Załącznik nr 1 do PPU

SPECYFIKACJA ILOŚCIOWO - TECHNICZNA

Kompleksowe wykonanie sieci WLAN w Składnicach RARS polegająca na:

1) dostarczeniu oraz konfiguracji dostarczonych urządzeń (spełniających minimalne wymagania zawarte w niniejszym dokumencie), jak i całości sieci WLAN w Składnicach oraz na poziomie Centrali,
2) wykonaniu okablowania strukturalnego sieci WLAN w magazynach Składnicy, wskazanych w „Dokumentacji Projektowo-kosztorysowej na sieć WLAN w Składnicach RARS";
3) wykonaniu pomiarów natężenia pola WLAN, porównania z założeniami zawartymi w „Dokumentacji Projektowo-kosztorysowej na sieć WLAN w Składnicach RARS" i ewentualnej korekty ustawień urządzeń Access Point;
4) świadczeniu serwisu gwarancyjnego, na warunkach określonych w PPU.

W ramach zamówienia Wykonawca jest zobowiązany do zastosowania takich rozwiązań aby sieć WLAN osiągała parametry nie gorsze niż przewidziane w „Dokumentacji Projektowo-kosztorysowej". Brak osiągnięcia tych parametrów skutkuje brakiem możliwości odbioru przedmiotu zamówienia. Zamawiający wskazuje, że przewiduje fakultatywną wizję, ale z uwagi na okoliczności, zasadnym jest skorzystanie z tej możliwości.

Zamówienie jest podzielone na części:

- Zadanie 1 - Wykonanie sieci WLAN w budynkach magazynowych Składnicy RARS w Ełku
- Zadanie 2 - Wykonanie sieci WLAN w budynkach magazynowych Składnicy RARS w Kamienicy Królewskiej
- Zadanie 3 - Wykonanie sieci WLAN w budynkach magazynowych Składnicy RARS w Lublińcu

Zamawiający wymaga, aby osoby wykonujące zamówienia z ramienia Wykonawcy, zatrudnione na umowę o pracę, posiadali upoważnienie do dostępu do informacji niejawnych o klauzuli „zastrzeżone" oraz ważne zaświadczenie w zakresie ochrony informacji niejawnych. W przypadku braku zaświadczenia Zamawiający umożliwi przeszkolenie pracowników Wykonawcy przez POIN w RARS.

Dla każdej z części wymagania są opisane zbiorczo poniżej.
Szczegółowy opis przedmiotu zamówienia oraz wymagane parametry ustanawiają:

1) Ogólne wymagania techniczne - urządzenia aktywne
    1. Wymaga się dostarczenia elementów aktywnych sieci (routery, przełączniki, punkty dostępowe) ww. lokalizacjach, które będą zarządzane, konfigurowane, monitorowane przez obecnie posiadane systemy centralne Zamawiającego.

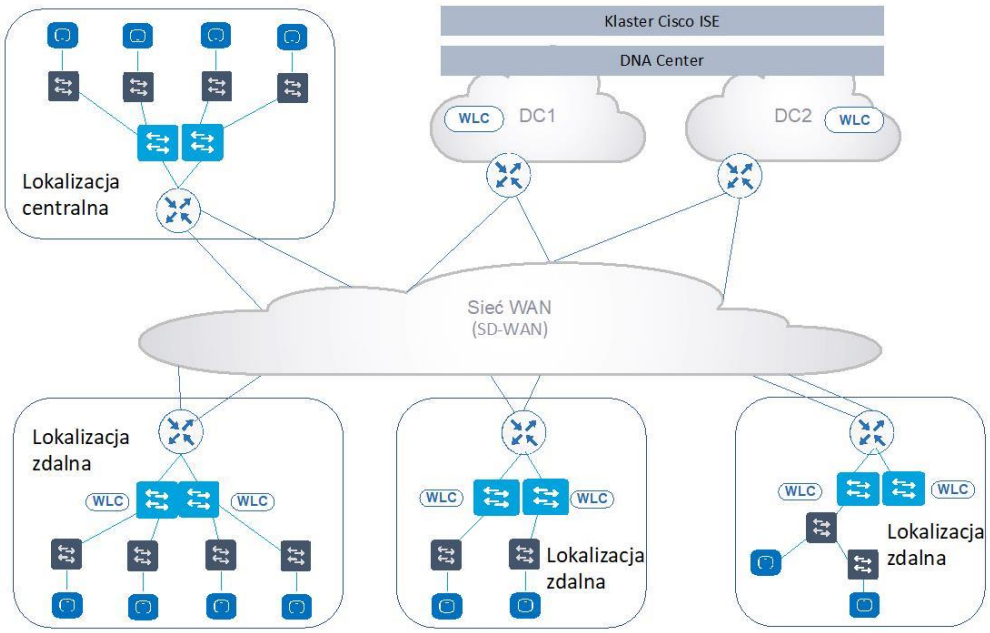
2. Każda lokalizacja zdalna będzie łączyła się z siecią WAN (SD-WAN) co najmniej dwoma niezależnymi linkami. Preferowane są łącza kablowe o przepustowości min. 30 Mb/s. Oba linki muszą jednocześnie pracować i na obu musi zachodzić transmisja danych do lokalizacji DC1 i DC2. Na etapie realizacji zamówienia wymagane jest wykorzystanie łączy aktualnie dostarczonych do Składnic oraz analiza potencjalnych dostawców i zarekomendowanie RARS łączy, które powinny być zapewnione w celu zapewnienia odpowiedniej wydajności i ciągłości działania sieci WAN (SD-WAN).
3. W lokalizacjach ośrodków przetwarzania danych RARS DC1 i DC2 należy przewidzieć dostawę niezbędnych urządzeń (serwery, routery) koniecznych do uruchomienia sieci SD-WAN. Zamawiający określa minimalne wymagania dla routerów, które muszą zostać dostarczone do DC1 i DC2 w sposób umożliwiający zapewnienie pełnej redundancji (2 pary urządzeń).
4. Wymagania dla routerów dla DC1 i DC2 zawierają „Minimalne parametry techniczne – Router DC”.
5. Wykonawca do każdej Składnicy dostarczy router. Urządzenie musi być zarządzane centralnie i uwzględniać lokalne wyjście do sieci Internet (Direct Internet Access).
6. Wymagania dla routerów dla Składnic zawierają „Minimalne parametry techniczne – Router Składnica”.
7. W składnicach, routery zostaną podłączone do przełączników agregujących linkami o przepływności min. 10Gb/s.
8. Przełączniki oraz radiowe punkty dostępowe muszą zostać dostarczone do każdej Składnicy zgodnie z zestawieniem sprzętu. Zamawiający definiuje następujące typy sprzętu wymagane do realizacji zamówienia:
    i. Switch PoE typ 1, który będzie 12-portowym przełącznikiem dostępowym i tranzytowym – wymagania zawierają „Minimalne parametry techniczne – Switch PoE typ 1”;
    ii. Switch PoE typ 2, który będzie 24-portowym przełącznikiem dostępowym – wymagania zawierają „Minimalne parametry techniczne – Switch PoE typ 2”;
    iii. Switch typ 3, który będzie przełącznikiem agregacyjnym – wymagania zawierają „Minimalne parametry techniczne – Switch typ 3”;
    iv. Kontroler WLAN – wymagania zawierają „Minimalne parametry techniczne – Kontroler WLAN”;
    v. AP typ 1, radiowy punkt dostępowy (access point) z wbudowanymi antenami – wymagania zawierają „Minimalne parametry techniczne – AP typ 1”;
    vi. AP typ 2, radiowy punkt dostępowy (access point) o zwiększonej odporności na warunki środowiskowe – wymagania zawierają „Minimalne parametry techniczne – AP typ 2”
9. Zestawienie sprzętu aktywnego zgodnie z tabelą poniżej:

Lokalizacja	Magazyn	Liczba AP w pomieszczeniu	Model AP	Typ przełącznika / urządzenia	Liczba przełączników dostępowych / agregujących bądź kontrolerów	Model przełącznika

Ełk	Magazyn 1	12	AP Typ 1	Dostępowy	1	Switch PoE Typ 2
Ełk	Magazyn 2	6	AP Typ 1	Dostępowy	1	Switch PoE Typ 1
Ełk	Magazyn 3	9	AP Typ 1	Dostępowy	1	Switch PoE Typ 1
Ełk	Magazyn 4	5	AP Typ 1	Dostępowy	1	Switch PoE Typ 1
Ełk	Magazyn 5	8	AP Typ 1	Dostępowy	1	Switch PoE Typ 1
Ełk	Magazyn 9	20	AP Typ 1	Dostępowy/ Dostępowy	1+1	Switch PoE Typ 2/ Switch PoE Typ 1
Ełk	Magazyn 10	6	AP Typ 1	Dostępowy	2	Switch PoE Typ 1
Ełk	Serwerownia			Agregacyjny	1	Switch Typ 3
Ełk	Serwerownia			Kontroler WLAN	1	Kontroler WLAN
Ełk	Serwerownia			Router	1	Router Składnica
Kamienica Królewska	Magazyn 1	17	AP Typ 1	Dostępowy	2	Switch PoE Typ 1
Kamienica Królewska	Magazyn 2	6	AP Typ 1	Dostępowy	2	Switch PoE Typ 1
Kamienica Królewska	Magazyn 3	9	AP Typ 1	Dostępowy	2	Switch PoE Typ 1
Kamienica Królewska	Magazyn 4	15	AP Typ 1	Dostępowy	3	Switch PoE Typ 1
Kamienica Królewska	Serwerownia			Agregacyjny	1	Switch Typ 4
Kamienica Królewska	Serwerownia			Kontroler WLAN	1	Kontroler WLAN
Kamienica Królewska	Serwerownia			Router	1	Router Składnica
Lubliniec	Magazyn 1	19	AP Typ 2	Dostępowy/ Dostępowy	1+1	Switch PoE Typ 2/ Switch PoE Typ 1
Lubliniec	Magazyn 2	20	AP Typ 2	Dostępowy/ Dostępowy	1+1	Switch PoE Typ 2/ Switch PoE Typ 1

Lubliniec	Magazyn 3	26	AP Typ 2	Dostępowy/ Dostępowy	2+1	Switch PoE Typ 2/ Switch PoE Typ 1
Lubliniec	Magazyn 4	27	AP Typ 1	Dostępowy/ Dostępowy	2+1	Switch PoE Typ 2/ Switch PoE Typ 1
Lubliniec	Serwerownia			Agregacyjny	1	Switch Typ 4
Lubliniec	Serwerownia			Kontroler WLAN	1	Kontroler WLAN
Lubliniec	Serwerownia			Router	1	Router Składnica

10. O ile inaczej nie oznaczono, wszystkie wymagania określone w „Minimalnych parametrach techniczny” są wymaganiami minimalnymi. Na przykład, zapis „Bufor pakietów – 6MB” należy czytać jako „Bufor pakietów – minimum 6MB”.
11. Routery, przełączniki oraz access pointy muszą być zarządzane, konfigurowane, monitorowane przez posiadane przez Zamawiającego centralny system Cisco DNAC i dodane do konfiguracji w centralnie zarządzanym systemie Cisco ISE.
12. Wykonawca musi dobrać wkładki optyczne zapewniające przepływność szkieletu sieci lokalizacji zdalnej (przełączniki agregacyjne i dostępowe) na poziomie 10Gb/s. Koszt wszystkich modułów optycznych niezbędnych do realizacji zamówienia musi być uwzględniona w koszcie prac instalacyjnych.
13. Przełączniki dostępowe muszą być podłączone do przełączników agregujących dwoma up-linkami.
14. Do przełączników dostępowych należy podłączyć odpowiednią liczbę punktów dostępowych access pointów (AP Typ 1, 2 i 3).
15. W dokumentacji do każdego magazynu zostały przedstawione mapy pokrycia wykonane za pomocą Ekahau. Wykonawca musi wykonać pomiar pokrycia radiowego w każdej składnicy (site survey) zgodnie z „Procedurą realizacji zamówienia”.
16. Należy dobrać parametry pracy sieci radiowej i rozmieszczenie access pointów w taki sposób, aby poziom sygnału nie spadał poniżej -63dBm, w miejscach pracy urządzeń końcowych (np. czytników kodów kreskowych). Miejsca te będą oznaczone poglądowo na rzutach magazynów przez Zamawiającego przed rozpoczęciem site survey.
17. Docelową sieć poglądowo przedstawia poniższy rysunek



18. Wykonawca wraz z Urządzeniami dostarczy zestaw montażowy rack, tj. wszystkie niezbędne elementy konieczne do ich montażu w Lokalizacjach Zamawiającego, w szczególności: śrubki, nakrętki koszykowe, kable zasilające, szyny montażowe, itp.
19. Urządzenia muszą ze sobą współdziałać i być ze sobą kompatybilne oraz być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą znajdować się na liście „end-of-sale", „end-of-life" oraz „end-of-support" producenta.
20. Urządzenia muszą posiadać najnowszą dostępną stabilną wersję Oprogramowania na moment podpisania protokołu odbiorowego. Wykonawca udziela na rzeczone oprogramowanie lub dokonuje przeniesie na Zamawiającego lub gwarantuje udzielenie, licencji niewyłącznej w zakresie związanym z realizacją przedmiotu zamówienia i późniejszym użytkowaniem urządzeń wraz z ich oprogramowaniem. Licencja jest bezterminowa i brak jest możliwości jej wypowiedzenia przez Wykonawcę, a jeżeli uzna się, że niemożliwość wypowiedzenia jest nieważna, uznaje się, że termin wypowiedzenia wynosi 10 lat.
21. Wszystkie elementy infrastruktury aktywnej (przełączniki, access pointy, kontrolery WLAN i routery) muszą być ze sobą kompatybilne i ze sobą współdziałać oraz muszą pochodzić z oficjalnego kanału sprzedaży. Wykonawca dostarczy wraz ze sprzętem zaświadczenia producenta zaoferowanych urządzeń dotyczące legalności źródła pochodzenia. Dostarczenie tego dokumentu jest warunkiem niezbędnym odbioru ilościowego.

2) „Dokumentacja Projektowo-kosztorysowa na sieć WLAN w Składnicach RARS"
    1. Składnica RARS w EŁKU, 19-301 Ełk, Nowa Wieś Ełcka, ul. Wilcza 2 woj. warmińsko-mazurskie – zadanie I
        i. Załącznik E1 do specyfikacji,
        ii. Załącznik E2 do specyfikacji.

2. Składnica RARS w KAMIENICY KRÓLEWSKIEJ, ul, Sosnowa 2, 83-342 Kamienica Królewska, woj. Pomorskie – zadanie II
    i. Załącznik K1 do specyfikacji,
    ii. Załącznik K2 do specyfikacji.
3. Składnica RARS w LUBLIŃCU, 42-700 Lubliniec, ul. Klonowa 40, woj. Śląskie – zadanie III
    i. Załącznik L1 do specyfikacji,
    ii. Załącznik L2 do specyfikacji.

Udostępnienie „Dokumentacji Projektowo-Kosztorysowej na sieć WLAN w Składnicach RARS" nastąpi wyłącznie na wniosek Wykonawcy zgodnie z trybem określonym w SWZ.

3) Treść niniejszego dokumentu m.in. minimalne wymagania techniczne dot. Urządzeń aktywnych sieci;

1. Wszelkie nazwy własne użyte w załącznikach „Dokumentacji Projektowo-Kosztorysowej" są przykładowe i zostały użyte wyłącznie w celach projektowych. Nie mają one charakteru wiążącego wykonawcę.
2. **Parametry urządzeń wyszczególnione w niniejszym dokumencie mają pierwszeństwo przed parametrami określonymi w „Dokumentacji Projektowo-Kosztorysowej" – w razie rozbieżności wiążące są parametry z niniejszego dokumentu.**

Minimalne wymagania techniczne – zadanie I, II, III

Parametry techniczne – Router DC

1) Szczegółowe wymagania dla każdego z Urządzeń.
    1. Musi posiadać 12 interfejsów, z czego 4 z nich ustawić w tryb 1GE lub 10 GE, a 8 w tryb 1GE. Interfejsy 1GE muszą być definiowane przez wkładki SFP, a interfejsy 10GE przez wkładki optyczne SFP+. W przypadku urządzeń o niekonfigurowalnych przepustowościach portów, urządzenie powinno być wyposażone w 4 portów 10GE i 10 portów 1GE.
    2. Musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR.
    3. Musi być wyposażone w min. 16 GB pamięci RAM i musi mieć możliwość rozbudowy do min. 32GB RAM.
    4. Musi być wyposażone w pamięć o pojemności min. 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych – oraz mieć możliwość rozbudowy do min. 32GB.
    5. Musi mieć możliwość redundancji zasilania oraz warstwy kontrolnej ze wsparciem NSF i SSO – dopuszczalna realizacja za pomocą zdublowanych modułów kontroli albo przez zapewnienie możliwości jednoczesnego uruchomienia dwóch instancji systemu operacyjnego.
    6. Musi obsługiwać min. 3.500.000 prefiksów w tablicach routingu IPv4 lub 2.000.000 prefiksów w tablicy routingu IPv6.
    7. Musi obsługiwać min. 4.000 list kontroli dostępu oraz min. 50.000 wpisów list kontroli dostępu.
    8. Musi oferować sumaryczną wydajność przesyłania pakietów 6 Mpps dla pakietów IMIX.
    9. Musi oferować sumaryczną wydajność dla pakietów IMIX na poziomie 18Gbps.
    10. Musi być przystosowane do montażu w szafie 19”, obudowa wykonana z metalu.
    11. Musi posiadać redundantne zasilacze przystosowane do zasilania prądem naprzemiennym 230V.
2) Funkcje Oprogramowania.
    1. Musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6.
    2. Musi posiadać wsparcie dla MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN).
    3. Musi być w stanie obsłużyć 8.000 instancji VRF (Virtual Route Forwarding).
    4. Musi posiadać ochronę warstwy zarządzającej (Control Plane Policing).
    5. Musi obsługiwać 4.000 ACL (Access Control Lists) z 50.000 wpisów ACE (Access Control Entries).
    6. Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2.
    7. Musi obsługiwać RPF (Reverse Path Forwarding).
    8. Musi obsługiwać zarządzanie ruchem (QoS).
    9. 16000 kolejek per system
        i. Hierarchiczne polityki QoS,
        ii. 3 poziomy hierarchii,

iii. dwie kolejki priorytetowe LLQ per polityka,
iv. opóźnienie dla ruchu priorytetowego na poziomie nie większym niż 200 mikrosekund.

10. Musi obsługiwać funkcjonalność Sflow lub odpowiednik (J-Flow, NetFlow) przy wydajności 13Gbps dla pakietów typu IMIX.
11. Musi posiadać funkcjonalność VRRP lub odpowiednika.
12. Musi umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3.
13. Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS).
14. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do Urządzenia i uruchomiona.
15. Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń-filtrów;
16. Urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem: AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.

3) Oprogramowanie/funkcjonalności dla trybu pracy SD-WAN.
    1. Szyfrowanie wszystkich łączy WAN z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łącza spełniające wymagania aplikacji zdefiniowane w polityce.
    2. Bezpieczne połączenie WAN lokalizacji, wykorzystując w tym celu dowolną kombinację połączeń przez sieć transportową (IP VPN), jak też opcjonalnie sieci publiczne (Internet).
    3. Aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy lokalizacjami, odpowiednio sterując ruchem zależnie od aktualnych warunków
    4. Elastyczne tworzenie topologii (gwiazda, częściowa lub pełna kratę, punkt-punkt) per segment.
    5. Monitorowanie wydajności wszystkich łączy systemu.
    6. Równoważenie obciążenia poszczególnych łącz (per sesja):
        i. statyczne (active/standby i active/active równoważne i ważone),
        ii. dynamiczne oparte o monitorowanie jakości w danym czasie.
    7. Redundancja active-active urządzeń na poziomie zakończenia usługi w każdej lokalizacji (jedno urządzenie CE obsługujące łącze podstawowe, drugie urządzenie CE obsługujące łącza podstawowe i zapasowe).
    8. Funkcjonalności z zakresu bezpieczeństwa:
        i. szyfrowanie wszystkich połączeń AES256,
        ii. funkcja skrótu SHA-2,
        iii. uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared),
        iv. obsługa list kontroli dostępu (ACL),
        v. segmentacja sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa 4-ech segmentów,

vi. obsługa translacji adresów NAT/PAT i NAT Traversal - wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji - ruch taki powinien być translowany i lokalnie wychodzić do Internetu,
vii. możliwość segmentacji routera na 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN,
viii. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall),
ix. funkcjonalność IPS,
x. funkcjonalność filtracji URL,
xi. funkcjonalność analizy ruchu pod kątem występowania w nim malware'u,
xii. funkcjonalność TLS Proxy – umożliwiająca rozszyfrowanie ruchu płynącego od użytkownika i poddania go inspekcji np. przez mechanizm wykrywania malware'u.

9. Polityki jakości obsługi aplikacji:
   i. wykrywanie aplikacji na bazie głębokiej inspekcji ruchu (DPI),
   ii. możliwość definicji polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki,
   iii. monitorowanie jakości dostępu do usług chmurowych typu SaaS (Google Apps, Office365, Dropbox) i IaaS (AWS, Azure) z możliwością optymalizacji dostępu do nich - system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi.
10. Mechanizmy zapewnienia jakości ruchu (QoS):
   i. obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma,
   ii. kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu,
   iii. mechnizm tail-drop i RED (Random Early Detect),
   iv. oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu,
   v. mechanizm odzyskiwania utraconych pakietów przez dodanie dodatkowych nadmiarowych danych do transmisji. Mechanizm powinien mieć możliwość skonfigurowania aplikacji, dla których jest aplikowany oraz możliwość załączenia się (wysyłania nadmiarowych danych) tylko, gdy warunki sieciowe ulegną degradacji,
11. Możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów analogowych.
12. Obsługa protokołów routingu dynamicznego:
   i. OSPFv2 (także na portach LAN),
   ii. BGP,
   iii. BFD,

iv. Multicast z obsługą replikacji w poszczególnych węzłach sieciowych (w celu uniknięcia replikacji u źródła).

13. Obsługa protokołów i funkcjonalności sieciowych:
    i. 802.1q,
    ii. VRRP,
    iii. Serwer DHCP,
    iv. SSHv2,
    v. SNMP v2c, v3,
    vi. NTP z uwierzytelnieniem,
    vii. Syslog.
14. Mechanizmy konfiguracji „zero touch" – możliwość skonfigurowanie urządzenia brzegowego w sposób automatyczny z wykorzystaniem centralnego kontrolera bez konieczności pre-konfiguracji samego urządzenia brzegowego (bez wpisywania kodów, tokenów, czy wspólnych haseł).
15. Rozwiązanie ma opierać się o centralny kontroler, routery CE uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi.
16. Interfejs kontrolera musi zapewniać:
    i. graficzny interfejs konfiguracyjny,
    ii. obsługę API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler; dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML,
    iii. obsługę RBAC (możliwość zróżnicowania ról administratorów w zakresie brak dostępu / tylko odczyt / pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa),
    iv. zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych,
    v. wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu,
    vi. zarządzanie oraz diagnostyka z poziomu GUI oraz CLI,
    vii. konfiguracja urządzeń oparta o wzorce konfiguracyjne,
    viii. dostarczone z wszystkimi niezbędnymi licencjami umożliwiającymi uruchomienie wymienionych funkcjonalności, obejmującymi możliwość instalacji kontrolera SD-WAN jako maszyny (maszyn) wirtualnych pracujących z wirtualizatorem VMWare ESXi.

Parametry techniczne – Router Składnica

1) Szczegółowe wymagania dla każdego z Urządzeń.
    1. Musi posiadać 6 interfejsów 1GE RJ45.
    2. Urządzenie musi pozwalać na rozszerzenie o 1 dodatkowy moduł z portem 10GE, wspierającym standard szyfrowania MACSec. W przypadku braku możliwości rozszerzenia, router powinien mieć 6 porty 1 GE RJ45 i 1 port 10GE SFP/SFP+.
    3. Urządzenie musi umożliwiać rozszerzenie o wbudowany moduł łączności poprzez sieć komórkową w standardzie LTE kategorii 6. Wbudowany moduł powinien pozwalać na przełączania między dwoma różnymi operatorami sieci komórkowej.
    4. Urządzenie musi umożliwiać rozszerzenie o platformę serwerową bądź mieć możliwość uruchomienia oprogramowania „hypervisora", na którym można instalować maszyny wirtualne.
    5. Urządzenie musi wspierać porty telefonii analogowej FXS do podłączania telefonów jako wbudowane w urządzenie lub w ramach modułów rozszerzenia. Oczekuje się możliwości rozszerzenia o 24 portów FXS.
    6. Urządzenie musi obsługiwać transkodowanie strumieni głosowych dla 256 kanałów.
    7. Musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR.
    8. Musi być wyposażone w 8 GB pamięci RAM.
    9. Musi być wyposażone w pamięć o pojemności 16 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych.
    10. Musi mieć możliwość redundancji zasilania.
    11. Musi obsługiwać 2.000.000 prefiksów w tablicach routingu IPv4/IPv6.
    12. Musi obsługiwać 50.000 prefiksów w tablicach routingu multicast i 1.000 grup.
    13. Musi oferować wydajność przesyłania pakietów 4 Mpps dla pakietów IMIX.
    14. Musi oferować wydajność dla pakietów IMIX na poziomie 10Gbps.
    15. Musi być przystosowane do montażu w szafie 19", obudowa wykonana z metalu;
    16. Musi posiadać redundantne zasilacze przystosowane do zasilania prądem naprzemiennym 230V.
2) Funkcje Oprogramowania.
    1. Musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6.
    2. Musi posiadać wsparcie dla MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN).
    3. Musi być w stanie obsłużyć 4000 instancji VRF (Virtual Route Forwarding).
    4. Musi posiadać ochronę warstwy zarządzającej (Control Plane Policing).
    5. Musi obsługiwać 4000 ACL (Access Control Lists) z 40.000 wpisów ACE (Access Control Entries).
    6. Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2.
    7. Musi obsługiwać RPF (Reverse Path Forwarding).
    8. Musi obsługiwać zarządzanie ruchem (QoS):
        i. 16000 kolejek per system,

ii. Hierarchiczne polityki QoS,
iii. 3 poziomy hierarchii,
iv. dwie kolejki priorytetowe LLQ per polityka,
v. opóźnienie dla ruchu priorytetowego na poziomie nie większym niż 200 mikrosekund.

9. Musi obsługiwać funkcjonalność Sflow lub odpowiednik (J-Flow, NetFlow) przy wydajności 3.5Gbps dla pakietów typu IMIX.
10. Musi posiadać funkcjonalność VRRP lub odpowiednika.
11. Musi umożliwiać zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3.
12. Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS).
13. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do Urządzenia i uruchomiona.
14. Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń-filtrów.
15. Urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.
16. Wymaga się szyfrowania ruchu z wykorzystaniem tuneli IPSec/GRE w trybie full-mesh.
17. Wymaga się obsługi MPLS, EoMPLS i VPLS na routerach.

3) Oprogramowanie/funkcjonalności dla trybu pracy SD-WAN.
1. Szyfrowanie wszystkich łączy WAN z centralnym, redundantnym kontrolerem zarządzającym i monitorującym całą sieć, z możliwością ustalania polityk związanych z jakością obsługi aplikacji i ew. przełączeniem ruchu aplikacji na łącza spełniające wymagania aplikacji zdefiniowane w polityce.
2. Bezpieczne połączenie WAN lokalizacji, wykorzystując w tym celu dowolną kombinację połączeń przez sieć transportową (IP VPN), jak też opcjonalnie sieci publiczne (Internet).
3. Aktywne wykorzystanie wszystkich dostępnych połączeń pomiędzy lokalizacjami, odpowiednio sterując ruchem zależnie od aktualnych warunków.
4. Elastyczne tworzenie topologii (gwiazda, częściowa lub pełna kratę, punkt-punkt) per segment.
5. Monitorowanie wydajności wszystkich łączy systemu.
6. Równoważenie obciążenia poszczególnych łącz (per sesja):
    i. statyczne (active/standby i active/active równoważne i ważone),
    ii. dynamiczne oparte o monitorowanie jakości w danym czasie.
7. Redundancja active-active urządzeń na poziomie zakończenia usługi w każdej lokalizacji (jedno urządzenie CE obsługujące łącze podstawowe, drugie urządzenie CE obsługujące łącza podstawowe i zapasowe).
8. Funkcjonalności z zakresu bezpieczeństwa:
    i. szyfrowanie wszystkich połączeń AES256,
    ii. funkcja skrótu SHA-2,
    iii. uwierzytelnienie urządzeń na bazie certyfikatów X.509 podpisanych zaufanymi kluczami prywatnymi – zintegrowane w systemie CA

z mechanizmem automatycznej dystrybucji kluczy (bez wykorzystania kluczy typu pre-shared),
   iv. obsługa list kontroli dostępu (ACL),
   v. segmentacja sieci, np. w oparciu o osobne tablice routingu (obsługa nakładających się przestrzeni adresowych); możliwość definicji topologii sieciowej per segment; obsługa 4-ech segmentów,
   vi. obsługa translacji adresów NAT/PAT i NAT Traversal - wsparcie dla lokalnego wyjścia do Internetu z pominięciem komunikacji przez sieć WAN dla zdefiniowanych aplikacji - ruch taki powinien być translowany i lokalnie wychodzić do Internetu,
   vii. możliwość segmentacji routera na 4 odseparowane na warstwie IP podsieci – poprzez funkcjonalność VPN,
   viii. funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall),
   ix. funkcjonalność IPS,
   x. funkcjonalność filtracji URL,
   xi. funkcjonalność analizy ruchu pod kątem występowania w nim malware'u,
   xii. funkcjonalność TLS Proxy – umożliwiająca rozszyfrowanie ruchu płynącego od użytkownika i poddania go inspekcji np. przez mechanizm wykrywania malware'u.
9. Polityki jakości obsługi aplikacji:
   i. wykrywanie aplikacji na bazie głębokiej inspekcji ruchu (DPI),
   ii. możliwość definicji polityki systemu określającej maksymalne tolerowane przez określoną aplikację parametry sieci: opóźnienie, zmienność opóźnień, straty w pakietach - w przypadku przekroczenia zdefiniowanych progów ruch aplikacyjny powinien zostać przekierowany na inne łącze WAN, jeśli spełnia ono wymogi aplikacji wg polityki,
   iii. monitorowanie jakości dostępu do usług chmurowych typu SaaS (Google Apps, Office365, Dropbox) i IaaS (AWS, Azure) z możliwością optymalizacji dostępu do nich - system musi umożliwiać przekierowanie ruchu do usług przez każdy węzeł dysponujący wyjściem do Internetu, zapewniający w danym czasie najlepszą jakość dostępu do usługi.
10. Mechanizmy zapewnienia jakości ruchu (QoS):
   i. obsługa kształtowania (shaping), ograniczania (policing) ruchu, gwarancje pasma,
   ii. kolejkowanie z kolejką priorytetową i model WFQ (Weighted Fair Queuing) dla pozostałych klas ruchu,
   iii. mechnizm tail-drop i RED (Random Early Detect),
   iv. oznaczanie i zmiana oznaczeń DSCP na bazie przekroczeń ograniczeń ruchu,
   v. mechanizm odzyskiwania utraconych pakietów przez dodanie dodatkowych nadmiarowych danych do transmisji. Mechanizm powinien mieć możliwość skonfigurowania aplikacji, dla których jest aplikowany oraz możliwość załączenia się (wysyłania nadmiarowych danych) tylko, gdy warunki sieciowe ulegną degradacji.

11. Możliwość pracy jako brama VoIP/PSTN z wykorzystaniem interfejsów analogowych.
12. Obsługa protokołów routingu dynamicznego:
    i. OSPFv2 (także na portach LAN),
    ii. BGP,
    iii. BFD ,
    iv. Multicast z obsługą replikacji w poszczególnych węzłach sieciowych (w celu uniknięcia replikacji u źródła).
13. obsługa protokołów i funkcjonalności sieciowych:
    i. 802.1q,
    ii. VRRP,
    iii. Serwer DHCP,
    iv. SSHv2,
    v. SNMP v2c, v3,
    vi. NTP z uwierzytelnieniem,
    vii. Syslog,
    viii. mechanizmy konfiguracji „zero touch" – możliwość skonfigurowanie urządzenia brzegowego w sposób automatyczny z wykorzystaniem centralnego kontrolera bez konieczności pre-konfiguracji samego urządzenia brzegowego (bez wpisywania kodów, tokenów, czy wspólnych haseł).
14. Rozwiązanie ma opierać się o centralny kontroler, routery CE uwierzytelniające się z innymi komponentami rozwiązania poprzez certyfikaty X.509 podpisane kluczami prywatnymi.
15. Interfejs kontrolera musi zapewniać:
    i. graficzny interfejs konfiguracyjny,
    ii. obsługę API umożliwiającego konfigurację wszystkich możliwości oferowanych przez kontroler; dopuszczalne standardy API to: Python, Ansible, REST, RESTConf, NETConf/Yang, XML,
    iii. obsługę RBAC (możliwość zróżnicowania ról administratorów w zakresie brak dostępu / tylko odczyt / pełen dostęp dla poszczególnych funkcjonalności systemu zarządzania – co najmniej alarmów, logów, monitorowania urządzeń, aktualizacji oprogramowania, interfejsów, polityk, routingu, bezpieczeństwa),
    iv. zarządzanie routerami ma odbywać się całkowicie z poziomu kontrolerów centralnych,
    v. wymaga się zarządzania aktualizacją oprogramowania z centralnego systemu,
    vi. zarządzanie oraz diagnostyka z poziomu GUI oraz CLI,
    vii. konfiguracja urządzeń oparta o wzorce konfiguracyjne,
    viii. dostarczone z wszystkimi niezbędnymi licencjami umożliwiającymi uruchomienie wymienionych funkcjonalności, obejmującymi możliwość instalacji kontrolera SD-WAN jako maszyny (maszyn) wirtualnych pracujących z wirtualizatorem VMWare ESXi.

Parametry techniczne – Switch PoE typ 1

1) Typ i liczba portów: 12 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP.
2) Moc dostępna dla PoE:
    1. 370W (z dwoma zasilaczami o mocy 600W pracującymi w układzie redundantnym),
    2. 740W (z dwoma zasilaczami o mocy 600W pracującymi w układzie współdzielenia mocy).
3) Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
    1. Gigabit Ethernet 1000Base-T,
    2. Gigabit Ethernet 1000Base-SX,
    3. Gigabit Ethernet 1000Base-LX/LH,
    4. Gigabit Ethernet 1000Base-EX,
    5. Gigabit Ethernet 1000Base-ZX,
    6. Gigabit Ethernet 1000Base-BX-D/U,
    7. 10Gigabit Ethernet 10GBase-SR,
    8. 10Gigabit Ethernet 10GBase-LR,
    9. 10Gigabit Ethernet 10GBase-ER,
    10. 10Gigabit Ethernet 10GBase-ZR,
    11. 10Gigabit Ethernet typu twinax (SFP+ - SFP+).
4) Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    1. Przepustowość w ramach stosu - 80Gb/s,
    2. 8 urządzeń w stosie,
    3. Zarządzanie poprzez jeden adres IP,
    4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad.
5) Zasilanie i chłodzenie:
    1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
    2. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
    3. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
    4. Redundantne wentylatory.
6) Parametry wydajnościowe:
    1. Przepustowość przełącznika (switching capacity): 128 Gb/s (bez podłączenia do stosu), 208 Gb/s (z podłączeniem do stosu),
    2. Prędkość przesyłania (forwarding rate): 95.23 Mpps,
    3. Bufor pakietów – 6MB,
    4. Pamięć DRAM – 2GB,
    5. Pamięć flash – 4GB,
    6. Obsługa:
        i. 500 aktywnych sieci VLAN,
        ii. 16000 adresów MAC,

iii. 3000 tras IPv4,
iv. 1500 tras IPv6.
v. Ilość wpisów w listach kontroli dostępu Security ACL – 1000,
vi. Ilość wpisów w listach kontroli dostępu QoS ACL – 1000,
vii. 512 interfejsów SVI L3,
viii. Jumbo frame 9198B,
ix. 48 połączeń zagregowanych typu „port channel”,
x. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.

7) Obsługa protokołu NTP.
8) Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
9) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    1. IEEE 802.1w Rapid Spanning Tree,
    2. Per-VLAN Rapid Spanning Tree (PVRST+),
    3. IEEE 802.1s Multi-Instance Spanning Tree,
    4. Obsługa 64 instancji protokołu STP,
    5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol),
    6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym, a drugi uplink zapasowym, a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywróceniu aktywności uplinku podstawowego.
10) Obsługa protokołu LLDP i LLDP-MED.
11) Realizacja funkcji 802.1Q tunneling (QinQ).
12) Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
13) Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
14) Możliwość uruchomienia funkcji serwera DHCP.
15) Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
13. Obsługa list kontroli dostępu (ACL) następujących typów:
    i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
14. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
16. Funkcja Private VLAN;

16) Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    2. bezpieczna sekwencja uruchamiania,
    3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
17) Mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,

7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

18) Obsługa protokołów i mechanizmów routingu:
    1. Routing statyczny dla IPv4 i IPv6,
    2. Routing dynamiczny – RIP, OSPF do 1000 routes,
    3. Policy-based routing (PBR),
    4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
    5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
19) Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
20) Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
21) Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
22) Funkcjonalność sondy IP SLA Responder,
23) Zarządzanie
    24) Port konsoli,
    25) Dedykowany port Ethernet do zarządzania out-of-band,
    26) Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
    27) Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    28) Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
    29) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    30) Wsparcie dla protokoły RESTCONF,
    31) Wsparcie dla protokołu gNMI,
    32) Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    33) Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
    34) Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
    35) Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe),

dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

36) Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
37) Monitoring pracy przełącznika w zakresie:
    1. Użycie CPU, użycie pamięci, temperatura pracy,
    2. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    3. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    4. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
    5. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    6. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    7. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
    8. Protokół REP (Resilient Ethernet Protocol),
    9. Protokół STP (Spanning Tree Protocol),
    10. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
38) Konfigurację przełącznika w zakresie:
    1. Konfiguracja interfejsów fizycznych:
        i. opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
        ii. w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
        iii. w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
        iv. przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
    2. Konfiguracja interfejsów logicznych:
        i. opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
        ii. w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,

iii. w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
iv. przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

3. Konfiguracja interfejsów wirtualnych typu SVI:
   i. opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP)

39) Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
40) Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
41) Konfiguracja mechanizmów SPAN i RSPAN,
42) Konfiguracja protokołu STP,
43) Konfiguracja protokołu REP,
44) Konfiguracja routingu statycznego i dynamicznego,
45) Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
46) Tworzenie i przypisanie list kontroli dostępu ACL,
47) Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
48) Konfiguracja i uruchomienie NetFlow,
49) Konfiguracja polityk QoS,
50) Administracja przełącznika w zakresie:
    1. Zdalne uruchamianie komend linii poleceń,
    2. Nazwa przełącznika,
    3. Tryb pracy L2/L3,
    4. Adres IP przełącznika do celów zarządzania zdalnego,
    5. Konfiguracja serwera DHCP,
    6. Konfiguracja DNS,
    7. Czas systemowy w tym protokół NTP,
    8. Konta administracyjne,
    9. Upgrade oprogramowania,
    10. Backup konfiguracji,
    11. Zdalny restart urządzenia,
    12. Konfiguracja i dostęp przez SNMP,
51) Diagnostyka urządzenia:
    1. Narzędzie PING i TRACEROUTE,
    2. Przeglądanie logów systemowych,
    3. Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
52) Parametry fizyczne:
    1. Możliwość montażu w szafie rack 19”,

2. Wysokość urządzenia maksimum 1 RU,
3. Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 30 cm
4. Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 33 cm

53) Funkcjonalności oprogramowania
   1. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
   2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
   3. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
   4. Wsparcie dla protokołu LISP zgodnie z RFC 6830,
54) Obsługa zaawansowanych protokołów routingu:
   1. IS-IS dla IPv4 i IPv6,
   2. OSPF,
   3. EIGRP (rfc7868),
   4. Routing multicastów - PIM-SM, PIM-SSM,
   5. Multicast Source Discovery Protocol (MSDP),
55) Możliwość enkapsulacji ruchu w pakiety VXLAN,
56) Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,
57) Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
   1. Statycznie w oparciu o port do którego podłączona jest stacja,
   2. Statycznie w oparciu o VLAN, w którym pracuje stacja,
   3. Statycznie w oparciu o adres IP stacji,
   4. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X.
58) Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
59) Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa.

Parametry techniczne – Switch PoE typ 2

1) Typ i liczba portów: 24 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2) Moc dostępna dla PoE:
    1. 740W (z dwoma zasilaczami o mocy 1kW pracującymi w układzie redundantnym),
    2. 1440W (z dwoma zasilaczami o mocy 1kW pracującymi w układzie współdzielenia mocy),
3) Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
    1. Gigabit Ethernet 1000Base-T,
    2. Gigabit Ethernet 1000Base-SX,
    3. Gigabit Ethernet 1000Base-LX/LH,
    4. Gigabit Ethernet 1000Base-EX,
    5. Gigabit Ethernet 1000Base-ZX,
    6. Gigabit Ethernet 1000Base-BX-D/U,
    7. 10Gigabit Ethernet 10GBase-SR,
    8. 10Gigabit Ethernet 10GBase-LR,
    9. 10Gigabit Ethernet 10GBase-ER,
    10. 10Gigabit Ethernet 10GBase-ZR,
    11. 10Gigabit Ethernet typu twinax (SFP+ - SFP+).
4) Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    1. Przepustowość w ramach stosu - 80Gb/s,
    2. 8 urządzeń w stosie,
    3. Zarządzanie poprzez jeden adres IP,
    4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
5) Zasilanie i chłodzenie:
    1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
    2. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
    3. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik umożliwia przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
    4. Redundantne wentylatory,
6) Parametry wydajnościowe:
    1. Przepustowość przełącznika (switching capacity): 176 Gb/s (bez podłączenia do stosu), 256 Gb/s (z podłączeniem do stosu)
    2. Prędkość przesyłania (forwarding rate): 130.95 Mpps
    3. Bufor pakietów – 6MB
    4. Pamięć DRAM – 2GB
    5. Pamięć flash – 4GB
    6. Obsługa:
        i. 500 aktywnych sieci VLAN
        ii. 16000 adresów MAC

iii. 3000 tras IPv4
iv. 1500 tras IPv6
v. Ilość wpisów w listach kontroli dostępu Security ACL – 1000
vi. ilość wpisów w listach kontroli dostępu QoS ACL – 1000
vii. 512 interfejsów SVI L3
viii. Jumbo frame 9198B
ix. 48 połączeń zagregowanych typu „port channel”
x. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.

7) Obsługa protokołu NTP
8) Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    1. IEEE 802.1w Rapid Spanning Tree
    2. Per-VLAN Rapid Spanning Tree (PVRST+)
    3. IEEE 802.1s Multi-Instance Spanning Tree
    4. Obsługa 64 instancji protokołu STP
    5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
    6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku
10) Obsługa protokołu LLDP i LLDP-MED.
11) Realizacja funkcji 802.1Q tunneling (QinQ).
12) Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
13) Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
14) Możliwość uruchomienia funkcji serwera DHCP.
15) Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
13. Obsługa list kontroli dostępu (ACL) następujących typów:
    i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).
14. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
16. Funkcja Private VLAN;

16) Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    2. bezpieczna sekwencja uruchamiania,
    3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
17) Mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
    7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

18) Obsługa protokołów i mechanizmów routingu:
    1. Routing statyczny dla IPv4 i IPv6,
    2. Routing dynamiczny – RIP, OSPF: 1000 routes,
    3. Policy-based routing (PBR),
    4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
    5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
19) Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
20) Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
21) Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
22) Funkcjonalność sondy IP SLA Responder,
23) Zarządzanie
    1. Port konsoli,
    2. Dedykowany port Ethernet do zarządzania out-of-band,
    3. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
    4. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    5. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
    6. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    7. Wsparcie dla protokoły RESTCONF,
    8. Wsparcie dla protokołu gNMI,
    9. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    10. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
    11. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
    12. Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
    13. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:

i. Monitoring pracy przełącznika w zakresie:
    1. Użycie CPU, użycie pamięci, temperatura pracy,
    2. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
    3. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
    4. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)
    5. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    6. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
    7. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
    8. Protokół REP (Resilient Ethernet Protocol),
    9. Protokół STP (Spanning Tree Protocol),Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),
ii. Konfigurację przełącznika w zakresie:
    1. Konfiguracja interfejsów fizycznych:
        a. opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,
        b. w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),
        c. w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,
        d. przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)
    2. Konfiguracja interfejsów logicznych:
        a. opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,

b. w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,
c. w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,
d. przypisanie listy kontroli dostępu w kierunku „do" oraz „z" urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

3. Konfiguracja interfejsów wirtualnych typu SVI:
   a. opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do" oraz „z", parametry protokołu DHCP Relay (adres IP serwera DHCP)

iii. Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
iv. Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
v. Konfiguracja mechanizmów SPAN i RSPAN,
vi. Konfiguracja protokołu STP,
vii. Konfiguracja protokołu REP,
viii. Konfiguracja routingu statycznego i dynamicznego,
ix. Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
x. Tworzenie i przypisanie list kontroli dostępu ACL,
xi. Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
xii. Konfiguracja i uruchomienie NetFlow,
xiii. Konfiguracja polityk QoS,
xiv. Administracja przełącznika w zakresie:
xv. Zdalne uruchamianie komend linii poleceń,
xvi. Nazwa przełącznika,
xvii. Tryb pracy L2/L3,
xviii. Adres IP przełącznika do celów zarządzania zdalnego,
xix. Konfiguracja serwera DHCP,
xx. Konfiguracja DNS,
xxi. Czas systemowy w tym protokół NTP,
xxii. Konta administracyjne,
xxiii. Upgrade oprogramowania,
xxiv. Backup konfiguracji,
xxv. Zdalny restart urządzenia,
xxvi. Konfiguracja i dostęp przez SNMP,
xxvii. Diagnostyka urządzenia:

1. Narzędzie PING i TRACEROUTE,
2. Przeglądanie logów systemowych,
3. Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

24) Parametry fizyczne:
1. Możliwość montażu w szafie rack 19”,
2. Wysokość urządzenia maksymalnie 1 RU,
3. Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 30 cm,
4. Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 33 cm.

25) Funkcjonalności oprogramowania
1. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
3. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
4. Wsparcie dla protokołu LISP zgodnie z RFC 6830,
5. Obsługa zaawansowanych protokołów routingu:
    i. IS-IS dla IPv4 i IPv6,
    ii. OSPF,
    iii. EIGRP (rfc7868),
    iv. Routing multicastów - PIM-SM, PIM-SSM,
    v. Multicast Source Discovery Protocol (MSDP),
6. Możliwość enkapsulacji ruchu w pakiety VXLAN,
7. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,
8. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
    i. Statycznie w oparciu o port do którego podłączona jest stacja,
    ii. Statycznie w oparciu o VLAN, w którym pracuje stacja,
    iii. Statycznie w oparciu o adres IP stacji,
    iv. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
9. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
10. Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących

wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa.

Parametry techniczne – Switch typ 3

1) Typ i liczba portów: 24 porty 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 możliwe do obsadzenia następującymi rodzajami wkładek:
    1. Gigabit Ethernet 1000Base-T,
    2. Gigabit Ethernet 1000Base-SX,
    3. Gigabit Ethernet 1000Base-LX/LH,
    4. Gigabit Ethernet 1000Base-EX,
    5. Gigabit Ethernet 1000Base-ZX,
    6. Gigabit Ethernet 1000Base-BX-D/U (zasięg do 10 km, SMF),
    7. Gigabit Ethernet 1000Base-BX40-D/U (zasięg do 40 km, SMF),
    8. Gigabit Ethernet 1000Base-BX80-D/U (zasięg do 80 km, SMF),
    9. 10Gigabit Ethernet 10GBase-SR,
    10. 10Gigabit Ethernet 10GBase-LR,
    11. 10Gigabit Ethernet 10GBase-ER,
    12. 10Gigabit Ethernet 10GBase-ZR,
    13. 10Gigabit Ethernet 10GBase-BX-D/U (zasięg do 10 km, SMF),
    14. 10Gigabit Ethernet 10GBase-BX40-D/U (zasięg do 40 km, SMF),
    15. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
    16. 25Gigabit Ethernet 25GBASE-SR,
    17. 25Gigabit Ethernet typu twinax (SFP28 – SFP28),
    18. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
    19. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);
2) Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami:
    1. 8x1/10/25G typu SFP/SFP+/SFP28
    2. 2x40/100G typu QSFP/QSFP28
    3. 8x100M/1G/2.5G/5G/10GBaseT RJ-45
3) Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    1. Przepustowość w ramach stosu jednorodnego złożonego z takich samych urządzeń - 1Tb/s,
    2. Przepustowość w ramach stosu mieszanego złożonego z różnych urządzeń pochodzących z tej samej rodziny przełączników dostępowych - 480Gb/s,
    3. 8 urządzeń w stosie,
    4. Zarządzanie poprzez jeden adres IP,
    5. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
    6. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),
    7. Możliwość współdzielenia mocy zasilaczy (grupa do 4 urządzeń w stosie) tzn. zasilacze stanowią zasób wspólny dla grupy przełączników (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania” mocy dla innych jednostek w stosie,

w tym dla przełączników wymagających większej mocy dla PoE, jeśli takie są zainstalowane w stosie),

4) Zasilanie i chłodzenie:
    1. Redundantne i wymienne moduły wentylatorów,
    2. Zainstalowany zasilacz redundantny AC 230V o mocy 1100W. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
5) Parametry wydajnościowe:
    1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):
        i. Przepustowość przełącznika (switching capacity): 1600 Gb/s (bez podłączenia do stosu), 2600 Gb/s (z podłączeniem do stosu)
        ii. Prędkość przesyłania (forwarding rate): 1190 Mpps (bez podłączenia do stosu), 1934 Mpps (z podłączeniem do stosu)
    2. Bufor pakietów – 32MB,
    3. Pamięć DRAM – 16GB
    4. Pamięć flash – 16GB
6) Obsługa:
    1. 1000 aktywnych sieci VLAN
    2. 32000 adresów MAC
    3. 15000 tras IPv4
    4. 7500 tras IPv6
    5. Ilość wpisów w listach kontroli dostępu Security ACL – 5000
    6. ilość wpisów w listach kontroli dostępu QoS ACL – 4000
    7. 1000 interfejsów SVI L3
    8. 128 interfejsów L3
    9. frame 9198B
    10. 128 połączeń zagregowanych typu „port channel”
    11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
7) Obsługa protokołu NTP
8) Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    1. IEEE 802.1w Rapid Spanning Tree
    2. Per-VLAN Rapid Spanning Tree (PVRST+)
    3. IEEE 802.1s Multi-Instance Spanning Tree
    4. Obsługa 256 instancji protokołu STP
    5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
    6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym, a drugi uplink zapasowym, a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego.
10) Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED.
11) Realizacja funkcji 802.1Q tunneling (QinQ)

12) Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
13) Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
14) Możliwość uruchomienia funkcji serwera DHCP
15) Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),
    12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
    13. Obsługa list kontroli dostępu (ACL) następujących typów:
        i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
        ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
        iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
        iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    14. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),
    15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

16. Realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),

16) Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    2. bezpieczna sekwencja uruchamiania,
    3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
17) Mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
    7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
18) Obsługa protokołów i mechanizmów routingu:
    1. Routing statyczny dla IPv4 i IPv6,
    2. Routing dynamiczny – RIP, OSPF: 1000 routes,
    3. Policy-based routing (PBR),
    4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
    5. Obsługa 100 tuneli GRE (Generic Routing Encapsulation);
19) Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
20) Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
21) Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.).
22) Funkcjonalność sondy IP SLA Responder,
23) Zarządzanie:
    1. Port konsoli,
    2. Dedykowany port Ethernet do zarządzania out-of-band,
    3. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,

4. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
5. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
6. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
7. Wsparcie dla protokoły RESTCONF,
8. Wsparcie dla protokołu gNMI,
9. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
10. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
11. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
12. Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności 240GB;
13. Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące.

24) Parametry fizyczne:
1. Możliwość montażu w szafie rack 19”,
2. Wysokość urządzenia maksymalnie 1 RU,

25) Funkcjonalności oprogramowania
1. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 128000 strumieni (flow),
2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
3. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
4. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
5. Wsparcie dla protokołu LISP zgodnie z RFC 6830,
6. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:
    i. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 256 połączeń wirtualnych VC,
    ii. L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,

   iii. L3 VPN - MPLS Virtual Private Network (VPN) – obsługa 7000 tras routingowych L3 VPN,
   iv. Multicast VPN (MVPN);
   v. Inter AS Option A i B,
   vi. EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
   vii. MPLS over GRE,
7. Obsługa 256 wirtualnych instancji routingu (VRF),
8. Obsługa zaawansowanych protokołów routingu
   i. IS-IS i BGP dla IPv4 i IPv6,
   ii. OSPF,
   iii. EIGRP (rfc7868),
   iv. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,
   v. Multicast Source Discovery Protocol (MSDP),
9. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
10. Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,
11. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256), Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
12. Możliwość enkapsulacji ruchu w pakiety VXLAN,
13. Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie funkcjonalności leaf oraz spine,
14. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
   i. Statycznie w oparciu o port, do którego podłączona jest stacja,
   ii. Statycznie w oparciu o VLAN, w którym pracuje stacja,
   iii. Statycznie w oparciu o adres IP stacji,
   iv. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
15. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
16. Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
17. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,
18. 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,
19. Funkcjonalność bramy dla usług mDNS,

20. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
21. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),
22. Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),
23. Wbudowany analizator pakietów,
24. System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
25. Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker,
26. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,
27. Wsparcie dla Audio Video Bridging (AVB),

Parametry techniczne – Switch typ 4

1) Typ i liczba portów: 12 porty 10/100/1000BaseT RJ-45 (zgodne z IEEE 802.3at) + uplink 4x10G SFP
2) Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
    1. Gigabit Ethernet 1000Base-T,
    2. Gigabit Ethernet 1000Base-SX,
    3. Gigabit Ethernet 1000Base-LX/LH,
    4. Gigabit Ethernet 1000Base-EX,
    5. Gigabit Ethernet 1000Base-ZX,
    6. Gigabit Ethernet 1000Base-BX-D/U,
    7. 10Gigabit Ethernet 10GBase-SR,
    8. 10Gigabit Ethernet 10GBase-LR,
    9. 10Gigabit Ethernet 10GBase-ER,
    10. 10Gigabit Ethernet 10GBase-ZR,
    11. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
3) Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
    1. Przepustowość w ramach stosu - 80Gb/s,
    2. 8 urządzeń w stosie,
    3. Zarządzanie poprzez jeden adres IP,
    4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
4) Zasilanie i chłodzenie:
    1. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
    2. Redundantne wentylatory,
5) Parametry wydajnościowe:
    1. Przepustowość przełącznika (switching capacity): 128 Gb/s (bez podłączenia do stosu), 208 Gb/s (z podłączeniem do stosu)
    2. Prędkość przesyłania (forwarding rate): 95.23 Mpps
    3. Bufor pakietów – 6MB
    4. Pamięć DRAM – 2GB
    5. Pamięć flash – 4GB
    6. Obsługa:
    7. 500 aktywnych sieci VLAN
    8. 16000 adresów MAC
    9. 3000 tras IPv4
    10. 1500 tras IPv6
    11. Ilość wpisów w listach kontroli dostępu Security ACL – 1000
    12. ilość wpisów w listach kontroli dostępu QoS ACL – 1000
    13. 512 interfejsów SVI L3
    14. Jumbo frame 9198B
    15. 48 połączeń zagregowanych typu „port channel”,
    16. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
6) Obsługa protokołu NTP
7) Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

8) Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    1. IEEE 802.1w Rapid Spanning Tree
    2. Per-VLAN Rapid Spanning Tree (PVRST+)
    3. IEEE 802.1s Multi-Instance Spanning Tree
    4. Obsługa 64 instancji protokołu STP
    5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
    6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym, a drugi uplink zapasowym, a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności uplinku podstawowego.
9) Obsługa protokołu LLDP i LLDP-MED
10) Realizacja funkcji 802.1Q tunneling (QinQ)
11) Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
12) Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
13) Możliwość uruchomienia funkcji serwera DHCP
14) Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
    5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
    6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
    7. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
    8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
    9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
    10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
    11. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard),

12. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
13. Obsługa list kontroli dostępu (ACL) następujących typów:
    i. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    ii. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    iii. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    iv. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
14. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128) z mechanizmem MACsec Key Agreement (MKA),
15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
16. Funkcja Private VLAN;

15) Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    2. bezpieczna sekwencja uruchamiania,
    3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
16) Mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
    3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
    4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
    5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
    6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
    7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
17) Obsługa protokołów i mechanizmów routingu:
    1. Routing statyczny dla IPv4 i IPv6,
    2. Routing dynamiczny – RIP, OSPF do 1000 routes,
    3. Policy-based routing (PBR),
    4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 64 grup,
    5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
18) Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,

19) Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
20) Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
21) Funkcjonalność sondy IP SLA Responder,
22) Zarządzanie
    23) Port konsoli,
    24) Dedykowany port Ethernet do zarządzania out-of-band,
    25) Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
    26) Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
    27) Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
    28) Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
    29) Wsparcie dla protokoły RESTCONF,
    30) Wsparcie dla protokołu gNMI,
    31) Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    32) Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
    33) Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
    34) Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,
    35) Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:
    36) Monitoring pracy przełącznika w zakresie:
        1. Użycie CPU, użycie pamięci, temperatura pracy,
        2. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,
        3. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,
        4. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy

pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)

5. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
6. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,
7. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,
8. Protokół REP (Resilient Ethernet Protocol),
9. Protokół STP (Spanning Tree Protocol),
10. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

37) Konfigurację przełącznika w zakresie:

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

38) Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,
39) Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
40) Konfiguracja mechanizmów SPAN i RSPAN,
41) Konfiguracja protokołu STP,
42) Konfiguracja protokołu REP,
43) Konfiguracja routingu statycznego i dynamicznego,
44) Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,
45) Tworzenie i przypisanie list kontroli dostępu ACL,
46) Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,
47) Konfiguracja i uruchomienie NetFlow,
48) Konfiguracja polityk QoS,
49) Administracja przełącznika w zakresie:
    1. Zdalne uruchamianie komend linii poleceń,
    2. Nazwa przełącznika,
    3. Tryb pracy L2/L3,
    4. Adres IP przełącznika do celów zarządzania zdalnego,
    5. Konfiguracja serwera DHCP,
    6. Konfiguracja DNS,
    7. Czas systemowy w tym protokół NTP,
    8. Konta administracyjne,
    9. Upgrade oprogramowania,
    10. Backup konfiguracji,
    11. Zdalny restart urządzenia,
    12. Konfiguracja i dostęp przez SNMP,
50) Diagnostyka urządzenia:
    1. Narzędzie PING i TRACEROUTE,
    2. Przeglądanie logów systemowych,
    3. Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
51) Parametry fizyczne:
    1. Możliwość montażu w szafie rack 19”,
    2. Wysokość urządzenia maksimum 1 RU,
    3. Głębokość chassis urządzenia bez wentylatorów i kabli zasilających mniejsza niż 30 cm
    4. Głębokość chassis urządzenia z wentylatorami i kablami zasilającymi mniejsza niż 33 cm
52) Funkcjonalności oprogramowania
    1. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 16000 strumieni (flow),
    2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie

danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,

3. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
4. Wsparcie dla protokołu LISP zgodnie z RFC 6830,

53) Obsługa zaawansowanych protokołów routingu:
    1. IS-IS dla IPv4 i IPv6,
    2. OSPF,
    3. EIGRP (rfc7868),
    4. Routing multicastów - PIM-SM, PIM-SSM,
    5. Multicast Source Discovery Protocol (MSDP),
54) Możliwość enkapsulacji ruchu w pakiety VXLAN,
55) Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci,
56) Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
    1. Statycznie w oparciu o port do którego podłączona jest stacja,
    2. Statycznie w oparciu o VLAN, w którym pracuje stacja,
    3. Statycznie w oparciu o adres IP stacji,
    4. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
57) Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
58) Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa.

Parametry techniczne – Kontroler WLAN

1) Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
    1. zarządzanie politykami bezpieczeństwa
    2. wykrywanie zagrożeń w sieci bezprzewodowej
    3. zarządzanie pasmem radiowym
    4. zarządzanie mobilnością
    5. zarządzanie jakością transmisji zgodnie z protokołem CAPWAP (RFC 5415)
2) Obsługa 250 punktów dostępowych (kratowe lub klasyczne) z możliwością rozszerzenia do 500 przez dodanie odpowiedniej licencji
3) Urządzenie wyposażone w liczbę licencji na obsługę AP wraz ze wsparciem producenta dla wszystkich access pointów określonych zamówieniem (w tym opcjonalnych, jeżeli Zamawiający zleci realizacje tego zakresu)
4) 4 interfejsy 2.5G/1G oraz 2 interfejsy 1/10G (SFP/SFP+)
5) Obsługa łączenia interfejsów w grupę logiczną by zabezpieczyć przed awarią pojedynczego interfejsu
6) Obsługa ruchu tunelowanego o przepustowości 5 Gbps z możliwością rozszerzenia do 10Gbps przez dodanie odpowiedniej licencji
7) Obsługa 5000 klientów sieci bezprzewodowej
8) Zarządzanie pasmem radiowym punktów dostępowych:
    1. automatyczna adaptacja do zmian w czasie rzeczywistym
    2. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia)
    3. dynamiczne przydzielanie kanałów radiowych
    4. wykrywanie, eliminacja i unikanie interferencji
    5. równoważenie obciążenia punktów dostępowych
    6. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych
    7. automatyczna dystrybucja klientów pomiędzy punkty dostępowe
    8. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych
    9. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe
9) Mapowanie SSID do segmentów VLAN w sieci przewodowej
    1. 1:1
    2. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty)
    3. możliwość tunelowania ruchu klientów do kontrolera oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID)
10) Obsługa sieci kratowych
    1. komunikacja między punktami dostępowymi bez medium kablowego
    2. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi)
    3. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo)
    4. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji)

5. autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC

11) Obsługa mechanizmów bezpieczeństwa:
    1. 802.11i, WPA3, WPA2, WPA
    2. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST)
    3. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników
    4. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID
    5. obsługa profilowania użytkowników:
        i. przydział sieci VLAN
        ii. przydział list kontroli dostępu (ACL)
    6. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w
    7. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty
    8. obsługa list kontroli dostępu (ACL)
    9. obsługa list kontroli dostępu opartych o nazwy domenowe
    10. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X
    11. wykrywanie i dezaktywacja obcych punktów dostępowych
    12. możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń
    13. ochrona kryptograficzna (DTLS) ruchu kontrolnego i ruchu użytkowników CAPWAP
    14. 1DHCP proxy, wsparcie dla DHCP Option 82
    15. obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa z wykorzystaniem mechanizmu out-of-band, który przekazuje mapowania aktualnych adresów IP stacji i znacznika
12) Zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
    1. kryptograficzne podpisywanie obrazów oprogramowania
    2. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych
    3. wbudowany moduł sprzętowy unikalnie identyfikujący urządzenie i jego pochodzenie
13) Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji
14) Obsługa ruchu unicast IPv4 i IPv6
15) Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201
16) Obsługa ruchu multicast IPv4 i IPv6
    1. IGMP / MLD snooping
    2. optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem a punktem dostępowym)
    3. obsługa konwersji ruchu multicast do unicast
17) Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami)
18) Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k
19) Obsługa mechanizmów QoS
    1. 802.1p

2. WMM, TSpec, U-APSD
3. Ograniczanie pasma per użytkownik
4. Call Admission Control, SIP CAC, Call Snooping
5. równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego
6. kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID
7. zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS

20) Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji; współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników
21) Obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów
22) Obsługa dostępu gościnnego (IPv4 i IPv6)
    1. przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony)
    2. przekierowanie użytkowników do strony logowania na zewnętrznym serwerze
    3. obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta
    4. obsługa konfiguracji jako dedykowany kontroler do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera w sposób zapewniający logiczną separację od ruchu wewnętrznego
23) Obsługa NTP (IPv4 oraz IPv6), możliwość ustawienia różnych serwerów NTP dla wybranych grup AP
24) Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny)
25) Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze)
26) Wsparcie dla IEEE 802.11u
27) Obsługa Hotspot 2.0
28) Obsługa redundancji rozwiązania (N+1)
29) Obsługa redundancji 1:1 (active/standby) zapewniającej:
    1. utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera
    2. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej
30) Dedykowany interfejs 1GE typu RJ45 służący do połączenia dwóch kontrolerów w redundantną parę 1:1
31) Dedykowany interfejs 1GE typu RJ45 do zarządzania
32) Port konsoli RJ45
33) Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, port konsoli szeregowej
34) Obsługa logowania Syslog, wsparcie dla IPSec w celu zabezpieczenia Syslog
35) Obsługa wbudowanego interpretera języka PYTHON

36) Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020)
37) Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem
38) Funkcjonalność oprogramowania
    1. zbieranie i eksport statystyk ruchowych za pomocą protokołu NetFlow, w tym również informacji zawartych w pakiecie od warstw 2 do 7 (w szczególności informacji o aplikacjach)
    2. obsługa mechanizmów wysokiej dostępności, takich jak możliwość wgrania łatki oprogramowania bez restartu kontrolera (hot patching), restartu danego procesu, odseparowania systemów operacyjnych punktów dostępowych od systemu kontrolera, sekwencyjnego uaktualniania oprogramowania punktów dostępowych (rolling upgrades)
    3. obsługa aktualizacji oprogramowania na parze kontrolerów w trybie ISSU (In-Service Software Upgrade); podczas aktualizacji ruch jest obsługiwany a sesje punktów dostępowych i urządzeń mobilnych są utrzymane
    4. współpraca z siecią dostępową typu SDN opartą o Network Fabric, wymiana informacji kontrolnych za pomocą protokołu LISP (Locator ID Separation Protocol)
    5. eksport dodatkowych pól w ramach statystyk NetFlow niezbędnych do analizy zagrożeń w ruchu zaszyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)
    6. rozszerzona współpraca z wybranymi urządzeniami Intel i Samsung pozwalająca na widoczność informacji takich jak: typ i model urządzenia, wersja oprogramowania, system operacyjny, RSSI najbliższych AP
    7. obsługa Wireless IDS/IPS pozwalająca na wykrywanie ataków na sieci bezprzewodowe w oparciu o sygnatury, takie jak: Auth/De-Auth Flood, Assoc/Dis-Assoc Flood, Broadcast Probe Flood, Broadcast Dis-Assoc Flood, Broadcast De-Auth Flood, EAPOL-Logoff Attack, CTS Flood, RTS Assoc Request, De-Auth Flood by Pair, Fuzzed Beacon, Fuzzed Probe Request/Response, PS Poll Flood, EAPOL Start Flood, Re-Assoc Request Flood by Destination, Beacon Flood, Probe Response Flood by Destination, Airdrop Session, Block Ack Flood, Malformed Assoc Request, Malformed Auth, RTS/CTS Virtual Carrier Sense Attack
    8. możliwość przechwycenia i wysłania materiału dowodowego wywołującego alarm IDS/IPS (packet capture) do dedykowanego systemu zarządzania
    9. logowanie alarmów IDS/IPS za pomocą syslog
    10. współpraca z oprogramowaniem i urządzeniami realizującymi usługi lokalizacyjne, obsługa tagów telemetrycznych

Parametry techniczne – AP typ 1

1) Obsługa standardów IEEE 802.11a/b/g/n/ac/ax
    1. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
    2. obsługa MU-MIMO – 4x4:4 (w 2,4 GHz oraz 5 GHz)
    3. obsługa kanałów 20, 40 MHz dla 802.11n
    4. obsługa kanałów 20, 40, 80,160 MHz dla 802.11ac/ax
    5. obsługa prędkości PHY do 3,4 Gbps (ac)
    6. obsługa prędkości PHY do 5,3 Gbps (ax)
    7. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    8. obsługa beamforming 802.11 ac/ax
    9. obsługa MRC (Maximal Ratio Combining)
2) Konfigurowalna moc nadajnika
    1. dla zakresu 2.4 GHz: do 100 mW
    2. dla zakresu 5GHz: do 200 mW
3) Praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz
4) Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
    1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
    2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
    3. obsługa 16 BSSID
    4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
    5. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
    6. 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)
    7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
    8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
    9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego pod kątem zagrożeń bezpieczeństwa (wykrywanie obcych AP oraz klientów)
    10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
    11. obsługa IPv6
    12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
    13. obsługa mechanizmów QoS:
        i. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik, per SSID
        ii. obsługa WMM, TSPEC, U-APSD
    14. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM

15. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting
16. wsparcie IEEE 802.11i, WPA2, WPA3
17. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)
18. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS
19. obsługa blokowania ruchu Peer-to-Peer

5) Funkcjonalności oprogramowania
    1. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
    2. obsługa aWIPS (Adaptive Wireless Intrusion Prevention System) polegająca na wykryciu i remediacji zagrożenia. AP będący częścią systemu WIPS pozwala na określenie m.in. następujących informacji: sygnatura ataku, rodzaj wykrytej anomalii i jej opis, czas zdarzenia
        i. wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOL Logoff Flood
        ii. wykrywanie ataków: EAPOL-Logoff, RTS/CTS Virtual Carrier Sense
    3. obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag)
    4. uruchamianie aplikacji w kontenerach bezpośrednio na AP
    5. obsługa VXLAN
6) Wbudowana funkcjonalność wykrywająca zakłócenia na obsługiwanym kanale radiowym (w pasmach 2,4 oraz 5 GHz), typu: kuchenka mikrofalowa, continuous wave (rejestrator AV, elektroniczna niańka), SI-FHSS (urządzenia Bluetooth, DECT)
7) Interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz
8) Interfejs konsoli RJ45
9) port USB 2.0
10) Dwa porty RJ-45
11) 2 GB RAM, 1 GB Flash
12) Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at), możliwość uruchomienia AP z wykorzystaniem PoE (802.3af) z ograniczonymi funkcjonalnościami (m.in.: redukcja układów radiowych do trybu 2x2)
13) Anteny zintegrowane o zysku 3 dBi dla pasma 2,4 GHz oraz 4 dBi dla pasma 5 GHz
14) Urządzenie przystosowane do pracy w zakresie temperatur 0 – 50^0C
15) Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
16) Certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi 6, Wi-Fi Enhanced Open, WMM, WMM-PS lub równoważne
17) Wbudowane radio Bluetooth Low Energy (BLE) 5.0.

Parametry techniczne – AP typ 2

1) Obsługa standardów IEEE 802.11a/b/g/n/ac/ax
    1. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring
    2. obsługa MU-MIMO –4x4:4 (w 2,4 GHz oraz 5 GHz)
    3. obsługa kanałów 20, 40 MHz dla 802.11n
    4. obsługa kanałów 20, 40, 80,160 MHz dla 802.11ac/ax
    5. obsługa prędkości PHY do 3,4 Gbps (ac)
    6. obsługa prędkości PHY do 5,3 Gbps (ax)
    7. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    8. obsługa beamforming 802.11 ac/ax
    9. obsługa MRC (Maximal Ratio Combining)
2) Konfigurowalna moc nadajnika
    1. dla zakresu 2.4 GHz: do 100 mW
    2. dla zakresu 5GHz: do 200 mW
3) Praca dwuzakresowa w pasmach: 2,4 GHz oraz 5 GHz
4) Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
    1. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN
    2. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany)
    3. obsługa 16 BSSID
    4. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID
    5. 1uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w
    6. 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)
    7. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników
    8. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
    9. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego pod kątem zagrożeń bezpieczeństwa (wykrywanie obcych AP oraz klientów)
    10. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h
    11. obsługa IPv6
    12. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r
    13. obsługa mechanizmów QoS:
        i. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik, per SSID
        ii. obsługa WMM, TSPEC, U-APSD
    14. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM

15. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting
16. wsparcie IEEE 802.11i, WPA2, WPA3
17. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP)
18. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS
19. obsługa blokowania ruchu Peer-to-Peer

5) Funkcjonalności oprogramowania:
    1. analiza ruchu pozwalająca na identyfikację, klasyfikację na poziomie aplikacji w warstwie 7 (rozpoznawanie ponad 1000 aplikacji) oraz kontrolę tych aplikacji (limitowanie, markowanie, dropowanie)
    2. obsługa aWIPS (Adaptive Wireless Intrusion Prevention System) polegająca na wykryciu i remediacji zagrożenia. AP będący częścią systemu WIPS pozwala na określenie m.in. następujących informacji: sygnatura ataku, rodzaj wykrytej anomalii i jej opis, czas zdarzenia
        i. wykrywanie sygnatur DoS: Auth/Deauth Flood, Assoc/Disassoc Flood, CTS/RTS Flood, Broadcast Deauth/Dissassoc Flood, Broadcast Probe Flood, EAPOL Logoff Flood
        ii. wykrywanie ataków: EAPOL-Logoff, RTS/CTS Virtual Carrier Sense
    3. obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag)
    4. uruchamianie aplikacji w kontenerach bezpośrednio na AP
    5. obsługa VXLAN
6) Wbudowana funkcjonalność wykrywająca zakłócenia na obsługiwanym kanale radiowym (w pasmach 2,4 oraz 5 GHz), typu: kuchenka mikrofalowa, continuous wave (rejestrator AV, elektroniczna niańka), SI-FHSS (urządzenia Bluetooth, DECT)
7) Interfejs MultiGigabit Ethernet (100/1000/2500) zgodny z IEEE 802.3bz
8) Interfejs konsoli RJ45
9) Port USB 2.0
10) Dwa porty RJ-45
11) 2 GB RAM, 1 GB Flash
12) Pełna funkcjonalność AP przy zasilaniu przez PoE+ (IEEE 802.3at), możliwość uruchomienia AP z wykorzystaniem PoE (802.3af) z ograniczonymi funkcjonalnościami (m.in.: redukcja układów radiowych do trybu 2x2)
13) Wyposażony w złącza dla anten zewnętrznych
14) Urządzenie przystosowane do pracy w zakresie temperatur -40 – 60^0C
15) Diodowa sygnalizacja stanu urządzenia z możliwością deaktywacji
16) Certyfikacja WiFi Alliance: Wi-Fi a/b/g/n/ac, Wi-Fi 6, Wi-Fi Enhanced Open, WMM, WMM-PS
17) Wbudowane radio Bluetooth Low Energy (BLE) 5.0.