Załącznik nr 2 do SWZ
FZ-2380/27/21/SS

Opis przedmiotu zamówienia

na dostawę sprzętu łączności w ramach I wyposażenia jednostek podległych KWP w Łodzi

Postanowienia ogólne do części 1 i 2

Wykonawca udziela Zamawiającemu gwarancji na dostarczone urządzenia wg zasad:

1. Do dostarczonego sprzętu będą dołączone karty gwarancyjne zawierające numer seryjny, termin i warunki ważności gwarancji, adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne (dopuszcza się zastosowanie jednej gwarancji zbiorczej)
2. W okresie gwarancji Wykonawca zapewnia nieodpłatne usługi serwisowe, autoryzowanego przez producenta urządzenia punktu serwisowego (lub jego oficjalnego przedstawiciela w Polsce).
3. Wykonawca zobowiązuje się do dokonania naprawy gwarancyjnej w ciągu maksymalnie 14 dni (zgodnie ze złożoną ofertą) od chwili pisemnego zgłoszenia uszkodzenia. W przypadku gdy naprawa w tym terminie nie jest możliwa, Wykonawca dostarczy Zamawiającemu urządzenie zastępcze o takich samych lub lepszych parametrach technicznych co naprawiany sprzęt.
4. Wykonawca dokona nieodpłatnej wymiany urządzenia na nowe w terminie 7 dni, gdy urządzenie po dwóch kolejnych naprawach tego samego elementu lub zespołu wykaże wady w działaniu.
5. Wymiana urządzenia automatycznie powoduje obowiązek Wykonawcy wystawienia nowej karty gwarancyjnej z określonym terminem gwarancji , począwszy od dnia wymiany.
6. Wszelkie zgłoszenia związane z wykonaniem warunków gwarancji, dokonywane w formie pisemnej będą przyjmowane w dni robocze. Wykonawca w karcie gwarancyjnej zamieści adres i numer faksu autoryzowanego punktu serwisowego.
7. Wszelkie koszty związane ze świadczeniem zobowiązań gwarancyjnych, w tym dojazdów i transportu w okresie gwarancji ponosi Wykonawca.

CZĘŚĆ 1

Dostawa urządzeń wraz z licencjami telefonii VoIP

1. Wszystkie dostarczone przez Wykonawcę urządzenia:

1.1. Muszą być fabrycznie nowe. Nie dopuszcza się dostaw pochodzących z demontażu, używanych lub uprzednio naprawianych.
1.2. Urządzenia muszą być dostarczony przez Wykonawcę w oryginalnych opakowaniach producenta wraz z instrukcją obsługi w języku polskim lub angielskim (instrukcja może być w formie elektronicznej).
1.3. Nie mogą być starsze niż 6 miesięcy od daty dostawy.
1.4. Muszą pochodzić z autoryzowanego kanału dystrybucji producenta.
1.5. Muszą być produktem przeznaczonym na rynek polski lub na rynek Unii Europejskiej
1.6. Muszą posiadać nie mniej niż 24 miesiące gwarancji producenta realizowanej na terenie Polski przez autoryzowany serwis.
1.7. Korzystanie przez Zamawiającego z zakupionych urządzeń i oprogramowania nie może naruszać majątkowych praw autorskich osób trzecich.

1.8. Zamawiający wymaga, by w chwili nabycia licencji stał się ich jedynym właścicielem z pełnymi prawami oraz pełnymi prawami do korzystania z oprogramowania.
1.9. Zamawiający posiada wiedzę na temat nadzoru i konfiguracji oraz używa w swojej infrastrukturze VoIP produktów marki Cisco. W związku z tym dostarczony sprzęt musi być w pełni kompatybilny z urządzeniami posiadanymi przez Zamawiającego oraz dawać możliwość wykorzystywania wszystkich funkcjonalności posiadanego przez Zamawiającego oraz dostarczonego przez Wykonawcę sprzętu.
1.10. W przypadku zaoferowania innych produktów niż posiada Zamawiający, Wykonawca będzie zobowiązany do:
  1.10.1. zainstalowania i uruchomienia urządzenia,
  1.10.2. w przypadku urządzeń zarządzalnych dostarczenia kompletu oprogramowania i okablowania do konfiguracji,
  1.10.3. przeszkolenia 4 administratorów w zakresie konfiguracji i zarządzania urządzeniami. (szkolenie powinno zapewnić poziom wiedzy pozwalający na wykorzystanie wszystkich funkcjonalności dostarczonych urządzeń).

2. Aparaty – wymagania dla wszystkich aparatów VoIP /minimum techniczne/:

2.1. Obsługa cyfrowych łączy Ethernet 10/100/1000 Mb/s z protokołem sygnalizacyjnym SCCP lub SIP (RFC 3261).
2.2. Obsługa kodeków G.711a, G.729a, G.722, iLBC.
2.3. Adres IP telefonu ustawiany statycznie lub przydzielany dynamicznie poprzez DHCP;
2.4. Zabezpieczenie transmisji poprzez zastosowanie protokołów Transport Layer Security (TLS) i Secure Real-Time Protocol (SRTP);
2.5. Zaimplementowane mechanizmy Quality Of Service (QOS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
2.6. Obsługa RTCP.
2.7. Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP.
2.8. Pełna współpraca z klastrem (CUCM) Cisco Unified Communication Manager wersja 12.5 (właściwa sygnalizacja zwrotna, BLF itp.).
2.9. Obsługa wszystkich funkcji oferowanych przez serwer VoIP a w szczególności:
  2.9.1. identyfikacja numeru dla połączeń przychodzących,
  2.9.2. warunkowe i bezwarunkowe przenoszenie wywołań,
  2.9.3. parkowanie połączeń,
  2.9.4. połączenia oczekujące,
  2.9.5. transferowanie połączeń,
  2.9.6. funkcja sygnalizacji zajętości (BLF)
  2.9.7. zestawianie telekonferencji.
2.10. Telefon musi posiadać następujące przyciski funkcyjne zdefiniowane jako klawisze stałe lub programowe (softkey):
  2.10.1. dostęp do listy kontaktów,
  2.10.2. dostęp do ustawień urządzenia,
  2.10.3. transfer rozmowy,
  2.10.4. dostęp do konferencji,
  2.10.5. zawieszenie połączenia,
  2.10.6. dostępu do poczty głosowej,
  2.10.7. sterowanie głośnością,
  2.10.8. włączenie/wyłączenie mikrofonu,
  2.10.9. włączenie/wyłączenie zestawu nagłownego,
  2.10.10. włączenie/wyłączenie trybu głośnomówiącego.
2.11. Zdalne wykonywanie zmian konfiguracyjnych oraz nadzoru z poziomu CUCM (poprzez interfejs zarządzania CUCM).
2.12. Automatyczny upgrade/downgrade firmware-u i pobieranie konfiguracji z serwera TFTP wbudowanego w CUCM (nie dopuszcza się innych serwerów wymiany plików dostępnych w sieci IP przeznaczonej dla telefonów).
2.13. Szyfrowanie plików konfiguracyjnych.

2.14. Uwierzytelnienie przy użyciu podpisu elektronicznego plików firmware i konfiguracyjnych.
2.15. Obsługa uwierzytelniania za pomocą mechanizmu IEEE 802.1X zarówno telefonu jak i komputera podłączonego do sieci poprzez telefon.
2.16. Wbudowana przeglądarka XML.
2.17. Zasilanie przez PoE w standardzie IEEE 802.3af lub 802.3at oraz z sieci elektroenergetycznej ~230V (zasilacz sieciowy 230V nie jest wymagany).
2.18. Dodatkowe gniazdo Ethernet RJ-45 10/100/1000 BASE-T do podłączenia komputera.
2.19. Transmisja głosu z telefonu i danych z komputera PC musi być przesyłana w dwóch różnych sieciach VLAN, przy czym konfiguracja VLAN-ów powinna być pobierana ze switcha dostępowego przy wykorzystaniu protokołu CDP.
2.20. Połączenie pomiędzy telefonem a przełącznikiem dostępowym powinno być realizowane przy wykorzystaniu trunku w standardzie IEEE 802.1Q.
2.21. Identyfikacja numeru dla połączeń przychodzących.
2.22. Wyświetlacz niedotykowy, z podświetleniem.
2.23. Ciemny kolor obudowy (czarny,grafit, antracyt itp.)
2.24. Dedykowane gniazdo do podłączenia zestawu nagłownego.
2.25. System głośnomówiący dwukierunkowy, działający w trybie pełnego dupleksu.
2.26. Niezależna regulacja głośności słuchawki i systemu głośnomówiącego.
2.27. Obsługa w języku polskim.
2.28. Instrukcja obsługi w języku polskim.
2.29. Możliwość montażu na ścianie (opcjonalny zestaw do montażu na ścianie nie jest wymagany);
2.30. Obsługa protokołu CDP (Cisco Discovery Protocol).

3. Aparat sekretarsko-dyrektorski - 10 szt. - aparat VoIP wraz z licencjami spełniający poniższe wymagania /minimum techniczne/:

3.1. Spełnia wymagania opisane w punkcie 2 - ” Aparaty – wymagania dla wszystkich aparatów VoIP”.
3.2. Obsługa nie mniej niż pięciu (5) linii (numerów) telefonicznych.
3.3. Nie mniej niż trzydzieści dwa (32) klawisze szybkiego wyboru z możliwością zaprogramowania funkcji BLF.
3.4. Kolorowy graficzny wyświetlacz o rozdzielczości nie mniejszej niż 800 x 480 pixeli.
3.5. Przy włączonym zasilaniu PoE pobór mocy nie może przekroczyć 25,5 W.
3.6. Możliwość rozbudowy telefonu o nie mniej niż dwadzieścia osiem (28) dodatkowych programowalnych klawiszy szybkiego wyboru obsługujących funkcję BLF (np. poprzez dołączenie dodatkowego modułu z klawiszami).
3.7. Zapewnia prowadzenie wideorozmowy z rozdzielczością pionową 720p przy wykorzystaniu kodeka H.264 AVC
3.8. Wbudowana kamera z przesłoną zapewniającą prywatność użytkownikowi aparatu.

4. Aparat z wideorozmową - 20 szt. - aparat VoIP wraz z licencjami spełniający poniższe wymagania /minimum techniczne/:

4.1. Spełnia wymagania opisane w punkcie 2 - ” Aparaty – wymagania dla wszystkich aparatów VoIP”.
4.2. Obsługa nie mniej niż pięciu (5) linii (numerów) telefonicznych.
4.3. Nie mniej niż cztery (4) klawisze szybkiego wyboru z możliwością zaprogramowania funkcji BLF.
4.4. Kolorowy graficzny wyświetlacz o rozdzielczości nie mniejszej niż 800 x 480 pixeli.
4.5. Przy włączonym zasilaniu PoE pobór mocy nie może przekroczyć 25.5 W.
4.6. Możliwość rozbudowy telefonu o nie mniej niż pięćdziesiąt sześć (56) dodatkowych programowalnych klawiszy szybkiego wyboru obsługujących funkcję BLF (np. poprzez dołączenie dodatkowego modułu z klawiszami).

4.7. Zapewnia prowadzenie wideorozmowy z rozdzielczością pionową nie mniejszą niż 720p przy wykorzystaniu kodeka H.264 AVC
4.8. Wbudowana kamera z przesłoną zapewniającą prywatność użytkownikowi aparatu.

5. Aparat abonencki -99 szt. aparat VoIP wraz z licencjami spełniający poniższe wymagania /minimum techniczne/:

5.1. Spełnia wymagania opisane w punkcie 2 - ” Aparaty – wymagania dla wszystkich aparatów VoIP”.
5.2. Obsługa nie mniej niż czterech (4) linii (numerów) telefonicznych.
5.3. Nie mniej niż trzy (3) klawisze szybkiego wyboru z możliwością zaprogramowania funkcji BLF.
5.4. Monochromatyczny graficzny wyświetlacz o rozdzielczości nie mniejszej niż 390 x 160 pixeli.
5.5. Przy włączonym zasilaniu PoE pobór mocy nie może przekroczyć 3,84 W.

6. Licencje do klastra Cisco Unified Communication Manager wersja 12.5.1

Wykonawca dostarczy licencje Flex Named User Calling Enhanced (A-FLEX-NUPL-E) do klastra CUCM wersji 12.5.1 spełniające następujące warunki /minimum techniczne/:

6.1. Ilość licencji nie mniejsza niż wymagana do uruchomienia wszystkich dostarczonych aparatów VoIP
6.2. Dostarczone licencje muszą zapewnić migrację do wyższych wersji CUCM w okresie nie krótszym niż 3 lata od daty podpisania umowy.
6.3. Czas ważności licencji nie może być krótszy niż 3 lata od daty podpisania umowy.
6.4. Dostawca licencji przypisze je do domeny „policja.gov.pl”

CZĘŚĆ 2

Dostawa urządzeń sieciowych.

1. Wszystkie dostarczone przez Wykonawcę urządzenia:

1.1. Muszą być fabrycznie nowe. Nie dopuszcza się dostaw pochodzących z demontażu, używanych lub uprzednio naprawianych.
1.2. Urządzenia muszą być dostarczony przez Wykonawcę w oryginalnych opakowaniach producenta wraz z instrukcją obsługi w języku polskim lub angielskim (instrukcja może być w formie elektronicznej).
1.3. Nie mogą być starsze niż 6 miesięcy od daty dostawy.
1.4. Muszą pochodzić z autoryzowanego kanału dystrybucji producenta
1.5. Muszą być produktem przeznaczonym na rynek polski lub na rynek Unii Europejskiej
1.6. Muszą posiadać nie mniej niż 24 miesiące gwarancji producenta realizowanej na terenie Polski przez autoryzowany serwis.
1.7. Korzystanie przez Zamawiającego z zakupionych urządzeń i oprogramowania nie może naruszać majątkowych praw autorskich osób trzecich.
1.8. Zamawiający wymaga, by w chwili nabycia licencji stał się ich jedynym właścicielem z pełnymi prawami oraz pełnymi prawami do korzystania z oprogramowania.
1.9. Zamawiający posiada wiedzę na temat nadzoru i konfiguracji oraz używa w swojej infrastrukturze VoIP produktów marki Cisco. W związku z tym dostarczony sprzęt musi być w pełni kompatybilny z urządzeniami posiadanymi przez Zamawiającego oraz dawać

możliwość wykorzystywania wszystkich funkcjonalności posiadanego przez Zamawiającego oraz dostarczonego przez Wykonawcę sprzętu

1.10. W przypadku zaoferowania innych produktów niż posiada Zamawiający, Wykonawca będzie zobowiązany do:
   1.10.1. zainstalowania i uruchomienia urządzenia,
   1.10.2. w przypadku urządzeń zarządzalnych dostarczenia kompletu oprogramowania i okablowania do konfiguracji,
   1.10.3. przeszkolenia 4 administratorów w zakresie konfiguracji i zarządzania urządzeniami. (szkolenie powinno zapewnić poziom wiedzy pozwalający na wykorzystanie wszystkich funkcjonalności dostarczonych urządzeń).

2. Switch dostępowy z POE – 1 szt. przełącznik sieciowy spełniający poniższe wymagania /minimum techniczne/:

2.1. Zasilanie POE standardu IEEE 802.3af (15.4W na port) dostępne na wszystkich portach jednocześnie oraz IEEE 802.3at (30W na port) dostępne jednocześnie na co najmniej połowie dostępnych portów Ethernet.
2.2. Możliwość dostarczenia zasilania PoE w standardzie IEEE 802.3at (30W na port) jednocześnie na wszystkie porty Ethernet (np. poprzez instalację dodatkowego zasilacza)
2.3. Możliwość zastosowania zasilania redundantnego.
2.4. Zabezpieczenie przed podaniem napięcia zasilającego do urządzenia końcowego, które nie wspiera standardu PoE.
2.5. Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP, tunelowania 802.1Q (QinQ).
2.6. Obsługa minimum 255 aktywnych VLAN-ów o numerach od 1 do 4094.
2.7. Obsługa minimum 255 interfejsów SVI L3
2.8. Przełączanie pakietów L3 (64 bajty) – minimum 40 Mpps
2.9. Tablice o pojemności nie mniejszej niż:
   2.9.1. MAC - 16000 adresów
   2.9.2. IPv4 - 3000 tras
   2.9.3. IPv6 - 1500 tras
   2.9.4. security ACL - 1000 wpisów
   2.9.5. QOS ACL - 1000 wpisów.
2.10. Przepustowość przełącznika (switching capacity) nie mniejsza niż 56Gb/s.
2.11. Zaimplementowane mechanizmy Quality Of Service (QOS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
2.12. Zdalne wykonywanie zmian konfiguracyjnych oraz nadzoru.
2.13. Obsługa IPV4 i IPV6.
2.14. W pełni nieblokowalna matryca przełączająca.
2.15. Zasilanie ze źródła prądu zmiennego 230V.
2.16. Dwadzieścia cztery (24) porty Ethernet 10/100/1000Base-T.
2.17. Nie mniej niż cztery (4) gniazda do podłączenia modułów światłowodowych SFP o przepływności nie mniejszej niż 1Gb/s,
2.18. Obsługa agregacji łączy w standardzie IEEE 802.3ad (LACP):
2.19. Osługą ramek „jumbo” o wielkości nie mniejszej niż 9 tysięcy bajtów.
2.20. Obsługa ruchu multicast z wykorzystaniem IGMP v1, v2, v3 oraz MLD v1 i v2.
2.21. Obsługa protokołu NTP.
2.22. Powinno być zapewnione wsparcie następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
   2.22.1. obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu,
   2.22.2. obsługa co najmniej jednej kolejki ze statusem priorytetowym (bezwzględne pierwszeństwo obsługi),
   2.22.3. przyporządkowanie ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie źródłowego lub docelowego adresu MAC, IP, portu TCP
   2.22.4. ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 10 kbps,
   2.22.5. kontrola sztormów dla ruchu broadcast, multicast oraz unicast,

2.22.6. mechanizm zmiany wartości pól CoS (protokołu IEEE 802.1p) i DSCP (protokołu IP)
2.23. Zdalne zarządzanie poprzez protokoły SNMPv3 i SSH v2.
2.24. Przekazywanie danych o ruchu w sieci przy wykorzystaniu SNMPv2, v3 oraz NetFlow.
2.25. Zapis komunikatów systemowych na serwerze Syslog.
2.26. Wbudowane mechanizmy zapewniające przekazywanie kopii całego ruchu z każdego portu/portów na dowolny wskazany port dowolnego przełącznika pracującego w tej samej sieci (SPAN, RSPAN).
2.27. Montaż w szafie 19" (Wykonawca dostarczy komplet akcesoriów montażowych).
2.28. Obsługa protokołów zapobiegających powstawaniu pętli: STP (IEEE 802.1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), PVRST+ (Per-VLAN Rapid Spanning Tree).
2.29. Obsługa protokołu Unidirectional Link Detection (UDLD) kompatybilnego z posiadanym przez Zamawiającego sprzętem Cisco
2.30. Definiowanie VLAN-u dla połączeń głosowych i wideo, używanego do automatycznej konfiguracji telefonu IP (poprzez CDP) i usług QOS.
2.31. Zaimplementowane mechanizmy związane z bezpieczeństwem sieci:
2.31.1. tworzenie nie mniej niż 30 kont lokalnych administratorów urządzenia
2.31.2. wiele poziomów dostępu administracyjnego (privilege-level),
2.31.3. uwierzytelnianie i autoryzacja za pośrednictwem protokołów RADIUS lub TACACS+ dla kont administratorów urządzenia
2.31.4. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
2.31.5. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
2.31.6. obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
2.31.7. uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
2.31.8. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
2.31.9. uwierzytelnianie wielu użytkowników na jednym porcie
2.31.10. jednoczesne uwierzytelnianie na porcie telefonu IP i komputera PC podłączonego za telefonem,
2.31.11. obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176,
2.31.12. możliwość wyboru kolejności uwierzytelniania – 802.1X/ uwierzytelnianie w oparciu o MAC adres/ uwierzytelnianie oparciu o portal www,
2.31.13. zabezpieczenie portu przed podłączeniem nieautoryzowanych urządzeń, rozpoznawanych za pomocą adresu MAC, osobno dla VLAN-u głosowego (Voice) i VLAN-u dla danych (Port security)
2.31.14. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego serwera DHCP (DHCP Snooping) lub DHCPv6 (DHCPv6 Guard)
2.31.15. zabezpieczenie przed zafałszowaniem tablicy MAC przełącznika (Dynamic ARP Inspection)
2.31.16. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego urządzenia, posiadającego prawidłowy adres IP (IP Source Guard),
2.31.17. zabezpieczenie przed rozgłaszaniem fałszywych komunikatów IPv6 Router Advertisement (RA Guard),
2.31.18. Obsługa list kontroli dostępu (ACL) następujących typów:
2.31.18.1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów przełącznika,
2.31.18.2. ·VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
2.31.18.3. ·Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
2.31.18.4. czasowe listy ACL (aktywne w określonych godzinach i dniach tygodnia);

2.31.19. ·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),

2.31.20. ·wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),

2.32. Wbudowany serwer DHCP.

2.33. Wbudowany klient DHCP.

2.34. Obsługa protokołu CDP (Cisco Discovery Protocol).

2.35. Obsługa protokołu LLDP-MED.

2.36. Routing statyczny.

2.37. Reflektometryczny test okablowania na każdym porcie Ethernet 10/100/1000Base-T, umożliwiający odczyt odległości od switcha w jakiej występuje uszkodzenie kabla.

2.38. Przełącznik musi umożliwiać stworzenie stosu przełączników (min. 8), w którym wszystkie przełączniki będą się zachowywały jak jedna logiczna jednostka. Funkcjonalność ta może zostać uzyskana poprzez zastosowanie dodatkowego modułu (dostarczenie takowego nie jest wymagane w tym postępowaniu).

2.39. Po połączeniu przełączników w stos muszą być zapewnione następujące parametry:

2.39.1. przepustowość przełączników (switching capacity) w ramach stosu nie mniejsza niż 136 Gb/s

2.39.2. obsługa agregacji łączy w standardzie IEEE 802.3ad (LACP) dla portów należących do różnych switchy w stosie (cross-stack link aggregation)

2.39.3. obsługa nie mniej niż 48 zagregowanych połączeń LACP

2.39.4. obsługa nie mniej niż 16 linków w ramach zagregowanego połączenia

2.39.5. przepustowość interfejsu stakującego nie mniejsza niż 80Gb/s.

2.40. Zamawiający posiada przełączniki Cisco C9200L-24P-4G-E, zaoferowane przełączniki muszą umożliwić podłączenie nowych urządzeń w stos z posiadanymi przełącznikami oraz zarządzanie wszystkimi urządzeniami w stosie jak jednym.

3. Switch dostępowy z POE – 9 szt. przełącznik stakowalny wraz z kablami stakującymi spełniający poniższe wymagania /minimum techniczne/:

3.1. Zasilanie POE standardu IEEE 802.3af (15.4W na port) dostępne na wszystkich portach jednocześnie oraz IEEE 802.3at (30W na port) dostępne jednocześnie na co najmniej połowie dostępnych portów Ethernet.

3.2. Możliwość dostarczenia zasilania PoE w standardzie IEEE 802.3at (30W na port) jednocześnie na wszystkie porty Ethernet (np. poprzez instalację dodatkowego zasilacza)

3.3. Możliwość zastosowania zasilania redundantnego.

3.4. Zabezpieczenie przed podaniem napięcia zasilającego do urządzenia końcowego, które nie wspiera standardu PoE.

3.5. Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP, tunelowania 802.1Q (QinQ).

3.6. Obsługa minimum 255 aktywnych VLAN-ów o numerach od 1 do 4094.

3.7. Obsługa minimum 255 interfejsów SVI L3

3.8. Przełączanie pakietów L3 (64 bajty) – minimum 40 Mpps

3.9. Tablice o pojemności nie mniejszej niż:

3.9.1. MAC - 16000 adresów

3.9.2. IPv4 - 3000 tras

3.9.3. IPv6 - 1500 tras

3.9.4. security ACL - 1000 wpisów

3.9.5. QOS ACL - 1000 wpisów.

3.10. Przepustowość przełącznika (switching capacity) nie mniejsza niż 56Gb/s.

3.11. Zaimplementowane mechanizmy Quality Of Service (QOS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).

3.12. Zdalne wykonywanie zmian konfiguracyjnych oraz nadzoru.

3.13. Obsługa IPV4 i IPV6.

3.14. W pełni nieblokowalna matryca przełączająca.

3.15. Zasilanie ze źródła prądu zmiennego 230V.
3.16. Dwadzieścia cztery (24) porty Ethernet 10/100/1000Base-T.
3.17. Nie mniej niż cztery (4) gniazda do podłączenia modułów światłowodowych SFP o przepływności nie mniejszej niż 1Gb/s,
3.18. Obsługa agregacji łączy w standardzie IEEE 802.3ad (LACP):
3.19. Osługą ramek „jumbo" o wielkości nie mniejszej niż 9 tysięcy bajtów.
3.20. Obsługa ruchu multicast z wykorzystaniem IGMP v1, v2, v3 oraz MLD v1 i v2.
3.21. Obsługa protokołu NTP.
3.22. Powinno być zapewnione wsparcie następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
  3.22.1. obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu,
  3.22.2. obsługa co najmniej jednej kolejki ze statusem priorytetowym (bezwzględne pierwszeństwo obsługi),
  3.22.3. przyporządkowanie ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie źródłowego lub docelowego adresu MAC, IP, portu TCP
  3.22.4. ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 10 kbps,
  3.22.5. kontrola sztormów dla ruchu broadcast, multicast oraz unicast,
  3.22.6. mechanizm zmiany wartości pól CoS (protokołu IEEE 802.1p) i DSCP (protokołu IP)
3.23. Zdalne zarządzanie poprzez protokoły SNMPv3 i SSH v2.,
3.24. Przekazywanie danych o ruchu w sieci przy wykorzystaniu SNMPv2, v3 oraz NetFlow.
3.25. Zapis komunikatów systemowych na serwerze Syslog.
3.26. Wbudowane mechanizmy zapewniające przekazywanie kopii całego ruchu z każdego portu/portów na dowolny wskazany port dowolnego przełącznika pracującego w tej samej sieci (SPAN, RSPAN).
3.27. Montaż w szafie 19" (Wykonawca dostarczy komplet akcesoriów montażowych).
3.28. Obsługa protokołów zapobiegających powstawaniu pętli: STP (IEEE 802.1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), PVRST+ (Per-VLAN Rapid Spanning Tree).
3.29. Obsługa protokołu Unidirectional Link Detection (UDLD) kompatybilnego z posiadanym przez Zamawiającego sprzętem Cisco
3.30. Definiowanie VLAN-u dla połączeń głosowych i wideo, używanego do automatycznej konfiguracji telefonu IP (poprzez CDP) i usług QOS.
3.31. Zaimplementowane mechanizmy związane z bezpieczeństwem sieci:
  3.31.1. tworzenie nie mniej niż 30 kont lokalnych administratorów urządzenia
  3.31.2. wiele poziomów dostępu administracyjnego (privilege-level),
  3.31.3. uwierzytelnianie i autoryzacja za pośrednictwem protokołów RADIUS lub TACACS+ dla kont administratorów urządzenia
  3.31.4. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  3.31.5. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
  3.31.6. obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  3.31.7. uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
  3.31.8. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  3.31.9. uwierzytelnianie wielu użytkowników na jednym porcie
  3.31.10. jednoczesne uwierzytelnianie na porcie telefonu IP i komputera PC podłączonego za telefonem,
  3.31.11. obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  3.31.12. możliwość wyboru kolejności uwierzytelniania – 802.1X/ uwierzytelnianie w oparciu o MAC adres/ uwierzytelnianie oparciu o portal www,
  3.31.13. zabezpieczenie portu przed podłączeniem nieautoryzowanych urządzeń, rozpoznawanych za pomocą adresu MAC, osobno dla VLAN-u głosowego (Voice) i VLAN-u dla danych (Port security)

3.31.14. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego serwera DHCP (DHCP Snooping) lub DHCPv6 (DHCPv6 Guard)
3.31.15. zabezpieczenie przed zafałszowaniem tablicy MAC przełącznika (Dynamic ARP Inspection)
3.31.16. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego urządzenia, posiadającego prawidłowy adres IP (IP Source Guard),
3.31.17. zabezpieczenie przed rozgłaszaniem fałszywych komunikatów IPv6 Router Advertisement (RA Guard),
3.31.18. obsługa list kontroli dostępu (ACL) następujących typów:
3.31.18.1. port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów przełącznika,
3.31.18.2. ·VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
3.31.18.3. ·routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
3.31.18.4. czasowe listy ACL (aktywne w określonych godzinach i dniach tygodnia);
3.31.19. ·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),
3.31.20. ·wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
3.32. Wbudowany serwer DHCP.
3.33. Wbudowany klient DHCP.
3.34. Obsługa protokołu CDP (Cisco Discovery Protocol).
3.35. Obsługa protokołu LLDP-MED.
3.36. Routing statyczny.
3.37. Reflektometryczny test okablowania na każdym porcie Ethernet 10/100/1000Base-T, umożliwiający odczyt odległości od switcha w jakiej występuje uszkodzenie kabla.
3.38. Przełącznik musi zapewnić stworzenie stosu przełączników (min. 8), w którym wszystkie przełączniki będą się zachowywały jak jedna logiczna jednostka..
3.39. Po połączeniu przełączników w stos muszą być zapewnione następujące parametry:
3.39.1. przepustowość przełączników (switching capacity) w ramach stosu nie mniejsza niż 136 Gb/s
3.39.2. obsługa agregacji łączy w standardzie IEEE 802.3ad (LACP) dla portów należących do różnych switchy w stosie (cross-stack link aggregation)
3.39.3. obsługa nie mniej niż 48 zagregowanych połączeń LACP
3.39.4. obsługa nie mniej niż 16 linków w ramach zagregowanego połączenia
3.39.5. przepustowość interfejsu stakującego nie mniejsza niż 80Gb/s.
3.40. Zamawiający posiada przełączniki Cisco C9200L-24P-4G-E. Zaoferowane przełączniki muszą umożliwić podłączenie nowych urządzeń w stos z posiadanymi przełącznikami oraz zarządzanie wszystkimi urządzeniami w stosie jak jednym.
3.41. Wykonawca dostarczy odpowiednie kable stakujące. Switche muszą zostać połączone w stosy przy użyciu kabli stakujących o długości nie mniejszej niż:
3.41.1. 50 cm - 9szt
3.41.2. 300 cm - 4 szt.

4. Switche dystrybucyjnye 1 kpl. – zestaw spełniający poniższe wymagania /minimum techniczne/:

4.1. Wymagany zestaw przełączników połączonych w stos.
4.2. Kable łączące przełączniki w stos powinny zapewnić montaż switchy w odległości nie mniejszej niż 1,5 m pomiędzy najdalszymi urządzeniami. Odpowiednie kable stakujące dostarczy Wykonawca.
4.3. Przełącznik musi umożliwiać stworzenie stosu nie mniej niż ośmiu (8) przełączników, w którym wszystkie przełączniki będą się zachowywały jak jedna logiczna jednostka.

Funkcjonalność ta może zostać uzyskana poprzez zastosowanie dodatkowych modułów.

4.4. Redundancja jednostek sterujących zapewniająca bezprzerwową pracę zestawu po awarii jednej z nich. Awaria jednostki sterującej w switchu pracującym w stosie nie może powodować przerwy w działaniu portów tego switcha.
4.5. Redundancja zasilania pozwalająca na pracę urządzenia bez utraty funkcjonalności po awarii jednego z zasilaczy.
4.6. Zestaw powinien zapewniać dzielenie mocy zasilaczy pomiędzy nie mniej niż czterema przełącznikami połączonymi w stos.
4.7. Wymiana kart liniowych, zasilaczy, wentylatorów musi się odbywać bez zatrzymywania urządzenia (Hot Swap).
4.8. Wymiana switcha w stosie nie może powodować zakłóceń w pracy pozostałych przełączników.
4.9. Wgrywanie poprawek oprogramowania bez konieczności restartu platformy.
4.10. Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP, tunelowania 802.1Q (QinQ).
4.11. Agregacja łączy w standardzie IEEE 802.3ad (LACP) zapewniająca:
  4.11.1. agregację portów należących do różnych switchy w stosie (Cross-Stack Link Aggregation)
  4.11.2. obsługę nie mniej niż 128 zagregowanych połączeń LACP
  4.11.3. obsługę nie mniej niż 16 linków w ramach zagregowanego połączenia
4.12. Obsługa nie mniej niż tysiąca (1000) aktywnych VLAN-ów o numerach od 1 do 4094.
4.13. Obsługa nie mniej niż tysiąca (1000) SVI L3 (Switched Virtual Interface)
4.14. Szybkość przełączania pakietów L3 (64 bajty) nie mniejsza niż:
  4.14.1. 154 Mpps na pojedynczym switchu,
  4.14.2. 511 Mpps na stosie switchy.
4.15. Tablice o pojemności nie mniejszej niż:
  4.15.1. MAC - 32000 adresów,
  4.15.2. IPv4 - 8000 tras,
  4.15.3. IPv6 - 4000 tras,
  4.15.4. Multicast - 8000 tras,
  4.15.5. Security ACL - 5000 wpisów,
  4.15.6. QOS ACL- 5000 wpisów.
4.16. Przepustowość przełączników (switching capacity) nie mniejsza niż
  4.16.1. 208 Gb/s dla pojedynczego switcha,
  4.16.2. 688 Gb/s dla stosu switchy
4.17. Przepustowość interfejsu stakującego nie mniejsza niż 480 Gb/s
4.18. Zaimplementowane mechanizmy Quality of Service (QoS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
4.19. Zdalne wykonywanie zmian konfiguracyjnych oraz nadzoru.
4.20. Obsługa IPv4 i IPv6.
4.21. W pełni nieblokowalna matryca przełączająca.
4.22. Zasilanie ze źródła prądu zmiennego 230V.
4.23. Nie mniej niż dwa switche połączone w stos. Każdy switch musi posiadać dwadzieścia cztery (24) porty SFP, o przepływności nie mniejszej niż 1Gb/s, oraz nie mniej niż 8 portów SFP+ o przepływności nie mniejszej niż10 Gb/s.
4.24. Każdy switch musi umożliwiać podłączenie nie mniej niż dwóch jednakowych wkładek w jednym z poniższych formatów:
  4.24.1. SFP 1Gb/s,
  4.24.2. SFP+ (10Gb/s),
  4.24.3. SFP28 (25Gb/s)
  4.24.4. QSFP (40Gb/s)
4.25. Możliwość rozbudowy zestawu o dwa switche zawierające nie mniej niż dwadzieścia cztery (24) gniazda Ethernet 10/100/1000Base-T każdy,
4.26. Wszystkie z zasilaniem PoE standardu IEEE 802.3af (15.4W na port) dostępne na wszystkich portach jednocześnie oraz IEEE 802.3at (30W na port) dostępne jednocześnie na co najmniej połowie dostępnych portów Ethernet.
4.27. Obsługą ramek „jumbo” o wielkości nie mniejszej niż 9 tysięcy bajtów.
4.28. Obsługa ruchu multicast z wykorzystaniem IGMP v1, v2, v3 oraz MLD v1 i v2.

4.29. Obsługa protokołu NTP
4.30. Powinno być zapewnione wsparcie następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
  4.30.1. obsługa co najmniej czterech kolejek sprzętowych dla różnego rodzaju ruchu,
  4.30.2. obsługa co najmniej jednej kolejki ze statusem priorytetowym (bezwzględne pierwszeństwo obsługi),
  4.30.3. przyporządkowanie ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie źródłowego lub docelowego adresu MAC, IP, portu TCP
  4.30.4. ograniczanie pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 10 kbps,
  4.30.5. kontrola sztormów dla ruchu broadcast, multicast oraz unicast,
  4.30.6. mechanizm zmiany wartości pól CoS (protokołu IEEE 802.1p) i DSCP (protokołu IP
4.31. Zdalne zarządzanie poprzez protokoły SNMPv3 i SSH v2.
4.32. Przekazywanie danych o ruchu w sieci przy wykorzystaniu SNMPv2, v3 oraz NetFlow.
4.33. Zapis komunikatów systemowych na serwerze Syslog.
4.34. Wbudowane mechanizmy zapewniające przekazywanie kopii całego ruchu z każdego portu/portów na dowolny wskazany port dowolnego przełącznika pracującego w tej samej sieci (SPAN, RSPAN).
4.35. Montaż w szafie 19” (Wykonawca dostarczy komplet akcesoriów montażowych).
4.36. Obsługa protokołów zapobiegających powstawaniu pętli: STP (IEEE 802.1d), RSTP (IEEE 802.1w), MSTP (IEEE 802.1s), PVRST+ (Per-VLAN Rapid Spanning Tree).
4.37. Obsługa protokołu Unidirectional Link Detection (UDLD) kompatybilnego z posiadanym przez Zamawiającego sprzętem Cisco
4.38. Definiowanie VLAN-u dla połączeń głosowych i wideo, używanego do automatycznej konfiguracji telefonu IP (poprzez CDP) i usług QOS.
4.39. Zaimplementowane mechanizmy związane z bezpieczeństwem sieci:
  4.39.1. tworzenie nie mniej niż 30 kont lokalnych administratorów urządzenia
  4.39.2. wiele poziomów dostępu administracyjnego (privilege-level),
  4.39.3. uwierzytelnianie i autoryzacja za pośrednictwem protokołów RADIUS lub TACACS+ dla kont administratorów urządzenia
  4.39.4. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  4.39.5. autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
  4.39.6. obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  4.39.7. uwierzytelnianie urządzeń na porcie w oparciu o adres MAC,
  4.39.8. możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  4.39.9. uwierzytelnianie wielu użytkowników na jednym porcie
  4.39.10. jednoczesne uwierzytelnianie na porcie telefonu IP i komputera PC podłączonego za telefonem,
  4.39.11. obsługa żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  4.39.12. możliwość wyboru kolejności uwierzytelniania – 802.1X/ uwierzytelnianie w oparciu o MAC adres/ uwierzytelnianie oparciu o portal www,
  4.39.13. zabezpieczenie portu przed podłączeniem nieautoryzowanych urządzeń, rozpoznawanych za pomocą adresu MAC, osobno dla VLAN-u głosowego (Voice) i VLAN-u dla danych (Port security)
  4.39.14. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego serwera DHCP (DHCP Snooping) lub DHCPv6 (DHCPv6 Guard)
  4.39.15. zabezpieczenie przed zafałszowaniem tablicy MAC przełącznika (Dynamic ARP Inspection)
  4.39.16. zabezpieczenie przed podłączeniem do sieci nieautoryzowanego urządzenia, posiadającego prawidłowy adres IP (IP Source Guard),
  4.39.17. zabezpieczenie przed rozgłaszaniem fałszywych komunikatów IPv6 Router Advertisement (RA Guard).

4.39.18. obsługa list kontroli dostępu (ACL) następujących typów:
4.39.18.1. port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów przełącznika,
4.39.18.2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
4.39.18.3. pouted ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
4.39.18.4. czasowe listy ACL (aktywne w określonych godzinach i dniach tygodnia);
4.39.19. ·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),
4.39.20. ·wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (Control Plane Policing),
4.40. Wbudowany serwer DHCP.
4.41. Wbudowany klient DHCP.
4.42. Obsługa protokołu CDP (Cisco Discovery Protocol).
4.43. Obsługa protokołu LLDP-MED.
4.44. Routing statyczny.
4.45. Routing dynamiczny oparty na protokołach: OSPF, EIGRP, BGP, IS-IS.
4.46. Routing multicast.PIM-SM
4.47. Routing w oparciu o zasady (Policy Based Routing).
4.48. Tworzenie tuneli GRE.
4.49. Funkcja Virtual Routing and Forvarding (VRF) lub analogiczna pozwalająca na utworzenie nie mniej niż dwustu pięćdziesięciu (250) sieci wirtualnych L3 o nakładającej się adresacji IP.
4.50. Segmentacja sieci przy użyciu protokołów MPLS, VXLAN.
4.51. Obsługa nie mniej niż czterystu (400) routowanych portów (routed ports).
4.52. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii w sieci dla potrzeb protokołów routingu
4.53. Reflektometryczny test okablowania na każdym porcie Ethernet 10/100/1000Base-T, umożliwiający odczyt odległości od switcha w jakiej występuje uszkodzenie kabla.
4.54. Wykonawca wyposaży switche w 38 szt. modułów SFP spełniających poniższe kryteria:
4.54.1. Wymagana współpraca z urządzeniami Cisco Zamawiającego oraz ze switchami dostarczonymi przez Wykonawcę.
4.54.2. Wymagana praca ze światłowodem jednomodowym 9/125um.
4.54.3. Transmisja danych po dwóch włóknach światłowodowych na odległość nie mniejszą niż 20 km.
4.54.4. Złącze Duplex LC/PC.
4.54.5. Prędkość transmisji danych 1Gb/s
4.55. Wykonawca wyposaży switch w 16 szt. modułów SFP 10/100/1000Base-T spełniających poniższe kryteria:
4.55.1. Wymagana współpraca z urządzeniami Cisco Zamawiającego oraz ze switchami dostarczonymi przez Wykonawcę.
4.55.2. Wymagana praca z kablem UTP na odległość nie mniejszą niż 100m.
4.55.3. Złącze Ethernet RJ-45 10/100/1000Base-T.
4.56. Wykonawca dołączy do przełącznika patchcordy światłowodowe jednomodowe 9/125um o długości 3 m:
4.56.1. SC/APC LC/PC - 10 szt.
4.56.2. LC/PC - 10 szt.

CZĘŚĆ 3

1. Przełącznik sieciowy zarządzalny typ1 wraz z dodatkowym wyposażeniem – 12 szt.

L.p.	Nazwa	Wymagania minimalne
1.	Typ	Przełącznik sieciowy zarządzalny
2.	Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 28. Porty na moduły światłowodowe SFP (IEEE 802.3z) z możliwością instalacji modułów 1000Base-SX/LX/LH/ZX - liczba portów co najmniej 4. Dopuszcza się, aby porty SFP były dzielone z portami 1000Base-T. Porty SFP powinny umożliwiać obsługę również modułów SFP 100Base-FX (IEEE 802.3u). Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Urządzenie powinno być zasilane napięciem AC 230V. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 56 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 41 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji). Pojemność tablicy MAC powinna wynosić nie mniej, niż 8000 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 250 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 128 MB. Pamięć Flash - nie mniej niż 32 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 10000 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 0,5 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -5 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 50 stopni Celsjusza. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 990000 godzin.
3.	Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 2, 3 (awareness) oraz obsługiwać nie mniej, niż 250 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 250 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s (co najmniej 32 instancji). Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej.

		Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 8 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy.
4.	Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 256 jednocześnie skonfigurowanych takich sieci. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
5.	Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 4 takich interfejsów. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 4 takich interfejsów. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 120 takich tras) oraz dla IPv6 (co najmniej 50 tras). Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.
6.	Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.
7.	Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.
8.	Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 60 takich adresów MAC na pojedynczym porcie fizycznym. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 120 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 16 Kbps), Multicast (z krokiem minimalnym co

		najwyżej 16 Kbps), Broadcast (z krokiem minimalnym co najwyżej 16 Kbps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.
9.	Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON. Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
10.	Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.
11.	Gwarancja	Czas trwania zgodnie ze złożoną ofertą (minimum 36 miesięcy).
12.	Wymagania dodatkowe	Wszystkie egzemplarze zaoferowanego urządzenia muszą być fabrycznie nowe oraz jednolite w ramach całej dostawy. Zamawiający wymaga dostarczenia wszystkich egzemplarzy zaoferowanego urządzenia w nienaruszonych opakowaniach fabrycznych Producenta. Wszystkie egzemplarze zaoferowanego urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży Producenta oraz być objęte minimum 5-letnią gwarancją Producenta obejmującą w okresie gwarancji dedykowaną opiekę techniczną Producenta, zawierającą: - wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez Producenta; - dostęp do wszystkich nowych wersji oprogramowania oferowanych przez Producenta; - dostęp do baz wiedzy Producenta i przewodników konfiguracyjnych;

		- wsparcie Producenta przy rozwiązywaniu problemów związanych z działaniem oprogramowania; - w razie awarii bezpłatną wymianę urządzenia przez Producenta lub wysyłkę sprzętu zastępczego w następnym dniu roboczym od zgłoszenia. Zamawiający przy odbiorze sprzętu zastrzega sobie prawo do weryfikacji spełnienia w/w wymagań bezpośrednio u Producenta.
13.	**Wyposażenie dodatkowe**	**Dla każdego egzemplarza urządzenia musi zostać dostarczone minimum:** - 25 szt. patchcordów UTP RJ-45 kat. 6 o długości 1,5 metra - kolor szary; - 25 szt. patchcordów UTP RJ-45 kat. 6 o długości 3,0 metra - kolor szary; - 1 szt. wkładka SFP 1000BaseLX (LC Duplex) - dedykowane do oferowanego modelu urządzenia; **Dodatkowe wyposażenie musi współpracować z przełącznikami sieciowymi dostarczonymi przez Wykonawcę.**

2. Przełącznik sieciowy zarządzalny typ2 wraz z dodatkowym wyposażeniem – 3 szt.

L.p.	Nazwa	Wymagania minimalne
1.	Typ	Przełącznik sieciowy zarządzalny
2.	Charakterystyka sprzętowa	Porty 1000Base-T (IEEE 802.3/802.3u/802.3ab) - liczba portów co najmniej 4. Porty na moduły światłowodowe SFP (IEEE 802.3z) z możliwością instalacji modułów 1000Base-SX/LX/LH/ZX - liczba portów co najmniej 24. Dopuszcza się, aby porty SFP były dzielone z portami 1000Base-T. Porty SFP powinny umożliwiać obsługę również modułów SFP 100Base-FX (IEEE 802.3u). Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X). Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu. Sprzęt powinien umożliwiać zainstalowanie co najmniej 4 modułów dla połączeń 10Gb/s (IEEE 802.3ae). Przełącznik powinien obsługiwać również moduły gigabitowe SFP obsadzane w zatokach SFP+. Sprzęt powinien być wyposażony w konsolę szeregową w standardzie RS-232 w celu umożliwienia zarządzania lokalnego oraz dedykowany port Ethernet do zarządzania Out-of-Band, a także w port umożliwiający podłączenie zewnętrznych czujników zdarzeń, których wyzwolenie spowoduje wysłanie powiadomienia SNMP i port umożliwiający podłączenie zewnętrznego elementu wykonawczego wyzwalanego po wystąpieniu alarmu. Urządzenie powinno umożliwiać łączenie w stosy o wielkości co najmniej 9 jednostek. Stos powinien być wyposażony w funkcjonalność zapewniającą, że w przypadku awarii głównego przełącznika stosu, praca stosu nie zostanie zakłócona, w szczególności nie nastąpi ponowne uruchomienie stosu. Protokół stackujący powinien, w przypadku pracy w topologii pierścienia, zapewniać przesyłanie ruchu pomiędzy przełącznikami krótszą drogą. Przepustowość magistrali stosu powinna wynosić co najmniej 80 Gb/s. Stos powinien umożliwiać agregację połączeń oraz kopiowanie ruchu przy użyciu dowolnych portów w stosie. Urządzenie powinno być zasilane napięciem AC 230V. Musi istnieć możliwość użycia dodatkowego zasilacza nadmiarowego. Magistrala przełączająca powinna posiadać wydajność nie mniejszą, niż 128 Gb/s. Wydajność przełączania dla pakietów 64B powinna wynosić nie mniej niż 95 Mp/s. Urządzenie musi posiadać architekturę nieblokującą (zapewniać przełączanie wire-speed - z pełną prędkością na wszystkich portach w maksymalnej konfiguracji).

		Pojemność tablicy MAC powinna wynosić nie mniej, niż 69000 adresów MAC. Powinna też istnieć możliwość wprowadzenia co najmniej 1020 wpisów statycznych. Dostępna pamięć RAM powinna wynosić nie mniej, niż 1024 MB. Pamięć Flash - nie mniej niż 1024 MB. Urządzenie powinno obsługiwać ramki typu Jumbo o rozmiarze co najmniej 12280 B. Bufor pamięci zarezerwowanej na przetwarzane pakiety powinien wynosić nie mniej, niż 4 MB. Minimalna temperatura pracy dla urządzenia nie powinna być większa, niż -5 stopni Celsjusza. Maksymalna temperatura pracy dla urządzenia nie powinna być mniejsza, niż 50 stopni Celsjusza. Przełącznik powinien posiadać ochronę przeciwprzepięciową na portach miedzianych co najmniej do 6 kV. Urządzenie powinno charakteryzować się średnim czasem pomiędzy awariami wynoszącym co najmniej 280000 godzin.
3.	Funkcjonalności warstwy 2	Urządzenie powinno posiadać funkcjonalność IGMP Snooping w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 8190 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Urządzenie powinno posiadać także funkcjonalność MLD Snooping w wersji co najmniej 2 oraz obsługiwać nie mniej, niż 4090 grup multicast w tym możliwość utworzenia co najmniej 64 grup statycznych. Powinna istnieć możliwość uwierzytelnienia klienta przed dostarczeniem mu strumienia Multicast. Urządzenie powinno umożliwiać konfigurację filtrów dla protokołu IGMP ograniczających adresy IPv4 grup multicast do których poszczególni klienci mogą się przyłączać. Urządzenie powinno umożliwiać również konfigurację filtrów dla protokołu MLD ograniczających adresy grup IPv6 multicast do których poszczególni klienci mogą się przyłączać. Przełącznik powinien obsługiwać protokoły umożliwiające unikanie pętli w warstwie 2: IEEE 802.1D, 802.1w, 802.1s (co najmniej 64 instancji). Powinno także wspierać funkcjonalność 802.1Q Restricted Role oraz 802.1Q Restricted TCN. Dodatkowo, urządzenie powinno umożliwiać skonfigurowanie portu zapasowego, który zostanie aktywowany w przypadku awarii połączenia poprzez port podstawowy. Wymagana jest obecność funkcjonalności powodującej, że w przypadku gdy wystąpi pętla w części sieci nie objętej protokołami drzewa rozpinającego, część ta zostanie odłączona od reszty sieci aby zapobiec rozprzestrzenianiu się burzy broadcastowej. Urządzenie musi umożliwiać tworzenie połączeń Link Aggregation - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie oraz obsługiwać protokół LACP. Przełącznik musi mieć wbudowaną funkcjonalność LLDP (802.1AB) oraz LLDP-MED. Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą rozpinanie pętli w topologii pierścienia z opóźnieniem nie gorszym, niż 50ms. Funkcjonalność ta powinna być kompatybilna z zaleceniami ITU-T G.8032 w wersji co najmniej 2. Sprzęt powinien obsługiwać co najmniej 26 jednocześnie skonfigurowanych pierścieni. Urządzenie musi posiadać obsługę funkcjonalności DHCP Relay w tym opcji 60 i 61 oraz opcji 82, a także umożliwiać przechwytywanie zapytań DHCP od klienta i, po dodaniu opcji 82, przekazywanie ich do serwera DHCP znajdującego się w tej samej sieci VLAN, w której znajduje się klient. Obsługa DHCP Relay musi być możliwa również dla protokołu IPv6. Przełącznik powinien posiadać funkcjonalność kopiowania ruchu z jednego lub wielu portów na port monitorujący w celu umożliwienia jego analizy. Musi istnieć możliwość kopiowania tylko wybranego ruchu na danym porcie (np. tylko

		kierowanego do określonego adresu IP) oraz kopiowania ruchu na port monitorujący znajdujący się w innym przełączniku. Urządzenie powinno umożliwiać dostarczanie ruchu na wiele portów fizycznych na których obecne są te same adresy IP i MAC co pozwala na bezpośrednie przyłączenie klastrów serwerów posługujących się pojedynczym wirtualnym adresem IP i MAC. Urządzenie powinno umożliwiać tunelowanie ruchu kontrolnego L2, w tym protokołów GVRP i STP oraz protokołów CDP i VTP (01-00-0C-CC-CC-CC i 01-00-0C-CC-CC-CD).
4.	Obsługa sieci VLAN	Przełącznik powinien umożliwiać konfigurację sieci VLAN w standardzie 802.1Q, co najmniej 4094 jednocześnie skonfigurowanych takich sieci, w tym powinien umożliwiać obsługę VLAN zgodnie z protokołem 802.1v oraz obsługiwać dynamiczne przyłączanie do VLANu i pozwalać na tworzenie tzw. podwójnych VLANów. Parametry podwójnego tagowania powinny być konfigurowalne przez administratora. Powinna być też możliwość tworzenia specjalnych sieci VLAN dla przenoszenia ruchu typu multicast i rozdzielenia tak przenoszonego ruchu na klientów żądających przyłączenia do danej grupy multicast. Urządzenie powinno umożliwić utworzenie co najmniej 5 takich sieci VLAN. Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN. Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 3070 wpisów MAC dla takiej sieci VLAN. Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane. Przełącznik powinien obsługiwać także sieci VLAN oparte o podsieci IP - co najmniej 510 wpisów. Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.
5.	Funkcjonalności warstwy 3	Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 256 takich interfejsów. Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 256 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 256 takich interfejsów. Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika (urządzenie powinno umożliwić konfigurację co najmniej 8 instancji takiego interfejsu). Musi istnieć możliwość skonfigurowania interfejsu, który będzie odrzucać cały kierowany do niego ruch (interfejs Null). Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN. Przełącznik musi posiadać funkcjonalność Gratuitous ARP. Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci. Urządzenie musi posiadać również funkcjonalność umożliwiającą przekazywanie zapytań DNS do odpowiednich serwerów DNS w sieci (wewnętrznych lub zewnętrznych). Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 96 pule adresów IP oraz wspierającego protokół IPv6. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP. Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6.

		Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 32K wpisów oraz umożliwiać wprowadzenie co najmniej 512 wpisów statycznych. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 32760 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 16384 takich tras dla IPv6. Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 16380 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 7168 takich tras dla IPv6. Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 510 takich tras) oraz dla IPv6 (co najmniej 250 tras). Urządzenie musi umożliwiać tunelowanie ruchu IPv6 w IPv4 (ISATAP, 6to4). Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP). Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu. Urządzenie powinno wspierać także funkcję uRPF (Unicast Reverse Path Forwarding) kontrolującą, czy nadchodzący pakiet IP posiada adres źródłowy IP znajduje się w tablicy routingu. Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng. Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6.
6.	Quality of Service	Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6. Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu. W przypadku wykrycia ruchu iSCSI, urządzenie powinno również być w stanie obsługiwać ten ruch ze skonfigurowanym dla niego priorytetem, WRR, WDRR. Urządzenie powinno obsługiwać tzw. CIR z minimalną granulacją nie mniejszą, niż 64 kb/s. Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED, a także obsługiwać Flow Control zgodnie ze standardem 802.1Qbb. Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 64 kb/s. Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 8 kb/s.
7.	Filtrowanie ruchu	Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika. Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.

8.	Funkcje bezpieczeństwa	Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 12280 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie. Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony. Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika. Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL. Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników. Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta. Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6. Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN. Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania. Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP. Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6. Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.). Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS. Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP. Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany. Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU. Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service. Przełącznik powinien umożliwiać filtrowanie pakietów kontrolnych L3 (np. IGMP-Query, PIM, DVMRP) i nie dopuszczanie ich do wnętrza sieci. Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 2 pps), Multicast (z krokiem minimalnym co najwyżej 2 pps), Broadcast (z krokiem minimalnym co najwyżej 2 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie. Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.

9.	Zarządzanie	Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+. Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP. Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia. Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6. Urządzenie musi mieć wbudowaną funkcjonalność klienta SSHv2. W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3. Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6. Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow. Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731 - w tym pomiar opóźnienia (Delay Measurement) i strat (Loss Measurement) na badanej ścieżce. Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta. Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych. Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu. Urządzenie musi posiadać wbudowanego klienta DHCP i DHCPv6 oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia. Przełącznik powinien posiadać wbudowanego klienta SMTP. Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN. Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6 oraz musi wspierać protokół synchronizacji czasu zgodny z IEEE1588. Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6. Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci. Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego oraz wspierać traceroute dla IPv6. Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6. Lokalny interfejs WWW przełącznika powinien umożliwiać graficzne monitorowanie ruchu na portach fizycznych urządzenia, a także umożliwiać przeglądanie tablicy adresów MAC. Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia. Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia. Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC. Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.

		Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji. Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików. Powinna istnieć możliwość automatycznego ponownego uruchomienia urządzenia o określonym czasie lub w określonym horyzoncie czasowym. Przełącznik powinien wspierać zarządzanie przez zewnętrzny kontroler zgodnie ze standardem OpenFlow 1.3. Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet). Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.
10.	Pozostałe	Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.
11.	Gwarancja	Czas trwania zgodnie ze złożoną ofertą (minimum 36 miesięcy).
14.	Wymagania dodatkowe	Wszystkie egzemplarze zaoferowanego urządzenia muszą być fabrycznie nowe oraz jednolite w ramach całej dostawy. Zamawiający wymaga dostarczenia wszystkich egzemplarzy zaoferowanego urządzenia w nienaruszonych opakowaniach fabrycznych Producenta. Wszystkie egzemplarze zaoferowanego urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży Producenta oraz być objęte minimum 5-letnią gwarancją Producenta obejmującą w okresie gwarancji dedykowaną opiekę techniczną Producenta, zawierającą: - wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez Producenta; - dostęp do wszystkich nowych wersji oprogramowania oferowanych przez Producenta; - dostęp do baz wiedzy Producenta i przewodników konfiguracyjnych; - wsparcie Producenta przy rozwiązywaniu problemów związanych z działaniem oprogramowania; - w razie awarii bezpłatną wymianę urządzenia przez Producenta lub wysyłkę sprzętu zastępczego w następnym dniu roboczym od zgłoszenia. Zamawiający przy odbiorze sprzętu zastrzega sobie prawo do weryfikacji spełnienia w/w wymagań bezpośrednio u Producenta.
12.	**Wyposażenie dodatkowe**	**Dla każdego egzemplarza urządzenia musi zostać dostarczone minimum:** - 20 szt. patchcordów Patchord LC/PC-LC/PC SM duplex G.652D – długość 3,0m - 20 szt. patchcordów Patchord SC/APC-LC/PC SM duplex G.652D – długość 3,0m - 16 szt. wkładka SFP 1000BaseLX (LC Duplex) - dedykowane do oferowanego modelu urządzenia; - 4 szt. wkładka SFP+ 10GBase-LR Transceiver 10km (LC Duplex) - dedykowane do oferowanego modelu urządzenia; - 7 szt. wkładka SFP RJ45 10/100/1000 BASE-T - dedykowane do oferowanego modelu urządzenia; **Dodatkowe wyposażenie musi współpracować z przełącznikami sieciowymi dostarczonymi przez Wykonawcę.**