ZESPÓŁ LABORATORIÓW TELEINFORMATYKI TRANSPORTU

ZAKŁAD INŻYNIERII TRANSPORTU LOTNICZEGO
I TELEINFORMATYKI (ITLIT)

Politechnika Warszawska | Wydział Transportu

LABORATORIUM ZITLIT

INSTRUKCJA DO ĆWICZENIA NR 5

Routing statyczny i dynamiczny w sieciach TCP/IP

Warszawa 2023

1. Cel ćwiczenia

Celem ćwiczenia jest zapoznanie studentów z podstawowymi zasadami konfiguracji sieci komputerowej w celu poprawnego trasowania pakietów danych w sieci komputerowej. Przedstawiono zasady routingu statycznego i dynamicznego w praktyce wykorzystując oprogramowanie symulacyjne Cisco Packet Tracer do symulacji trzech sieci LAN połączonych ze sobą routerami.

2. Wykaz wykorzystanych przyrządów i oprogramowania

- komputer PC z systemem Windows 10,
- Cisco Packet Tracer pobrany po uprzedniej rejestracji na stronie kursów Cisco.

3. Wprowadzenie

Pakiety przesyłane przez sieć opatrzone są adresem nadawcy i odbiorcy. Zadaniem routerów jako węzłów pośrednich między nadawcą a odbiorcą jest przesłanie pakietów do celu po jak najlepszej ścieżce. Typowy router bierze pod uwagę tylko informacje z nagłówka IP, czyli sprawdza tylko informacje z warstwy sieci (trzeciej) modelu OSI. Obowiązkiem routera IP przy przekazywaniu pakietu dalej do celu jest obniżenie o jeden wartości TTL (ang *Time To Live*, czasu życia pakietu). Datagram IP, który trafia do routera z wartością 1 (a zostanie ona zmniejszona na tym routerze do 0) w polu TTL zostanie utracony, a do źródła router odsyła datagram ICMP z kodem TTL Exceeded.

Routery utrzymują tablice trasowania, na podstawie których kierują pakiety od określonych nadawców do odbiorców, bądź kolejnych routerów. Tablica może być budowana statycznie (trasowanie statyczne) lub dynamicznie (protokoły trasowania dynamicznego, takie jak RIP, IGRP, EIGRP, OSPF, BGP, IS-IS).

Tablica routingu (trasowania) to baza informacji o trasach. Z punktu widzenia administratora ma ona format tabeli w postaci: adres-sieci/hosta, maska-podsieci, adres-następnego-routera, metryka. W zależności od implementacji, tablica może zawierać szereg dodatkowych informacji.

Trasowanie ma na celu możliwie najlepiej (optymalnie) dostarczyć pakiet do celu. Pierwotnie jedynym kryterium wyboru było posiadanie jak najdokładniejszej trasy do celu, ale obecnie protokoły trasowania mogą uwzględniać podczas wyboru trasy również takie parametry jak priorytet pakietu (standardy ToS/DSCP), natężenie ruchu w poszczególnych segmentach sieci itp. W przypadku trasowania brzegowego (wykorzystującego BGP) w Internecie wybór trasy jest silnie związany z

polityką poszczególnych dostawców (i zawartymi między nimi umowami o wymianie ruchu) i bywa daleki od optymalnego.
Najbardziej podstawowymi rodzajami routingu są routing statyczny i routing dynamiczny.

Routing statyczny występuje wtedy gdy trasy routowania są wpisane do tablicy routingu przez administratora. Administrator sam określa wszystkie parametry trasy.

Zalety to:

- wszystkie trasy w routerach są dobrze znane i kontrolowane,
- błędy jeśli występują, to z powodu błędnych wpisów,
- nie obciąża łącz dodatkową wymianą informacji,
- jest wygodny do konfiguracji w małych sieciach.

Wady to:

- trudno jest tworzyć połączenia redundantne,
- trudno jest dynamicznie rozkładać obciążenie łączy,
- trudno jest zbudować dużą sieć, gdyż jakakolwiek zmiana sieci powoduje konieczność konfiguracji sporej części jej routerów.

Routing dynamiczny występuje gdy zawartość tablicy routingu jest wpisywana poprzez protokół routingu dynamicznego RIP.

Zalety to:

- pozwala na zbudowanie bardziej skalowalnej sieci, gdyż zwalnia administratora z konieczności konfigurowania wszystkich routerów,
- pozwala na elastyczne reagowanie na zmiany struktury sieci - dołączenie kolejnego routera sprowadza się do konfiguracji parametrów dołączanego routera oraz routerów z nim sąsiadujących,
- w przypadku awarii jednego z węzłów, routery są w stanie wytyczyć automatycznie nową drogę, pod warunkiem, że taka droga istnieje.

Wady to:

- wymaga większej wiedzy administratora,
- większe wymagania sprzętowe (im większa sieć i bardziej skomplikowana sieć, tym te wymagania większe).

Najbardziej rozpowszechnionym protokołem routowania jest protokół RIP. jest on wewnętrznym protokołem działającym na podstawie wektora odległości, przeznaczonym dla małych sieci. Jest on zdefiniowany w dokumentach RFC organizacji IETF o numerach: 1058, 1388 i 1723. Był jednym z pierwszych protokołów trasowania używanych w Internecie. W celu wprowadzenia obsługi przestrzeni adresów bezklasowych opracowano drugą wersję tego protokołu. Dokumenty uaktualniające protokół RIP do wersji 2 powstały około 1998 roku. Protokół RIP jest protokołem wektora odległości. Protokoły te opisuje się zwykle jako protokoły implementujące algorytm Bellmana-Forda służący do znajdowania najlepszych ścieżek. Ale sama klasa protokołów została uprzednio zdefiniowana w książce Forda i Fulkersona *Flows in Networks*. Chociaż protokół RIP ma dugi rodowód sięgający wstecz do sieci Xerox, został on zaprojektowany do routingu IP. Protokół RIP jest protokołem trasowania, który korzysta z wymiany tablic w celu aktualizacji sąsiednich routerów. Pomysł polega na tym, że każdy router wysyła swoją własną tablicę trasowania z aktywnych interfejsów, korzystając z protokołu datagramów użytkownika (UDP). Intersieci protokołu RIP s ograniczone pod względem rozmiaru do 15 przeskoków (*hops*). To oznacza, przynajmniej dla protokołu RIP, że wartość 16 równa się nieskończoności lub nieosiągalności. To liczenie przeskoków określa metryka używana przez protokół RIP do mierzenia odległości. Protokół RIP nie bierze pod uwag żadnych danych czasu rzeczywistego, takich jak koszt, stopień wykorzystania czy szybkość . W ten sposób każda ścieżka jest mierzona przy użyciu tego samego standardu. Routery otrzymują aktualizację RIP od bezpośrednio z nimi połączonych sąsiednich routerów. Router otrzymujący aktualizacje wysyła z kolei swoją własną aktualizację. Zanim router będzie mógł wysłać zaktualizowane ogłoszenie routingu, musi zwiększyć metrykę wszystkich poznanych ścieżek o 1. Nowa aktualizacja zostanie wysłana z adresem IP nowego routera. Ten adres IP będzie adresem routera „następnego przeskoku” (*next hop*) wprowadzonym do tablicy routingu sąsiadów, a metryka będzie określała odległość do miejsca docelowego tras prowadząc przez ten adres IP.

Pozycja w tablicy routingu utrzymuje dane o wieku informacji, adresie docelowym, następnym przeskoku lub bramie z punktu widzenia routera, lokalnym interfejsie używanym do osiągnięcia następnego przeskoku oraz koszcie trasy. Korzystając z tych informacji, router może podjąć opartą

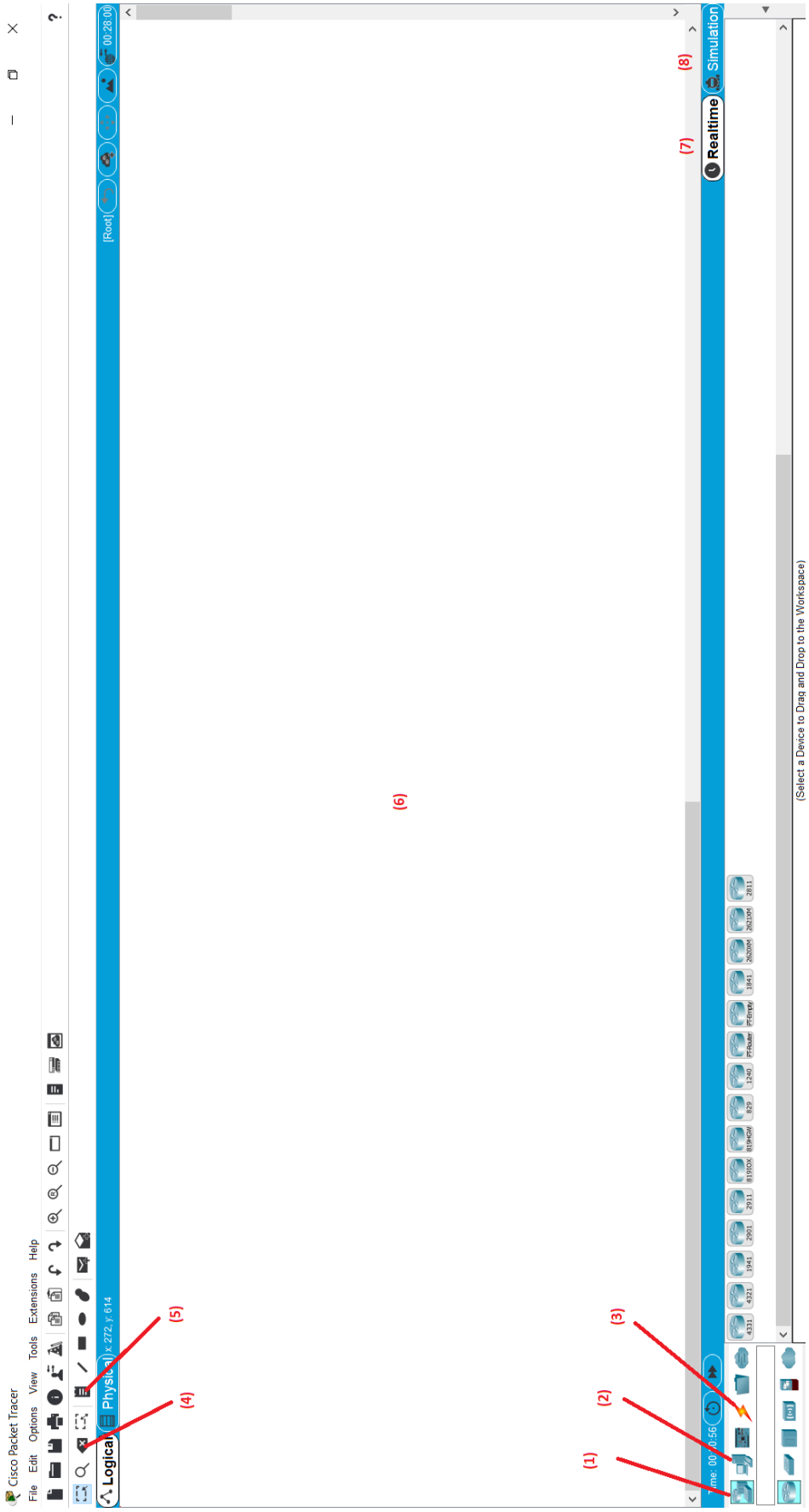
na wektorze odległości decyzje dotyczącą efektywności trasy. Ponieważ te informacje są przesyłane do sąsiednich routerów, a wszelkie wynikające stąd aktualizacje s także rozsyłane, możliwe jest „zrozumienie" topologii całego zbioru sieci dzięki dialogowi prowadzonemu tylko przez sąsiadujące ze sobą routery.

4. Oprogramowanie Cisco Packet Tracer

Oprogramowanie Cisco Packet Tracer jest symulatorem sieciowym, który pozwala tworzyć zaawansowane topologie oraz konfigurować urządzenia w sieci bez większych ograniczeń. Podstawową zaletą symulatora jest możliwość konfiguracji urządzeń w sposób kompletnie darmowy bez konieczności zakupu jakiejkolwiek infrastruktury sieciowej. W celu pobrania i zainstalowania oprogramowania symulacyjnego Cisco Packet Tracer należy zarejestrować się na stronie darmowych kursów Cisco znajdujących się na stronie:
https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer

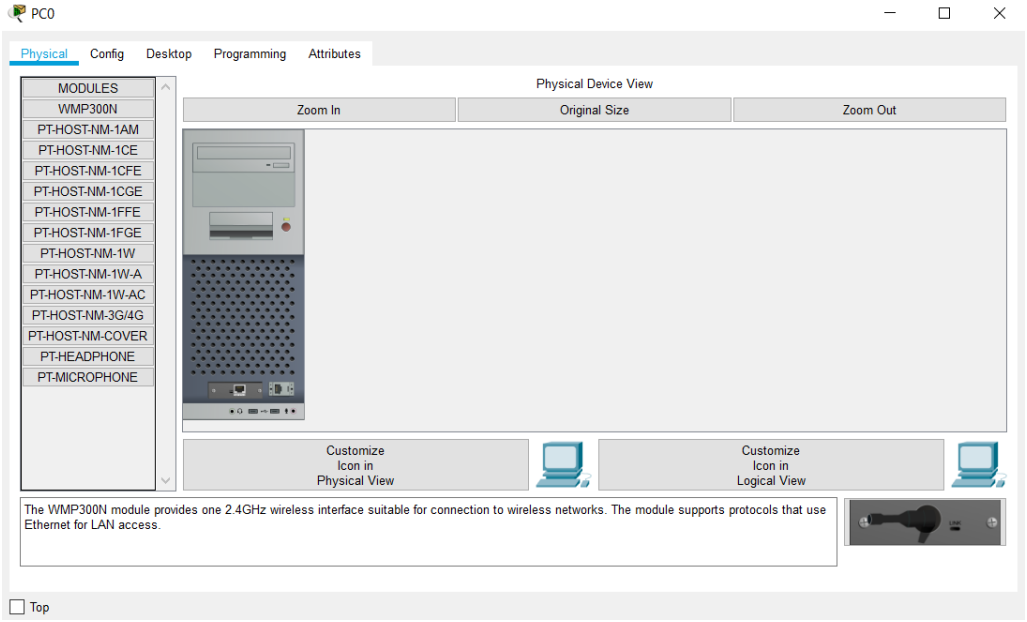
Aby zarejestrować się należy kliknąć żółty przycisk „Sign up today !". Następnie należy wypełnić kwestionariusz na stronie oraz aktywować swoje konto Cisco odbierając mail aktywacyjny przesłany po wypełnieniu kwestionariusza. Oprogramowanie można pobrać ze strony Cisco lub z Okna PW. Po uruchomieniu oprogramowania należy wpisać login i hasło przypisane do założonego konta Cisco aby program symulacyjny zaczął działać.

Okno programu symulacyjnego przedstawiono na rysunku 4.1. wraz z zaznaczeniem jego podstawowych elementów funkcjonalnych które będą wykorzystywane w trakcie zajęć. Na zajęciach będą wykorzystywane komponenty w postaci urządzeń sieciowych (1), urządzeń końcowych (2) i media transmisyjne kablowe (3). Wśród urządzeń sieciowych do tych podstawowych wykorzystywanych można wyróżnić routery, przełączniki, huby, urządzenia bezprzewodowe, urządzenia zabezpieczające oraz emulator „chmury" sieciowej. Wśród urządzeń końcowych sieci na uwagę w ramach zajęć będą zasługiwać komputery PC, laptopy i serwery. Z pozostałych elementów w ramach tych ćwiczeń nie będziemy korzystać. Na uwagę zasługują jeszcze elementy Del (4) do usuwania elementów z obszaru roboczego programu symulacyjnego oraz Place Note (5) umożliwiający wpisanie dowolnego tekstu w obszarze roboczym programu (6). Oprogramowanie można uruchomić w trybie symulacji (7) lub w czasie rzeczywistym (8), który w tym ćwiczeniu będzie realizowany.

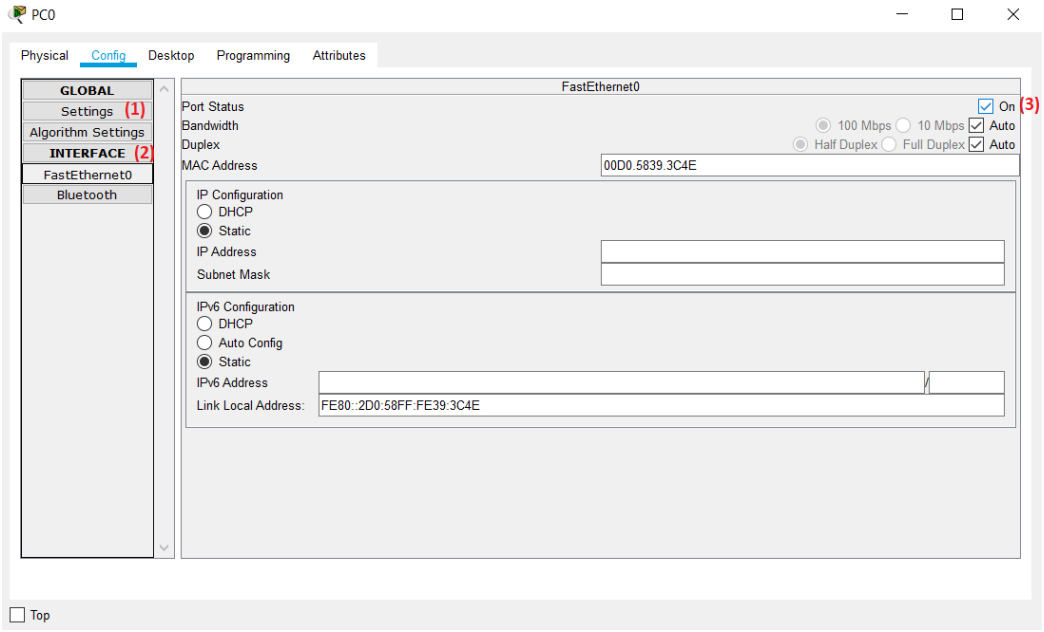


Rys. 4.1 Okno programu Cisco Packet Tracer

Większość z elementów wykorzystywanych na zajęciach posiada swój fizyczny obraz reprezentowany jako panel frontowy urządzenia przedstawiony na rysunku 4.2. Najważniejszymi elementami urządzeń uczestniczących w symulacji sa ich parametry sieciowe (1) oraz rodzaje interfejsów (2) jakie mogą być podłączone do tych urządzeń – okablowanie miedziane, światłowód albo bezprzewodowe media typu bluetooth i wiele innych – rysunek 4.3. Aby dany interfejs był aktywny należy zaznaczyć opcję ON (3) w zakładce konfiguracji urządzenia sieciowego.

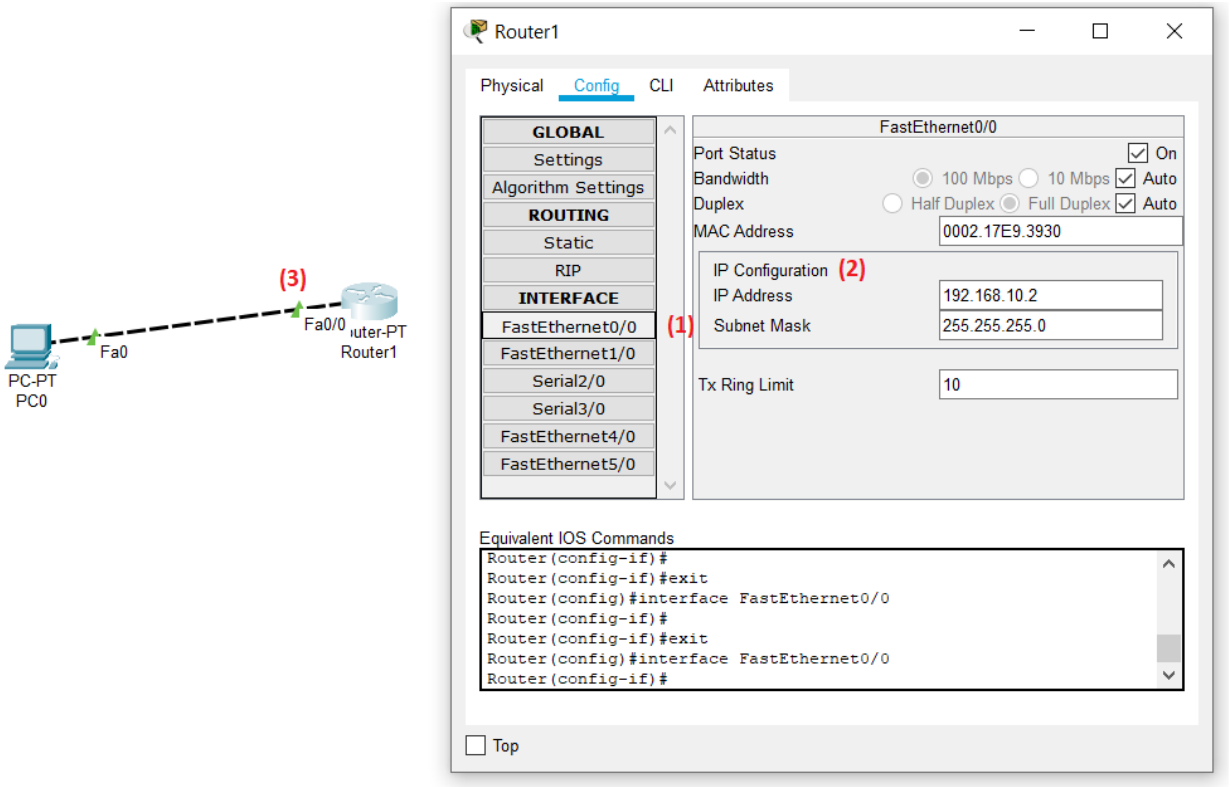


Rys. 4.2 Panel frontowy wraz z modułami komputera PC w oprogramowaniu Cisco Packet Ttracer



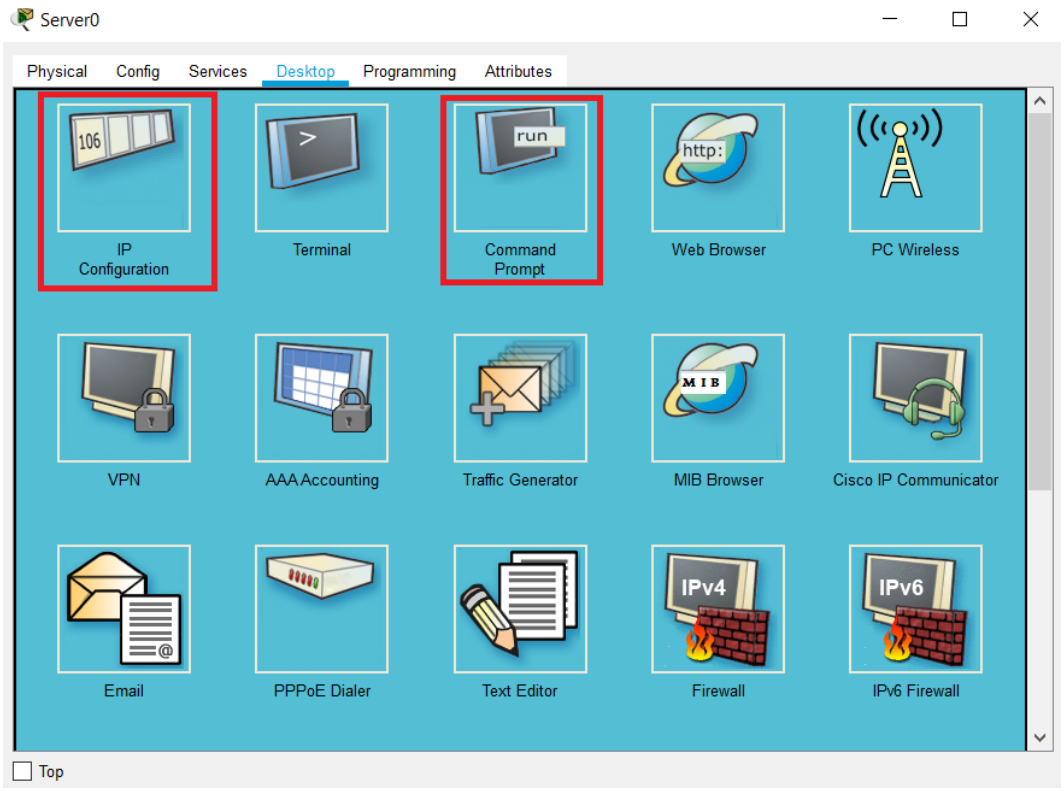
Rys. 4.3 Zakładka konfiguracji komputera PC w oprogramowaniu Cisco Packet Ttracer

Aby poprawnie skonfigurować urządzenie podłączone do sieci w oprogramowaniu symulacyjnym należy po podłączeniu go najechać strzałką na medium transmisyjne aby oznaczenie rodzaju interfejsu (1) jaki został przydzielony przez program po podłączeniu urządzenia do sieci – rysunek 4.4. przedstawia w tym przypadku Fa0/0 czyli FastEthernet0/0. Można również samodzielnie wybrać rodzaj medium jakie będzie wykorzystywane do spinania urządzeń w sieci. Poprawna konfiguracja nadania numerów IP (2) urządzeniom sieciowym sygnalizowana jest zaświeceniem się na zielono węzłów sieci (3) jak przedstawiono na rysunku 4.4.



Rys. 4.3 Zakładka konfiguracji routera w oprogramowaniu Cisco Packet Ttracer

Dodatkowo oprócz zakładek konfiguracji urządzeń sieciowych, podstawowymi parametrami które będą konieczne do modyfikacji i uzupełnienia podczas realizacji ćwiczenia są parametry sieciowe IP configuration oraz konsola Command Prompt znajdujące się w zakładce desktop urządzenia sieciowego. Zakładka wraz z opcjami zaznaczonymi na czerwono została przedstawiona na rysunku 4.4.



Rys. 4.4 Zakładka desktop urządzenia sieciowego w oprogramowaniu Cisco Packet Ttracer

5. Uwagi praktyczne

Pod żadnym pozorem nie należy „upraszczać" ćwiczenia i próbować wykonywać pomiarów/obserwacji jednocześnie z kilku punktów instrukcji. Jest to najszybsza droga do pomyłki co skutkuje odrzuceniem sprawozdania.

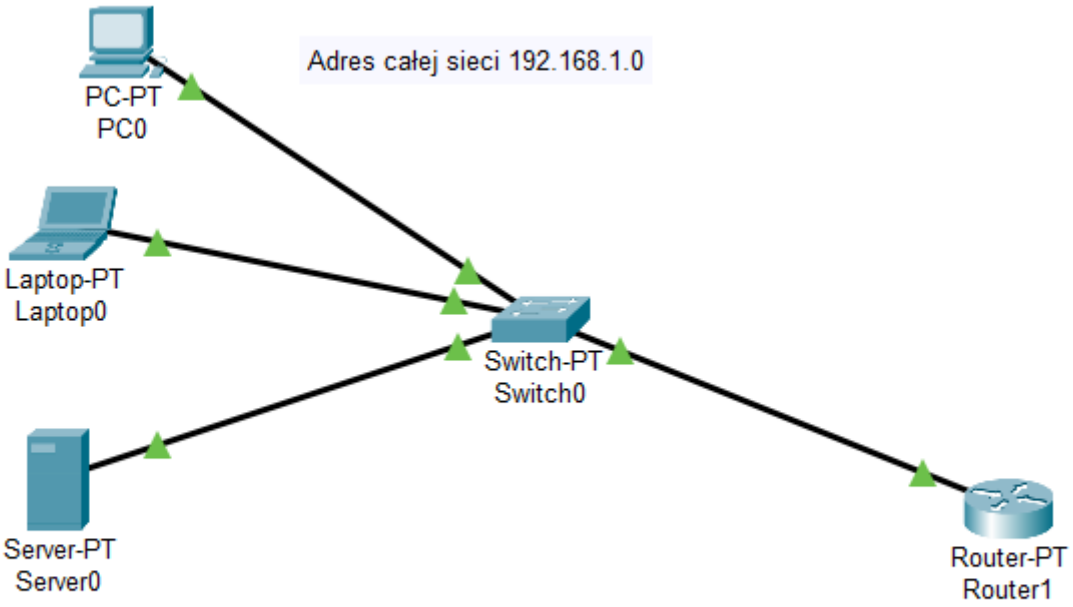
Dla uproszczenia i zwiększenia przejrzystości instrukcji wprowadzono poniższe symbole, które zostały wykorzystane w tekście:

zapisz przebieg lub zrzut ekranu/okna na dysku,

pytanie, na które odpowiedź musi znaleźć się w sprawozdaniu.

6. Przebieg ćwiczenia

6.1 Uruchom na komputerze PC oprogramowanie symulacyjne Cisco Packet Tracer. Utwórz podstawową sieć komputerową LAN składającą się komputera PC, laptopa oraz serwera. Elementy te powinny być podłączone do przełącznika sieciowego oraz przełącznik do routera będącego zakończeniem sieci i zarówno wyjściem tej sieci na zewnątrz. Elementy sieci należy połączyć zgodnie ze schematem 6.1 przedstawionym poniżej.



Rys. 6.1 Struktura sieci LAN1

UWAGA !

Pamiętaj że do celów ćwiczenia adres całej sieci LAN1 musi być 192.168.1.0. natomiast adres bramy sieciowej powinien być 192.168.1.1., maska podsieci domyślna nadana przez system.

Na podstawie wstępnej konfiguracji sieci podanej powyżej proszę samodzielnie skonfigurować pozostałe adresy IP urządzeń znajdujących się w sieci LAN w odpowiedni sposób zgodnie z ogólnie przyjętą konwencją nadawania numerów IP w sieciach LAN zgodnie z informacjami przedstawianymi na zajęciach wykładowych. Poprawnie skonfigurowana sieć na schemacie powinna sygnalizować zielonym zaświeceniem się poszczególnych portów urządzeń w sieci jak to jest pokazane na rysunku 6.1.

6.3 W celu weryfikacji poprawności podłączenia urządzeń w sieci LAN należy sprawdzić dostępność urządzeń w tak utworzonej sieci. W tym celu należy uruchomić z laptopa konsolę Command Prompt i wpisać polecenie ping do poszczególnych adresów IP każdego z elementów utworzonych w sieci LAN wraz z routerem (4 elementy aktywne sieci LAN). Może zaistnieć sytuacja gdy część pakietów zostanie utracona i wtedy należy po pewnym czasie ponownie zastosować

polecenie ping w celu sprawdzenia widoczności danego elementu aktywnego w sieci (dlaczego tak się dzieje ?). Należy zrobić zrzut ekranu z konsoli z wynikami polecenia ping poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników. Czy wszystkie urządzenia w utworzonej sieci są widoczne i odpowiadają na polecenie ping ?

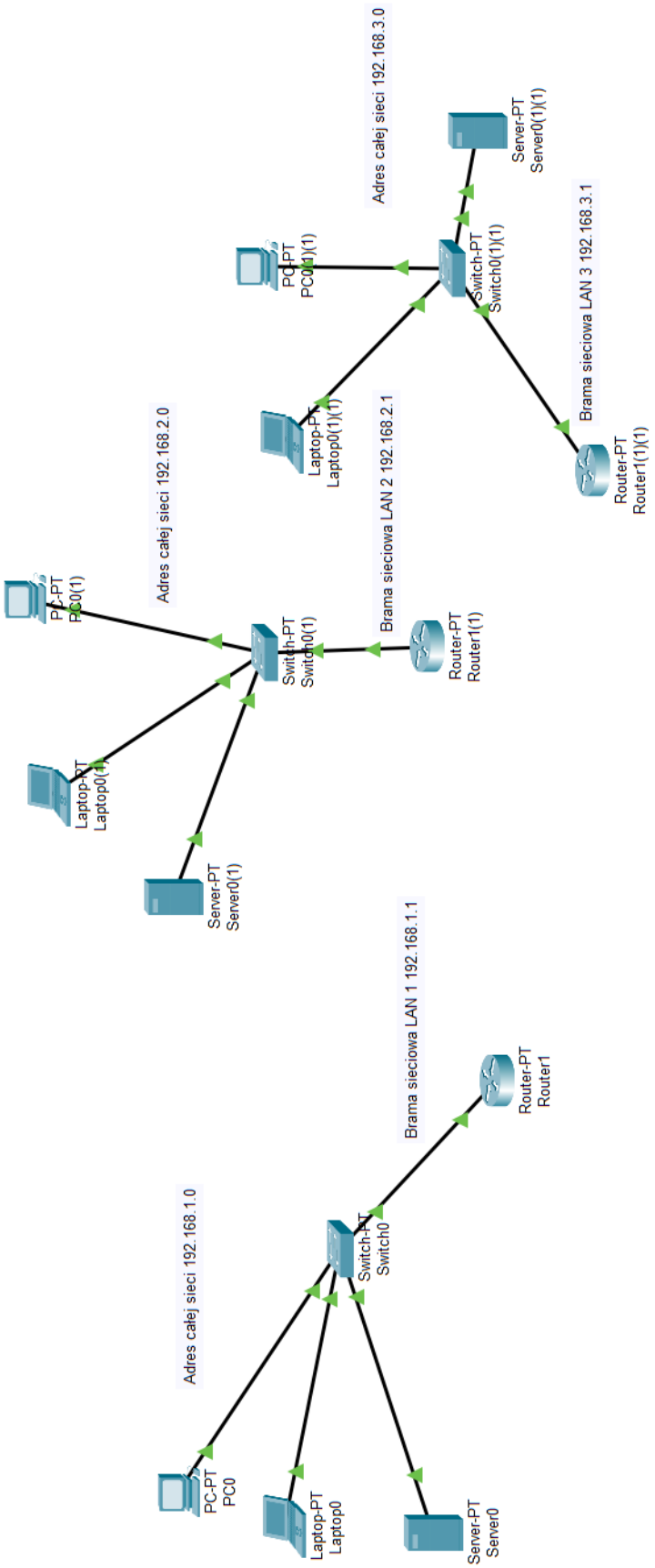
Jeżeli nie to dlaczego i od czego to zależy ?

6.4 W podobny sposób należy sprawdzić trasę jaką pokonują pakiety w utworzonej sieci do poszczególnych urządzeń w sieci LAN. W tym celu należy wpisać w konsoli Command Prompt laptopa polecenie tracert. W podobny sposób, jak powyżej należy zrobić zrzut ekranu z konsoli z wynikami polecenia tracert poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników. Co oznaczają wyniki otrzymane poleceniem tracert ? Ile elementów sieci bierze udział w trasowaniu pakietów w danej sieci w każdym z analizowanych przypadków ? Co się dzieje w przypadku użycia polecenia tracert na urządzeniu z którego następuje analiza trasowania pakietów i dlaczego tak się dzieje ?

6.5 W kolejnym kroku proszę utworzyć dwie dodatkowe sieci LAN2 i LAN3, w podobny sposób jak miało to miejsce w punkcie 6.1, do utworzonej już poprzednio sieci LAN1 z punktu 6.1. Kolejne sieci LAN2 i LAN3 powinny mieć adresy IP odpowiednio **192.168.2.0** oraz **192.168.3.0**, struktura sieci podobnie jak pokazano na rysunku 6.2 poniżej.

Uwaga !

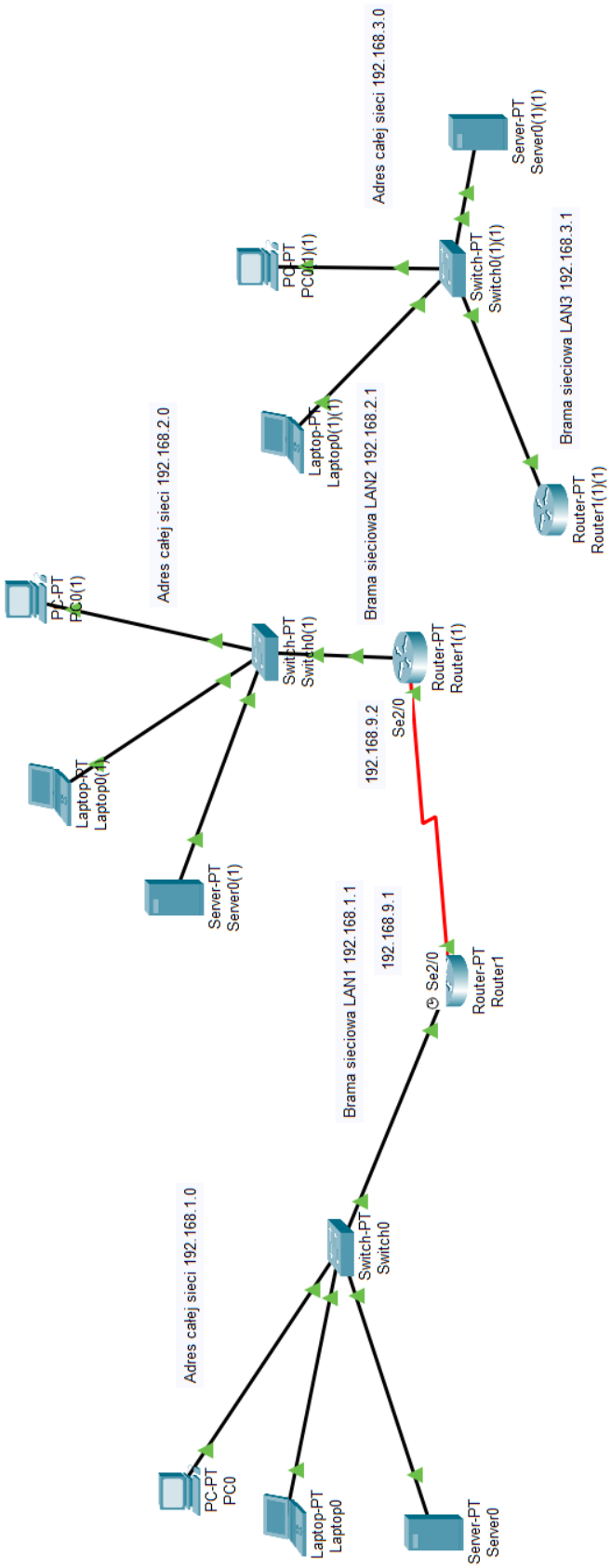
Tym razem należy włączyć usługę DHCP w każdym z serwerów znajdujących się w każdej z trzech utworzonych sieci LAN. W ten sposób każdy z elementów sieci LAN otrzyma z serwera swój własny indywidualnie nadany adres IP w sieci. Należy pamiętać aby na serwerach ustawić również poprawny adres IP bramy sieciowej każdej podsieci. Należy również sprawdzić czy poszczególne urządzenia w sieci otrzymały z serwera DHCP adresy IP wraz z poprawnymi adresami bram sieciowych których adresy IP odpowiadają urządzeniom końcowym poszczególnych sieci LAN czyli Routerom-PT na końcach sieci.



Rys. 6.2 Struktury kolejnych podsieci LAN

6.6 Analogicznie jak to miało miejsce w punkcie 6.3 instrukcji należy sprawdzić dostępność urządzeń w każdej z trzech utworzonych sieci LAN z aktywną usługą DHCP w każdym z serwerów sieci LAN. Należy zrobić zrzut ekranu z konsoli Command Prompt z wynikami polecenia ping poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników. Czy wszystkie urządzenia w utworzonych sieciach są widoczne i odpowiadaja na polecenie ping ?

6.7 Należy połączyć routery zewnętrzne na razie dwóch utworzonych sieci LAN ze sobą w sposób przedstawiony na rysunku 6.3. Routery należy połączyć kablem automatycznie dobranym przez program symulacyjny czyli domyślnie kabel szeregowy Serial2/0 lub Serial3/0 dobrany w zależności od dostępnych portów w poszczególnych routerach. Następnie należy odpowiednio skonfigurować adresy IP po dwa adresy portów wyjściowych dla każdego routera zgodnie ze schematem na rysunku 6.3. Poprawne połączenie jest sygnalizowane zielonym zaświeceniem się poszczególnych portów urządzeń w sieci.



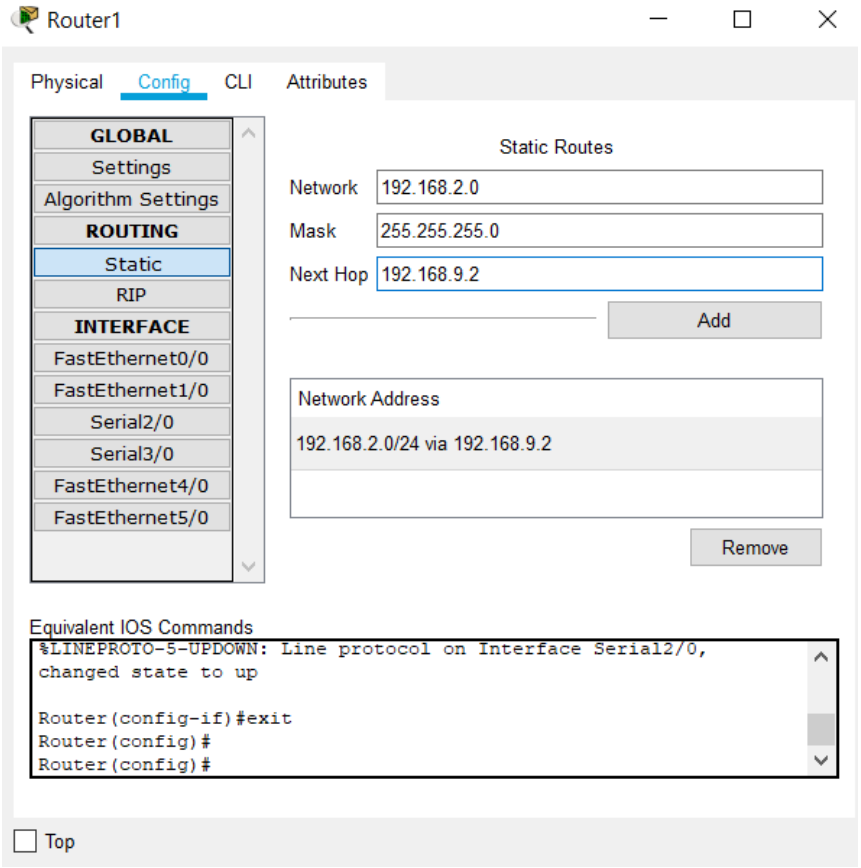
Rys. 6.3 Struktura połączenia i numeracji IP portów poszczególnych routerów sieci LAN1 i LAN2

6.7 Należy sprawdzić czy urządzenia sieciowe w połączonych dwóch sieciach LAN1 i LAN2 są widoczne i osiągalne z poziomu pierwszej sieci LAN1 i odwrotnie z poziomu drugiej sieci LAN2. W tym celu należy w konsoli Command Prompt aktywnego elementu sieciowego (laptop, PC lub serwer) każdej z dwóch połączonych sieci LAN na rysunku 6.3 wpisać polecenie ping z numerem IP elementu docelowego w celu sprawdzenia widoczności urządzeń z sąsiedniej sieci LAN. Należy zrobić zrzut ekranu z konsoli Command Prompt z wynikami polecenia ping poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników.

Czy wszystkie urządzenia w połaczonych sąsiadujących dwóch sieciach LAN1 i LAN2 są widoczne między sobą i odpowiadaja na polecenie ping ?

Jeżeli nie to dlaczego tak się dzieje i co należy zrobić ?

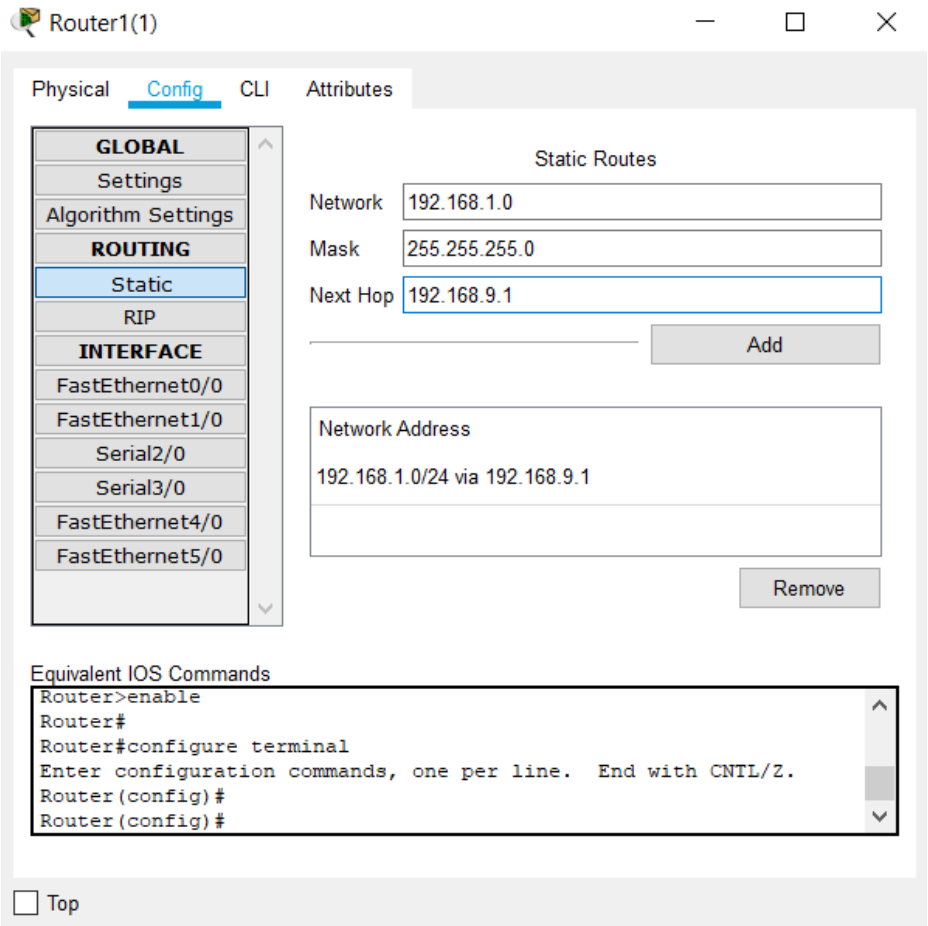
6.8 Aby elementy sieci LAN1 były widoczne z poziomu sieci LAN2 i odwrotnie należy w każdym z routerów brzegowych sieci LAN1 i LAN2 wpisać odpowiednie reguły routowania. W tym celu w routerze brzegowym sieci LAN 1 (Router1 na rysunku 6.3) należy wpisać regułę routingu zgodnie z rysunkiem 6.4.



Rys. 6.4 Konfiguracja reguł dla routera Router1 sieci LAN 1

Czy teraz urządzenia sieciowe sieci LAN2 są widoczne z poziomu sieci LAN1 i odwrotnie ? Dlaczego tak się dzieje i co należy zrobić ?

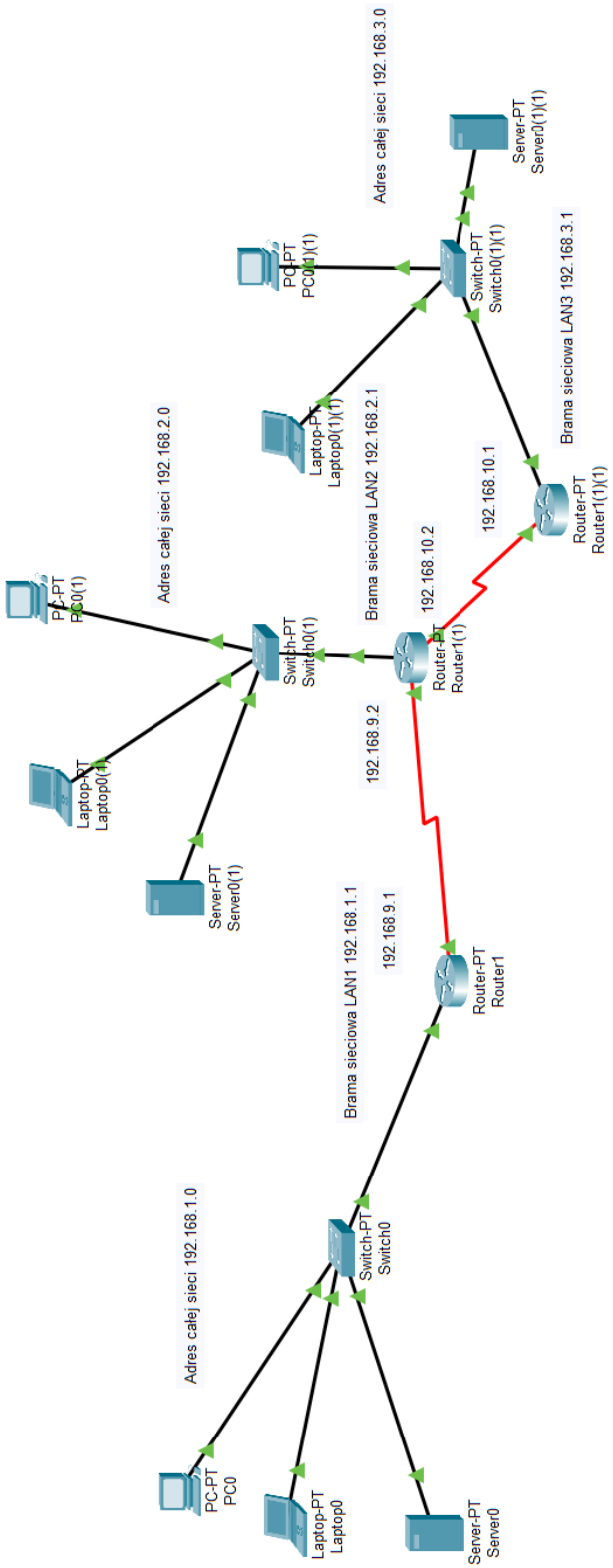
6.8 Aby poprawić sytuację należy skonfigurować również router sieci LAN2 tak by pakiety przesyłane z jednej sieci do drugiej mogły wrócić z powrotem do sieci z której zostały wysłane. Należy wpisać regułę routingu dla routera sieci LAN2 o nazwie Router1(1) na rysunku 6.3, zgodnie z rysunkiem 6.5.



Rys. 6.5 Konfiguracja reguł dla routera Router1(1) sieci LAN 2

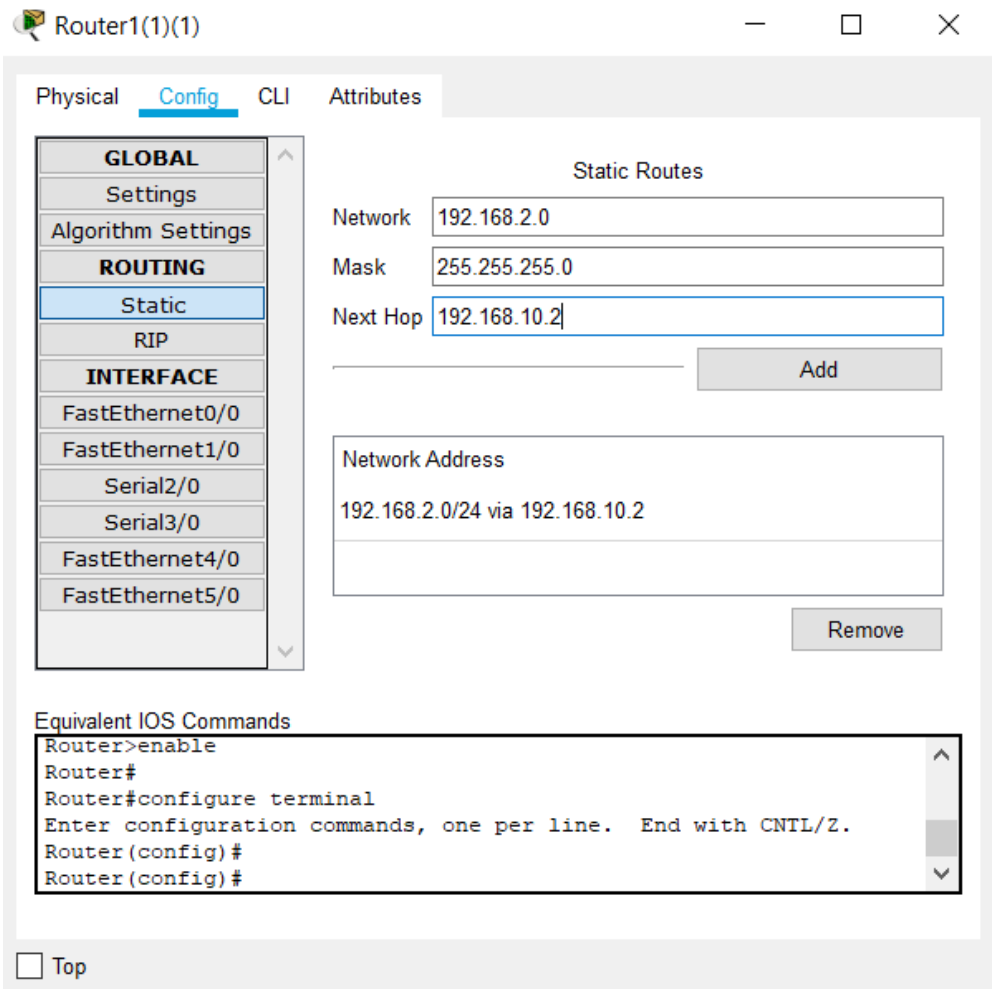
Czy teraz urządzenia sieciowe sieci LAN2 są widoczne z poziomu sieci LAN1 i odwrotnie ? Należy zrobić zrzut ekranu z konsoli Command Prompt z wynikami polecenia ping poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników. Wyjaśnij dlaczego tak się dzieje i napisz interpretacje otrzymanych wyników w sprawozdaniu.

6.8 Kolejnym krokiem jest podłączenie trzeciej sieci LAN3 i odpowiednia konfiguracja protokołów routowania w tej sieci. W tym celu podłącz sieć LAN3 do sieci LAN2 zgodnie z rysunkiem 6.6. i numeracją IP poszczególnych portów routerów.

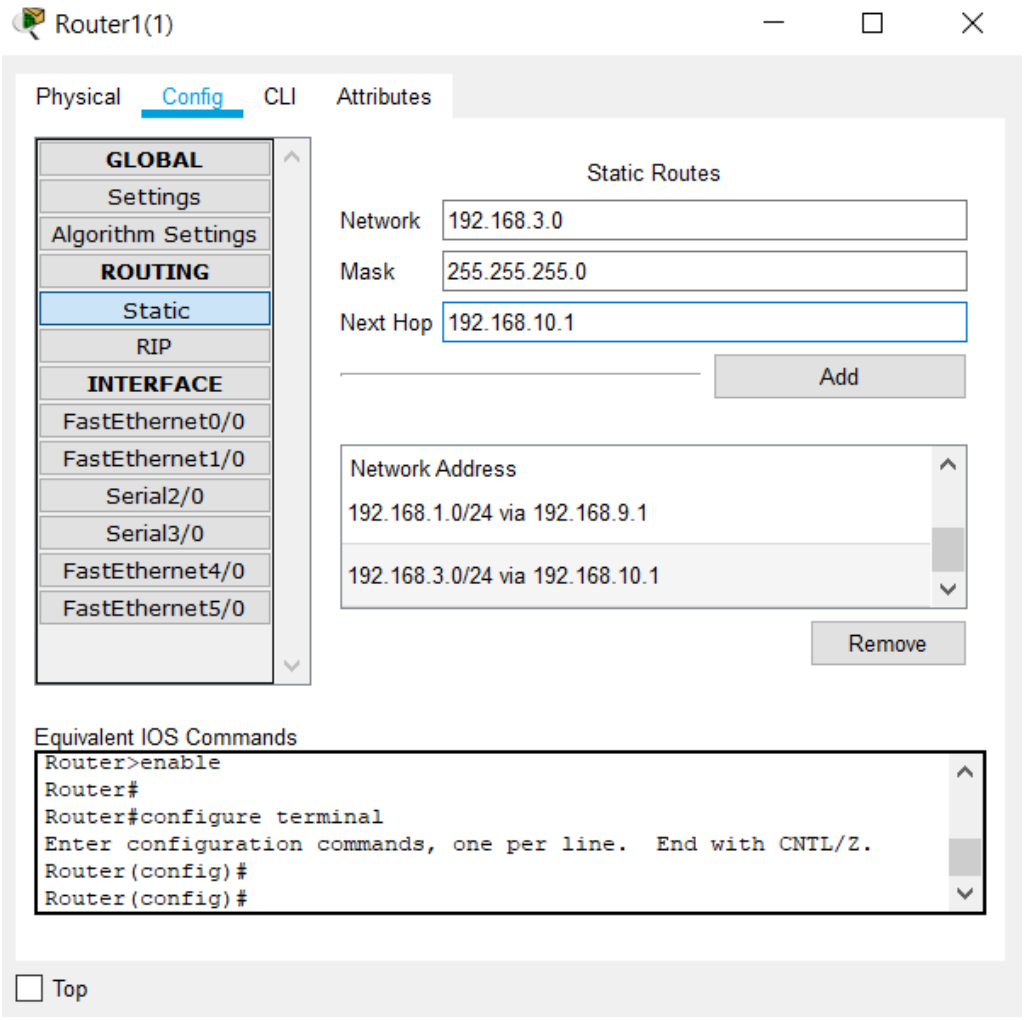


Rys. 6.6 Struktura połączenia i numeracji IP portów poszczególnych routerów sieci LAN3 i LAN2

6.9 Kolejnym krokiem jest poprawna konfiguracja reguł routowania statycznego dla routerów LAN2 i LAN3. W tym celu należy wpisać regułę routingu zgodnie z rysunkami 6.7 i 6.8 odpowiednio dla routera sieci LAN3 o nazwie Router1(1)(1) z rysunku 6.6 oraz routera sieci LAN2 o nazwie Router 1(1) z rysunku 6.6.



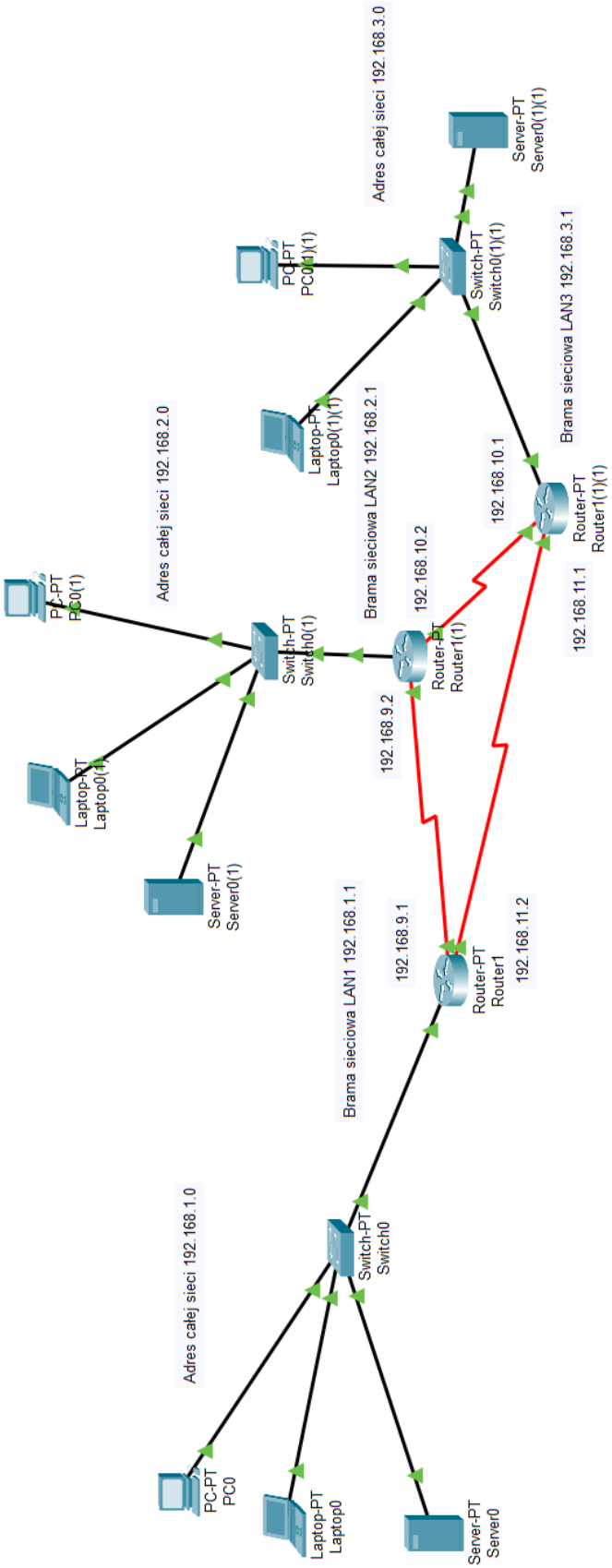
Rys. 6.7 Konfiguracja reguł dla routera Router1(1)(1) sieci LAN3



Rys. 6.8 Konfiguracja reguł dla routera Router1(1) sieci LAN2

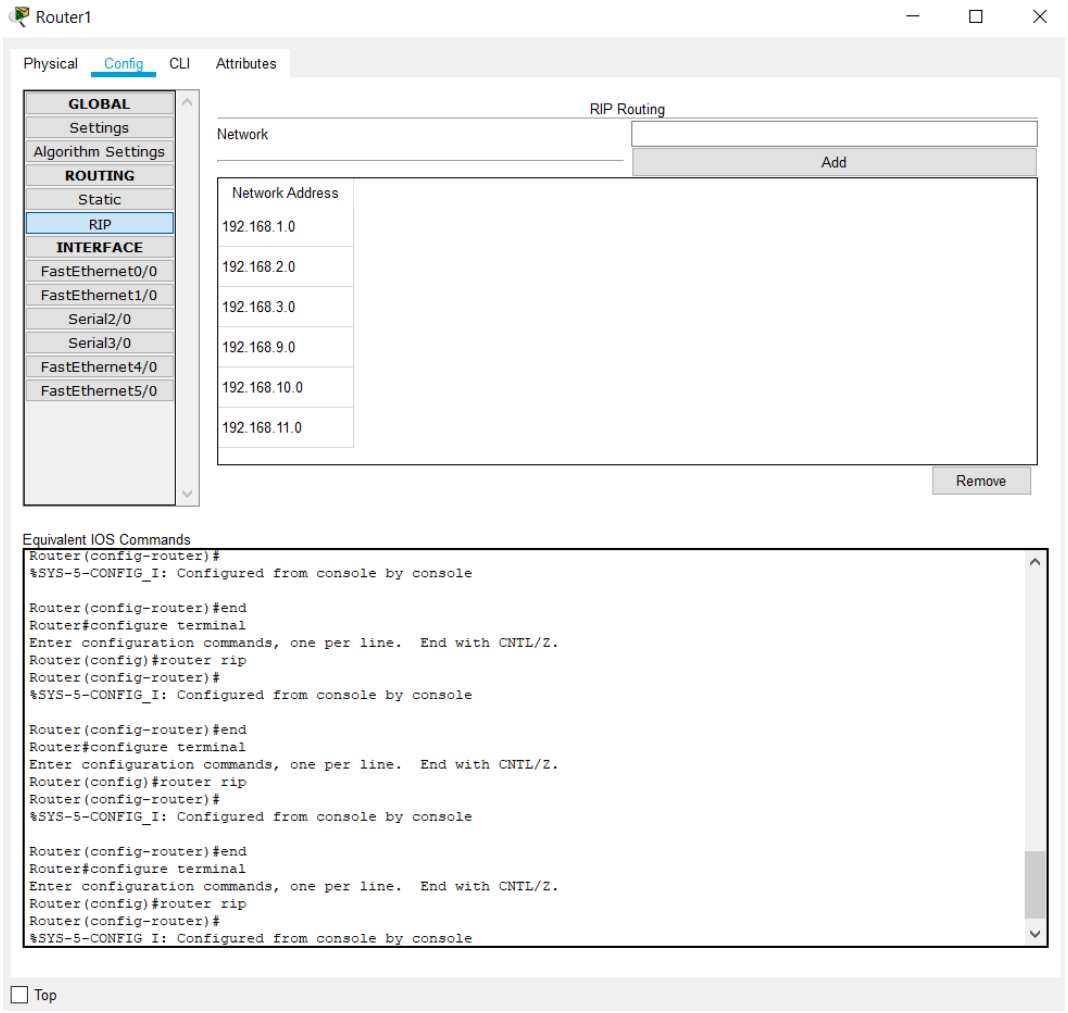
6.10 Należy teraz sprawdzić, analogicznie jak poprzednio, widoczność urządzeń sieciowych w poszczególnych sieciach LAN. Należy zrobić zrzut ekranu z konsoli Command Prompt z wynikami polecenia ping poszczególnych elementów sieci załączając je do sprawozdania wraz z interpretacją otrzymanych wyników. Które elementy sieciowe są niewidoczne z innej sieci i jakiej ?

6.11 Na podstawie dotychczasowych wyników i doświadczenia należy samodzielnie podłączyć trzeci router do pozostałych dwóch routerów w magistrali pierścieniowej i poprawnie skonfigurować reguły routowania poszczególnych routerów tak by wszystkie elementy sieci LAN1, LAN2 i LAN3 były widoczne i osiągalne dla siebie w sieci. Strukturę sieci należy połączyć zgodnie z rysunkiem 6.9 oraz samodzielnie wpisać reguły do poszczególnych routerów. Podobnie jak poprzednio należy sprawdzić widoczność i dostępność urządzeń sieciowych z każdej z trzech podłączonych sieci LAN1, LAN2 i LAN3. Wyniki i wnioski opisać w sprawozdaniu.



Rys. 6.9 Struktura połączenia i numeracji IP portów poszczególnych routerów sieci LAN1, LAN2 i LAN3

6.12 Kolejnym krokiem jest utworzenie reguł dynamicznego routingu RIP dla routerów znajdujących się w cieci przedstawionej na rysunku 6.9. Wykorzystując protokół RIP należy samodzielnie przekonfigurować reguły statyczne na reguły dynamiczne i sprawdzić widoczność poszczególnych elementów w sieciach LAN1, LAN2 i LAN3. Na początku w tym celu należy skonfigurować router1 sieci LAN1 z rysunku 6.9. Należy usunąć wszystkie reguły routowania statycznego i zastąpić je regułami routingu dynamicznego RIP wpisując zakresy wszystkich dostępnych sieci znajdujących się w pobliżu routera brzegowego sieci LAN1 zgodnie z rysunkiem 6.10.



Rys. 6.10 Konfiguracja reguł routingu dynamicznego RIP dla routera Router1 sieci LAN1

Należy sprawdzić widoczność elementów poszczególnych sieci LAN. Czy wszystkie elementy sieci poszczególnych sieci LAN są widoczne ? Dlaczego tak się dzieje ?

6.13 W tym kroku należy samodzielnie przekonfigurować pozostałe routery wszystkich sieci LAN1, LAN2 i LAN3 tak by wszystkie urządzenia aktywne (komputery PC, laptopy i serwery) były widoczne i osiągalne z każdego punktu sieci. Należy przedstawić wyniki w postaci zrzutów ekranu poleceń ping poszczególnych elementów sieci z interpretacja wyników. To samo proszę wykonać dla polecenia tracert z poszczególnych urządzeń aktywnych sieci LAN1, LAN2 i LAN3 wraz z interpretacją przedstawionych wyników w postaci zrzutów ekranu z konsoli Command Prompt poszczególnych urządzeń z których wykonywana była operacja odpowiedzi poleceniem ping i trasowania pakietów poleceniem tracert. 

1. Literatura:

[1] Materiały wykładowe z przedmiotu systemy komutacyjne.

[2] Karanjit S. Siyan, Tim Parker., *TCP/IP. Księga eksperta. Wydanie II*, Wydawnictwo Helion, Warszawa 2000r.

[3] Kabaciński W., Żal M., *Sieci telekomunikacyjne*, WKiŁ, Warszawa 2008r.