenie o grubości do uzyskania współczynnika max. k= 0,28W/m²;
  - w ścianach otwory technologiczne pod wentylator wywiewowy, klimatyzator oraz przepust kablowy;
  - ściany wewnętrzne gładkie w kolorze białym, konstrukcja umożliwiająca zawieszenie urządzeń o ciężarze co najmniej 30kg;
  - ściany zewnętrzne odporne na czynniki atmosferyczne oraz na uszkodzenia mechaniczne;
  - odporność ogniowa 120 minut.
- Dach:
  - wodoszczelny,
  - docieplenie o grubości do uzyskania współczynnika max. k = 0,28 W/m²;
  - odporność ogniowa 30 minut.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Typ kontenerów i rozwiązania technologiczne wymagają każdorazowo pisemnej akceptacji Zamawiającego.

3.9.3 Wytyczne dotyczące pomieszczeń i infrastruktury towarzyszącej węzłów szkieletowych

Wymagania zasilania:

- Pomieszczenie węzła szkieletowego powinno być zasilane ze źródła zasilania z umową gwarantującą dostarczanie energii w sposób bezprzerwowy.

Dodatkowo:

- dla zapewnienia ciągłości zasilania gwarantowanego pomieszczenie powinno być wyposażone w 2 UPS-y, pracujące równolegle i połączone z rozdzielnicą R-UPS;
- system UPS podłączony do skrzynki mocy agregatu prądotwórczego kontenerowego (lub agregatu przystosowanego do pracy na zewnątrz) do rozdzielnicy R-UPS;
- każdy z UPS'ów powinien być wyposażony w hermetyczną baterię, umożliwiającą bezprzerwowe zasilanie przez min. 10 minut, przy maksymalnym obciążeniu;
  - UPSy powinny być podłączone za pomocą przełącznika obejścia serwisowego „BYPASS" realizującego przełączenia bezprzerwowe; przełącznik powinien umożliwiać bezprzerwowe odłączenie jednego lub dwóch UPS-ów w celach serwisowych i wykonania zabiegów konserwacyjnych;
  - agregat prądotwórczy (wyposażony w zbiornik paliwa umożliwiający autonomiczne zasilanie przez czas 8-10 godzin przy pełnym obciążeniu), którego typ i moc zostanie dobrana na etapie projektu; wstępnie można przyjąć użycie agregatu prądotwórczego pracującego na zewnątrz budynku; moc agregatu powinna pokrywać całkowite zapotrzebowanie na energię wszystkich urządzeń zainstalowanych w pomieszczeniu węzła szkieletowego;
  - automatyka sterująca agregatem powinna umożliwić uruchomienie go po czasie od 5 do 60 sekund po zaniku zasilania z sieci energetycznej oraz samoczynne przełączanie zasilania;
  - uziemienie wyposażone w główną szynę uziemiającą do której podłączone zostaną wszystkie elementy metalowe znajdujące się w pomieszczeniu węzła szkieletowego oraz elementy uziemiające kabli i fiderów wprowadzonych do wewnątrz budynku.

W ramach projektu należy wyznaczyć pobór mocy i zajętość przestrzeni dla każdego obiektu według poniższego przykładu wyznaczającego szacunkowe parametry

3.9.3.1 Szacunkowy pobór mocy i zajętość przestrzeni

Węzły szkieletowe, będą wyposażone co najmniej w:

- redundantne urządzenia transmisyjne;
- systemy zasilania awaryjnego;
- system klimatyzacji;
- system kontroli dostępu;
- system gaszenia.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Przyjmując poniższe założenia można uznać iż cała moc pobierana przez urządzenia zamieniana jest na ciepło; redundantne zasilacze pracują z mocą rzeczywistą równą mocy zasilacza/ilość zasilaczy, można szacunkowo określić pobór mocy dla całości systemów.

Tabela 8. Wyznaczenie szacunkowego poboru mocy węzła - przykład

L.p.	Rodzaj wyposażenia węzła	Szacowana moc
1.	Urządzenia teletransmisyjne	- 2*9kW;
2.	System HVAC	- 10kW;
3.	Oświetlenie + sprzęt pomiarowy	- 0,5kW;
4.	Pozostałe systemy	- 1kW;
	SUMA	**- 29,5kW.**

Urządzenia teletransmisyjne powinny zostać rozlokowane w dwóch szafach teletechnicznych. Instalacje kablowe zlokalizowane zostaną w osobnej szafie teletransmisyjnej. Dodatkowa szafa przewidziana jest na ewentualną kolokację urządzeń innych operatorów.

3.10 Organizacja Dolnośląskiej Sieci Szkieletowej

W ramach DSS należy zaprojektować następujące struktury:

- Strukturę transportową opartą na technice zwielokrotniania częstotliwości DWDM na bazie wydzielonej liczby włókien – na potrzebę realizacji dla podmiotów zbiorowych i klientów wewnętrznych:
  - Usług sieci szkieletowej,
  - Usług sieci dystrybucyjnej,
- Strukturę transportową oparta na technice Ethernet poprzez światłowód na potrzebę realizacji sieci zarządzania infrastrukturą i usługami Dolnośląskiej Sieci Szkieletowej.

3.11 Zawartość dokumentacji projektowej w zakresie infrastruktury sieciowej - (wymagania minimalne)

W ramach dokumentacji opisowej należy posługiwać się ujednoliconą stroną opisową tabela dokumentacji projektu technicznego przedstawiona jak poniżej.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Stadium:	**(np. PROJEKT WYKONAWCZY)**	
Temat opracowania:	…	
Obiekt:	…	
Branża:	…	
Inwestor:	…	
Jednostka projektowa:	…	
	Nr archiwalny:	…
	Tom:	… / …
	Egzemplarz:	… / …

Funkcja	**Imię i Nazwisko**	**Uprawnienia/ specjalność**	**Numer uprawnień**	**Data**	**Podpis**
Projektował :					
Opracował:					
Opracował					

Miejscowość - Data

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Jednocześnie należy stosować stopkę dokumentu (co najmniej w stronie opisowej jak i części opisowej projektu) zgodnie z wzorem przedstawionym na rysunku

Rysunek 2. Wzór stopki dokumentu projektowego

Oświadczenie projektanta

O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust. 4 Ustawy Prawo budowlane z dnia 7 lipca 1994 (Dz. U. 2006.156.1118 z późniejszymi zmianami)

oświadczam jako projektant/sprawdzający

że projekt:

„ … ”

został sporządzony zgodnie z obowiązującymi przepisami, normami i zasadami wiedzy technicznej oraz że jest on kompletny z punktu widzenia celu jakiemu ma służyć. Oświadczam zarazem, że zawartość projektu spełnia wymagania Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 (Dz. U. 2004.202.2072) w sprawie szczegółowego zakresu i formy dokumentacji projektowej.

.....

(data, podpis)

Rysunek 3. Wzór oświadczenia projektanta

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

3.11.1 Zawartość dokumentacji projektowej

1. Część ogólna

1.1. Przedmiot opracowania

Należy określić przedmiot opracowania (np. „Przedmiotem opracowania jest projekt wykonawczy węzła sieci w ramach Dolnośląskiej Sieci Szkieletowej (DSS)”).

Należy zamieścić informację o szerszym kontekście opracowania (np. jeśli opracowanie wchodzi w skład wielobranżowej dokumentacji projektowej należy podać nazwę przedsięwzięcia i wymienić już opracowane projekty budowlane i wykonawcze, specyfikacje techniczne wykonania i odbioru, lub przedmiary prac powiązane z opracowaniem).

1.2. Podstawa opracowania projektu

Należy określić podstawę wykonania opracowania oraz wykorzystane źródła danych.

1.3. Opis ogólny inwestycji

1.3.1. Położenie geograficzne

Należy zdefiniować lokalizację/lokalizacje obiektu/obiektów.

1.3.2. Zakres rzeczowy

Należy określić główne wskaźniki zakresu rzeczowego.

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

2. Słownik, terminologia i symbolika

2.1. Słownik i terminologia

Należy zdefiniować pojęcia i terminy używane w opracowaniu, które nie są powszechnie stosowane

2.2. Symbolika

Należy zdefiniować symbole stosowane na rysunkach

2.3. Oznaczenia i numeracja

Należy zdefiniować stosowane oznaczenia i zasady numeracji elementów.
Np.:

DSS	-	Dolnośląska Sieć Szkieletowa
WS_x	-	Węzeł szkieletowy o numerze „x”
WD_x	-	Węzeł dystrybucyjny o numerze „x”
CZS	-	Centrum Zarządzania Siecią
ZCZS	-	Zapasowe Centrum Zarządzania Siecią

3. Bazowe dokumenty normatywne i dokumenty odniesienia

3.1. Wykaz norm i dokumentów odniesienia

Należy wymienić wszystkie dokumenty odniesienia i normy bazowe cytowane w opracowaniu.

4. Charakterystyka techniczna projektowanego obiektu

4.1. Szczegółowe rozwiązania i obliczenia projektowe.
4.2. Szczegółowe wytyczne realizacyjne.
4.3. Szczegółowe wytyczne w zakresie wdrożenia.
4.4. Szczegółowe wytyczne w zakresie szkoleń i eksploatacji.
4.5. Szczegółowe wytyczne w zakresie procedur i kolejności „uruchamiania i zamykania” poszczególnych składników

5. Tabele

5.1. Spis obiektów objętych projektem

Wymienić obiekty objęte opracowaniem i podać ich lokalizację.

L.p.	Oznaczenie	Obiekt	Adres

5.2. Zestawienie typów i liczby kart/ urządzeń / zespołów urządzeń

Wymienić elementy dostaw materiałów i urządzeń, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

L.p.	Nazwa urządzenia	Zakres/Liczba	Opis Wymagań
…	…		

5.3. Zestawienie typów i systemów monitoringu/zarządzania wraz ze wskazaniem urządzeń monitorowanych/zarządzanych

L.p.	Nazwa systemu monitoringu/zarządzania	Urządzenia monotorowane/zarządzane	Lokalizacja
…	…		

5.4. Zestawienie monitorowanych urządzeń

L.p.	Serwer	Producent	Monitowanie systemu plików	Monitorowanie obciążenia procesora	Monitorowanie procesów
…					

5.5. Zestawienie monitorowanych zdarzeń/procesów dla poszczególnych urządzeń

L.p.	Dostawca	Serwer	Zdarzenia/monitorowane elementy
…			

5.6. Zestawienie prac podstawowych

Wymienić prace, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

L.p.	Opis czynności	Zakres/Liczba	Wymagania/Uwagi
	…	…	…

6. Spis rysunków

Należy zamieścić spis rysunków wykorzystanych w opracowaniu. Np.:

Rysunek 1. Schemat ogólny infrastruktury węzła

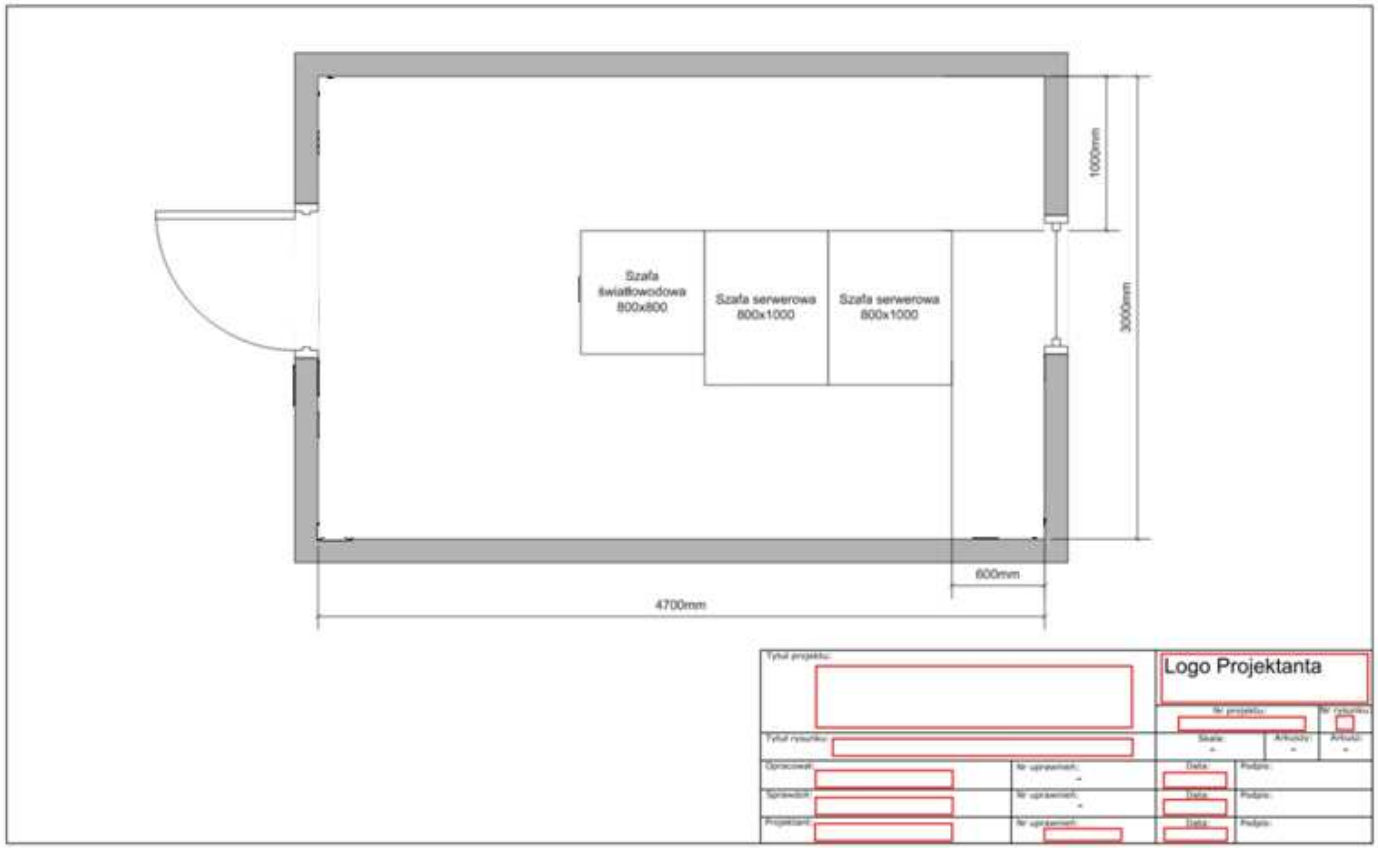
Rysunek 2. Rzut pomieszczeń … wraz z oznaczeniem projektowanej lokalizacji urządzeń/szaf węzła

Rysunek 3. Lokalizacja urządzeń systemu w szafie … w węźle …

Rysunek 4. Lokalizacja urządzeń systemu w szafie … w węźle …

Rysunek 5. ….

3.11.2 Wzór rysunku - dokumentacja projektowa dla węzła transmisyjnego



Rysunek 4. Wzór graficznej prezentacji węzła transmisyjnego

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

4 Centrum Zarządzania Siecią

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 wykonują operacje takie jak zmiany konfiguracji, uaktualnianie oprogramowania urządzeń, oraz wdrażanie nowych i podłączanie nowych klientów.

4.1 Wymagania ogólne

Platforma Zarządzania eksploatowana w ramach DSS winna posiadać grupę cech umożliwiających zarówno zarządzenia znanymi elementami sieci jak i wszystkimi nowymi technologiami, które w danej sieci będą implementowane. Zaprojektowana platforma musi być:

- **modularna i skalowalna** – rozmiar sieci, jej konfiguracja oraz stosowane technologie ulegają ciągłym zmianom. System zarządzania musi podążać za ewolucją sieci w sposób naturalny i wymagający jak najmniejszych zmian w samej platformie,
- **zorientowana geograficznie** - sieci telekomunikacyjne mają strukturę hierarchiczną i sposób zarządzania poszczególnymi jej elementami często zależy od ich rzeczywistego posadowienia. Platforma powinna więc odzwierciedlać nie tylko logiczną ale i geograficzną strukturę sieci oraz umiejscowienie we współrzędnych geograficznych zarządzanych elementów sieci,
- **niezawodna** – w miejscach krytycznych dla platformy i systemu zarządzania szczególnie narażonych na utratę danych i funkcjonalności, powinny wystąpić sprzętowe i programowe mechanizmy gwarantujące zachowanie danych i funkcji systemu,
- **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 *„de facto”* standardem wymiany informacji funkcjonującym w tym zakresie w technologiach IT,
- **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 niepowołanym dostępem.

Powszechnie przyjętym modelem systemów zarządzania siecią jest model ISO znany pod angielskim skrótem FCAPS (w oparciu o standard ISO 7498-4), od pierwszych liter głównych funkcjonalności:

- **Fault** - zarządzanie awariami, wykrywanie problemów, filtrowanie i korelacja wydarzeń, analiza wpływu na usługi.
- **Configuration** - zarządzanie konfiguracjami, a także oprogramowaniem urządzeń: weryfikacja wersji i dystrybucja aktualizacji oprogramowania, obsługa wzorców konfiguracji, robienie kopii zapasowych i dystrybuowanie konfiguracji.
- **Accounting** - zbieranie informacji ilościowych o ruchu, usługach i urządzeniach
- **Performance -** zbieranie informacji wydajnościowych o ruchu, usługach i urządzeniach

- **Security** - nadzorowanie bezpieczeństwa poprzez weryfikację uprawnień osób dokonujących zmian w sieci, tworzenie logów i innych informacji audytowych, zapobieganie zmianom niepożądanym.

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

- wizualizacja topologii łączy i urządzeń, w tym inwentaryzacja automatyczna wraz z możliwością eksportu do systemu ewidencji. Moduł taki bywa częścią systemu zarządzania konfiguracjami, lub awariami. Jest to jedna z podstawowych funkcji.
- wprowadzanie usług (ang. provisioning), moduł umożliwia podłączanie kolejnych klientów i usług w sposób zautomatyzowany i dostosowany do procesów operatora sieci. Taka funkcjonalność zwykle pojawia się w sieciach usługowych większej skali.

By system zarządzania mógł działać, konieczne jest zapewnienie dla niego lokalnej sieci zawierającej działające pod kontrolą systemu serwery przyjmujące dane pochodzące z urządzeń, ale także serwery i systemy dyskowe do archiwizacji danych zgodnie z przyjętą polityką retencji, sieć lokalną łączącą wszystkie elementy centrum zarządzania, i niezbędne zabezpieczenia (przeważnie firewall) zapobiegające atakom na centrum.

Informacje o sieci i usługach są 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 żeby miała użyteczną wartość musi być realizowana sprzętowo i w sposób rozproszony, na poszczególnych kartach liniowych. Można wtedy osiągnąć wartość próbkowania 1:N, gdzie N może mieć wartość na poziomie od jeden do kilkuset oraz do kilkudziesięciu tysięcy „flow". W przypadku stosowania takiego mechanizmu na potrzeby Dolnośląskiej Sieci Szkieletowej rekomenduje się co najmniej wersję Netflow 9, która wspiera multicast, IPv6 oraz MPLS.

Urządzenia potrzebują także dodatkowych informacji pochodzących z rozmaitych elementów systemu zarządzania, na przykład informacji o autoryzacji i uprawnieniach użytkowników, przesyłane zwykle za pomocą protokołów RADIUS, TACACS+ lub LDAP.

Ze względu na krytyczne znaczenie centrum zarządzania siecią dla operatora, oraz dla klientów usług, centrum winno być zduplikowane dla uzyskania niezbędnej redundancji geograficznej. Systemy licencjonowanie umożliwiają uzyskanie takiej funkcjonalności taniej, niż uruchomienie dwóch równolegle działających centrów.

4.2 Minimalny obszar sprzętowy objęty mechanizmami zarządzania i monitorowania

Metodyka bezpieczeństwa musi bowiem być kompromisem nakładami i kosztami oraz potencjalnymi stratami. Należy więc zdefiniować jakie zasoby w zależności od rodzaju urządzeń powinny podlegać ochronie. Poniżej w Tabeli przedstawiono minimalny wymagany zestaw zasobów, które w zależności od rodzaju urządzeń mogą podlegać ochronie w ramach realizacji sieci DSS.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Tabela 9. Zestaw zasobów, które w zależności od rodzaju urządzeń mogą podlegać ochronie

L.p.	Obszar (rodzaj urządzeń) Mechanizmy bezpieczeństwa	
I.	**Urządzenia sieciowe: Access Serwery, Routery dostępowe**	
	I.1.	uruchomienie access-list limitujących dostęp do urządzenia dla osób niepowołanych
	I.2.	konfiguracja zdalnego oraz lokalnego uwierzytelnienia dla uprawnionych administratorów
	I.3.	konfiguracja uwierzytelniania sąsiadów dla protokołu routingu OSPF
	I.4.	konfiguracja uwierzytelniania dla protokołu synchronizacji czasu NTP
	I.5.	kontrola zmian konfiguracji
	I.6.	konfiguracja monitorowania systemu poprzez protokół SNMP,
	I.7.	konfiguracja raportowania zdarzeń do systemu zarządzania z wykorzystaniem protokołu SYSLOG,
II.	**Serwery usługowe**	
	II.1.	ograniczenie ilości działających usług i zainstalowanych pakietów w systemie do niezbędnego minimum,
	II.2.	ograniczenie dostępu administracyjnego do szyfrowanych sesji ze stacji zarządzania
	II.3.	instalacja uaktualnień systemowych w miarę pojawiania się nowych wersji (patches)
	II.4.	uruchomienie oprogramowania weryfikującego uprawnienia do zasobów systemowych i weryfikacja konfiguracji systemu (ograniczenie ilości skryptów suid, konfiguracja i optymalizacja jądra systemu)
	II.5.	uruchomienie aplikacji weryfikującej zmiany w plikach systemowych
	II.6.	uruchomienie systemu archiwizacji
	II.7.	konfiguracja raportowania zdarzeń do systemu zarządzania z wykorzystaniem protokołu SYSLOG
	II.8.	konfiguracja monitorowania systemu poprzez protokół SNMP
	II.9.	zabezpieczenie dostępu do serwerów za pomocą urządzeń FireWall
III.	**Serwery AAA**	
	III.1.	ograniczenie ilości działających usług i zainstalowanych pakietów w systemie do niezbędnego minimum
	III.2.	instalacja uaktualnień systemowych w miarę pojawiania się nowych wersji (patches)
	III.3.	uruchomienie oprogramowania weryfikującego uprawnienia do zasobów systemowych i weryfikacja konfiguracji systemu (ograniczenie ilości skryptów suid, konfiguracja i optymalizacja jądra systemu)
	III.4.	uruchomienie aplikacji weryfikującej zmiany w plikach systemowych
	III.5.	uruchomienie systemu archiwizacji
	III.6.	konfiguracja raportowania zdarzeń do systemu zarządzania z wykorzystaniem protokołu SYSLOG
	III.7.	konfiguracja monitorowania systemu poprzez protokół SNMP
	III.8.	zabezpieczenie dostępu do serwerów za pomocą urządzeń FireWall,

L.p.	Obszar (rodzaj urządzeń) Mechanizmy bezpieczeństwa	
IV.	**Urządzenia sieciowe : Przełączniki**	
	IV.1.	uruchomienie access-list limitujących dostęp do urządzenia dla osób niepowołanych,
	IV.2.	konfiguracja zdalnej oraz lokalnej autentykacji dla uprawnionych administratorów
	IV.3.	konfiguracja autentykacji dla protokołu synchronizacji czasu NTP
	IV.4.	kontrola zmian konfiguracji
	IV.5.	konfiguracja monitorowania systemu poprzez protokół SNMP
	IV.6.	konfiguracja raportowania zdarzeń do systemu zarządzania z wykorzystaniem protokołu SYSLOG
	IV.7.	konfiguracja zabezpieczeń portów przełącznika
V.	**Urządzenia sieciowe: Rutery szkieletowe**	
	V.1.	uruchomienie access-list limitujących dostęp do urządzenia dla osób niepowołanych
	V.2.	konfiguracja zdalnej oraz lokalnej autentykacji dla uprawnionych administratorów
	V.3.	konfiguracja autentykacji sąsiadów dla protokołu routingu OSPF
	V.4.	konfiguracja autentykacji dla protokołu synchronizacji czasu NTP
	V.5.	kontrola zmian konfiguracji
	V.6.	konfiguracja monitorowania systemu poprzez protokół SNMP
	V.7.	konfiguracja raportowania zdarzeń do systemu zarządzania z wykorzystaniem protokołu SYSLOG
VI.	**Serwery zarządzania / stacje zarządzania**	
	VI.1.	ograniczenie ilości działających usług i zainstalowanych pakietów w systemie do niezbędnego minimum
	VI.2.	instalacja uaktualnień systemowych w miarę pojawiania się nowych wersji
	VI.3.	uruchomienie oprogramowania weryfikującego uprawnienia do zasobów systemowych i weryfikacja konfiguracji systemu (ograniczenie ilości skryptów suid, konfiguracja i optymalizacja jądra systemu)
	VI.4.	uruchomienie aplikacji weryfikującej zmiany w plikach systemowych
	VI.5.	konfiguracja monitorowania systemu poprzez protokół SNMP
	VI.6.	uruchomienie systemu archiwizacji

4.3 Zarządzanie ruchem

4.3.1 Zabezpieczenia urządzeń i sieci

Część wymienionych standardów zawiera opisy zabezpieczeń rozmaitych protokołów, jednak znacząca część mechanizmów zabezpieczających nie jest zestandaryzowana i zależy od implementacji poszczególnych producentów. Poniżej wymieniono minimalistyczny przegląd podstawowej funkcjonalności.

Filtrowanie ruchu tranzytowego (ang. data plane) – urządzenia muszą zapewniać możliwość konfiguracji filtrów pozwalających urządzeniom na blokowanie pakietów IPv4/v6 na podstawie parametrów takich jak docelowy/źródłowy adres IP, numer protokółu, numery portów docelowych/źródłowych TCP/UDP i podobne.

W przypadku urządzeń agregacyjnych przesyłających (tunelujących) cały ruch dalej w warstwie drugiej taka funkcjonalność nie musi być konieczna – filtrowanie przeprowadzi dopiero router szkieletowy. Oznacza to obniżenie ceny urządzeń agregujących, ale także i mniej efektywne wykorzystanie przepustowości, gdyż ruch niepożądany będzie odrzucony dopiero po przebyciu łącza do szkieletu, zabierając niepotrzebnie miejsce ruchowi normalnemu.

Filtrowanie ruchu odbieranego (ang. control plane) – analogiczny mechanizm musi być także dostępny by zabezpieczyć dostęp do samego urządzenia. Filtr (definiowany podobnie jak dla ruchu tranzytowego) dotyczy całości ruchu odbieranego i terminowanego przez router, począwszy od protokołów routingu poprzez „pingi" i wszelkie inne pakiety wymagające przetwarzania przez główny procesor.

Ograniczanie ruchu odbieranego – o ile filtr pozwala przyjąć lub odrzucić ruch, ograniczniki pozwalają na zmniejszenie przepustowości dla takiego ruchu. Podnosi to stabilność urządzenia w wypadku ataków typu „przeciążenie urządzenia" (ang. Denial of Service), gdyż nie są one obciążane przetwarzaniem nadmiernych i niepotrzebnych danych.

Weryfikacja adresu źródłowego (ang. uRPF, unicast Reverse Path Forwarding Check) – mechanizm sprawdza czy adres źródłowy pakietu który ma być przełączony przez router zgadza się z tablicą routingu i nie jest podrobiony. Mechanizm ten odsiewa dużą część ruchu niepożądanego w sieci. Mechanizm ten jest częściowo opisany w RFC 3704 „Ingress Filtering for Multihomed Networks".

4.4 Infrastruktura Centrum Zarządzania Siecią (CZS)

Urządzenia wchodzące w skład Centrum Zarządzania Siecią (przełącznik CZS oraz urządzenia typu firewall z obsługą IDS/IPS) wraz z elementami Systemu Zarządzania Siecią i systemami prezentacji stanu sieci powinny tworzyć spójną całość umożliwiającą realizację powierzonych im funkcji.

4.4.1 Przełącznik sieciowy 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 zatem następujące wymagania:

w przypadku urządzenia modularnego:

- możliwość montażu w szafie 19'';
- zasilane prądem przemiennym 230V;
- wydajność urządzenia nie mniej niż 80GB/s;

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- jeżeli chodzi o zapewnienie ciągłości usług:
  - redundancja krytycznych elementów urządzenia (karty zarządzające, matryca przełączająca, zasilacze, wentylatory),
  - umożliwienie wymiany modułów kart rozszerzeń, „na gorąco" (ang. *hot swap*),
  - zaimplementowana obsługa portów o prędkości 1Gbps,
  - możliwość rozbudowy celem uzyskania obsługi portów o prędkości 10Gbps,
  - wymagana jest redundancja krytycznych elementów urządzenia (karty zarządzające, matryca przełączająca, zasilacze),
- dla urządzenia tworzącego stos:
  - zaimplementowana obsługa portów o prędkości 1Gbps
  - możliwość rozbudowy w celu uzyskania obsługi portów o prędkości 10Gbps
  - wymagane jest łączenie urządzeń w stos realizowane przez dedykowane interfejsy o przepustowości co najmniej 32Gbps,
- obsługi protokołów i standardów:
  - IPv4: RIP, OSPF, BGP-4, IS-IS, PIM-SM/SSM, IGMP, BGP-MP for multicast, MSDP i Anycast RP,
  - IPv6 : RIPng, OSPFv3, IS-IS for IPv6, BGP-MP for IPv6 (BGP4+), PIM-SM/SSM i MLD,
  - Bidirectional Forwarding Detection (BFD) m.in. dla OSPFv2, IS-IS, PIM, tras statycznych, Multi hop BFD
  - NonStop Forwarding (BGP, OSPF, IS-IS, MPLS-TE, LDP, VPLS),
  - obsługa VRRP lub odpowiednika,
  - 802.1ad, QinQ, 802.1Q, obsługa agregacji 802.3ad,
  - obsługa mechanizmów QoS (klasyfikacja, oznaczanie, policing,) per VLAN, klasyfikacji ruchu w oparciu o: MPLS EXP, IP DSCP, VLAN , adresy MAC i IP, protokół,
- możliwość montażu w szafie 19",
- zasilanie prądem zmiennym 230V,
- możliwość obsługi protokołów warstwy 3 i zgodność ze standardami:
  - IPv4: RIP,OSPF, IS-IS, PIM-SM/SSM, IGMP, MSDP i Anycast RP,
  - IPv6: RIPng, OSPFv3, IS-IS, PIM-SM/SSM I MLD,
  - Obsługa BFD lub odpowiednika,
  - Obsługa VRRP lub odpowiednika,
  - Obsługa standardów IEEE 802.1Q, IEEE802.1ad, IEEE802.3ad,

- funkcjonalności bezpieczeństwa sieciowego:
  - listy kontroli dostępu (ACL) L2 i L3 (IPv4 i IPv6),
  - Unicast Reverse Path Forwarding (uRPF),
  - DHCP snooping, DHCP relay,
  - mechanizmy ochrony przed sztormami ruchu (ang. *broadcast/multicast storm*),
  - obsługa autoryzacji administratorów/użytkowników za pośrednictwem RADIUS,
- zarządzanie urządzeniem:
  - możliwość definicji uprawnień poszczególnych administratorów urządzenia,
  - możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej, jak i import na urządzenie,
  - możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń regularnych,
  - zarządzanie przez CLI (konsola szeregowa, SSHv2), SNMPv3,
  - syslog,
  - obsługa tworzenia i przywracania kopii zapasowych konfiguracji z lokalnej pamięci urządzenia lub serwera,

4.4.2 Router

Urządzenie modularne:

- możliwość montażu w szafie 19”;
- wysokość maksymalna 5RU;
- min 512 MB pamięci DRAM
- min 256 MB pamięci Flash min 2 portów Ethernet 10/100/1000 Base-T, każdy w pełni konfigurowalny z pkt. widzenia warstwy 3 modelu IOS/OSI (dopuszczalne wbudowane, jak i w formie wkładek);
- oprogramowanie/system umożliwiający wsparcie dla usług/protokołów: DHCP (client i server), listy dostępowe ACL, BGP, RIP, Frame Relay, 802.1Q, IGMPv3, NAT, NetFlow lub równoważny, OSPF, PIM, PPP, SNMP, LLDP, VRRP, IPSec (DES, 3DES), Firewall, GRE, IS-IS, RADIUS, TACACS+, MPLS, SIP;
- wydajność przetwarzania pakietów IPv4 – co najmniej 340 kpps;
- zasilania ze źródła zmiennoprądowego 230V;
- minimum dwa porty dedykowane dla zarządzania: port konsoli oraz port asynchroniczny lub USB;
- możliwość instalacji kart rozszerzeń z interfejsami szeregowymi;
- zarządzanie urządzeniem:

- możliwość definicji uprawnień poszczególnych administratorów urządzenia,
- możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej, jak i import na urządzenie,
- zarządzanie przez CLI (konsola szeregowa, SSHv2), SNMPv3,
- syslog,
- obsługa tworzenia i przywracania kopii zapasowych konfiguracji z lokalnej pamięci urządzenia lub serwera,

UWAGA: dopuszcza się połączenie w jednym urządzeniu funkcjonalności routera określonych w niniejszym rozdziale z funkcjonalnościami Firewall z IDS/IPS określonymi w rozdziale 4.4.3, w ten sposób, że jedno urządzenie pełnić będzie jednocześnie rolę routera i firewalla z IDS/IPS.
Dopuszcza się także rozwiązanie z osobnymi urządzeniami pełniącymi funkcje routera, firewalla oraz sondy z IDS/IPS. W takim wypadku komplet 3 takich urządzeń musi posiadać wszystkie funkcjonalności wymagane w rozdziale 4.4.2 oraz 4.4.3.

4.4.3 Firewall z IDS/IPS

Urządzenie powinno spełniać poniższe warunki:

- Ściana ogniowa śledząca stan połączeń z funkcją weryfikacji informacji charakterystycznej dla warstwy aplikacji;
- Możliwość montażu w szafie 19”;
- Zasilanie prądem zmiennym 230V;
- Urządzenie klasy Enterprise lub Campus;
- Pracę w trybie wysokiej dostępności (HA) – klaster;
- Wsparcie lub obsługa 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;
- Sprzętowe wsparcie szyfrowania połączeń IPsec (DES, 3DES, AES 128, AES 192 oraz AES256);
- Wydajność w trybie firewall co najmniej 5Gbps dla obsługi typowego ruchu IPv4;
- Wydajność w trybie IPS wynoszącą co najmniej 1Gbps dla obsługi typowego ruchu IPv4;
- Obsługa co najmniej 20 000 połączeń na sekundę;
- Obsługę co najmniej 250 000 jednoczesnych sesji połączeniowych;
- Filtrowanie alarmów

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- Działanie w oparciu o wzorce ataków, możliwość definiowania wzorców przez użytkownika;
- Działanie w oparciu o analizę anomalii ruchu;
- Aktualizacja basy sygnatur winna odbywać się ręcznie i automatycznie;
- Wykrywanie i blokowanie technik i ataków (m.in. IP Spoofing, DDoS, SYN Attack, ICMP Flood, UDP Flood, Port Scan) i niebezpiecznych komponentów;
- Zarządzanie z poziomu aplikacji z interfejsem graficznym oraz przez linię komend (protokoły SSH oraz telnet);
- Powiadamianie o zdarzeniach do systemu prezentacji stanu sieci;
- Umożliwia wykrywanie ataków ukrytych w wielu następujących po sobie pakietach;
- Umożliwiać ograniczenie ruchu (ang. rate limiting);
- Umożliwiać inspekcję protokołów IP, ICMP, TCP, UDP;
- Urządzenie nie może posiadać ograniczeń na ilość jednocześnie pracujących użytkowników w sieci chronionej;
- Obsługa wirtualnych interfejsów VLAN;
- Inspekcja aplikacyjna protokołów TCP/UDP;
- Wykrywanie ataków w warstwie 2 modelu OSI;
- Urządzenie powinno być wyposażone w dedykowany port do zarządzania;
- Możliwość instalacji redundantnego zasilacza;
- Możliwość obsługi interfejsów 10Gbps
-

UWAGA: dopuszcza się połączenie w jednym urządzeniu funkcjonalności routera określonych w niniejszym rozdziale z funkcjonalnościami Firewall z IDS/IPS określonymi w rozdziale 4.4.3, w ten sposób, że jedno urządzenie pełnić będzie jednocześnie rolę routera i firewalla z IDS/IPS.
Dopuszcza się także rozwiązanie z osobnymi urządzeniami pełniącymi funkcje routera, firewalla oraz sondy z IDS/IPS. W takim wypadku komplet 3 takich urządzeń musi posiadać wszystkie funkcjonalności wymagane w rozdziale 4.4.2 oraz 4.4.3.

4.4.4 System zarządzania siecią

Pakiet lub dedukowane urządzenie realizujące poniższe funkcjonalności:

- dla urządzenia dedykowanego: możliwość instalacji w szafie 19”;
- dla urządzenia dedykowanego: zasilane prądem przemiennym 230V;
- obsługa urządzeń sieciowych różnych producentów
- analizowania informacji typu syslog;

- zbieranie statystyk z wykorzystaniem SNMP, RMON;
- posiadać narzędzia automatycznej identyfikacji urządzeń instalowanych w sieci;
- zarządzania oprogramowaniem zainstalowanym na urządzeniach;
- inwentaryzacja urządzeń, zarządzanie konfiguracjami i zmianami;
- zbieranie alarmów:
    - o stanie portów urządzenia,
    - o wykorzystaniu procesora,
    - o nieprawidłowej pracy wentylatorów,
    - o błędach pamięci,
    - o przekroczeniu zakresu temperatury pracy,
- monitorowanie zdarzeń, zbieranie informacji o alarmach;
- archiwizowanie informacji historycznych na zewnętrznym lub wewnętrznym zasobie dyskowym;
- powiadamianie użytkowników o alarmach;
- monitorowanie urządzeń warstwy 2 i 3 modelu ISO/OSI;
- tworzenie graficznych map sieć w warstwie 2;
- praca w trybie pozwalającym administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień);
- wsparcie dla protokołu RADIUS;
- dla urządzenia dedykowanego: możliwość instalacji redundantnego zasilacza;

System powinien udostępnić interfejs w technologii Web Services zgodny ze standardem SOA (ang. Service Oriented Architecture), pozwalający na integrację poprzez szynę integracyjną z systemem paszportyzacji oraz systemami klasy Fault Management i Trouble Ticketing (w terminologii eTOM/TMForum).

4.4.4.1 System prezentacji stanu sieci

Wymagania dotyczące systemu:

- system musi komunikować się z panelami LCD, (które stanowić będą rodzaj ściany graficznej prezentującej stan sieci w danym momencie);
- w formie dedykowanego urządzenia lub pakiety programowego działającego w środowisku wirtualnym;
- sygnalizacji stanów funkcjonowania wszystkich urządzeń;
- sygnalizacji stanów funkcjonowania wszystkich serwisów (np. DNS, DHCP, SYSLOG, RADIUS, LDAP, BGP) ;
- sygnalizacji stanów połączeń wewnętrznych;

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- sygnalizacji stanów połączeń do operatorów zewnętrznych;
- sygnalizacji stanów wykorzystania zasobów serwerów Linux/Windows: CPU, RAM, HDD;
- sygnalizacji stanów utylizacji procesorów i pamięci w urządzeniach;
- prezentacja kluczowych informacji pochodzących z systemu analizy komunikatów sieciowych oraz systemu zarządzania siecią;
- dla urządzenia dedykowanego: obsługa interfejsów 1GE;
- dla urządzenia dedykowanego: możliwość instalacji w szafie 19”.

4.5 Zawartość dokumentacji projektowej dla Centrum Zarządzania Siecią - wymagania minimalne

W ramach dokumentacji opisowej należy posługiwać się ujednoliconą stroną opisową tabela dokumentacji projektu technicznego przedstawiona jak poniżej.

Stadium:	**(np. PROJEKT WYKONAWCZY)**	
Temat opracowania:	**…**	
Obiekt:	**…**	
Branża:	**…**	
Inwestor:	…	
Jednostka projektowa:	**…**	
	Nr archiwalny:	**…**
	Tom:	**… / …**
	Egzemplarz:	**… / …**

Funkcja	**Imię i Nazwisko**	**Uprawnienia/ specjalność**	**Numer uprawnień**	**Data**	**Podpis**
Projektował :					
Opracował:					
Opracował					

Miejscowość - Data

Rysunek 5. Wzór strony opisowej - tabela dokumentacji projektu technicznego

Jednocześnie należy stosować stopkę dokumentu (co najmniej w stronie opisowej jak i części opisowej projektu) zgodnie z wzorem przedstawionym na rysunku:

Rysunek 6. Wzór stopki dokumentu projektowego

Oświadczenie projektanta

O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust. 4 Ustawy Prawo budowlane z dnia 7 lipca 1994 (Dz. U. 2006.156.1118 z późniejszymi zmianami)

oświadczam jako projektant/sprawdzający

że projekt:

„ … ”

został sporządzony zgodnie z obowiązującymi przepisami, normami i zasadami wiedzy technicznej oraz że jest on kompletny z punktu widzenia celu jakiemu ma służyć. Oświadczam zarazem, że zawartość projektu spełnia wymagania Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 (Dz. U. 2004.202.2072) w sprawie szczegółowego zakresu i formy dokumentacji projektowej.

.....

(data, podpis)

Rysunek 7. Wzór oświadczenia projektanta

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

4.5.1 Zawartość dokumentacji projektowej

1. Część ogólna

1.1. Przedmiot opracowania

Należy określić przedmiot opracowania (np. „Przedmiotem opracowania jest projekt wykonawczy Centrum Zarządzania Siecią (CZS) w ramach Dolnośląskiej Sieci Szkieletowej (DSS)”).

Należy zamieścić informację o szerszym kontekście opracowania (np. jeśli opracowanie wchodzi w skład wielobranżowej dokumentacji projektowej należy podać nazwę przedsięwzięcia i wymienić już opracowane projekty budowlane i wykonawcze, specyfikacje techniczne wykonania i odbioru, instrukcje BIOZ lub przedmiary prac powiązane z opracowaniem).

1.2. Podstawa opracowania projektu

Należy określić podstawę wykonania opracowania oraz wykorzystane źródła danych.

1.3. Opis ogólny inwestycji

1.3.1. Położenie geograficzne

Należy zdefiniować lokalizację/lokalizacje obiektu/obiektów.

1.3.2. Zakres rzeczowy

Należy określić główne wskaźniki zakresu rzeczowego.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

2. Słownik, terminologia i symbolika

2.1. Słownik i terminologia

Należy zdefiniować pojęcia i terminy używane w opracowaniu, które nie są powszechnie stosowane

2.2. Symbolika

Należy zdefiniować symbole stosowane na rysunkach

2.3. Oznaczenia i numeracja

Należy zdefiniować stosowane oznaczenia i zasady numeracji elementów.
Np.:

CZS	-	*Centrum Zarządzania Siecią*
ZCZS	-	*Zapasowe Centrum Zarządzania Siecią*

3. Bazowe dokumenty normatywne i dokumenty odniesienia

3.1. Wykaz norm i dokumentów odniesienia

Należy wymienić wszystkie dokumenty odniesienia i normy bazowe cytowane w opracowaniu.

4. Charakterystyka techniczna projektowanego obiektu

4.1. Szczegółowe rozwiązania i obliczenia projektowe.
4.2. Szczegółowe wytyczne realizacyjne.
4.3. Szczegółowe wytyczne w zakresie wdrożenia.
4.4. Szczegółowe wytyczne w zakresie szkoleń i eksploatacji.
4.5. Szczegółowe wytyczne w zakresie procedur i kolejności „uruchamiania i zamykania” poszczególnych składników

5. Tabele

5.1. Spis obiektów objętych projektem

Wymienić obiekty objęte opracowaniem i podać ich lokalizację.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

L.p.	Oznaczenie	Obiekt	Adres

5.2. Zestawienie typów i liczby kart/ urządzeń / zespołów urządzeń

Wymienić elementy dostaw materiałów i urządzeń, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

Lp.	Nazwa urządzenia	Zakres/Liczba	Opis Wymagań
…	…		

5.3. Zestawienie typów i systemów monitoringu/zarządzania wraz ze wskazaniem urządzeń monitorowanych/zarządzanych

Lp.	Nazwa systemu monitoringu/zarządzania	Urządzenia monotorowane/zarządzane	Lokalizacja
…	…		

5.4. Zestawienie monitorowanych urządzeń

L.p.	Serwer	Producent	Monitowanie systemu plików	Monitorowanie obciążenia procesora	Monitorowanie procesów
…					

5.5. Zestawienie monitorowanych zdarzeń/procesów dla poszczególnych urządzeń

L.p.	Dostawca	Serwer	Zdarzenia/monitorowane elementy
…			

5.6. Zestawienie prac podstawowych

Wymienić prace, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Lp.	Opis czynności	Zakres/Liczba	Wymagania/Uwagi
	…	…	…

6. Spis rysunków

Należy zamieścić spis rysunków wykorzystanych w opracowaniu. Np.:

Rysunek 1. Schemat ogólny systemu zarządzania

Rysunek 2. Rzut pomieszczenia/pomieszczeń wraz z oznaczeniem projektowanej lokalizacji urządzeń systemu zarządzania

Rysunek 3. Lokalizacja urządzeń systemu w szafie … w węźle …

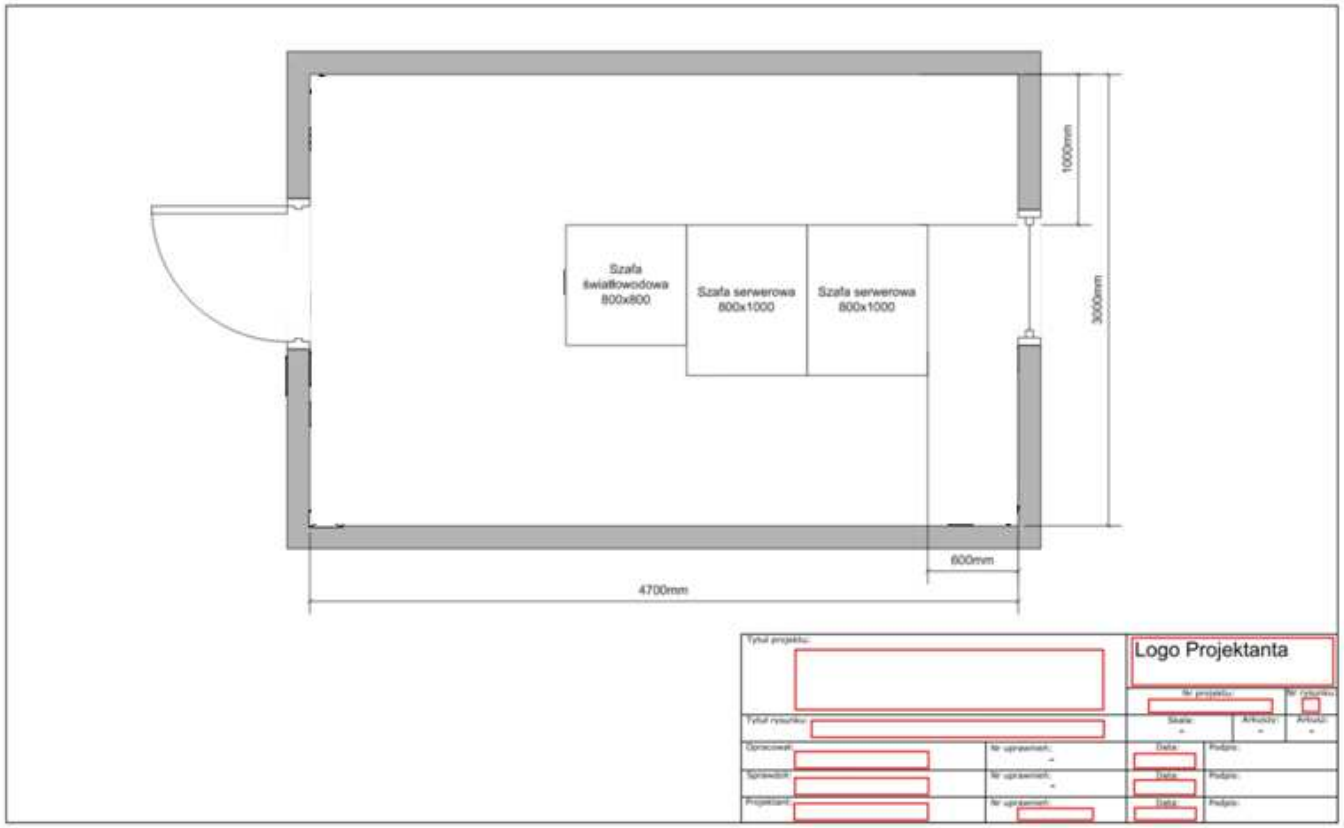
Rysunek 4. Lokalizacja urządzeń systemu w szafie … w węźle …

Rysunek 5. ….

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

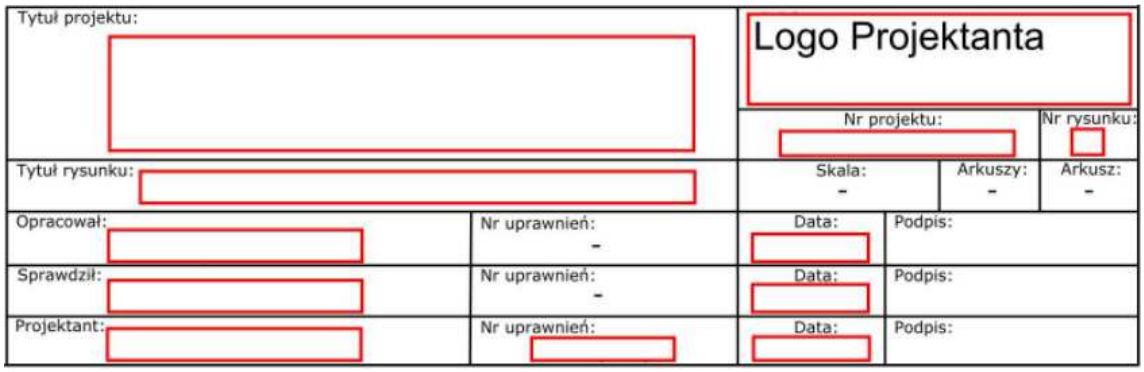
4.5.2 Wzór rysunku – dokumentacja projektowa dla Centrum Zarządzania Siecią



Rysunek 8. Wzór graficznej prezentacji posadowienia infrastruktury Centrum Zarządzania Siecią

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego



Rysunek 9. Tabela opisu rysunku (zgodnie z wzorem rysunku) umieszczona w prawym dolnym rogu

5 Zintegrowany System Nadzoru

5.1 Wymagania ogólne dla wykonania dokumentacji projektowej Zintegrowanego Systemu Nadzoru (ZSN)

Zawartość minimalną i układ opracowania projektowego zdefiniowano w punkcie 5.2 Wzór tabeli opisującej rysunki zdefiniowano w punkcie 5.3.

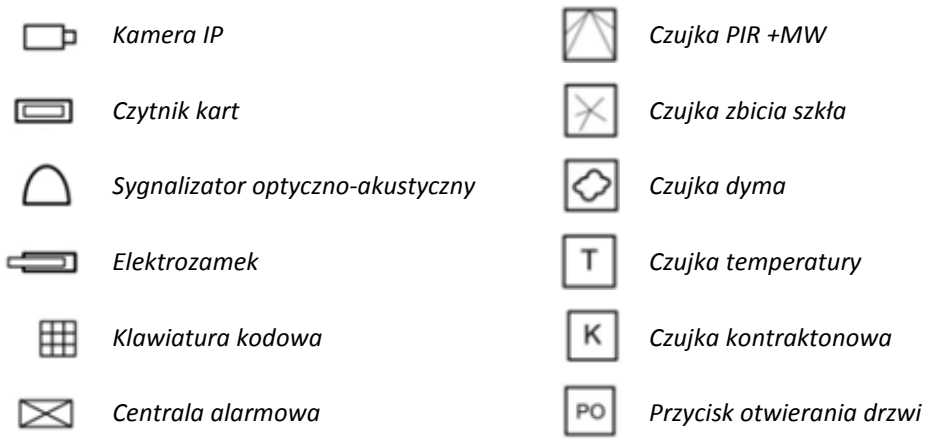
5.1.1 Słownik, terminologia i symbolika

5.1.1.1 Słownik i terminologia

W opracowaniach projektowych należy stosować terminologię zdefiniowaną w normie PN-E-08390-1:1996 Systemy alarmowe.

5.1.1.2 Symbolika

W opracowaniach projektowych należy stosować następującą symbolikę graficzną przedstawioną na rysunku poniżej.



Rysunek 10. Symbolika do zastosowania w obszarze Zintegrowanego Systemu Nadzoru

Do opisu poszczególnych lokalizacji należy przyjąć następujące oznaczenia literowe:

- DSS - Dolnośląska Sieć Szkieletowa
- WS_x - Węzeł szkieletowy o numerze „x”
- WD_x - Węzeł dystrybucyjny o numerze „x”
- CZS - Centrum Zarządzania Siecią
- ZCZS - Zapasowe Centrum Zarządzania Siecią

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

5.2 Wytyczne dla przygotowania dokumentacji projektowej Zintegrowanego Systemu Nadzoru (ZSN)

5.2.1 Wymagania technologiczne – ogólne

Tabela 10. Wymagania ogólne na zintegrowany system nadzoru

L.p.	Opis wymagania
1.	Zaprojektowany system nadzoru bezpieczeństwa fizycznego infrastruktury musi integrować następujące podsystemy: - system kontroli dostępu, - system sygnalizacji włamania, - system monitoringu wizyjnego, - system sygnalizacji i gaszenia pożaru.
2.	Komunikację w systemie należy oprzeć na technologii IP, tak, aby możliwe było zarządzanie i nadzór nad odległym elementem systemu z dowolnego miejsca, poprzez przeglądarkę (min. Internet Explorer lub Firefox). W sieci IP pracować będzie serwer z aplikacją zarządzającą, centralki alarmowe oraz sterowniki sieciowe.
3.	Komunikacja między aplikacją zarządzającą systemem bezpieczeństwa fizycznego, a stacją roboczą (stanowisko wizualizacji, punkt zdalnego zarządzania) będzie odbywała się z wykorzystaniem protokółu SSL.
4.	Komunikacja między elementami systemu (serwerem, sterownikami sieciowymi) będzie odbywała się w wydzielonym VLAN-ie.
5.	Aplikacja zarządzająca systemem będzie znajdowała się na serwerze i udostępniała interfejs w postaci strony HTML.
6.	Funkcjonalność systemu winna umożliwiać pracę poprzez przeglądarkę internetową kilku użytkownikom jednocześnie.
7.	Pakiet wizualizacyjny systemu musi zapewnić wizualizację on-line stanu elementów systemu oraz przegląd zdarzeń z monitoringu wizyjnego w oknie przeglądarki.
8.	W systemie wymagany jest moduł zarządzania alarmami, który pozwali na przygotowanie scenariusza zdarzeń dla operatora i będzie potrafił inteligentnie kierować raporty o zdarzeniach do odpowiednich użytkowników, dla zdefiniowanych wcześniej zdarzeń alarmowych.
9.	Funkcjonalność system musi umożliwiać dokonywanie wzajemnych powiązań między zdarzeniami napływającymi z podsystemów: kontroli dostępu, sygnalizacji włamania, monitoringu wizyjnego (opartego o kamery IP) oraz sygnalizacji i gaszenia pożaru.
10.	Funkcjonalność systemu musi zapewnić możliwość jego programowej konfiguracji, wprowadzania podziału logicznego na strefy zagrożeń, umożliwiać przypisanie kamer do stref oraz wspierać przeszukiwanie i analizę zdarzeń poprzez notowanie transakcji pomiędzy podsystemami.
11.	Funkcjonalność systemu musi zapewnić możliwość odzwierciedlenia na stacji roboczej stanu osobowego na dowolnym chronionym obiekcie w zadanej chwili.
12.	Funkcjonalność systemu powinna obejmować dokonywanie wydruków raportów zawierających scenariusze zdarzeń i szczegółowe informacje nt. zdarzenia oraz liczby osób

L.p.	Opis wymagania
	na kontrolowanym obiekcie. Nadto wymagana jest możliwość archiwizowania lub przesyłania raportów w formie elektronicznej oraz automatyczne generowanie raportów.
13.	Wymagania minimalne dla oprogramowania do zarządzania i wizualizacji: 1. zarządzanie uprawnieniami i personalizacja stanowiska pracy na poziomie profilu użytkownika, 2. przypisanie w bazie danych do użytkownika co najmniej następujących danych: - imienia i nazwiska - numeru karty dostępowej - sklasyfikowania do grupy użytkowników – np. administrator, serwisant, gość, - telefonu - adresu - innych notatek 3. formułowanie i uruchamianie procedur programowych (język skryptowy) wyzwalających zaplanowane reakcje systemu w zależności od stanu portów przyłączonych sterowników. 4. przechowywanie informacji o minimum 5 000 ostatnich zdarzeń. Oprócz tego powinna istnieć możliwość regularnego archiwizowania bazy danych, 5. raportowanie poprzez wysyłanie maili oraz zapisywanie plików PDF, XML i CSV. System powinien umożliwiać tworzenie własnych raportów, 6. dokonywanie powiązań między zdarzeniami w podsystemach, umożliwiające np. w trakcie przeglądania zdarzenia z systemu kontroli dostępu odtworzenie filmu z powiązanej z czytnikiem kamery, 7. tworzenie połączeń z centralkami oraz sterownikami za pomocą TCP/IP oraz kodowanie tych połączeń np. za pomocą AES256, 8. możliwość korzystanie z pinów 4 i 6-cio cyfrowych, 9. dystrybucja alarmów, pozwalająca na przekazywanie różnych zdarzeń do różnych użytkowników/operatorów, 10. interaktywne mapy/ikony w pakiecie wizualizacyjnym, 11. kontrola dostępu powinna obsługiwać funkcje: anti-passback i rejestrację obecności gości, 12. integracja z zewnętrznymi systemami poprzez sieć IP oraz opcje importu/exportu XML lub ODBC/JDBC, 13. wsparcie dla kamer PTZ (Pan Tilt Zoom), 14. możliwość pracy przynajmniej 5-ciu użytkowników jednocześnie, 15. obsługa co najmniej 1000 kart/użytkowników, 16. obsługa gości oraz personalizację kart, 17. współpraca z oprogramowaniem monitoringu wizyjnego, 18. polska wersja oprogramowania, 19. oprogramowanie powinno być zainstalowanie na serwerze platformy zarządzania i wizualizacji.
14.	Wymagania minimalne dla oprogramowania do zarządzania monitoringiem wizyjnym: 1. wyświetlanie obrazów w formatach: JPEG, JPEG2000, MPEG4, H.264, we wszystkich

L.p.	Opis wymagania
	trybach pracy kamer zdefiniowanych dla podsystemu, 2. możliwość wyświetlania obrazów z kamer na żywo, obrazów z materiału zarejestrowanego, wielowarstwowych map, stron HTML, 3. możliwość swobodnego wyboru co ma być wyświetlane na wybranym polu: widok z kamery, mapa, strona HTML, 4. wyszukiwanie zarejestrowanego materiału wideo w oparciu o wielorakie kryteria np. zdarzenia, indeksy, oś czasu, itp., 5. funkcja dołączania programu klienckiego do oglądania nagrań eksportowanych na zewnętrzne nośniki np: CD lub DVD, 6. cyfrowy zoom w podglądzie na żywo oraz przy odtwarzaniu nagrań z archiwum, 7. kontrola bieżącego stanu i alarmów z serwerów rejestrujących, kamer sieciowych, urządzeń wejść/wyjść, innych urządzeń zewnętrznych (np. czujek PIR), podsystemu kontroli dostępu, 8. wielopoziomowe, hierarchiczne, przejrzyste mapy, 9. możliwość wyboru kamery z poziomu mapy terenu, 10. możliwość przekazania informacji z tego samego alarmu wielu operatorom systemu, 11. pełne zarządzanie opcjami alarmów (przejmowanie, zatwierdzanie), 12. sterowanie kamerami obrotowymi za pomocą myszy komputerowej lub sterownika podłączonego do stacji monitoringu za pomocą złącza USB, 13. system powinien oferować wsparcie dla różnych dostawców kamer CCTV IP, 14. polska wersja oprogramowania, 15. oprogramowanie powinno być zainstalowane na serwerze platformy monitoringu wizyjnego.
15.	Wymagania minimalne dla serwera platformy zarządzania i wizualizacji: 1. obudowa dedykowana do zamontowania w szafie Rack 19" z zestawem szyn do mocowania w szafie, 2. minimum dwa redundantne zasilacze 230V AC, 3. parametry procesora/procesorów i wielkość pamięci powinny być tak dobrane aby zapewnić odpowiednią wydajność dla oprogramowania do zarządzania kontrolą dostępu, sygnalizacją włamania i pożaru oraz integracji z systemem monitoringu wizyjnego; parametry minimalne: pamięć - 4GB RAM, procesor - Xeon 3.0 GHz, 4. co najmniej 2 wewnętrzne dyski twarde 500 GB, 10kRPM, , 5. co najmniej 2 porty sieciowe Gigabit Ethernet, RJ-45, 6. system operacyjny wymagany przez oprogramowanie do zarządzania kontrolą dostępu i sygnalizacją włamania.
16.	Wymagania minimalne dla serwera platformy monitoringu wizyjnego: 1. obudowa dedykowana do zamontowania w szafie Rack 19" z zestawem szyn do mocowania w szafie, 2. minimum dwa redundantne zasilacze 230V AC, 3. parametry procesora/procesorów i wielkość pamięci powinny być tak dobrane aby zapewnić odpowiednią wydajność dla oprogramowania do zarządzania monitoringiem wizyjnym dla projektowanego zespołu kamer IP, pracujących w trybie 1280 x 960 @ 15

L.p.	Opis wymagania
	klatek/s z kompresją MJPEG, parametry minimalne: pamięć - 4GB RAM, procesor - 3,0 GHz, 4. co najmniej 2 wewnętrzne dyski twarde, o pojemności nie mniejszej niż 2TB, możliwość zainstalowania 12 dysków w wewnętrznych zatokach serwera, 5. pojemność dysków powinna pozwalać na przechowywanie filmów z kamer z ostatnich 4 tygodni, 6. kontroler macierzowy SATA, umożliwiający konfigurację dysków w macierzach RAID 0/1/5, 7. możliwość zatrzymania dysku w przypadku wysłania do naprawy komputera – zabezpieczenie przed wypłynięciem poufnych danych, 8. system operacyjny wymagany przez oprogramowanie do zarządzania monitoringiem wizyjnym.
17.	Platformę zarządzania systemem (rozumianą jako zespół oprogramowania służącego do zarządzania, wizualizacji i zarządzania monitoringiem wizyjnym) powinna cechować prostota i ergonomia obsługi.
18.	Jakość systemu powinna być potwierdzona: • świadectwem kwalifikacyjnym Klasy ”S” (wg PN-93/E-08390-14:1993), • spełnieniem norm EN50131, EN50133, EN50136.

5.2.2 Wymagania technologiczne - podsystem kontroli dostępu

Tabela 11. Wymagania na podsystem kontroli dostępu

L.p.	Opis wymagania
1.	Podsystem kontroli dostępu powinien umożliwić: pracę z wykorzystaniem kart zbliżeniowych, określenie uprawnień pracowników w dostępie do wybranych pomieszczeń, określenie przedziałów czasowe (wybrane godziny) dostępu dla pracowników, przypisanie karty dostępowej do konkretnej osoby, personalizację kart dostępowych, powinny one posiadać możliwość nadruku imienia, nazwiska a także zdjęcia pracownika, pełną rejestracja zdarzeń, kontrolę czasu pracy, opcjonalnie (do decyzji Operatora Infrastruktury)- funkcję wymuszenia kolejności wejścia / wyjścia ("antipassback", zapobiega ona używaniu tej samej karty), funkcje alarmowe (możliwość dołączenia dowolnych czujek), graficzne zobrazowanie obiektów chronionych za sprawą map z naniesionymi aktywnymi ikonami, zapewnienie czasowego dostępu, rejestrację obecności pracowników, rejestrację obecności gości.
2.	Baza danych o użytkownikach oraz aplikacja zarządzająca podsystemem powinny być umieszczone na serwerze sieciowym (zlokalizowanym w CZS, ZCZS lub innej wskazanej lokalizacji). Serwer ten powinien również zarządzać wszystkimi sterownikami systemu

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

L.p.	Opis wymagania
	kontroli dostępu oraz zbierać sygnały z centralek sygnalizacji włamania i sygnalizacji pożaru.
3.	Niezbędną funkcjonalnością systemu musi być (po jego poprawnym skonfigurowaniu) możliwość pracy bez dostępu do serwera np. w przypadku awarii DSS lub awarii zasilania.
4.	Sygnały z całego systemu powinny być obsługiwane na stanowisku operatora DSS.
5.	Uzupełnieniem sytemu kontroli dostępu musi być integracja z monitoringiem wizyjnym. Oprócz podglądu obrazu z kamer w czasie zdarzenia musi być możliwa szybka weryfikacja zdarzeń z historii. Przeglądając aktywność użytkownika (posiadacza karty dostępowej) w systemie kontroli dostępu w określonym przedziale czasu, operator powinien mieć możliwość odwołania się do krótkiego nagrania z pobliskiej kamery.
6.	Sterowniki (kontrolery) sieciowe muszą mieć możliwość przypisania adresu IP, zdolność do obsługi zamków i czytników oraz pośredniczenia w komunikacji między tymi urządzeniami a serwerem.
7.	Zasilanie kontrolera sieciowego powinno stanowić jednocześnie zasilanie przyłączonych do niego czytników i zamków. W celu zapewnienia działania kontrolerów w czasie zaniku napięcia muszą być one wyposażone w akumulator (baterię). Zamontowane sterowniki sieciowe powinny umożliwiać kontrolowanie stanu zasilania. W momencie gdy podzespoły przechodzą w stan zasilania awaryjnego (bateryjnego) musi to być widoczne i zgłoszone w systemie – na stanowisku wizualizacji.
8.	Dostęp do pomieszczeń/szaf chronionych będzie możliwy po odczytaniu przez czytnik numeru karty zbliżeniowej (przesunięcie karty w pobliżu czytnika) i zweryfikowaniu przez system kontroli dostępu jako uprawnionej do otwarcia.
9.	Wymagania minimalne dla kontrolera sieciowego: obsługa min. 2 czytników oraz 12 programowalnych wej./wyj. NO, zgodność ze standardem ISO 14443 type A , pamięć 32 MB RAM, 32MB Flash, przechowywanie co najmniej 4,000 transakcji, wyposażenie w interfejsy: ethernet port RJ45 do połączenia przez sieć IP, port komunikacyjny RS232/RS485 lub Ethernet, port diagnostyczny RS232/RS485 lub Ethernet, napięcie zasilania 24 VDC (powinien zostać dostarczony zasilacz) lub PoE, akumulator zasilania awaryjnego - 12V min.7Ah, opcjonalna obudowa ze stykami antysabotażowymi, kodowanie połączenia od sterownika do serwera np. za pomocą AES-256, Pobór mocy – do 3W.
10.	Wymagania rekomendowane dla czytnika kontroli dostępu: Powinien pracować w standardzie ISO 14443 type A , Powinien działać z dostarczonym kontrolerem sieciowym
11.	Wymagania rekomendowane dla klawiatury kodowej: Klawiatura dotykowa, bez wypukłych elementów, brak przycisków, Komunikacja RS485,

L.p.	Opis wymagania
	Wyświetlacz LCD 2x18 znaków.
12.	Wymagania minimalne dla zamków elektromagnetycznych: Typ 1 (przeznaczony do montażu w drzwiach szafy teleinformatycznej) -otwarcie zamka następuje po podaniu napięcia, po zaniku napięcia pozostaje zamknięty. Typ 2 (przeznaczony do montażu w drzwiach wejściowych) - otwarcie zamka następuje po zaniku napięcia, gdy napięcie jest podawane zamek pozostaje zamknięty; minimalna wartość siły niezbędnej do przełamania blokady: 3000N

5.2.3 Wymagania technologiczne - podsystem sygnalizacji włamania

Tabela 12. Wymagania na podsystem sygnalizacji włamania

L.p.	Opis wymagania
1.	Centralnym elementem podsystemu są centralki alarmowe (CA). Każda centralka zarządza działaniem podsystemu w obrębie chronionego obiektu, przetwarza dostępne informacje z dołączonych do niej czujników oraz podejmuje decyzje o wyzwoleniu alarmu. Dopuszcza się realizację funkcji CA przez urządzenie pełniące jednocześnie funkcję centrali systemu alarmu pożarowego (SAP).
2.	Centralki CA powinny spełniać wymagania zawarte w normie PN-E-08290-3:1998, w której określono wymagania, metody badań oraz funkcjonalność CA.
3.	Każda CA powinna być wyposażona w port Ethernet RJ-45 i mieć możliwość przypisania adresu IP.
4.	Podstawowe i awaryjne zasilanie centralki, które powinno spełniać wymagania normy PN-93/E-08390.12.
5.	Wykrywanie naruszenia strefy chronionej powinno być zapewnione przez linie dozorowe z pasywnymi czujnikami podczerwieni reagującymi na ruch (PIR), czujkami dualnymi PIR+mikrofala lub czujkami magnetycznymi (kontaktrony - umieszczane na oknach, drzwiach). Urządzenia te powinny spełniać wymagania właściwych norm bazowych.
6.	CA musi zapewniać możliwość dołączenia czujek zbicia szkła (np. czujek w których wykorzystano mikroprocesorową technologię analizy dźwięku (SAT) do rozpoznawania określonych częstotliwości towarzyszących tłuczeniu szkła).
7.	Naruszenie strefy chronionej musi powodować uruchomienie przyłączonych do centrali alarmowej sygnalizatorów optycznych i akustycznych, a także wysłanie informacji do systemu wizualizacji.
8.	Funkcjonalność podsystemu musi zapewnić możliwość uzbrajania/rozbrajania przez kart dostępu wykorzystywanych w podsystemie kontroli dostępu lub przez wpisanie na klawiaturze specjalnego kodu ustalonego przez użytkownika.
9.	Oprócz sygnalizowania o ewentualnych zagrożeniach kradzieżą czy włamaniem, podsystem winien posiadać także możliwość sygnalizacji braku uzbrojenia systemu alarmowego oraz prezentowania na stacji roboczej operatora informacji dotyczącej identyfikacji ostatniego użytkownika.
10	CA musi umożliwiać kontrolowanie stanu zasilania. W momencie gdy podzespoły przejdą

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

L.p.	Opis wymagania
	w stan zasilania awaryjnego (akumulatorowego) będzie to zgłoszone i widoczne w systemie – na stanowisku wizualizacji.
11	Wymagania minimalne dla centralki alarmowej: Obsługa min. 8 linii, Obsługa min. 8 manipulatorów (klawiatur kodowych), Możliwość wysterowania 2 wyjść, Obsługa PIN-ów 4 lub 6 cyfrowych, możliwość korzystania z 256 PIN kodów, Komunikacja IP, port Ethernet, Opcjonalnie- obsługa szyny M-Bus, Zasilanie 230V AC, w przypadku innego należy dostarczyć zasilacz, Akumulator podtrzymania - min. 7 Ah.

5.2.4 Wymagania technologiczne - podsystem monitoringu wizyjnego

Tabela 13. Wymagania na podsystem monitoringu wizyjnego

L.p.	Opis wymagania
1.	Podsystem powinien składać się z kamer IP zainstalowanych w monitorowanych (chronionych) obiektach.
2.	Zarządzanie kamerami powinno odbywać się poprzez oprogramowanie systemu wizualizacji za pomocą przeglądarki lub za pomocą specjalizowanej aplikacji do zarządzania podsystemem monitoringu wizyjnego.
3.	Podsystem monitoringu wizyjnego winien zapewnić możliwość: powiązania zdarzeń między podsystemami (kontroli dostępu, sygnalizacji włamania, sygnalizacji pożaru i monitoring wizyjnego), podglądu wizji z zadanej kamery w oknie przeglądarki, łatwego wyszukiwania zdarzeń, zapisywania stop-klatki w momencie wystąpienia zdefiniowanego wcześniej zdarzenia, procentowego wykrywania ruchu (Video Motion Detection), archiwizacji nagrań według profili zdefiniowanych przez użytkownika np. zapis ciągły tylko w zdefiniowanym okresie, w pozostałym okresie zapis z detekcji ruchu, funkcji antysabotażowej, np. przy wymuszonym obrocie kamery system wygeneruje alarm, wyświetlania obrazów z kamer na żywo, obrazów z materiału zarejestrowanego, wyboru widoku z wielowarstwowych map - podgląd będzie dowolnie modyfikowany przez użytkownika poprzez zastosowanie wirtualnej krosownicy, uruchomienia alarmu lub podglądu z odpowiedniej kamery w przypadku wystąpienia określonego zdarzenia np. otwarciu drzwi do serwerowni.
4.	Wymagania minimalne dla kamer IP: Przetwornik klasy CCD 1/3” Kompatybilność z dostarczonym serwerem Obiektyw 3.7~8 mm /F1.4~2.8

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

	Kąt widzenia 77 ° ~ 23° Mechaniczny filtr podczerwieni Kompresja Motion JPEG lub MPEG-4 Rozdzielczość : 1280 x 960 @ 15 fps lub mniejsza; Czułość kamer 0.2 lux w kolorze w trybie bW 0.03 (f1.2) Wejście/wyjście AUDIO – Full duplex (JACK) Protokoły TCP/IP; UDP/IP; HTTP; SMTP; DNS; DHCP; NTP; ARP; ICMP; DDNS; FTPc; FTPs Pasmo : max 8mbs Zasilanie DC 12V; AC24V; (4.2W), POE (802.3af), zasilacz wraz z adapterem PoE dostarczony wraz z kamerami, Kamera w obudowie metalowej.

5.2.5 Wymagania technologiczne - podsystem sygnalizacji i gaszenia pożaru

Tabela 14. Wymagania na podsystem sygnalizacji i gaszenia pożaru

L.p.	Opis wymagania
1.	Podsystem sygnalizacji pożarowej powinien spełniać wymagania zawarte w normie PN-EN 54-1:1998, w której określono części składowe systemów wykrywania pożarów i alarmowania oraz opisano wzajemne powiązania pomiędzy tymi częściami.
2.	Centralnymi elementami podsystemu są centralki systemu alarmu pożarowego (SAP), które pełnią rolę pełni rolę nadrzędną w stosunku do innych instalacji i urządzeń przeciwpożarowych, w tym np. instalacji oddymiania. Każda centralka zarządza działaniem podsystemu w obrębie chronionego obiektu, przetwarza dostępne informacje z dołączonych do niej czujników oraz podejmuje decyzje o wyzwoleniu alarmu pożarowego. Dopuszcza się realizację funkcji centralki SAP przez urządzenie pełniące jednocześnie funkcję centrali podsystemu sygnalizacji włamania (CA).
3.	Centralki SAP powinny spełniać wymagania zawarte w normie PN-EN 54-2:2002, w której określono wymagania, metody badań oraz funkcjonalność central SAP stosowanych w systemach wykrywania pożaru i alarmowania.
4.	Każda centralka SAP powinna być wyposażona w port Ethernet RJ-45 i mieć możliwość przypisania adresu IP.
5.	Podstawowe i awaryjne zasilanie centralki, które powinno spełniać wymagania normy PN-EN 54-4:2001.
6.	Wykrywanie dymu i skoku temperatury spowodowanego ogniem powinno być zapewnione przez linie dozorowe z czujkami optycznymi dymu, wykrywającymi zarówno dym jak i gaz gaśniczy oraz czujkami termicznymi. Urządzenia te powinny spełniać wymagania przytoczonych, właściwych norm bazowych.
7.	Podsystem powinien zapewnić możliwość dołączenia aerozolowych generatorów gaśniczych (typu FirePro lub inne o nie gorszych właściwościach) o pojemności środka gaśniczego dostosowanej do wielkości chronionego pomieszczenia. Tego typu urządzenia

	powinny posiadać atest wydany przez Centrum Naukowo Badawcze Ochrony Przeciwpożarowej (CNBOP) dotyczący stałych urządzeń gaśniczych w postaci aerozolowych generatorów gaśniczych oraz posiadać atest wydany przez Państwowy Zakład Higieny (PZH). Środek gaśniczy powinien być bezpieczny dla ludzi oraz nie powinien powodować trwałych uszkodzeń urządzeń elektronicznych.
8.	Podsystem powinien być wyposażony w sygnalizatory akustyczne (syrena) i/lub optyczne (optyczno-akustyczne) służące do alarmowania sygnałem dźwiękowym i/lub świetlnie po wyzwoleniu alarmu przez centralkę. Sygnalizatory tego typu powinny spełniać wymagania przytoczonych, właściwych norm bazowych.
9.	Alarmy pożarowe z centralek umieszczonych w węzłach powinny być transmitowane do platformy integrującej podsystemy z wykorzystaniem możliwie niezawodnych systemów transmisji. Urządzenia do transmisji sygnałów alarmowych powinny spełniać wymagania normy PN-EN 54-21:2006, w której podane zostały wymagania, metody badań i kryteria według których oceniana jest efektywność i niezawodność sprzętu przemysłowego służącego do przesyłania alarmu pożarowego i/lub sygnału ostrzeżenia o usterce.
10.	Systemy i urządzenia sygnalizacji i gaszenia pożaru powinny spełniać wymagania kompatybilności elektromagnetycznej z zakresu odporności urządzeń i systemów włamaniowych według normy PN-EN 50130-4:2002 oraz zostać poddane próbom środowiskowym według normy PN-EN 50130-5:2002.

5.2.6 Wymagania w zakresie wykonania i odbioru prac systemu

Tabela 15. Wymagania w zakresie wykonania i odbioru prac systemu ZSN

L.p.	Opis wymagania
1.	Projektant winien określić w dokumentacji projektowej kwalifikacje i uprawnienia jakie posiadać powinni instalatorzy poszczególnych części systemu.
2.	Projektant winien określić oznaczenia i spójną numerację wszystkich elementów systemu oraz przypisać nadane oznaczenia i numery do wszystkich symboli elementów na rysunkach. Przypisanie elementu do jego lokalizacji geograficznej musi być czytelne i precyzyjne.
3.	Projektant winien precyzyjnie opisać procedurę instalacji systemu oraz wskazać właściwe narzędzia i oprzyrządowanie. W szczególności opisana procedura musi zapewnić ułożenie przewodów linii dozorowych bez jakiegokolwiek łączenia i sztukowania jako nieprzerwanych odcinków oraz pewne i niezawodne łączenie przewodów na zaciskach elementów systemu.
4.	Po zakończeniu prac montażowych Wykonawca powinien oznaczyć wszystkie elementy składowe systemu w sposób opisany w projekcie oraz wykonać co najmniej następujące sprawdzenia i pomiary instalacji: kontrolę jakości i topologicznej poprawności wykonanych połączeń, sprawdzenie instalacji pod kątem przerw i zwarć, pomiar napięć zasilających wszystkie elementy systemu, sprawdzenie poprawności działania zastosowanych urządzeń, sprawdzenie komunikacji elementów systemu z wykorzystaniem protokołu IP.
5.	Dane z sprawdzeń i pomiarów należy zapisać w protokole powykonawczym i załączyć do

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

	protokołu odbioru instalacji.
6.	Wykonawca instalacji powinien (jeżeli nie zapewnia tego producent systemu) opracować instrukcję jej obsługi technicznej i konserwacji.
7.	Wykonawca winien przekazać użytkownikowi dokumentację powykonawczą (dokumentację projektową z naniesionymi powykonawczo zmianami) oraz wszelkie dokumenty dotyczące montowanych urządzeń dostarczane wraz z nimi przez ich producentów (dokumentacje techniczno-ruchowe, instrukcje montażu, obsługi i konserwacji, itp.). Niezależnie winien dostarczyć książkę eksploatacji systemu, w której będą odnotowywane wszystkie zdarzenia związane z eksploatacją systemu.

5.2.7 Wymagania w zakresie wdrożenia i szkoleń

Tabela 16. Wymagania w zakresie wdrożenia i szkoleń systemu ZSN

Nr	Opis wymagania
1.	Po wykonaniu instalacji i dokonaniu jej odbioru technicznego Wykonawca winien dokonać właściwego zaprogramowania, a dalej uruchomienia i przekazania całego systemu do eksploatacji. W szczególności winien zaprogramować tryb pracy poszczególnych centralek i sterowników sieciowych i przydzielić właściwe uprawnienia użytkownikom.
2.	Programowanie systemu należy wykonać w oparciu o instrukcję obsługi (dokumentację fabryczną) producenta systemu, uwzględniając wymogi użytkownika oraz obowiązujące przepisy i normy. W miarę możliwości programowanie przeprowadzić przy udziale przedstawicieli użytkownika odpowiedzialnych w przyszłości za nadzór systemu.
3.	Po zakończeniu programowania Wykonawca winien uruchomić system i sprawdzić poprawność jego działania w zakresie określonym przez przepisy, normy oraz wskazania producenta. Wykonawca winien zasymulować odpowiednie sytuacje i przeprowadzić testy, tak aby sprawdzenie miało charakter kompleksowy i nie budziło wątpliwości, co do pewności działania całego systemu. Wyniki testów należy zapisać w protokołach i przekazać użytkownikowi.
4.	Przed oddaniem systemu do użytkowania Wykonawca winien dokonać przeszkolenia osoby (osób) przewidzianej do nadzoru systemu w zakresie jego właściwej eksploatacji. Szkolenie powinno obejmować swoim zakresem co najmniej: wprowadzenie do systemu, omówienie poszczególnych urządzeń tworzących system, omówienie architektury systemu – poszczególnych modułów (kontroli dostępu, sygnalizacji włamania i pożaru, monitoringu wizyjnego) i ich interakcji, wprowadzenie do konfiguracji systemów, tworzenie wizualizacji obiektów w systemie, praca z systemem DEMO – ćwiczenia praktyczne, utrzymanie, obsługa i diagnozowanie usterek. Minimalny czas trwania szkolenia określa projektant w dokumentacji projektowej.
5.	Odbiór szkoleń następuje poprzez potwierdzenie przez przeszkolone osoby, własnoręcznym podpisem w protokole, faktu przeszkolenia i uzyskania wiedzy potrzebnej do właściwego nadzorowania systemu.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Nr	Opis wymagania
6.	Odbiór prac wdrożeniowych i przekazanie systemu do eksploatacji następuje po uzyskaniu pozytywnych wyników testów i przeprowadzeniu szkoleń.

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

5.3 Zawartość dokumentacji projektowej dla Zintegrowanego Systemu Nadzoru - (wymagania minimalne)

W ramach dokumentacji opisowej należy posługiwać się ujednoliconą stroną opisową tabela dokumentacji projektu technicznego przedstawiona jak na rysunku poniżej.

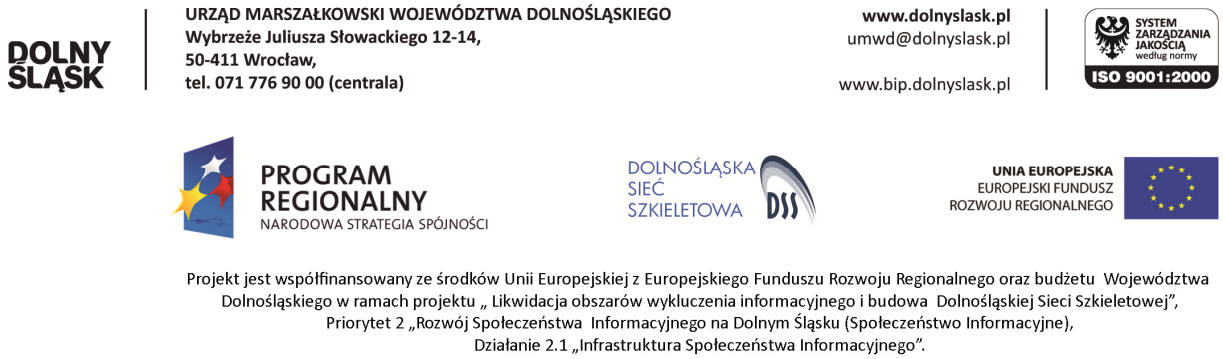
Stadium:	**(np. PROJEKT WYKONAWCZY)**	
Temat opracowania:	…	
Obiekt:	…	
Branża:	…	
Inwestor:	…	
Jednostka projektowa:	…	
	Nr archiwalny:	…
	Tom:	… / …
	Egzemplarz:	… / …

Funkcja	Imię i Nazwisko	Uprawnienia/ specjalność	Numer uprawnień	Data	Podpis
Projektował :					
Opracował:					
Opracował					

Miejscowość - Data

Rysunek 11. Wzór strony opisowej - tabela dokumentacji projektu technicznego

Jednocześnie należy stosować stopkę dokumentu (co najmniej w stronie opisowej jak i części opisowej projektu) zgodnie z wzorem przedstawionym na rysunku



Rysunek 12. Wzór stopki dokumentu projektowego

Oświadczenie projektanta

O Ś W I A D C Z E N I E

Zgodnie z art. 20 ust. 4 Ustawy Prawo budowlane z dnia 7 lipca 1994 (Dz. U. 2006.156.1118 z późniejszymi zmianami)

oświadczam jako projektant/sprawdzający

że projekt:

„ … ”

został sporządzony zgodnie z obowiązującymi przepisami, normami i zasadami wiedzy technicznej oraz że jest on kompletny z punktu widzenia celu jakiemu ma służyć. Oświadczam zarazem, że zawartość projektu spełnia wymagania Rozporządzenia Ministra Infrastruktury z dnia 2 września 2004 (Dz. U. 2004.202.2072) w sprawie szczegółowego zakresu i formy dokumentacji projektowej.

.....

(data, podpis)

Rysunek 13. Wzór oświadczenia projektanta

5.3.1 Zawartość dokumentacji projektowej

7. Część ogólna

7.1. Przedmiot opracowania

Należy określić przedmiot opracowania (np. „Przedmiotem opracowania jest projekt wykonawczy zintegrowanego systemu nadzoru bezpieczeństwa fizycznego infrastruktury DSS").

Należy zamieścić informację o szerszym kontekście opracowania (np. jeśli opracowanie wchodzi w skład wielobranżowej dokumentacji projektowej należy podać nazwę przedsięwzięcia i wymienić już opracowane projekty budowlane i wykonawcze, specyfikacje techniczne wykonania i odbioru, instrukcje BIOZ lub przedmiary prac powiązane z opracowaniem).

7.2. Podstawa opracowania projektu

Należy określić podstawę wykonania opracowania oraz wykorzystane źródła danych.

7.3. Opis ogólny inwestycji

7.3.1. Położenie geograficzne

Należy zdefiniować lokalizację/lokalizacje obiektu/obiektów.

7.3.2. Zakres rzeczowy

Należy określić główne wskaźniki zakresu rzeczowego.

8. Słownik, terminologia i symbolika

8.1. Słownik i terminologia

Należy zdefiniować pojęcia i terminy używane w opracowaniu, które nie są powszechnie stosowane

8.2. Symbolika

Należy zdefiniować symbole stosowane na rysunkach

8.3. Oznaczenia i numeracja

Należy zdefiniować stosowane oznaczenia i zasady numeracji elementów.

Np.:

WS_x	-	*Węzeł szkieletowy o numerze „x”*
WD_x	-	*Węzeł dystrybucyjny o numerze „x”*
CZS	-	*Centrum Zarządzania Siecią*
ZCZS	-	*Zapasowe Centrum Zarządzania Siecią*

9. Bazowe dokumenty normatywne i dokumenty odniesienia

9.1. Wykaz norm i dokumentów odniesienia

Należy wymienić wszystkie dokumenty odniesienia i normy bazowe cytowane w opracowaniu.

10. Charakterystyka techniczna projektowanego obiektu

10.1. Szczegółowe rozwiązania i obliczenia projektowe.
10.2. Szczegółowe wytyczne realizacyjne.
10.3. Szczegółowe wytyczne w zakresie wdrożenia.
10.4. Szczegółowe wytyczne w zakresie szkoleń i eksploatacji.

11. Tabele

11.1. Spis obiektów objętych projektem

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

Wymienić obiekty objęte opracowaniem i podać ich lokalizację.

L.p.	Oznaczenie	Obiekt	Adres

11.2. Zestawienie typów i liczby urządzeń / zespołów urządzeń

Wymienić elementy dostaw materiałów i urządzeń, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

Lp.	Nazwa urządzenia	Zakres/Liczba	Opis Wymagań
1	Serwer kontroli dostępu		opis w punkcie …
2	Serwer monitoringu video		…
3	Oprogramowanie systemu kontroli dostępu i sygnalizacji włamania		
4	Oprogramowanie systemu monitoringu video		
5	Czytnik kart kontroli dostępu		
6	Centrala alarmowa / Centrala SAP		
7	Klawiatura kodowa		
8	Sterownik sieciowy z akumulatorem		
9	Półka do szafy 19”		
10	Czujka PIR + MW		
11	Czujka zbicia szkła		
12	Czujka dymu		
13	Czujnik temperatury wraz z regulatorem		
14	Czujka kontaktronowa		
15	Sygnalizator optyczno-akustyczny		
16	Zamek elektromagnetyczny typ 1		
17	Zamek elektromagnetyczny typ 2		
18	Kamera IP		
19	Patchcord kat. 5e - 2m		
20	Kabel UTP 4x2x0,5 lub YTKSY 3x2x0,5		
21	Kabel LiYCY 8x0,75		
22	Koryto kablowe 25x15mm		
…	…		

11.3. Zestawienie prac podstawowych

Wymienić prace, ich zakresy rzeczowe oraz odnośniki do wymagań. Np.:

Lp.	Opis czynności	Zakres/Liczba	Wymagania/Uwagi
1	Montaż, podłączenie i uruchomienie serwera w szafie 19”		opis w punkcie …
2	Montaż czytnika kart kontroli dostępu na ścianie		…
3	Montaż czytnika kart kontroli dostępu na drzwiach szafy		
4	Montaż i uruchomienie centrali alarmowej		
5	Montaż i podłączenie klawiatury kodowej		
6	Montaż półki w szafie 19”		
7	Montaż i uruchomienie sterownika sieciowego z akumulatorem		
8	Montaż czujki PIR + MW		
9	Montaż czujki zbicia szkła		
10	Montaż czujki dymu		
11	Montaż czujki temperatury wraz z regulatorem		
12	Montaż czujki kontaktronowej		
13	Montaż sygnalizatora optyczno-akustycznego		
14	Montaż zamka elektromagnetycznego typ 1 na drzwiach szafy teleinformatycznej		
15	Montaż zamka elektromagnetycznego typ 2 na drzwiach wejściowych do pomieszczenia		
16	Montaż i uruchomienie kamery IP		
17	Montaż koryta kablowego 25x15mm		
18	Ułożenie kabla w korycie		
19	Sprawdzenie instalacji		
20	Programowanie i uruchomienie systemu		
21	Szkolenie osób, które będą obsługiwać system		
	…	…	…

12. Spis rysunków

Należy zamieścić spis rysunków wykorzystanych w opracowaniu. Np.:

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

13. Informacja BIOZ

13.1. Podstawa

Informację BIOZ należy opracować 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.

13.2. Zakres stosowania

Określić

13.3. Zakres wykonywanych robót

Określić

13.4. Przewidywane zagrożenia

13.4.1. Wykaz elementów – potencjalnych źródeł zagrożenia

Określić

13.4.2. Wykaz zagrożeń i ryzyk

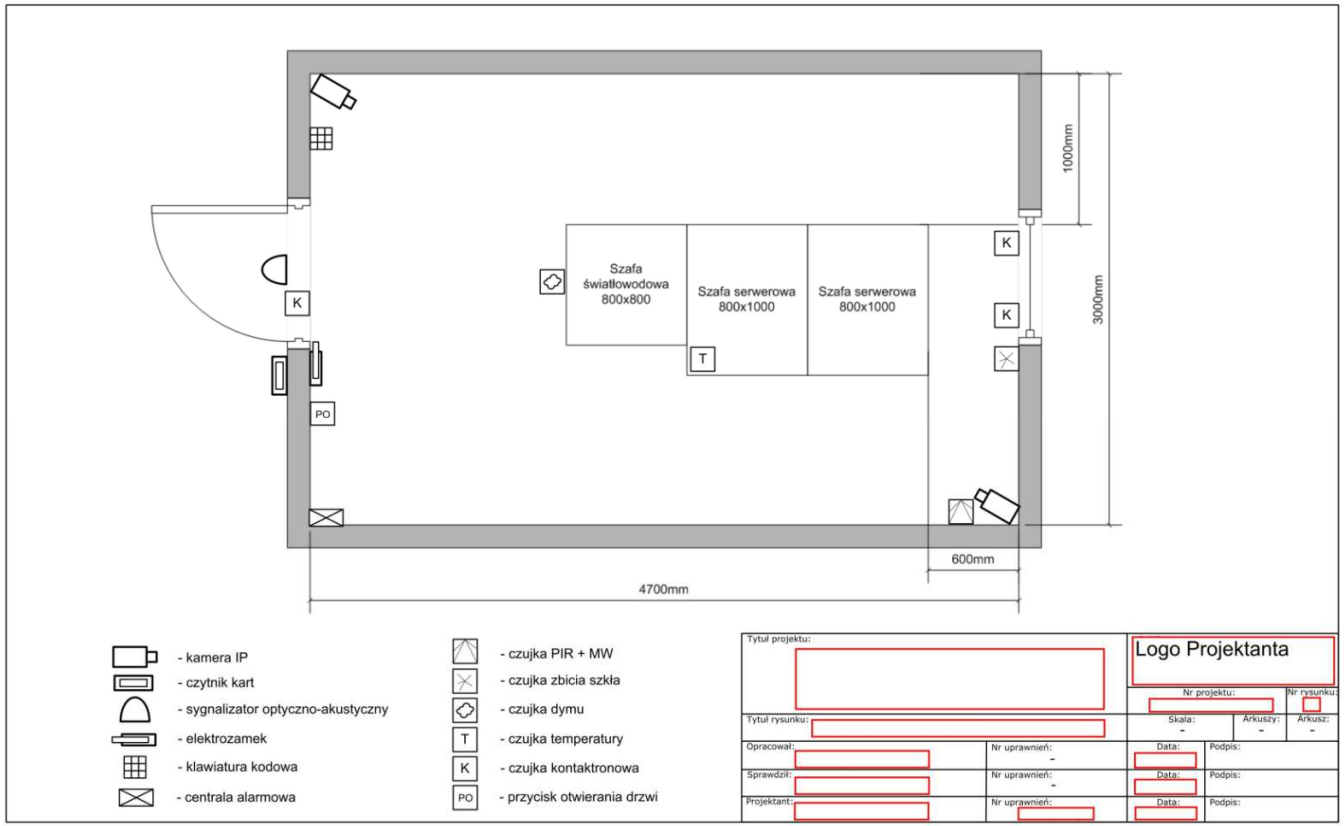
Określić

13.5. Środki zapobiegania niebezpieczeństwom

Opisać

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

5.4 Wzór rysunku - dokumentacja projektowa dla Zintegrowanego Systemu Nadzoru



Rysunek 14. Wzór graficznej prezentacji urządzeń Zintegrowanego Systemu Nadzoru

PROGRAM REGIONALNY NARODOWA STRATEGIA SPÓJNOŚCI
DOLNY ŚLĄSK
DOLNOŚLĄSKA SIEĆ SZKIELETOWA DSS
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

6 Dokumentacja w zakresie szkoleń

6.1 Szkolenia

W ramach prac projektowych należy uwzględnić optymalny (a co najmniej wymagalny zakres szkoleniowy dla pracowników Inwestora. Optymalny zakres szkoleń winien dostarczyć umiejętności w zakresie:

- instalacji i uruchamiania poszczególnych elementów sieci DSS,
- konfiguracji poszczególnych elementów sieci DSS
- administrowania poszczególnymi elementami sieci DSS,
- konfiguracji sieci DSS,
- administrowania Siecią DSS,
- konfiguracji usług sieci DSS,
- administrowania siecią DSS,
- monitorowania i zarządzania ruchem w sieci DSS
- zarządzania usługami sieci (z uwzględnieniem zarządzania elementami siecim menadżerami sieci, itp.) na potrzeby realizacji celów strategicznych sieci
- zarządzania usługami sieci (z uwzględnieniem zarządzania elementami siecim menadżerami sieci, itp.) w celu zapewnienia należytego poziomu jakości świadczonych usług

6.1.1 Dokumentacja szkoleniowa

W ramach planowania i projektowania szkoleń związanych z dostawa i uruchamianiem sieci DSS przedstawić należy w postaci udokumentowanej:

- Szczegółowy program szkolenia obejmujący:
  - Część teoretyczną szkolenia:
    - wyszczególnienie czasu na poszczególne partie materiału i formy zajęć
    - metodyka (wykład, warsztaty, laboratorium)
  - Część praktyczna szkolenia
    - wyszczególnienie czasu na poszczególne partie materiału i formy zajęć
    - metodyka (wykład, warsztaty, laboratorium)
  - Zasoby niezbędne do przeprowadzenia szkolenia
- Zakres wiedzy i umiejętności niezbędny do przystąpienia do szkolenia
- Zakres kompetencji i umiejętności uzyskany po odbyciu szkolenia
- Wzór certyfikatu, lub zaświadczenia dotyczącego ukończenia danego szkolenia. Wymienione dokumenty powinny zawierać minimum:
  - imię i nazwisko kursanta,
  - nazwę i adres Wykonawcy,
  - zakres tematyczny i godzinowy szkolenia.
  - podpis prowadzącego,
- Wzór ankiety ewaluacyjnej badającej ocenę szkolenia przez uczestnika. Wymieniony dokument powinien zawierać odpowiedzi na minimum X pytań dotyczących szkolenia.

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej" jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego

- Wzór testu egzaminacyjnego badającego zmiany poziomu wiedzy uczestników. W/w dokument powinien zawierać odpowiedzi na minimum Y pytań dotyczących wiedzy zdobywanej podczas szkolenia

Wykonawca szkolenia zobowiązany będzie w ramach realizacji szkoleń do prowadzenia następującej dokumentacji:

- list obecności uczestników poszczególnych szkoleń, będących jednocześnie dokumentami odbioru materiałów szkoleniowych zaopatrzonych podpisem prowadzącego oraz list odbioru certyfikatów.
- ankiet ewaluacyjnych, badających ocenę szkolenia przez uczestnika,
- testów egzaminacyjnych badających zmiany poziomu wiedzy uczestników.

Wykonawca szkolenia zobowiązany będzie w ramach realizacji szkoleń do przygotowania dokumentacji szkoleniowej w nastepującym układzie:

- Skrypt omawiający materiał szkolenia (rekomendowany format: plik Word)
- Prezentacja elektroniczna materiału (rekomendowany format: plik Power Point)
- Skrypty laboratoryjne/warsztatowe (rekomendowany format: plik Word)

7 Wymagania dla dokumentacji powykonawczej przeznaczonej do ewidencji elektronicznej

System paszportyzacji sieci jest nieodzownym narzędziem do sprawnego i efektywnego zarządzania zasobami sieciowymi, które zostaną wytworzone w procesie budowy i eksploatacji Dolnośląskiej Sieci Szerokopasmowej. Przewidywane do zastosowania technologie budowy sieci pasywnej i aktywnej spowodują wygenerowanie bardzo dużej liczby zasobów o zróżnicowanej charakterystyce i rozmieszczonych na obszarze całego województwa.

Tylko elektroniczne systemy ewidencji i wsparcia zarządzania siecią, a do nich należy system paszportyzacji sieci, pozwolą poprawnie identyfikować poszczególne elementy oraz efektywnie eksploatować sieć.

W systemie paszportyzacji każdy element sieci posiada tzw. paszport, dokument ewidencyjny elementu .

Zawartość takiego dokumentu powinna zawierać informacje z czterech obszarów:

a. Klasyfikacja obiektu
   - Rodzaj
   - Typ
   - Kategoria (np.; obiekt liniowy, obiekt punktowy)
   - Kod obiektu:

DSS	- Dolnośląska Sieć Szkieletowa
WS_x	- Węzeł szkieletowy o numerze „x”
WD_x	- Węzeł dystrybucyjny o numerze „x”
CZS	- Centrum Zarządzania Siecią
ZCZS	- Zapasowe Centrum Zarządzania Siecią

   - Numer obiektu

b. Właściciel i administrator

c. Lokalizacja
   - Adres pocztowy
   - Adres geodezyjny (obręb geodezyjny, nr działki), w przypadku obiektów liniowych podajemy adresy początku i końca obiektu.

d. Dane dodatkowe (parametry , stopień wykorzystania, sposób dostępu do elementu, zasady serwisowania, terminy gwarancji)

Projekt „Likwidacja obszarów wykluczenia informacyjnego i budowa Dolnośląskiej Sieci Szkieletowej” jest współfinansowany ze środków Unii Europejskiej Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Województwa Dolnośląskiego w ramach Regionalnego Programu Operacyjnego Priorytet 2 Rozwój Społeczeństwa Informacyjnego na Dolnym Śląsku (Społeczeństwo Informacyjne) Działanie 2.1 Infrastruktura Społeczeństwa Informacyjnego