

Załącznik nr 5 do zapytania ofertowego pn. Dostawa – Infrastruktura sieciowa i komunikacyjna CBR

KARTA RÓWNOWAŻNOŚCI

Opis zakresu wymaganych parametrów dla zamówienia:

Dostawa – Infrastruktura sieciowa i komunikacyjna CBR

Zgodnie z zapisami Wytyczne w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014 – 2020 z dnia z dnia 19 lipca 2017 r. wszelkie projektowane urządzenia oraz rozwiązania materiałowe zdefiniowane w Dokumentacji Projektowej po nazwach własnych zostają w poniższym dokumencie opisane w zakresie wymaganych parametrów i jakości przez co dopuszcza się stosowanie rozwiązań równoważnych spełniających co najmniej niżej podane parametry.

Element	Specyfikacja	Ilość sztuk
Infrastruktura IT laboratoriów obliczeniowych		
Nazwa	Minimalny parametr	Ilość szt.
Główne szkieletowe przełączniki sieciowe	Funkcjonalność i wydajność co najmniej taka jak: Przełącznik modularny, kompatybilny lub lepszy niż Cisco model 9606R o minimalnych parametrach: • Modularny, obsługujący porty 1Gb, 10Gb, 40Gb oraz w opcji 100Gb, obsługujące zapasowy silniki tzw. supervisor, • 1 x kartę zarządzająco-przełączającą wyposażoną w port Ethernet RJ45/SFP/SFP+ służący do zarządzania urządzeniem (supervizor) • Minimum dodatkowy wolny slot do zainstalowania dodatkowej karty zarządzającej. • 2 x karta rozszerzeń 48x1/10/25Gb • Minimum dodatkowe 2 wolne sloty do zainstalowania kart rozszerzeń • dysk SSD min. 240GB	2

- minimum 16GB pamięci DRAM, 16GB pamięci FLASH oraz bufor pakietów 108MB
- 10 x wkładki SFP-10G-SR
- 2 zasilacze o mocy min. 2000W AC każdy
- Usługą serwisową producenta na okres 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego

Przełącznik szkieletowy - szt.2 (np. Cisco model 9606R) lub równoważny spełniający minimalne wymagania równoważności:

Parametry Ogólne

1. Urządzenie o architekturze modularnej – przynajmniej 6-słotowe (w tym minimum 4 sloty przeznaczone na moduły liniowe i 2 sloty na kart zarządzająco-przełączające)
2. Urządzenie musi mieć możliwość obsadzenia modułami liniowymi:
 - z minimum 48 portami 1GE/10GE/25GE SFP/SFP+; lub
 - z minimum 24-portami 40GE (QSFP) lub minimum 12-portami 100GE (QSFP);
3. Porty w modułach muszą mieć możliwość obsługi obsadzonych modułów z następującymi rodzajami wkładek (wymagania minimalne):
 - Porty SFP/SFP+:
10GBase-SR, 10GBase-LR

Kable twinax10G, 25GBASE-SR, kable twinax 25G,

10/25GBASE-CSR (MMF), 10/25GBASE-LR (SMF);
 - Porty 40GE QSFP:
40G-SR4, 40G-LR4, kable twinax 40G;
 - Porty 100GE QSFP:
100G-SR4, 100G-CWDM4, 100G-LR4, kable twinax 100G;

Architektura

4. Urządzenie musi posiadać redundantne i wymienne moduły wentylatorów; oraz musi mieć możliwość wymiany modułów interfejsowych „na gorąco” – ang. hot swap;

Oczekiwana wydajność

5. Urządzenie musi zapewniać pasmo minimum 2,4 Tb/s per slot
6. Urządzenie powinno posiadać minimalnie 16GB pamięci DRAM, 16GB pamięci FLASH oraz bufor pakietów minimum 108MB
7. Urządzenie powinno obsługiwać minimalnie

1000 aktywnych sieci VLAN,
32000 adresów MAC,
200 000 tras IPv4,
200 000 tras IPv6,
1000 interfejsów SVI L3,
1000 interfejsów L3,
128 połączeń zagregowanych typu „port channel”,
16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;

Oprogramowanie\Funkcjonalność

8. Urządzenie powinno mieć wsparcie dla protokołu NTP;
9. Powinno obsługiwać IGMPv1/2/3 i MLDv1/2 Snooping;
10. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
IEEE 802.1w Rapid Spanning Tree,
IEEE 802.1s Multi-Instance Spanning Tree,
Obsługa minimum 128 instancji protokołu STP
11. Przełącznik musi mieć wsparcie dla protokołów LLDP i LLDP-MED lub równoważnych
12. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - Wiele poziomów dostępu administracyjnego poprzez konsolę.
 - 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;
 - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
 - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
 - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
 - Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS)
 - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+;
 - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 256-bitów;
 - Funkcja Private VLAN;
 - Obsługa list kontroli dostępu (ACL)
13. Urządzenie musi mieć mechanizmy związane z zapewnieniem jakości usług w sieci poprzez:
 - implementacje min 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
 - klasyfikacja ruchu do klas różnej jakości obsługi (QoS),
 - ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting); ograniczenia pasma dostępnego na danym porcie.
 - Kontrola sztormów dla ruchu broadcast/multicast/unicast
 - możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
14. Wsparcie dla protokołu LISP zgodnie z RFC 6830,
15. Urządzenie musi wspierać protokół MPLS:
16. Urządzenie musi mieć możliwość obsługi zaawansowanych protokołów routingu
RIP, OSPF, IS-IS i BGP PIM-SM, PIM-SSM; MSDP;
17. Urządzenie powinno mieć wsparcie dla protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu z obsługą przynajmniej 128 sesji BFD;

18. Urządzenie powinno realizować funkcjonalności translacji adresów IP NAT (Network Address Translation)
19. Urządzenie powinno mieć możliwość enkapsulacji ruchu w pakiety VXLAN;
20. Przełącznik musi mieć wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii;

Zarządzanie i konfiguracja

21. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
22. Urządzenie musi mieć możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow
23. Urządzenie powinno mieć możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku;
24. System operacyjny urządzenia musi umożliwiać wgrzywanie poprawek bez konieczności restartowania platformy;
25. Urządzenie musi umożliwiać łączenie w klastery z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze muszą zachowywać się jak jedno urządzenie w punkcie widzenia protokołów L2 i L3;
26. Dostarczone urządzenie do zarządzania powinno posiadać port konsoli, dodatkowy port Ethernet RJ45 / SFP / SFP+ do zarządzania out-of-band oraz port USB do podłączenia zewnętrznego nośnika danych
27. Dostarczone urządzenie musi obsługiwać protokół SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6;
28. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów;
29. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją.

Obudowa

30. Urządzenie musi mieć możliwość montażu w szafie rack 19" i musi zostać dostarczone z zestawem umożliwiającym montaż.

Wyposażenie

31. Każde urządzenie musi być wyposażone w co najmniej:
 - a) 1 kartę zarządzająco-przełączającą wyposażoną w port Ethernet RJ45/SFP/SFP+ służący do zarządzania urządzeniem;
 - b) 2 karty liniowe 48-portowe 1GE/10GE/25GE SFP/SFP+;
 - c) 2 zasilacze o mocy niezbędnej do prawidłowego działania urządzenia w pełni wyposażonego;
 - d) Dysk SSD o pojemności min 240GB jako lokalny magazyn
 - e) Zestaw akcesoriów niezbędnych do konfiguracji jako jedno urządzenie tzw. virtual stack
 - f) Kabel konsoli szeregowy USB
32. Urządzenie musi być dostarczone z 10 modułami SFP-10G-SR spełniającymi następujące wymagania
 - musi spełniać wymagania IEEE 802.3: 10Gigabit Ethernet
 - musi oferować zasięg co najmniej 26m dla standardowego kabla FDDI-grade MMF
 - musi oferować zasięg co najmniej 300m dla kabla MMF (OM3)
 - musi oferować zasięg co najmniej 400m dla kabla MMF (OM4)
 - musi posiadać podwójny konektor LC/PC
 - musi pracować z długością fali 850 nm

33. Urządzenie musi być dostarczone z usługą serwisową producenta na okres co najmniej 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego

Wypożyczenie stanowisk pracy w laboratoriach komputerowych - urządzenia

Nazwa	Minimalny parametr	Ilość szt
Telefon IP1	Funkcjonalność i wydajność co najmniej taka jak model klasy: Cisco CP-8851-K9 o minimalnych parametrach: • min. 5 linie, • 2X 1G interface, • wyświetlacz kolorowy • współpraca z Cisco Unified Communication Manager 11.5 oraz nowszymi • zasilanie 230V, PoE	140
Telefon IP2	Funkcjonalność i wydajność co najmniej taka jak model klasy: Cisco CP-8851-K9 o minimalnych parametrach: • min. 5 linie, • 2X1G interface, • wyświetlacz kolorowy, • współpraca z Cisco Unified Communication Manager 11.5 oraz nowszymi • Zasilanie 230V, PoE • Licencja typu standard umożliwiającą podłączenie użytkownika wraz z urządzeniami do infrastruktury Cisco CUCM (wersj 11.5 i wyżej), Umożliwiającą uruchomienie usług (CSF, IPC, BOT, SEP itp)	20
Telefon konferencyjny IP	Funkcjonalność i wydajność co najmniej taka jak model klasy: Cisco CP-8832-K9 o minimalnych parametrach: • Interface minimum 10/100Base-T • Zasilanie: 230V, PoE	4

Telefon IP1 - 140 szt. (Cisco CP-8851-K9) lub równoważny, spełniające poniższe wymagania równoważności:

1. Aparat biurowy z wyświetlaczem kolorowym min 5 cali.
2. Urządzenie posiadające min 4 przycisków szybkiego wyboru z możliwością rozszerzenia o dodatkowe przyciski i zaprogramowania funkcji np. BLF
3. Urządzenie bazujące na protokole sygnalizacyjnym SIP (RFC 3261).
4. Urządzenie obsługujące kodeki G.711a, G.729a, G.722, iLBC.
5. Zabezpieczenie transmisji poprzez zastosowanie protokołów Transport Layer Security (TLS 1.2) i Secure Real-Time Protocol (SRTP);
6. Urządzenie musi posiadać wbudowaną funkcjonalność klienta VPN (Phone VPN)
7. Zaimplementowane mechanizmy Quality of Service (QoS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
8. Obsługa RTCP.
9. Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP.
10. Urządzenie musi współpracować z posiadanym klastrem (CUCM) Cisco Unified Communication Manager 11.5 i 12.5 a także musi współpracować z pozostałymi urządzeniami oferowanymi przez Wykonawcę w ramach niniejszego zamówienia
11. Telefon musi obsługiwać wszystkie oferowane przez serwer CUCM funkcje a w szczególności:
 - identyfikacja numeru dla połączeń przychodzących,
 - warunkowe i bezwarunkowe przenoszenie wywołań,
 - podgląd połączeń nieodebranych
 - parkowanie połączeń,
 - połączenia oczekujące,
 - transferowanie połączeń,
 - zamawianie połączeń,
 - funkcja sygnalizacji zajętości (BLF)
 - zestawianie telekonferencji.
 - funkcja książki telefonicznej
 - sygnalizacja wiadomości głosowych
12. Obsługa uwierzytelniania za pomocą mechanizmu IEEE 802.1X zarówno telefonu jak i komputera podłączonego do sieci poprzez telefon.
13. Telefon zasilany przez PoE w standardzie IEEE 802.3af oraz z sieci elektroenergetycznej ~230V (zasilacz sieciowy 230V nie jest wymagany).
14. Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100/1000 Mbps
15. Transmisja głosu z telefonu i danych z komputera PC musi być przesyłana w dwóch różnych sieciach VLAN,
16. Połączenie pomiędzy telefonem a przełącznikiem dostępowym powinno być realizowane przy wykorzystaniu trunku w standardzie IEEE 802.1Q.
17. Ciemny kolor obudowy (czarny, grafit lub inny stonowany kolor nie rozpraszający uwagi użytkownika)
18. Urządzenie posiada wbudowany interfejs radiowy Bluetooth 3.0 lub nowszy do podłączenia słuchawek
19. Urządzenie musi posiadać gniazdo USB
20. Dedykowane gniazdo do podłączenia zestawu nagłownego.
21. System głośnomówiący dwukierunkowy, działający w trybie pełnego duplexu.
22. Niezależna regulacja głośności słuchawki i systemu głośnomówiącego.
23. Obsługa przynajmniej w języku polskim, angielskim
24. Możliwość montażu na ścianie (opcjonalny zestaw do montażu na ścianie nie jest wymagany);
25. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:
 - Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych (tftp)
 - Obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne
 - Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonentkie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU)
 - Możliwości zdalnego restartu urządzenia lub grupy urządzeń

- Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego

Telefon IP2 - 20 szt. (Cisco CP-8851-K9) lub równoważny, spełniające poniższe wymagania:

- Aparat biurowy z wyświetlaczem kolorowym min 5 cali.
- Urządzenie posiadające min 4 przycisków szybkiego wyboru z możliwością rozszerzenia o dodatkowe przyciski i zaprogramowania funkcji np. BLF
- Urządzenie bazujące na protokole sygnalizacyjnym SIP (RFC 3261).
- Urządzenie obsługujące kodeki G.711a, G.729a, G.722, iLBC.
- Zabezpieczenie transmisji poprzez zastosowanie protokołów Transport Layer Security (TLS 1.2) i Secure Real-Time Protocol (SRTP);
- Urządzenie musi posiadać wbudowaną funkcjonalność klienta VPN (Phone VPN)
- Zaimplementowane mechanizmy Quality of Service (QOS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
- Obsługa RTCP.
- Obsługa protokołów IEEE 802.1Q, 802.1p, ICMP.
- Urządzenie musi współpracować z posiadanym klastrem (CUCM) Cisco Unified Communication Manager 11.5 i 12.5 a także musi współpracować z pozostałymi urządzeniami oferowanymi przez Wykonawcę w ramach niniejszego zamówienia
- Telefon musi obsługiwać wszystkie oferowane przez serwer CUCM funkcje a w szczególności:
 - identyfikacja numeru dla połączeń przychodzących,
 - warunkowe i bezwarunkowe przenoszenie wywołań,
 - podgląd połączeń nieodebranych
 - parkowanie połączeń,
 - połączenia oczekujące,
 - transferowanie połączeń,
 - zamawianie połączeń,
 - funkcja sygnalizacji zajętości (BLF)
 - zestawianie telekonferencji.
 - funkcja książki telefonicznej
 - sygnalizacja wiadomości głosowych
- Obsługa uwierzytelniania za pomocą mechanizmu IEEE 802.1X zarówno telefonu jak i komputera podłączonego do sieci poprzez telefon.
- Telefon zasilany przez PoE w standardzie IEEE 802.3af oraz z sieci elektroenergetycznej ~230V (zasilacz sieciowy 230V nie jest wymagany).
- Urządzenie musi posiadać wbudowany przełącznik Ethernet, z dwoma portami 10/100/1000 Mbps
- Transmisja głosu z telefonu i danych z komputera PC musi być przesyłana w dwóch różnych sieciach VLAN,
- Połączenie pomiędzy telefonem a przełącznikiem dostępowym powinno być realizowane przy wykorzystaniu trunku w standardzie IEEE 802.1Q.
- Ciemny kolor obudowy (czarny, grafit lub inny stonowany kolor nie rozpraszający uwagi użytkownika)
- Urządzenie posiada wbudowany interfejs radiowy Bluetooth 3.0 lub nowszy do podłączenia słuchawek
- Urządzenie musi posiadać gniazdo USB
- Dedykowane gniazdo do podłączenia zestawu nagłownego.
- System głośnomówiący dwukierunkowy, działający w trybie pełnego duplexu.
- Niezależna regulacja głośności słuchawki i systemu głośnomówiącego.
- Obsługa przynajmniej w języku polskim, angielskim
- Możliwość montażu na ścianie (opcjonalny zestaw do montażu na ścianie nie jest wymagany);
- Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:
 - Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych (tftp)
 - Obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne

- Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU)
- Możliwości zdalnego restartu urządzenia lub grupy urządzeń
- Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego

Wyposażenie

26. Wykonawca dostarczy dla każdego urządzenia licencję umożliwiającą współpracę telefonu z istniejącą infrastrukturą w ramach klastra CUCM w wersji 11.5 lub 12.5:

- zamawiający wymaga dostarczenia licencji dla 20 użytkowników, pozwalające na uruchomienie min 5 dostępnych usług (CSF, IPC, BOT, itp.)
- dostarczone licencje muszą zapewnić migrację do wyższych wersji CUCM w okresie nie krótszym niż 1 rok od daty podpisania umowy,
- nie dopuszcza się licencji o ograniczonym czasie ważności.

Telefon konferencyjny IP - 4 szt. (Cisco CP-8832-K9) lub równoważny spełniający poniższe wymagania:

1. Musi być urządzeniem dedykowanym do sal konferencyjnych i umożliwiać prowadzenie rozmów w trybie głośnomówiącym.
2. Urządzenie powinno być wyposażone w podświetlany wyświetlacz o przekątnej minimum 3,5 cala
3. Musi bazować na protokole sygnalizacyjnym SIP (RFC 3261).
4. Urządzenie musi obsługiwać kodeki G.711a, G.729a, G.722, iLBC. i OPUS
5. Zabezpieczenie transmisji poprzez zastosowanie protokołów Transport Layer Security (TLS 1.2) i Secure Real-Time Protocol (SRTP);
6. Zaimplementowane mechanizmy Quality Of Service (QOS) bazujące na protokole IEEE 802.1p oraz na Differentiated Services Code Point (DSCP).
7. Obsługa RTCP.
8. Musi obsługiwać protokoły markowania ruchu IEEE 802.1Q, 802.1p
9. Urządzenie musi współpracować z posiadanym klastrem (CUCM) Cisco Unified Communication Manager 11.5 i 12.5 a także musi współpracować z pozostałymi urządzeniami oferowanymi przez Wykonawcę w ramach niniejszego zamówienia
10. Telefon musi obsługiwać wszystkie oferowane przez serwer CUCM funkcje a w szczególności:
 - identyfikacja numeru dla połączeń przychodzących,
 - warunkowe i bezwarunkowe przenoszenie wywołań,
 - podgląd połączeń nieodebranych
 - parkowanie połączeń,
 - połączenia oczekujące,
 - transferowanie połączeń,
 - zamawianie połączeń,
 - zestawianie telekonferencji.
 - funkcja książki telefonicznej
 - sygnalizacja wiadomości głosowych
11. Musi być urządzeniem dołączanym do sieci LAN przynajmniej poprzez port sieciowy Ethernet 10/100Base-T
12. Musi mieć możliwość zasilania z sieci komputerowej (802.3af) oraz z wykorzystaniem lokalnego zasilacza 230V. (zasilacz sieciowy 230V nie jest wymagany).
13. Musi mieć możliwość pracy w sieci IPv4 oraz IPv6.
14. Musi mieć możliwość regulacji rozmowy oraz głośności dzwonka
15. Musi umożliwiać podłączenie min. dwóch mikrofonów przewodowych i bezprzewodowych zamiennie
16. Musi umożliwiać dołączenie drugiego terminala w kaskadę, tworząc jedno logiczne urządzenie, w celu rozszerzenia zasięgu dźwięku
17. Panel sterujący musi posiadać co najmniej 4 klawisze programowalne
18. W zakresie bezpieczeństwa telefon musi umożliwiać możliwość identyfikacji w momencie dołączania do infrastruktury sieciowej za pomocą protokołu 802.1X EAP-FAST oraz EAP-TLS
19. Menu telefonu musi być zrealizowane przynajmniej w języku polskim, angielskim

20. Urządzenie powinno być zarządzane centralnie poprzez system komunikacyjny Zamawiającego w zakresie co najmniej:

- Pobierania oraz wymiany plików konfiguracyjnych oraz oprogramowania z serwerów komunikacyjnych (tftp)
- Obsługi oprogramowania (firmware), które jest podpisany cyfrowo przez producenta oraz pliki konfiguracyjne zaszyfrowane przez serwery komunikacyjne Zamawiającego
- Możliwości zdalnej zmiany ustawień urządzenia: numer i opis linii, funkcje przypisane do programowalnych klawiszy funkcyjnych, uprawnienia abonenckie dla danych linii urządzenia, przypisanie do właściwych elementów infrastruktury (bramy i mostki MCU)
- Możliwości zdalnego restartu urządzenia lub grupy urządzeń
- Możliwości dystrybucji certyfikatów dla urządzeń z serwerów komunikacyjnych Zamawiającego

Infrastruktura sieci Internet i Intranet w CBR

Nazwa	Minimalny parametr	Ilość szt.
WIFI Sieć bezprzewodowa - kontroler	Funkcjonalność i wydajność co najmniej taka jak model klasy: Cisco 3504-K9 o minimalnych parametrach: • 4 interfejsy 1GE, • Wydajność kontrolera minimum 4 Gbps • Obsługa minimum 3000 klientów sieci bezprzewodowej • Obsługa przynajmniej 150 punktów dostępowych • Licencja umożliwiająca podłączenie 39 bezprzewodowych punktów dostępowych • Usługą serwisową producenta na okres 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego	2
WIFI Sieć bezprzewodowa – punkt dostępowy	Funkcjonalność i wydajność co najmniej taka jak model klasy: Cisco AIR-AP1832I-E o minimalnych parametrach: • 1 interfejs Gigabit Ethernet (10/100/1000) • interfejs konsoli RJ45 • port USB 2.0 , • 1 GB RAM, 256 MB Flash • Zasilanie: 230V, PoE, PoE+	39

	• Usługą serwisową producenta na okres 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego	
Przełącznik sieciowy dostępowy	Funkcjonalność i wydajność co najmniej taka jak model klasy Cisco 9200 o minimalnych parametrach: • Porty 48x1Gb rj45, • Moduł 4 x 10Gb SFP+ • 2 x wkładka SFP-10G-SR • Redundantny zasilacz • Stackowalne, wyposażone w moduły do stackowania i kable 0,5m	10
Przełącznik sieciowy dostępowy	Funkcjonalność i wydajność co najmniej taka jak model klasy Cisco 9200 o minimalnych parametrach: • Porty 48x1Gb rj45 PoE+ • Wolny slot na moduł rozszerzeń SFP\SFP+ • Redundantny zasilacz • Stackowalne, wyposażone w moduły do stackowania i kable 0,5m	15
Przełącznik sieciowy dostępowy	Funkcjonalność i wydajność co najmniej taka jak model klasy Cisco 9200 o minimalnych parametrach: • Porty 48x1Gb rj45, • Wolny slot na moduł rozszerzeń SFP\SFP+ • Redundantny zasilacz • Stackowalne, wyposażone w moduły do stackowania i kable 1 m	6
WiFi - bezprzewodowy punkt dostępowy wewnętrzny - szt. 39 (np. Cisco AIR-AP1832i-E) lub równoważny o minimalnych wymaganiach Obsługa\Funkcjonalność 1. Urządzenie musi obsługiwać standardy 802.11a/b/g/n/ac (Wave 2) • obsługa SU-MIMO – min. 3x3:2 • obsługa MU-MIMO – min. 3x3:2 • obsługa kanałów 20 i 40 MHz dla 802.11n		

- obsługa kanałów 20, 40 i 80 MHz dla 802.11ac
 - obsługa prędkości PHY do 867 Mbps lub większej
 - obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
 - obsługa TxBF (transmitbeamforming) dla klientów 802.11ac
 - obsługa MRC
2. Urządzenie musi obsługiwać szeroki zakres kanałów radiowych:
 - dla zakresu 2.4 GHz: 13 kanały
 - dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów
 - dla zakresu 5GHz (extended UNII-2): min. 8 kanałów
 3. Urządzenie musi posiadać konfigurowalną moc nadajników radiowych
 - dla zakresu 2.4 GHz: do 100 mW
 - dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW
 - dla zakresu 5GHz (extended UNII-2): do 200 mW
 4. Urządzenie musi być zgodne z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN który umożliwia realizację co najmniej następujących funkcji:
 - automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
 - obsługa min 16 BSSID
 - definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
 - uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
 - obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN)
 - jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS)
 - obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
 - obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
 - obsługa mechanizmów QoS:
 - ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik
 - obsługa WMM, TSPEC, U-APSD
 - współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne
 - wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM
 - wsparcie IEEE 802.11i, WPA2, WPA
 5. Urządzenie musi umożliwiać pracę jako kontroler sieci bezprzewodowej o następujących funkcjonalnościach:
 - obsługa przynajmniej do 15 punktów dostępowych
 - obsługa przynajmniej do 150 klientów
 - możliwość konfiguracji do 8 sieci bezprzewodowych
 - obsługa mechanizmów wsparcia roamingu – IEEE 802.11k
 - konfiguracja polityk bezpieczeństwa per SSID
 - obsługa WPA2 Personal oraz Enterprise (z możliwością tworzenia lokalnej bazy użytkowników)
 - współpraca z serwerami autoryzacyjnymi RADIUS (konfigurowane per SSID)
 - tworzenie list kontroli dostępu
 - obsługa mechanizmów QoS (WMM, priorytetyzacja, Voice CAC z TSPEC)
 6. Urządzenie musi posiadać minimum
 - 1 interfejs Gigabit Ethernet (10/100/1000)
 - interfejs konsoli RJ45
 - port USB 2.0 lub nowszy ,

7. Urządzenia musi posiadać anteny zintegrowane o zysku min. 3dBi dla pasma 2,4 GHz oraz zysku min. 5 dBi dla pasma 5 GHz
8. Obudowa urządzenia przystosowana do warunków pracy w pomieszczeniach biurowych (5 – 35°C)
9. Posiada sygnalizację wizualną stanu urządzenia z możliwością deaktywacji
10. Urządzenie musi być zgodne z dyrektywą 1999/5/EC i 93/42/ECC

Zasilanie

11. Urządzenie musi posiadać co najmniej następujące opcje zasilania:
 - zasilacz sieciowy 230V AC
 - zasilanie PoE+ (802.3at) w sposób zapewniający pełną wydajność
 - zasilanie PoE (802.3af) w sposób zapewniający wszystkie funkcjonalności, lecz z wyłączonym portem USB

Wypożyczenie

12. Urządzenia muszą zostać dostarczone z akcesoriami umożliwiającymi montaż na podwieszanym suficie.
13. Urządzone musi być dostarczone z usługą serwisową producenta na okres 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego.

WiFi - kontroler sieci bezprzewodowej – 2 szt. (AIR-CT3504-K9) lub równoważny o minimalnych wymaganiach

1. Kontroler musi umożliwiać centralną kontrolę punktów dostępu bezprzewodowego oraz musi współpracować z zamawianymi punktami dostępowymi stanowiącymi integralną część tego projektu
2. Musi być zgodny z protokołem CAPWAP (RFC 5415)
3. Urządzenie musi być zoptymalizowane do działania z technologią 802.11ac (Wave 2)
4. Musi posiadać minimum 4 interfejsy 1GE
5. Musi obsługiwać łączenie interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu

Oczekiwana wydajność

6. Kontroler powinien obsługiwać przynajmniej 150 punktów dostępowych (kratowe lub klasyczne)
7. Wydajność kontrolera minimum 4 Gbps
8. Powinien obsługiwać minimalnie 1000 klientów sieci bezprzewodowej

Funkcjonalność

9. Zarządzanie pasmem radiowym punktów dostępowych:
 - Automatyczna adaptacja do zmian w czasie rzeczywistym
 - Optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
 - Dynamiczne przydzielanie kanałów radiowych
 - Wykrywanie, eliminacja i unikanie interferencji
 - Równoważenie obciążenia punktów dostępowych
 - Tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
 - Dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
10. Urządzenie musi mieć możliwość mapowania SSID do segmentów VLAN w sieci przewodowej:
 - 1:1
 - 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
 - Możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
11. Obsługa sieci kratowych
 - Komunikacja między punktami dostępowymi bez medium kablowego,
 - Separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)

- Automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
 - Automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)
 - Autoryzacja punktów dostępowych w oparciu o certyfikaty X.509, adresy MAC
12. Kontroler musi obsługiwać co najmniej następujące mechanizmy bezpieczeństwa:
- 802.11i, WPA2, WPA
 - 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
 - Obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
 - Kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
 - Obsługa profilowania użytkowników:
 - Przydział sieci VLAN
 - Przydział list kontroli dostępu (ACL)
 - Uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 (wykrywanie podszywania się punktów dostępowych użytkowników pod adresy infrastruktury) – IEEE 802.11w
 - Uwierzytelnianie punktów dostępowych w oparciu o certyfikaty X.509
 - Obsługa list kontroli dostępu (ACL)
 - Obsługa list kontroli dostępu opartych o nazwy domenowe
 - Wykrywanie i dezaktywacja obcych punktów dostępowych
 - Wbudowany system IDS wykrywający typowe ataki na sieci bezprzewodowe (fake AP, net-stumbler, deauthentication flood itp.)
 - Współpraca z systemami IDS/IPS
 - Ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP
 - DHCP proxy
13. Obsługa ruchu unicast ipv4 i ipv6
14. Obsługa ruchu multicast ipv4 i ipv6
- IGMP / MLD snooping
 - Obsługa konwersji ruchu multicast do unicast
15. Obsługa mobilności (roaming-u) użytkowników (L2 i L3 – ipv4 i ipv6, w ramach i pomiędzy kontrolerami)
16. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k
17. Wsparcie dla IEEE 802.11u
18. Kontroler powinien obsługiwać następujące mechanizmy QoS:
- 802.1p
 - WMM, TSPEC
 - Ograniczanie pasma per użytkownik
 - Call Admission Control – ze statyczną definicją pasma i dynamiczną w oparciu o analizę profili ruchu
 - U-APSD
19. Kontroler musi obsługiwać dostęp dla Gości (ipv4 i ipv6) a w szczególności:
- Przekierowanie użytkowników o określonym SSID do strony logowania (z możliwością personalizacji strony)
 - Obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta
20. Kontroler musi współpracować z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych
21. Musi obsługiwać protokół NTP wersji 4 (ipv4 oraz ipv6)
22. Rozwiązanie musi zapewnić obsługę redundancji (N+1)
23. Obsługa redundancji 1:1 (active/standby)

Zarządzanie i konfiguracja

24. Urządzenie musi mieć możliwość analizy ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu
25. Zbieranie i eksport statystyk ruchowych za pomocą protokołu Netflow/jflow lub odpowiednika
26. Profilowanie urządzeń podłączających się do sieci bezprzewodowej oraz przydzielanie na podstawie typu urządzenia odpowiednich uprawnień i parametrów dostępowych (np.: lista kontroli dostępu, VLAN, polityka QoS, czas sesji)

27. Zarządzanie przynajmniej przez protokoły HTTPS, snmpv3, SSH oraz port konsoli szeregowej

Obudowa

28. Urządzenie musi mieć możliwość montażu w szafie rack 19 i musi zostać dostarczone z zestawem umożliwiającym montaż.

Wyposażenie

29. Zmawiający wymaga dostarczenia niewygasających licencji na podłączenie 39 szt. punktów dostępowych do kontrolera

30. Urządzone musi być dostarczone z usługą serwisową producenta na okres 1 roku, umożliwiającą tworzenie zgłoszeń, wymianę sprzętu w przypadku awarii ponadto dającą możliwość aktualizacji oprogramowania systemowego

Switch dostępowy z modulem 4x10SFP+ - 10 szt. (np. C9200-48T-E) lub równoważny spełniający poniższe wymagania

Rodzaj urządzenia

1. Przełącznik stackowalny z minimum 48 portami 10/100/1000BaseT RJ45
2. Urządzenie musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń SFP\SFP+
3. Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
 - Min. 4-portowy moduł Gigabit Ethernet z gniazdami SFP
 - Min. 4-portowy moduł 10 Gigabit Ethernet SFP+
4. Porty w modułach powinny mieć możliwość obsadzenia co najmniej następującymi rodzajami wkładek:
 - Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH,
 - Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, twinax

Architektura

5. Urządzenie umożliwia instalację wewnętrznego zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
6. Stackowanie przełączników z zapewnieniem następujących funkcjonalności:
 - przepustowość w ramach stosu - 160Gb/s
 - min 8 urządzeń w stosie
 - zarządzanie poprzez jeden adres IP
 - możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad

Oczekiwana wydajność

7. Urządzenie musi posiadać przynajmniej 4GB pamięci DRAM, 4GB pamięci Flash oraz bufor pakietów 6MB
8. Urządzenie powinno obsługiwać min. 32000 adresów MAC
9. Urządzenie powinno posiadać wsparcie dla co najmniej 4000 sieci VLAN oraz 4000 VLAN ID.
10. Urządzenie powinno obsługiwać min. 3000 tras IPv4 oraz min. 2500 tras IPv6

Oprogramowanie/funkcjonalność

11. Obsługa protokołu NTP
12. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
13. Wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
 - IEEE 802.1w Rapid Spanning Tree
 - IEEE 802.1s Multi-Instance Spanning Tree
 - Obsługa minimum 128 instancji protokołu STP
14. Przełącznik musi mieć wsparcie dla protokołu LLDP i LLDP-MED lub równoważnego
15. Funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
16. Urządzenie musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego
17. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - Wiele poziomów dostępu administracyjnego poprzez konsolę.
 - 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
 - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
 - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
 - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
 - Możliwość obsługi 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 w oparciu o portal www)
 - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
 - Zapewnienie mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
 - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
 - Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
 - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
 - Funkcja Private VLAN
19. Obsługa protokołów routingu
 - Routing statyczny dla IPv4 i IPv6
 - Routing dynamiczny – RIP, OSPF
 - Policy-based routing (PBR)
 - Obsługa protokołu redundancji bramy HSRP/VRRP lub mechanizmu równoważnego

Zarządzanie i konfiguracja

20. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
21. Urządzenie powinno mieć możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
22. Urządzenie powinno posiadać port konsoli, dodatkowy port Ethernet RJ45 / SFP / SFP+ do zarządzania out-of-band oraz port USB do podłączenia zewnętrznego nośnika danych

23. Urządzenie powinno obsługiwać protokół SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6;
24. Urządzenie musi mieć możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
25. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją.

Obudowa

26. Urządzenie musi mieć możliwość montażu w szafie rack 19" i dostarczone z zestawem umożliwiającym montaż.
27. Urządzenie musi mieć wysokość 1 U

Wyposażenie

28. Zainstalowane moduły stackujące dostarczone wraz z niezbędnymi kablami
29. Zainstalowany redundantny zasilacz
30. Slot rozszerzeń obsadzony min. 4-portowym modułem 10Gbit Ethernet SFP+
31. Urządzenie musi być dostarczone z 2 wkładkami SFP-10G-SR spełniającymi następujące wymagania
 - muszą spełniać wymagania IEEE 802.3: 10Gigabit Ethernet
 - muszą oferować zasięg co najmniej 26m dla standardowego kabla FDDI-grade MMF
 - muszą oferować zasięg co najmniej 300m dla kabla MMF (OM3)
 - muszą oferować zasięg co najmniej 400m dla kabla MMF (OM4)
 - muszą posiadać podwójny konektor LC/PC
 - muszą pracować z długością fali 850 nm

Switch dostępowy PoE - 15 szt. (np. C9200-48P-E) lub równoważny spełniający poniższe wymagania

Rodzaj urządzenia

1. Przełącznik stackowalny z minimum 48 portami PoE+ 10/100/1000BaseT RJ45
2. Porty dostępne urządzenia muszą wspierać usługę zasilania kablem Ethernet (PoE+) do 30W na port (zgodnie z IEEE 802.3at typ 2). Wydajność pojedynczego zasilacza powinna zapewniać zasilanie, min 24 portów mocą 30W lub 48 portów mocą 15,4W
3. Urządzenie musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń SFP\SFP+
4. Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
 - Min. 4-portowy moduł Gigabit Ethernet z gniazdami SFP
 - Min. 4-portowy moduł 10 Gigabit Ethernet SFP+
5. Porty w modułach powinny mieć możliwość obsadzenia co najmniej następującymi rodzajami wkładek:
 - Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH,

- Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, twinax

Architektura

6. Urządzenie umożliwia instalację wewnętrznego zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
7. Moc dostępna dla PoE (z jednym zasilaczem – bądź zasilaczami pracującymi w układzie redundantnym/z dwoma zasilaczami) 740W/1440W
8. Przełączniki umożliwiające podtrzymanie zasilania z portów PoE podczas restartu urządzenia
9. Stackowanie przełączników z zapewnieniem następujących funkcjonalności:
 - przepustowość w ramach stosu - 160Gb/s
 - min 8 urządzeń w stosie
 - zarządzanie poprzez jeden adres IP
 - możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad

Oczekiwana wydajność

10. Urządzenie musi posiadać przynajmniej 4GB pamięci DRAM, 4GB pamięci Flash oraz bufor pakietów 6GB
11. Urządzenie powinno obsługiwać min. 32000 adresów MAC
12. Urządzenie powinno posiadać wsparcie dla co najmniej 4000 sieci VLAN oraz 4000 VLAN ID.
13. Urządzenie powinno obsługiwać min. 3000 tras IPv4 oraz min. 2500 tras IPv6

Oprogramowanie/funkcjonalność

14. Obsługa protokołu NTP
15. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
16. Wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
 - IEEE 802.1w Rapid Spanning Tree
 - IEEE 802.1s Multi-Instance Spanning Tree
 - Obsługa minimum 128 instancji protokołu STP
17. Przełącznik musi mieć wsparcie dla protokołu LLDP i LLDP-MED lub równoważnego
18. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
19. Urządzenie musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego
20. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
21. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - Wiele poziomów dostępu administracyjnego poprzez konsolę.
 - 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
 - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
 - Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
 - Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
 - Możliwość obsługi 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 w oparciu o portal www)
 - Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard

- Zapewnienie mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
 - Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
 - Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
 - Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
 - Funkcja Private VLAN
22. Obsługa protokołów routingu
- Routing statyczny dla IPv4 i IPv6
 - Routing dynamiczny – RIP, OSPF
 - Policy-based routing (PBR)
 - Obsługa protokołu redundancji bramy HSRP/VRRP lub mechanizmu równoważnego

Zarządzanie i konfiguracja

23. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
24. Urządzenie powinno mieć możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
25. Urządzenie powinno posiadać port konsoli, dodatkowy port Ethernet RJ45 / SFP / SFP+ do zarządzania out-of-band oraz port USB do podłączenia zewnętrznego nośnika danych
26. Urządzenie powinno obsługiwać protokół SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6;
27. Urządzenie musi mieć możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
28. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją.

Obudowa

29. Urządzenie musi mieć możliwość montażu w szafie rack 19" i dostarczone z zestawem umożliwiającym montaż.
30. Urządzenie musi mieć wysokość 1 U

Wypozażenie

31. Zainstalowane moduły stackujące dostarczone wraz z niezbędnymi kablami
32. Zainstalowany redundantny zasilacz
33. Slot rozszerzeń nieobsadzony żadnym modulem, zabezpieczony przed nieczystościami rozwiązaniem producenta

Switch dostępowy - 6 szt. (np. C9200-48T-E) lub równoważny spełniający poniższe wymagania

Rodzaj urządzenia

1. Przełącznik stackowalny z minimum 48 portami 10/100/1000BaseT RJ45
2. Urządzenie musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń SFP\SFP+
3. Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły:
 - Min. 4-portowy moduł Gigabit Ethernet z gniazdami SFP
 - Min. 4-portowy moduł 10 Gigabit Ethernet SFP+
4. Porty w modułach powinny mieć możliwość obsadzenia co najmniej następującymi rodzajami wkładek:
 - Porty SFP – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH,
 - Porty SFP+ - wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, twinax

Architektura

5. Urządzenie umożliwia instalację wewnętrznego zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
6. Stackowanie przełączników z zapewnieniem następujących funkcjonalności:
 - przepustowość w ramach stosu - 160Gb/s
 - min 8 urządzeń w stosie
 - zarządzanie poprzez jeden adres IP
 - możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad

Oczekiwana wydajność

7. Urządzenie musi posiadać przynajmniej 4GB pamięci DRAM, 4GB pamięci Flash oraz bufor pakietów 6GB
8. Urządzenie powinno obsługiwać min. 32000 adresów MAC
9. Urządzenie powinno posiadać wsparcie dla co najmniej 4000 sieci VLAN oraz 4000 VLAN ID.
10. Urządzenie powinno obsługiwać min. 3000 tras IPv4 oraz min. 2500 tras IPv6

Oprogramowanie/funkcjonalność

11. Obsługa protokołu NTP
12. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
13. Wsparcie dla następujących mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
 - IEEE 802.1w Rapid Spanning Tree
 - IEEE 802.1s Multi-Instance Spanning Tree
 - Obsługa minimum 128 instancji protokołu STP
14. Przełącznik musi mieć wsparcie dla protokołu LLDP i LLDP-MED lub równoważnego
15. Funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
16. Urządzenie musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego
17. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP
18. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
 - Wiele poziomów dostępu administracyjnego poprzez konsolę.
 - 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
 - Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC

- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
- Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
- Możliwość obsługi 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 w oparciu o portal www)
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard
- Zapewnienie mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
- Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia)
- Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host)
- Funkcja Private VLAN

19. Obsługa protokołów routingu

- Routing statyczny dla IPv4 i IPv6
- Routing dynamiczny – RIP, OSPF
- Policy-based routing (PBR)
- Obsługa protokołu redundancji bramy HSRP/VRRP lub mechanizmu równoważnego

Zarządzanie i konfiguracja

20. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN
21. Urządzenie powinno mieć możliwość uruchamiania skryptów Python poprzez Embedded Event Manager
22. Urządzenie powinno posiadać port konsoli, dodatkowy port Ethernet RJ45 / SFP / SFP+ do zarządzania out-of-band oraz port USB do podłączenia zewnętrznego nośnika danych
23. Urządzenie powinno obsługiwać protokół SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6;
24. Urządzenie musi mieć możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
25. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją.

Obudowa

26. Urządzenie musi mieć możliwość montażu w szafie rack 19" i dostarczone z zestawem umożliwiającym montaż.
27. Urządzenie musi mieć wysokość 1 U

Wyposażenie

28. Zainstalowane moduły stackujące dostarczone wraz z niezbędnymi kablami 1 m
29. Zainstalowany redundantny zasilacz

30. Slot rozszerzeń nieobsadzony żadnym modulem, zabezpieczony przed nieczystościami rozwiązaniem producenta