

OPIS PRZEDMIOTU ZAMÓWIENIA (parametry i wymagania minimalne)

Dostawa fabrycznie nowego, nie używanego przełącznika (switcha) wraz z modulem światłowodowym do budynku Zakładu Nauk o Człowieku wraz z rozbudową posiadanej infrastruktury sieciowej.

Opis przedmiotu zamówienia:

I. Przełącznik (switch) w Zakładzie Nauk o Człowieku na. ul Leszka Czarnego ma zostać wyposażony w urządzenia o parametrach nie niższych niż:

1. Typ i liczba portów:
 - Minimum 48 porty 10BASE-T/100BASE-TX/1000BASE-T wspierające standard PoE+ (802.1at) umieszczonych z przodu obudowy
 - Minimum 4 porty SFP Gigabit (muszą być niezależne od portów 10BASE-T/100BASE-TX/1000BASE-T) umieszczonych z przodu obudowy
 - Minimum 2 porty 10Gb SFP+ umieszczonych z przodu obudowy
2. Możliwość rozbudowy o minimum 4 porty SFP+, CX4, XFP. Ze względu na niezawodność, wymaga się żeby wymagane w tym punkcie porty 10Gb dostępne były w postaci minimum dwóch niezależnych modułów.
3. Możliwość rozbudowy o minimum 16 portów gigabitowych (miedzianych i SFP)
4. Sloty SFP muszą umożliwiać instalację modułów światłowodowych zarówno 100Mb/s jak i 1000Mb/s
Wraz z przełącznikiem należy dostarczyć moduł SFP+ działający w standardzie: 10GBaseER, umożliwiający transmisję na odległość min 40km
5. Modularny wewnętrzny zasilacz prądu zmiennego, dodatkowo slot na drugi zasilacz. Przy wykorzystaniu obydwu źródeł zasilania – zasilacze powinny pracować w trybie redundantnym oraz być wymieniane na gorąco.
6. Budżet mocy dla PoE+ minimum 800W na pojedynczym zasilaczu.
7. Wydajność: minimum 224Gb/s (prędkość przełączania „wirespeed” dla każdego portu przełącznika)
8. Przepustowość: minimum 166,6Mp/s
9. Przełączanie w warstwie 2 i 3 modelu OSI
10. Wielkość tablicy routingu: minimum 12000 wpisów
11. Funkcja łączenia w stos grupy przełączników, urządzenia połączone w stos widziane jako jedno logiczne urządzenie. Wymagane jest by urządzenia tworzące stos mogły posiadać łącznie nie mniej niż 500 portów 10BASE-T/100BASE-TX/1000BASE-T. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
12. Łączenie w stos z wykorzystaniem portów 10Gb zarówno CX4 jak i światłowodowych
13. Możliwość realizacji link aggregation w ramach różnych przełączników będących w stosie
14. Tablica adresów MAC o wielkości min. 32000 pozycji
15. Obsługa ramek Jumbo
16. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol

17. Obsługa sieci IEEE 802.1Q VLAN – 4000 sieci VLAN oraz IEEE 802.1ad QinQ
18. Obsługa IGMP v1/v2/v3 oraz IGMP Snooping
19. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
20. Funkcja BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BPDU w celu przeciwdziałania pętlom
21. Routing IPv4 – statyczny i dynamiczny (min. RIP, OSPF, ISIS, BGP)
22. Routing IPv6 – statyczny i dynamiczny (min. RIPng, OSPFv3, IS-ISv6, BGP4+)
23. Obsługa Policy Based Routing
24. Obsługa Virtual Private LAN Service (VPLS)
25. Obsługa PIM-SSM, PIM-DM i PIM-SM (dla IPv4 i IPv6)
26. Obsługa Multicast VLAN
27. Obsługa Multicast Border Gateway Protocol (MBGP)
28. Obsługa Multicast Source Discovery Protocol (MSDP)
29. Obsługa tunelowania IPv6
30. Obsługa ECMP (Equal Cost Multi Path)
31. Obsługa Unicast Reverse Path Forwarding (uRPF, RFC 3704)
32. Obsługa Virtual Router Redundancy Protocol (VRRP)
33. Funkcja typu Smart Link Backup – umożliwiająca szybkie (poniżej 50ms) przełączanie pomiędzy redundantnymi ścieżkami
34. Obsługa protekcji DHCP
35. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.
Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
36. Obsługa standardu 802.1p
37. Możliwość ograniczania pasma na porcie
38. Możliwość zmiany wartości pola DSCP i/lub wartości priorytetu 802.1p
39. Funkcja mirroringu portów: co najmniej 1 to 1 Port mirroring, Many to co najmniej 1 port mirroring
40. Inteligentny port mirroring - kopiowanie ruchu wybranego przy pomocy listy ACL z wybranego portu lub VLANu na lokalny lub zdalny port
41. Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x:
 - i. Możliwość uwierzytelniania wielu użytkowników na jednym porcie
 - ii. Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS
 - iii. Możliwość przypisania profilu QoS dla użytkownika lub grupy użytkowników
42. Możliwość centralnej autoryzacji stacji końcowej na podstawie MAC – funkcja dla stacji, które nie mają klienta IEEE 802.1x:
 - i. Możliwość przydziału stacji do wskazanej sieci wirtualnej po autoryzacji MAC
 - ii. Możliwość uwierzytelniania wielu urządzeń na jednym porcie
43. Obsługa RADIUS Accounting
44. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
45. Obsługa Guest VLAN – VLAN dla gości
46. Funkcja izolowania portów
47. Zarządzanie poprzez port konsoli, co najmniej SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
48. Obsługa Syslog
49. Obsługa Secure FTP
50. In-service software upgrade (ISSU)
51. Obsługa standard IEEE 802.1AB Link Layer Discovery Protocol (LLDP) oraz LLDP-MED

52. Obsługa Network Time Protocol (NTP) v3
53. Obsługa protokołu typu Unidirectional Link Detection (UDLD) lub równoważnego
54. Przechowywanie wielu wersji oprogramowania na przełączniku
55. Przechowywanie wielu plików konfiguracyjnych na przełączniku, możliwość przegrywania pliku konfiguracyjnego w postaci tekstowej do i z stacji roboczej
56. Zakres pracy min. od 0 do 45°C
57. Wysokość w szafie 19" – 1U. Głębokość nie większa niż 50cm
58. Maksymalny pobór mocy (bez PoE), nie większy niż 250W
59. Dostarczony sprzęt powinny pochodzić z oficjalnego kanału dystrybucji producenta. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta, że dostarczony sprzęt pochodził z oficjalnego i legalnego kanału dystrybucyjnego.
60. W celu zapewnienia pełnej kompatybilności w ramach całej sieci UR wszystkie urządzenia sieciowe i akcesoria (np. moduły SFP+) muszą w pełni ze sobą współpracować.
61. Dostarczony moduł światłowodowy SFP+ do przełącznika musi być kompatybilny oraz nie powodujący problemów serwisowych i gwarancyjnych. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta, że zastosowany moduł światłowodowy SFP+ jest kompatybilny z urządzeniem aktywnym będącym przedmiotem zamówienia.
62. Wszystkie przełączniki muszą być fabrycznie nowe i nieużywane w innych projektach.
63. Wyposażenie dodatkowe: min. Patchcord światłowodowy

II. Rozbudowa posiadanego przełącznika HP 7500 w budynku G4:

1. Do przełącznika HP 7500 należy dostarczyć moduł SFP+ działający w standardzie 10GBaseER, umożliwiający transmisję na odległość min. 40km
2. W celu zapewnienia pełnej kompatybilności moduł i przełącznik muszą w pełni ze sobą współpracować.
3. Dostarczony moduł światłowodowy SFP+ do przełącznika musi być kompatybilny oraz nie powodować problemów serwisowych i gwarancyjnych. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta posiadanego przełącznika, że zastosowany moduł światłowodowy SFP+ jest kompatybilny z urządzeniem aktywnym.
4. Wyposażenie dodatkowe: min. Patchcord światłowodowy

Prace instalacyjno-konfiguracyjne:

W ramach rozbudowy istniejącej sieci, wyszczególniony w punktach powyżej sprzęt sieciowy (fabrycznie nowy, nie używany) należy dostarczyć do siedziby Zamawiającego oraz wykonać jego montaż, instalację, konfigurację i uruchomienie zgodnie z poniższymi wymogami.

Nowy punkt dystrybucyjny:

- W nowym punkcie dystrybucyjnym (Rzeszów, ul. Leszka Czarnego) zamontować przełącznik wraz z dostarczonym wyposażeniem (zasilacze, moduły światłowodowe, patchcordsy, itp....)
- Wykonać połączenie pomiędzy dostarczonym przełącznikiem w nowym punkcie dystrybucyjnym, a przełącznikiem HP 7500 (działającym przełącznikiem na Uniwersytecie Rzeszowskim) umieszczonym w rdzeniu sieci w budynku ul. Warzywna G4 (punkty dystrybucyjne połączone linkiem światłowodowym jednomodowym), połączenie min. 10Gbp po światłowodzie jednomodowym (należy również skonfigurować istniejący przełącznik w budynku G4)
- Wykonać konfigurację nowo dostarczonego przełącznika zgodnie z zaleceniami Zamawiającego

- W ramach instalacji przełącznika w sieci należy również dostarczyć niezbędne elementy do prawidłowego montażu dostarczanego sprzętu jak również dostarczyć niezbędne okablowanie (patchcord światłowodowy) niezbędne do zestawienia połączenia.

Rozbudowa posiadanego przełącznika HP 7500 w budynku G4:

- W budynku G4 (Rzeszów, ul. Warzywna) zamontować moduł w istniejącym przełączniku modularnym.
- Wykonać konfigurację przełącznika
- W ramach instalacji modułu w przełączniku w sieci należy również dostarczyć niezbędne elementy do prawidłowego montażu dostarczanego modułu jak również dostarczyć niezbędne okablowanie (patchcord światłowodowy) niezbędne do zestawienia połączenia.
- Przełącznik należy podłączyć linkiem min. 10Gbps do nowo dostarczanego przełącznika w punkcie dystrybucyjnym (Rzeszów, ul. Leszka Czarnego)

Dodatkowo prace:

Wszystkie połączenia pomiędzy przełącznikami należy skonfigurować w typ trunk i przepuszczać wszystkie dostępne vlan-y na danym przełączniku.

LAN i adresacja

W celu zapewnienia dostępu do sieci należy przepuścić ruch następujących rodzajów vlan-ów:

- Vlan „zarządzający”, służyć ma adresacji urządzeń sieciowych w celu zapewnienia zdalnego dostępu do nich oraz możliwości ich monitorowania
- Vlany „pracownicze”, służyć mają dostępowi pracowników URZ do zasobów udostępnianych w sieci oraz Internetu
- Vlan „gościnnie”, służyć ma dostępowi osób z poza URZ do dostępu do Internetu
- Vlany „pracownie”, służyć mają wyodrębnieniu sieci do obsługi sali pracowni(pomieszczeń laboratoryjnych)

Routing

Dla wszystkich nowo konfigurowanych sieci LAN należy skonfigurować routing według następujących zasad:

- Sieć „zarządzająca” ma być doprowadzona do firewall-a(bramą domyślną dla tej sieci ma być adres firewall-a), ruch do/z sieci ma być ograniczony za pomocą odpowiednich reguł do ruchu niezbędnego do zarządzania/monitorowania urządzeń
- Sieci „pracownicze” należy routować na przełączniku rdzeniowym(bramą domyślną dla tych sieci ma być adres IP odpowiedniego vlan-u skonfigurowany na przełączniku – istniejącym klastrze)
- Sieć „gościnnie” ma być doprowadzona do firewall-a(bramą domyślną dla tej sieci ma być adres firewall-a), ruch z sieci do Internetu ma być ograniczony za pomocą odpowiednich reguł do ruchu umożliwiającego korzystania z poczty, stron WWW dla gości URZ. Ruch do/z innych sieci powinien być zablokowany i logowany.
- Sieci „pracownie” mają być doprowadzona do firewall-a(bramą domyślną dla tych sieci ma być adres firewall-a), ruch do/z sieci ma być ograniczony za pomocą odpowiednich reguł do ruchu niezbędnego do zarządzania i dostępu do Internetu

Należy również dokonać rekonfiguracji istniejących przełączników rdzeniowych i firewalli na UR w celu zapewnienia prawidłowego działania nowo tworzonych sieci np. routingu, tak aby z nowo definiowanych sieci zapewniły dostęp do udostępnianych zasobów centralnych (serwerów i systemów) tak jak w innych budynkach UR oraz Internetu.

Konfiguracja parametrów i portów przełącznika dostarczonego przełącznika

Nowo dostarczony przełącznik należy skonfigurować w taki sposób, aby były spełnione następujące założenia działania sieci LAN, które funkcjonują na UR:

- Propagacja vlan-ów pomiędzy przełącznikami ma odbywać się z wykorzystaniem protokołu co najmniej GVRP
- Uruchomienie protokołu co najmniej LLDP na przełączniku w celu rozpoznawania podłączonych urządzeń
- Konfiguracja protokołów służących do zdalnego zarządzania przełącznikiem co najmniej:
 - o Ssh
 - o https
 - o SNMP
- Zabezpieczenie wszystkich portów dostępowych z wykorzystaniem co najmniej następujących mechanizmów (zabezpieczenie portów dostępowych może różnić się dla każdego z rodzajów vlan-ów do jakich będzie przypisany port):
- Wszystkie porty dostępne mają być skonfigurowane w trybie „access”
- Port-security, tylko jeden adres MAC może pojawić się na porcie, w przypadku wykrycia większej liczby adresów MAC port powinien wyłączyć się automatycznie.
- Adresy MAC nie mają być zapamiętywane w konfiguracji urządzenia.
- W przypadku wykrycia pakietów BPDU na porcie, port powinien zostać zablokowany tzw. „BPDU Protection”.
- Zabezpieczenie przed negocjacją root-a w protokole STP na każdym z portów dostępowych tzw. Root Guard
- o ochrona przed wpięciem nieautoryzowanego serwera DHCP, zablokowanie możliwości wysyłania adresów IP z urządzeń podłączonych do portów dostępowych,
- Zablokowanie możliwości używania na wyznaczonych portach dostępowych adresów statycznych. Użytkownicy podpięci do sieci mogą wykorzystywać jedynie adresy przyznane przez serwer DHCP.
- Zabezpieczenie przed nadmiernym ruchem broadcast-owym na portach dostępowych, w przypadku przekroczenia zdefiniowanych progów, ruch powinien być ograniczony lub port powinien zostać wyłączony.
- Należy skonfigurować protokół SNMP w celu monitoringu/zarządzania przełącznikiem, ruch SNMP należy ograniczyć wyłącznie z/do serwerów monitorujących sieć i urządzenia
- Czas na przełączniku należy synchronizować z serwerem czasu wskazanym przez zamawiającego

Konfiguracja posianego serwera DHCP

Dla nowo powstałych sieci LAN w ramach wdrożenia należy dokonać rekonfiguracji posiadanego serwera DHCP. Na serwerze należy skonfigurować dodatkowe pule adresów dla poszczególnych vlanów, z których adresy IP będą przydzielane użytkownikom jako rozszerzenie istniejącej spójnej sieci UR.

Szczegóły adresacji sieci, zakres adresów DHCP, adres bramy domyślnej dla każdej z sieci, adresy IP serwerów DNS i innych parametrów niezbędnych do prawidłowego działania zostaną określone przez Zamawiającego.

Wykonawca musi również skonfigurować wszystkie urządzenia pośrednie, aby zapytania z sieci trafiały do odpowiedniego serwera DHCP.

Rekonfiguracja posiadanego Firewall-a

Należy dokonać rekonfiguracji posiadanego firewall-a(klaster) jako rozszerzenie spójnej ochrony sieci UR. Rekonfiguracja w szczególności będzie dotyczyć:

- Stworzenie dodatkowych wirtualnych interfejsów dla odpowiednich vlan-ów.
- Konfiguracji reguł dostępowych dla każdej z nowo powstałych sieci LAN, ograniczając ruch do niezbędnego (reguły muszą być analogiczne jak dla innych sieci aby tworzyły wspólny system zabezpieczeń dla całego UR)
- Uruchomienie ochrony IPS, antywirusowej, URL filteringu dla nowo definiowanych sieci LAN w ramach jednego kompleksowego zabezpieczenia UR.
- Konfiguracja routingu dla nowo definiowanych sieci, które muszą współpracować z posiadanymi innymi działającymi sieciami na UR i tworzyć integralną spójną sieć.

Konfiguracja systemu monitoringu

Nowy dostarczony przełącznik ma być monitorowany jednym z wybranym sposobów:

- nowo dostarczany przełącznik ma posiadać oprogramowanie, które zapewni monitoring/zarządzanie co najmniej w zakresie, które posiadane oprogramowanie IMC działające na UR oraz ma zostać zintegrowane z posiadanym oprogramowaniem IMC, które pozwala na centralne zarządzanie istniejącą i nowo dostarczaną infrastrukturą z zachowaniem uruchomionych już funkcjonalności.
- wykonanie integracji bezpośrednio z oprogramowaniem IMC, które UR posiada (Wykonawca wykorzysta posiadane oprogramowanie działające na UR).

Szkolenie, ddokumentacja powykonawcza i testy poprawności

- Przeprowadzenie bezpłatnego szkolenia do dostarczonego sprzętu w zakresie obsługi i konfiguracji min 5 godzin
- Po zakończeniu prac instalacyjno - konfiguracyjnych należy zaproponować i wykonać testy potwierdzające prawidłowe działanie nowo wytworzonej części sieci
- Warunkiem odbioru końcowego będzie dostarczenie zaakceptowanej przez Zamawiającego dokumentacji technicznej z wykonanych prac

Gwarancja na całość przedmiotu zamówienia wynosi: min. 12 miesięcy

Oferty uzyskują maksymalną ilość punktów, gdy czas gwarancji wynosi 24 miesięcy lub więcej. Oferty z okresem gwarancji krótszym od wymaganego zostaną odrzucone.