Załącznik nr 1 do Zapytania Ofertowego/ Umowy

Szczegółowy Opis Przedmiotu Zamówienia

Spis treści

1. Definicje:

1) ACL – lista kontroli dostępu.

2) BE Best Effort – usługa Best effort (BE) transmituje dane w sieci o możliwie najwyższej przepustowości, ale za to bez gwarancji poziomu usług QoS.

3) BFD – protokół sieciowy wykrywający problemy pomiędzy dwoma procesami przekazującymi ruch, połączonymi między sobą. Wspierane protokoły trasowania to BGP, IS-IS ,OSPF, RSVP. Został on opisany w RFC 5880.

4) CG-NAT / NAT – (Network Address Translation) – translacja adresów sieciowych zdefiniowana w RFC6598 oraz RFC1918.

5) GUA – Global Unicast Address – Adres publiczny IPv6.

6) CLI – Command Line Interface, Interfejs wiersza poleceń służący do wprowadzania konfiguracji Urządzenia.

7) Oprogramowanie System Zarządzanie (Element Manager) – Oprogramowanie do zarządzania Urządzeniami, umożliwiające kreowanie usług, zmianę i tworzenie konfiguracji oraz monitorowanie stanu pracy Urządzeń.

8) IGP (Interior Gateway Protocol) – rodzina protokołów trasowania pakietów danych wewnątrz systemu autonomicznego.

9) LAN (Local Area Network) – lokalna sieć komputerowa łącząca komputery na określonym obszarze.

10) LDP (Label Distribution Protocol) – protokół, w którym Urządzenie zdolne do wieloprotokołowego przełączania etykiet (MPLS) wymieniają informacje mapowania etykiety zgodnie z RFC 5036.

11) LSP (Label Switched Paths) – połączenie punkt – punkt bazujące na wieloprotokołowym przełączaniu etykiet MPLS.

12) MIB – Rodzaj bazy danych wykorzystywanej do zarządzania Urządzeniami w sieci komunikacyjnej (RFC1213).

13) NETCONF – protokół zarządzania siecią opracowanym i znormalizowanym przez IETF zgodnie z RFC 6241.

14) NTP – protokół synchronizacji czasu, zdefiniowany w RFC 5905.

15) OSS/BSS (operations support system / business support system) – systemy utrzymania zasobów, zabezpieczenia usług, konfiguracji komponentów sieci i zarządzania błędami.

16) PBR (Policy Based Routing) - przekazywanieuje i trasowanie pakietów danych w oparciu o reguły lub filtry.

17) PVSTP/VSTP – funkcjonalność RSTP dla VLAN.

18) RADIUS – protokół zdalnego uwierzytelniania użytkowników opisany w RFC2865.

19) SSH – protokół szyfrowania komunikacji typu klient – serwer, a także serwer – klient.

20) RIPE – otwarte stowarzyszenie zajmujące się rozwojem Internetu w Europie.

21) RSTP (Rapid Spanning Tree Protocol) – protokół komunikacyjny wykorzystywany przez sieci komputerowe (np. LAN) w drugiej warstwie modelu sieciowego OSI, opracowany przez(IEEE) i opisany w dokumencie IEEE 802.1D.

22) SIEM (Security Information and Event Management) – system do zarządzania informacją związaną z bezpieczeństwem i zdarzeniami.

23) SNMPv2/ SNMPv3 – rodzina protokołów sieciowych wykorzystywanych do zarządzania urządzeniami sieciowymi i serwerami za pośrednictwem sieci IP, zgodnie z RFC2570, RFC1901.

24) TACACS+ – protokół uwierzytelniania, używany do komunikacji ze zdalnym serwerem uwierzytelniania opisany w RFC 1492.

25) T-LDP (Targeted Label Distribution Protocol) – funkcjonalność umożliwiająca ustanowienia sesji LDP pomiędzy dwoma odległymi urządzeniami bez konieczności użycia ruchu multicastowego do redystrybucji etykiet.

26) TELNET – standard protokołu komunikacyjnego używanego w sieciach komputerowych do obsługi odległego terminala w architekturze klient-serwer.

27) Węzeł Agregacyjny – Węzeł, do którego dołączone są łącza dostępowe do szkół, węzeł ten nie ma bezpośredniego połączenia do sieci Internet.

28) Węzeł Regionalny – zbiór infrastruktury sieciowej OSE zlokalizowany w Obiekcie, pełniący rolę Węzła Agregacyjnego oraz Regionalnego Węzła Bezpieczeństwa.

29) Węzeł Bezpieczeństwa – zestaw urządzeń wraz z oprogramowaniem, realizujących funkcje bezpieczeństwa (m.in. dekrypcja SSL, filtrowanie treści, funkcjonalność IDP, itd.), sposób

działania tego węzła oraz jego budowa są poza zakresem niniejszego zapytania. W zależności od lokalizacji – węzeł Regionalny lub Centralny.

30) Węzeł Szkieletowy – węzeł OSE zapewniający przeniesienie ruchu z węzłów agregacyjnych do sieci Internet, a także inżynierię ruchu, na styku sieci OSE z Internetem.

31) Węzeł Centralny – zbiór infrastruktury sieciowej OSE zlokalizowany w Obiekcie, pełniący rolę Węzła Szkieletowego oraz Centralnego Węzła Bezpieczeństwa.

32) Urządzenia – urządzenia realizujące funkcje Sieci OSE.

33) VPWS – usługa zapewniająca sieci opartej na Ethernecie, połączenie punkt-punkt za pośrednictwem sieci IP lub MPLS.

34) VLAN (Virtual Local Area Network) – sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej.

35) VPLS – usługa zapewniająca sieci opartej na Ethernecie, połączenia wielopunktowe za pośrednictwem sieci IP lub MPLS.

36) VRF (Virtual Routing and Forwarding) – wirtualne routery sieciowe, które pozwalają na istnienie wielu wystąpień tabeli routingu w routerze działających jednocześnie.

37) VRRP – protokół zapewniający automatyczne przydzielanie redundantnych zasobów sieciowych.

38) uRPF – funkcjonalność, która umożliwia sprawdzenie osiągalności źródła pakietu IP.

39) OpenConfig – nieformalna grupa robocza operatorów sieci, której celem jest zdefiniowanie, programowalnej infrastruktury SDN.

40) QinQ (IEEE 802.1ad) – standard opisujący działanie wirtualnych sieci LAN (VLAN), realizowanych w standardzie IEEE 802.1q.

41) QoS (Quality of Service – QoS) – poziom gwarantowanych osiągów parametrów sieciowych standard został opisany w RFC 2676 i RFC 2386.

42) Zasoby obliczeniowe OSE / Chmura obliczeniowa OSE – infrastruktura serwerowa udostępniona w celu zapewnienia mocy obliczeniowej t.j. procesory, pamięć RAM, przestrzeń dyskowa wybudowana na potrzeby systemów i usług OSE. Zasoby są umieszczone w Węzłach Centralnych w Warszawie i Poznaniu.

43) Multicast IPv4 i IPv6 – metoda przekazywania pakietów telekomunikacyjnych IP do grupy zainteresowanych odbiorców.

44) RFC 1112 „Host Extensions for IP Multicasting” – obsługa multicast (w tym IGMP) przez urządzenia końcowe.

45) RFC 2362 „Protocol Independent Multicast Sparse Mode PIM-SM” – podstawowy protokół routingu multicast.

46) RFC 2858 „Multiprotocol extensions for BGP4” – rozszerzenia BGP do obsługi multicast.

47) RFC 3376 „Internet Group Management Protocol Version 3” – najnowsza wersja IGMP – zarządzanie grupami multicastowymi w sieciach opartych na protokole IP.

48) RFC 3618 „Multicast Source Discovery Protocol” – protokół MSDP przenoszący informacje o źródłach multicast pomiędzy domenami administracyjnymi.

49) RFC 4607 „Source-specific multicast" – sposób dostarczania pakietów multicast, w których jedynymi pakietami dostarczanymi do adresu docelowego są pakiety pochodzące z konkretnego adresu źródłowego żądanego przez odbiorcę.

50) RFC 3569 „Source-specific multicast" – sposób dostarczania pakietów multicast, w których jedynymi pakietami dostarczanymi do adresu docelowego są pakiety pochodzące z konkretnego adresu źródłowego żądanego przez odbiorcę.

51) OSPF – Protokół trasowania dynamicznego oparty o analizę stanu łącza.

- 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.

52) IS-IS – Protokół trasowania stanu łącza (ang. link-state) oparty na otwartych standardach.

- 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.

53) BGP – Zewnętrzny protokół trasowania (routingu) EGP. BGP w wersji czwartej jest podstawą działania współczesnego Internetu. Istnieje wiele rozszerzeń BGP stosowanych przy implementacji MPLS VPN, IPv6 czy Multicast VPN.

- 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).

54) MPLS – Technika stosowana przez routery, w której trasowanie pakietów zostało zastąpione przez tzw. przełączanie etykiet.

- 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.

55) L2VPN i L3VPN

- 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 siecią 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,

56) MPLS-TE

- 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.

57) Router – urządzenie pracujące w trzeciej warstwie modelu OSI, służy do łączenia różnych sieci komputerowych.

58) Shadow Router – dedykowane urządzenie, emulujące urządzenie abonenckie (CPE), przeznaczone do testów parametrów jakości usług sieciowych, tj. opóźnienia, straty pakietów, jitter.

59) Route Reflector – jest elementem sygnalizacyjnym dla BGP opisany w RFC 4456.

2. Wstęp

2.1. Podstawa opracowania projektu

Ogólnopolska Sieć Edukacyjna ma na celu zapewnienie dostępu do szybkiego, bezpiecznego Internetu dla szkół. OSE jest publiczną siecią telekomunikacyjną, opartą o istniejącą infrastrukturę szerokopasmową wybudowaną w ramach inwestycji komercyjnych oraz dofinansowanych ze środków publicznych w ramach Programu Operacyjnego Polska Cyfrowa. Za uruchomienie i utrzymanie Sieci, oraz w szczególności za dostarczenie szkołom usługi dostępu do Internetu o symetrycznej przepustowości co najmniej 100 Mb/s wraz z kompleksowymi usługami bezpieczeństwa sieciowego, w tym ochrony przed zagrożeniami dla prawidłowego rozwoju uczniów, odpowiedzialny jest Operator OSE, którym jest NASK PIB.

2.2. Przedmiot przedsięwzięcia

W Polsce istnieje ok. 25 000 szkół zlokalizowanych w ok. 20 000 lokalizacjach. Podstawowym zadaniem OSE ma być zapewnienie szkołom w Polsce możliwości dostępu do bezpiecznego Internetu i zasobów edukacyjnych wraz z szeregiem usług powiązanych, w tym:

- Zapewnienie usług dostępu do sieci Internet o przepływności minimum 100 Mb/s symetrycznie,
- Zapewnienie usług bezpieczeństwa umożliwiających ochronę użytkowników,
- Zapewnienie dostawcom treści edukacyjnych dostępu do użytkowników sieci OSE.

2.3. Założenia projektowe

Poniżej opisano główne założenia koncepcyjne jak również zestaw wymagań, jakie musi spełniać sieć OSE, w celu umożliwienia realizacji usług zgodnie z założeniami.

2.3.1. Podstawowe założenia

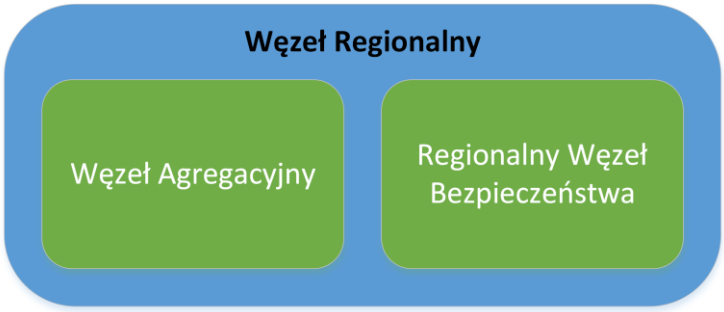
W ramach budowy OSE planuje się uruchomienie sieci rozległej transmisji danych, systemów bezpieczeństwa wraz z systemami wsparcia obejmującymi m.in. systemy Zarządzania Tożsamością, OSS, BSS, SIEM jak również urządzenia abonenckie (CPE), przełączniki, punkty dostępowe sieci bezprzewodowej. Usługi obejmować będą swoim zasięgiem terytorium Polski.

Sieć OSE, zbudowana będzie z Węzłów zlokalizowanych na terenie 16 województw.

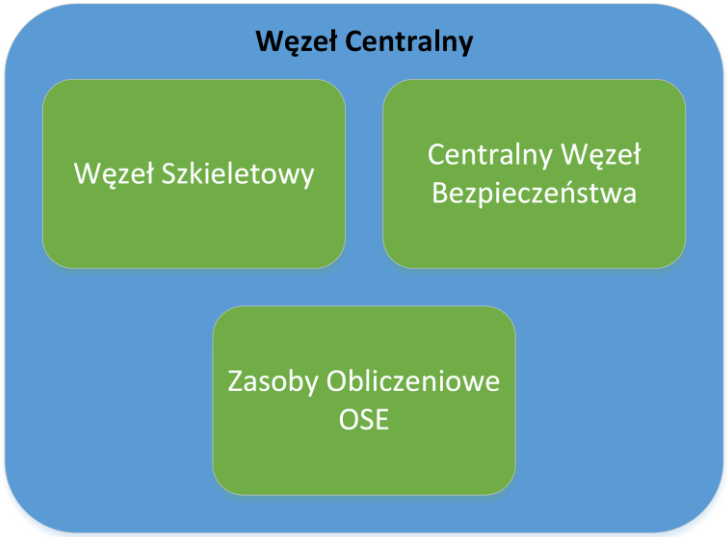
2.3.2. Węzły sieci

W sieci OSE będą dwa rodzaje Węzłów:

- Węzły Regionalne, w których skład będą wchodzić Węzły Agregacyjne (do których będą dołączone łącza ze szkół) oraz Regionalne Węzły Bezpieczeństwa.
- Węzły Centralne, w których skład będą wchodzić Węzły Szkieletowe, Centralne Węzły Bezpieczeństwa oraz Zasoby Obliczeniowe OSE (będące platformą dla systemów OSS / BSS).
  Do Węzłów Szkieletowych dołączone będą Węzły Agregacyjne. Węzły te będą także zapewniały łączność do sieci Internet.



Komponenty Węzła Regionalnego



Komponenty Węzła Centralnego

Węzły Szkieletowe będą zlokalizowane w tych samych miejscach co Węzły Agregacyjne, za wyjątkiem węzła WAW / WAW Core, w którym Węzeł Agregacyjny będzie umieszczony w innej lokalizacji niż Węzeł Szkieletowy (oba węzły będą zlokalizowane na terenie Warszawy). Urządzenia pełniące funkcje obu węzłów będą oddzielne, za wyjątkiem przełączników sieci lokalnej, które będą świadczyć usługi na rzecz zarówno Węzła Agregacyjnego jak i Węzła Szkieletowego.

2.3.3. Koncepcja świadczenia usługi dla szkoły

W szkołach zainstalowane będą urządzenia CPE, świadczące usługi dla sieci lokalnych w szkołach (urządzenia te w całości pozostają poza zakresem niniejszego zapytania).

Na urządzeniach tych lokalne adresy IPv4 z pul prywatnych zgodnych z RFC1918 / BCP5 translowane są (NAT 1:1) do adresów z puli 100.64.0.0/10 (Shared Address Space zgodnie z RFC6598 / BCP153). Jednocześnie dla klientów IPv6 zaalokowana jest pula adresów GUA z puli przydzielonej dla sieci OSE przez RIPE (w sieci OSE nie będą używane adresy prywatne IPv6).

Ruch od urządzeń CPE umieszczonych w szkołach przenoszony jest przez łącza, w technologii Ethernet, operatorów agregujących do Węzłów Agregacyjnych sieci OSE, gdzie jest oddawany do urządzeń agregujących sieci OSE na interfejsach 10GE oraz 1GE. Ruch do każdego urządzenia CPE jest oddawany na oddzielnych VLANach, przy następujących założeniach:

- każda szkoła jest terminowana na oddzielnym VLANie lub VLANach,
- z każdej szkoły może być utworzonych kilka VLANów (do pięciu), przy czym każdy z nich terminowany jest po stronie szkoły w oddzielnym VRF, a od strony sieci OSE każdy traktowany jest jako oddzielne łącze z własną adresacją i routingiem; Separacja VLANów tworzona jest na potrzeby kreowania różnych usług, w tym usług posiadających różne polityki bezpieczeństwa;
- ruch zarządzania do urządzenia CPE jest oddzielony od ruchu produkcyjnego szkoły obsługiwanej przez to CPE i terminowany jest na oddzielnym VLANie,
- ww. VLANy mogą być oddane w jednym z dwóch modeli:
  - jako VLAN z pojedynczym tagowaniem, zgodnie ze standardem IEEE 802.1q lub,
  - jako VLAN z podwójnym tagowaniem, zgodnie ze standardem IEEE 802.1ad, przy czym ruch z pojedynczej szkoły ma wspólny S-TAG oraz EtherType = 0x88a8.

Ruch odebrany w Węźle Agregacyjnym kierowany jest do Regionalnego Węzła Bezpieczeństwa.

Następnie odebrany ruch z Regionalnego Węzła Bezpieczeństwa kierowany jest do Węzłów Szkieletowych, a następnie do sieci Internet. Pomiędzy Regionalnym Węzłem Bezpieczeństwa, a wyjściem do sieci Internet ruch IPv4 przechodzi przez instancję CG-NAT, gdzie jest translowany do publicznych adresów IPv4 przydzielonych dla sieci OSE.

Separacja ruchu

Ruch zarządzania (zarówno dla urządzeń CPE jak też urządzeń sieci OSE) traktowany jest jako ruch zaufany i jest oddzielony od ruchu produkcyjnego do / ze szkół. Separacja tego ruchu w sieci OSE powinna nastąpić na poziomie VFR, logical system lub podobnym (tj. zapewniającym separację tablic routingu oraz wykluczającym wzajemny dostęp do ruchu z poszczególnych strumieni).

QoS

W sieci OSE wdrożony będzie QoS z następującymi założeniami:

- klasyfikacja odbywa się na urządzeniu agregacyjnym sieci OSE,
- najwyższy priorytet w sieci ma ruch z klasy Network Control, obejmujący ruch kontrolny protokołów routingu (IGP, BGP, MPLS, itd.) – ruch ma zagwarantowane pasmo na interfejsach szkieletowych sieci (tj. interfejsach pomiędzy urządzeniami sieci OSE bez uwzględnienia urządzeń CPE);
- ruch w klasie MGMT (ruch zarządzania, w szczególności ruch do / z systemów OSS, ruch sesji terminalowych do urządzeń sieciowych, ruch do kolektorów logów) – ruch ma zagwarantowane pasmo na interfejsach sieci (w tym na interfejsach pomiędzy urządzeniami sieci OSE a urządzeniami CPE);
- ruch w klasie BE (Best Effort) obejmujący ruch produkcyjny do / ze szkół – ruch ma zagwarantowane pasmo na wszystkich interfejsach;

- w sieci OSE musi być przygotowana możliwość uruchomienia ruchu w klasach:
  - voice – ruch priorytetowy;
  - network control – ruch o najwyższym priorytecie (poza voice) – ruch ma zagwarantowane pasmo;
  - interactive video – ruch o priorytecie niższym niż network control – ruch ma zagwarantowane pasmo;
  - best effort – ruch ma gwarantowane pasmo;
  - scavenger (less-than best-effort) – ruch bez gwarancji pasma.

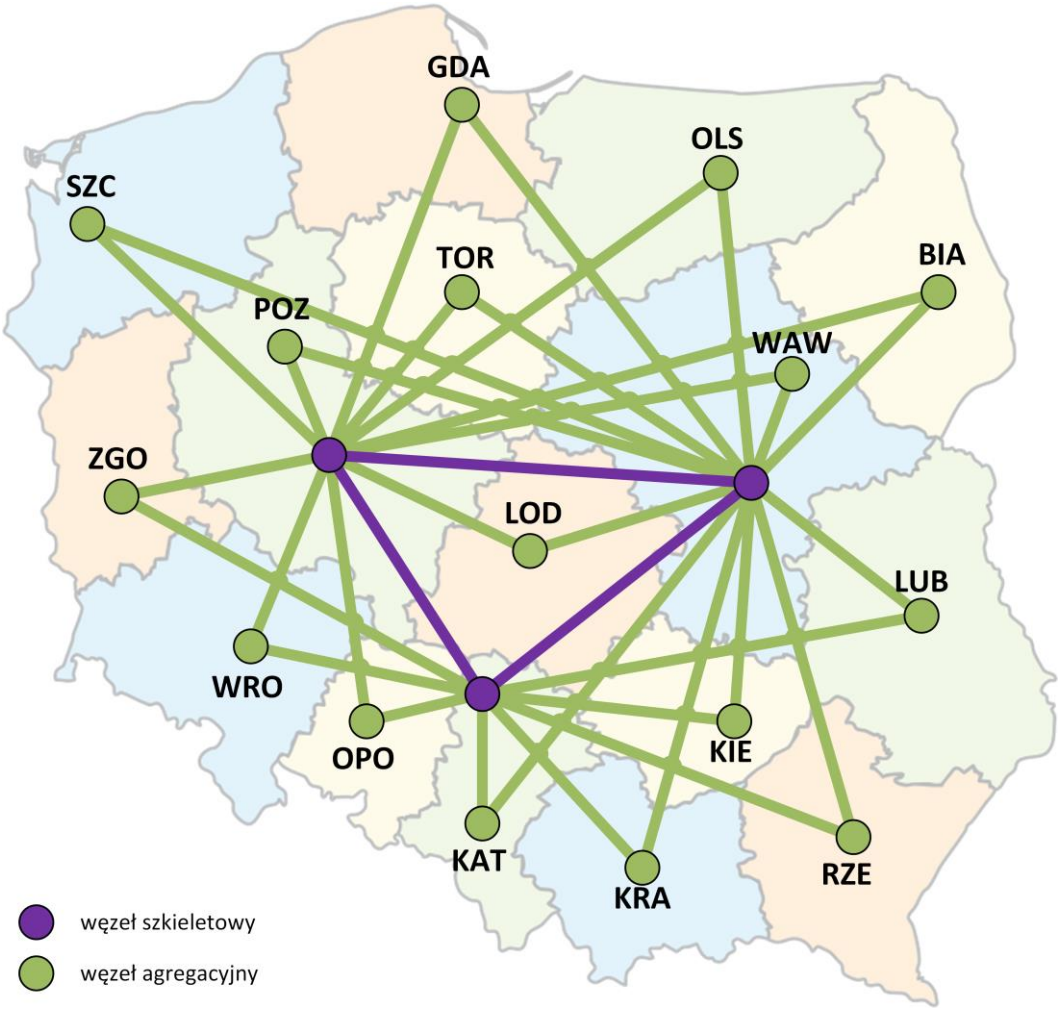
3. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostarczenie Urządzeń i Oprogramowania niezbędnych do zbudowanie Węzłów Agregacyjnych i Szkieletowych stanowiących jedną sieć.

Miejsca lokalizacji Węzłów sieci (Obiekty) podano poniżej:

województwo	lokalizacja węzła	Węzeł Agregacyjny	Węzeł Szkieletowy
mazowieckie	Warszawa	WAW	WAW Core
śląskie	Katowice	KAT	KAT Core
wielkopolskie	Poznań	POZ	POZ Core
dolnośląskie	Wrocław	WRO	-
kujawsko-pomorskie	Toruń	TOR	-
lubelskie	Lublin	LUB	-
lubuskie	Zielona Góra	ZGO	-
łódzkie	Łódź	LOD	-
małopolskie	Kraków	KRA	-
opolskie	Opole	OPO	-
podkarpackie	Rzeszów	RZE	-
podlaskie	Białystok	BIA	-
pomorskie	Gdańsk	GDA	-
świętokrzyskie	Kielce	KIE	-
warmińsko-mazurskie	Olsztyn	OLS	-
zachodniopomorskie	Szczecin	SZC	-

Schemat połączeń Węzłów Agregacyjnych i Węzłów Szkieletowych jest pokazany poniżej.



Każdy Węzeł sieci OSE wyposażony zostanie w urządzenia sieciowe, infrastrukturę bezpieczeństwa, przełączniki sieci lokalnej, systemy OSS/BSS (tylko w Węzłach Szkieletowych) oraz w urządzenia sieci zarządzania, zapewniające dostęp administracyjny do wszystkich urządzeń zlokalizowanych w węźle.

3.1. Wymagane Ogólne funkcjonalności Węzłów Szkieletowych i Agregacyjnych

Każdy z 16 Węzłów Agregacyjnych będzie zawierać komponenty realizujące funkcjonalności, m.in:

- agregacja łączy dostępowych do szkół w celu dostarczenia usług OSE,
- przesyłania ruchu ze szkół do Regionalnego Węzła Bezpieczeństwa,
- przesyłania ruchu do Węzłów Szkieletowych, w celu przesłania do sieci Internet,
- zapewnianie funkcjonalności CG-NAT;
- dołączanie dostawców treści edukacyjnych,
- wykonywanie pomiarów jakości sieci (za pomocą shadow routerów),
- zapewnianie sieci LAN dla Regionalnego Węzła Bezpieczeństwa oraz systemów OSS,
- zapewnianie łączności w ramach sieci zarządzania.

Trzy Węzły Szkieletowe będzie zawierać komponenty realizujące funkcjonalności, m.in:

- przesyłanie ruchu z Węzłów Agregacyjnych do zewnętrznych styków sieci OSE (łącza tranzytujące ruch do światowego Internetu, łącza do punktów wymiany ruchu internetowego – IXP, łącza do zewnętrznych dostawców treści, itd.)

- zapewnianie stabilnej sygnalizacji dla protokołów routingu (ze szczególnym uwzględnieniem BGP),
- wykonywanie pomiarów jakości sieci (za pomocą shadow routerów).

We wskazanym przez Zamawiającego miejscu Wykonawca zainstaluje Węzeł Laboratoryjny realizujący wszystkie funkcjonalność opisaną w dalszej części dokumentu. Węzeł Laboratoryjny pozwoli na przeprowadzenie:

- testów aktualizacyjnych oprogramowania
- testów przy większych zmianach konfiguracyjnych,
- testów nowych usług sieciowych wdrażanych w sieci OSE.

Wszystkie urządzenia muszą zostać wdrożone zgodnie z wymaganiami Zamawiającego zawartymi w niniejszym dokumencie. Wszystkie wymagania i parametry, w tym techniczne, funkcjonalne i wydajnościowe zawarte w niniejszym dokumencie mają charakter obligatoryjny i Wykonawca zobowiązany jest do ich spełnienia w ramach oferowanego rozwiązania. Wykonawca jest zobowiązany do takiego doboru urządzeń, który zapewni efektywność energetyczną oferowanego rozwiązania i optymalizację ponoszonych przez Zamawiającego kosztów utrzymania rozwiązania.

Wszystkie podane wymagania i parametry musza być spełnione łącznie. Wszystkie wymagania podane w niniejszym dokumencie muszą być spełnione dla dowolnej wielkości ruchu, w szczególności dla całkowitego ruchu podanego w powyżej, chyba że w opisie danej funkcjonalności podano inaczej.

W przypadku wymienienia wielu wymagań, konieczne jest spełniania wszystkich z nich (np. umieszczenie wygania „Urządzenie musi obsługiwać multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP)" oznacza konieczność obsługi przez urządzenie wszystkich wymienionych protokołów).

Wykonawca jest proszony o dobór odpowiednich Urządzeń do realizacji potrzeb Zamawiającego w zakresie budowy Węzłów Szkieletowych i Agregacyjnych. Zamawiający dopuszcza oferowanie wielu urządzeń realizujących zadania węzłów lub też jednego urządzenia realizującego wszystkie niezbędne funkcje przy zachowaniu parametrów niezawodnościowych (HA). Jednocześnie proponowane rozwiązania dla poszczególnych węzłów powinny być zunifikowane i umożliwiać prostą politykę serwisową.

Wykonawca jest zobowiązany do wdrożenia Węzłów Szkieletowych (3 szt.) i Agregacyjnych (16 szt.) oraz węzła laboratoryjnego (1 szt.). Wdrożenie obejmuje dostawę Urządzeń i Oprogramowania (w tym systemu zarządzania), instalację, konfigurację, uruchomienie i przeprowadzenie procedury odbiorów, a następnie utrzymanie przez okres przejściowy. Wykonawca będzie również zobowiązany do współpracy z innymi dostawcami wskazanymi przez Zamawiającego przy integracji dostarczonych Urządzeń i Oprogramowania z innymi systemami wskazanymi przez Zamawiającego.

3.2. Wymagania w zakresie wydajności i przepustowości sieci (Węzłów Agregacyjnych i Szkieletowych)

Na potrzeby skalowania urządzeń (zarówno w Węzłach Szkieletowych jak i Agregacyjnych) należy przyjąć, że całość ruchu do / ze szkoły kierowana jest z / do sieci Internet.

Sumaryczna ilość ruchu z sieci Internet do szkół wyniesie 1 058Gb/s, a ze szkół do sieci Internet 385Gb/s (wartości szacowane na rok 2025).

Całkowity, planowany, ruch w poszczególnych węzłach będzie następujący:

Węzeł agregacyjny	Ruch do szkół		Ruch ze szkół	
	pasmo [Mb/s]	pakiety [kpps]	pasmo [Mb/s]	pakiety [kpps]
WAW	160 990	55 531	58 610	20 217
KAT	145 810	50 293	53 080	18 310
POZ	92 380	31 865	33 630	11 601
KRA	91 240	31 471	33 220	11 458
LOD	65 690	22 659	23 920	8 249
WRO	60 240	20 777	21 930	7 564
GDA	57 650	19 887	20 990	7 240
LUB	57 020	19 668	20 760	7 160
RZE	56 170	19 376	20 450	7 054
TOR	50 510	17 421	18 390	6 342
OLS	47 880	16 516	17 430	6 013
SZC	39 850	13 744	14 510	5 004
KIE	38 960	13 438	14 180	4 892
BIA	38 960	13 438	14 180	4 892
ZGO	30 120	10 388	10 960	3 782
OPO	24 620	8 492	8 960	3 092

Planowane jest, że ok. 60% ww. ruchu będzie wychodziło do Internetu przez węzeł WAW-Core, a pozostałe 40% będzie równomiernie rozłożone pomiędzy pozostałe węzły KAT-Core i POZ-Core. W przypadku awarii dowolnego Węzła Szkieletowego, ruch przechodzący przez ten węzeł rozłoży się proporcjonalnie na pozostałe dwa Węzły Szkieletowe.

Zakładane wielkości ruchowe (ilość szkół , wolumen ruchu, parametry intensywności ruchu) są parametrami wymaganymi dla odpowiedniego przygotowania wydajności Urządzeń w Węzłach (stanowiących sieć). W przypadku gdy ruch rzeczywisty będzie się różnić od planowanego, wskazanego w tabeli powyżej, Zamawiający wymaga aby sieć:

- dalej realizowała wszystkie wymagane funkcjonalności zgodnie z wymaganiami podanymi w niniejszym załączniku, oraz
- zapewniała obsługę poszczególnych parametrów ruchowych do wielkości wskazanych w powyższej tabeli.

Składając ofertę Wykonawca potwierdza, że zaoferowane przez niego Urządzenia tworzące sieć spełniają powyższe wymagania.

4. Wymagania dla Węzła Szkieletowego

W sieci zbudowane będą trzy Węzły Szkieletowe. Zadaniem tych Węzłów będzie zebranie ruchu z Węzłów Agregacyjnych i skierowanie go zewnętrznych styków sieci (łącza tranzytujące ruch

do światowego Internetu, łącza do punktów wymiany ruchu internetowego – IXP, łącza do zewnętrznych dostawców treści, itd.), a także skierowanie ruchu powrotnego do szkół.

Dodatkowo do Węzłów Szkieletowych dołączone zostaną zasoby obliczeniowe OSE (chmura prywatna OSE), stanowiące podstawę dla systemów OSS / BSS.

Każdy z 3 Węzłów Szkieletowych będzie stanowił komplet Urządzeń wraz z Oprogramowaniem, dostarczanych, instalowanych oraz uruchamianych, konfigurowanych i odbieranych (testy odbiorcze) niezależnie od pozostałych węzłów sieci. Łącza szkieletowe pomiędzy Węzłami Szkieletowymi będą dostarczane przez Zamawiającego.

W skład Węzła Szkieletowego wchodzi:

- Router Szkieletowy,
- w dwóch węzłach Szkieletowych (WAW-Core oraz KAT-Core) zainstalowane będą Route Reflectory (wygania dla Route Reflectorów opisane są w pkt. 4.2),
- w dwóch węzłach (WAW-Core oraz POZ-Core) w ramach wyposażenia Węzła Szkieletowego, dostarczony będzie Oprogramowanie System Zarządzania (wymagania dla tego systemu opisane są w pkt 4.3).
- Shadow Router (wymagania dla Shadow Routerów opisane są w pkt. 4.3).

W ramach wdrożenia należy przyjąć, że wdrożenie węzła oznacza wdrożenie urządzeń z każdej z wymienionych grup na zasadach opisanych poniżej. Dla Oprogramowania System Zarządzania należy przyjąć, że system musi być zainstalowany oraz skonfigurowany do pracy z wszystkimi dostarczonymi Urządzeniami we wszystkich Węzłach Szkieletowych i Agregacyjnych.

4.1. Wymagania dla Routera Szkieletowego

Router Szkieletowy jest Systemem Urządzeń (w szczególności jednym Urządzeniem) zainstalowany w Węźle Szkieletowym spełniającym następujące wymagania:

1. Wymagania ogólne
   - 1.1. Wszystkie oferowane Routery Szkieletowe (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
   - 1.2. Zamawiający wymaga, aby wszystkie Routery Szkieletowe były tego samego modelu.
     - 1.2.1. Dopuszczalne jest różne wyposażenie Routerów Szkieletowych w karty interfejsów liniowych (w zależności od potrzeb), przy czym wskazane jest, aby do wyposażenia Routerów w różnych węzłach użyta była jak najmniejsza ilość modeli kart interfejsów.
   - 1.3. Router musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297).
     - 1.3.1. Router musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
     - 1.3.2. Router musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   - 1.4. Router musi być wyposażony w zasilacze dostosowane do napięcia przemiennego 230V AC wraz z odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.
     - 1.4.1. Dostarczone zasilacze muszą umożliwiać dołączenie Routera do dwóch niezależnych obwodów zasilających (dwa zestawy paneli zasilających) oraz poprawną pracę

urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełnej funkcjonalności urządzenia.

1.4.2. Dostarczony Router musi umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu co jednego zasilacza.

1.4.3. Maksymalny pobór mocy Routerów Szkieletowych nie może przekroczyć poniższych wartości:

węzeł	maksymalny pobór prądu
WAW Core	15 kW
KAT Core	14 kW
POZ Core	14 kW

1.5. Router musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.

1.6. Router musi poprawnie pracować przy wilgotności powietrza w zakresie od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

1.7. Router musi umożliwiać instalację, wymianę lub zamianę poszczególnych modułów (takich jak np. zasilacze, wentylatory, karty z interfejsami sieciowymi, moduły optyczne typu SFP / XFP / itd.) w trakcie pracy urządzenia (ang. hot-swap).

1.8. Wszystkie wymagane funkcjonalności Routera muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

1.9. Oprogramowanie Routera musi być modularne, co oznacza że poszczególne funkcjonalności (np. routing, SNMP, itd.) są obsługiwane przez oddzielne procesy, a każdy proces musi mieć możliwość restartu, bez wpływu na inne procesy.

1.10. Dokumentacja do Routera (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta Routera (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

2. Wymagania na interfejsy

2.1. Karty liniowe lub moduły Routera zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów[1]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na urządzenie ani ograniczeń w świadczeniu usług serwisowych.

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu Routera, ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie

[1] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji Routera, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

funkcjonalności dla całego urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.2. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)[2] zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne.

2.3. Router musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

2.4. Wszystkie interfejsy liniowe zainstalowane w Routerze (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

2.5. Router musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.6. Router musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP). Pojedynczy interfejs zagregowany musi składać się z ośmiu interfejsów składowych, przy czym nie może być ograniczeń co do lokalizacji tych interfejsów na kartach interfejsów (dla urządzeń modularnych), zaś dla urządzeń wirtualnych zbudowanych z wielu urządzeń składowych musi być zapewniona możliwość składania interfejsów umieszczonych w różnych urządzeniach fizycznych (MC-LAG).

2.7. Znaczenie pola VID (VLAN ID) musi mieć znaczenie lokalne dla interfejsu fizycznego, co oznacza, że ten sam znacznik VID może być użyty niezależnie na wielu interfejsach fizycznych urządzenia.

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1. Cała konfiguracja Routera musi być zapisywana do pojedynczego pliku tekstowego.

Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2. Router musi zapewniać minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji),

3.1.3. Router musi zapewniać możliwość cofnięcia zmian konfiguracji,

3.1.4. Router musi zapewniać możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

3.1.5. Router musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

3.1.6. CLI Routera (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Router musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności

[2] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Router musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Router musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.4.2. Router musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób nie powodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruchu dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- statystyki ruchu dla ścieżek LSP,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Router musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Router musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.).

3.7. Router musi wspierać wysyłanie (np. gRPC lub OpenConfig), informacji takich jak:

- statystyki ruchu dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- statystyki ruch dla interfejsów logicznych,
- statystyki ruchu dla ścieżek LSP,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.8. Router nie może wprowadzać ograniczeń na dostęp dowolnych systemów OSS do urządzenia (dotyczy to także systemów OSS nie oferowanych w ramach niniejszego postępowania), przy wykorzystaniu dowolnego protokołu (w szczególności SNMP i NETCONF). Jeżeli urządzenie wymaga dodatkowych licencji zapewniających taki dostęp, to licencje te muszą być uwzględnione w ofercie.

3.9. Router musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.10. Router musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.11. Na Routerze musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.12. Router musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.12.1. Router musi mieć zaimplementowany mechanizm ISSU (In Service Software Upgrade) zapewniający aktualizację oprogramowania bez przerywania pracy urządzenia (dopuszczalna jest przerwa w pracy kart liniowych nie dłuższa niż 0,5s nie wpływająca na działanie protokołów routingu).

3.13. Router musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.14. Router musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

3.15. Router musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.16. Router musi obsługiwać protokół NTP.

3.17. Router musi obsługiwać automatyczną ochronę modułów sterujących przed atakami typu DDoS (Distributed Denial of Service). Funkcjonalność musi pozwalać na odrzucanie (pomijanie) pakietów sterujących (np. związanych z protokołami i mechanizmami działającymi na module sterującym) kierowanych do modułu sterującego, których ilość przekracza założony próg. Router musi zapewniać możliwość konfiguracji parametrów mechanizmu ochrony DDoS dla poszczególnych protokołów (np. ograniczenie wielkości ruchu) oraz rejestrować wystąpienie zdarzeń związanych z działaniem tego mechanizmu (takich jak: czas wystąpienia ostatniego przekroczenia parametrów, czas trwania przekroczenia, liczbę pakietów odebranych, liczbę pakietów odrzuconych).
Włączenie mechanizmu ochrony DDoS nie może skutkować wykluczeniem, ograniczeniem lub pogorszeniem jakichkolwiek wymaganych przez Zamawiającego parametrów funkcjonalnych, wydajnościowych i eksploatacyjnych.

3.18. Router musi obsługiwać IPFIX lub NetFlow (wersje 5 i 9) dla IPv4, IPv6, MPLS z granularnym sterowaniem próbkowaniem od 1:1 do 1:10000.

3.19. Router musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.19.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list kontroli dostępu.

3.19.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.

3.19.3. Router musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.19.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

3.20. Router musi obsługiwać mechanizm lokalizacji uszkodzeń w sieci na podstawie IEEE 802.1ag (Connectivity Fault Management), ITU-T Y.1731 Fault Monitoring, ITU-T Y.1731 Performance Monitoring.

3.21. Router musi obsługiwać mechanizm wykrywania uszkodzeń (ang. Connectivity Fault Management) dla poszczególnych instancji VPLS zgodny ze standardem IEEE 802.1ag.

3.22. Router musi mieć zaimplementowaną funkcjonalność MPLS OAM, która pozwala na wykonanie sprawdzenia poprawności działania ścieżki LSP (ang. LSP ping) oraz jej trasy (ang. LSP traceroute). Funkcje te muszą być dostępne zarówno dla ścieżek zestawianych przy pomocy protokołu LDP jak i RSVP.

3.23. Dla usług IP VPN urządzenie musi obsługiwać funkcje ping i traceroute dla każdej z sieci wirtualnych.

4. Architektura Routera Szkieletowego
   4.1. Router musi mieć architekturę modularną. Za urządzenie modularne Zamawiający uznaje urządzenie, który umożliwia rozbudowę o nowe, dodatkowe lub wymianę istniejących na nowsze elementy składowe, poprzez ich instalację w odpowiednich slotach przeznaczonych na moduły sprzętowe, takie jak np. interfejsy liniowe, matryce przełączające, karty procesorowe, itd. Nie dotyczy to wymiennych wkładek optycznych.
      4.1.1. Każdy oferowany Router musi dysponować takim wyposażaniem, aby wszystkie elementy istotne z punktu widzenia pracy urządzenia miały nadmiarowość (jako elementy istotne Zamawiający uznaje m.in. wszystkie elementy konieczne dla prawidłowej pracy urządzenia, tj. zasilacze, wentylatory, karty procesorowe, matryce przełączające, itd., z wyłączeniem kart interfejsów liniowych). Wszystkie elementy mogące mieć zainstalowane elementy nadmiarowe muszą być w nie wyposażone. Wykonawca przedstawi sposób realizacji wymogu nadmiarowości w oferowanych urządzeniach w ramach Opisu rozwiązania, wg Załącznika nr 11 do Zapytania Ofertowego.
      4.1.2. W przypadku przełączenia na zapasowe elementy (matryce przełączające, karty procesorowe) konieczne jest zachowanie ciągłej pracy protokołów routingu (ISIS, OSPFv2, OSPFv3, RSVP-TE, LDP, BGP dla wszystkich obsługiwanych AFI/SAFI), tj. utrzymanie sesji z wszystkimi sąsiadami w sensie tych protokołów routingu. Funkcjonalność ta musi być realizowana przy wykorzystaniu wewnętrznych mechanizmów urządzenia.
   4.2. Architektura Routera musi zapewniać przełączanie pakietów pomiędzy dowolnymi dwoma interfejsami bez żadnych ograniczeń wydajnościowych przy założeniu obsadzenia urządzenia wszystkimi wymaganymi interfejsami.
      4.2.1. Jeżeli karty interfejsów liniowych mają ograniczenia wydajnościowe (nadsubskrypcja), to do ilości interfejsów wymaganych liczone mogą być tylko interfejsy zapewniające pracę bez ograniczeń wydajnościowych. Pozostałe interfejsy, mimo że nie są zaliczane do interfejsów wymaganych, nie mogą mieć wprowadzonych żadnych blokad (muszą być dostępne do wykorzystania bez konieczności zakupu dodatkowych licencji, itd.).

4.3. Zamawiający dopuszcza, aby interfejsy 1GE były zainstalowane na modułach wyniesionych.

4.3.1. Użycie modułów wyniesionych nie może wpływać na skalowanie Routera Szkieletowego, a w szczególności (choć nie wyłącznie) na pojemność tablic routingu.

4.3.2. Wszystkie moduły wyniesione używane przez Routery Szkieletowe musza być tego samego typu.

5. Wymagane funkcjonalności routingu IP:
   5.1. Router musi obsługiwać IPv4 oraz IPv6 (routing statyczny, BGP, OSPF, ISIS), przy czym rozkład ruchu pomiędzy oba protokoły (tj. IPv4 i IPv6) nie może wpływać na funkcjonalność ani wydajność Routera,
      5.1.1. Obsługa IPv4 oraz IPv6 musi być możliwa bez żadnych ograniczeń co do interfejsów.
      5.1.2. Dla protokołu BGP konieczna jest obsługa 4 bajtowych ASN,

5.1.3. Dla protokołu BGP wymagana jest konieczność zestawienia nie mniej niż 500 sesji eBGP, w tym wielu sesji do jednego AS zewnętrznego,

5.2. Router musi obsługiwać multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP),

5.3. Router musi obsługiwać multicast IPv6 (MLD, PIM SM, SSM),

5.4. Router musi obsługiwać Policy Based Routing (PBR) (kierowanie pakietów na podstawie innych kryteriów niż adres docelowy),

5.5. Router musi obsługiwać Bidirectional Forwarding Detection (BFD) min. dla OSPFv2/3, ISIS, BGP, routingu statycznego, LDP, dla interfejsów fizycznych oraz interfejsów logicznych, dla IPv4 oraz IPv6,

5.6. Router musi obsługiwać NonStop Forwarding (dla protokołów: BGP, OSPF, IS-IS, MPLS-TE, LDP, VPLS, multicast),

5.7. Urządzenie musi obsługiwać VRRP dla IPv4 i IPv6,

5.8. Router musi obsługiwać mechanizm multi-VRF, umożliwiający utrzymywanie oddzielnych tablic routingu (ang. Virtual Routing and Forwarding) dla sieci wirtualnych,

5.9. Router musi obsługiwać IP FRR z LFA (co najmniej dla protokołów ISIS i OSPF dla IPv4 i IPv6).

5.10. Router musi obsługiwać uRPF dla IPv4 i IPv6

6. Funkcjonalności przełączania MPLS:

6.1. Router musi mieć możliwość pracy jako router brzegowy LER (ang. Label Edge Router) oraz szkieletowy LSR (ang. Label Switch Router),

6.2. Router musi obsługiwać LDP, targeted LDP, RSVP-TE,

6.3. Router musi obsługiwać VPLS,

6.4. Router musi obsługiwać VPWS,

6.5. Router musi obsługiwać MPLS L3VPN (IPv4 i IPv6),

6.6. Router musi obsługiwać EVPN (L2/L3),

6.7. Router musi obsługiwać Multicast VPN dla IPv4 i IPv6,

6.8. Router musi obsługiwać MPLS TE (z mechanizmami ochrony ścieżki – path protection),

6.9. Router musi obsługiwać mechanizm MPLS Fast ReRoute (FRR),

6.10. Router musi obsługiwać ścieżki w trybie adaptacyjnym, umożliwiającym zmianę parametrów ścieżki (zmiana ścieżki podstawowej, zmiana deklaracji pasma) bez konieczności jej rozłączania (mechanizm make before break),

6.11. Router musi obsługiwać mechanizmy SRLG, wymuszające zestawianie alternatywnych/ backupowych połączeń LSP (ang. Label Switched Path) inną drogą niż ścieżki podstawowe

7. Funkcjonalności Segment Routing:

7.1. Router musi mieć możliwość wykorzystania mechanizmów transportowych MPLS i IPv6 (SRv6) (IPv6 opcjonalnie),

7.2. Router musi obsługiwać SR dla OSPF, ISIS, BGP,

7.3. Router musi obsługiwać alokację etykiet w modelach SRGB, SRLB,

7.4. Router musi obsługiwać SR-TE (Traffic engineering), TI-LFA (Topology Independent Loop Free Alternate),

7.5. Router musi obsługiwać funkcjonalności PCE, mapping server, mapping client,

7.6. Router musi obsługiwać SR OAM (ping, traceroute).

4.1.1. Wymagania na ilość interfejsów dla Routerów Szkieletowych

Węzły Szkieletowe w chwili instalacji połączone zostaną łączami 10GE, które w miarę wzrostu ruchu w sieci będą rozbudowywane do łącz n * 10GE ($n \leq 5$), a następnie 100GE i 2 * 100GE.

Wszystkie interfejsy do zapewnienia łączności pomiędzy Węzłami, wg powyższego modelu, muszą być zainstalowane do urządzeń (wymagane jest, aby w ofercie uwzględnić wkładki optyczne w standardzie 10GBase-LR lub 100GBase-LR4).

Ilość interfejsów do Węzłów Agregacyjnych należy wyliczyć zgodnie z wytycznymi podanymi w pkt. 5 „Wymagania dla Węzła Agregacyjnego", ppkt. „Inne wymagane parametry wydajnościowe dla Routerów Agregacyjnych".

W każdym z Routerów należy założyć styki do operatorów zewnętrznych oferujących wymianę ruchu, a także do zewnętrznych dostawców treści edukacyjnych. Wymagane ilości interfejsów są następujące:

węzeł	**ilość interfejsów**			
	100GE	40GE	10GE	1GE
WAW-Core	15	6	15	10
POZ-Core	6	2	10	10
KAT-Core	8	4	10	10

Wszystkie podane interfejsy muszą być obsadzone wkładkami optycznymi w standardzie 1000Base-LX, 10GBase-LR, 40GBase-LR4 lub 100GBase-LR4.

Zaoferowane Routery muszą mieć możliwość rozbudowy w przyszłości o interfejsy 400GE, w momencie ich dostępności komercyjnej w postaci kart liniowych, bez konieczności wymiany obudowy, matryc przełączających ani kart procesorowych. Dostawa kart z interfejsami 400GE jest poza zakresem niniejszego postępowania.

Dodatkowo, w każdym z Routerów Szkieletowych należy zapewnić 2 interfejsy 40GE lub 8 interfejsów 10GE na styk do chmury prywatnej OSE, obsługującej systemy OSS/BSS sieci OSE. Interfejsy te muszą być umieszczone na dwóch różnych kartach interfejsów (w przypadku interfejsów 10GE nie więcej niż cztery na jednej karcie).

Wszystkie te interfejsy muszą być obsadzone wkładkami optycznymi w standardzie 40GBase-SR4 lub 10GBase-SR.

Pozostałe wymagane parametry wydajnościowe są następujące:

4.1.2. Inne wymagania wydajnościowe dla Routerów Szkieletowych

8. Router musi obsługiwać co najmniej 2 000 000 prefiksów IPv4 oraz 1 000 000 prefiksów IPv6 (jednocześnie). Wszystkie prefiksy muszą być używane do przełączania ruchu - tzn. zainstalowane w bazie FIB (ang. Forwarding Information Base).
   8.1. Ilość prefiksów przechowywanych w tablicy RIB (Routing Information Base) to 5 000 000 prefiksów IPv4 i 3 000 000 prefiksów IPv6 (jednocześnie).
9. Router musi obsługiwać co najmniej 2 000 sieci VPLS.
   9.1. Router musi obsługiwać nie mniej niż 256 000 adresów MAC zarejestrowanych w sieciach VPLS
10. Router musi obsługiwać jednocześnie co najmniej 16 000 grup multicast dla IPv4 oraz 16 000 grup multicast dla IPv6.
11. Router musi obsługiwać co najmniej 50 000 tranzytowych ścieżek LSP (RSVP-TE).
12. Router musi obsługiwać co najmniej 12 000 źródłowych ścieżek LSP (RSVP-TE head-end).
13. Router musi obsługiwać co najmniej 12 000 zakończeń ścieżek LSP (RSVP-TE egress).
14. Router musi obsługiwać co najmniej 1 000 sesji LDP typu targeted.
15. Router musi obsługiwać co najmniej 4 000 połączeń L2VPN, nie wliczając do tego sieci VPLS.

16. Router musi obsługiwać co najmniej 2 000 sieci L3VPN.

4.2. Wymagania dla Route Reflectorów

W sieci OSE zainstalowane będą dwa Route Reflectory (RR), zapewniające spójną sygnalizację BGP w całej sieci.

Wykonawca musi dostarczyć RR w jednym z dwóch wariantów:

- jako urządzenia wirtualne,
- jako dedykowane urządzenia fizyczne.

Route Reflectory będą zainstalowane docelowo w węzłach WAW Core i KAT Core. W przypadku dedykowanych urządzeń, Wykonawca musi zapewnić dodatkowe interfejsy (co najmniej jeden interfejs 1GE lub szybszy) do połączenia Routerów Szkieletowych z RR.

W każdym z wypadków, RR muszą wykorzystywać to samo oprogramowanie co Routery Szkieletowe lub Routery Agregacyjne (dopuszczalne jest ograniczenie wydajnościowe oprogramowania, rozumiane jako ograniczenie możliwości przesyłania ruchu bez ograniczeń w sygnalizacji, ze względu na umieszczenie RR poza ścieżką przesyłania ruchu).

Wymagania dla Route Reflectorów:

1. RR musi wspierać sygnalizację BGP dla: IPv4 (unicast i multicast), IPv6 (unicast i multicast), MPLS, L3VPN, L2VPN, EVPN.
2. Pojemność tablicy routingu (RIB): 16 000 000 prefixów.
3. W przypadku maszyny wirtualnej możliwość instalacji na wirtualizatorze ESXi.
4. Dla dedykowanego urządzenia fizycznego:
   - 4.1. Urządzenie musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
     - 4.1.1. Urządzenie musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja Urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych profili zginania przewodów.
   - 4.2. Urządzenie musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.
   - 4.3. Dostarczone zasilacze muszą umożliwiać dołączenie urządzenia do dwóch niezależnych obwodów zasilających (dwa zestawy paneli zasilających) oraz poprawną pracę urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełniej funkcjonalności urządzenia.
   - 4.4. Dostarczone urządzenie musi umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu jednego zasilacza.
   - 4.5. Urządzenie musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.
   - 4.6. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.
   - 4.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być

wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

4.8. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

4.8.1. Karty liniowe lub moduły urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów[3]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na urządzenie ani ograniczeń w świadczeniu usług serwisowych.

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

4.8.2. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)4 zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

4.8.3. Wszystkie interfejsy liniowe zainstalowane w urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

4.8.4. Urządzenie musi posiadać port terminalowy do dołączenia konsoli (RS-232).

4.8.5. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

4.8.6. Urządzenie musi obsługiwać automatyczną ochronę modułów sterujących przed atakami typu DDoS (Distributed Denial of Service). Funkcjonalność musi pozwalać na odrzucanie (pomijanie) pakietów sterujących (np. związanych z protokołami i mechanizmami działającymi na module sterującym) kierowanych do modułu sterującego, których ilość przekracza założony próg. Przełącznik musi zapewniać możliwość konfiguracji parametrów mechanizmu ochrony DDoS dla poszczególnych protokołów (np. ograniczenie wielkości ruchu) oraz rejestrować wystąpienie zdarzeń związanych z

[3] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji urządzenia, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[4] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

działaniem tego mechanizmu (takich jak: czas wystąpienia ostatniego przekroczenia parametrów, czas trwania przekroczenia, liczbę pakietów odebranych, liczbę pakietów odrzuconych).

Włączenie mechanizmu ochrony DDoS nie może skutkować wykluczeniem, ograniczeniem lub pogorszeniem jakichkolwiek wymaganych przez Zamawiającego parametrów funkcjonalnych, wydajnościowych i eksploatacyjnych.

4.3. Wymagania na Oprogramowanie System Zarządzania

Oprogramowanie umożliwiające zarządzanie dostarczanymi Urządzeniami (nazywane także Element Manager), zgodnie z przedstawionymi poniżej wymaganiami funkcjonalnymi. Oprogramowanie, dedykowane dla określonej rodziny urządzeń, musi być kompatybilne z każdym Urządzeniem danego rodzaju występującym w Węźle Szkieletowym lub w Węźle Agregacyjnym (z wyłączeniem serwera terminalowego sieci zarządzania).

Wymagania:

1. System zarządzania musi mieć możliwość pracy jako maszyna wirtualna uruchamiana na jednym z wirtualizatorów: ESXi, Hyper-V, KVM lub XEN.
2. Licencja dostarczona wraz z Systemem zarządzania musi umożliwiać równoczesne działanie co najmniej 2 maszyn wirtualnych w trybie wysokiej dostępności, tak aby awaria wyłączająca jedną z maszyn wirtualnych nie powodowała przerwy w działaniu systemu zarządzania.
3. System zarządzania musi obsługiwać uwierzytelnianie i autoryzację użytkowników z wykorzystaniem zewnętrznego serwera (TACACS+ lub RADIUS) lub licencja dostarczona wraz z Systemem zarządzania musi zapewnić możliwość zarejestrowania nie mniej niż 200 unikalnych użytkowników.
4. System zarządzania musi zapewniać możliwość tworzenia i różnicowania poziomów dostępu użytkowników. Różnicowanie musi umożliwić co najmniej:
   4.1. przydzielanie użytkownikom dostępu do poszczególnych modułów (funkcji) systemu zarządzania poprzez przypisywanie ról użytkownikom,
   4.2. korzystanie z predefiniowanych i własnych ról użytkowników (np. administrator, operator).
5. System zarządzania musi obsługiwać jednoczesną pracę wielu użytkowników bez spadku wydajności. Liczba użytkowników korzystających jednocześnie z platformy systemu zarządzania nie może być mniejsza niż 50.
6. Interfejs użytkownika Systemu zarządzania musi być dostępny z poziomu przeglądarki WWW. Dopuszczalne jest stosowanie dedykowanej aplikacji klienckiej, przy założeniu że dostarczona licencja nie ogranicza ilości pobranych i zainstalowanych aplikacji, zaś aplikacja jest dostępna na platformy systemowe używane na stacjach roboczych używanych przez Zamawiającego. Zamawiający informuje, że na stacjach roboczych używa platform systemowych Microsoft Windows oraz Linux.
   6.1. Cała komunikacja pomiędzy system zarządzania a przeglądarką administratora musi odbywać się przez połączenie szyfrowane (np. przy wykorzystaniu protokołu HTTPS).
   6.2. Interfejs użytkownika Systemu musi być dostępny w polskiej lub angielskiej wersji językowej.
7. Licencja dostarczona wraz z systemem zarządzania musi zapewnić zarządzanie wszystkimi Urządzeniami dostarczonymi w ramach niniejszego postępowania (z wyłączeniem serwera terminalowego sieci zarządzania).

8. System zarządzania musi zapewniać podgląd stanu komponentów monitorowanych urządzeń (m.in. interfejsy, moduły, zasilacze).
9. System zarządzania musi zapewniać monitorowanie awarii i pokazywanie aktualnych alarmów. Minimalny wymagany zakres alarmów to:
   - awaria któregokolwiek elementu urządzenia monitorowanego,
   - awaria łącza,
   - przekroczenie zadanego poziomu obciążenia łącza, CPU, RAM urządzenia
   - przekroczenie warunków środowiskowych, a w szczególności temperatury urządzenia, temperatury powietrza chłodzącego, braku zasilania na jednym lub wielu zasilaczach.
10. System zarządzania musi zapewniać wywołanie komend diagnostycznych dla wybranej grupy Urządzeń (routerów), co najmniej w zakresie przełączania IPv4/IPv6 oraz MPLS i protokołów sygnalizacyjnych (takich jak BGP, ISIS, OSPF, LDP, RSVP)
11. System zarządzania musi zapewniać archiwizację i wersjonowanie plików konfiguracyjnych (a także ich eksport w postaci pliku tekstowego (ang. plain text) lub w formacie XML lub JSON o ile zarządzane urządzenia wykorzystują te formaty do zapisu konfiguracji) oraz dystrybucję (w tym aktualizację) Oprogramowania na Urządzenia.
12. System zarządzania musi zapewniać zarządzanie (tworzenie, modyfikacja i usuwanie) wszystkimi elementami usługi realizowanej w z wykorzystaniem technologii MPLS (ang. end-to-end), takimi jak definicja usługi, zarządzanie punktami końcowymi oraz mechanizmami transportowymi.
13. System zarządzania musi zapewniać odbieranie komunikatów SNMP trap z zarządzanych Urządzeń.
14. System zarządzania musi zapewniać odbieranie logów systemowych przesyłanych przez protokół syslog z zarządzanych Urządzeń.
15. System zarządzania musi zapewniać tworzenie, usuwanie i edycję szablonów konfiguracji oraz ich późniejsze wykorzystanie.
16. System zarządzania musi zapewniać zakładanie pomiarów na „shadow routerach".
17. System zarządzania musi zapewniać pobieranie wyników pomiarów z „shadow routerów" i prezentowanie ich w formie statystyk.
18. System zarządzania musi zapewnić integrację z nadrzędnym systemem zarządzania Zamawiającego poprzez standardowe protokoły i otwarte mechanizmy integracyjne. W szczególności system zarządzania musi umożliwiać Zamawiającemu integrację z systemem zarządzania poprzez API (co najmniej REST API, pliki płaskie), do którego producent udostępnia dokumentację.
    18.1. API (podobnie ja same urządzenia) musi umożliwiać przekazywanie do systemu nadrzędnego informacji o alarmach.
    18.2. API (podobnie jak same urządzenia) musi umożliwiać przekazywanie informacji inwentarzowych.
    18.3. API (podobnie jak same urządzenia) musi umożliwiać przekazywanie konfiguracji urządzeń.
    18.4. API musi umożliwiać provisioning konfiguracji usług co najmniej w zakresie:
        18.4.1. konfiguracji parametrów L2 interfejsu (pojedynczy VLAN albo podwójne tagowanie – QinQ),
        18.4.2. konfiguracji adresacji IPv4 / IPv6 na interfejsie (adresy połączeniowe),
        18.4.3. konfiguracji routingu statycznego w stronę szkoły oraz community dla tych adresów (przy redystrybucji do BGP),
        18.4.4. konfiguracji QoS na łączu (policer, shaper, RED),
    18.5. API musi umożliwiać zakładanie pomiarów na shadow routerach,

18.6. API musi umożliwiać cykliczne pobieranie wyników pomiarów (zakładanych na „shadow routerach") do Centralnego Systemu Raportowego (export raw / aggregated data),

18.7. API musi umożliwiać cykliczne pobieranie raportów z wynikami pomiarów zakładanych na shadow routerach w postaci plików graficznych lub w formacie JSON lub XML.

19. System zarządzania musi umożliwiać tworzenie za pomocą interfejsu graficznego (typu web) wzorców usług typu: VPLS (w topologiach hub&spoke oraz full mesh), L3 VPN (w topologiach hub&spoke oraz full mesh)

4.4. Wymagania dla urządzeń typu „shadow router"

W sieci OSE zaimplementowany zostanie system pomiarów jakości usług. Oparty on zostanie o mechanizm badania jakości sieci w oparciu o wykorzystanie shadow routerów oraz mechanizm klasy IP SLA / RPM / NQA / SAA lub równoważny.

Shadow routery to dedykowane urządzenia, dołączone bezpośrednio do Routerów Agregacyjnych lub Szkieletowych emulujące urządzenia abonenckie (CPE). Z urządzeń tych wysyłane będą próbki testujące podstawowe parametry definiujące jakość usług sieciowych, tj. opóźnienia, straty pakietów, jitter. Do jednego Routera Agregacyjnego lub Szkieletowego będzie dołączony jeden shadow router interfejsem 1GE, ze stykiem fizycznym 1000Base-SX lub 1000Base-T (do wyboru Wykonawcy).

1. Wymagania ogólne
   1.1. Wszystkie oferowane urządzenia (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
      1.1.1. Wykonawca musi być oficjalnym sprzedawcą w Polsce oferowanych urządzeń.
      1.1.2. Wykonawca musi mieć możliwość świadczenia autoryzowanego przez producenta serwisu gwarancyjnego.
   1.2. Zamawiający wymaga, aby urządzenia shadow router były jednego typu, w jednakowej konfiguracji we wszystkich Węzłach Szkieletowych i Agregacyjnych.
   1.3. Urządzenie musi być przystosowane do instalacji w standardowych 19" szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
      1.3.1. Urządzenie musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   1.4. Urządzenie musi być wyposażone w co najmniej jeden zasilacz dostosowany do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.
   1.5. Urządzenie musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.
   1.6. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.
   1.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

1.8. Dokumentacja do Urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

2. Wymagania na interfejsy

2.1. Karty liniowe lub moduły Urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów[5]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na Urządzenie ani ograniczeń w świadczeniu usług serwisowych

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu Urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.2. Dostarczone moduły optyczne (o ile Urządzenie jest w nie wyposażone) muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)[6] zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

2.3. Urządzenie musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

2.4. Wszystkie interfejsy liniowe zainstalowane w Urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym Urządzeniu.

2.5. Znaczenie pola VID (VLAN ID) musi mieć znaczenie lokalne dla interfejsu fizycznego, co oznacza, że ten sam znacznik VID może być użyty niezależnie na wielu interfejsach fizycznych Urządzenia.

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2. Urządzenie musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

[5] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji Urządzenia, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[6] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

3.1.3. CLI Urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Urządzenie musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Urządzenie musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.4.2. Urządzenie musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób nie powodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruch dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- [usunięto]
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie Urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.7. Urządzenie musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.8. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.9. Urządzenie musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.10. Urządzenie musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.11. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

3.12. Urządzenie musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.13. Urządzenie musi obsługiwać protokół NTP.

3.14. Urządzenie musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.14.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

3.14.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 50 wpisów każda.

3.14.3. Urządzenie musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.14.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

4. Wymagane funkcjonalności routingu IP:
   4.1. Urządzenie musi obsługiwać IPv4 oraz IPv6 przy czym rozkład ruchu pomiędzy oba protokoły (tj. IPv4 i IPv6) nie może wpływać na funkcjonalność urządzenia,
   4.1.1. Obsługa IPv4 oraz IPv6 musi być możliwa bez żadnych ograniczeń co do interfejsów.
   4.2. Urządzenie musi obsługiwać mechanizm multi-VRF, umożliwiający utrzymywanie oddzielnych tablic routingu (ang. Virtual Routing and Forwarding) dla sieci wirtualnych,
   4.2.1. Urządzenie musi umożliwiać utworzenie i jednoczesne działanie nie mniej niż 8 VRF.
5. Wymagania na pomiary
   5.1. Urządzenie musi wspierać mechanizm IP SLA lub RPM lub NQA lub SAA lub równoważny.
   5.2. Urządzenie musi umożliwiać pomiar następujących parametrów:
      5.2.1. opóźnienie (RTT),
      5.2.2. straty pakietów,
      5.2.3. jitter.
   5.3. Urządzenie musi umożliwiać próbkowanie przy pomocy protokołów:
      5.3.1. ICMP,
      5.3.2. TCP,
      5.3.3. UDP,
      5.3.4. HTTP (pobranie strony WWW z podanego adresu),
      5.3.5. DNS (wysłanie zapytania DNS – UDP/53 lub UDP-ECHO na port docelowy 53).
   5.4. Wszystkie wymienione powyżej pomiary (w pkt. 5.2 i 5.3) muszą być wykonywane dla IPv4 i IPv6.
   5.5. Urządzenie musi mieć możliwość oznaczania pakietów używanych do próbkowania zadanymi wartościami DSCP;
   5.6. Urządzenie musi mieć możliwość wykonywania cyklicznych pomiarów. Pomiar musi być wykonywany nie rzadziej niż raz na 5 minut.
   5.7. Urządzenie musi mieć możliwość badania wszystkich parametrów wewnątrz dowolnego VRF.
   5.8. Urządzenie musi umożliwiać jednoczesne pomiary w co najmniej 8 VRF.

5. Wymagania dla Węzła Agregacyjnego

Podstawowym zadaniem 16 Węzłów Agregacyjnych będzie agregacja łączy dostępowych do szkół w celu dostarczenia usług OSE oraz przesyłania ruchu ze szkół do Regionalnego Węzła Bezpieczeństwa, a następnie do Węzłów Szkieletowych, w celu przesłania do sieci Internet (oraz analogiczna obsługa ruchu powracającego z Internetu do szkół). Węzły Agregacyjne będą dostarczane w formie kompletów Urządzeń wraz z Oprogramowaniem. Każdy z Węzłów Agregacyjnych będzie dostarczany, instalowany oraz uruchamiany i konfigurowany i odbieranych (testy odbiorcze) niezależnie od pozostałych węzłów sieci. Łącza szkieletowe, pomiędzy Węzłami Agregacyjnymi, a węzłami Szkieletowymi będą dostarczane przez Zamawiającego.

W skład Węzeł Agregacyjnego wchodzi:

- Router Agregacyjny,
- Przełączniki Sieci Lokalnej (wymagania dla przełączników opisane są w pkt 5.3),
- urządzenia sieci zarządzania (wymagania dla urządzeń sieci zarządzania opisane są w pkt 5.4),
- Shadow Routery (wymagania dla Shadow Routerów opisane są w pkt 5.5).

W ramach wdrożenia należy przyjąć, że wdrożenie węzła oznacza wdrożenie urządzeń z każdej z wymienionych grup na zasadach opisanych poniżej.

5.1. Wymagania dla Routerów Agregacyjnych

Router Agregacyjny jest Systemem Urządzeń (w szczególności jednym Urządzeniem) zainstalowanym w Węźle Agregacyjnym spełniającym następujące wymagania:

1. Wymagania ogólne
   - 1.1. Wszystkie oferowane Routery Agregacyjne (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
   - 1.2. Routery Agregacyjne, dostarczane w ramach Umowy do poszczególnych Węzłów, mogą być różnych modeli, zależnie od wielkości Węzła. Ilość modeli Routerów Agregacyjnych nie może być większa dwa.
     - 1.2.1. W przypadku oferowania Urządzeń modularnych dopuszczalne jest różne wyposażenie urządzeń w karty interfejsów liniowych, przy czym wskazane jest, aby do wyposażenia Urządzeń w różnych węzłach użyta była jak najmniejsza ilość modeli kart interfejsów.
     - 1.2.2. Dopuszczalne jest użycie dodatkowego typu Routera Agregacyjnego dla węzłów WAW i KAT. Router ten musi mieć wymienne karty interfejsów z pozostałymi typami Routerów Agregacyjnych.
   - 1.3. Router musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297).
     - 1.3.1. Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
     - 1.3.2. Router musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   - 1.4. Router musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone Urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.
     - 1.4.1. Dostarczone zasilacze muszą umożliwiać dołączenie Urządzenia do dwóch niezależnych obwodów zasilających (dwa zestawy paneli zasilających) oraz poprawną pracę urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełniej funkcjonalności urządzenia.
     - 1.4.2. Dostarczone urządzenie musi umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu jednego zasilacza.
     - 1.4.3. Maksymalny pobór mocy Routerów Agregacyjnych nie może przekroczyć poniższych wartości:

węzeł	**maksymalny pobór prądu**
WAW	15 kW

KAT	15 kW
POZ	15 kW
WRO	14 kW
TOR	14 kW
LUB	14 kW
ZGO	14 kW
LOD	14 kW
KRA	14 kW
OPO	14 kW
RZE	14 kW
BIA	14 kW
GDA	14 kW
KIE	14 kW
OLS	14 kW
SZC	14 kW

1.5. Router musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.

1.6. Router musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

1.7. Router musi umożliwiać możliwość instalacji, wymiany lub zamiany poszczególnych modułów (takich jak np. zasilacze, wentylatory, karty z interfejsami sieciowymi, moduły optyczne typu SFP / XFP / itd.) w trakcie pracy urządzenia (ang. hot-swap).

1.8. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

1.9. Oprogramowanie urządzenia musi być modularne, co oznacza że poszczególne funkcjonalności (np. routing, SNMP, itd.) są obsługiwane przez oddzielne procesy. Musi istnieć możliwość restartu pojedynczego procesu, bez wpływu na inne procesy.

1.10. Dokumentacja do Urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

2. Wymagania na interfejsy

2.1. Karty liniowe lub moduły urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów[7]. Instalacja modułów optycznych pochodzących od

[7] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji Routera, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na Urządzenie ani ograniczeń w świadczeniu usług serwisowych

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu Routera ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego Urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.2. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)8 zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

2.3. Router musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

2.4. Wszystkie interfejsy liniowe zainstalowane w Routerze (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym Urządzeniu.

2.5. Router musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.6. Router musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP). Pojedynczy interfejs zagregowany musi składać się z ośmiu interfejsów składowych, przy czym nie może być ograniczeń co do lokalizacji tych interfejsów na kartach interfejsów (dla urządzeń modularnych), zaś dla urządzeń wirtualnych zbudowanych z wielu urządzeń składowych musi być zapewniona możliwość składania interfejsów umieszczonych w różnych Urządzeniach (MC-LAG).

2.7. Znaczenie pola VID (VLAN ID) musi mieć znaczenie lokalne dla interfejsu fizycznego, co oznacza, że ten sam znacznik VID może być użyty niezależnie na wielu interfejsach fizycznych urządzenia.

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1. Cała konfiguracja Routera musi być zapisywana do pojedynczego pliku tekstowego. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2. Router musi zapewniać minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji).

3.1.3. Router musi zapewniać możliwość cofnięcia zmian konfiguracji.

3.1.4. Router musi zapewniać możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

3.1.5. Router musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

[8] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

3.1.6. CLI Routera (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Router musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Router musi wspierać RADIUS Accounting zgodnie z RFC2866, umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Router musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.4.2. Router musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób niepowodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruch dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- statystyki ruchu dla ścieżek LSP,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.7. Urządzenie musi wspierać wysyłanie, bez pośrednictwa modułów zarządzających (np. gRPC lub OpenConfig), informacji takich jak:

- statystyki ruch dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- statystyki ruchu dla ścieżek LSP,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.8. Router nie może wprowadzać ograniczeń na dostęp dowolnych systemów OSS do Urządzenia (dotyczy to także systemów OSS nieoferowanych w ramach niniejszego postępowania), przy wykorzystaniu dowolnego protokołu (w szczególności SNMP i NETCONF). Jeżeli Urządzenie wymaga dodatkowych licencji zapewniających taki dostęp, to licencje te muszą być uwzględnione w ofercie.

3.9. Router musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.10. Router musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.
3.11. Na Routerze musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).
3.12. Router musi mieć możliwość zdalnej aktualizacji oprogramowania.
    3.12.1. Router musi mieć zaimplementowany mechanizm ISSU (In Service Software Upgrade) zapewniający aktualizację oprogramowania bez przerywania pracy Urządzenia (dopuszczalna jest przerwa w pracy kart liniowych nie dłuższa niż 0,5s niewpływająca na działanie protokołów routingu).
3.13. Router musi posiadać port terminalowy do dołączenia konsoli (RS-232).
3.14. Router musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie Urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).
3.15. Router musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez Urządzenie zdarzeniach do zdalnego serwera syslog.
3.16. Router musi obsługiwać protokół NTP.
3.17. Router musi obsługiwać automatyczną ochronę modułów sterujących przed atakami typu DDoS (Distributed Denial of Service). Funkcjonalność musi pozwalać na odrzucanie (pomijanie) pakietów sterujących (np. związanych z protokołami i mechanizmami działającymi na module sterującym) kierowanych do modułu sterującego, których ilość przekracza założony próg. Przełącznik musi zapewniać możliwość konfiguracji parametrów mechanizmu ochrony DDoS dla poszczególnych protokołów (np. ograniczenie wielkości ruchu) oraz rejestrować wystąpienie zdarzeń związanych z działaniem tego mechanizmu (takich jak: czas wystąpienia ostatniego przekroczenia parametrów, czas trwania przekroczenia, liczbę pakietów odebranych, liczbę pakietów odrzuconych).
    Włączenie mechanizmu ochrony DDoS nie może skutkować wykluczeniem, ograniczeniem lub pogorszeniem jakichkolwiek wymaganych przez Zamawiającego parametrów funkcjonalnych, wydajnościowych i eksploatacyjnych.
3.18. Router musi obsługiwać IPFIX lub NetFlow (wersje 5 i 9) dla IPv4, IPv6, MPLS z granularnym sterowaniem próbkowaniem od 1:1 do 1:10000.
3.19. Router musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.
    3.19.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.
    3.19.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.
    3.19.3. Router musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.
    3.19.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. Router musi umożliwiać aktywacje obu typów na interfejsie logicznym.
3.20. Router musi obsługiwać mechanizm lokalizacji uszkodzeń w sieci na podstawie IEEE 802.1ag (Connectivity Fault Management), ITU-T Y.1731 Fault Monitoring, ITU-T Y.1731 Performance Monitoring.
3.21. Router musi obsługiwać mechanizm wykrywania uszkodzeń (ang. Connectivity Fault Management) dla poszczególnych instancji VPLS zgodny ze standardem IEEE 802.1ag.

3.22. Router musi mieć zaimplementowaną funkcjonalność MPLS OAM, która pozwala na wykonanie sprawdzenia poprawności działania ścieżki LSP (ang. LSP ping) oraz jej trasy (ang. LSP traceroute). Funkcje te muszą być dostępne zarówno dla ścieżek zestawianych przy pomocy protokołu LDP jak i RSVP.

3.23. Dla usług IP VPN Router musi obsługiwać funkcje ping i traceroute dla każdej z sieci wirtualnych.

4. Architektura Routerów Agregacyjnych

4.1. Routery Agregacyjne muszą mieć architekturę modularną. Za modularne Zamawiający uznaje Urządzenie, który umożliwia rozbudowę o nowe, dodatkowe lub wymianę istniejących na nowsze elementy składowe, poprzez ich instalację w odpowiednich slotach przeznaczonych na moduły sprzętowe, takie jak np. interfejsy liniowe, matryce przełączające, karty procesorowe, itd. Nie dotyczy to wymiennych wkładek optycznych.

4.1.1. Każdy oferowany Router musi mieć takie wyposażanie, aby wszystkie elementy istotne z punktu widzenia pracy urządzenia miały nadmiarowość (jako elementy istotne Zamawiający uznaje m.in. wszystkie elementy konieczne dla prawidłowej pracy urządzenia, tj. zasilacze, wentylatory, karty procesorowe, matryce przełączające, itd., z wyłączeniem kart interfejsów liniowych). Wszystkie elementy mogące mieć zainstalowane elementy nadmiarowe będą w nie wyposażone. Wykonawca opisze sposobu realizacji wymogu nadmiarowości w oferowanych urządzeniach.

4.1.2. W przypadku przełączenia na zapasowe elementy (matryce przełączające, karty procesorowe) konieczne jest zachowanie ciągłej pracy protokołów routingu (ISIS, OSPFv2, OSPFv3, RSVP-TE, LDP, BGP dla wszystkich obsługiwanych AFI/SAFI), tj. utrzymanie sesji z wszystkimi sąsiadami w sensie tych protokołów routingu. Funkcjonalność ta musi być realizowana przy wykorzystaniu wewnętrznych mechanizmów urządzenia.

4.2. Dopuszczalne jest zaoferowanie Urządzeń o stałej konfiguracji przy następujących założeniach:

4.2.1. Połączenie Urządzeń będzie zrealizowane w sposób nieograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu (Routera Agregacyjnego), jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność Routera Agregacyjnego),

4.2.2. Zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia Systemu Urządzeń,

4.2.3. Wszystkie elementy Systemu Urządzeń będą spełniały wymagania związane z zarządzaniem,

4.2.4. Wykonawca przedstawi szczegółowy opis Systemu Urządzeń, obejmujący schematy połączeń, określenie, które elementy zestawu odpowiadają za poszczególne funkcjonalności itp., w ramach Opisu rozwiązania, wg Załącznika nr 11.

4.2.5. W przypadku łączy uplink zostaną one dołączone do dwóch różnych urządzeń fizycznych,

4.2.6. Łącza do elementów usługowych Systemu Urządzeń (sieć lokalna, węzeł bezpieczeństwa) zostaną dołączone do dwóch różnych Urządzeń,

4.2.7. Sumaryczna ilość zaoferowanych modeli nie przekroczy ograniczeń podanych w pkt. 1.2.

4.2.8. Wymagania dotyczące niezawodności dla Urządzeń modularnych związane z przełączeniem kart procesowych będą zachowane dla przełączenia urządzeń master (kontrolujących urządzenie wirtualne),

4.2.9. Wymagania pojemnościowe Urządzeń (tj. ilości sesji, pojemności tablic RIB i FIB, ilości obsługiwanych VPN i grup multicast) będą spełniane przez każde Urządzenie.

4.3. Architektura Routera musi zapewniać przełączanie pakietów pomiędzy dowolnymi dwoma interfejsami bez żadnych ograniczeń wydajnościowych przy założeniu obsadzenia urządzenia wszystkimi wymaganymi interfejsami.

4.3.1. Jeżeli karty interfejsów liniowych mają ograniczenia wydajnościowe (nadsubskrypcja), to do ilości interfejsów wymaganych liczone mogą być tylko interfejsy zapewniające pracę bez ograniczeń wydajnościowych. Pozostałe interfejsy, mimo że nie są zaliczane do interfejsów wymaganych, nie mogą mieć wprowadzonych żadnych blokad (muszą być dostępne do wykorzystania bez konieczności zakupu dodatkowych licencji, itd.).

4.4. Router musi mieć możliwość kopiowania całości ruchu przechodzącego przez wskazany interfejs logiczny do innego interfejsu. Proces ten musi być całkowicie transparentny dla kopiowanego ruchu.

4.5. Zamawiający dopuszcza, aby interfejsy 1GE były zainstalowane na modułach wyniesionych.

4.5.1. Użycie modułów wyniesionych nie może wpływać na skalowanie Routera Szkieletowego, a w szczególności (choć nie wyłącznie) na pojemność tablic routingu.

4.5.2. Wszystkie moduły wyniesione używane przez Routery Agregacyjne musza być tego samego typu.

4.5.3. Router Agregacyjny z modułem wyniesionym nie jest traktowany jako dodatkowy model urządzenia.

5. Wymagane funkcjonalności routingu IP:

5.1. Router musi obsługiwać IPv4 oraz IPv6 (routing statyczny, BGP, OSPF, ISIS) przy czym rozkład ruchu pomiędzy oba protokoły (tj. IPv4 i IPv6) nie może wpływać na funkcjonalność ani wydajność Routera,

5.1.1. Obsługa IPv4 oraz IPv6 musi być możliwa bez żadnych ograniczeń co do interfejsów.

5.1.2. Dla protokołu BGP konieczna jest obsługa 4 bajtowych ASN,

5.1.3. Dla protokołu BGP wymagana jest konieczność zestawienia nie mniej niż 500 sesji eBGP, w tym wielu sesji do jednego AS zewnętrznego,

5.2. Router musi obsługiwać multicast IPv4 (IGMPv2/3, PIM SM, SSM, MSDP),

5.3. Router musi obsługiwać multicast IPv6 (MLD, PIM SM, SSM),

5.4. Router musi obsługiwać Policy Based Routing (PBR) (kierowanie pakietów na podstawie innych kryteriów niż adres docelowy),

5.5. Router musi obsługiwać Bidirectional Forwarding Detection (BFD) min. dla OSPFv2/3, ISIS, BGP, routingu statycznego, LDP, dla interfejsów fizycznych oraz interfejsów logicznych, dla IPv4 oraz IPv6,

5.6. Router musi obsługiwać VRRP dla IPv4 i IPv6,

5.7. Router musi obsługiwać mechanizm multi-VRF, umożliwiający utrzymywanie oddzielnych tablic routingu (ang. Virtual Routing and Forwarding) dla sieci wirtualnych,

5.8. Router musi obsługiwać IP FRR z LFA (co najmniej dla protokołów ISIS i OSPF dla IPv4 i IPv6).

5.9. Router musi obsługiwać uRPF dla IPv4 i IPv6

6. Funkcjonalności przełączania MPLS:

6.1. Router musi mieć możliwość pracy jako router brzegowy LER (ang. Label Edge Router) oraz szkieletowy LSR (ang. Label Switch Router),

6.2. Router musi obsługiwać LDP, targeted LDP, RSVP-TE,

6.3. Router musi obsługiwać VPLS,
6.4. Router musi obsługiwać VPWS,
6.5. Router musi obsługiwać MPLS L3VPN (IPv4 i IPv6),
6.6. Router musi obsługiwać EVPN (L2/L3),
6.7. Router musi obsługiwać Multicast VPN dla IPv4 i IPv6,
6.8. Router musi obsługiwać MPLS TE (z mechanizmami ochrony ścieżki – path protection),
6.9. Router musi obsługiwać mechanizm MPLS Fast ReRoute (FRR),
6.10. Router musi obsługiwać ścieżki w trybie adaptacyjnym, umożliwiającym zmianę parametrów ścieżki (zmiana ścieżki podstawowej, zmiana deklaracji pasma) bez konieczności jej rozłączania (mechanizm make before break),
6.11. Router musi obsługiwać mechanizmy SRLG, wymuszające zestawianie alternatywnych/ backupowych połączeń LSP (ang. Label Switched Path) inną drogą niż ścieżki podstawowe

7. Funkcjonalności Segment Routing:
7.1. Router musi mieć możliwość wykorzystania mechanizmów transportowych MPLS i IPv6 (SRv6) (IPv6 opcjonalnie),
7.2. Router musi obsługiwać SR dla OSPF, ISIS, BGP,
7.3. Router musi obsługiwać alokację etykiet w modelach SRGB, SRLB,
7.4. Urządzenie musi obsługiwać SR-TE (Traffic engineering), TI-LFA (Topology Independent Loop Free Alternate),
7.5. Router musi obsługiwać funkcjonalności PCE, mapping server, mapping client,
7.6. Router musi obsługiwać SR OAM (ping, traceroute).

8. Lawful Intercept
8.1. Router musi mieć możliwość przechwytywania kopii ruchu do i z wybranej szkoły na potrzeby organów ścigania w zakresie wymaganym przez Prawo Telekomunikacyjne (uprawniony podsłuch, ang. Lawful Intercept).
8.2. Do oferty muszą być dołączone Urządzenia i licencje wymagane dla jednoczesnego przechwycenia ruchu ze szkół w węźle w liczbie podanej w poniższej tabeli:

Węzeł	liczba szkół do jednoczesnego przechwytywania ruchu
WAW	5
KAT	5
POZ	5
KRA	5
LOD	3
WRO	3
GDA	3
LUB	3
RZE	3
TOR	3
OLS	3
SZC	2
KIE	2
BIA	2

Węzeł	liczba szkół do jednoczesnego przechwytywania ruchu
ZGO	2
OPO	2

5.1.1. Wymagania na wydajność przesyłania dla Routerów Agregacyjnych

Do Routerów Agregacyjnych w poszczególnych województwach dołączone będą następujące ilości szkół:

województwo	węzeł	liczba dołączonych szkół
mazowieckie	WAW	3 806
śląskie	KAT	3 447
wielkopolskie	POZ	2 184
małopolskie	KRA	2 157
łódzkie	LOD	1 553
dolnośląskie	WRO	1 424
pomorskie	GDA	1 363
lubelskie	LUB	1 348
podkarpackie	RZE	1 328
kujawsko-pomorskie	TOR	1 194
warmińsko-mazurskie	OLS	1 132
zachodniopomorskie	SZC	942
świętokrzyskie	KIE	921
podlaskie	BIA	921
lubuskie	ZGO	712
opolskie	OPO	582

Oferowane Routery Agregacyjne należy tak skalować, aby zapewniły obsłużenie podanej ilości szkół, przy założeniu planowanego poziomu ruchu dla pojedynczej szkoły:

	pasmo	pakiety
ruch do szkoły	42,3 Mb/s	14 590 pakietów/s
ruch ze szkoły	15,4 Mb/s	5 310 pakietów/s

W tabeli podano wielkości mierzone jako średnia z 30 sekund pomiaru.

W tabeli jak powyżej podano parametry projektowe sieci, w przypadku gdy ruch rzeczywisty będzie się różnić od planowanego Zamawiający wymaga, aby Routery Agregacyjne:

- dalej realizowały wszystkie wymagane funkcjonalności zgodnie z wymaganiami podanymi w niniejszym dokumencie, oraz
- zapewniały obsługę poszczególnych parametrów ruchowych do wielkości wskazanych w powyższej tabeli.

5.1.2. Wymagania na ilość interfejsów dla Routerów Agregacyjnych

Routery Agregacyjne wyposażone muszą być w następujące ilości portów agregujących ruch do / ze szkół:

węzeł	minimalna ilość interfejsów	
	10GE	1GE
WAW	30	45
KAT	24	15
KRA	12	20
POZ	15	15
RZE	8	35
LUB	8	35
WRO	10	20
LOD	10	15
GDA	10	15
TOR	8	20
SZC	6	15
OLS	8	15
KIE	6	15
BIA	6	15
OPO	5	15
ZGO	5	15

Podane powyżej wartości są ilościami minimalnymi i węzeł może być wyposażony w większą ilość interfejsów agregujących.

Wszystkie interfejsy agregacyjne muszą być obsadzone wkładkami optycznymi w standardzie 1000Base-LX lub 10GBase-LR.

Ilości interfejsów uplink do Węzłów Szkieletowych należy wyliczyć na postawie szacowanego poziomu ruchu, przy czym należy założyć, że w początkowym okresie Węzeł będzie dołączany interfejsami 10GE, a wraz z dołączeniami kolejnych szkół oraz wzrostem ruchu do szkół będzie następowała rozbudowa łączy w modelu:

1 * 10GE -> n * 10GE ($n \leq 5$) -> 1 * 100GE -> 2 *100GE

Ilości interfejsów uplink w każdym z Węzłów Agregacyjnych zostaną opisane w Tabeli nr 26 w Załączniku nr 10, przy czym w urządzeniach muszą być zainstalowane wszystkie interfejsy potrzebne do realizacji połączeń wg podanego powyżej modelu. Należy przyjąć, że porty prowadzące do różnych Węzłów Szkieletowych umieszczone będą na różnych kartach w Urządzeniu Agregacyjnym.

Wszystkie interfejsy uplink muszą być obsadzone wkładkami optycznymi w standardzie 10GBase-LR, 40GBase-LR4 lub 100GBase-LR4.

5.1.3. Interfejsy do Regionalnego Węzła Bezpieczeństwa oraz sieci lokalnej

Każdy z Routerów Agregacyjnych musi być wyposażony w interfejsy służące do dołączenia Regionalnego Węzła Bezpieczeństwa oraz sieci lokalnej (sposób połączenia Routera Agregacyjnego, Regionalnego Węzła Bezpieczeństwa i sieci lokalnej przedstawiony jest w pkt. 5.3 „Wymagania na Przełączniki Sieci Lokalnej").

W przypadku instalowania jako Routera Agregacyjnym więcej niż jednego urządzenia fizycznego (zgodnie z pkt. 4.2), interfejsy te muszą być rozłożone równomiernie na więcej niż jedno urządzenie.

węzeł	interfejsy do Regionalnego Węzła Bezpieczeństwa		interfejsy do sieci lokalnej w węźle	
	100GE	40GE	40GE	10GE
WAW	4		2	
KAT	4		2	
KRA	3		2	
POZ	3		2	
RZE	2		2	
LUB	2		2	
WRO	2		2	
LOD	2		2	
GDA	2		2	
TOR	2		2	
SZC		2		4
OLS		2		4
KIE		2		4
BIA		2		4
OPO		2		4
ZGO		2		4

Wszystkie interfejsy dodatkowe muszą być obsadzone wkładkami optycznymi w standardzie 10Gbase-SR, 40GBase-SR4 lub 100GBase-SR4 (w węźle WAW 2 porty 40GE muszą być obsadzone optyką w standardzie 40GBase-LR4).

Dla połączeń do Urządzeń Agregacyjnych, w węzłach WAW, KAT, POZ, KRA, RZE, LUB, WRO, LOD, GDA, TOR, jest możliwa zamiana 2 portów 40GE na 8 portów 10GE (należy także skorygować ilość i rodzaj interfejsów oraz optyki w Urządzeniach Agregacyjnych).

W węźle WAW oznacza to wymianę optyki 40GBase-LR4 (2 wkładki) na:

- optykę CWDM (co najmniej cztery różne okna transmisyjne),
- dwie pary pasywnych (tj. nie wymagających zasilania), ośmiokanałowych splitterów CWDM, przystosowanych do montażu w szafie 19".

W przypadku wyżej opisanej zmiany, konieczne jest także odpowiednie skorygowanie ilości i rodzaju interfejsów oraz optyki w Przełącznikach Sieci Lokalnej.

5.1.4. Inne wymagane parametry wydajnościowe dla Routerów Agregacyjnych

Pozostałe wymagane parametry wydajnościowe są następujące:

9. Router musi obsługiwać co najmniej 1 500 000 prefiksów IPv4 oraz 500 000 prefiksów IPv6 (jednocześnie). Wszystkie prefiksy muszą być używane do przełączania ruchu - tzn. zainstalowane w bazie FIB (ang. Forwarding Information Base).
    9.1. Ilość prefiksów przechowywanych w tablicy RIB (Routing Information Base) to 3 000 000 prefiksów IPv4 i 1 000 000 prefiksów IPv6 (jednocześnie).
10. Router musi obsługiwać co najmniej 2 000 sieci VPLS.
    10.1. Router musi obsługiwać nie mniej niż 128 000 adresów MAC zarejestrowanych w sieciach VPLS
11. Router musi obsługiwać jednocześnie co najmniej 16 000 grup multicast dla IPv4 oraz 16 000 grup multicast dla IPv6.
12. Router musi obsługiwać co najmniej 10 000 tranzytowych ścieżek LSP (RSVP-TE).
13. Router musi obsługiwać co najmniej 1 500 źródłowych ścieżek LSP (RSVP-TE head-end).
14. Router musi obsługiwać co najmniej 1 500 zakończeń ścieżek LSP (RSVP-TE egress).
15. Router musi obsługiwać co najmniej 500 sesji LDP typu targeted.
16. Router musi obsługiwać co najmniej 2 000 połączeń L2VPN, nie wliczając do tego sieci VPLS.
17. Router musi obsługiwać co najmniej 1 000 sieci L3VPN.

5.2. Wymagania dla CG-NAT

Routery Agregacyjne będą wyposażone w funkcjonalność CG-NAT, tj. translacji adresów IPv4 z adresacji Shared Space do adresacji publicznej używanej przez sieć OSE oraz translacji pomiędzy protokołami IPv4 i IPv6.

Dopuszczalne jest, aby funkcjonalność CG-NAT była realizowana przez dedykowane Urządzenia zlokalizowane w Węzłach Agregacyjnych (inne niż Routery Agregacyjne), bądź też przez Urządzenia zlokalizowane w Węzłach Szkieletowych (jako funkcjonalność Routerów Szkieletowych lub dedykowane urządzenia).

1. System CG-NAT musi umożliwiać translacje:
    1.1. NAT44 – pomiędzy adresami prywatnymi (Shared Space) oraz adresami publicznymi IPv4, przy czym adres źródłowy może być statyczny (mapowanie 1:1) lub dynamiczny (mapowanie do puli adresowej zewnętrznej n:1),
    1.2. NAT44 twice – jednoczesne mapowanie adresu źródłowego i docelowego na potrzeby nakładających się pul adresacji prywatnych,
    1.3. NAT64 – umożlwiający klientom pracującym wyłącznie przy wykorzystaniu IPv6 dostęp do zasobów dostępnych w IPv4,
        1.3.1. NAT64 musi umożliwiać pracę w trybie stateful,
    1.4. NAT46 – umożlwiający klientom pracującym wyłącznie przy wykorzystaniu IPv4 dostęp do zasobów dostępnych w IPv6.
    1.5. DS-Lite – umożliwiający tunelowanie pakietów IPv4 przez sieć IPv6.
    1.6. Dla wszystkich translacji pracujących w trybie n:1 konieczne jest zapewnienie wsparcia dla trybu pracy PBA (Port Block Allocation) z agregacją logowania.
    1.7. W ramach CG-NAT musi być zapewniona obsługa translacji adresów wewnątrz protokołów warstw 4 – 7 modelu ISO/OSI, w tym co najmniej:
        - ICMP

- TCP
- UDP
- DNS
- FTP
- TFTP
- H.323
- SIP
- IKE
- IP Sec

5.2.1. Logowanie

2. System CG-NAT musi umożliwiać logowanie danych na potrzeby retencji danych telekomunikacyjnych. Dane zapisywane będą na kolektorze logów, zlokalizowanym w tej samej lokalizacji co urządzenie.
   W gestii Wykonawcy leży oszacowanie ilości i wydajności portów sieciowych w urządzeniach realizujących funkcjonalność CG-NAT, koniecznych do przesłania wymaganych logów. Minimalna wydajność logowania nie może być mniejsza niż 20 000 EPS.
   Minimalny zakres logowania to:
   - adres i port źródłowy,
   - adres i port docelowy,
   - czas translacji.

5.2.2. Architektura systemu CG-NAT

Funkcjonalność CG-NAT może być zrealizowana na dedykowanych kartach zainstalowanych bezpośrednio do Routerów Szkieletowych lub Agregacyjnych, bądź jako dedykowane Urządzenia, realizujące wyłącznie funkcjonalność CG-NAT.

W przypadku kart instalowanych do Routerów Szkieletowych lub Agregacyjnych, dostarczona musi być taka ilość kart, aby zapewnić pełną funkcjonalność CG-NAT dla całości ruchu, oszacowanego zgodnie z pkt. 5 ppkt. Inne wymagane parametry wydajnościowe dla Routerów Agregacyjnych.

W przypadku użycia dedykowanych urządzeń, Wykonawca musi doliczyć do oferty wszystkie niezbędne elementy, konieczne do dołączenia urządzeń CG-NAT do sieci OSE, a w szczególności interfejsy w Routerach Szkieletowych lub Agregacyjnych (w zależności od lokalizacji Urządzeń realizujących funkcje CG-NAT), przy czym należy założyć, że od razu zostaną zainstalowane docelowe łącza, w maksymalnej wymaganej wydajności.

Dodatkowo dedykowane Urządzenia muszą spełniać następujące wymagania:

3. Wymagania ogólne dla urządzenia dedykowanego:
   3.1. Wykonawca musi być oficjalnym sprzedawcą w Polsce oferowanych urządzeń.
   3.2. Wykonawca musi mieć możliwość świadczenia autoryzowanego przez producenta serwisu gwarancyjnego.
   3.3. Urządzenie musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
      3.3.1. Urządzenie musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o

takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.

3.4. Urządzenie musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.

3.4.1. Dostarczone zasilacze muszą umożliwiać poprawną pracę Urządzenia w pełnej (wymaganej przez Zamawiającego) konfiguracji z wykorzystaniem połowy zainstalowanych zasilaczy, przy zachowaniu pełniej funkcjonalności urządzenia.

3.5. Urządzenie musi poprawnie pracować w temperaturze od 5 do 40 °C.

3.6. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

3.7. Urządzenie musi umożliwiać możliwość instalacji, wymiany lub zamiany poszczególnych modułów (takich jak np. zasilacze, wentylatory, karty z interfejsami sieciowymi, moduły optyczne typu SFP / XFP / itd.) w trakcie pracy urządzenia (ang. hot-swap).

3.8. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

3.9. Dokumentacja do Urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

4. Wymagania na interfejsy dla urządzenia dedykowanego

4.1. Karty liniowe lub moduły Urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów9. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na Urządzenie ani ograniczeń w świadczeniu usług serwisowych
Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu Urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych.

4.2. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)10 zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

4.3. Urządzenie musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

[9] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji urządzenia, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[10] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

4.4. Wszystkie interfejsy liniowe zainstalowane w Urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym Urządzeniu.

4.5. Urządzenie musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP). Pojedynczy interfejs zagregowany musi składać się z czterech interfejsów składowych, przy czym nie może być ograniczeń co do lokalizacji tych interfejsów na kartach interfejsów (dla urządzeń modularnych), zaś dla urządzeń wirtualnych zbudowanych z wielu Systemu Urządzeń musi być zapewniona możliwość składania interfejsów umieszczonych w różnych urządzeniach fizycznych (MC-LAG).

5. Zarządzanie i monitorowanie urządzeń (dla urządzenia dedykowanego)

5.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

5.1.1. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego.

5.1.2. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

5.1.3. Urządzenie musi zapewniać możliwość cofnięcia zmian konfiguracji,

5.1.4. Urządzenie musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

5.1.5. CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

5.2. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

5.3. Urządzenie musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

5.4. Urządzenie musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

5.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

5.4.2. Urządzenie musi pozwalać na zbieranie pełnych statystyk przez protokół SNMP w sposób nie powodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 na 5 minut

5.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

5.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 4741, NETCONF Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

5.7. Urządzenie nie może wprowadzać ograniczeń na dostęp dowolnych systemów OSS do urządzenia (dotyczy to także systemów OSS nie oferowanych w ramach niniejszego postępowania), przy wykorzystaniu dowolnego protokołu (w szczególności SNMP i NETCONF). Jeżeli Urządzenie wymaga dodatkowych licencji zapewniających taki dostęp, to licencje te muszą być uwzględnione w ofercie.

5.8. Urządzenie musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

5.9. Urządzenie musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

5.10. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

5.11. Urządzenie musi mieć możliwość zdalnej aktualizacji oprogramowania.

5.12. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB.

5.13. Urządzenie musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez Urządzenie zdarzeniach do zdalnego serwera syslog.

5.14. Urządzenie musi obsługiwać protokół NTP.

5.15. Urządzenie musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

5.15.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

5.15.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.

5.15.3. Urządzenie musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

5.15.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

5.16. W przypadku użycia systemu CG-NAT dostarczonego przez innego producenta niż producent Routerów Szkieletowych i Agregacyjnych, zaoferowany zostanie dedykowany system zarządzania urządzeniami realizującymi funkcjonalność CG-NAT.

5.16.1. System ten umożliwi spójne zarządzanie wszystkimi urządzeniami realizującymi funkcjonalność CG-NAT z pojedynczej konsoli operatora.

5.16.2. System ten będzie miał funkcjonalności analogiczne do właściwości systemu zarzadzania opisanego w pkt. 4.3), z uwzględnieniem różnic wynikających z funkcjonalności urządzeń (brak konieczności provisioningu interfejsów, brak konieczności monitoringu protokołów routingu, koniczność monitoringu zasobów CG-NAT oraz stanu tablic translacji, itd.).

6. Redundancja

6.1. Zamawiający wymaga zapewnienia redundancji dla systemu CG-NAT. W ramach zapewniania redundancji Zamawiający wymaga zaoferowania dodatkowej karty instalowanej do routera Agregacyjnego lub dodatkowego urządzenia dedykowanego (przy braku redundancji wewnętrznej tego urządzenia) lub zapewnia redundancji urządzenia dedykowanego analogicznie do wymagań opisanych w pkt 5.1 ppkt 1.4 i 4.1.1.

6.2. Zamawiający wymaga, aby przełączanie na zapasową instancję CG-NAT nastąpiło automatycznie, przy czym dopuszczalne jest zerwanie bieżących translacji w momencie przełączenia.

6.3. Dopuszczalne jest zaoferowanie rozwiązania, w którym obie instancje CG-NAT będą pracowały równocześnie, a w przypadku awarii jednej z nich, druga przejmie obsługę całości ruchu (tryb active - active).

6.4. Zamawiający dopuszcza utratę 20% wydajności przy przełączeniu na zapasową instancje CG-NAT (w czasie pracy wyłączenie na zapasowej instancji CG-NAT konieczne jest obsłużenie co najmniej 80% ruchu wg wymagań podanych w pkt. 5.2.3).

5.2.3. Wymagania wydajnościowe CG-NAT

Urządzenia powinny zapewniać poprawną pracę przy założeniu poniższych wartości obciążenia.

W przypadku zaoferowania rozwiązania, w którym funkcje CG-NAT realizowane są przez Urządzenia zainstalowane w Węzłach Szkieletowych, należy zapewnić taką wydajność urządzeń, aby cały ruch przechodzący przez dany Węzeł Szkieletowy był przez nie poprawnie obsługiwany.

Węzeł	nowe sesje [CPS]	aktywne sesje
WAW	1 174 800	31 328 000
KAT	1 063 800	28 368 000
POZ	674 100	17 976 000
KRA	665 700	17 752 000
LOD	479 400	12 784 000
WRO	439 500	11 720 000
GDA	420 600	11 216 000
LUB	416 100	11 096 000
RZE	409 800	10 928 000
TOR	368 400	9 824 000
OLS	349 500	9 320 000
SZC	290 700	7 752 000
KIE	284 400	7 584 000
BIA	284 400	7 584 000
ZGO	219 600	5 856 000
OPO	179 700	4 792 000

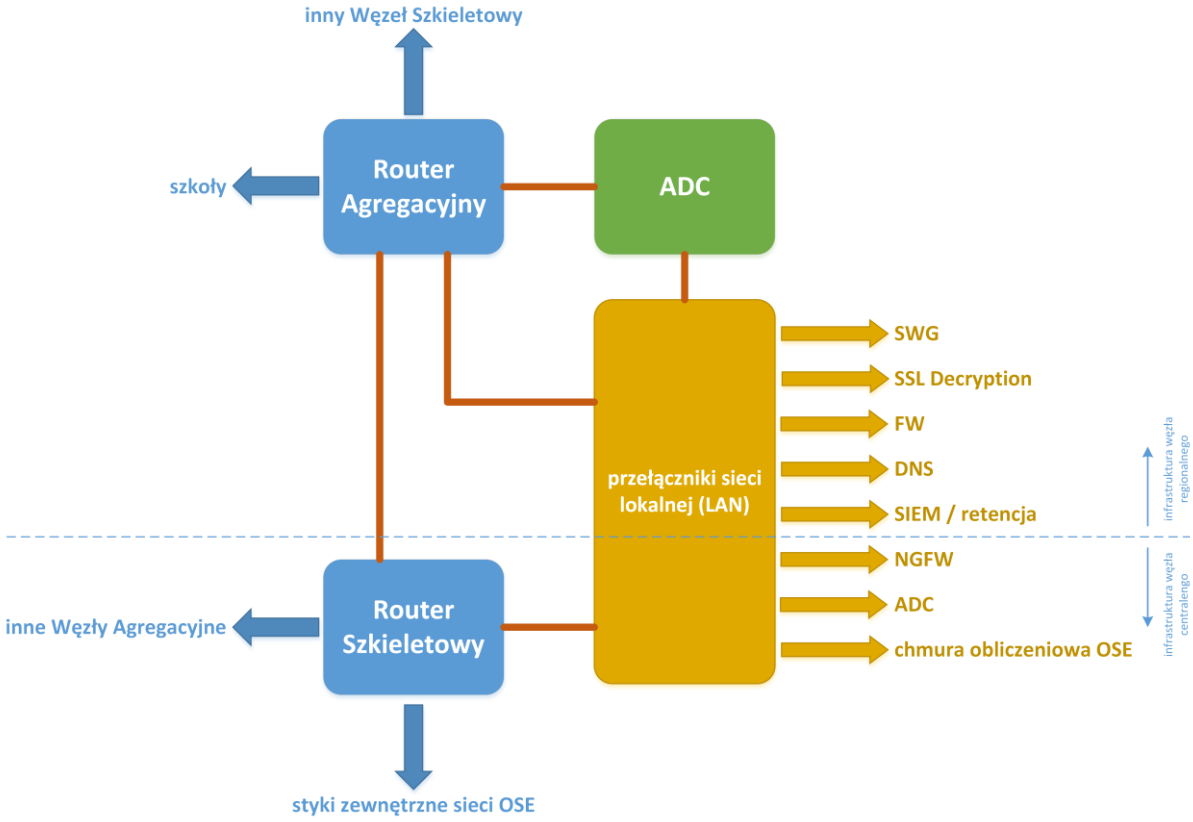
W przypadku gdy ruch rzeczywisty będzie się różnić od planowanego, jaki wskazano w tabeli, Zamawiający wymaga aby Urządzenia realizujące funkcjonalność CG-NAT

- dalej realizowały wszystkie wymagane funkcjonalności zgodnie z wymaganiami, oraz
- zapewniały obsługę poszczególnych parametrów ruchowych (w szczególności zapewniały translację adresów) do wielkości wskazanych w powyższej tabeli.

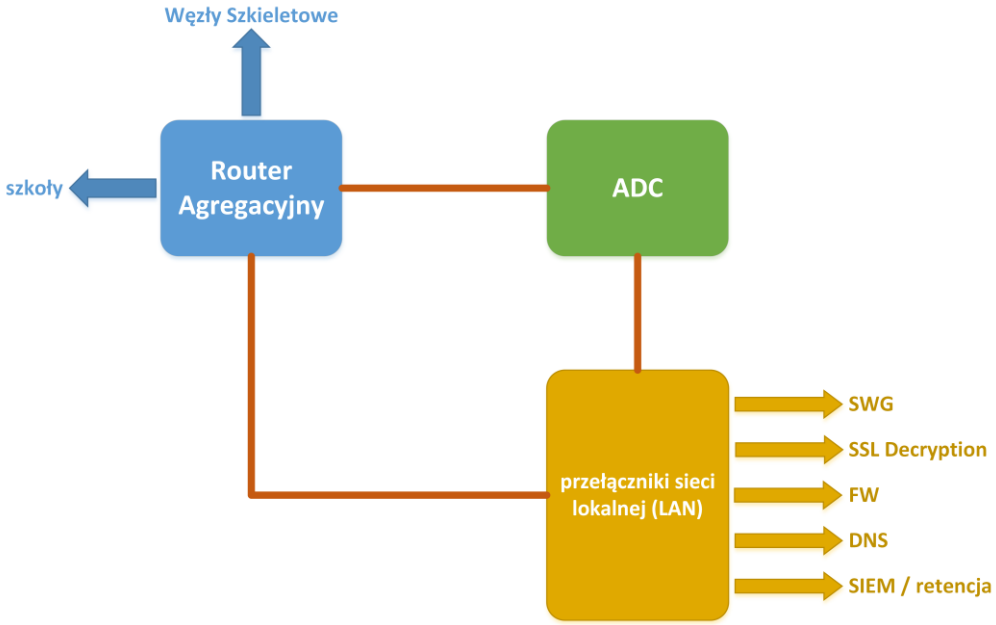
5.3. Wymagania na Przełączniki Sieci Lokalnej

Przełączniki Sieci Lokalnej będą zainstalowane w każdym z Węzłów. Przełączniki te będą obsługiwały urządzenia zainstalowane w węzłach, w szczególności urządzenia Węzła Bezpieczeństwa (Regionalnego i Centralnego), systemy zbierania i retencji logów telekomunikacyjnych oraz systemy komputerowe, na których będą posadowione systemy OSS/BSS sieci OSE.

Struktura połączeń poszczególnych elementów Węzła Centralnego i Regionalnego przedstawiona jest poniżej:



Struktura połączeń Węzła Centralnego



Struktura połączeń Węzła Regionalnego

W dalszej części punktu słowa przełącznik oraz urządzenie używane są wymiennie.

Wszystkie przełączniki musza spełniać następujące wymagania:

1. Wymagania ogólne
   - 1.1. Wszystkie oferowane przełączniki (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
   - 1.2. Urządzenie musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
     - 1.2.1. Urządzenie musi posiadać wymiary umożliwiające montaże w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   - 1.3. Urządzenie musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone Urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone Urządzenie do standardowych gniazd zasilających.
     - 1.3.1. Dostarczone zasilacze muszą umożliwiać dołączenie urządzenia do dwóch niezależnych obwodów zasilających (dwa zestawy paneli zasilających) oraz poprawną pracę urządzenia w pełnej, wymaganej przez Zamawiającego, konfiguracji z wykorzystaniem zasilania z jednego obwodu, przy zachowaniu pełniej funkcjonalności urządzenia.
     - 1.3.2. Dostarczone Urządzenie musi umożliwiać pracę z pełną funkcjonalnością w pełnej, wymaganej przez Zamawiającego, konfiguracji przy wyłączeniu co najmniej jednego zasilacza.
     - 1.3.3. Maksymalny pobór mocy Przełączników Sieci Lokalnej w węźle nie może przekroczyć poniższych wartości:

węzeł	maksymalny pobór prądu
WAW	9 kW
KAT	9 kW
POZ	8 kW
WRO	6 kW
TOR	6 kW
LUB	6 kW
ZGO	6 kW
LOD	6 kW
KRA	6 kW
OPO	6 kW
RZE	6 kW
BIA	6 kW
GDA	6 kW
KIE	6 kW
OLS	6 kW
SZC	6 kW

1.4. Urządzenie musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.

1.5. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

1.6. Urządzenie musi umożliwiać możliwość instalacji, wymiany lub zamiany poszczególnych modułów (takich jak np. zasilacze, wentylatory, karty z interfejsami sieciowymi, moduły optyczne typu SFP / XFP / itd.) w trakcie pracy urządzenia (ang. hot-swap).

1.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

1.8. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

2. Wymagania na interfejsy

2.1. Interfejsy 1GE, 10 GE, 25GE, 40GE i 100GE muszą być zgodne z właściwą dla danego typu interfejsu normą IEEE 802.3.

2.2. Karty liniowe lub moduły urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu),

pochodzącymi od różnych producentów[11]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na urządzenie ani ograniczeń w świadczeniu usług serwisowych

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego Urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.3. Dostarczone moduły optyczne muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)[12] zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

2.4. Urządzenie musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

2.5. Wszystkie interfejsy liniowe zainstalowane w Urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym Urządzeniu.

2.6. Urządzenie musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.7. Przełącznik musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP).

2.7.1. Przełącznik musi umożliwiać utworzenie nie mniej niż 64 interfejsów zagregowanych.

2.7.2. Przełącznik musi umożliwiać tworzenie grup LAG składających się z co najmniej 8 interfejsów składowych, przy czym nie może być ograniczeń co do lokalizacji tych interfejsów na kartach interfejsów (dla urządzeń modularnych), zaś dla urządzeń wirtualnych zbudowanych z wielu Systemu Urządzeń musi być zapewniona możliwość składania interfejsów umieszczonych w różnych urządzeniach fizycznych (MC-LAG).

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2. Urządzenie musi zapewniać minimum dwustopniowe zatwierdzanie komend (wprowadzenie komendy, aktywacja konfiguracji),

3.1.3. Urządzenie musi zapewniać możliwość cofnięcia zmian konfiguracji,

3.1.4. Urządzenie musi zapewniać możliwość tworzenia punktów kontrolnych konfiguracji i ich odtwarzania,

3.1.5. Urządzenie musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

[11] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji przełącznika, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[12] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

3.1.6. CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Urządzenie musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Urządzenie musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.4.2. Urządzenie musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób nie powodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruch dla interfejsów fizycznych,
- statystyki ruch dla interfejsów logicznych,
- statystyki zajętości tablic MAC,
- statystyki przypisania adresów MAC do VLAN,
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.7. Urządzenie nie może wprowadzać ograniczeń na dostęp dowolnych systemów OSS do urządzenia (dotyczy to także systemów OSS nie oferowanych w ramach niniejszego postępowania), przy wykorzystaniu dowolnego protokołu (w szczególności SNMP i NETCONF). Jeżeli urządzenie wymaga dodatkowych licencji zapewniających taki dostęp, to licencje te muszą być uwzględnione w ofercie.

3.8. Urządzenie musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.9. Urządzenie musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.10. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.11. Urządzenie musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.11.1. Urządzenie musi mieć zaimplementowany mechanizm ISSU (In Service Software Upgrade) zapewniający aktualizację oprogramowania bez przerywania pracy urządzenia

(dopuszczalna jest przerwa w pracy kart liniowych nie dłuższa niż 0,5s nie wpływająca na działanie protokołów routingu).

3.12. Urządzenie musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.13. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

3.14. Urządzenie musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.15. Urządzenie musi obsługiwać protokół NTP.

3.16. Urządzenie musi obsługiwać IPFIX lub NetFlow (wersje 5 i 9) dla IPv4, IPv6.

3.17. Urządzenie musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.17.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

3.17.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.

3.17.3. Urządzenie musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.17.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

4. Architektura przełączników

4.1. Przełączniki muszą mieć architekturę modularną. Za urządzenie modularne Zamawiający uznaje urządzenie, który umożliwia rozbudowę o nowe, dodatkowe lub wymianę istniejących na nowsze elementy składowe, poprzez ich instalację w odpowiednich slotach przeznaczonych na moduły sprzętowe, takie jak interfejsy liniowe, matryce przełączające, karty procesorowe, itd. Nie dotyczy to wymiennych wkładek optycznych.

4.1.1. Każdy oferowany przełącznik musi mieć takie wyposażanie, aby wszystkie elementy istotne z punktu widzenia pracy urządzenia miały nadmiarowość (jako elementy istotne Zamawiający uznaje wszystkie elementy konieczne dla prawidłowej pracy urządzenia, tj. zasilacze, wentylatory, karty procesorowe, matryce przełączające, itd. z wyłączeniem kart interfejsów liniowych). Wszystkie urządzenia mogące mieć zainstalowane elementy nadmiarowe będą w nie wyposażone. Prosimy o opisanie sposobu realizacji wymogu nadmiarowości w oferowanych urządzeniach.

4.2. Dopuszczalne jest zaoferowanie urządzeń wirtualizowanych, zbudowanych z wielu urządzeń składowych (w szczególności z urządzeń o stałej konfiguracji), przy następujących założeniach:

4.2.1. Połączenie urządzeń będzie zrealizowane w sposób nieograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),

4.2.2. Zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zestawu urządzeń,

4.2.3. Wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,

4.2.4. Do oferty zostanie dołączony szczegółowy opis zestawu, obejmujący schematy połączeń, określenie, które elementy zestawu odpowiadają za poszczególne funkcjonalności itp.

4.2.5. Wymagania dotyczące niezawodności dla urządzeń modularnych związane z przełączeniem kart procesowych będą zachowane dla przełączenia urządzeń master (kontrolujących urządzenie wirtualne).

4.3. Architektura oferowanego przełącznika musi zapewniać bezstratne przełączanie pakietów pomiędzy dowolnymi dwoma interfejsami bez żadnych ograniczeń wydajnościowych przy założeniu, że wszystkie porty pracują z pełną wydajnością (tj. nadają i odbierają pakiety z pełną prędkością interfejsu). Dla interfejsów 10GE/25GE należy przyjąć że powyższe wymaganie będzie spełnione dla prędkości pracy portu 10Gb/s.

4.3.1. Jeżeli karty interfejsów liniowych mają ograniczenia wydajnościowe (nadsubskrypcja), to do ilości interfejsów wymaganych liczone mogą być tylko interfejsy zapewniające pracę bez ograniczeń wydajnościowych. Pozostałe interfejsy, mimo że nie są zaliczane do interfejsów wymaganych, nie mogą mieć wprowadzonych żadnych blokad (muszą być dostępne do wykorzystania bez konieczności zakupu dodatkowych licencji, itd.).

5. Wymagania na funkcjonalności przełączania
   5.1. Przełącznik musi obsługiwać protokoły RSTP i MSTP.
   5.2. Przełącznik musi obsługiwać protokół PVSTP lub równoważny (umożliwiający utworzenie oddzielnego drzewa rozpinającego (ang. spanning tree) dla każdego skonfigurowanego VLANu).
   5.3. Przełącznik musi obsługiwać mechanizm typu BUM (Broadcast/Unknown/Multicast) storm control.
   5.4. Przełącznik musi obsługiwać protokół LLDP Link Layer Discovery Protocol (LLDP) zgodnie z IEEE 802.1ab.
   5.5. Przełącznik musi obsługiwać jednocześnie co najmniej 4 000 sieci VLAN.
   5.6. Przełącznik musi zapewniać wsparcie dla sieci VXLAN,
      5.6.1. Przełącznik musi spełniać funkcjonalność VXLAN L2 Gateway,
      5.6.2. Przełącznik musi spełniać funkcjonalność VXLAN L3 Gateway,
      5.6.3. Przełącznik musi wspierać EVPN, w tym EVPN multihoming.
   5.7. Przełącznik musi obsługiwać tablicę MAC o pojemności 128 000 wpisów
   5.8. Przełącznik musi zapewniać wsparcie dla IPv4 oraz IPv6.
      5.8.1. Przełącznik musi obsługiwać tablice routingu o pojemności co najmniej 32 000 prefixów dla każdego z protokołów IPv4 i IPv6.
      5.8.2. Przełącznik musi obsługiwać tablice ARP o wielkości 16 000 adresów,
      5.8.3. Przełącznik musi obsługiwać tablice ND (neighbor discovery) o wielkości 16 000 adresów.
   5.9. Przełącznik musi obsługiwać protokół BGP.
   5.10. Przełącznik musi obsługiwać protokół OSPF.
   5.11. Przełącznik musi obsługiwać protokół ISIS.
   5.12. Przełącznik musi obsługiwać VRRP v2 i v3.

5.3.1. Wymagania na ilość interfejsów w Przełącznikach Sieci Lokalnej

W każdym z węzłów muszą być następujące ilości portów w przełącznikach:

węzeł	100GE	40GE	10GE / 25GE	wkładki 10GE
WAW	4	68	316	229
KAT	4	62	174	96
POZ	3	37	260	194

węzeł	100GE	40GE	10GE / 25GE	wkładki 10GE
KRA	3	35	94	28
RZE	2	29	98	52
LUB	2	26	98	52
WRO	2	26	100	54
LOD	2	26	104	58
GDA	2	26	98	52
TOR	2	23	94	48
SZC		23	90	44
OLS		20	86	50
KIE		20	80	44
BIA		20	80	44
OPO		17	60	34
ZGO		17	64	38

gdzie:

- 100GE – porty 100GE wyposażone w optykę w standardzie 100GBase-SR4,
- 40GE – porty 40GE wyposażone w optykę 40GBase-SR4, w węźle WAW 2 wkładki muszą być typu 40GBase-LR4,
  Dla połączeń do Urządzeń Agregacyjnych, w węzłach WAW, KAT, POZ, KRA, RZE, LUB, WRO, LOD, GDA, TOR, jest możliwa zamiana 2 portów 40GE na 8 portów 10GE (należy także skorygować ilość i rodzaj interfejsów oraz optyki w Urządzeniach Agregacyjnych).
  W węźle WAW oznacza to wymianę optyki 40GBase-LR4 (2 wkładki) na:
  - optykę CWDM (co najmniej cztery różne okna transmisyjne),
  - dwie pary pasywnych (tj. nie wymagających zasilania) ośmiokanałowych splitterów CWDM, przystosowanych do montażu w szafie 19”,

  Należy także skorygować ilość i rodzaj interfejsów oraz optyki w Routerze Agregacyjnym.
- 10GE / 25GE – porty 10GE lub 10GE / 25GE (porty o zmiennej prędkości pracy), porty bez wkładek,
- wkładki 10GE – ilość wkładek 10GBase-SR do instalacji w przełączniku,

W każdym z węzłów porty 40GE oraz 10GE / 25GE muszą być umieszczone równomiernie, na co najmniej dwóch kartach interfejsów (w przypadku urządzeń modularnych) lub na co najmniej dwóch urządzeniach składowych (w przypadku urządzeń wirtualizowanych zbudowanych z wielu Systemu Urządzeń). Należy przyjąć, że każde urządzenie końcowe (serwer) wyposażone jest w dwa identyczne porty (40GE lub 25GE lub 10GE) i każdy z tych portów musi być dołączony do portu przełącznika zlokalizowanym na innej karcie / Urządzeniu.

5.4. Wymagania na sieć zarządzania

Urządzenia sieci zarządzania zapewniają dostęp do urządzeń telekomunikacyjnych oraz urządzeń sieci lokalnej, stanowiących wyposażenie Węzła Agregacyjnego.

W ramach realizacji umowy Dostawca dostarczy:

- do każdego z Węzłów Agregacyjnych komplet Urządzeń (tj. router sieci zarządzania, przełącznik LAN oraz serwer terminalowy),
- do węzła WAW dodatkowy zestaw, tj. router sieci zarządzania, przełącznik LAN oraz serwer terminalowy.

5.4.1. Wymagania na zasilanie urządzeń sieci zarządzania

Maksymalny pobór mocy wszystkich urządzeń sieci zarządzania nie może przekroczyć 1,5 kW w żadnym z węzłów.

5.4.2. Wymagania dla routera sieci zarządzania

W ramach oferty Wykonawca zapewni routery sieci zarządzania spełniające następujące funkcje:

1. Wymagania ogólne
   - 1.1. Router musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297).
     - 1.1.1. Router musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
     - 1.1.2. Dopuszczalne jest zaoferowanie urządzeń nie posiadających możliwości instalacji w szafie teleinformatycznej. W takim wypadku konieczne jest dodanie do oferty standardowej półki do takiej szafy, zaś jako wysokość urządzenia należy przyjąć wysokość urządzenia (nie mniej niż 1 RU) oraz wysokość półki (nie mniej niż 1 RU).
     - 1.1.3. Router musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   - 1.2. Router musi być wyposażony w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających. Urządzenie musi być wyposażone w co najmniej jeden zasilacz.
   - 1.3. Router musi poprawnie pracować w temperaturze od 5 do 40 °C.
   - 1.4. Router musi poprawnie pracować przy wilgotności powietrza od 5% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.
   - 1.5. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.
   - 1.6. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta Urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.
2. Wymagania na interfejsy
   - 2.1. Router będzie posiadał co najmniej interfejsy:

2.1.1. Interfejs WAN – Ethernet 10/100/1000 do dołączenia do urządzenia agregacyjnego lub szkieletowego. Interfejs ten musi umożliwiać utworzenie nie mniej niż 10 interfejsów logicznych.

2.1.2. Interfejs LAN - Ethernet 10/100/1000 do dołączenia do dedykowanego przełącznika sieci zarządzenia

2.1.3. Interfejs WAN (backup) - moduł WAN ze slotem na kartę SIM zapewniający transmisję w sieci LTE. Przy braku modułu wewnętrznego możliwość zainstalowania zewnętrznego modułu obsługującego transmisję LTE: karta do routera/urządzenie zewnętrzne, z zachowaniem funkcji routingu IP na routerze.

2.2. Wszystkie interfejsy liniowe zainstalowane w urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym Urządzeniu.

2.3. Router musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.4. Router musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP). Pojedynczy interfejs zagregowany musi składać się z czterech interfejsów składowych.

2.5. Znaczenie pola VID (VLAN ID) musi mieć znaczenie lokalne dla interfejsu fizycznego, co oznacza, że ten sam znacznik VID może być użyty niezależnie na wielu interfejsach fizycznych urządzenia.

3. Zarządzanie i monitorowanie routerów

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.2. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego.

3.2.1. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.3. Router musi zapewniać możliwość cofnięcia zmian konfiguracji,

3.4. Router musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

3.5. CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.6. Router musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.7. Router musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.8. Router musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.8.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.9. Router musi wspierać mechanizm SNMP Trap (STD 62).

3.10. Router musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 4741, NETCONF Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.11. Router musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.12. Router musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.13. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.14. Router musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.15. Router musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.16. Router musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.17. Router musi obsługiwać protokół NTP.

3.18. Router musi obsługiwać automatyczną ochronę modułów sterujących przed atakami typu DDoS (Distributed Denial of Service). Funkcjonalność musi pozwalać na odrzucanie (pomijanie) pakietów sterujących (np. związanych z protokołami i mechanizmami działającymi na module sterującym) kierowanych do modułu sterującego, których ilość przekracza założony próg. Przełącznik musi zapewniać możliwość konfiguracji parametrów mechanizmu ochrony DDoS dla poszczególnych protokołów (np. ograniczenie wielkości ruchu) oraz rejestrować wystąpienie zdarzeń związanych z działaniem tego mechanizmu (takich jak: czas wystąpienia ostatniego przekroczenia parametrów, czas trwania przekroczenia, liczbę pakietów odebranych, liczbę pakietów odrzuconych).

Włączenie mechanizmu ochrony DDoS nie może skutkować wykluczeniem, ograniczeniem lub pogorszeniem jakichkolwiek wymaganych przez Zamawiającego parametrów funkcjonalnych, wydajnościowych i eksploatacyjnych.

3.19. Router musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.19.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

3.19.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.

3.19.3. Router musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.19.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

3.20. Dla usług IP VPN router musi obsługiwać funkcje ping i traceroute dla każdej z sieci wirtualnych.

4. Wymagania routingowe

4.1. Router musi wspierać protokoły routingu dynamicznego dla IPv4 i IPv6:

4.1.1.OSFP

4.1.2.BGP

4.1.3.ISIS

4.2. Router musi mieć możliwość obsługi nie mniej niż 8 000 tras dla IPv4 i 8 000 tras dla IPv6 jednocześnie.

4.3. Router musi umożliwiać zestawienie łącz IP Sec w trybie site-to-site.

4.3.1. Ilość tuneli IP Sec nie może być mniejsza niż 50.

4.3.2. Ilość ruchu zaszyfrowanego nie może być mniejsza niż 10Mb/s.

5.4.3. Wymagania dla przełączników LAN sieci zarządzania

W ramach oferty Wykonawca zapewni przełączniki LAN sieci zarządzania spełniające następujące funkcje:

1. Wymagania ogólne
   1.1. Przełącznik musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297).
      1.1.1. Przełącznik musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
      1.1.2. Przełącznik musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.
   1.2. Przełącznik musi być wyposażony w zasilacze dostosowane do napięcia przemiennego 230V AC. Dostarczony przełącznik będzie wyposażony w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających. Przełącznik musi być wyposażony w co najmniej jeden zasilacz.
   1.3. Przełącznik musi poprawnie pracować w temperaturze od 5 do 40 °C.
   1.4. Przełącznik musi poprawnie pracować przy wilgotności powietrza od 5% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.
   1.5. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.
   1.6. Możliwe jest zaoferowanie, w każdym z węzłów, wielu przełączników pracujących jako jedno urządzenie logiczne (w szczególności wykorzystując technologię stackowania, Virtual Chassis lub podobną).
   1.7. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.
2. Wymagania na interfejsy
   2.1. Przełącznik wyposażony w porty ethernet 10/100/1000 (ilość portów zgodnie z tabelą powyżej).
   2.2. Wszystkie porty muszą wspierać detekcję MDI/MDI-X.
   2.3. Wszystkie porty muszą mieć możliwość pracy w trybie full duplex.

2.4. Wszystkie interfejsy liniowe zainstalowane w urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

2.5. Przełącznik musi wspierać pojedyncze i podwójne tagowanie ramek ethernet (zgodnie ze standardem IEEE 802.1q i IEEE 802.1ad).

2.6. Przełącznik musi wspierać agregację łączy ethernet zgodną ze standardem 802.3ad (LACP). Pojedynczy interfejs zagregowany musi składać się z co najmniej czterech interfejsów składowych.

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.2. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego.

3.2.1. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.3. Przełącznik musi zapewniać możliwość cofnięcia zmian konfiguracji,

3.4. Przełącznik musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

3.5. CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.6. Przełącznik musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.7. Przełącznik musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.8. Przełącznik musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.8.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.9. Przełącznik musi wspierać mechanizm SNMP Trap (STD 62).

3.10. Przełącznik musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 4741, NETCONF Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.11. Przełącznik musi zapewniać możliwość tworzenia wielu poziomów dostępu do urządzenia (nie mniej niż czterech – full-access, read-only, różne poziomy ograniczenia dostępu, np. operator 1 / 2 linii wsparcia, systemy provisioningu ograniczone do wybranych funkcjonalności).

3.12. Przełącznik musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.13. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).
3.14. Przełącznik musi mieć możliwość zdalnej aktualizacji oprogramowania.
3.15. Przełącznik musi posiadać port terminalowy do dołączenia konsoli (RS-232).
3.16. Przełącznik musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez Urządzenie zdarzeniach do zdalnego serwera syslog.
3.17. Przełącznik musi obsługiwać protokół NTP.
3.18. Przełącznik musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.
3.18.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.
3.18.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 500 wpisów.
3.18.3. Przełącznik musi mieć możliwość założenia ACL, na każdym interfejsie logicznym z obsługą protokołu IPv4 i/lub IPv6, w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.
3.18.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. przełącznik musi umożliwiać aktywacje obu typów na interfejsie logicznym.

4. Wymagania przełączania
4.1. Przełącznik musi mieć nieblokującą architekturę, zapewniającą bezstratną transmisję ramek pomiędzy dwoma dowolnymi portami, przy założeniu, ze wszystkie porty nadają i odbierają ruch z pełną prędkością.
4.2. Przełącznik musi mieć możliwość utworzenia nie mniej niż 100 VLAN o dowolnej numeracji zgodnie z 802.1q.
4.3. Przełącznik musi obsługiwać nie mniej niż 16 000 adresów MAC (dla węzłów WAW, POZ, KAT 24 000 adresów MAC).
4.4. Przełącznik musi wspierać następujące protokoły:
4.4.1.RSTP (802.1w)
4.4.2.PVSTP lub równoważny (za protokół równoważny uważny jest taki, który umożliwia stworzenie oddzielnego drzewa rozpinającego (ang. spanning tree) dla każdego skonfigurowanego VLANu, czyli nie mniej niż 100 drzew rozpinających).

5.4.4. Wymagania dla serwera terminalowego

W ramach oferty Wykonawca zapewni serwery terminalowe spełniające następujące funkcje:

1. Urządzenie umożliwiające zdalny dostęp do konsol urządzeń zainstalowanych w węzłach przez porty RS-232.
1.1. Urządzenie musi umożliwiać jednoczesną pracę nie mniej niż czterech (4) operatorów, dołączonych do różnych linii terminalowych.
2. Urządzenie może być zrealizowane jako:
2.1. dedykowana karta do routera sieci zarządzania, wyposażona w odpowiednią ilość kabli (za wyjątkiem standardowych kabli UTP zakończonych obustronnie wtyczkami RJ45),
2.2. Dedykowane urządzenie (bez redundancji).
3. W przypadku realizacji jako dedykowane urządzenie serwer terminalowy mu spełniać następujące wymagania:
3.1. Urządzenie musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.

3.2. Dopuszczalne jest zaoferowanie urządzeń nie posiadających możliwości instalacji w szafie teleinformatycznej. W takim wypadku konieczne jest dodanie do oferty standardowej półki do takiej szafy, zaś jako wysokość urządzenia należy przyjąć wysokość urządzenia (nie mniej niż 1 RU) oraz wysokość półki (nie mniej niż 1 RU).

3.3. Urządzenie musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.

3.4. Urządzenie musi być wyposażone w zasilacze dostosowane do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających. Urządzenie musi być wyposażone w co najmniej jeden zasilacz.

3.5. Urządzenie musi poprawnie pracować w temperaturze od 5 do 40 °C.

3.6. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 5% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

3.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

3.8. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta Urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

3.9. Urządzenie będzie wyposażone w co najmniej jeden port Ethernet 10/100 do dołączenia do sieci zarządzania.

3.10. Wszystkie interfejsy zainstalowane w urządzeniu muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

3.11. Interfejs konfiguracyjny urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.12. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ lub RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.13. Alternatywnie możliwe jest zapewnienie autoryzacji użytkowników przy wykorzystaniu LDAP, przy założeniu funkcjonalności jak w zdaniu poprzednim.

3.14. Urządzenie musi obsługiwać protokół NTP.

5.4.5. Wymagania na ilość interfejsów w urządzeniach sieci zarządzania

Ilości portów w sieci zarządzania w poszczególnych węzłach są następujące:

Węzeł	sieć LAN	RS232
WAW	160	57
WAW dodatkowy	24	12
KAT	121	54
POZ	127	34
KRA	78	33
RZE	77	42
LUB	76	41
WRO	77	42
LOD	79	44
GDA	76	41
TOR	73	38
SZC	69	34
OLS	66	36
KIE	63	33
BIA	63	33
OPO	52	27
ZGO	54	29

5.5. Wymagania na urządzenia „shadow router”

W sieci OSE zaimplementowany zostanie system pomiarów jakości usług. Oparty on zostanie o mechanizm badania jakości sieci w oparciu o wykorzystanie shadow routerów oraz mechanizm klasy IP SLA / RPM / NQA / SAA lub równoważny.

Shadow routery to dedykowane urządzenia, dołączone bezpośrednio do Routerów Agregacyjnych lub Szkieletowych emulujące urządzenia abonenckie (CPE). Z urządzeń tych wysyłane będą próbki testujące podstawowe parametry definiujące jakość usług sieciowych, tj. opóźnienia, straty pakietów, jitter. Do jednego Routera Agregacyjnego lub Szkieletowego będzie dołączony jeden shadow router interfejsem 1GE, ze stykiem fizycznym 1000Base-SX lub 1000Base-T (do wyboru Wykonawcy).

1. Wymagania ogólne
   - 1.1. Wszystkie oferowane urządzenia (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
     - 1.1.1. Wykonawca musi być oficjalnym sprzedawcą w Polsce oferowanych urządzeń.
     - 1.1.2. Wykonawca musi mieć możliwość świadczenia autoryzowanego przez producenta serwisu gwarancyjnego.
   - 1.2. Zamawiający wymaga, aby urządzenia typu shadow router były jednego typu, w jednakowej konfiguracji we wszystkich Węzłach Szkieletowych i Agregacyjnych.

1.3. Urządzenie musi być przystosowane do instalacji w standardowych 19” szafach teleinformatycznych (EIA-310-D, IEC 60297). Urządzenie musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.

1.3.1. Urządzenie musi posiadać wymiary umożliwiające montaż w szafie teleinformatycznej o głębokości 1000mm, tj. głębokość i konstrukcja urządzenia muszą zapewnić w szafie o takiej głębokości dołączenie zasilania, przewodów światłowodowych oraz miedzianych przy zapewnieniu wymaganych promieni zginania przewodów.

1.4. Urządzenie musi być wyposażone w co najmniej jeden zasilacz dostosowany do napięcia przemiennego 230V. Dostarczone urządzenie będzie wyposażone w odpowiednią liczbę kabli zasilających pozwalających na podłączenie wszystkich zasilaczy, w jakie jest wyposażone urządzenie do standardowych gniazd zasilających.

1.5. Urządzenie musi poprawnie pracować w temperaturze otoczenia od 5 do 40 °C.

1.6. Urządzenie musi poprawnie pracować przy wilgotności powietrza od 10% do 80% zakładając brak występowania zjawiska kondensacji pary wodnej.

1.7. Wszystkie wymagane funkcjonalności muszą być dostępne w jednej, komercyjnie dostępnej wersji oprogramowania, tj. wersji oferowanej wszystkim klientom. Wersja ta musi być wersją rekomendowaną przez producenta. Niedopuszczalne jest wytwarzanie wersji oprogramowania wyłącznie na potrzeby Zamawiającego, nie oferowanej innym klientom.

1.8. Dokumentacja do urządzenia (w tym oprogramowania) musi być dostępna w całości w języku polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML) lub dostępna na stronie producenta urządzenia (jeżeli dostęp do tej dokumentacji wymaga autoryzacji Wykonawca zapewni do niej dostęp dla wskazanych pracowników Zamawiającego lub podmiotów wskazanych przez Zamawiającego). W przypadku dokumentacji on-line musi istnieć możliwość jej pobrania do przeglądania off-line.

2. Wymagania na interfejsy

2.1. Karty liniowe lub moduły urządzenia zawierające interfejsy przeznaczone do obsadzenia modułami optycznymi (ang. transceiver), muszą współpracować z modułami optycznymi (zgodnymi z ogólnie przyjętymi normami właściwymi dla danego typu interfejsu), pochodzącymi od różnych producentów[13]. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na Urządzenie ani ograniczeń w świadczeniu usług serwisowych

Wykorzystywanie modułów optycznych innych producentów nie może wymagać restartu urządzenia ani nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych (dopuszczalne jest jednorazowe uruchomienie funkcjonalności dla całego urządzenia umożlwiające korzystanie z ww. wkładek instalowanych w dowolnym momencie).

2.2. Dostarczone moduły optyczne (o ile urządzenie jest w nie wyposażone) muszą umożliwiać możliwość sprawdzenia mocy odbieranego sygnału, tj. muszą wspierać funkcjonalność digital diagnostics monitoring (DDM)[14] zgodną z SFF-8472 (Digital Diagnostics Monitoring, Digital Optical Monitoring) lub równoważne

[13] W przypadku, gdy wykorzystanie modułów optycznych pochodzących od innych producentów, wymaga wykonania dodatkowych czynności polegających na rekonfiguracji Urządzenia, Wykonawca zobowiązany jest przedstawić szczegółową dokumentację techniczną, zawierającą informację na temat sposobu ich przeprowadzenia.

[14] Funkcjonalność często określaną również jako digital optical monitoring (DOM).

2.3. Urządzenie musi obsługiwać ramki Ethernet o wielkości co najmniej 9100B.

2.4. Wszystkie interfejsy liniowe zainstalowane w urządzeniu (bezpośrednio w chassis lub na kartach interfejsów) muszą być odblokowane. Oznacza to, że nie mogą posiadać żadnych blokad umożliwiających ich wykorzystanie dopiero po wprowadzeniu jakiejkolwiek licencji, klucza, kodu lub innego mechanizmu odblokowującego. Dotyczy to wszystkich interfejsów znajdujących się fizycznie w oferowanym urządzeniu.

2.5. Znaczenie pola VID (VLAN ID) musi mieć znaczenie lokalne dla interfejsu fizycznego, co oznacza, że ten sam znacznik VID może być użyty niezależnie na wielu interfejsach fizycznych urządzenia.

3. Zarządzanie i monitorowanie urządzeń

3.1. Wszystkie opcje konfiguracyjne muszą być możliwe do zmiany z wykorzystaniem interfejsu tekstowego (ang. Command Line Interface = CLI).

3.1.1. Cała konfiguracja urządzenia musi być zapisywana do pojedynczego pliku tekstowego. Plik ten musi być w formacie umożliwiającym jego bezpośrednie odczytanie przez administratora oraz jego bezpośrednią edycję (tj. przy użyciu dowolnego edytora tekstu np. vi, notepad++).

3.1.2. Urządzenie musi zapewniać możliwość tworzenia i przywracania kopii zapasowych konfiguracji,

3.1.3. CLI urządzenia (generowane komunikaty i wydawane komendy) musi bazować na języku angielskim lub polskim (dopuszczalne jest stosowanie skrótów lub nazw własnych mających jednak za bazę języki polski lub angielski).

3.2. Urządzenie musi zapewniać możliwość współpracy z serwerami autoryzacji TACACS+ i RADIUS (zgodnie z RFC2865), w szczególności przy umożliwianiu dostępu do CLI), bez konieczności tworzenia lokalnej informacji o każdym użytkowniku wraz z przypisaniem użytkownika do odpowiedniej grupy na podstawie informacji otrzymanych z serwera autoryzującego.

3.3. Urządzenie musi wspierać RADIUS Accounting zgodnie z RFC2866 umożliwiający rejestrowanie co najmniej następujących zdarzeń: informacji o logowaniu i wylogowaniu się administratora, wydaniu komendy (wraz z jej treścią), zapisania konfiguracji.

3.4. Urządzenie musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).

3.4.1. Dane zbierane przy wykorzystaniu protokołu SNMP muszą być identyczne z danymi jakie można zebrać przez CLI.

3.4.2. Urządzenie musi pozwalać na zbieranie następujących statystyk przez protokół SNMP w sposób nie powodujący znacznego obciążenia procesorów urządzenia z cyklicznością 1 pobranie danych na 5 minut:

- statystyki ruch dla interfejsów (w tym wolumenu ruchu przechodzącego przez urządzenie – jednocześnie dla wszystkich interfejsów fizycznych i logicznych, w tym sub-interfejsów),
- [usunięto]
- informacje o wykorzystaniu kolejek,
- statystyki dla ACL.

3.5. Urządzenie musi wspierać mechanizm SNMP Trap (STD 62).

3.6. Urządzenie musi oferować interfejs programowy do współpracy z aplikacjami (API lub SDK). Wymagana jest obsługa NETCONF (RFC 6241, Network Configuration Protocol), za pomocą

którego możliwe będzie konfigurowanie urządzenia oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itd.)

3.7. Urządzenie musi zapewniać możliwość uwierzytelniania administratora poprzez klucz SSH.

3.8. Na urządzeniu musi być możliwość wyłączenia dostępu terminalowego przy wykorzystaniu protokołów nieszyfrowanych (telnet).

3.9. Urządzenie musi mieć możliwość zdalnej aktualizacji oprogramowania.

3.10. Urządzenie musi posiadać port terminalowy do dołączenia konsoli (RS-232).

3.11. Urządzenie musi posiadać dodatkowy port typu Ethernet (10/100/1000 lub 10/100), za pomocą którego możliwe będzie zarządzanie urządzeniem poza pasmem (ang. out-of-band management = OOB). Opcją alternatywną jest możliwość skonfigurowania jednego z portów jako portu OOB (port musi mieć styk 1000Base-T lub 10/100/1000).

3.12. Urządzenie musi obsługiwać mechanizm syslog, pozwalający na przesyłanie informacji o zarejestrowanych przez urządzenie zdarzeniach do zdalnego serwera syslog.

3.13. Urządzenie musi obsługiwać protokół NTP.

3.14. Urządzenie musi mieć możliwość tworzenia list kontroli dostępu (ACL) dla IPv4 i IPv6.

3.14.1. Muszą być dostępne liczniki trafień w poszczególne wpisy list.

3.14.2. Listy kontroli dostępu muszą mieć długość nie mniejszą niż 50 wpisów każda.

3.14.3. Urządzenie musi mieć możliwość założenia ACL na każdym interfejsie logicznym w kierunku wejściowym i wyjściowym. Dotyczy to jedoczesnego założenia ACL na wszystkich skonfigurowanych interfejsach, przy czym każdy interfejs może mieć inną listę kontroli dostępu.

3.14.4. Listy ACL IPv4 i IPv6 nie mogą się wykluczać, tj. urządzenie musi umożliwiać aktywacje obu typów na interfejsie logicznym.

4. Wymagane funkcjonalności routingu IP:

4.1. Urządzenie musi obsługiwać IPv4 oraz IPv6 przy czym rozkład ruchu pomiędzy oba protokoły (tj. IPv4 i IPv6) nie może wpływać na funkcjonalność urządzenia,

4.1.1. Obsługa IPv4 oraz IPv6 musi być możliwa bez żadnych ograniczeń co do interfejsów.

4.2. Urządzenie musi obsługiwać mechanizm multi-VRF, umożliwiający utrzymywanie oddzielnych tablic routingu (ang. Virtual Routing and Forwarding) dla sieci wirtualnych,

4.2.1. Urządzenie musi umożliwiać utworzenie i jednoczesne działanie nie mniej niż 8 VRF.

5. Wymagania na pomiary

5.1. Urządzenie musi wspierać mechanizm IP SLA lub RPM lub NQA lub SAA lub równoważny.

5.2. Urządzenie musi umożliwiać pomiar następujących parametrów:

5.2.1. opóźnienie (RTT),

5.2.2. straty pakietów,

5.2.3. jitter.

5.3. Urządzenie musi umożliwiać próbkowanie przy pomocy protokołów:

5.3.1. ICMP,

5.3.2. TCP,

5.3.3. UDP,

5.3.4. HTTP (pobranie strony WWW z podanego adresu),

5.3.5. DNS (wysłanie zapytania DNS – UDP/53 lub UDP-ECHO na port docelowy 53).

5.4. Wszystkie wymienione powyżej pomiary (w pkt. 5.2 i 5.3) muszą być wykonywane dla IPv4 i IPv6.

5.5. Urządzenie musi mieć możliwość oznaczania pakietów używanych do próbkowania zadanymi wartościami DSCP;
5.6. Urządzenie musi mieć możliwość wykonywania cyklicznych pomiarów. Pomiar musi być wykonywany nie rzadziej niż raz na 5 minut.
5.7. Urządzenie musi mieć możliwość badania wszystkich parametrów wewnątrz dowolnego VRF.
5.8. Urządzenie musi umożliwiać jednoczesne pomiary w co najmniej 8 VRF.

6. Wymagania na Węzeł Laboratoryjny

Wykonawca dostarczy do miejsca wskazanego przez Zamawiającego kompletne środowisko laboratoryjne (Węzeł Laboratoryjny), zgodnie z poniższymi wymaganiami.

6.1. Wymagania na środowisko fizyczne

Celem ww. środowiska będzie możliwość odtworzenia dowolnego fragmentu sieci OSE na potrzeby rozwiązywanie problemów sieciowych, a także na potrzeby testowania nowych wersji oprogramowania przez jego wdrożeniem w sieci OSE.

Z ww. powodów środowisko musi objąć po jednym urządzeniu z dostarczonych modeli Urządzeń szkieletowych i agregacyjnych, przy takim wyposażeniu w karty, aby reprezentowane były wszystkie modele Urządzeń i kart zainstalowanych w węzłach sieci OSE.

Do środowiska fizycznego należy dołączyć komplet Urządzeń sieci zarządzania (router, przełącznik 48 portowy oraz serwer terminalowy 24 portowy).

6.2. Wymagania na przełącznik sieci lokalnej

Wykonawca dostarczy przełącznik sieci lokalnej, spełniający wymagania wymienione w pkt. 5.3 „Wymagania na Przełączniki Sieci Lokalnej”.

Przełącznik będzie wyposażony w 20 portów 10GE / 25GE, z czego 12 portów będzie obsadzonych optyką w standardzie 10GBase-SR.

Dodatkowo przełącznik będzie miał możliwość dołączenia serwera hostującego środowisko wirtualne. W gestii Wykonawcy jest zapewnienie odpowiednich ilości wkładek, zarówno po stronie przełącznika, jak też serwera. Dopuszczalne jest wykorzystanie przełącznika sieci zarządzania do dołączenia serwera środowiska wirtualnego. W takim wypadku konieczne jest zapewnienie bezpośredniego połączenia pomiędzy przełącznikami.

6.3. Wymagania na środowisko wirtualne

Wykonawca dostarczy kompletne środowisko wirtualne zapewniające modelowanie sieci OSE.

Środowisko to musi zapewniać zamodelowanie całej sieci OSE, to znaczy Urządzeń szkieletowych, agregacyjnych oraz pełniej funkcjonalności CG-NAT oraz dodatkowo nie mniej niż 30 urządzeń CPE (urządzenia zgodne z wymaganiami POPC). Środowisko to musi zapewniać możliwość testowania nowych funkcjonalności przed wdrożeniem do sieci OSE, a co za tym idzie musi mieć możliwość pracy z wersjami oprogramowania identycznymi z tymi, które są używane w sieci OSE.

W ramach środowiska wirtualnego, Wykonawca dostarczy odpowiednio wyskalowany serwer wraz ze wszystkimi wymaganymi licencjami.

6.4. Wymagania na testową instalację Oprogramowania System Zarządzania

Zamawiający dostarczy oprogramowanie identyczne z oferowanym Systemem Zarządzania (możliwe jest nałożenie ograniczeń wydajnościowych) wraz z licencją umożliwiającą wykorzystanie tego oprogramowania wyłącznie do celów rozwojowo-testowych (bez prawa do wykorzystania w sieci eksploatowanej komercyjnie).

Oferowane oprogramowanie (wraz z licencję) musi zapewniać możliwość współpracy z oferowanym testowym środowiskiem fizycznym oraz współpracy z systemami testowymi OSS/BSS Zamawiającego.

7. Warunki dostawy

1. Wykonawca będzie dostarczał Urządzenia do każdego Węzła, odpowiednio Szkieletowego, Agregacyjnego lub Laboratoryjnego wraz z Urządzeniami sieci lokalnej i zarządzania, realizujących wszystkie opisane w wymaganiach funkcje, zapewniające określoną funkcjonalność oraz ilość portów o zdefiniowanych przepustowościach. Całość 16 Węzłów Agregacyjnych oraz 3 Węzłów Szkieletowych stanowi System.
2. Wszystkie oferowane Urządzenia (wraz z zainstalowanym na nich oprogramowaniem) muszą pochodzić od jednego producenta.
   Z powyższego wyłączne są:
   - urządzenia realizujące funkcjonalność CG-NAT (pkt 5.2),
   - urządzenia „shadow router” (pkt 4.4 i 5.5),
   - serwery terminali sieci zarządzania (pkt 5.4.4),
   - modemy LTE sieci zarządzania (pkt. 5.4.2, ppkt 2.1.3).
3. Dostarczane Urządzenia muszą być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed dniem dostawy, w oryginalnych opakowaniach transportowych producenta. Zamawiający dopuszcza rozpakowanie urządzeń przez Wykonawcę w celu przeprowadzenia przez Wykonawcę testu sprawności Urządzeń i wykonania ich konfiguracji wstępnej. Po dostarczeniu Urządzeń do miejsca ich instalacji i wykonaniu prac instalacyjnych Wykonawca jest zobowiązany do usunięcia opakowań transportowych na własny koszt.
4. Każde z dostarczonych urządzeń, wchodzących w skład kompletu stanowiącego Węzeł, musi mieć zainstalowane rekomendowane do stosowania przez producentów Urządzeń wersje Oprogramowania. Ww. Oprogramowanie w dostarczonej wersji musi posiadać wsparcie techniczne producenta dostarczanych Urządzeń.
5. Wszystkie Urządzenia, należące do jednej rodziny Urządzeń, w ramach całego zamówienia będą wyposażone w tą samą (identyczną) wersję Oprogramowania. W przypadku gdyby producent urządzeń zmienił rekomendowaną wersje oprogramowania dla danej rodziny Urządzeń, Wykonawca powiadomi o tym Zamawiającego, a następnie uzgodni z Zamawiającym wersję Oprogramowania, która będzie instalowana na Urządzeniach w ramach kolejnych dostaw oraz wykona aktualizację Oprogramowania na Urządzeniach.
6. Każde z dostarczonych Urządzeń, stanowiących elementy składowe poszczególnych Węzłów, będzie pochodzić z oficjalnego kanału dystrybucyjnego producenta, zapewniającego w szczególności realizację uprawnień gwarancyjnych oraz autoryzowanego serwisu na terenie

Polski. Na żądanie Zamawiającego Wykonawca dostarczy w ciągu 14 dni oficjalne potwierdzanie tego faktu wystawione przez producenta Urządzeń.

7. Dostarczone Urządzenia w dniu złożenia oferty nie będą znajdować się na liście sprzętu przeznaczonego do wycofania z produkcji lub sprzedaży na terenie Polski.

8. Wdrożenie

8.1. Przebieg wdrożenia

1. Przez cały okres trwania wdrożenia Wykonawca wydeleguje osobę odpowiedzialną za realizację przedmiotu zamówienia (Kierownika Projektu), która będzie współpracowała z osobą o analogicznych odpowiedzialnościach ze strony Zamawiającego.
2. Przedstawiciele Stron, odpowiedzialni za realizację Wdrożenia będą realizować cykliczne spotkania w celu m.in. wymiany informacji o postępach w pracach, rozwiązywania problemów. Szczegóły dotyczące częstości i miejsc spotkań zostaną uzgodnione w trybie roboczym.
3. Zamawiający, w ramach przygotowania do wdrożenia, jest zobowiązany do zapewnienia, z zachowaniem odpowiedniego wyprzedzenia w stosunku do planowanych dostaw sprzętu, następujące zasoby niezbędne do uruchomienia węzła:
   - powierzchnię kolokacyjną wraz z wyposażeniem w szafy,
   - zasilanie szaf w energię elektryczną,
   - elementy pasywne umożliwiające budowę okablowania pomiędzy szafami,
   - okablowanie stacyjne pomiędzy szafą a punktem koncentracji infrastruktury kablowej Obiektu oraz pomiędzy szafami,
   - łącza szkieletowe służące do komunikacji pomiędzy poszczególnymi węzłami OSE,
4. Zamawiający jest zobowiązany do uzyskania w terminach wynikających z Szczegółowego Harmonogramu Wdrożenia Węzła wszelkich niezbędnych zezwoleń i zgód umożliwiających prowadzenie instalacji i uruchomienia Urządzeń i Oprogramowania w Obiekcie.
5. Zamawiający jest zobowiązany do umożliwienia pracownikom Wykonawcy dostępu do Obiektu, w godzinach od 8.00 do 18.00 w Dniach roboczych oraz w szczególnych przypadkach w uzgodnionych przez Strony godzinach, a także dostęp do niezbędnych mediów (np. energia elektryczna).
6. Wykonawca jest zobowiązany do dostarczenia i instalacji Urządzeń oraz Oprogramowania wraz z licencjami, niezbędnych do funkcjonowania Systemu, w tym między:
   - Wykonania Okablowania stacyjnego, łączącego ze sobą Urządzenia w obrębie szafy oraz Urządzenia w różnych szafach, zgodnie z Dokumentacją,
   - Zapewnienie kabli przyłączeniowych, do łączenia instalowanych Urządzeń ze sobą oraz z panelami połączeniowymi,
   - Zapewnienie osprzętu i materiałów instalacyjnych do montażu dostarczonych Urządzeń,
7. Wykonawca dostarczy, w terminach wynikających ze Szczegółowego Harmonogramu Wdrożenia, Urządzenia stanowiące kompletne wyposażenie Węzła, odpowiednio Szkieletowego lub Agregacyjnego, realizującego wszystkie założone funkcjonalności w skali ruchu określonego w pkt. 3 „” i pkt. 5 „Wymagania dla Węzła Agregacyjnego”, a następnie wykona prace instalacyjne w lokalizacji wskazanej przez Zamawiającego.
8. Wszystkie dostarczone Urządzenia zostaną przez Wykonawcę trwale zainstalowane w szafach telekomunikacyjnych z zastosowaniem dedykowanych uchwytów mocujących, a następnie okablowane w sposób umożliwiający komunikację pomiędzy nimi, zgodnie z Projektem Technicznym.
9. W celu komunikacji pomiędzy Urządzeniami instalowanymi w różnych szafach Wykonawca zastosuje kable korespondencyjne instalowane w Szafach i kończona na panelach połączeniowych. Standardem styku dla optycznych paneli połączeniowych, stosowanych do zakańczania kabli

światłowodowych w szafach będzie SC/APC. Złącza powinny być wykonane w klasie Premium. Kable korespondencyjne pomiędzy szafami będą wykonywane z wykorzystaniem istniejącej infrastruktury technicznej, takiej jak drabinki bądź koryta kablowe. Nie dopuszcza się prowadzenia okablowania przez ściany boczne szaf. Dla przypadków stosowania połączeń z użyciem kabli typu DAC nie będzie konieczności budowy kabli korespondencyjnych.

10. Wykonawca dostarczy i zainstaluje kable połączeniowe umożliwiające połączenie pomiędzy Urządzeniami w tej samej szafie oraz pomiędzy Urządzeniami a panelem połączeniowym. Wykonawca ułoży wszystkie kable połączeniowe w sposób uporządkowany, z zastosowaniem dostarczonych przez siebie organizerów okablowania. Wykonawca przytwierdzi ułożone okablowanie w sposób umożliwiający dostęp do poszczególnych urządzeń w szafie, jak również w sposób umożliwiający wymianę uszkodzonych elementów Urządzeń (kart) bez konieczności deinstalacji okablowania.
11. Położone przez Wykonawcę okablowanie korespondencyjne, kable połączeniowe oraz kable DAC zostaną w sposób czytelny oznaczone, a oznaczenie to zostanie udokumentowane w Dokumentacji Powykonawczej. Sposób oznaczania okablowania zostanie uzgodniony pomiędzy stronami w trybie roboczym.
12. Wykonawca po wykonaniu instalacji oraz okablowania dokona podłączenia Urządzeń do zainstalowanych w szafach listew dystrybucji zasilania. Włączenie Urządzeń do zasilania odbędzie się w oparciu o regulacje obowiązujące w zakresie podłączania odbiorników energii elektrycznej na terenie danego Obiektu. Pracownicy lub podwykonawcy Wykonawcy, realizujący podłączenie Urządzeń do zasilania, będą posiadali stosowne kwalifikacje.
13. Wykonawca wykona konfigurację dostarczonych Urządzeń zgodnie z uzgodnionym Projektem Technicznym. Zakres konfiguracji Urządzeń będzie obejmował pełen zakres wdrożenia.
14. Wykonawca, w oparciu o dostarczone przez Zamawiającego łącza szkieletowe OSE uruchomi komunikację z innymi węzłami, zgodnie ze strukturą połączeń określoną w pkt. 5 „Wymagania dla Węzła Agregacyjnego" ppkt. „Inne wymagane parametry wydajnościowe dla Routerów Agregacyjnych". Łącza szkieletowe będą kończone w szafach na panelach połączeniowych realizowanych poza Umową. Wykonawca zapewni kable połączeniowe umożliwiające połączenie Urządzeń z w/w panelami połączeniowymi. W przypadku uruchamiania pierwszego Węzła struktura połączeń z innymi węzłami nie będzie jeszcze istniała, zatem w tym aspekcie uruchomienie nie nastąpi.
15. W trakcie prac instalacyjnych i konfiguracyjnych Wykonawca jest zobowiązany wysyłać Zamawiającemu cykliczne raporty z zaawansowania prac. prac. Raport musi zawierać informacje o stopniu zawansowania prac, planowanych pracach na kolejny okres oraz wskazywać ewentualne ryzyka i sposoby ich zarządzenia. Raport będzie przekazywany podczas cyklicznych spotkań, o których mowa w ust. 2.
16. Zamawiający ma prawo uczestniczyć na każdym etapie prac instalacyjnych i konfiguracyjnych. W ramach uczestniczenia w pracach Wykonawca ma prawo m.in. kontrolować jakość wykonywanych prac instalacyjnych jak również dotrzymywanie zasad prowadzenia prac na Obiekcie.
17. Po zakończeniu prac wdrożeniowych Wykonawca przygotuje i przekaże do Zamawiającego Dokumentację Powykonawczą. Zakres dokumentacji powykonawczej został określony w Załączniku nr 6 do Umowy.
18. Wraz z realizacją Węzła Szkieletowego w Warszawie Wykonawca zainstaluje i skonfiguruje wg Dokumentacji Technicznej oraz wytycznych Zamawiającego Oprogramowanie System Zarządzania. Wykonawca skonfiguruje Urządzenia do współpracy z Oprogramowaniem, a także do współpracy

z innymi wskazanymi systemami OSS Zamawiającego, realizowane w ramach Integracji. Za przygotowanie platform sprzętowo-programowych do instalacji systemów nadzoru odpowiedzialny jest Zamawiający.

19. Wykonawca przeprowadzi, wspólnie z Zamawiającym, procedurę testów odbiorczych węzła, w oparciu o zatwierdzony Plan testów, zgodnie z opisem zawartym w § 4 Umowy.
20. Wykonawca zobowiązany jest zapewnić, aby wszystkie czynności odbiorcze, w tym również związane z uwzględnianiem uwag i zastrzeżeń Zamawiającego do Dokumentacji Powykonawczej zostały zakończone w terminach wynikających ze Szczegółowego Harmonogramu Wdrożenia Węzła.

8.2. Podział obowiązków stron przy realizacji Umowy

Wykonawca przy tworzeniu oferty oraz podczas wdrożenia węzłów i świadczenia usług (w tym usług gwarancji), musi uwzględnić poniższy podział obowiązków:

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
1.	Podpisanie Umowy	x	x	
2.	Wyznaczenie Kierowników Projektu	x	x	2 dni
3.	Przygotowanie i przedstawienie do wypełnienia ankiety w zakresie HLD		x	
4.	Wypełnienie ankiety w zakresie HLD wraz z konsultacjami	x		5 dni
5.	Przygotowanie Dokumentacji Technicznej w zakresie HLD i przekazanie do akceptacji		x	
6.	Akceptacja Dokumentacji Technicznej w zakresie HLD lub zgłoszenie uwag.	x		5 dni
7.	Przeprowadzenie instruktaży		x	
8.	Utrzymanie		x	
9.	Świadczenie gwarancji w okresie trwania umowy		x	
10.	Przekazanie listy uprawnionych przedstawicieli do dostępu zdalnego do systemu		x	
11.	Zapewnienie dostępu zdalnego uprawnionym przedstawicielom	x		
12.	Zapewnienie uprawnionym przedstawicielom Wykonawcy do urządzeń zainstalowanych w węzłach	x		

8.3. Podział obowiązków stron przy wdrożeniu Węzła

Wykonawca stworzy Szczegółowy Harmonogram Wdrożenia Węzła na podstawie następującego podziału obowiązków pomiędzy Strony:

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
1.	Wydanie Polecenia Wdrożenia Węzła	x		
2.	Przygotowanie Szczegółowego Harmonogramu Wdrożenia Węzła		x	
3.	Przygotowanie i przedstawienie do wypełnienia ankiety w zakresie LLD		x	

L.p.	Zadanie	Zamawiający	Wykonawca	Czas wykonania
4.	Wypełnienie ankiety w zakresie LLD wraz konsultacjami	x		5 dni
5.	Przygotowanie Dokumentacji Technicznej w zakresie LLD i przekazanie do akceptacji		x	
6.	Akceptacja Dokumentacji Technicznej w zakresie LLD lub zgłoszenie uwag	x		5 dni
7.	Przygotowanie i przedstawienie do akceptacji Planu Testów Odbiorczych		x	
8.	Weryfikacja i zatwierdzenie Planu Testów Odbiorczych lub zgłoszenie uwag	X		5 dni
9.	Przygotowanie Obiektów do instalacji Urządzeń zgodnie z Rozdziałem 11 ust. 3	x		60 dni od Polecenia wdrożenia Węzła
10.	Zgłoszenie gotowości dostawy Urządzeń		x	
11.	Potwierdzenie gotowości dostawy Urządzeń	x		2 dni
12.	Dostawa i odbiór ilościowy	x	x	
13.	Przekazanie listy uprawnionych przedstawicieli do wstępu na obiekty, w których będą instalowane urządzenia		x	
14.	Zapewnienie dostępu uprawnionym przedstawicielom Wykonawcy.	x		3 dni
15.	Instalacja Urządzeń w szafach zgodnie z Rozdziałem 11 ust. 6		x	
16.	Podłączenie Urządzeń do zasilania i uziemienia		x	
17.	Uruchomienie Urządzeń		x	
18.	Konfiguracja Urządzeń		x	
19.	Zestawienie łączy szkieletowych do szafy	x		
20.	Dołączenie łączy szkieletowych do zainstalowanych urządzeń		x	
21.	Uczestniczenie w pracach instalacyjnych i wdrożeniowych	x		
22.	Zgłoszenie gotowości do Testów Odbiorczych		x	
23.	Testy Odbiorcze	x	x	2 tygodnie
24.	Przygotowanie dokumentacji powykonawczej		x	
25.	Akceptacja dostarczonej Dokumentacji, akceptacja wykonanych prac instalacyjnych węzła lub wniesienie uwag	x		5 dni
26.	Podpisanie Protokołu Odbioru Wstępnego	x	x	
27.	Stabilizacja		x	
28.	Zgłoszenie gotowości do Odbioru Końcowego		x	
29.	Weryfikacja poprawności zakończenia Okresu Stabilizacji lub wniesienie uwag	x		
30.	Odbiór Końcowy Węzła	x	x	
31.	Podpisanie Protokołu Odbioru Końcowego	x	x	