**Specyfikacja Istotnych Warunków Zamówienia**

**Opis przedmiotu zamówienia „Modernizacja infrastruktury sieciowej w Centrum Informatyki D-17 Katedry Informatyki WIET AGH”**

# Opis obecnej sieci KI

Sieć komputerowa budynku D-17 została oddana do użytku w roku 2012. Szkielet okablowania zbudowano z użyciem kabli światłowodowych Muliti Mode OC3/XG zakończonych gniazdami MT-RJ XG 50/125/900. Łączą one 8 punktów dystrybucyjnych rozmieszczonych w kluczowych punktach budynku, oraz serwerownię. Pozostałe połączenia pomiędzy punktami dystrybucyjnymi oraz połączenia w obrębie poszczególnych pomieszczeń oparto na okablowaniu miedzianym z kablem PiMF 1200MHz kat. 7a, zakończonym gniazdami kategorii 6e.

Rdzeń sieci składa się z trzech głównych punktów dystrybucyjnych połączonych za pomocą kabli światłowodowych. Do punktów tych dołączone są pozostałe punkty dystrybucyjne oraz punkty dostępowe. Wszystkie elementy sieci o kluczowym znaczeniu mają zapewnioną redundancję sprzętową (układy podwójne przełączników pracujące w konfiguracji Active-Active), oraz odpowiednią redundancję w okablowaniu.

W sieci wyodrębniono następujące warstwy funkcjonalne:

* **Warstwa Core** – z sześcioma urządzeniami Cisco Catalyst C6506-E (VSS) z przełączaniem w technologii MPLS, z redundancją uzyskaną poprzez zwielokrotnienie fizycznych połączeń pomiędzy głównymi punktami szkieletu, oraz zastosowanie przełączników działających w układzie podwójnym. Filtrowanie ruchu zrealizowana na dwóch firewallach ASA5585X.
* **Warstwa Distribution** – z przełącznikami Cisco Catalyst 3750X, w punktach dystrybucyjnych o dużym zagęszczeniu łączonymi w stos.
* **Warstwa Access** – z przełącznikami Cisco Catalyst 2960S, w punktach o większej liczbie urządzeń końcowych, łączonymi w stosy.
* **Warstwa DataCenter** – odrębna infrastruktura obsługująca serwerownię zbudowana na dwóch przełącznikach NEXUS 5548UP oraz dwunastu extenderach NEXUS 2248TP-E.

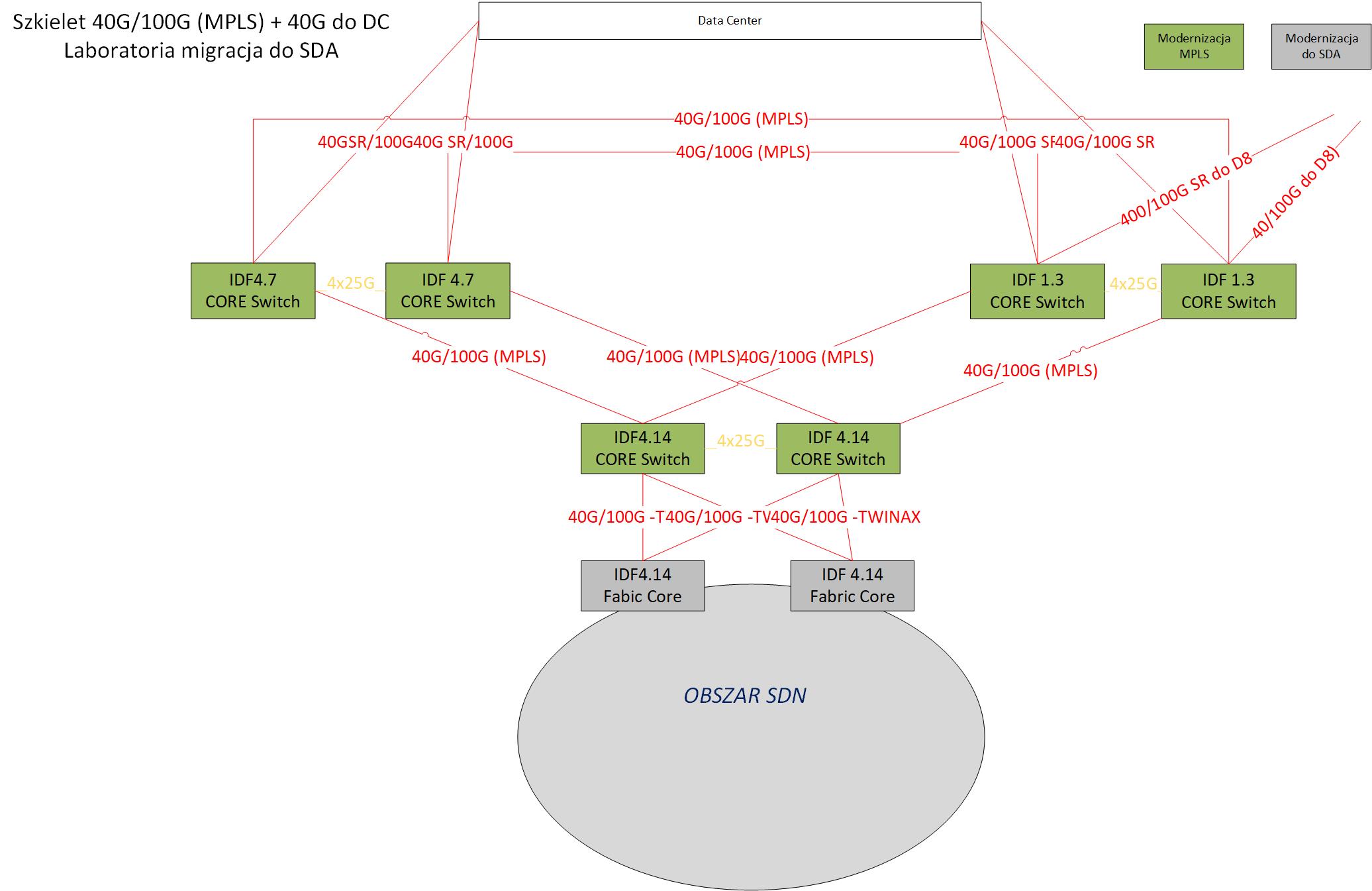
W serwerowni wykorzystywana jest platforma wirtualizacyjna VMware w wersji 6.5 i 6.7.

# Obszary przewidziane do modernizacji

# Modernizacja infrastruktury sieciowej w Centrum Informatyki będąca przedmiotem zamówienia obejmuje następujące obszary:

* Wymiana przełączników na nowe (oznaczone jako Core Switch) w węzłach szkieletowych sieci MPLS tj. IDF 4.7, IDF1.3, IDF4.14.
* Wymiana przełączników w części DC (opisane jako DC CORE).
* Uruchomienie połączeń optycznych szkieletowych pomiędzy wskazanymi IDF z przepustowością 40G lub 100 Gb/s na bazie obecnie eksploatowanych włókien światłowodowych MMF (należy dostarczyć wkładki obsługujące oba standardy i uruchomić najwyższą możliwą przepustowość).
* Podłączenie do przełączników Core Switch istniejącego bloku DC (DC CORE) za pomocą łącza przepustowością 40G lub 100 Gb/s za pomocą wkładek obsługujących obydwa standardy.
* Zmiana technologii dostępu do sieci z laboratoriów studenckich. Obecnie wykorzystywana technologia dostępowa oparta na tradycyjnych przełączanych sieciach VLAN L2/L3 zostanie zastąpiona siecią definiowaną programowo (SDN) opartą o tzw. Network Fabric (opisaną w sekcji 3).
* Podłączenie SDN Network Fabric do szkieletu sieci poprzez połączenia L3 40G lub 100 Gb/s na bazie istniejących połączeń światłowodowych MMF.

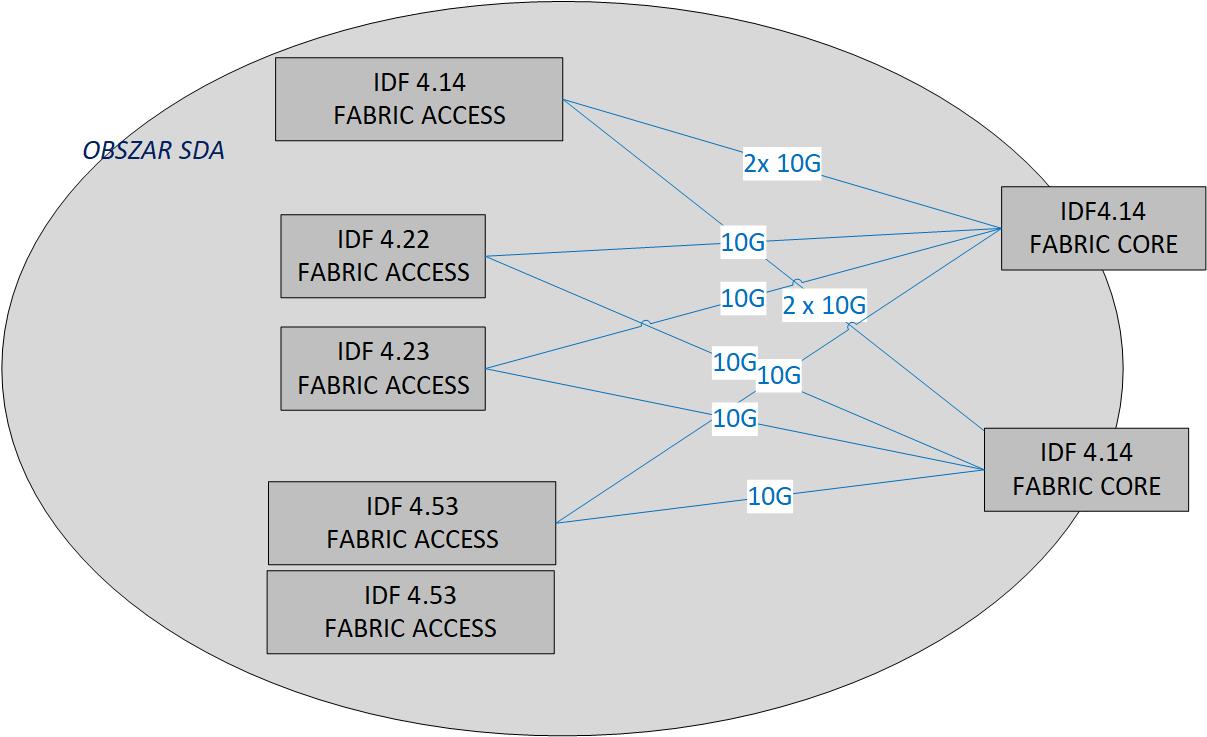
Połączenia sieciowe w sieci po modernizacji przestawione są na poniższych rysunkach.



# Charakterystyka techniczna i funkcjonalna rozwiązania SDN Network Fabric

W prezentowanej koncepcji sieć definiowana programowo SDN Network Fabric składa się z następujących komponentów:

* Przełączniki rdzeniowe określone na rysunku jako FABRIC CORE
* Przełączniki dostępowe, określone na rysunku jako FABRIC ACCESS
* System zarządzania i monitorowania siecią SDN Network Fabric w postaci pojedynczego urządzenia sieciowego – 1 urządzenie wraz z oprogramowaniem i wymaganymi licencjami
* System kontroli dostępu oraz zarządzania politykami bezpieczeństwa w sieci SDN Network Fabric w postaci dwóch maszyn wirtualnych pracujących w środowisku zwirtualizowanym VMware – 2 maszyny wirtualne wraz z wymaganymi licencjami
* Komponenty zarządzające i monitorujące sieć SDN powinny być zainstalowane w części DC, zasoby pod maszyny wirtualne – zostaną zapewnione przez zamawiającego.



## Opis funkcjonalny SDN Network Fabric:

Funkcjonalności podstawowe:

* Programowalność urządzeń sieciowych wchodzących w skład SDN Network Fabric
* Mechanizm sieci podkładowej (transport dla usług sieciowych) oraz nakładkowej (warstwa, gdzie definiowane są usługi sieciowe: segmentacja, wymuszanie polityki bezpieczeństwa)
* Scentralizowane tworzenie logicznej segmentacji i polityki bezpieczeństwa w sieci
* Automatyczne udostępnienie urządzeń tworzących sieć
* Centralny system zarządzania i monitorowania umożliwiający centralne programowanie urządzeń oraz centralny monitoring i analizę danych telemetrycznych z sieci w celu wykrywania nieprawidłowości w jej działaniu
* Zautomatyzowane wykrywanie urządzeń sieciowych przez system zarządzania i monitorowania
* Zarządzanie wersjami oprogramowania wraz ze wskazaniem wersji głównych
* Monitoring sieci i wizualizacja dla poszczególnych urządzeń sieciowych, użytkowników oraz aplikacji

## Funkcjonalności dodatkowe (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

Segmentacja sieci i tworzenie polityk bezpieczeństwa:

* 1. Centralne zarządzanie polityką bezpieczeństwa poprzez określenie relacji pomiędzy segmentami logicznymi w sieci (grupami urządzeń, użytkowników lub aplikacji) z możliwością tworzenia filtrów (prześlij, blokuj, prześlij selektywnie, blokuj selektywnie, prześlij i skopiuj do wskazanego miejsca) dla wymiany ruchu pomiędzy tymi grupami wraz z możliwością wskazania typu ruchu np. protokoły sieciowe (TCP, UDP), porty, typy aplikacji identyfikowane w warstwie L7
  2. Filtrowanie ruchu niezależne od adresacji IP w oparciu o rolę użytkownika lub urządzenia w sieci i zdefiniowane relacje
  3. Logiczny podział sieci na wiele sieci wirtualnych (VN) rozumianych, jako domeny routingowe z pełną separacją ruchu pomiędzy VN
  4. Logiczny podział użytkowników i urządzeń na grupy wg. kryteriów takich jak:
* Typ urządzenia
* Użytkownik wykorzystujący urządzenie (uwierzytelnienie użytkownika 802.1x lub poprzez formularz WWW)
* Adres MAC urządzenia
* Rodzaj urządzenia np. drukarka, telefon IP itd.
* Czas dnia
* Miejsce i sposób podłączenia
  1. Możliwość filtrowania ruchu pomiędzy urządzeniami pracującymi w jednej grupie logicznej i/lub podsieci IP jak również pomiędzy różnymi grupami logicznymi i/lub podsieciami IP bez konieczności stosowania filtrów ruchu opartych o adresy IP

Zasady działania:

1. Możliwość tworzenia podsieci IP rozciągniętej na dowolne porty dostępowe w ramach Network Fabric
2. Mobilność adresu IP urządzenia końcowego w obrębie Network Fabric
3. Eliminacja mechanizmów L2 oraz protokołu spanning tree z sieci podkładowej
4. Możliwość tworzenia nakładkowych sieci L3 i L2 bez konieczności używana sieci VLAN

Automatyzacja:

1. Automatyzacja procesu tworzenia sieci Network Fabric (dodawanie urządzeń, przypisywanie im roli w sieci, określanie poziomów uwierzytelnienia użytkowników i urządzeń na brzegu sieci) bez konieczności używania linii komend (CLI) i bez konieczności indywidualnego „urządzenie po urządzeniu” konfigurowania sieci

## System zarządzania i monitorowania siecią SDN Network Fabric:

### Funkcjonalności podstawowe:

* Graficzny interfejs do zarządzania i monitorowania sieci kampusowej oraz do tworzenia logicznej segmentacji i polityki bezpieczeństwa w sieci
* Inwentaryzacja urządzeń oraz oprogramowania
* Zarządzanie wersjami oprogramowania
* Narzędzie do wizualizacji topologii
* Wykrywanie urządzeń sieciowych
* Monitoring dostępności i osiągalności urządzeń sieciowych
* Szczegółowe informacje o urządzeniu sieciowym takie jak: typ, wersja oprogramowania, adres IP, lokalizacja, obciążenie CPU, wykorzystanie pamięci, temperatura, dostępność interfejsów, obciążenie interfejsów

### Funkcjonalności dodatkowe (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

* Generowanie automatycznych komunikatów o stwierdzonych nieprawidłowościach w pracy sieci wraz z sugestią przyczyny, sposobu rozwiązania problemu oraz dalszych kroków diagnostycznych dla poszczególnych urządzeń sieciowych
* Narzędzie do śledzenia ścieżki dla danego ruchu w sieci np. w relacji pomiędzy dwoma hostami wraz podaniem informacji o wszystkich węzłach na ścieżce
* Szczegółowe informacje o użytkowniku końcowym takie jak:
  1. identyfikator użytkownika,
  2. nazwa urządzenia końcowego na którym pracuje, adresy MAC oraz IP tego urządzenia,
  3. typ urządzenia końcowego,
  4. opis urządzenia, do którego jest podłączone urządzenie końcowe wykorzystywane przez użytkownika,
  5. informacje o generowanym ruchu sieciowym per wykorzystywana aplikacja: nazwa aplikacji, ilość ruchu (w bajtach), średnia przepustowość (w b/s), straty pakietów, opóźnienie sieciowe
* Szczegółowe informacje o aplikacjach wykorzystywanych w sieci takie jak: lista wszystkich wykrytych aplikacji z podaniem nazw aplikacji, klas ruchu, ilości ruchu generowanego, średniej przepustowości, straty pakietów, opóźnienia sieciowego
* Obsługa REST API

## System kontroli dostępu do SDA Network Fabric:

System kontroli dostępu obejmuje oprogramowanie i licencje na dwie maszyny wirtualne oraz 125 permanentnych licencji bazowych (uwierzytelnienie podstawowe) oraz 125 3-letnich licencji dodatkowych (profilowanie stacji, wykrywanie typu stacji, współpraca z systemem zarządzania i monitoringu sieci SDN Network Fabric).

### Funkcjonalności podstawowe:

* Uwierzytelnienie i kontrola dostępu dla sieci LAN niezależnie od miejsca uzyskiwania dostępu przez urządzenie końcowe
* Centralna kontrola dostępu do sieci z komputerów typu PC, smartfonów i tabletów, telefonii, terminali video, urządzeń BYOD (Bring Your Own Device) oraz wszystkich pozostałych urządzeń podłączonych do sieci
* Wysoka dostępność elementów funkcjonalnych systemu, w tym:

1. redundancja 1:1 dla elementu funkcjonalnego zarządzania (Administration),   
   czyli jego zdublowanie
2. redundancja 1:1 dla elementu funkcjonalnego logowania i rozwiązywania problemów   
   (Monitoring and Troubleshooting), czyli jego zdublowanie
3. zapewnienie ciągłości obsługi uwierzytelnień stacji końcowych za pomocą mechanizmu redundancji grup serwerów RADIUS konfigurowanych na urządzeniach dostępowych (Network Access Devices, NAD)

* Obsługa następujących protokołów i standardów uwierzytelniania:
  1. RADIUS
  2. RADIUS Proxy dla zewnętrznego serwera RADIUS
  3. Protokół Windows Active Directory
  4. Protokół Lightweight Directory Access Protocol (LDAP)
* Obsługa następujących protokołów uwierzytelniania:
  1. PAP/ASCII
  2. CHAP
  3. MS-CHAPv1
  4. MS-CHAPv2
  5. EAP-MD5
  6. LEAP
* Uwierzytelnianie maszyn i użytkowników zgodne ze standardem IEEE 802.1X
* Obsługa implementacji standardu IEEE 802.1X z następującymi suplikantami:
  1. Wbudowanym klientem 802.1X dla Windows Vista
  2. Wbudowanym klientem 802.1X dla Windows 7
  3. Wbudowanym klientem 802.1X dla Windows 8 i 8.1
  4. Wbudowanym klientem 802.1X dla Windows 10
  5. Google Android w wersji 6 lub nowszych
* Tworzenie polityk uwierzytelniania oraz kontroli dostępu zgodnych z IEEE 802.1X opartych o złożone reguły
* Uwierzytelnianie w oparciu o lokalną bazę stacji końcowych, którą można tworzyć per stacja końcowa na podstawie unikalnego adresu MAC
* Uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC za pomocą mechanizmu MAB (MAC Authentication Bypass)

### Funkcjonalności dodatkowe (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

Uwierzytelnienie:

* + Uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, która może być stosowana, jako metoda zastępcza w sytuacji, gdy stacja ma niepoprawnie skonfigurowany lub niedziałający suplikant 802.1X
  + Zapewnienie funkcjonalności centralnego portalu uwierzytelniania web (CWA – Central Web Authentication) na serwerach systemu

API:

* + Obsługa RESTful API opartego o HTTPS, dla następujących operacji:
  1. zarządzanie sesjami obsługiwanymi przez system
  2. zarządzanie operacją CoA (Change of Authorization) dla uwierzytelnionych sesji

Segmentacja logiczna sieci:

* + Mechanizm bezpiecznej segmentacji logicznej sieci w oparciu o znaczniki bezpieczeństwa
  + Możliwość przypisania stacji lub użytkownika do grupy bezpieczeństwa (przypisania znacznika bezpieczeństwa) w procesie uwierzytelnienia i kontroli dostępu 802.1X
  + Możliwość konfiguracji filtrowania ruchu za pomocą znaczników bezpieczeństwa
  + Wizualizacja polityki bezpieczeństwa w systemie zarządzania

Profilowanie stacji sieciowych:

* + Profilowanie stacji końcowych i realizacja zróżnicowanej polityki bezpieczeństwa na podstawie zidentyfikowanych typów
  + Profilowanie stacji końcowych poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, HTTP, RADIUS, NMAP, DNS, SNMP QUERY, SNMP TRAP

Skalowalność:

* System umożliwia zwiększenie ilości równocześnie obsługiwanych stacji końcowych do 10000,   
  z wykorzystaniem dwóch maszyn wirtualnych poprzez zwiększenie mocy tych maszyn i ewentualny zakup dodatkowych licencji.

# Infrastruktura niezbędna do zrealizowania założeń projektowych

Infrastruktura bazuje na przełącznikach rdzeniowych i dostępowych, które podzielone zostały na kilka kategorii:

* Przełączniki rdzeniowe dla MPLS: Core Switch
* Przełączniki rdzeniowe dla SDN Network Fabric: Fabric Core
* Przełączniki dostępowe dla SDN Network Fabric: Fabric Access
* Przełączniki datacenter: DC Core
* Moduły optyczne i akcesoria dodatkowe do realizacji połączeń: 10Gb/s, 40 Gb/s lub 100 Gb/s

## Przełączniki MPLS Core Switch

### Funkcjonalności podstawowe przełącznika MPLS CORE Switch:

* Przełącznik typu standalone wyposażony w 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+ oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP
* Porty SFP/SFP+ umożliwiają zastosowanie następujących modułów interfejsowych:
  1. Dla transmisji 1Gb/s (SFP):
* 1000Base-SX,
* 1000Base-LX/LH,
* 1000Base-EX,
* 1000Base-ZX,
* 1000Base-BX;
  1. Dla transmisji 10Gb/s (SFP+):
* 10GBase-SR,
* 10GBase-LR,
* 10GBase-ZR,
* 10GBase-ER;
  1. Dla transmisji 25Gb/s:
* 25GBASE-SR
* Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych:
  1. Dla transmisji 40Gb/s:
* 40GBASE-LR4
* 40GBASE-ER4
* 40GBASE-SR4
* 40GBASE-BIDI
  1. Dla transmisji 100Gb/s:
* 100GBASE-SR4
* 100GBASE-LR4
* 100GBASE-CWDM4
* 100GBASE-BIDI
* Urządzenie jest wyposażone w wymienne moduły wentylatorów
* Urządzenie jest wyposażone w zasilacz redundantny do pracy w trybie 1:1
* Urządzenie posiada 32MB bufor pamięci per ASIC
* Wydajność przełączania co najmniej 3.2 Tbps full duplex dla pakietów co najmniej 187 bajtowych
* Wydajność przesyłania 1 Miliard pps
* Obsługa:
  1. co najmniej 1000 sieci VLAN
  2. co najmniej 80 000 adresów MAC
  3. co najmniej 212 000 tras IPv4
  4. co najmniej 212 000 tras IPv6
  5. co najmniej 27 000 wpisów w listach kontroli dostępu Security ACL
  6. co najmniej 16 000 wpisów w listach kontroli dostępu QoS ACL
  + Obsługa protokołu NTP
  + Obsługa IGMPv1/2/3
  + Obsługa następujących mechanizmów związanych 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 minimum 128 instancji protokołu STP
  + Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED
  + Funkcja serwera DHCP
  + Obsługa 3 poziomów dostępu administracyjnego poprzez konsolę
  + Możliwość zalogowania się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
  + Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
  + Obsługa następujących mechanizmów związanych z zapewnieniem jakości usług w sieci:
  1. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  2. implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
  3. możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych,
  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). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik
  6. kontrola burz 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
  + Obsługa następujących mechanizmów routingu statycznego i dynamicznego:
  1. dla IPv4: OSPF, BGP, ISIS
  2. dla IPv6: OPSFv3,
  3. policy-based routing,
  4. routing dla transmisji grupowej: PIM-SM, PIM-SSM
  + Obsługa następujących funkcjonalności z zakresu MPLS:
  1. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC
  2. L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji L3 VPN - MPLS Virtual Private Network (VPN)
  3. Multicast VPN (MVPN)
  + Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi 98 000.
  + Dedykowany port Ethernet do zarządzania out-of-band
  + Port konsoli USB
  + Obsługa protokołów SNMPv3, SSHv2, SCP, HTTPS, syslog – z wykorzystaniem protokołów IPv4 i IPv6
  + Możliwość montażu w szafie rack 19”, wysokość urządzenia - 1 RU

### Funkcjonalności dodatkowe (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

* + Obsługa standardu 802.1AE (szyfrowanie ruchu) 256-bit z prędkością line rate dla każdego z interfejsów
  + System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania urządzenia
  + Wsparcie sprzętowe do łączenia w klaster z drugim takim samym urządzeniem (tzw. virtual stack) - urządzenia w klastrze zachowują się jak jedno urządzenie w punktu widzenia protokołów L2 i L3
  + System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
  + Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
  + Urządzenie posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
  + Obsługa następujących dodatkowych funkcjonalności z zakresu MPLS:

1. IPv6 Provider Edge over MPLS (6PE)
2. IPv6 VPN Provider Edge over MPLS (6VPE)
3. Współpraca z mechanizmem MACSEC (802.1AE), czyli możliwość szyfrowania przy pomocy połączeń MPLS

## Przełączniki Fabric

### Przełączniki rdzeniowe Fabric Core

* Przełącznik typu standalone wyposażony w 24 porty 1/10/25 Gigabit Ethernet SFP/SFP+ oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP
* Porty SFP/SFP+ umożliwiają zastosowanie następujących modułów interfejsowych:
  1. Dla transmisji 1Gb/s (SFP):
* 1000Base-SX,
* 1000Base-LX/LH,
* 1000Base-EX,
* 1000Base-ZX,
* 1000Base-BX;
  1. Dla transmisji 10Gb/s (SFP+):
* 10GBase-SR,
* 10GBase-LR,
* 10GBase-ZR,
* 10GBase-ER;
  1. Dla transmisji 25Gb/s:
* 25GBASE-SR
* Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych:
  1. Dla transmisji 40Gb/s:
* 40GBASE-LR4
* 40GBASE-ER4
* 40GBASE-SR4
* 40GBASE-BIDI
  1. Dla transmisji 100Gb/s:
* 100GBASE-SR4
* 100GBASE-LR4
* 100GBASE-BIDI
* Architektura:
  1. Urządzenie jest wyposażone w wymienne moduły wentylatorów
  2. Urządzenie może zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1
* Wydajność:
  1. Urządzenie posiada 32MB bufor pamięci per ASIC
  2. 16GB pamięci DRAM i 16GB pamięci flash
  3. Wydajność przełączania 1600 Gbps full duplex
  4. Wydajność przesyłania 1 Miliard pps
  5. Obsługa:
  6. 1000 sieci VLAN
  7. 80 000 adresów MAC
  8. 212 000 tras IPv4
  9. 212 000 tras IPv6
  10. Ilość wpisów w listach kontroli dostępu Security ACL – 27 000
  11. Ilość wpisów w listach kontroli dostępu QoS ACL – 16 000
* Oprogramowanie/funkcjonalność:
  1. Obsługa protokołu NTP
  2. Obsługa IGMPv1/2/3
  3. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
  4. Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia.
* Przełącznik realizuje 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 minimum 128 instancji protokołu STP
  5. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED
  6. Funkcja serwera DHCP
* Obsługa standardu 802.1AE
* Obsługa 3 poziomów dostępu administracyjnego poprzez konsolę.
* Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
* Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+
* Przełącznik realizuje następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:
  1. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
  2. Implementacja algorytmu Shaped Round Robin lub podobnego 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). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik
  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
* Urządzenie realizuje routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
  1. dla IPv4: OSPF, BGP, ISIS
  2. dla IPv6: OPSFv3,
  3. Funkcjonalności Policy-based routing
  4. multicast routing (PIM-SM, PIM-SSM)
* Urządzenie umożliwia enkapsulację ruchu przy pomocy VXLAN’ów
* Funkcjonalności z zakresu MPLS:
  1. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:
  2. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC
  3. L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji
  4. L3 VPN - MPLS Virtual Private Network (VPN)
  5. Multicast VPN (MVPN)
* Zarządzanie i konfiguracja:
  1. Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o NetFlow, wielkość tablicy monitorowanych strumieni wynosi 98 000.
  2. Urządzenie posiada dedykowany port Ethernet do zarządzania out-of-band
  3. Urządzenie jest wyposażone w port konsoli USB
  4. Urządzenie umożliwia tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie
  5. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
* Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

### Funkcjonalności dodatkowe dla przełączników Fabric Core (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

* + Obsługa standardu 802.1AE (szyfrowanie ruchu) 256-bit z prędkością line rate dla każdego z interfejsów
  + System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania urządzenia
  + Urządzenie jest przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3.
  + System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.
  + Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
  + Urządzenie posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB
  + Obsługa następujących dodatkowych funkcjonalności z zakresu MPLS:

1. IPv6 Provider Edge over MPLS (6PE)
2. IPv6 VPN Provider Edge over MPLS (6VPE)
3. Współpraca z mechanizmem MACSEC (802.1AE), czyli możliwość szyfrowania przy pomocy MACSEC połączeń MPLS

### Przełączniki dostępowe Fabric Access

W rozwiązaniu występują 5 przełączniki dostępowe Fabric Access.

* Przełącznik wyposażony w 48 portów 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at)
* Przełącznik udostępnia do wyprowadzenia za pomocą technologii PoE moc 437W
* Moc PoE może zostać zwiększona przez dodanie drugiego zasilacza do przełącznika do poziomu 1152W
* Przełącznik posiada slot rozszerzeń dzięki któremu można rozbudować przełącznik o dodatkowe porty
* Przełącznik należy wyposażyć w moduł 8x1/10G SFP+
  1. Wymagana obsługa wkładek w standardach Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax
* Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
  1. 8 urządzeń w stosie
  2. Zarządzanie poprzez jeden adres IP
  3. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad
* Zasilanie i chłodzenie
  1. Redundantne i wymienne moduły wentylatorów
  2. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap)
  3. Przełącznik wspiera IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności)
* Parametry wydajnościowe:
  1. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate)
  2. Bufor pakietów – 16MB
  3. Pamięć DRAM – 8GB
  4. Pamięć flash – 16GB
* Obsługa
  1. 1 000 sieci VLAN
  2. 32 000 adresów MAC
  3. 8 000 tras IPv4
  4. 4000 tras IPv6
* Obsługa protokołu NTP
* Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
* 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 128 instancji protokołu STP
* Obsługa protokołu LLDP i LLDP-MED.
* Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
* Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
* Możliwość uruchomienia funkcji serwera DHCP
* Mechanizmy związane z bezpieczeństwem sieci:
* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level)
  1. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
  2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL
  3. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
  4. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
  5. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
  6. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem
  7. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176
  8. 5000 wpisów dla list kontroli dostępu (Security ACE)
  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), 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. Funkcja Private VLAN
* 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

* Obsługa protokołów routingu:

1. Routing statyczny dla IPv4 i IPv6
2. Routing dynamiczny – RIP, OSPF
3. Policy-based routing (PBR)
4. Obsługa protokołu redundancji bramy (VRRP)

* Obsługa zaawansowanych protokołów routingu

1. IS-IS i BGP dla IPv4 i IPv6
2. EIGRP (rfc7868)
3. Routing multicastów - PIM-SM, PIM-SSM
4. Multicast Source Discovery Protocol (MSDP)
5. VRF-Lite

* Możliwość enkapsulacji ruchu w pakiety VXLAN
* Zarządzanie

1. Port konsoli
2. Dedykowany port Ethernet do zarządzania out-of-band
3. 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
4. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6

* Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
* Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7)
* Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Pacekt) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa)

### Funkcjonalności dodatkowe dla przełączników Fabric Access (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

* + Rozbudowa:
  + Możliwość instalacji w slocie przeznaczonym na moduł rozszerzeń następujących modułów:

1. 2x40G QSFP
2. 2x25G SFP28
3. 4x100M/1G/2.5G/5G/10GBaseT RJ-45
   * Porty SFP/SFP+/QSFP możliwe do obsadzenia wkładkami:
4. porty QSFP: wkładki 40 Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, adapter 40G QSFP->10G SFP+
5. porty SFP28 25G: wkładka 25GBASE-SR SFP+

* Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
  1. Przepustowość w ramach stosu - 480Gb/s
  + Zasilanie:

1. możliwość współdzielenia mocy zasilaczy (grupy 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)
2. Możliwość instalacji zasilacza redundantnego AC 230V
3. Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia
   * Dodatkowe mechanizmy związane z bezpieczeństwem sieci:
4. funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal WWW)
5. realizacja podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard)
6. możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128 bitów

* Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania
  1. Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny
  2. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego
  3. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
* 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
* Wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.)
* Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów
* Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych

## Przełączniki DC Core

### Funckjonalności podstawowe przełącznika DC Core

1. Przełącznik posiada:
   1. 48 portów 1/10/25 GE definiowanych za pomocą wkładek SFP/SFP+/SFP28 bezpośrednio w obudowie przełącznika lub na karcie liniowej
   2. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps
2. Parametry wydajnościowe:
   1. Prędkość przełączania „wirespeed” dla każdego portu przełącznika
   2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
   3. Obsługiwana łączna przepływność (pasmo) min. 3 Tbps
   4. Obsługiwana łączna przepustowość pakietowa przełącznika min. 2000 mpps
   5. opóźnienie przełączania pakietów nie większe niż 2 µs
3. Przełącznik posiada następującą funkcjonalność warstwy L2:
   1. Trunking IEEE 802.1Q VLAN;
   2. Wsparcie dla 4094 sieci VLAN;
   3. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   4. Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC
   5. IEEE 802.1w Rapid Spanning Tree (RST)
   6. IEEE 802.1s Multiple Spanning Tree (MST)
   7. Wsparcie sprzętowe dla tunelowania QinQ
   8. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree
   9. Internet Group Management Protocol (IGMP) Versions 2, 3;
   10. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   11. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce
   12. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
4. Przełącznik posiada następująca funkcjonalność 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) dla IPv4
   5. VRRP v3
   6. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol)
   7. Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP
   8. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast)
   9. Wsparcie dla IGMPv3 oraz MSDP
   10. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
   11. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking)
   12. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP)
   13. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list
   14. Jeśli funkcjonalność powyższa wymaga dostarczenia dodatkowej licencji to nie jest ona wymagana na tym etapie
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   1. Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint)
   2. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway)
   3. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP
   4. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   5. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol)
   6. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   1. Layer 2 IEEE 802.1p (CoS);
   2. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4;
   3. Kolejkowanie na wyjściu w oparciu o CoS 802.1p;
   4. Bezwzględne (strict-priority) kolejkowanie na wyjściu;
   5. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający
   6. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych
   7. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   8. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   1. Wejściowe ACL (standardowe oraz rozszerzone);
   2. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu;
   3. Standardowe oraz rozszerzone 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 VLAN-y (VACL);
   5. ACL oparte o porty (PACL);
   6. DHCP Snooping
   7. ARP Inspection
   8. IP Source Guard
   9. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
8. 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, v2, v3;
   10. RMON (przynajmniej grupy Events, Alarms)
   11. sFlow
   12. IEEE 802.1ab LLDP
   13. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   14. Role-Based Access Control RBAC
   15. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   16. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirror)
   17. Network Time Protocol (NTP)
   18. Precision Time Protocol IEEE 1588
   19. Diagnostyka procesu BOOT
   20. Ping
   21. Traceroute
9. Przełącznik może być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych lub połączeń zasilających urządzenia
10. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”

### Funkcjonalności dodatkowe dla przełącznika DC Core (nie są bezwzględnie wymagane, za ich udostępnienie przyznawane są dodatkowe punkty):

1. Narzędzia programowania i zarzadzania 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) 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. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika
   4. Interfejs programistyczny REST API wraz z upublicznionym SDK
   5. Możliwość zainstalowania klienta Chef
   6. Możliwosć zainstalowania agenta Puppet
   7. Wsparcie dls NETCONF i zarządzania poprzez XML
   8. Wsparcie dla OpenStack Neutron plugin
2. Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree) ani L3 a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika centralnego.

## Zestawienie ilościowe komponentów

Do realizacji modernizacji wymagane jest dostarczenie następujących komponentów:

|  |  |
| --- | --- |
| System zarządzania i monitorowania siecią wraz z wymaganą platformą sprzętową | 1 szt. |
| System kontroli dostępu | 2 maszyny wirtualne +125 licencji podstawowych i 125 3-letnich licencji na profilowanie urządzeń |
| Przełącznik MPLS Core Switch | 6 szt. |
| Przełącznik Fabric Core | 2 szt. |
| Przełącznik Fabric Access | 5 szt. |
| Przełącznik DC Core | 6 szt. |

## Moduły optyczne i akcesoria dodatkowe do realizacji połączeń 10Gb/s, 40 Gb/s lub 100 Gb/s

W ramach dostarczonego rozwiązania na potrzeby zrealizowania połączeń wymagana jest dostawa wkładek i kabli:

36 szt. Wkładek 10GBASE-SR SFP+

24 szt. Wkładek 100/40GB w standardzie SR-BD

2 szt. Wkładek SFP+ 10GBASE-LR-S

12 szt. Kabli SFP28 25-GBASE-CU (kabel miedziany zakończony wkładkami SFP28) 3m.

4 szt. Aktywnego kabla optycznego 3m. w standardzie 100Gbase QSFP.

# Licencjonowanie produktów

1. Dostarczane licencje na oprogramowanie muszą być zgodne z warunkami licencyjnymi producenta oferowanego rozwiązania.
2. Zamawiający musi mieć możliwość zarządzania dostarczanymi licencjami poprzez dedykowane konto na stronie internetowej producenta.
3. Urządzenia sieciowe muszą zostać dostarczone z 3-letnimi licencjami w ramach funkcjonalności SDN – dotyczy to przełączników MPLS Core, Fabric Core oraz Fabric Access. System kontroli dostępu obejmuje oprogramowanie i licencje na dwie maszyny wirtualne oraz 125 permanentnych licencji bazowych (uwierzytelnienie podstawowe) oraz 125 3-letnich licencji dodatkowych (profilowanie stacji, wykrywanie typu stacji, współpraca z systemem zarządzania i monitoringu sieci SDN Network Fabric).

# Wymagania gwarancyjne, serwisowe

1. Dostarczone urządzenia muszą być nowe, nie używane w innych projektach oraz pochodzić z bieżącej produkcji (muszą być wyprodukowane nie wcześniej niż 6 miesięcy od daty dostarczenia).
2. Dla urządzeń Fabric CORE, Fabric Access i DC Core wymagana jest gwarancja dożywotnia producenta dla dostarczanych urządzeń (świadczona przez okres 5 lat od daty ogłoszenia końca sprzedaży urządzeń) zapewniająca wymianę uszkodzonego urządzenia na sprawne w reżimie 8x5xNBD. Wymagany jest dostęp do aktualizacji i poprawek oraz nowych wersji oprogramowania przez czas świadczenia gwarancji.
3. Dla systemu zarządzania i monitorowania siecią SDN Network Fabric wymagana jest gwarancja producenta na okres 12 miesięcy zapewniające wymianę uszkodzonego urządzenia na sprawne w reżimie 8x5xNBD oraz wymagane jest dostęp do aktualizacji i poprawek oraz nowych wersji oprogramowania przez czas świadczenia gwarancji.
4. Dla systemu kontroli dostępu i zarządzania politykami bezpieczeństwa wymagane jest wsparcie serwisowe na okres 36 miesięcy zapewniające dostęp do nowych wersji i uaktualnień systemu.
5. Całość dostarczanego rozwiązania (urządzenia i oprogramowanie) musi zostać objęta usługą wsparcia serwisowego producenta na okres 12 miesięcy zapewniającą możliwość zgłaszania i rozwiązywania tzw. zgłoszeń serwisowych. Serwis ma umożliwiać możliwość bezpośredniego dokonywania zgłoszeń (bez pośrednictwa dostawcy) i bezpośredni kontakt z inżynierami producenta z centrum serwisowego.

# Wdrożenie

Całość systemu musi zostać zainstalowana i uruchomiona przez Wykonawcę. Zakres wdrożenia obejmuje zarówno sieć MPLS Core, jak i sieć SDN Network Fabric.

# Szkolenia

W ramach projektu Wykonawca dostarczy vouchery szkoleniowe z tematyki budowy, implementacji, zarządzania i monitorowania sieci SDN Network Fabric oraz MPLS Core dla 2 osób. Szkolenie swoim zakresem ma obejmować zajęcia teoretyczne i praktyczne oraz tematycznie pokrywać całość funkcjonalności wdrażanych rozwiązań. Vouchery muszą być ważne co najmniej przez okres 12 miesięcy. Szkolenie powinno trwać co najmniej 5 dni / co najmniej 40 godzin szkoleniowych i odbywać się w ośrodku szkoleniowym autoryzowanym przez producenta dostarczanego sprzętu na terenie Polski. Za rozszerzony zakres szkolenia przyznawane będą dodatkowe punkty.