**Opis Przedmiotu Zamówienia (OPZ)**

# Przedmiot Zamówienia - CZĘŚĆ I

Przedmiotem Zamówienia – CZĘŚĆ I jest dostawa fabrycznie nowych 17 sztuk switchy (przełączników sieciowych) do szaf dostępowych wraz z gwarancją na minimum 36 miesięcy.

Zaoferowane urządzenia muszą być fabrycznie nowe, przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz. U. z 2023 r. poz. 215) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished).

Zamawiający wymaga, aby wszystkie dostarczone urządzenia pochodziły z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń́ i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.

Zaoferowane przełączniki sieciowe oraz oprogramowanie muszą pochodzić od tego samego producenta.

**Wymagania techniczne dotyczące fabrycznie nowych przełączników sieciowych wraz z niezbędnym wyposażeniem**

Minimalne parametry i funkcjonalności przełączników dostępowych:

1. dostarczone przełączniki dostępowe muszą być typu „standalone”, 48 portów 10/100/1000BaseT RJ-45 PoE+ zgodne z IEEE 802.3at, uplink 4x10G SFP+
2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
3. Gigabit Ethernet 1000Base-T,
4. Gigabit Ethernet 1000Base-SX,
5. Gigabit Ethernet 1000Base-LX/LH,
6. Gigabit Ethernet 1000Base-BX-D/U,
7. 10Gigabit Ethernet 10GBase-SR,
8. 10Gigabit Ethernet 10GBase-LR,
9. Musi być możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
10. Przepustowość w ramach stosu nie mniejsza niż 80Gb/s,
11. Minimum 8 urządzeń w stosie,
12. Zarządzanie poprzez jeden adres IP,
13. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
14. W przypadku gdy wymagane są dodatkowe moduły do zapewnienia funkcjonalności stacka, urządzenie musi być w nie wyposażone na obecnym etapie zamówienia, wraz z kablem stackującym o długości nie mniejszej niż 50 cm (14 szt.) oraz 200 cm (3 szt.) i pozwalającej na stackowanie 6 urządzeń jednocześnie.
15. Zapewnienie możliwości rozbudowy stosu zbudowanego w oparciu obecnie posiadane urządzenia.
16. Wymagania w zakresie zasilania:
17. przełączniki muszą posiadać możliwość instalacji zasilacza redundantnego AC 230V,
18. muszą mieć możliwość instalacji/wymiany zasilaczy „na gorąco” (ang. hot swap),
19. przełączniki muszą być wyposażone w pojedyncze zasilacze
podstawowe i redundantne wentylatory, z możliwością rozbudowy do dwóch redundantnych zasilaczy,
20. budżet mocy dostępny dla PoE z pojedynczym zasilaczem nie niższy niż 740W,
21. Przełączniki muszą umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
22. W przypadku wyłączenia przełącznika, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika).
23. Przełączniki muszą spełniać następujące wymagania w zakresie parametrów wydajnościowych:
24. Przepustowość przełączników (switching capacity) nie mniejsza niż 170 Gb/s (bez podłączenia do stosu), 250 Gb/s (z podłączeniem do stosu),
25. Prędkość przesyłania (forwarding rate) nie mniejsza niż 120 Mpps,
26. Bufor pakietów nie mniejszy niż 5MB,
27. Obsługa:
28. Minimum 500 aktywnych sieci VLAN jak i interfejsów SVI L3,
29. Nie mniej niż 15000 adresów MAC,
30. Minimum 2000 tras IPv4,
31. Nie mniej niż 900 wpisów w listach kontroli dostępu Security ACL,
32. Nie mniej niż 900 wpisów w listach kontroli dostępu QoS ACL,
33. Wparcie dla jumbo frame o wielkości 9198B,
34. Minimum 40 połączeń zagregowanych typu „port channel” ,
35. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
36. Przełączniki muszą wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
37. IEEE 802.1w Rapid Spanning Tree,
38. Per-VLAN Rapid Spanning Tree (PVRST+),
39. IEEE 802.1s Multi-Instance Spanning Tree,
40. Wsparcie dla protokołu REP (Resilient Ethernet Protocol),
41. Redundancja połączeń uplink bez używania protokołu Spanning-Tree lub funkcji „portchannel” umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego, wraz z możliwością wskazania uplinku podstawowego i zapasowego dla poszczególnych sieci VLAN.
42. Przełączniki muszą zapewniać obsługę następujących protokołów:
43. IGMPv1/2/3 i MLDv1/2 Snooping,
44. LLDP i LLDP-MED.
45. Przełączniki muszą realizować funkcje:
46. 802.1Q tunneling (QinQ),
47. Layer 2 traceroute umożliwiającej śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC,
48. Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego,
49. Możliwość uruchomienia serwera DHCP.
50. Przełączniki muszą wspierać mechanizmy związane z bezpieczeństwem sieci:
51. Wiele poziomów dostępu administracyjnego poprzez konsolę, możliwość zalogowania się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
52. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
53. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
54. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
55. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
56. Możliwość uwierzytelniania użytkowników w oparciu o portal web dla klientów bez suplikanta 802.1X,
57. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
58. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
59. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
60. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
61. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
62. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
63. Obsługa list kontroli dostępu (ACL) następujących typów:
64. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
65. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
66. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
67. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia),
68. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
69. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
70. Funkcja Private VLAN.
71. Przełączniki muszą wspierać mechanizmy zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
72. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
73. bezpieczna sekwencja uruchamiania,
74. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
75. Przełączniki muszą obsługiwać następujące funkcje związane z zapewnieniem jakości usług w sieci:
76. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
77. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
78. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
79. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
80. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
81. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
82. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
83. Przełączniki muszą zapewnić obsługę następujących protokołów i mechanizmów routingu:
84. Routing statyczny dla IPv4 i IPv6,
85. Routing dynamiczny – RIP i OSPF, nie mniej niż 900 wpisów,
86. Obsługa PIM Stub, nie mniej niż 900 wpisów,
87. Policy-based routing (PBR),
88. Obsługa protokołu redundancji bramy (VRRP),
89. Obsługa tuneli GRE (Generic Routing Encapsulation).
90. Przełączniki muszą:
91. Umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
92. Posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
93. Posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
94. Posiadać funkcjonalność sondy IP SLA Responder.
95. Przełącznik musi wspierać następujące mechanizmy i narzędzia zarządzania:
96. Port konsoli,
97. Dedykowany port Ethernet do zarządzania out-of-band,
98. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera USB Bluetooth podłączanego do portu USB przełącznika. Kontrola dostępu dla tej funkcjonalności musi być realizowana poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
99. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
100. Obsługa protokołów SNMPv3, SSHv2, SCP, SFTP (SSH File Transfer Protocol), HTTPS, Syslog,
101. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
102. Wsparcie dla protokołów RESTCON i gNMI,
103. Wbudowana dioda umożliwiająca identyfikację konkretnego urządzenia podczas akcji serwisowych,
104. Wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
105. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
106. Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne startowe, dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
107. Wbudowany graficzny interfejs zarządzania przełącznikiem.
108. Przełączniki muszą spełniać następujące parametry fizyczne:
109. Możliwość montażu w szafie rack 19”,
110. Wysokość urządzenia 1 RU,
111. Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 35 cm.
112. Przełącznik musi wspierać funkcjonalność NetFlow w zakresie:
113. możliwości próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow i obsługą minimum 15000 strumieni (flow),
114. realizacji rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7 OSI.
115. Przełączniki muszą posiadać deklarację CE lub równoważną.
116. Przełączniki muszą być wyprodukowane zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważny.
117. Przełączniki muszą być zgodne z normami UE i być przeznaczone na rynek UE.
118. Przełączniki wraz z dostarczonym wyposażeniem muszą być objęte wsparciem technicznym minimum 36 miesięcznym na poziomie 8x5xNBD.
119. Wraz z przełącznikami zostanie dostarczone niezbędne do zapewnienia wymaganych funkcjonalności i prawidłowego działania do którego są przeznaczone, oprogramowanie w ilości umożliwiającej spełnienie wymagań funkcjonalnych. Oprogramowanie zostanie dostarczone, w postaci stałej licencji lub minimum 36 miesięcznej subskrypcji, o ile producent nie oferuje oprogramowania w innej formie niż subskrypcja.
120. przełączniki muszą być objęte minimum 36 miesięczną gwarancją opartą na serwisie producenta świadczonym w reżimie 8x5xNBD.
121. Wszystkie zaoferowane elementy muszą pochodzić od jednego producenta i z oficjalnej dystrybucji.

# Przedmiot Zamówienia - CZĘŚĆ II

Przedmiotem zamówienia - CZĘŚĆ II jest zakup:

1. switche Core – 2 sztuki
2. switche Datacenter – 2 sztuki

wraz z dodatkowym wyposażeniem, wdrożeniem i zapewnieniem wsparcia technicznego dla zakupionych przełączników i wyposażenia.

W chwili obecnej Zamawiający posiada infrastrukturę sieciową opartą o cztery rodzaje przełączników firmy CISCO: Cisco Catalyst 3650, 9200, 9300 i Cisco Nexus 9000. Sprzęt będący przedmiotem niniejszego zamówienia musi być kompatybilny z posiadaną przez Zamawiającego infrastrukturą. Zaoferowany sprzęt nie może powodować zmniejszenia funkcjonalności posiadanych przełączników sieciowych

Zaoferowane urządzenia muszą być fabrycznie nowe, przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz. U. z 2023 r. poz. 215) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów „odnawianych" (ang. Refurbished).

Zamawiający wymaga, aby wszystkie dostarczone urządzenia pochodziły z oficjalnego kanału dystrybucyjnego danego producenta, a serwis gwarancyjny był autoryzowany przez producenta urządzeń́ i oprogramowania oraz świadczony przez producenta lub autoryzowanych partnerów w centrach serwisowych na terenie Unii Europejskiej.

Zaoferowane przełączniki sieciowe oraz oprogramowanie muszą pochodzić od tego samego producenta.

1. **Switch Core (2 sztuki)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **NAZWA KOMPONENTU** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO dot. Switcha Core** |
| **1.** | **Przełącznik typu standalone, minimalne wyposażenie** | * 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28,
* 4 porty definiowane za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi posiadać możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps.
 |
| **2.** | **Porty SFP/SFP+/SFP28 muszą umożliwiać zastosowanie następujących modułów** | * Gigabit Ethernet 1000Base-T,
* Gigabit Ethernet 1000Base-SX,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-SR-S,
* 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet typu twinax (SFP+ - SFP+ DAC),
* 25Gigabit Ethernet 25GBASE-SR,
* 25Gigabit Ethernet typu twinax (SFP28 – SFP28 DAC),
* 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);
 |
| **3.** | **Porty QSFP muszą umożliwiać zastosowanie następujących modułów** | Dla transmisji 40Gb/s:* 40G-SR4,
* 40G-CSR,
* 40G-CSR4,
* 40G-LR4,
* 40G-SR-BD,
* Adaptera 40G QSFP->10G SFP+,
* 40Gigabit Ethernet typu twinax (QSFP – QSFP DAC);

Dla transmisji 100Gb/s:* 100GBASE-SR4,
* 100Gigabit Ethernet typu twinax (QSFP – QSFP DAC).
 |
| **4.** | **Przełącznik musi spełniać następujące wymagania w zakresie parametrów wydajnościowych** | * Urządzenie musi posiadać bufor pamięci o wielkości minimum 32MB,
* Urządzenie musi posiadać nie mniej 16GB pamięci DRAM i 16GB pamięci Flash,
* Przepustowość przełącznika (switching capacity) nie może mniejsza niż 3.2 Tbps,
* Prędkość przesyłania (forwarding rate) nie mniejsza niż 1 miliard pps,
* Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika.
 |
| **5.** | **Urządzenie musi zapewniać wsparcie dla:** | * 1000 aktywnych sieci VLAN,
* 1000 interfejsów SVI L3,
* 80 000 adresów MAC,
* 200 000 tras IPv4,
* Ramek Jumbo dla wszystkich portów (minimum 9216 bajtów),
* Obsługi Link Aggregation Control Protocol (LACP): IEEE 802.3ad.
* 128 połączeń zagregowanych typu „Port Channel”,
* Terminowania pojedynczej wiązki „Port Channel” na 2 niezależnych przełącznikach,
* 16 interfejsów fizycznych w ramach jednego połączenia zagregowanego typu „port channel” LACP.
 |
| **6.** | **Szyfrowanie** | * Urządzenie musi wspierać standard IEEE 802.1ae (MACSec) - szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika,
* Szyfrowanie MACSec musi być wspierane na portach tworzących połączenia zagregowane L2 i L3.
 |
| **7.** | **Przełącznik musi wspierać następujące tryby pracy Spanning-Tree Protocol** | * IEEE 802.1w Rapid Spanning Tree,
* Per-VLAN Rapid Spanning Tree (PVRST+),
* IEEE 802.1s Multi-Instance Spanning Tree,
 |
| **8.** | **Przełącznik musi zapewniać wsparcie dla następujących typów list kontroli dostępu (ACL):** | * Port ACL umożliwiających kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
* VLAN ACL umożliwiających kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
* Routed ACL umożliwiających kontrolę ruchu routowanego pomiędzy sieciami VLAN,
* Musi być możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
 |
| **9.** | **Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:** | * 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnych klasach jakości usług,
* Implementację algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
* Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do różnych klas jakości obsługi poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie jakości usług z dokładnością do 8 Kbps (policing, rate limiting),
* Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast.
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
 |
| **10.** | **Mechanizm ochrony** | * Urządzenie musi posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
 |
| **11.**  | **Przełącznik musi wspierać routing i mechanizmy L3 dla protokołów IPv4 i IPv6, w zakresie:** | * Routing statyczny dla IPv4 i IPv6,
* Routing dynamiczny dla IPv4: BGP, ISIS,
* Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),
* Routing dynamiczny dla IPv6: OSPFv3,
* Funkcjonalności Policy-Based Routing,
* Multicast routing (PIM-SM, PIM-SSM),
* Obsługa IGMPv2/3,
* Obsługa 1000 wirtualnych instancji routingu (VRF),
* Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu,
 |
| **12.** | **Przełącznik musi zapewniać wsparcie dla następujących funkcjonalności:** | * Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED,
* Realizacja funkcji tunelowania 802.1 QinQ (802.1Q Tunneling),
* Funkcjonalność izolowania portów znajdujących się w tym samym VLAN,
* Funkcja serwera DHCP,
* Obsługa różnych poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwić zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji,
* Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
* Funkcja translacji adresów IP NAT (Network Address Translation),
* Obsługa protokołu LISP zgodnie z RFC 6830,
* Enkapsulacja ruchu sieciowego w nagłówkach VXLAN,
* Obsługa BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf /spine /border,
* Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
* sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,
* Możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego (mechanizmy SPAN, RSPAN)
* Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającej na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
* Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, udp-echo, udp-jitter, tcp-connect,
* Funkcjonalność przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowania zewnętrznego,
* Wbudowany analizator pakietów,
* Wsparcie dla tworzenia statystyk ruchu w oparciu o pełen protokół NetFlow (bez próbkowania) i Flexible NetFlow.
 |
| **13.** | **System operacyjny przełącznika musi zapewniać wsparcie dla:** | * Wgrywania poprawek bez konieczności restartowania platformy,
* Konfiguracji poprzez API za pomocą protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020),
* Obsługi protokołu RESTCONF,
* Tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
* Uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
* Obsługi SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
 |
| **14.** | **Przełącznik musi wspierać możliwość programowej modyfikacji takich parametrów jak:** | * ilości pozycji w tablicy MAC,
* ilość tras routingu unicast i multicast,
* ilości obsługiwanych sesji Netflow,
 |
| **15.** | **Urządzenie musi zapewnić możliwość łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Przełącznik musi być dostarczony wraz ze wszystkimi wymaganymi do tego licencjami.** | * Urządzenia w klastrze powinny zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,
* Klaster powinien wspierać funkcję eliminacji przesyłania ruchu BUM (broadcast, unknown-unicast and multicast traffic) poprzez link między tworzącymi go przełącznikami.
 |
| **16.** | **Przełącznik musi wspierać mechanizm segmentacji logicznej i kontrolę ruchu w oparciu o znaczniki bezpieczeństwa (Secure Tag), w zakresie:** | * Możliwości tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
* Statycznie w oparciu o port, do którego podłączona jest stacja,
* Statycznie w oparciu o VLAN, w którym pracuje stacja,
* Statycznie w oparciu o adres IP stacji,
* Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
* Możliwości dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa z centralnego systemu zarządzania kontrolą dostępu,
* Wsparcia dla propagacji informacji o przypisaniu stacji danego znacznika bezpieczeństwa bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
 |
| **17.** | **Urządzenie musi spełniać następujące wymagania sprzętowe:** | * Musi posiadać wymienne moduły wentylatorów,
* Musi być wyposażone w dwa zasilacze zmiennoprądowe, pracujące w konfiguracji redundantnej,
* Musi umożliwiać montaż w szafie rack 19”.
* Wysokość obudowy nie może przekraczać 1 RU.
* Musi posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
* Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
 |
| **18.** | **Certyfikaty** | 1. Switch musi posiadać deklaracja CE lub równoważną.
2. Switch musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
3. Switch musi być zgodny z normami UE i przeznaczony na rynek UE, musi posiadać certyfikat CE lub równoważny.
 |

1. **Switch Datacenter (2 sztuki)**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **NAZWA KOMPONENTU** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO dot. switcha Datacenter** |
| **1.** | **Przełącznik musi posiadać:**  | * 48 portów 1/10/25GE SFP/SFP+/SFP28,
* 6 portów definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP musi mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps,
 |
| **2.** | **Porty SFP/SFP+/SFP28 muszą umożliwiać zastosowanie następujących modułów:** | * Gigabit Ethernet 1000Base-T,
* Gigabit Ethernet 1000Base-SX,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-SR-S,
* 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet typu twinax (SFP+ - SFP+ DAC),
* 25Gigabit Ethernet 25GBASE-SR,
* 25Gigabit Ethernet typu twinax (SFP28 – SFP28 DAC),
* 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);
 |
| **3.** | **Porty QSFP muszą umożliwiać zastosowanie następujących modułów:** | Dla transmisji 40Gb/s:* 40G-SR4,
* 40G-CSR,
* 40G-CSR4,
* 40G-LR4,
* 40G-SR-BD,
* Adaptera 40G QSFP->10G SFP+,
* 40Gigabit Ethernet typu twinax (QSFP – QSFP DAC);

Dla transmisji 100Gb/s:* 100GBASE-SR4,
* 100Gigabit Ethernet typu twinax (QSFP – QSFP DAC);
 |
| **4.** | **Przełącznik musi spełniać następujące wymagania w zakresie parametrów wydajnościowych:** | * Urządzenie musi posiadać bufor pamięci o wielkości minimum 40MB,
* Urządzenie musi posiadać min. 16GB pamięci DRAM i 64GB pamięci Flash,
* Przepustowość łączna przełącznika (switching capacity) nie może być mniejsza niż 3 Tbps,
* Prędkość przesyłania (forwarding rate) nie mniejsza niż 1 miliard pps,
* Wymagana jest prędkość przełączania „wirespeed” dla każdego portu przełącznika,
* Opóźnienie przełączania pakietów nie większe niż 2 µs,
 |
| **5.** | **Przełącznik musi posiadać następującą funkcjonalność warstwy L2 OSI:** | * Trunking IEEE 802.1Q VLAN,
* Możliwość izolowania portów znajdujących się w tym samym segmencie VLAN,
* Wsparcie sprzętowe dla minimum 90 000 adresów MAC,
* IEEE 802.1w Rapid Spanning Tree (RST),
* IEEE 802.1s Multiple Spanning Tree (MST),
* Wsparcie sprzętowe dla tunelowania QinQ (802.1Q Tunneling),
* Funkcja statycznej i dynamicznej translacji adresów IP NAT (Network Address Translation),
* Obsluga IGMP v2/3;
* Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach,
* Wsparcie dla Link Aggregation Control Protocol (LACP): IEEE 802.3ad.
* 32 interfejsów fizycznych w ramach jednego połączenia zagregowanego typu „Port Channel” LACP;
* Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
 |
| **6.** | **Przełącznik musi posiadać następującą funkcjonalność warstwy L3 OSI:** | * Routing statyczny dla protokołów IPv4 oraz IPv6,
* Routing dynamiczny w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6,
* Policy Based Routing (PBR) dla IPv4 i IPv6,
* Wsparcie sprzętowe dla minimum 768 000 prefixów LPM/wpisów hosta w tablicy routingu IP,
* Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast),
* Wsparcie dla IGMPv2/v3 oraz MSDP,
* Wsparcie sprzętowe dla minimum 100 000 tras multicast,
* Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
* Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP),
* Obsługa protokołu BFD (Bidirectional Forwarding Detection) dla protokołów IPv4 i IPv6, umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu,
* Wsparcie dla protokołu VRRP v3,
* Wsparcie dla Microsoft NLB,
* Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list.
* Jeśli funkcjonalność warstwy L3 OSI opisana w powyższym punkcie wymaga dostarczenia dodatkowej licencji, to jest ona wymagana na tym etapie.
 |
| **7.** | **Funkcja load-balancera** | Urządzenie musi posiadać możliwość uruchomienia sprzętowego load-balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL. |
| **8.** | **Przełącznik musi posiadać możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet.**  | * Dołączenie modułów lub przełączników nie może być realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3, a jedynie w ramach domeny fizycznej bądź stosu urządzeń,
* Porty modułu wyniesionego muszą być udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego,
* Przełącznik musi umożliwiać programową konwersję własnego trybu pracy do trybu modułu wyniesionego, zarządzanego z innego przełącznika macierzystego.
 |
| **9.** | **Urządzenie musi posiadać sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad na blokach 128 bit oraz 256 bit oraz wykorzystaniem trybu GCM-AES-XPN.** | Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie. |
| **10.** | **Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN:** | * Sprzętowa implementacja VTEP (VXLAN Tunnel Endpoint),
* Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway),
* Wymiana ruchu z co najmniej 255 innymi sprzętowymi VTEP,
* Obsługa ruchu rozgłoszeniowego BUM (broadcast, multicast, unknown-unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP,
* Obsługa ruchu rozgłoszeniowego BUM poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast),
* Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol),
* Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN),
* Jeśli funkcjonalność VXLAN opisana powyżej wymaga dostarczenia dodatkowej licencji to jest ona wymagana na tym etapie.
 |
| **11.** | **Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:** | * Obsługa Layer 2 IEEE 802.1p (CoS),
* Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2-4 OSI. Klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP,
* Kolejkowanie w oparciu o CoS 802.1p na wyjściu,
* Kolejkowanie z bezwzględnym priorytetem (Strict-Priority) na wyjściu,
* Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny,
* Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych,
* Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych,
* Obsługa protokołu PFC (Priority Flow Control) IEEE 802.1Qbb,
* Urządzenie musi posiadać architekturę pamięci przystosowaną dla obsługi buforów, QoS oraz ruchu typu microburst (chwilowe wzrosty ruchu), zapewniając skuteczną obsługę zarówno małych jak i bardzo dużych przepływów danych. Urządzenie musi potrafić monitorować wykorzystanie buforów i sygnalizować przekraczanie zdefiniowanych przez użytkownika progów wielkości przepływu przypadku zaistnienia zjawiska microburst.
 |
| **12.** | **Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa i stabilności w sieci:** | * Wejściowe ACL (standardowe oraz rozszerzone),
* Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC,
* Standardowe oraz rozszerzone ACL dla warstw 3-4 OSI w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
* ACL oparte o VLAN-y (VACL) i porty (PACL),
* Mechanizmy DHCP Snooping, ARP Inspection i IP Source Guard,
* Funkcja zabezpieczenia przed niekontrolowanym wzrostem ilości ruchu (storm control) dla ruchu unicast, multicast i broadcast.
 |
| **13.** | **Urządzenie musi wspierać funkcjonalności z obszaru zarządzania i zabezpieczenia przełącznika:** | * Port konsoli CLI;
* Zarządzanie In-band - obsługa protokołów SSHv2, SNMPv3, HTTPS, Syslog.
* Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
* 802.1x i dynamiczny przydział VLAN do portu,
* Wsparcie dla protokołów sFlow lub NetFlow,
* Wsparcie sprzętowe dla telemetrii przepływów z możliwością eksportu z wykorzystaniem protokołu gRPC,
* Wsparcie dla IEEE 802.1ab LLDP,
* Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback),
* Obsluga Role-Based Access Control RBAC,
* Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
* Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror, SPAN),
* Obsługa Network Time Protocol (NTP) i Precision Time Protocol IEEE 1588
* Diagnostyka procesu BOOT;
 |
| **14.**  | **Urządzenie musi posiadać sprzętowe i programowe wsparcie dla architektury SDN dedykowanej przez jego producenta dla infrastruktury Data Center. Dodanie przełącznika do rozwiązania SDN musi być możliwe z wykorzystaniem jego istniejącego oprogramowania, bądź po jego wymianie na odpowiednie oprogramowanie, bez żadnych ingerencji czy modyfikacji sprzętowych.**  | Jeśli funkcjonalność SDN wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie. |
| **15.** | **Przełącznik musi posiadać narzędzia programowania i zarzadzania:** | * Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API,
* Wbudowana powłoka bash do zarządzania systemem Linux przełącznika,
* Wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych,
* Interfejs programistyczny REST API wraz z upublicznionym SDK,
* Wsparcie dla NETCONF i zarządzania poprzez XML.
 |
| **16.** | **Urządzenie musi spełniać następujące wymagania sprzętowe:** | * Musi być wyposażone w dwa zasilacze zmiennoprądowe, pracujące w konfiguracji redundantnej,
* Musi posiadać wymienne moduły wentylatorów, w konfiguracji zapewniającej wyrzut ciepłego powietrza od strony portów liniowych,
* Musi umożliwiać montaż w szafie rack 19”.
* Wysokość obudowy nie może przekraczać 1 RU.
 |
| **17.** | **Certyfikaty** | 1. Switch musi posiadać deklaracja CE lub równoważną.
2. Switch musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001 lub równoważną.
3. Switch musi być zgodny z normami UE i przeznaczony na rynek UE, musi posiadać certyfikat CE lub równoważny.
 |

1. **Dodatkowe wyposażenie - moduły światłowodowe i kable DAC**

|  |  |  |
| --- | --- | --- |
| **Lp.** | **NAZWA KOMPONENTU** | **MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO dot. Zakupu dodatkowego wyposażenia - modułów światłowodowych i kabli DAC.** |
| **1.** | **6 modułów SFP-25G-AOC5M** | * Kable umożliwiająca rozszerzenie funkcjonalności przełączników z portem SFP/SFP+/SFP28 o interfejs światłowodowy 25 Gbps.
* Kabel o długości 5 m.
* Zamawiający wymaga, aby kable pochodziły od tego samego producenta co dostarczone przełączniki Data Center.
 |
| **2.** | **4 moduły QSFP-100G-AOC3M** | * Kable umożliwiająca rozszerzenie funkcjonalności przełączników z portem QSFP+ o interfejs światłowodowy 100 Gbps.
* Kabel o długości 3m.
* Zamawiający wymaga, aby kable pochodziły od tego samego producenta co dostarczone przełączniki Data Center.
 |
| **3.** | **20 szt Patchord LC-LC – Typ 1** | * [Patchcord światłowodowy wielomodowy, LC-LC, OM3 MM 50/125, duplex, 2m](https://www.fcnet.pl/patchcord-swiatlowodowy-wielomodowy-lc-pc-lc-pc-om3-50-125-duplex-2m.html)
 |
| **4.** | **30 szt Patchord LC-LC – Typ 2** | * [Patchcord światłowodowy wielomodowy, LC-LC, OM3 MM 50/125, duplex, 5m](https://www.fcnet.pl/patchcord-swiatlowodowy-wielomodowy-lc-pc-lc-pc-om3-50-125-duplex-2m.html)
 |

Zamawiający wymaga dla przedmiotu zamówienia w część II zapewnienie wsparcia technicznego na zakupione przełączniki i wyposażenie.

Wymagane jest zapewnienie następującego wsparcia dla urządzeń i całego wyposażenia:

* Minimum. 36 miesięczne wsparcie techniczne na poziomie 8x5xNBD;
* Stała licencja lub 36 miesięczna subskrypcja (w przypadku gdy jest ona niezbędna dla zapewnienia wymaganej funkcjonalności).

Wszystkie elementy zaoferowane w części II przedmiotu zamówienia muszą pochodzić od jednego producenta i z oficjalnej dystrybucji.

# USŁUGA WDROŻENIA PRZEŁĄCZNIKÓW SIECIOWYCH Switch CORE I Switch DATACENTER

1. Prace w centralnym węźle sieci:
	1. Instalacja i konfiguracja przełączników typu 1 w rdzeniu sieci w centralnym węźle sieci:
		1. uzgodnienie konfiguracji połączeń i podsieci VLAN na portach,
		2. konfiguracja wirtualnego połączenia przełączników rdzenia w jeden przełącznik logiczny,
		3. uruchomienie zarządzania przełącznikami przez WWW i SSH,
		4. skonfigurowanie serwera VTP,
		5. aktualizacja firmware,
		6. konfiguracja ustawień czasowych i protokołu NTP
		7. konfiguracja interfejsów sieciowych,
		8. konfiguracja redundantnego połączenia między przełącznikami i firewall,
		9. konfiguracja agregacji portów i protokołu LACP,
		10. konfiguracja sieci VLAN, konfiguracja VLAN-ów na portach,
		11. konfiguracja routingu IP,
		12. konfiguracja protokołu RSTP, konfiguracja ustawień portów związanych z RSTP,
		13. możliwość konfiguracji innych funkcjonalności potrzebnych do optymalnego działania wdrażanych przełączników;
		14. montaż przełączników w szafie;
		15. przeniesienie połączeń sieciowych pracujących w centralnym węźle sieci na nowe przełączniki typu 1.
2. Prace w podrzędnych węzłach sieci
	1. Instalacja nowych urządzeń dostępowych z równoczesnym wyłączaniem starych urządzeń:
		1. uzgodnienie konfiguracji połączeń i podsieci VLAN na portach;
		2. konfiguracja wirtualnego połączenia przełączników rdzenia w jeden przełącznik logiczny;
		3. aktualizacja firmware;
		4. konfiguracja agregacji portów i protokołu LACP;
		5. konfiguracja sieci VLAN, konfiguracja VLAN-ów na portach;
		6. konfiguracja protokołu RSTP, konfiguracja ustawień portów związanych z RSTP;
		7. konfiguracja ustawień czasowych i protokołu NTP;\
		8. możliwość konfiguracji innych funkcjonalności potrzebnych do optymalnego działania wdrażanych przełączników;
		9. montaż przełączników w szafach;
		10. konfiguracja interfejsów sieciowych;
3. Dokumentacja techniczna sieci:
	* 1. opracowanie dokumentacji węzła centralnego;
		2. opracowanie dokumentacji węzła podrzędnego.