**Przełącznik Typ 1**

1. Przełącznik posiada:
   1. 48 portów 1/10/25G definiowanych za pomocą wkładek SFP/SFP+
   2. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m)
2. Parametry wydajnościowe:
   1. Prędkość przełączania wirespeed dla wszystkich portów
   2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
   3. 32GB DRAM
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   1. Trunking IEEE 802.1Q VLAN
   2. Wsparcie dla 3000 sieci VLAN
   3. Wsparcie sprzętowe dla 250 000 adresów MAC
   4. IEEE 802.1w Rapid Spanning Tree (RST)
   5. IEEE 802.1s Multiple Spanning Tree (MST)
   6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   7. Internet Group Management Protocol (IGMP) Versions 2, 3
   8. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad
   10. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów)
   11. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   12. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   1. Sprzętowe przełączanie pakietów w warstwie L3
   2. Routing w oparciu o trasy statyczne
   3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6
   4. Policy Based Routing (PBR)
   5. VRRP lub HSRP
   6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
   7. Wsparcie sprzętowe dla minimum 750 000 prefixów LPM/ wpisów hosta w tablicy routingu IP
   8. Wsparcie dla 1000 VRF
   9. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP)
   10. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   11. Wsparcie dla IGMPv3 oraz MSDP
   12. Wsparcie sprzętowe dla 32.000 tras multicastowych
   13. Obsługa 5000 wpisów dla ACL (access control list)
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   1. Zintegrowany, sprzętowy VXLAN Bridging/Routing
   2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   3. Implementacja VXLAN BGP EVPN (Ethernet VPN)
   4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
   5. Mechanizm wykrywania i zapobiegania efektom pętli w podłączone infrastrukturze L2 poprzez mechanizm VXLAN OAM
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   1. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   2. Klasyfikacja QoS w oparciu o listy ACL (Access Control List) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   3. Kolejkowanie bezwzględne (strict-priority)
   4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   5. Ograniczanie ruchu (policing) do zadanej przepływności
   6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
   8. Protokół RDMA/RoCE oraz ECN
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   1. Obsługa list kontroli dostępu (ACL)
   2. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu
   3. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP)
   4. ACL oparte o porty (PACL)
   5. DHCP Snooping
   6. ARP Inspection
   7. IP Source Guard
   8. Unicast reverse path forwarding (uRPF)
   9. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
   10. Możliwość rozszerzenia funkcjonalności (poprzez zakup odpowiedniej licencji) o wsparcie dla MACSEC na wszystkich portach
   11. Możliwość rozszerzenia funkcjonalności (poprzez zakup odpowiedniej licencji) o wsparcie dla szyfrowania AES 256 w warstwie overlay (VTEP do VTEP - tunel VXLAN)
8. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   1. Port zarządzający 100/1000 Mbps
   2. Port konsoli CLI
   3. Zarządzanie In-band
   4. SSHv2
   5. Authentication, authorization, and accounting (AAA)
   6. RADIUS
   7. TACACS+
   8. Syslog
   9. SNMP v1, v2c, v3
   10. Role-Based Access Control RBAC
   11. IEEE 802.1ab LLDP
   12. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   13. 802.1x
   14. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   15. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   16. Pełen Netflow v9
   17. Network Time Protocol (NTP)
   18. Precision Time Protocol IEEE 1588
   19. Diagnostyka procesu BOOT
   20. Ping
   21. Traceroute
   22. Zgodność z wykorzystywanym oprogramowaniem zarządzającym Cisco APIC,
9. Możliwość rozszerzenia funkcjonalności (poprzez zakup odpowiedniej licencji) o telemetrię z control/data plane eksportowaną w interwałach co najmniej 100 milisekund bezpośrednio z układu ASIC przełącznika. Wsparcie dla narzędzi programistycznych w standardzie „OpenTelemetry”. Eksportowane dane w formacie gRPC lub GPB dostarczają następujące informacje (dla każdego przepływu/flow):
   1. Informacji o przepływie (flow), zawierają dane o adresach IP, protokołach, portach, kiedy przepływ się rozpoczął, jak długo przepływ był aktywny, ile było w nim sumarycznie danych itp.
   2. Zmienność między pakietami, daje wgląd w zmiany pomiędzy pakietami w danym przepływie. Przykłady obejmują zmiany czasu życia (TTL), flagi IP i TCP, długość payload itp.
   3. Szczegóły kontekstu przepływu, informacje te są uzyskiwane poza nagłówkiem pakietu, w tym zmiany w wykorzystaniu bufora kolejki, powód odrzucania pakietów w przepływie (bufor, routing, ACL), powiązanie z końcami tunelu VXLAN (VTEP) itp.
   4. Dodatkowo funkcjonalność telemetrii pozwalająca na pozyskanie metadanych o każdym przepływie, który spełnia określone kryteria (np. odrzucenie, opóźnienie, microburst) z dodatkowymi informacjami identyfikującymi przyczynę (np. ACL/routing/bufor drop, opóźnienie dla scieżki, wystąpienie microburst itp.)
10. Narzędzia programowania i zarządzania przełącznikiem:
    1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
    2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
    3. Wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika
    4. Interfejs programistyczny REST API wraz z upublicznionym SDK
    5. Możliwość zainstalowania klienta Chef
    6. Możliwość zainstalowania agenta Puppet
11. Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony zasilaczy
12. Obudowa o rozmiarach 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”
13. Urządzenie dostarczane z licencją wieczystą (perpetual) zapewniającą pracę z opisanymi powyżej funkcjonalnościami
14. Urządzenie musi posiadać gwarancję producent na okres 36 miesięcy w standardzie NBD
15. Wyposażenie przełącznika obejmuje:
    1. Cisco Cisco QSFP-40G-SR4-S x 6 sztuk per urządzenie

**Przełącznik Typ 2**

1. Przełącznik musi posiadać: 48 portów 100M/1G/2.5G/5GBaseT RJ-45 UPoE (do 60W per port)
2. Przełącznik musi posiadać moduł uplinkowy 2x 25G
3. Przełącznik musi zapewnić moc dostępną dla portów PoE:
   1. 645W (z jednym zasilaczem o mocy 1100W),
   2. 645W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie redundantnym),
   3. 1745W (z dwoma zasilaczami o mocy 1100W pracującymi w układzie współdzielenia mocy)
4. Przełącznik musi posiadać slot na moduł rozszerzeń (dający możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
   1. 4x1G SFP
   2. 8x1/10G SFP/SFP+
   3. 2x40G QSFP
   4. 2x25G SFP28
   5. 4x100M/1G/2.5G/5G/10GBaseT RJ-45
5. Przełącznik musi posiadać porty SFP/SFP+/SFP28/QSFP możliwe do obsadzenia następującymi rodzajami wkładek:
   1. Porty SFP:
      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
   2. Porty SFP/SFP+:
      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-LRM,
      10. 10Gigabit Ethernet 10GBase-ER,
      11. 10Gigabit Ethernet 10GBase-ZR,
      12. 10Gigabit Ethernet 10GBase-BX-D/U,
      13. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
   3. Porty SFP/SFP+/SFP28:
      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 10GBase-BX-D/U,
      12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
      13. 25Gigabit Ethernet 25GBASE-SR,
      14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28)
      15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF)
      16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF)
   4. Porty QSFP:
      1. 40G-SR4,
      2. 40G-LR4,
      3. 40G-ER4,
      4. 40G-SR-BD,
      5. adapter 40G QSFP->10G SFP+
      6. kable twinax
6. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
   1. Min. przepustowość w ramach stosu - 480Gb/s,
   2. Min. 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. 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),
   6. 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),
7. Wymagania w zakresie zasilania i chłodzenia:
   1. Przełącznik musi posiadać redundantne i wymienne moduły wentylatorów,
   2. Przełącznik musi posiadać możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze muszą być wymienne (i mieć możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
   3. Przełącznik musi umożliwiać podtrzymanie zasilania z portów PoE podczas restartu urządzenia,
   4. W przypadku wyłączenia przełącznika np. w wyniku zaniku zasilania, przełącznik musi umożliwiać przywrócenie zasilania PoE do zasilanego urządzenia PD (powered device) w czasie nie dłuższym niż 30 sekund od włączenia przełącznika (od powrotu zasilania przełącznika),
   5. Przełącznik musi wspierać IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),
8. Wymagania w zakresie parametrów wydajnościowych:
   1. Szybkość przełączania musi zapewnić pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):
      1. Przepustowość przełącznika (switching capacity) musi wynosić min.: 640 Gb/s (bez podłączenia do stosu), 1120 Gb/s (z podłączeniem do stosu)
      2. Prędkość przesyłania (forwarding rate) musi wynosić min.: 476.19 Mpps (bez podłączenia do stosu), 833.33 Mpps (z podłączeniem do stosu)
   2. Pojemność buforu pakietów musi wynosić mi.n. – 32MB
   3. Min. 8 GB pamięci DRAM
   4. Pamięć flash – min. 16GB
   5. Przełącznik musi zapewnić obsługę:
      1. 1000 aktywnych sieci VLAN
      2. 32000 adresów MAC
      3. 8000 tras IPv4
      4. 4000 tras IPv6
      5. 5000 wpisów w listach kontroli dostępu Security ACL
      6. 5000 wpisów w listach kontroli dostępu QoS ACL
      7. 1000 interfejsów SVI L3
      8. 128 interfejsów L3
      9. Jumbo frame 9198B
      10. 128 połączeń zagregowanych typu „port channel”
      11. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
9. Przełącznik musi umożliwiać obsługę protokołu NTP
10. Przełącznik musi obsługiwać IGMPv1/2/3 i MLDv1/2 Snooping
11. Przełącznik musi wspierać 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. Obsługę 128 instancji protokołu STP
    5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
    6. Redundancję połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności linku podstawowego
12. Przełącznik musi wspierać obsługę protokołu LLDP (IEEE 802.1ab) i LLDP-MED
13. Urządzenie musi realizować funkcję 802.1Q tunneling (QinQ)
14. Urządzenie musi umożliwiać realizacje funkcjonalności Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
15. Urządzenie musi obsługiwać funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
16. Urządzenie musi posiadać możliwość uruchomienia funkcji serwera DHCP
17. Urządzenie musi posiadać mechanizmy związane z bezpieczeństwem sieci:
    1. Wpoziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
    2. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
    3. Autoryzację użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
    4. Obsługę 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. Obsługę 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:
        1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
        2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
        3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    14. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
    15. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
    16. Musi realizować funkcję 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),
18. Przełącznik musi obsługiwać mechanizmy zapewaniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
    2. bezpieczną sekwencję uruchamiania,
    3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
19. Przełącznik musi obsługiwać mechanizmy związane z zapewnieniem jakości usług w sieci:
    1. Musi umożliwiać implementację 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    2. Musi umożliwiać implementację algorytmu Shaped Round Robin dla obsługi kolejek,
    3. Musi posiadać 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;
20. Przełącznik musi umożliwiać obsługę min. następujących protokołów i mechanizmów routingu:
    1. Routing statyczny dla IPv4 i IPv6,
    2. Routing dynamiczny – RIP, OSPF,
    3. Routing dynamiczny zaawansowany - IS-IS, BGP dla IPv4 i IPv6,
    4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,
    5. Multicast Source Discovery Protocol (MSDP),
    6. Policy-based routing (PBR),
    7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
    8. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);
21. Przełącznik musi umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
22. Przełącznik musi posiadać wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),
23. Przełącznik musi posiadać funkcjonalność sondy IP SLA Responder,
24. Przełącznik musi wspierać obsługę dla protokołu OpenFlow 1.3,
25. Przełącznik musi posiadać funkcjonalność Time Domain Reflectometer (TDR) umożliwiającą wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,
26. Wymagania w zakresie zarządzania:
    1. Urządzenie musi być wyposażone w port konsoli,
    2. Urządzenie musi posiadać dedykowany port Ethernet do zarządzania out-of-band,
    3. Urządzenie musi mieć 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 muszą być możliwe 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. Urządzenie musi zapewniać możliwość obsługi protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
    6. Urządzenie musi posiadać wsparcie dla protokoły RESTCONF,
    7. Urządzenie musi posiadać wsparcie dla protokołu gNMI,
    8. Przełącznik musi posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
    9. Urządzenie musi posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć uruchomienia z nośnika danych umieszczonego w porcie USB;
    10. Urządzenie musi posiadać możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności min. 120GB;
    11. Urządzenie musi posiadać funkcję 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,
27. Wymagania w zakresie parametrów fizycznych:
    1. Urządzenie musi być możliwe do zamontowania w szafie rack 19”,
    2. Wysokość urządzenia nie może przekraczać 1 RU,
    3. Głębokość chassis urządzenia z wentylatorami, zasilaczami i kablami zasilającymi musi być mniejsza niż 57 cm,
28. Urządzenie musi umożliwiać realizację 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,
29. Przełącznik musi posiadać możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
30. Przełącznik musi posiadać możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,
31. Przełącznik musi zapewniać wsparcie dla protokołu LISP zgodnie z RFC 6830,
32. Przełącznik musi umożliwiać obsługę 256 wirtualnych instancji routingu (VRF),
33. Przełącznik musi zapewniać obsługę protokołu BFD (Bidirectional Forwarding Detection), który umożliwia szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
34. Przełącznik musi umożliwiać realizację funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,
35. Przełącznik musi posiadać możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256) dla 16 pierwszych portów downlinkowych przełącznika i wszystkich portów uplinkowych przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
36. Przełącznik musi posiadać możliwość enkapsulacji ruchu w pakiety VXLAN,
37. Urządzenie musi zapewniać wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności leaf oraz spine,
38. Przełącznik musi posiadać 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, tc-connect, udp-echo, udp-jitter,
39. Przełącznik musi posiadać 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,
40. Przełącznik musi posiadać funkcjonalność bramy dla usług mDNS,
41. Przełącznik musi umożliwiać zdalną obserwację 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),
42. Przełącznik musi zapewniać widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),
43. Przełącznik musi umożliwiać eksport dodatkowych pól 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),
44. Przełącznik musi posiadać wbudowany analizator pakietów,
45. Przełącznik musi posiadać system operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,
46. Urządzenie musi umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
47. Urządzenie musi umożliwiać integrację 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,
48. Urządzenie musi posiadać wsparcie dla Audio Video Bridging (AVB).
49. Wymagania w zakresie wyposażenia urządzenia:
    1. Przełącznik musi być wyposażony w zasilacz redundantny o mocy 1100W,
    2. Przełącznik musi być wyposażony jest w moduł do łączenia w stos data wraz z kablem stakującym o długości min. 50 cm,
    3. Przełącznik musi być wyposażony w kabel o długości min. 30 cm umożliwiający podłączenie do grupy przełączników współdzielących energię elektryczną,
    4. Każdy przełącznik musi być wyposażony w moduł: 2x25G SFP28
    5. Urządzenie musi posiadać gwarancję producent na okres 36 miesięcy w standardzie NBD