OPIS PRZEDMIOTU ZAMÓWIENIA - ZMIENIONY

pn. Dostawa wielofunkcyjnych routerów z interfejsami 10/40/100GE

1. Wymagania podstawowe

W ramach niniejszego postepowania Wykonawca musi dostarczyć 2 (dwa) nowe wielofunkcyjne urządzenia sieciowe, sklasyfikowane jako „router" spełniające wymagania opisane w dalszych punktach specyfikacji.
Wraz z urządzeniami muszą być dostarczone 4 (cztery) kompatybilne moduły optyczne QSFP+ 40GB zakończone złączem LC/PC. Moduły muszą posiadać interfejs DDMI oraz umożliwiać transmisję na odległość do 10km.
Klasyfikacja urządzenia jako „router" jest dokonywana na podstawie funkcji realizowanych przez urządzenie sieciowe i jest niezależna od klasyfikacji dokonywanej przez danego producenta sprzętu sieciowego. Zamawiający uzna, że występujące w literaturze (dokumentacji) technicznej nazwy router i przełącznik MPLS są tożsame o ile jest to urządzenie sieciowe realizujące przełączanie pakietów na podstawie etykiet opisane w dokumentach IETF:

- RFC 3031 „Multiprotocol Label Switching Architecture"
- RFC 3032 „MPLS LabelStack Encoding"

W dalszej części opisu technicznego, o ile nie zaznaczono inaczej, **router** i/lub **przełącznik MPLS** nazywany jest **routerem**. Użycie tego określenia nie wpływa na ograniczenie lub wyróżnienie innych funkcji realizowanych przez urządzenia będące przedmiotem zamówienia, przynależnych do urządzeń określonego typu (np. przełączania pakietów IP wykonywanego przez routery lub przełączania ramek Ethernet przez przełączniki Ethernet).
W przypadku określenia wymagań odnoszących się do standardów i dokumentów normatywnych, jako oczywiste dopuszczalne są rozwiązania oparte na nowszych wersjach standardów (dokumentów normatywnych) lub zastępujących (zgodnie z zasadami przyjętymi przez organ standaryzacyjny) podane w specyfikacji. Wszystkie routery oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane za wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. „end of sale") ani wsparcia technicznego (ang. „end of life").
Wszystkie routery (wraz z działającym na nich oprogramowaniem sterującym) muszą pochodzić od jednego producenta. Jeżeli w wymaganiach nie określono inaczej, wymagana liczba prefiksów (IPv4/IPv6), adresów MAC, ścieżek LSP, VLL/VPLS oraz filtrów oznacza ilości jakie muszą być aktywne (tj. używane aktualnie przez router) a nie jedynie przechowywane w pamięci (np. w bazie RIB).

2. Parametry sprzętowe

2.1. Router musi być przystosowany do instalacji w standardowych 19" szafach teleinformatycznych (EIA-310). Router musi posiadać wszystkie elementy potrzebne do zainstalowania go w szafie.
2.2. Router musi mieć wysokość maksymalnie 1RU.
2.3. Router musi poprawnie pracować w temperaturze od 0 do 40 °C.
2.4. Router musi poprawnie pracować przy wilgotności powietrza od 5% do 90% zakładając brak występowania zjawiska kondensacji pary wodnej.
2.5. Router musi umożliwiać instalację, wymianę lub zamianę poszczególnych elementów (takich jak np. zasilacze, karty z interfejsami sieciowymi, moduły typu SFP/XFP) w trakcie pracy urządzenia (ang. hot-swap).
2.6. W celu zachowania redundancji zasilania, każdy router musi poprawnie działać po podłączeniu do dwóch niezależnych, obwodów napięcia przemiennego (AC). Zanik napięcia na jednym z obwodów zasilających, nie może spowodować przerwy w działaniu routera oraz ograniczenia jego funkcjonalności i wydajności (w zakresie wymaganym przez Zamawiającego).

3. Parametry interfejsów sieciowych

3.1. Router musi posiadać minimum 4 interfejsy pozwalające na pracę w trybie 40G/100G w standardzie QSFP28/QSFP+. Jednocześnie musi istnieć możliwość rozszycia każdego z interfejsów 40G na 4 interfejsy 10G przy pomocy wkładek QSFP+.

3.2. Router musi posiadać minimum 8 interfejsów pozwalających na pracę w trybie 10G/1G w standardzie QSFP+/SFP.

3.3. Interfejsy 10GE muszą umożliwiać wybór następujących trybów pracy (za pomocą interfejsu CLI):

- LAN PHY,
- WAN PHY.

3.4. Zmiana trybu pracy nie może wiązać się z koniecznością wymiany jakiegokolwiek z elementów routera (modułu optycznego itp.) lub restartu routera lub karty.

3.5. 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. Instalacja modułów optycznych pochodzących od innych producentów nie może powodować utraty, ograniczenia lub zawieszenia gwarancji na routery. Restart routera nie może powodować konieczności wykonania prac serwisowych, utrzymaniowych lub konfiguracyjnych, które pozwolą na wykorzystywanie modułów optycznych innych producentów.

3.6. Interfejsy 10 Gigabit Ethernet muszą być zgodne z normą IEEE 802.3ae.

3.7. Wszystkie wymagane przez Zamawiającego interfejsy liniowe routera (z wyłączeniem interfejsów przeznaczonych do zarządzania routerem out-of-band) muszą umożliwiać podłączenie użytkowników końcowych (ang. *access interface*) i realizację połączenia z innym routerem MPLS (ang. *core interface*). Jednoczesna realizacja obu funkcjonalności musi być realizowana za pomocą niezależnych interfejsów logicznych zdefiniowanych dla interfejsu fizycznego.

3.8. Router musi obsługiwać ramki Ethernet o wielkości co najmniej 9216B (liczonej łącznie z preambułą (7 oktetów), polem FCS (4 oktety), Frame Delimiter (1 oktet) i Interframe Gap (12 oktetów)).

3.9. Router musi posiadać mechanizm umożliwiający ograniczenie liczby umieszczanych w tablicy FIB (ang. *forwarding information base*) adresów MAC rejestrowanych na danym interfejsie (dotyczy usługi VPLS oraz EVPN).

3.10. Router musi obsługiwać znakowanie ramek Ethernet zgodnie z normą IEEE 802.1Q.

3.11. Router musi umożliwiać agregację łączy (interfejsów) w oparciu o standard IEEE 802.3ad oraz balansowanie ruchem co najmniej na podstawie adresów MAC (źródłowy i docelowy) lub adresów IPv4/IPv6 (źródłowy i docelowy) dla punktów zakończenia usług VLL/VPLS, adresów IPv4/IPv6 (źródłowych i docelowych) dla ruchu przełączanego w warstwie trzeciej OSI oraz dodatkowo na podstawie portu źródłowego i docelowego dla pakietów TCP i UDP 2 zewnętrznych etykiet MPLS dla ruchu MPLS.

3.12. Wymagane jest uruchomienie i poprawna obsługa łączy zagregowanych (ang. LAG) w każdym z następujących wariantów:

- Co najmniej 12 łączy zagregowanych, gdzie każde zawiera co najmniej 2 interfejsy fizyczne,
- Co najmniej 2 łącza zagregowane, gdzie każde zawiera co najmniej 12 interfejsów fizycznych.

3.13. Moduły optyczne dla interfejsów 1/10/40/100GE muszą umożliwiać sprawdzenie mocy odbieranego sygnału. Routery muszą w tym zakresie współpracować z modułami optycznymi posiadającymi taką funkcjonalność.

3.14. Znaczenie pola VID (VLAN ID) musi być lokalne dla interfejsów fizycznych (ang. *local VLAN significance*). Oznacza to, ze na każdym z interfejsów liniowych ramki mogą być znakowane niezależnie tym samym znacznikiem VID. Router musi zatem obsługiwać wykorzystanie tego samego VID dla wielu niezależnych interfejsów logicznych (zakończonych na różnych interfejsach fizycznych) bez konieczności dodawania kolejnych znaczników VID (VLAN stacking/double tagging). Lokalne znaczenie pola VID dla interfejsu fizycznego, musi być zachowane zarówno dla punktów zakończenia usług VLL/VPLS oraz dla protokołów IPv4, IPv6 i MPLS.

3.15. Wszystkie interfejsy liniowe (100GE, 40GE, 10GE i 1GE) znajdujące się na routerze 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 oferowanych routerach.

3.16. Router musi umożliwiać rozbudowę o wyniesione karty liniowe. Funkcjonalność musi być realizowana w oparciu o protokół 802.1BR. Podłączenie kart liniowych musi odbywać się z wykorzystaniem dostępnych na urządzeniu interfejsów.

4. Parametry wydajnościowe routerów

4.1. Router musi obsługiwać co najmniej 20,000,000 prefiksów IPv4 oraz 20,000,000 prefiksów IPv6 w tablicy RIB (ang. Routing Infromation Base).

4.2. Router musi obsługiwać co najmniej 10,000,000 prefiksów IPv4 oraz 10,000,000 prefiksów IPv6 w tablicy FIB (ang. Forwarding Infromation Base).
4.3. Router brzegowy musi obsługiwać co najmniej 4000 sieci VPLS.
4.4. Router musi obsługiwać co najmniej 120,000 grup multicast.
4.5. Router musi obsługiwać co najmniej 70,000 tranzytowych ścieżek LSP (RSVP-TE).
4.6. Router musi obsługiwać co najmniej 25,000 źródłowych ścieżek LSP (RSVP-TE head-end).
4.7. Router musi obsługiwać co najmniej 50,000 zakończeń ścieżek LSP (RSVP-TE egress).
4.8. Router musi obsługiwać co najmniej 1,500 sesji LDP typu targeted.
4.9. Router musi obsługiwać co najmniej 150,000 tras dla protokołu IS-IS.
4.10. Router musi obsługiwać co najmniej 500 sesji BGP.
4.11. Router musi obsługiwać co najmniej 4094 sieci VLAN jednocześnie(zgodnie z IEEE 802.1q).
4.12. Router musi być w stanie bezstratnie przesłać 350 milionów pakietów na sekundę dla ruchu składającego się z IPv4 oraz 300 milionów pakietów na sekundę dla ruchu składającego się z IPv6.

5. Warstwa sieciowa (ang. L*ayer 3*)

5.1. Router musi obsługiwać przełączanie w warstwie 3 modelu OSI pakietów protokołów IPv4 (protokół IP wersja 4) oraz IPv6 (protokół IP wersja 6).
5.2. Router musi obsługiwać routing statyczny protokołów IPv4 oraz IPv6 oraz protokoły routingu dynamicznego OSPF, IS-IS i BGP dla protokołu IPv4 oraz IPv6.
5.3. Dla protokołu BGP muszą być obsługiwane następujące funkcje, mechanizmy i rozszerzenia:
- BGP communities (RFC 1997)
- BGP route-reflector (RFC 2796)
- BGP MD5 authentication (RFC 2385)
- BGP 4-byte AS (RFC 4893)
- BGP - Multi-protocol Extensions (RFC 2858)
- BGP - Multi-protocol Extension for IPv6 (RFC 2545)
- Carrying Label Information in BGP-4 (3107)

5.4. Wymagana jest obsługa protokołu OSPF v2.
5.5. Wymagana jest obsługa protokołu OSPF v3 (RFC 2740).
5.6. Dla protokołu OSPF wymagana jest obsługa uwierzytelniania opartego na MD5 (RFC 2154).
5.7. Dla protokołu IS-IS (RFC 1142) wymagana jest obsługa uwierzytelniania opartego na MD5 (RFC 3567).
5.8. Router musi obsługiwać ruch multicastowy (IPv4 multicast) oraz następujące protokoły i mechanizmy z nim związane:
- Protokół IGMP v2 (RFC 2236)
- Protokół IGMP v3 (RFC 3376),
- Protokół PIM (Sparse Mode),
- Protokół PIM-SSM,
- Protokół MSDP.

5.9. Router musi obsługiwać routing IPv6 multicast z uwzględnieniem protokołów:
- PIM-SM
- MLDv1 (RFC2710)
- MLDv2 (RFC3810).

5.10. Router musi obsługiwać mechanizm tworzenia wirtualnych routerów VRF (ang. *Virtual Routing and Forwarding*) umożliwiających routing pakietów w oparciu o niezależne tablice routingu. Urządzenie musi posiadać możliwość obsługi nie mniej niż 32 takich wirtualnych routerów.
5.11. Router musi obsługiwać sieci VPN dla protokołu IPv6 (ang. *IPv6 Layer 3 VPNs*) w oparciu o RFC4659.
5.12. Router musi pozwalać na kontrolę rozpływu ruchu multicastowego z wykorzystaniem co najmniej jednej z poniższych technologii:
- PIM-oraz IGMP-snooping dla usług VPLS lub
- sieci VPN warstwy trzeciej dla ruchu IPv4 multicast (ang. *IPv4 multicast over Layer 3 VPN*).

5.13. Router musi obsługiwać sieci VPN warstwy trzeciej dla ruchu IPv4 multicast (ang. IPv4 multicast over Layer 3 VPN) na podstawie RFC4364 i dokumentu IETF draft-rosen-vpn-mcast.
5.14. Wymagana jest obsługa mechanizmów typu Policy Based Routing lub Filter Based Forwarding.
5.15. Router musi obsługiwać funkcję unicast RPF (ang. Reverse Path Forwarding) dla pakietów protokołu IPv4.
5.16. Router musi obsługiwać mechanizm VRRP (RFC 3768).

5.17. Router musi obsługiwać protokół VRRP v3 (RFC5798).
5.18. Dla protokołów IPv4 oraz IPv6, router musi obsługiwać mechanizm pozwalający na używanie jako bramy (ang. *next-hop*) routera, który nie jest do niego bezpośrednio podłączony lub został określony przez inny protokół IGP (ang. *indirect next-hop*). Działanie tego mechanizmu nie może powodować problemów z konwergencją sieci. Czas konwergencji sieci w przypadku wykorzystywania tej funkcjonalności nie może być większy niż 200ms.
5.19. Router musi obsługiwać przenoszenie prefiksów IPv4 i IPv6 przez jedną sesję BGP (zestawioną za pomocą protokołu IPv4) włączając w to przenoszenie ruchu IPv4 i IPv6 przez sieć MPLS oraz urządzenia tranzytowe nie obsługujące protokołu IPv6.
5.20. Router musi obsługiwać konfigurację znaczników lub parametru community (BGP) dla tras statycznych.
5.21. Router musi obsługiwać utrzymywanie w tablicy routingu tras statycznych w przypadku awarii interfejsu wyjściowego.
5.22. Router musi umożliwiać dodawanie tras statycznych wskazujących na bramę (next-hop/Gateway), która znajduje się w podsieci nie podłączonej bezpośrednio do danego routera.
5.23. Router musi obsługiwać dla protokołu OSPF wiele tras to tej samej podsieci docelowej (ang. *multipath*) oraz umożliwiać podział ruchu między te trasy na podstawie strumieni danych (ang. *flow-based*).
5.24. Router musi obsługiwać określenie maksymalnej liczby prefiksów importowanych przez protokół OSPF z innych protokołów.
5.25. Dla protokołu OSPF muszą być obsługiwane obszary typu
- Stub – RFC 2328
- NSSA (Not So Stubby Area) – RFC 3101

5.26. Dla protokołu OSPF muszą być obsługiwane łącza wirtualne (ang. virtual links) zgodnie z RFC 2328
5.27. Router musi obsługiwać protokół IS-IS (RFC 1142 i RFC1195).
5.28. Dla protokołu IS-IS musi być obsługiwane
- TLV 135 (traffic-engineering router ID)
- TLV dla protokołu IPv6 (RFC 5308).

5.29. Protokół IS-IS musi umożliwiać pracę tryb punkt-punkt na interfejsach typu Ethernet (RFC5309).
5.30. Router musi obsługiwać rozszerzenie SRLG dla protokołu IS-IS (RFC 5307).
5.31. Router musi obsługiwać mechanizm Route Reflector dla protokołu BGP (RFC 4456). Mechanizm musi pozwalać na modyfikację następujących parametrów tras:
- NEXT_HOP
- AS_PATH
- LOCAL_PREF
- MED.

5.32. Dla protokołu BGP musi być obsługiwany mechanizm blokowania częstych zmian dla danego prefiksu (ang. route flap dampening) zgodnie z RFC 2439.
5.33. Router musi obsługiwać wieloprotokołowe rozszerzenia dla protokołu BGP (ang. *Multi-Protocol Extensions to BGP-4*) zgodnie z RFC 4760.
5.34. Router musi umożliwiać zestawienie sesji BGP-4 wykorzystując interfejs typu „Loopback" (jako źródłowy).
5.35. Dla protokołu BGP router musi umożliwiać usuwanie prywatnych numerów AS przed rozgłoszeniem prefiksu do sąsiedniego systemu AS.
5.36. Router musi obsługiwać wykrywanie MTU (ang.path-MTU) dla sesji BGP-4.
5.37. Router musi obsługiwać funkcjonalność pozwalającą na rozpoczęcie rozgłaszania prefiksu przez protokół BGP, po określonym czasie od umieszczenia w tablicy routingu (MinRouteAdvertisementIntervalTimer –RFC4271).
5.38. Router musi obsługiwać 4-bajtowe numery systemów AS dla protokołu BGP-4 zgodnie z RFC4893.
5.39. Router musi obsługiwać rozgłaszanie wielu tras dla pojedynczego prefiksu za pomocą BGP-4 (IETF draft-ietf-idr-add-paths). Funkcjonalność musi być dostępna dla prefiksów typu IPv4, IPv4 labeled-unicast, IPv6 oraz IPv6 labeled unicast.
5.40. Router musi obsługiwać sesje typu eBGP multihop (sesja BGP między dwoma systemami autonomicznymi, niepołączonymi bezpośrednio ze sobą).
5.41. Router musi obsługiwać wiele ścieżek dla sesji typu eBGP (ang. *multipath*) w celu możliwości przesyłania ruchu przez ścieżki równoległe. Podział ruchu na ścieżki równoległe musi odbywać się na podstawie strumieni danych (ang. *flow based*).
5.42. Router musi obsługiwać mechanizm umożliwiający weryfikowanie poprawności odbieranych za pomocą BGP prefiksów (ang. RPKI*/Prefix validation*).
5.43. Na połączeniu z sąsiednim routerem w szkielecie sieci MPLS, router musi obsługiwać wykorzystanie na interfejsach sieciowych typu Ethernet adresów IPv4 z maską 31-bitową (/31).

5.44. Router musi umożliwiać wykorzystanie mechanizmu monitorowania i próbkowania ruchu w warstwach 3 i 4 dla ruchu IPv4 przy pomocy protokołu sFlow, IPFIX (RFC 5101) lub równoważnego. Za mechanizm równoważny Zamawiający uznaje uzyskanie agregacji próbkowania odpowiadającej netflow v8 lub wyższej.

6. Funkcjonalność MPLS

6.1. Router musi poprawnie działać w sieci MPLS, jako urządzenia dostępowe LER (ang. *Label Edge Router*) oraz szkieletowe LSR (ang. *Label Switch Router*).

6.2. Router musi obsługiwać zestawienie ścieżek LSP za pomocą protokołu RSVP (RSVP-TE). Musi on także obsługiwać ścieżkę zapasową dla danego LSP w trybie standby (zestawioną permanentnie, na którą nastąpi automatyczne przekierowanie ruchu w przypadku awarii na trasie ścieżki podstawowej).

6.3. Router musi obsługiwać mechanizmy FastReroute (RFC 4090) w trybach one-to-one backup i facility backup (ang. *bypass LSP*).

6.4. Router musi obsługiwać ścieżki LSP działające w trybie adaptacyjnym (ang. *adaptive LSP*) umożliwiające zmianę następujących parametrów ścieżki w trakcie jej pracy i bez konieczności jej rozłączania (ang. *make before brake*):
- Zmiana ścieżki podstawowej
- Zmiana deklaracji pasma

6.5. Router musi obsługiwać uwierzytelnianie sąsiadów dla sesji protokołu RSVP.

6.6. Wymaga się, aby uruchomienie protokołu MPLS było możliwe łącznie z protokołami IPv4 oraz IPv6. Wymaga się, aby na wybranych interfejsach logicznych przypisanych do danego interfejsu fizycznego możliwa była realizacja zakończenia usług bazujących na MPLS natomiast na pozostałych (przypisanych do tego samego interfejsu fizycznego) połączenia do wymiany ruchu z innym routerami sieci MPLS oraz routing IPv4 i IPv6.

6.7. Wymagana jest obsługa rozszerzenia Traffic Engineering dla protokołów OSPF (RFC3630) oraz IS-IS (3784).

6.8. Router musi obsługiwać routing i przełączanie pakietów IPv4 oraz IPv6 przez ścieżki LSP zestawianych przez RSVP-TE (ang. *IP over MPLS*) z wykorzystaniem protokołów:
- BGP (ang. BGP shortcuts),
- IS-IS (ang. IS-IS shortcuts),
- OSPF (ang. OSPF shortcuts).

6.9. Dla celów inżynierii ruchu (ang. *Traffic Engineering*), router musi umożliwiać wykorzystanie następujących parametrów ścieżki LSP:
- Deklaracja zajętości pasma
- Priorytet zestawiania i podtrzymania ścieżki LSP
- Ograniczenie liczby węzłów, przez które zestawiona będzie ścieżka (ang. *hop-limit*)
- Klasa usług (ang. *Class of Service*)
- Włączenie/Wyłączenie zapisywania przebiegu ścieżki LSP na podstawie obiektu Route Record (ang. *RSVP Route Record Object*)
- Metryka (wykorzystywana przez protokoły routingu do wyboru ścieżki LSP)
- Okres optymalizacji drogi, wzdłuż której zestawiona jest ścieżka LSP (ang. *reoptimize timer*)
- Dozwolone i zabronione grupy administracyjne (ang. *administrative groups*)

6.10. Router musi umożliwiać przenoszenie sygnalizacji LDP przez RSVP (ang. *LDP over RSVP*) zarówno dla urządzeń pracujących jako LSR (router typu P) jak i LER (router typu PE).

6.11. Dla ścieżek LSP router musi obsługiwać automatyczne dostosowywanie deklaracji zajętości pasma do ruchu przesyłanego przez LSP. W tym zakresie musi być możliwość określania następujących parametrów:
- Interwał pomiaru wielkości ruchu
- Procentowy poziom zmiany wielkości ruchu wpływający na zmianę deklaracji
- Liczba następujących po sobie przekroczeń wielkości ruchu generująca zmianę deklaracji pasma
- Maksymalna wielkość pasma jaka może być zadeklarowana
- Minimalna wielkość pasma jaka może być zadeklarowana

6.12. Router musi obsługiwać protokół LDP pracujący w trybie Downstream on Demand.

6.13. Router musi obsługiwać zestawianie ścieżek typu P2MP (ang. *Point-to-Multipoint*) za pomocą mLDP (RFC6388).

6.14. Router musi obsługiwać mechanizm LDP Upstream Label Assignment (RFC 6389).

6.15. Router musi obsługiwać RSVP-TE dla łączy nienumerowanych (bez adresu IP / „unnumbered") na podstawie RFC3477.

6.16. Router musi obsługiwać mechanizm RSVP Refresh reduction (RFC 2961).

6.17. Router musi obsługiwać autentykację MD5 dla RSVP-TE.

6.18. Router musi umożliwiać pominięcie mechanizmu CSPF dla obliczania ścieżki LSP poprzez bezpośrednie określenie ERO (ang. *EXPLICIT_ROUTE object*).
6.19. Router musi obsługiwać mechanizm automatycznego zestawiania ścieżek LSP do innych routerów typu PE na podstawie prefiksów wymienianych za pomocą protokołu BGP (ang. *auto mesh*).
6.20. Router musi obsługiwać mechanizm SRLG dla protokołu IS-IS (na podstawie RFC5307), który umożliwi ponowne wyznaczenie ścieżki przez mechanizm CSPF w przypadku zmian stanu interfejsu SRLG.
6.21. Router musi obsługiwać P2MP MPLS-TE dla protokołu RSVP-TE (RFC 4875):
- Dodawanie nowych i usuwanie istniejących gałęzi dla ścieżki P2MP LSP nie może powodować strat pakietów na pozostałych gałęziach tej ścieżki.
- W przypadku awarii na trasie ścieżki P2MP LSP urządzenie inicjujące (ang. *root LSR*) musi wyznaczyć nową trasę (o ile pozwala na to topologia i konfiguracja sieci) oraz zestawić ścieżkę wykorzystując nową trasę.

6.22. Router musi obsługiwać mechanizm PCE Stateful (IETF draft draft-ietf-pce-stateful-pce-00).
6.23. Router musi obsługiwać przełączanie pakietów MPLS oznakowanych co najmniej pięcioma etykietami MPLS (niepodzielny stos pięciu etykiet w nagłówku pakietu MPLS).

7. Usługi realizowane z zastosowaniem MPLS

7.1. Wymagana jest poprawna obsługa następujących usług MPLS:
- VLL (Virtual Leased Lines),
- VPLS (Virtual Private LAN Services, RFC 4762).

7.2. Sieci VPN warstwy 3 (ang. *Layer 3 VPN*) w oparciu o protokół BGP (RFC 4364 „BGP/MPLS IP Virtual Private Networks (VPNs)" oraz RFC4659 „BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN")
7.3. Router musi obsługiwać międzyoperatorskie sieci VPN (ang. *Interprovider VPNs*) dla protokołu IPv4 w oparciu o RFC3107 i RFC4364. W szczególności dotyczy implementacji opcji A, B i C (RFC 4364 sekcja 10).
7.4. Router musi obsługiwać funkcjonalność Carrier of Carriers (Carriers' Carriers) na podstawie RFC4364 sekcja 9.
7.5. Dla usług IPv4 VPN Router musi umożliwiać konfigurację tras statycznych oraz wykorzystywania tras dynamicznych (za pomocą protokołu OSPFv2) dla każdej z sieci wirtualnych.
7.6. Dla usług IPv6 VPN router musi umożliwiać konfigurację tras statycznych oraz wykorzystywania tras dynamicznych (za pomocą protokołu OSPFv3) dla każdej z sieci wirtualnych.
7.7. Dla sieci VPN warstwy 3 router musi obsługiwać wewnątrz sieci VPN protokół OSPF do wymiany prefiksów IPv4 z urządzeniami użytkownika końcowego. Router musi obsługiwać redystrybucję tych prefiksów do protokołu BGP (ang. *BGP-VPNv4*) w celu przeniesienia przez sieć szkieletową.
7.8. Router musi obsługiwać redundantne podłączenie punktów końcowych dla usług VPLS (ang. VPLS *multihoming*) pozwalające na zabezpieczenie przed powstaniem pętli dla ruchu warstwy drugiej, przenoszonego przez sieć operatora. Funkcjonalność musi być realizowana bez konieczności uruchamiania sygnalizacji (za wyjątkiem protokołu BFD) na styku z urządzeniami dołączonymi do sieci VPLS (CE).
7.9. Router musi umożliwiać transparentne przenoszenie ramek Ethernet przez sieć MPLS, niezależnie od VLAN ID, zawartego w ramkach odbieranych na interfejsach wejściowych. Funkcjonalność ta musi być dostępna dla usług warstwy drugiej bazujących na MPLS (VLL/VPLS). Zamawiający dopuszcza realizację tej funkcjonalności również poprzez zmianę typu znakowania (ang. *Tag Protocol Identifier*) dla danego interfejsu końcowego i utworzenie instancji VLL lub VPLS zawierającej nietagowany (ang. *untagged*) interfejs dostępowy.
7.10. Dla usług realizowanych w oparciu o MPLS VLL i VPLS, wymagana jest możliwość stosowania różnych VLAN ID na każdym z punktów końcowych usługi.
7.11. Router musi obsługiwać następujące typy punktów końcowych dla usług VLL i VPLS
- Nietagowany,
- Tagowany (IEEE 802.1q),
- Podwójnie tagowane (IEEE 802.1QinQ / IEEE 802.1ad)

7.12. Dla usługi VPLS, router musi obsługiwać mechanizm automatycznego wykrywania (ang. *autodiscovery*) routerów PE (ang. *Provider Edge*) bazujący na protokole BGP. Funkcjonalność ta musi być zgodna z dokumentem IETF draft draft-ietf-l2vpn-signaling-08 lub RFC 6074).
7.13. Wymagana jest obsługa lokalnego przełączania dla usług typu VLL (ang. *VLL-local*) pomiędzy dwoma interfejsami na tym samym routerze(z zachowaniem braku „uczenia się" adresów MAC w ramach tych usług).
7.14. Wprowadzenie pętli w punkcie zakończenia usług VLL i VLL-local nie może wpływać na destabilizację pracy routera oraz działających na nim usług.

7.15. Dla usług VPLS musi być dostępny mechanizm ograniczania liczby adresów MAC, jakie będą przechowywane w pamięci routera (ang. *per VPLS MAC table limit*).
7.16. Dla usług VPLS router musi umożliwiać przypisanie ścieżki LSP jaka będzie używana w celu przesłania ruchu do określonego sąsiada.
7.17. Router musi obsługiwać zastosowanie tego samego znacznika VLAN ID na różnych interfejsach fizycznych tego samego urządzenia dla różnych usług typu VLL/VPLS. W takiej sytuacji nie może występować zjawisko mieszania ruchu między tymi usługami. Funkcjonalność ta musi być dostępna również dla usług VPLS wykorzystujących pojedynczy znacznik VLAN ID (VID).
7.18. Dla usług VLL/VPLS router musi umożliwiać transparentne przenoszenie BPDU:
- Spanning Tree (IEEE 802.1d),
- MST (IEEE 802.1s)

7.19. W przypadku usługi VPLS sygnalizowanej za pomocą protokołu BGP wymagana jest możliwość zdefiniowania podstawowego i zapasowego punktu (interfejsu) zakończenia usługi na danym routerze. W przypadku poprawnej pracy router musi automatycznie blokować przesyłanie ruchu na zapasowym punkcie (interfejsie) zakończenia usługi VPLS, zapobiegając powstaniu pętli bez konieczności wykorzystywania innych protokołów (np. STP lub MSTP).
7.20. Router musi obsługiwać wirtualne łącza (ang. *pseudowire*) następujących typów
- 0x000B (IP Layer2 Transport)
- 0x0015 (CESoPSN basic mode)

7.21. Router musi obsługiwać zakończenie usługi VPWS (Virtual Private Wire Service) w sieci wirtualnej warstwy 3 (L3VPN VRF).
7.22. Router musi obsługiwać mechanizm BFD dla VCCV (ang. *Bidirectional Forwarding Detection for the Pseudowire Virtual Circuit Connectivity Verification*).
7.23. Router musi obsługiwać wykrywanie awarii łącza wirtualnego (ang. *pseudowire*) z wykorzystaniem Pseudowire Status TLV (RFC 4447).
7.24. Router musi obsługiwać sieci EVPN (BGP MPLS Based Ethernet VPN) zgodnie z dokumentem RFC 7432 (BGP MPLS-Based Ethernet VPN).
7.25. Router musi obsługiwać łącza zagregowane (ang. *LAG*), których interfejsy składowe znajdują się na różnych routerach fizycznych (ang. *multi chassis LAG/etherchannel/mLACP*). Router musi poprawnie obsługiwać za-równo zakończenie na takim łączu zagregowanym usługi VLL (VPWS) jak i współpracować z sąsiadami (PE), na których usługa VLL (VPWS) zakończona jest na łączu zagregowanym.

8. Filtrowanie ruchu oraz gwarancje jakości usług (ang. *Quality of Service*)

8.1. Wymaga się możliwości filtrowania ruchu (pakietów IPv4, IPv6) wchodzącego i wychodzącego na wszystkich wymaganych przez Zamawiającego interfejsach liniowych routera, na których odbywa się przełączanie w warstwie trzeciej OSI.
8.2. Wymaga się możliwości filtrowania ruchu dla usług VLL/VPLS (ramek Ethernet) wchodzącego i wychodzącego na wszystkich wymaganych przez Zamawiającego interfejsach liniowych routera.
8.3. Router musi wspierać mechanizm QoS w tym WRED (ang. *Weighted Random Early Detection*).
8.4. Router musi posiadać mechanizmy pozwalające na kontrolę pasma. Muszą one pozwalać na ograniczanie zarówno ruchu wejściowego jak i wyjściowego na interfejsie na podstawie znaczników VLAN (VLAN ID) dla usług realizowanych w oparciu o MPLS (VLL/VPLS)
8.5. Router musi posiadać mechanizmy pozwalające na ograniczanie pasma wejściowego i wyjściowego dla poszczególnych:
- usług VLL/VPLS na podstawie VLAN ID na każdym z portów liniowych (per VLAN ID per port),
- interfejsów liniowych,
- interfejsów liniowych z uwzględnieniem list ACL.

8.6. Wymagana jest obsługa mechanizmów kolejkowania ruchu wyjściowego na podstawie:
- CoS (IEEE 802.1p)
- DSCP (odpowiednio dla IPv4 i IPv6 dla ruchu przełączanego w warstwie 3 OSI)
- Pola EXP nagłówka MPLS

8.7. Router musi umożliwiać ustawienie pola EXP nagłówka MPLS na podstawie danych zawartych w polach:
- DSCP
- CoS

8.8. Router musi obsługiwać mechanizmy kształtowania ruchu wyjściowego na interfejsach liniowych (ang. *Traffic shaping*). Funkcja ta musi być realizowana na podstawie danych zawartych w nagłówku (CoS, DSCP, MPLS Experimental).

8.9. Router musi zapewnić hierarchiczną strukturę CoS/QoS z co najmniej 3 poziomami kształtowania ruchu.
8.10. Router musi obsługiwać co najmniej 32,000 kolejek.
8.11. Router musi posiadać mechanizmy filtrowania ramek dla interfejsów realizujących usługi VPLS na podstawie:
- adresów MAC (ruch wejściowy/wyjściowy),
- VLAN ID (ruch wejściowy).

8.12. Router musi posiadać mechanizmy filtrowania pakietów dla interfejsów na podstawie:
- adresów IPv6, protokołów i numerów portów (ruch wejściowy/wyjściowy),
- adresów IPv4 protokołów i numerów portów (ruch wejściowy/wyjściowy).

8.13. Mechanizmy opisane w punktach 8.11 i 8.12 muszą być dostępne dla wszystkich wymaganych przez Zamawiającego interfejsów liniowych (w tym zagregowanych).
8.14. Router musi umożliwiać zabezpieczenie modułu zarządzającego (ang. *control plane*) przed nieuprawnionym dostępem oraz atakami typu DoS poprzez zastosowanie filtracji pakietów przynajmniej na poziomie protokołów IPv4 oraz IPv6 (bez konieczności stosowania filtrów na interfejsach liniowych). Wymagana jest obsługa pojedynczego punktu filtracji dla realizacji tej funkcjonalności (np. aplikacja filtra na interfejsie typu loopback).
8.15. Router musi umożliwiać wprowadzenie ograniczenia pasma dla pakietów kierowanych do modułu zarządzającego (ang. *control plane*) dla poszczególnych usług, które są przez niego obsługiwane (np. ICMP, Radius, FTP).

9. Zarządzanie i monitorowanie routera

9.1. Wymagana jest obsługa mechanizmu syslog, pozwalająca na przesyłanie informacji o zarejestrowanych przez router zdarzeniach do zdalnego serwera syslog.
9.2. Wymagana jest obsługa protokołu NTP lub SNTP dla synchronizacji czasu.
9.3. Router musi obsługiwać funkcje umożliwiające prowadzenie diagnostyki poprzez podgląd działania procesów (ang. *debug*) i zdarzeń (ang. *log*).
9.4. Router musi obsługiwać wirtualizację zasobów. Oznacza to, że musi obsługiwać przekazanie kontroli nad wydzielonym zestawem interfejsów wybranemu użytkownikowi. Użytkownik ten musi mieć możliwość sterowania przepływem ruchu przez wydzielony dla niego zestaw interfejsów np. poprzez kontrolę nad odpowiednimi mechanizmami sygnalizacyjnymi (protokoły routingu, MPLS), przy czym:
    - Operacje wykonywane przez użytkownika nie mogą powodować kolizji z pozostałymi mechanizmami działającymi na routerze
    - Użytkownik nie może kontrolować mechanizmów poza wydzielonym dla niego środowiskiem wirtualnym.

9.5. 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 umożliwiać konfigurację parametrów mechanizmu ochrony DDoS dla poszczególnych protokołów (np. ograniczenie wielkości ruchu) oraz rejestrować wystąpienie zdarzeń związanych z działaniem tego mechanizmu (czas wystąpienia ostatniego przekroczenia parametrów, czas trwania przekroczenia, liczbę pakietów odebranych, liczbę pakietów odrzuconych). W przypadku gdy mechanizm ten nie jest domyślnie włączony:
    a) Wykonawca musi dołączyć do oferty szczegółową konfigurację tego mechanizmu dla routera,
    b) wszystkie routery muszą być dostarczone z zaimplementowaną konfiguracją ochrony DDoS,
    c) dostarczona konfiguracja musi pozwalać na utrzymanie takiego samego poziomu ochrony DDoS, bez konieczności wprowadzania do niej zmian przez administratora routera, w przypadku gdy wykonywane są zwykłe operacje związane z utrzymaniem i działaniem routera, w szczególności takie jak:
        - dodawanie i usuwanie interfejsów sieciowych oraz ich parametrów (adresy IPv4/IPv6)
        - uruchamianie i usuwanie protokołów sieciowych oraz zmiana ich parametrów
        - uruchamianie i usuwanie usług sieciowych oraz zmiana ich parametrów
    d) włączenie mechanizmu ochrony DDoS nie może wykluczać i ograniczać wykorzystania innych funkcjonalności i wydajności wymaganych przez Zamawiającego.

9.6. Wymagana jest obsługa mechanizmów lokalizacji uszkodzeń w sieci na podstawie IEEE 802.1ag (ang. *Connectivity Fault Management*), ITU-T Y.1731 (ang. *Fault Monitoring*), ITU-T Y.1731 (ang. *Performance Monitoring*).
9.7. Router musi obsługiwać mechanizm wykrywania uszkodzeń (ang. *Connectivity Fault Management*) dla poszczególnych instancji VPLS zgodny ze standardem IEEE 802.1ag.
9.8. 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.

9.9. Dla usług IP VPN router musi obsługiwać funkcje ping i traceroute dla każdej z sieci wirtualnych.
9.10. Router musi obsługiwać mechanizm BFD dla protokołów IS-IS (IPv4/IPv6), OSPFv2, OSPFv3, BGP (IPv4), RSVP-TE (LSP).
9.11. W celu zapewnienia monitorowania sieci router musi udostępniać za pomocą protokołu SNMP liczniki (co najmniej 64 bitowe) ramek (pakietów) i bajtów (oktetów) wysłanych i odebranych na poszczególnych interfejsach liniowych.
9.12. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach liniowych.
9.13. Router musi umożliwiać komunikację z urządzeniem za pomocą protokołu SNMPv2 (RFC1901) zgodnie z MIB-2 (RFC1213) oraz SNMPv3 (RFC2570).
9.14. Router musi umożliwiać wysyłanie za pomocą protokołu SNMP wiadomości informacyjno-ostrzegawczych (ang. *trap messages*).
9.15. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach liniowych.
9.16. Ze względu na konieczność monitorowania dodatkowych parametrów ruchu w sieci IP/MPLS router musi posiadać funkcjonalność sFlow lub NetFlow (lub podobne mechanizmy cFlow / J-Flow).
9.17. Router musi umożliwiać współpracę z serwerami autoryzacji TACACS+ (zgodnie z RFC1492) i RADIUS (zgodnie z RFC2138 i RFC2139).
9.18. W okresie gwarancji Wykonawca musi zapewnić Zamawiającemu dostęp do aktualizacji oprogramowania, po załadowaniu których możliwy będzie dostęp do interfejsu CLI (ang. Command Line Interface) routera za pomocą protokołu SSH (SSH wersja 2). Aktualizacja oprogramowania nie może wpływać na ograniczenie pozostałych wymagań Zamawiającego.
9.19. Router musi posiadać port terminalowy do dołączenia konsoli (RS232 lub USB).
9.20. Router musi posiadać dodatkowy port (lub porty) typu Fast Ethernet lub GE do komunikacji z routerem, za pomocą którego możliwe będzie zarządzanie poza pasmem (ang. *out-of-band management*).
9.21. Router musi działać pod kontrolą oprogramowania, które może zostać zakupione przez dowolnego klienta producenta routera i dostępnego, jako aktualizacja dla pozostałych użytkowników oferowanego routera, posiadających prawo do pobierania i używania aktualizacji. Zamawiający nie dopuszcza stosowania oprogramowania dedykowanego, stworzonego na potrzeby niniejszego postępowania. Przy ocenie tego wymagania Zamawiający uwzględni restrykcje eksportowe obowiązujące w kraju producenta routerów, związane z rozpowszechnianiem wybranych mechanizmów szyfrujących.
9.22. Router musi umożliwiać wyłączenie dostępu do urządzenia z wykorzystaniem protokołu telnet.
9.23. Interfejs 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). Dokumentacja do oprogramowania sterującego musi być dostępna w całości w językach polskim lub angielskim. Dokumentacja musi być dostarczona w formie elektronicznej, w formacie ogólnodostępnym (PDF, DOC, DOCX, ODF, HTML).
9.24. Router musi umożliwiać zliczanie pakietów dopasowanych do filtra (ACL).
9.25. Router musi obsługiwać uruchomienie z poziomu interfejsu CLI (ang. *Command Line Interface*) następujących funkcji:
- automatycznego sprawdzania konfiguracji (lub zmian konfiguracji) urządzenia pod kątem zdefiniowanych przez użytkownika warunków (np. konieczność określenia nazwy interfejsu sieciowego lub sąsiada BGP) oraz wykonania zdefiniowanych akcji na podstawie tej weryfikacji (np. odrzucenie zmian)
- automatycznego cofnięcia wprowadzonych zmian konfiguracyjnych w przypadku braku ponownego ich potwierdzenia w założonym przez administratora czasie bez konieczności restartu routera
- zamianę w aktualnej konfiguracji określonych ciągów znaków zgodnie ze wzorcem określonym przez administratora.

9.26. Router musi umożliwiać automatyczne wykonywanie kopii zapasowej jego konfiguracji na wskazany serwer. Wykonanie kopii zapasowej musi być inicjowane przez każdy router indywidualnie. W tym zakresie wymagana jest współpraca przynajmniej z wykorzystaniem protokołu i serwera FTP.
9.27. Router musi umożliwić wyświetlenie co najmniej 5 ostatnich zmian jakie zostały wprowadzone w jego konfiguracji.
9.28. Oprogramowanie sterujące musi pozwalać na restart wybranych procesów (np. procesu obsługi SNMP) bez konieczności restartowania pozostałych procesów.
9.29. Router musi umożliwiać zaprogramowanie restartu w określonym czasie.
9.30. Router musi oferować interfejs programowy do współpracy z aplikacjami. Wymagana jest obsługa Netconf (RFC 4741, NETCONF Configuration Protocol), za pomocą którego możliwe będzie konfigurowanie routera oraz sprawdzanie jego stanu (stan interfejsów, protokołów, liczniki pakietów/ramek itp.)

9.31. Router musi oferować wsparcie dla RFC 6020 (YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)).
9.32. Router musi pozwalać na dynamiczną instalację filtrów bezpieczeństwa z wykorzystaniem protokołu FlowSpec zgodnie z RFC5575.
9.33. Router musi zapewniać wsparcie dla protokołu IEEE 1588 PTP.
9.34. Router musi zapewniać wsparcie dla protokołu SyncE.
9.35. Router musi umożliwiać tworzenie aplikacji pracujących bezpośrednio na routerze. Wspierany musi być przynajmniej język programowania Python. Aplikacje mają mieć możliwość rozszerzania funkcjonalności udostępnianej przez producenta routerów.

10. Pomoc techniczna i gwarancja

10.1. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
10.2. Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej przez okres 36-miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta, polskiego dystrybutora sprzętu lub autoryzowanego partnera serwisowego producenta, wymianę uszkodzonego sprzętu w ciągu 2 dni roboczych, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.