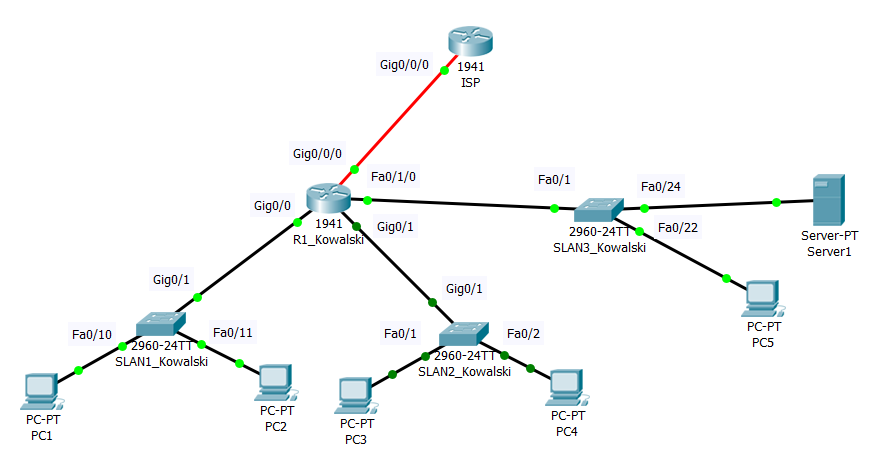
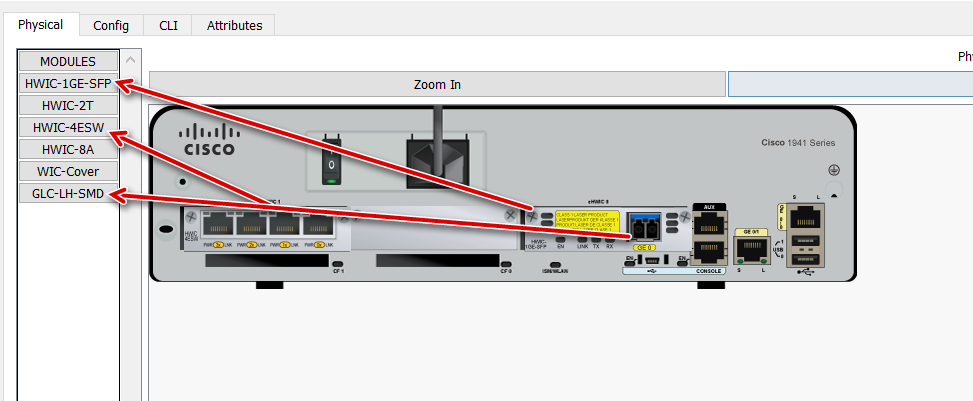
Zadania integrujące umiejętności do samodzielnej realizacji dla „Sieci komputerowe i Internet” *– Radosław Terelak*

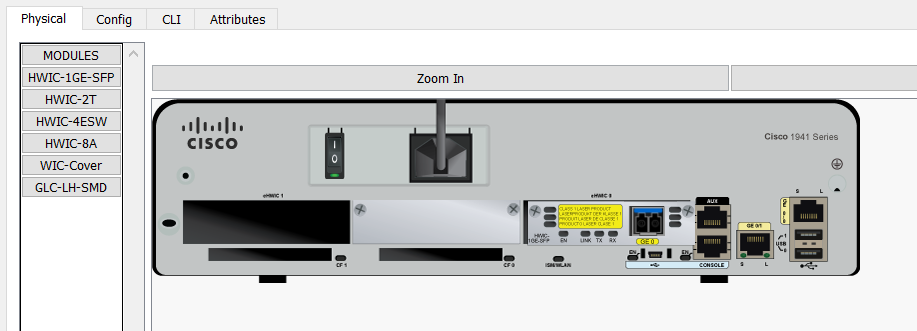
1. Topologia do przygotowania w aplikacji *Packet Tracer*:



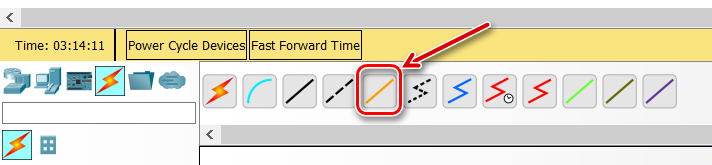
Tj. w ramach oprogramowania *Packet Tracer* należy utworzyć topologię składającą się z dwóch obiektów rutera (model 1941), oraz trzech osobnych fizycznych segmentów sieci, gdzie w dwóch z nich znajdować się ma po jednym obiekcie przełącznika (model 2960) oraz dwóch obiektów komputera, a w trzecim segmencie fizycznym sieci obiektu przełącznika (model 2960) oraz obiektu serwera i komputera, które to wszystkie urządzenia są ze sobą połączone odpowiednimi kablami w odpowiedni sposób (zgodnie z informacjami na w/w rysunku).  
*Podpowiedź: w ruterze R1 należy dodać odpowiedni moduł z dodatkowymi czterema interfejsami FastEthernet (HWIC-4ESW) jak również moduł z portem SFP (HWIC-1GE-SFP), w którym należy również zainstalować wkładkę optyczną SFP (GLC-LH-SMD), jak na poniższym rysunku:*



*W ruterze ISP należy również zainstalować* *moduł z portem SFP (HWIC-1GE-SFP), w którym należy następnie zainstalować wkładkę optyczną SFP (GLC-LH-SMD), jak na poniższym rysunku:*



Łącząc ruter R1 z ruterem ISP należy pamiętać, aby jako kabla użyć światłowód (*Fiber*):



W ruterze ISP należy także w ramach przygotowania środowiska do zadań, wprowadzić następującą konfigurację, przebywając w trybie konfiguracji globalnej (pozostałe urządzenia zostaną skonfigurowane w ramach dalszych zadań):

Router(config)# **hostname ISP**

ISP(config)# **interface g0/0/0**

ISP(config-if)# **ip address 155.21.1.1 255.255.255.252**

ISP(config-if)# **ipv6 address 2001:ACAD:B:1::1/64**

ISP(config-if)# **no shutdown**

ISP(config-if)# **interface loopback0**

ISP(config-if)# **ip address 80.1.1.1 255.255.255.255**

ISP(config-if)# **ipv6 address 2001:db8:acad::1/64**

ISP(config-if)# **no shutdown**

ISP(config-if)# **exit**

ISP(config)# **ip route 155.21.22.0 255.255.254.0 155.21.1.2**

ISP(config)# **ipv6 route 2001:ACAD:A::/48****2001:ACAD:B:1::2**

ISP(config)# **end**

ISP# **copy running-config startup-config**

ISP#

Scenariusz

Twoja firma zdobyła kontrakt na skonfigurowanie małej sieci dla właściciela firmy XYZ ulokowanej w trzech budynkach znajdujących się obok siebie. W każdym z tychże trzech budynków znajdujących się obok siebie jest osobna serwerownia, która ma obsługiwać tenże „swój” budynek ze względów bezpieczeństwa i względów wydajnościowych, jako osobny segment fizyczny sieci, przy czym wszystkie budynki współdzielą jedno połączenie internetowe doprowadzone od rutera dostawcy (ruter ISP) do rutera (R1) znajdującego się w głównym budynku firmy. Wyposażenie i okablowanie jest już w tejże sieci zainstalowane. Twoim zadaniem jest zaprojektowanie schematu adresowania IPv4 oraz IPv6 w ramach przydzielonych podsieci, oraz skonfigurowanie wyznaczonych urządzeń zgodnie z podanymi założeniami i sprawdzenie łączności.

Forma realizacji sprawozdania z zadań:

W ramach sprawozdania z wykonanych zadań należy umieścić w czystym nowym pliku na samym początku tego sprawozdania poniżej zawarte 4 tabele z zaprojektowanym schematem adresacji, a następnie należy umieścić zrzuty ekranowe (**pełnego ekranu, a nie wycinków**) z kolejnych kroków wykonywanych zadań w aplikacji Packet Tracer według kolejności punktów poniżej zawartych.

Wykonane sprawozdanie należy wysłać korzystając z odpowiedniej pozycji w kursie w platformie e-learningowej jako plik *.pdf*, *.docx* lub *.odt*

Założenia do realizacji zadań:

* Dostawca internetowy na potrzeby sieci lokalnych firmy przydzielił pulę adresów zewnętrznych IPv4 *155.21.22.0/23*, oraz pulę adresów unikalnych globalnych IPv6 *2001:ACAD:A::/48*. W sieci z przełącznikiem SLAN1 zakładane jest iż będzie się znajdować max. 250 urządzeń, w sieci z przełącznikiem SLAN2 zakładane jest iż będzie się znajdować max. 120 urządzeń, natomiast w sieci z przełącznikiem SLAN3 zakładane jest iż będzie się znajdować max. 80 urządzeń. Na potrzeby samego łącza internetowego dostawca internetowy przydzielił pulę adresów zewnętrznych IPv4 *155.21.1.0/30* gdzie adres IP rutera pod stronie dostawcy to *155.21.1.1*, oraz pulę adresów unikalnych globalnych IPv6 *2001:ACAD:B:1::/64* gdzie adres IP rutera pod stronie dostawcy to *2001:ACAD:B:1::1* a dla naszego rutera jest prośba, aby przydzielić adres IPv6 *2001:ACAD:B:1::2/64*

Biorąc pod uwagę powyższe informacje, należy zaprojektować przydział podsieci/pól adresowych dla segmentów fizycznych sieci i urządzeń się w nich aktualnie znajdujących, zakładając, że poza samymi przełącznikami, pozostałe urządzenia będą pracować w ramach tzw. podwójnego stosu TCP/IP, i uzupełnić poniższe **Tabele adresacji** odpowiednimi danymi:

|  |  |
| --- | --- |
| **Nazwa sieci lokalnej** | **Przydzielona pula adresowa IPv4** |
| SLAN1 |  |
| SLAN2 |  |
| SLAN3 |  |

|  |  |
| --- | --- |
| **Nazwa sieci lokalnej** | **Przydzielona pula adresowa IPv6** |
| SLAN1 |  |
| SLAN2 |  |
| SLAN3 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IPv4 | Maska podsieci | Adres IPv4 bramy domyślnej |
| R1 | G0/0 |  |  |  |
| G0/0/0 |  |  |  |
| F0/1/0 |  |  |  |
| SLAN1 | VLAN1 |  |  |  |
| SLAN2 | VLAN1 |  |  |  |
| SLAN3 | VLAN1 |  |  |  |
| PC1 | Interfejs sieciowy |  |  |  |
| PC2 | Interfejs sieciowy |  |  |  |
| PC3 | Interfejs sieciowy |  |  |  |
| PC4 | Interfejs sieciowy |  |  |  |
| PC5 | Interfejs sieciowy |  |  |  |
| Server1 | Interfejs sieciowy |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IPv6 | Prefix | Adres IPv6 bramy domyślnej |
| R1 | G0/0 |  |  |  |
| G0/0/0 |  |  |  |
| F0/1/0 |  |  |  |
| Server1 | Interfejs sieciowy |  |  |  |

*Uwaga: dla komputerów PC zostanie użyty do konfiguracji adresacji TCP/IP mechanizm SLAAC, stąd nie wymagają one zaprojektowania dla nich danych adresowych, sam serwer będzie miał przydzielony ręcznie statyczny adres IPv6, a przełączniki będą na razie posiadały skonfigurowane tylko dane adresowe IPv4.*

* Należy skonfigurować router R1 uwzględniając następujące założenia:
  1. Nazwij router: **R1\_{Nazwisko}** *(gdzie pod {Nazwisko} należy podstawić swoje własne nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: R1\_Kowalski)*
  2. Użyj **Zaq12wsx** jako hasło do trybu EXEC użytkownika dla wszystkich linii
  3. Użyj **{Imię}X@a12#** jako hasło do uprzywilejowanego trybu EXEC *(gdzie pod {Imię} należy podstawić swoje własne imię, co jest warunkiem zaliczenia sprawozdania, np.: JanX@a12#)*
  4. Skonfiguruj adresowanie wszystkich interfejsów według zaprojektowanej tabeli adresacji (zarówno IPv4 jak i IPv6)  
     *Uwaga:* *moduł z dodatkowymi czterema interfejsami FastEthernet (HWIC-4ESW) jest modułem przełącznikowym, i nie daje możliwości nadania adresu IP na wskazanym interfejsie fizycznym, a konfiguracja dla niego odbywa się na podobnej zasadzie jak konfiguracja dla przełącznika (czyli adres IP przypisuje się do interfejsu SVI, w tym przypadku „vlan1”)*
  5. Uruchom możliwość automatycznego przydzielania danych adresowych IPv6 przez ruter urządzeniom dostępowym we wszystkich trzech sieciach lokalnych w ramach mechanizmu SLAAC
  6. Ustaw datę oraz zegar na routerze na aktualne dane
  7. Wyłącz wyszukiwanie DNS, aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń jako nazwy DNS hostów
  8. Skonfiguruj tzw. trasę domyślną (nazywaną także bramą domyślną) dla protokołu IPv4 oraz IPv6, która umożliwi prawidłowe połączenie z siecią Internet.   
     Poniżej zawarto pomocne polecenia jakich należy do rozwiązania powyższego założenia użyć:

R1\_Kowalski(config)# **ip route 0.0.0.0 0.0.0.0 155.21.1.2**

R1\_Kowalski(config)# **ipv6 route ::/0 2001:ACAD:B:1::1**

* 1. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony:  
     *Nieautoryzowany dostęp jest zabroniony i ścigany w pełnym zakresie prawa.  
     Administrator urządzenia: {Imię Nazwisko}*(gdzie pod *{Imię Nazwisko}* należy podstawić swoje imię oraz nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: *Administrator urządzenia: Jan Nowak*)
  2. Zapisz konfigurację
* Należy skonfigurować przełącznik S1 uwzględniając następujące założenia:
  1. Nazwij przełącznik: **SLAN1\_{Nazwisko}** *(gdzie pod {Nazwisko} należy podstawić swoje własne nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: SLAN1\_Kowalski)*
  2. Użyj **Zaq12wsx** jako hasło do trybu EXEC użytkownika dla wszystkich linii
  3. Użyj **{Imię}X@a12#** jako hasło do uprzywilejowanego trybu EXEC *(gdzie pod {Imię} należy podstawić swoje własne imię, co jest warunkiem zaliczenia sprawozdania, np.: JanX@a12#)*
  4. Skonfiguruj adresowanie interfejsu SVI według tabeli adresacji (tylko dla IPv4)
  5. Ustaw datę oraz zegar na przełączniku na aktualne dane
  6. Wyłącz wyszukiwanie DNS, aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń jako nazwy DNS hostów
  7. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony:  
     *Nieautoryzowany dostęp jest zabroniony i ścigany w pełnym zakresie prawa.  
     Administrator urządzenia: {Imię Nazwisko}*(gdzie pod *{Imię Nazwisko}* należy podstawić swoje imię oraz nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: *Administrator urządzenia: Jan Nowak*)
  8. Zapisz konfigurację
* Należy skonfigurować przełącznik S2 uwzględniając następujące założenia:
  1. Nazwij przełącznik: **SLAN2\_{Nazwisko}** *(gdzie pod {Nazwisko} należy podstawić swoje własne nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: SLAN1\_Kowalski)*
  2. Użyj **Zaq12wsx** jako hasło do trybu EXEC użytkownika dla wszystkich linii
  3. Użyj **{Imię}X@a12#** jako hasło do uprzywilejowanego trybu EXEC *(gdzie pod {Imię} należy podstawić swoje własne imię, co jest warunkiem zaliczenia sprawozdania, np.: JanX@a12#)*
  4. Skonfiguruj adresowanie interfejsu SVI według tabeli adresacji (tylko dla IPv4)
  5. Ustaw datę oraz zegar na przełączniku na aktualne dane
  6. Wyłącz wyszukiwanie DNS, aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń jako nazwy DNS hostów
  7. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony:  
     *Nieautoryzowany dostęp jest zabroniony i ścigany w pełnym zakresie prawa.  
     Administrator urządzenia: {Imię Nazwisko}*(gdzie pod *{Imię Nazwisko}* należy podstawić swoje imię oraz nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: *Administrator urządzenia: Jan Nowak*)
  8. Zapisz konfigurację
* Należy skonfigurować przełącznik S3 uwzględniając następujące założenia:
  1. Nazwij przełącznik: **SLAN3\_{Nazwisko}** *(gdzie pod {Nazwisko} należy podstawić swoje własne nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: SLAN1\_Kowalski)*
  2. Użyj **Zaq12wsx** jako hasło do trybu EXEC użytkownika dla wszystkich linii
  3. Użyj **{Imię}X@a12#** jako hasło do uprzywilejowanego trybu EXEC *(gdzie pod {Imię} należy podstawić swoje własne imię, co jest warunkiem zaliczenia sprawozdania, np.: JanX@a12#)*
  4. Skonfiguruj adresowanie interfejsu SVI według tabeli adresacji (tylko dla IPv4)
  5. Ustaw datę oraz zegar na przełączniku na aktualne dane
  6. Wyłącz wyszukiwanie DNS, aby zapobiec próbom tłumaczenia niepoprawnie wprowadzonych poleceń jako nazwy DNS hostów
  7. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony:  
     *Nieautoryzowany dostęp jest zabroniony i ścigany w pełnym zakresie prawa.  
     Administrator urządzenia: {Imię Nazwisko}*(gdzie pod *{Imię Nazwisko}* należy podstawić swoje imię oraz nazwisko, co jest warunkiem zaliczenia sprawozdania, np.: *Administrator urządzenia: Jan Nowak*)
  8. Zapisz konfigurację
* Skonfigurować ręcznie adresowanie IPv4 dla wszystkich pozostałych urządzeń dostępowych (tj. PC oraz serwer) według tabeli adresacji, oraz dodatkowo ustawić w komputerach PC jako serwer DNS adres IPv4 serwera *Serwer1*
* Uruchomić automatyczne pobieranie danych adresowych IPv6 z wykorzystaniem mechanizmu SLAAC dla wszystkich urządzeń dostępowych PC (i zweryfikować prawidłowość pobrania odpowiednich danych adresowych przez każdy komputer, a jeżeli się nie powiodło, należy znaleźć i naprawić problem), jak również ręcznie przypisać zaprojektowany wcześniej statyczny adres IPv6 do serwera *Serwer1*
* Sprawdzić z urządzenia *PC1* oraz *PC3*, czy możliwa jest komunikacja przez sieć komputerową z wszystkimi pozostałymi urządzeniami zarówno z wykorzystaniem adresów IPv4 jak i IPv6 (jeżeli komunikacja się gdzieś nie powiodła, należy znaleźć i naprawić problem)
* Sprawdzić z urządzenia *PC1* oraz *PC3*, czy możliwa jest komunikacja przez sieć komputerową z adresami IP: *80.1.1.1* oraz *2001:db8:acad::1*, co ma zweryfikować prawidłowe działanie łącza internetowego (jeżeli komunikacja się nie powiodła, należy znaleźć i naprawić problem)
* Przejść do konsoli przełącznika *SLAN1*, i korzystając tylko i wyłącznie z konsoli tegoż przełącznika wyszukać następujące informacje:
  1. Znając tylko sam adres IPv4 komputera *PC1* oraz komputera *PC2* należy odczytać adres MAC interfejsów sieciowych tychże komputerów
  2. Znając adres MAC komputera *PC1* oraz komputera *PC2*, należy odczytać na jakim porcie/interfejsie zostały te dwa w/w komputery do tegoż przełącznika podłączone
* Przejść do konsoli rutera *R1*, i korzystając tylko i wyłącznie z konsoli tegoż rutera wyszukać następujące informacje:
  1. Odczytać do jakich grup multicastowych przystąpił interfejs sieciowy *G0/1*
  2. Odczytać jakie adresy IPv4 oraz IPv6 są skonfigurowane na interfejsach sieciowych
  3. Odczytać z jakiej wersji systemu IOS ruter korzysta, oraz jak duży dysk flash jest tam zainstalowany

Zadania na dodatkowe punkty (można z nich uzyskać dodatkowe 10 punktów):

* W serwerze *Serwer1* należy skonfigurować strefę DNS dla domeny *sklep.pl* (pamiętając o konieczności odpowiedniego skonfigurowania rekordów SOA oraz NS), i utworzyć rekordy typu A dla nazw *sklep.pl* oraz *www.sklep.pl* nakierowane na adres IP serwera *Serwer1*, a następnie zweryfikować możliwość prawidłowego rozwiązania w/w nazw z komputerów *PC-1*, *PC-3*, oraz *PC-5* (w realizacji tegoż zadania może trochę pomóc materiał z filmu: <https://www.youtube.com/watch?v=-SU87C27U_A&feature=youtu.be>)
* W serwerze *Serwer1* domyślnie jest udostępniona witryna internetowa, zweryfikować możliwość wczytania jej w przeglądarce internetowej z komputerów *PC1*, *PC3*, oraz *PC5* używając adresu *www.sklep.pl*
* W przełączniku *SLAN3* zmienić aktualnie wykorzystywany obraz systemu *Cisco IOS c2960-lanbase-mz.122-25.FX.bin* na znajdujący się obecnie w serwerze *Serwer1* i udostępniony za pomocą usługi TFTP nowszy obraz systemu Cisco IOS dla tegoż modelu przełącznika tj. *c2960-lanbasek9-mz.150-2.SE4.bin*, jak również usunąć plik ze „starym” IOS’em i następnie przekopiować z tegoż przełącznika na w/w serwer TFTP plik z konfiguracją urządzenia, tak aby w razie czego istniała jego kopia zapasowa  
  (w realizacji tegoż zadania może trochę pomóc materiał z artykułu: <http://slow7.pl/sieci-komputerowe/item/39-zarzadzanie-routerem-cisco>)
* W ruterze *R1* oraz we wszystkich trzech przełącznikach *SLAN* należy skonfigurować zdalny dostęp z wykorzystaniem protokołu SSH, i następnie zweryfikować możliwość połączenia SSH z w/w urządzeniami z komputerów *PC1*, *PC3*, oraz *PC5*

(w realizacji tegoż zadania może trochę pomóc materiał z artykułu: <http://slow7.pl/item/36-dostep-zdalny-oraz-prawa-uzytkownika-w-urzadzeniach-cisco> oraz <https://techfreak.pl/konfiguracja-routera-cisco-ssh/>)  
Aby zweryfikować połączenie z komputera klienckiego, należy w tymże PC uruchomić wiersz poleceń, i tam wykorzystać polecenie: *ssh -l username target*, gdzie *username* to nazwa użytkownika jakiego wykorzystamy do uwierzytelnienia się, a *target* to adres IP urządzenia z którym chcemy się połączyć (czyli przykładowo: *ssh -l jkowalski 192.168.1.3*)