Załącznik nr 1.1 do SWZ

**Opis przedmiotu zamówienia – specyfikacja techniczna oferowanego sprzętu**

Katolicki Uniwersytet Lubelski Jana Pawła II posiada sieć zbudowaną w oparciu o kilkaset przełączników firmy Cisco, 3 urządzenia szkieletu sieci firmy Cisco oraz wykwalifikowany zespół administratorów zarządzających tymi urządzeniami. **Zamawiający kontynuuje rozpoczętą w 2023 roku (zakupem 3 rdzeniowych przełączników) modernizację szkieletu sieci. W związku z powyższym wymaga się pełnej kompatybilności z zakupionymi przełącznikami.**

W przypadku zaoferowania sprzętu sieciowego innego producenta Zamawiający wymaga w ramach dostawy:

* **pełnego wdrożenia** wraz z instalacją i konfiguracją urządzeń zgodnie z wytycznymi od Zamawiającego w siedzibie Zamawiającego w terminie 60 dni kalendarzowych z wyłączeniem dni wolnych od pracy, w godzinach pracy Zamawiającego
* **przeszkolenia** w uzgodnionym czasie 4 administratorów Zamawiającego. Szkolenia administratorów mają być szkoleniami certyfikowanymi przez producenta sprzętu, mają odbyć się w Polsce poza siedzibą Zamawiającego np. w certyfikowanym centrum szkoleniowym producenta w odrębnych maksymalnie 5-dniowych (po 40 godzin) cyklach po 2 administratorów. Szkolenia maja być prowadzone w języku polskim w trybie do 8 godzin dziennie wraz z przerwami kawowymi. Szkolenia mają być prowadzone przez szkoleniowców legitymujących się certyfikatem producenta urządzenia w danym zakresie. Szkolenia mają obejmować minimum:
1. aspekty dotyczące budowy (pozyskanie wiedzy o architekturze, możliwościach, pozycjonowaniu i wdrażaniu przełączników),
2. aspekty z zakresu instalacji i uruchomienia (pozyskanie wiedzy umożliwiającej wgląd w przełączniki i ich komponenty, instalowanie wraz z obsługą i konfiguracją; weryfikacją podstawowych sieci IPv4 i IPv6),
3. aspekty dotyczące administrowania urządzeniem (pozyskanie wiedzy o zarządzaniu przełącznikami za pomocą minimum 2 metod, omówienie podstawowych i ważnych funkcji, automatyzacji zarządzania, administrowaniu zespołem urządzeń w dużej organizacji, obsługi i rozwiązywania problemów w sieci korporacyjnej),
4. aspekty dotyczące bezpieczeństwa (pozyskanie wiedzy umożliwiającej identyfikowanie różnych zagrożeń bezpieczeństwa, nabycie umiejętności i technologii potrzebnych do wdrożenia podstawowych rozwiązań bezpieczeństwa w celu zapewnienia zaawansowanej ochrony przed cyberatakami…. )

Wymagane minimum 120 godzin szkoleń dla jednego administratora. Wszystkie szkolenia mają być zakończone uzyskaniem certyfikatów potwierdzonych przez producenta sprzętu w zakresie minimum: administracji, bezpieczeństwa.

W ramach szkoleń wymagane są praktyczne ćwiczenia na zaoferowanych modelach urządzeń fizycznych.

Dostawca pokrywa koszty utrzymania a także zapewnia noclegi oraz pełne wyżywienie na czas trwania szkolenia)

**Zadanie 1: Dostawa przełączników sieciowych typ 1 – 99 szt.**

**Przełączniki dostępowe wyposażone w 48 portów 10/100/1000Base-T oraz 4 porty 1G/10G SFP/SFP+ wraz z licencjami na podstawowe funkcjonalności o poniższych parametrach.**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** |  |
| **Producent:** |  |
| **Typ/model/kod producenta:** |  |
| **Zadanie 1: Przełącznik sieciowy typ 1 – 99 sztuk** |
| **parametr** | **Minimalne wymagania** |
| **Parametry i funkcjonalności** | 1. Typ i liczba portów:* 48 portów 10/100/1000BaseT RJ-45
* 4 porty uplink 1G/10G SFP/SFP+

2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:* Gigabit Ethernet 1000Base-T,
* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,
* Gigabit Ethernet 1000Base-EX,
* Gigabit Ethernet 1000Base-ZX,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet 10GBase-ER,
* 10Gigabit Ethernet 10GBase-ZR,
* 10Gigabit Ethernet – kable połączeniowe typu DAC (SFP+ - SFP+),

3. Umożliwiający rozbudowę o funkcjonalność stackowania przełączników z zapewnieniem następujących funkcjonalności:* Przepustowość w ramach stosu - 80Gb/s,
* 8 urządzeń w stosie,
* Zarządzanie poprzez jeden adres IP,
* Umożliwiający tworzenie połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

4. Zasilanie i chłodzenie:* **Zainstalowany zasilacz**
* Umożliwiający instalację zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap**)**
* Redundantne wentylatory,

5. Parametry wydajnościowe:* Przepustowość przełącznika (switching capacity) minimum 170 Gb/s,
* Prędkość przesyłania (forwarding rate) minimum 130 Mpps
* Bufor pakietów – 6MB
* Pamięć DRAM – 2GB
* Pamięć flash – 4GB
* Obsługa:
* 500 aktywnych sieci VLAN
* 16000 adresów MAC
* 3000 tras IPv4
* 1500 tras IPv6
* Ilość wpisów w listach kontroli dostępu Security ACL – 1000
* ilość wpisów w listach kontroli dostępu QoS ACL – 1000
* 512 interfejsów SVI L3
* Jumbo frame 9198B
* 48 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP

6. Obsługujący protokół NTP7. Obsługujący IGMPv1/2/3 i MLDv1/2 Snooping8. Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługa 64 instancji protokołu STP
* Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
* 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, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

9. Obsługa protokołu LLDP i LLDP-MED10. Realizujący funkcje 802.1Q tunneling (QinQ)11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC12. Obsługujący funkcję Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego13. Umożliwiający uruchomienie funkcji serwera DHCP14. Mechanizmy związane z bezpieczeństwem sieci:* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiający zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
* Obsługujący funkcje Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
* Umożliwiający uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
* Umożliwiający uwierzytelnianie użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
* Umożliwiający uwierzytelnianie wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
* Umożliwiający obsługę żądań Change of Authorization (CoA) zgodnie z RFC 5176,
* Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
* Obsługujący funkcje Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Zapewniający podstawowe mechanizmy 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),
* Umożliwiający autoryzację prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługujący listy kontroli dostępu (ACL) następujących typów:
	+ Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
	+ VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
	+ Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
	+ Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
* Umożliwiający szyfrowanie 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),
* Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
* Funkcja Private VLAN;

15. Obsługujący mechanizmy zapewaniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:* sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

16. Mechanizmy związane z zapewnieniem jakości usług w sieci:* Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
* Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
* Umożliwiający obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Umożliwiający ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
* Kontrola sztormów dla ruchu broadcast/multicast/unicast,
* Umożliwiający zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

17. Obsługa protokołów i mechanizmów routingu:* Routing statyczny dla IPv4 i IPv6,
* Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes,
* Policy-based routing (PBR),
* Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
* Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

18. Przełącznik umożliwiający 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,19. Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,20. Przełącznik posiadający 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.),21. Funkcjonalność sondy IP SLA Responder,22. Zarządzanie:* Port konsoli,
* Dedykowany port Ethernet do zarządzania out-of-band,
* Umożliwiający realizację dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwiająca kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
* 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,
* Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
* Umożliwiający konfigurację za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
* Wsparcie dla protokoły RESTCONF,
* Wsparcie dla protokołu gNMI,
* Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
* Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
* Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
1. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
2. Monitoring pracy przełącznika w zakresie:
	1. Użycie CPU, użycie pamięci, temperatura pracy,
	2. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
	3. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
	4. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
	5. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
	6. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
	7. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
	8. Protokół REP (Resilient Ethernet Protocol),
	9. Protokół STP (Spanning Tree Protocol),
	10. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
3. Konfigurację przełącznika w zakresie:
	1. Konfiguracja interfejsów:
		* Fizycznych:

- opis interfejsu, prędkość, tryb pracy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)* Logicznych typu „port channel”:

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)* Wirtualnych typu SVI:

- opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP)* Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
* Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
* Konfiguracja mechanizmów SPAN i RSPAN,
* Konfiguracja protokołu STP,
* Konfiguracja protokołu REP,
* Konfiguracja routingu statycznego i dynamicznego,
* Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
* Tworzenie i przypisanie list kontroli dostępu ACL,
* Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
* Konfiguracja i uruchomienie NetFlow (sprzętowe wsparcie protokołu Netflow bez samplowania oraz eksportu statystyk ruchu do zewnętrznych kolektorów danych),
* Konfiguracja polityk QoS,
* Administracja przełącznika w zakresie:
	+ Zdalne uruchamianie komend linii poleceń,
	+ Nazwa przełącznika,
	+ Tryb pracy L2/L3,
	+ Adres IP przełącznika do celów zarządzania zdalnego,
	+ Konfiguracja serwera DHCP,
	+ Konfiguracja DNS,
	+ Czas systemowy w tym protokół NTP,
	+ Konta administracyjne,
	+ Upgrade oprogramowania,
	+ Backup konfiguracji,
	+ Zdalny restart urządzenia,
	+ Konfiguracja i dostęp przez SNMP,
* Diagnostyka urządzenia:
	+ Narzędzie PING i TRACEROUTE,
	+ Przeglądanie logów systemowych,
	+ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
1. Umożliwiający tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
 |
| Właściwości fizyczne | * Umożliwiający montaż w szafie rack 19”
* Wysokość urządzenia 1 RU,
* Głębokość chassis urządzenia bez wentylatorów i kabli zasilających nie większa niż 30 cm,
 |
| Wyposażenie | 1. Urządzenie wyposażone w licencję subskrypcyjną na okres **zaoferowanej** gwarancji
2. Uchwyty montażowe do szafy rack 19”
3. Moduł GLC-TE CML (CML SFP [10/100/1000M] RJ45 100m) – pakiet **10 szt** **do całego Zadania**; Zamawiający dopuszcza moduły wyprodukowane przez innego producenta, ale z potwierdzoną kompatybilnością jednak w przypadku zaoferowania urządzeń sieciowych innego producenta Zamawiający wymaga modułów oryginalnych od producenta)
4. Kabel konsolowy USB-A - RJ45 – pakiet **10 szt** **do całego Zadania**;
5. Patchcord kat 6a. klasa EA UTP, LSOH, zabezpieczony wtyk przed wyłamaniem, 1,5 mb – **4 szt** (dla każdego przełącznika)
6. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 2 mb – **4 szt** (dla każdego przełącznika)
7. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 3 mb – **10 szt** (dla każdego przełącznika)
8. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 5 mb – **5 szt** (dla każdego przełącznika)
9. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 7 mb – **10 szt** (dla każdego przełącznika)
10. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 10 mb – **5 szt** (dla każdego przełącznika)

Wszystkie kable mają być wykonane zgodnie z obowiązującym standardem dla okablowania strukturalnego - **T568B, złącza** z wysokiej jakości **kontaktami platerowanymi złotem,** kształt zalewanej osłony o niewielkich rozmiarach ma zapewniać możliwość stosowania w panelach krosowych o dużej gęstości upakowania portów. Minimalny promień gięcia - 4 średnice kabla. Pasmo pracy do 500 MHz. Wraz z dostawą Wykonawca dostarczy kartę katalogową producenta.**Zasilacz dodatkowy** – przeznaczony do zainstalowania do oferowanych przełączników (2 zasilacze dodatkowe do całej dostawy przełączników), stanowiący awaryjny zapas. Moc zasilacza taka jak zasilaczy zainstalowanych w przełączniku. Zasilacz nowy z pełną gwarancją. |
| Gwarancja | * Min. 36 miesięcy (zgodnie z ofertą Wykonawcy) gwarancji z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365/366.
 |

**Zadanie 2. Dostawa przełączników sieciowych typ 2 – 20 szt.**

**Przełączniki dostępowe wyposażone w 48 portów 10/100/1000Base-T z funkcjonalnością PoE oraz 4 porty 1G/10G SFP/SFP+ wraz z licencjami na podstawowe funkcjonalności o poniższych parametrach.**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** |  |
| **Producent:** |  |
| **Typ/model/kod producenta:** |  |
| **Zadanie 2: Przełącznik sieciowy typ 2 – 20 sztuk** |
| **parametr** | **Minimalne wymagania** |
| **Parametry i funkcjonalności** | 1. Typ i liczba portów:* 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at),
* 4 porty uplink 1G/10G SFP/SFP+

2. Moc dostępna dla PoE:* 740W (z jednym zasilaczem o mocy 1KW),
* 740W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie redundantnym),
* 1440W (z dwoma zasilaczami o mocy 1KW pracującymi w układzie współdzielenia mocy),

3. Porty SFP/SFP+ umożliwiające obsadzenie następującymi rodzajami wkładek:* Gigabit Ethernet 1000Base-T,
* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,
* Gigabit Ethernet 1000Base-EX,
* Gigabit Ethernet 1000Base-ZX,
* 10Gigabit Ethernet 10GBase-SR,
* 10Gigabit Ethernet 10GBase-LR,
* 10Gigabit Ethernet 10GBase-ER,
* 10Gigabit Ethernet 10GBase-ZR,
* 10Gigabit Ethernet – kable połączeniowe typu DAC (SFP+ - SFP+),

4. Możliwość rozbudowy o funkcjonalność stackowania przełączników z zapewnieniem następujących funkcjonalności:* Przepustowość w ramach stosu - 80Gb/s,
* 8 urządzeń w stosie,
* Zarządzanie poprzez jeden adres IP,
* Umożliwiający tworzenie połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,

5. Zasilanie i chłodzenie:* **Zainstalowany zasilacz**
* Umożliwiający instalację zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap**)**
* Przełącznik umożliwiający podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
* W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwiający przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
* Redundantne wentylatory,

6. Parametry wydajnościowe:* Przepustowość przełącznika (switching capacity) minimum 170 Gb/s,
* Prędkość przesyłania (forwarding rate) minimum 130 Mpps
* Bufor pakietów – 6MB
* Pamięć DRAM – 2GB
* Pamięć flash – 4GB
* Obsługa:
* 500 aktywnych sieci VLAN
* 16000 adresów MAC
* 3000 tras IPv4
* 1500 tras IPv6
* Ilość wpisów w listach kontroli dostępu Security ACL – 1000
* ilość wpisów w listach kontroli dostępu QoS ACL – 1000
* 512 interfejsów SVI L3
* Jumbo frame 9198B
* 48 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP

7. Obsługujący protokół NTP8. Obsługujący IGMPv1/2/3 i MLDv1/2 Snooping9. Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługujący 64 instancji protokołu STP
* Wspierający protokół REP (Resilient Ethernet Protocol)
* 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, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego

10. Obsługujący protokół LLDP i LLDP-MED11. Realizujący funkcje 802.1Q tunneling (QinQ)12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC13. Obsługujący funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego14. Umożliwiający uruchomienie funkcji serwera DHCP15. Mechanizmy związane z bezpieczeństwem sieci:* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
* Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
* Umożliwiający uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
* Umożliwiający uwierzytelnianie użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
* Umożliwiający uwierzytelnianie wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
* Umożliwiający obsługę żądań Change of Authorization (CoA) zgodnie z RFC 5176,
* Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
* Obsługujący funkcje Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Zapewniający podstawowe mechanizmy 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),
* Umożliwiający autoryzację prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługujący list kontroli dostępu (ACL) następujących typów:
	+ Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
	+ VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
	+ Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
	+ Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
* Umożliwiający szyfrowanie 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),
* Posiadający wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
* Funkcja Private VLAN;

16. Obsługujący mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:* sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

17. Mechanizmy związane z zapewnieniem jakości usług w sieci:* Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
* Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
* Umożliwiający obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Umożliwiający ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
* Kontrolujący sztormy dla ruchu broadcast/multicast/unicast,
* Umożliwiający zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

18. Obsługujący protokoły i mechanizmy routingu:* Routing statyczny dla IPv4 i IPv6,
* Routing dynamiczny – RIP, OSPF do 1000 routes, PIM Stub do 1000 routes,
* Policy-based routing (PBR),
* Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
* Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

19. Przełącznik umożliwiający 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,20. Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,21. Przełącznik posiadający 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.),22. Funkcjonalność sondy IP SLA Responder,23. Zarządzanie:* Port konsoli,
* Dedykowany port Ethernet do zarządzania out-of-band,
* Umożliwiający realizację dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
* 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,
* Obsługujący protokoły SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
* Umożliwiający konfigurację za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
* Wsparający protokoły RESTCONF,
* Wsparający protokół gNMI,
* Przełącznik posiadający diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
* Przełącznik posiadający wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
* Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
1. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
2. Monitoring pracy przełącznika w zakresie:
	1. Użycie CPU, użycie pamięci, temperatura pracy,
	2. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
	3. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
	4. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
	5. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
	6. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
	7. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
	8. Protokół REP (Resilient Ethernet Protocol),
	9. Protokół STP (Spanning Tree Protocol),
	10. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
3. Konfigurację przełącznika w zakresie:
	1. Konfiguracja interfejsów:
		* Fizycznych:

- opis interfejsu, prędkość, tryb pracy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)* Logicznych typu „port channel”:

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)* Wirtualnych typu SVI:

- opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP)* Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
* Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
* Konfiguracja mechanizmów SPAN i RSPAN,
* Konfiguracja protokołu STP,
* Konfiguracja protokołu REP,
* Konfiguracja routingu statycznego i dynamicznego,
* Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
* Tworzenie i przypisanie list kontroli dostępu ACL,
* Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
* Konfiguracja i uruchomienie NetFlow (sprzętowe wsparcie protokołu Netflow bez samplowania oraz eksportu statystyk ruchu do zewnętrznych kolektorów danych),
* Konfiguracja polityk QoS,
* Administracja przełącznika w zakresie:
	+ Zdalne uruchamianie komend linii poleceń,
	+ Nazwa przełącznika,
	+ Tryb pracy L2/L3,
	+ Adres IP przełącznika do celów zarządzania zdalnego,
	+ Konfiguracja serwera DHCP,
	+ Konfiguracja DNS,
	+ Czas systemowy w tym protokół NTP,
	+ Konta administracyjne,
	+ Upgrade oprogramowania,
	+ Backup konfiguracji,
	+ Zdalny restart urządzenia,
	+ Konfiguracja i dostęp przez SNMP,
* Diagnostyka urządzenia:
	+ Narzędzie PING i TRACEROUTE,
	+ Przeglądanie logów systemowych,
	+ Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
1. Umożliwiający tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
 |
| Parametry fizyczne  | * Umożliwiający montaż w szafie rack 19”
* Wysokość urządzenia 1 RU,
* Głębokość chassis urządzenia bez wentylatorów i kabli zasilających nie większa niż 30 cm,
 |
| Wyposażenie | 1. Urządzenie wyposażone w licencję subskrypcyjną na okres zaoferowanej gwarancji2. uchwyty montażowe do szafy Rack 19”3. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 1,5 mb – **4 szt** (dla każdego przełącznika)4. Patchcordkat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 2 mb – **10 szt** (dla każdego przełącznika)5. Patchcord kat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 3 mb – **10 szt** (dla każdego przełącznika)7. Patchcordkat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 5 mb – **5 szt** (dla każdego przełącznika)8. Patchcordkat 6a. UTP, LSOH, klasa EA zabezpieczony wtyk przed wyłamaniem, 7 mb – **10 szt** (dla każdego przełącznika)9. Patchcordkat 6a. UTP, LSOH, klasa EA, zabezpieczony wtyk przed wyłamaniem, 10 mb – **5 szt** (dla każdego przełącznika)Wszystkie kable mają być wykonane zgodnie z obowiązującym standardem dla okablowania strukturalnego - **T568B, złącza** z wysokiej jakości **kontaktami platerowanymi złotem,** kształt zalewanej osłony o niewielkich rozmiarach ma zapewniać możliwość stosowania w panelach krosowych o dużej gęstości upakowania portów. Minimalny promień gięcia - 4 średnice kabla. Pasmo pracy do 500 MHz.Wraz z dostawą Wykonawca dostarczy kartę katalogową producenta.10. Moduł SFP+ 10gbps SR (Zamawiający dopuszcza moduły wyprodukowane przez innego producenta, ale z potwierdzoną kompatybilnością jednak w przypadku zaoferowania urządzeń sieciowych innego producenta Zamawiający wymaga modułów oryginalnych od producenta) – **pakiet 60 szt. do całego zadania** 11. Moduł SFP+ 10gbps LR z obsługą do 10 km. (Zamawiający dopuszcza moduły wyprodukowane przez innego producenta, ale z potwierdzoną kompatybilnością jednak w przypadku zaoferowania urządzeń sieciowych innego producenta Zamawiający wymaga modułów oryginalnych od producenta) – **pakiet 60 szt. do całego zadania** **12. Zasilacze dodatkowe** – przeznaczone do zainstalowania do oferowanych przełączników (**2 dodatkowe zasilacze do całego zadania**), stanowiące awaryjny zapas. Moc zasilacza taka jak zasilaczy zainstalowanych w przełączniku. Zasilacz nowy z pełną gwarancją tak jak urządzenia. |
| Gwarancja | * Min. 36 miesięcy ( zgodnie z ofertą Wykonawcy) gwarancji z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365/366.
 |

**Zadanie 3. Dostawa przełącznika sieciowego typ 3 – 3 szt.**

**Przełącznik dostępowy wyposażone w 48 portów 1/10/25G SFP+ oraz 4 porty 40/100G QSFP+ wraz z licencjami na funkcjonalności o poniższych parametrach.**

|  |  |  |
| --- | --- | --- |
|  | **Nazwa oferowanego urządzenia:** |  |
|  | **Producent:** |  |
|  | **Typ/model/kod producenta:** |  |
|  | **Zadanie 3: Przełącznik sieciowy – 3 sztuki** |
|  | **parametr** | **Minimalne wymagania** |
|  | **Parametry i funkcjonalności** | 1. Typ i liczba portów:
2. 48 portów 1G/10G/25G SFP/SFP+
3. 4 porty uplink 40/100G QSFP+
4. Porty SFP/SFP+ umożliwiające obsadzenie następującymi rodzajami wkładek:
5. Gigabit Ethernet 1000Base-T,
6. Gigabit Ethernet 1000Base-SX,
7. Gigabit Ethernet 1000Base-LX/LH,
8. Gigabit Ethernet 1000Base-EX,
9. Gigabit Ethernet 1000Base-ZX,
10. 10Gigabit Ethernet 10GBase-SR,
11. 10Gigabit Ethernet 10GBase-LR,
12. 10Gigabit Ethernet 10GBase-ER,
13. 10Gigabit Ethernet 10GBase-ZR,
14. 10Gigabit Ethernet DAC (SFP+ - SFP+),
15. Porty QSFP umożliwiające zastosowanie następujących modułów interfejsowych:
16. 40G-SR4,
17. 40G-LR4,
18. 40G-ER4,
19. 40G-SR-BD,
20. 40G-CSR4,
21. 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
22. adapter 40G QSFP->10G SFP+
23. 40Gigabit Ethernet DAC QSFP+ (QSFP+ - QSFP+),
24. Zasilanie i chłodzenie:
25. Zainstalowane **2** redundantne zasilacze AC230V do pracy w trybie 1:1.
26. Zainstalowane **2** redundantne wentylatory,
27. Parametry wydajnościowe:
28. Przepustowość przełącznika (switching capacity) 1200 Gb/s**,**
29. Prędkość przesyłania 64-bit (64-bit forwarding rate) 900 Mpps
30. Pamięć DRAM – 8GB
31. Pamięć flash – 8GB
32. Obsługa:
* 980 aktywnych sieci VLAN
* 30000 adresów MAC
* 23000 tras IPv4
* Jumbo frame 9198B
1. Obsługa protokołu NTP
2. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
3. Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
4. IEEE 802.1w Rapid Spanning Tree
5. Per-VLAN Rapid Spanning Tree (PVRST+)
6. IEEE 802.1s Multi-Instance Spanning Tree
7. Obsługa 128 instancji protokołu STP
8. Wspierający protokół REP (Resilient Ethernet Protocol)
9. 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, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego
10. Obsługujący protokoły CDP, LLDP i LLDP-MED
11. Realizujący funkcj 802.1Q tunneling (QinQ)
12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
13. Obsługujący funkcje Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
14. Umożliwiający uruchomienie funkcji serwera DHCP
15. Mechanizmy związane z bezpieczeństwem sieci:
16. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
17. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
18. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
19. Obsługujący funkcje Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
20. Umożliwiający uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
21. Umożliwiający uwierzytelnianie użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
22. Umożliwiający uwierzytelnianie wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
23. Umożliwiający obsługę żądań Change of Authorization (CoA) zgodnie z RFC 5176,
24. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
25. Obsługujący funkcje Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
26. Zapewniający podstawowe mechanizmy 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),
27. Umożliwiający autoryzację prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
28. Obsługujący list kontroli dostępu (ACL) następujących typów:
* Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
* Umożliwiający konfigurację tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
1. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
2. Umożliwiający próbkowanie i eksport statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym – NetFlow – obsługa 48.000 strumieni
3. Umożliwiający szyfrowanie ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128)
4. Private VLAN
5. Mechanizmy związane z zapewnieniem jakości usług w sieci:
6. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
7. Umożliwiający obsługę jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
8. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
9. Umożliwiający ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
10. Kontrolujący sztormy dla ruchu broadcast/multicast/unicast,
11. Umożliwiający zmianę przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
12. Obsługujący protokoły i mechanizmy routingu:
13. Routing statyczny dla IPv4 i IPv6,
14. Routing dynamiczny – RIP, OSPF do 1000 tras
15. Policy-based routing (PBR),
16. Przełącznik umożliwiający 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,
17. Przełącznik posiadający funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
18. Przełącznik posiadający 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.),
19. Zarządzanie:
20. Port konsoli,
21. Dedykowany port Ethernet do zarządzania out-of-band,
22. 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,
23. Obsługujący protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
24. Umożliwiający konfigurację za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
25. Wspierający protokół RESTCONF,
26. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
27. Umożliwiający tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
28. Wbudowany analizator pakietów,
29. Funkcjonalność bramy dla usług mDNS
30. Obsługujący protokół redundancji bramy – VRRP
 |
|  | **Parametry fizyczne** | * Umożliwiający montaż w szafie rack 19”,posiadający w zestawie uchwyty
* Wysokość urządzenia 1 RU,
* Głębokość chassis urządzenia z wentylatorami, i zasilaczami mniejsza niż 50 cm,
 |
|  | **Wyposażenie urządzenia** | 1. Uchwyty montażowe do szafy rack 19”,
2. wkładka 40GBASE-SR BIDI QSFP Module for Duplex MMF (QSFP+, 40GB, SR, 850nm, 100m, MPO, moduł 40GBASE-SR); Zamawiający dopuszcza moduły wyprodukowane przez innego producenta, ale z potwierdzoną kompatybilnością, jednak wprzypadku zaoferowania urządzeń innego producenta Zamawiający wymaga wkładek oryginalnych od producenta. – **3 szt**. (do każdego urządzenia)
3. kabel DAC QSFP 100Gbit do łączenia uplinków - **2 szt**. (do każdego urządzenia; )
 |
|  | **Gwarancja**  | * Min 36 miesięcy( zgodnie z ofertą wykonawcy) gwarancji na sprzęt.
 |

**\*Uwaga, wymagane jest uzupełnienie tabeli**

**Wykonawca zobowiązany jest do podania nazwy oferowanego urządzenia, producenta, typu/modelu /kodu producenta. Podane dane oraz uzupełniona kolumna pn: Parametry oferowane muszą pozwolić Zamawiającemu na jednoznaczną identyfikację oferowanego produktu.**

**Każdorazowo gdy Zamawiający używa nazwy własnej, certyfikatu, standardu lub normy należy przez to rozumieć treść danego parametru łącznie ze sformułowaniem 'lub równoważny".**

**DOKUMENT NALEŻY PODPISAĆ KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM.**

Rozwiązania równoważne – odpowiednio dla każdego z zadań:

1. W przypadku użycia w SWZ lub załącznikach odniesień do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy, Zamawiający dopuszcza rozwiązania równoważne opisywanym. Wykonawca analizując opis przedmiot zamówienia powinien założyć, że każdemu odniesieniu o którym mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy użytemu w opisie przedmiotu zamówienia dla każdego z zadań towarzyszy wyraz „lub równoważne”.
2. W przypadkach użycia w SWZ lub załącznikach nazw własnych, dopuszcza się złożenie oferty z asortymentem równoważnym do wskazanego przedmiotu zamówienia. Zamawiający określił referencyjnego producenta/dostawcę, w celu dokładnego sprecyzowania wymagań, jaki musi spełniać oferowany przez Wykonawców asortyment. Wykonawca analizując opis przedmiot zamówienia powinien założyć, że każdemu odniesieniu o którym mowa w art. 101 ust. 1 pkt 2 i ust. 3 ustawy użytemu w opisie przedmiotu zamówienia dla każdego z zadań towarzyszy wyraz „lub równoważne”. Zamawiający dopuszcza zaoferowanie asortymentu i rozwiązań, równoważnych jakościowo, eksploatacyjnie i technicznie do materiałów wskazanych przez Zamawiającego z określeniem referencyjnego producenta/dostawcy. Wykonawca składający ofertę z asortymentem równoważnym, musi spełnić warunki określone w niniejszym SWZ pod rygorem odrzucenia oferty jako niezgodnej z treścią SWZ.
3. W przypadku, gdy w SWZ lub załącznikach zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować asortyment równoważny, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie rozwiązań przyjętych w opisie przedmiotu zamówienia dla każdego z zadań. Wykonawca, który zastosuje standardy równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego rozwiązania spełniają wymagania określone przez Zamawiającego. Użycie w SWZ lub załącznikach oznakowania oznacza, że Zamawiający akceptuje także wszystkie inne oznakowania potwierdzające, że dane dostawy spełniają równoważne wymagania. W przypadku, gdy Wykonawca z przyczyn od niego niezależnych nie może uzyskać określonego przez Zamawiającego oznakowania lub oznakowania potwierdzającego, że dane dostawy spełniają równoważne wymagania, Zamawiający w terminie przez siebie wyznaczonym akceptuje inne odpowiednie środki dowodowe, w szczególności dokumentację producenta, o ile dany Wykonawca udowodni, że dostawy, które mają zostać przez niego wykonane, spełniają wymagania określonego oznakowania lub określone wymagania wskazane przez Zamawiającego.

Wykonawca, który powołuje się na produkty równoważne wyszczególnione w formularzu Opis przedmiotu zamówienia – specyfikacja techniczna oferowanego sprzętu odpowiednio dla każdego z zadań zobowiązany jest:

 - W przypadku oferowania rozwiązania równoważnego, Wykonawca jest zobowiązany wykazać, że oferowane przez niego rozwiązanie równoważne spełnia wymagania określone przez Zamawiającego, poprzez załączenie do oferty dowodów potwierdzających, że rozwiązanie równoważne spełnia wszystkie parametry równoważności. Dowody te powinny zawierać informacje umożliwiające Zamawiającemu weryfikację spełniania przez rozwiązanie równoważne poszczególnych parametrów równoważności,

- Zamawiający wymaga, aby zaoferowane przez Wykonawcę rozwiązania równoważne nie wiązały się z koniecznością wykonania dodatkowych prac testowych, migracyjnych czy integracyjnych po stronie Zamawiającego, tym samym poniesienia niezaplanowanych, dodatkowych kosztów