

Instrukcja laboratoryjna z przedmiotu: Sieci komputerowe

Ćwiczenie 1: Model OSI. Enkapsulacja danych

Marta Szarmach
Zakład Telekomunikacji Morskiej
Wydział Elektryczny
Uniwersytet Morski w Gdyni

02.2022

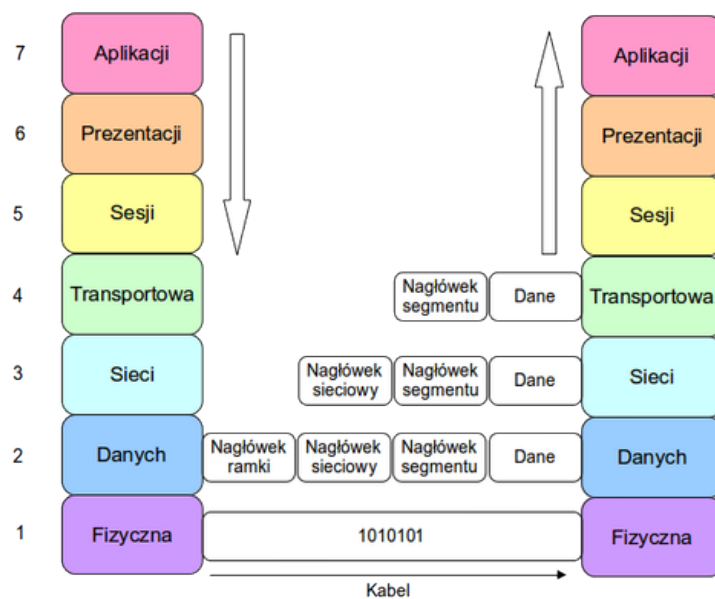
I. Wprowadzenie

Założeniem **modelu OSI** jest podział sieci komputerowej na 7 warstw. Każda z warstw pełni dedykowaną rolę, na każdej działają inne protokoły (wymienne w ramach warstwy bez wpływu na działanie pozostałych warstw), przykładowo:

- warstwa 1. — **fizyczna** — zapewnia przesył danych poprzez wskazane medium transmisyjne,
- warstwa 2. — **łącza danych** — ma za zadanie przekazać dane wewnątrz sieci lokalnej, to ona zarządza dostępem do medium transmisyjnego, najpopularniejszy na tej warstwie jest protokół **Ethernet**,
- warstwa 3. — **sieciowa** — odpowiada za przekazywanie danych pomiędzy sieciami (routing), działa tu m.in. protokół **IP**,
- warstwa 4. — **transportowa** — przekazuje dane do konkretnej usługi na wskazanym urządzeniu zdalnym (np. poprzez protokół **TCP** czy **UDP**),
- warstwa 7. — **aplikacyjna** — stanowi miejsce, w którym użytkownik generuje dane wprowadzane do sieci poprzez dedykowane aplikacje (przeglądarkę internetową, klienta poczty elektronicznej, itp.).

Kiedy dane przekazywane są z warstwy wyższej do warstwy niższej, następuje proces **enkapsulacji**. Dane spływające z wyższej warstwy stanowią zawartość (ładunek) jednostki danych niższej warstwy, po czym dodawany jest do nich nagłówek z danymi niezbędnymi do prawidłowego działania tej warstwy (np. zapewniające zlokalizowanie urządzenia docelowego):

- dane z warstw wyższych (aplikacyjnej-sesji) zamykane są na warstwie transportowej w tzw. **segmenty**,
- segmenty z warstwy transportowej stanowią zawartość **pakietów** na warstwie sieciowej,
- pakiet otoczony nagłówkiem warstwy łącza danych tworzy **ramkę**,
- na warstwie najniższej (fizycznej) ramki konwertowane są na bity, a bity na poziomy napięcie, impulsy świetlne, zmodulowane fale elektromagnetyczne, itp.



Źródło: <https://sieci.infopl.info/>

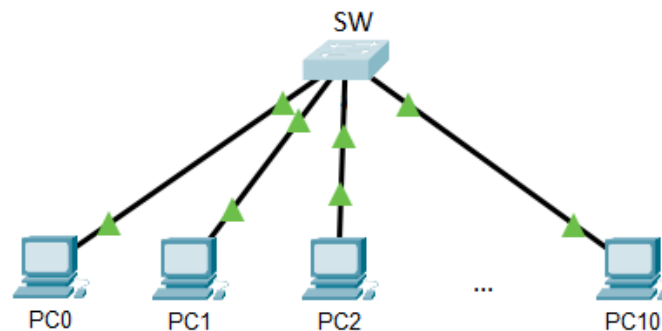
II. Cel ćwiczenia

Celem niniejszego ćwiczenia jest zapoznanie się z funkcjonowaniem modelu OSI w sieciach komputerowych poprzez:

- przechwytywanie w programie Wireshark prostego ruchu sieciowego, odczytywanie zawartości nagłówków dodawanych przez protokoły na każdej warstwie modelu OSI i zaobserwowanie procesu enkapsulacji danych,
- zbudowanie i skonfigurowanie prostej sieci laboratoryjnej i przeanalizowanie błędów w konfiguracji, które mogą pojawić się na różnych warstwach modelu OSI.

III. Stanowisko laboratoryjne

Do wykonania ćwiczenia niezbędne jest stanowisko laboratoryjne składające się z komputerów klasy PC z zainstalowanym systemem Windows oraz oprogramowaniem Wireshark oraz Apache, połączonych w sieć za pomocą przełącznika sieciowego.



Do drugiej części ćwiczenia potrzebne też są przewody UTP oraz odpowiednie złączki oraz koncentrator sieciowy.

Przed przystąpieniem do ćwiczenia:

- Włącz komputer do lokalnej sieci laboratoryjnej, uruchamiając na nim kartę sieciową o nazwie *LAB*. Kliknij *Start* \Rightarrow *Ustawienia* \Rightarrow *Połączenia sieciowe*. Prawym klawiszem wybierz kartę sieciową *LAB* i kliknij *Włącz*, podobnie wybierz kartę sieciową Internet i wybierz *Wyłącz* (od tego momentu komputer straci połączenie z internetem na rzecz sieci laboratoryjnej).
- Ustaw statycznie adres IP według schematu:
IP: 172.16.1.*numer_Twojego_stanowiska*
Maska podsieci: 255.255.255.0

IV. Przebieg ćwiczenia

1 Analiza nagłówków w programie Wireshark

Wireshark jest programem służącym do przechwycenia ruchu sieciowego i jego analizy. Jeśli w sieci wystąpił jakiś problem, poprzez zaobserwowanie, jak wyglądała komunikacja w sieci, tj. jakie wiadomości były wymieniane pomiędzy urządzeniami, administrator sieciowy jest w stanie zorientować się, gdzie leży błąd i co należy poprawić.

1.1 Uruchom przechwytywanie danych.

- a) Otwórz program Wireshark: na laboratoryjnym komputerze kliknij w *Start* \Rightarrow *Programy* \Rightarrow *Wireshark*.
- b) W programie Wireshark wybierz z menu *Capture (Przechwytyuj)* \Rightarrow *Options (Opcje)*.
- c) Upewnij się, czy wybrana jest właściwa (fizyczna) karta sieciowa oraz czy zaznaczona jest opcja „*Capture packets in promiscuous mode*” („*Enable promiscuous mode on all interfaces*”). Tryb *promiscuous* umożliwia Wiresharkowi przechwytywanie wszystkich ramek, które pojawiły się na interfejsie karty sieciowej komputera, nie tylko tych adresowanych do badanego komputera, co umożliwia dokonanie głębszej analizy tego, co dzieje się w sieci.
Uwaga. Włączenie trybu *promiscuous* miało większy sens w czasach, kiedy urządzenia w sieci łączone były za pomocą koncentratora, który wysyłał otrzymane dane na każdy port. W dzisiejszych czasach bardziej popularne są switchy, które kontrolują, na który port wysłać otrzymaną ramkę, aby dotarła ona tylko do docelowego odbiorcy.
- d) Kliknij *Start*, aby rozpocząć przechwytywanie ruchu sieciowego na wybranej karcie sieciowej.

1.2 Wygeneruj ruch sieciowy.

Mając uruchomione przechwytywanie danych w programie Wireshark, pora wygenerować ruch sieciowy, aby mieć co przechwycić i analizować. W pierwszym kroku wygenerujemy prosty ruch, za pomocą polecenia *ping* zmuszając sąsiednie komputery do sprawdzenia, czy istnieje komunikacja pomiędzy nimi.

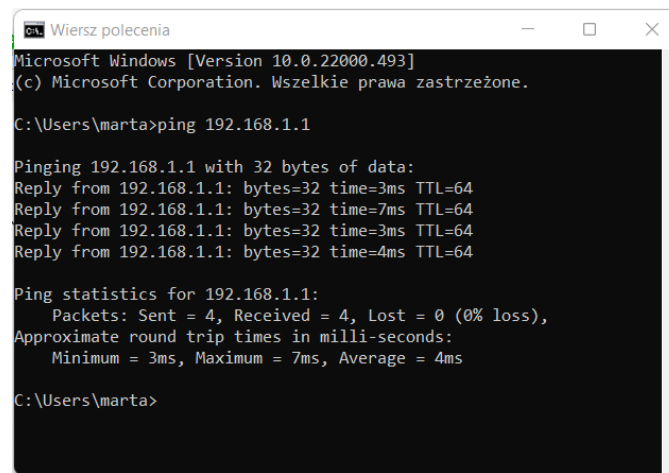
- a) Uruchom Wiersz polecenia systemu Windows (*Start* \Rightarrow *Uruchom...* \Rightarrow *cmd*).

- b) W Wierszu polecenia wydaj polecenie *ipconfig*. Pozwoli ono na sprawdzenie konfiguracji sieciowej Twojego komputera, między innymi adresu IP. Możesz też wyświetlić bardziej dokładną konfigurację:

```
ipconfig/all
```

- c) Zapytaj osobę siedzącą obok o adres IP jej komputera. Wyślij ping na adres IP tego komputera:

```
ping adres_IP_komputera
```



```
Microsoft Windows [Version 10.0.22000.493]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Users\marta>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=7ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 4ms

C:\Users\marta>
```

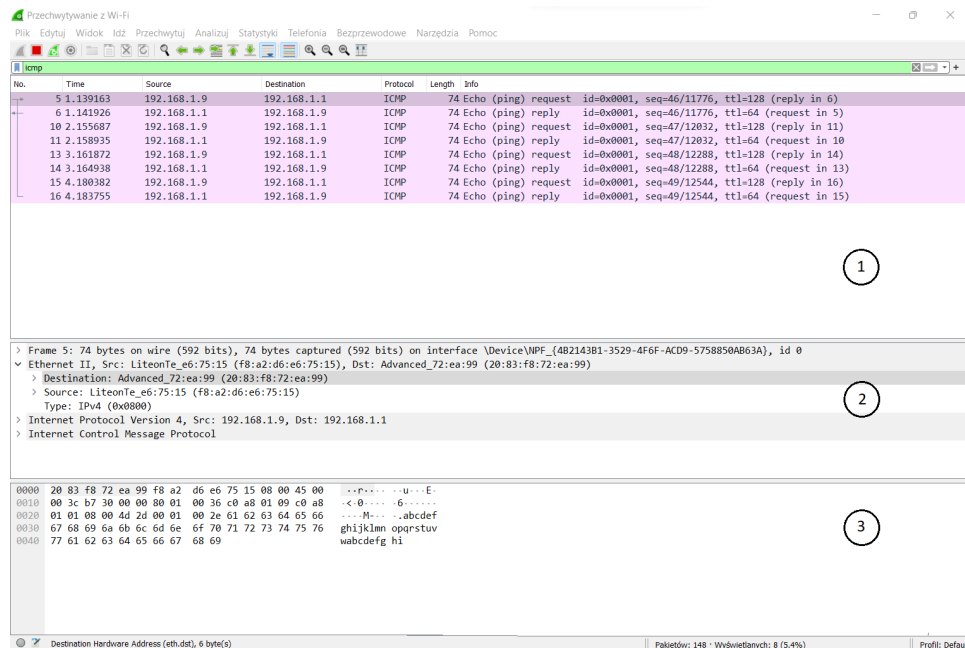
- d) Przejdź do okna z programem Wireshark. W polu *Filter* („Zastosuj filtr wyświetlania...”) wpisz nazwę protokołu, z którego ruch sieciowy chcesz oglądać (w przypadku rezultatów polecenia *ping*, będzie to protokół ICMP), aby wyświetlały się tylko interesujące nas przechwycone ramki.
- e) Zatrzymaj przechwytywanie danych, klikając albo w *Capture* (*Przechwytyj*) \Rightarrow *Stop*, albo w odpowiednią czerwoną ikonę na pasku narzędziowym.

1.3 Przyjrzyj się przechwyconemu ruchowi sieciowemu.

Wireshark, po przechwyceniu ruchu sieciowego, przedstawia go w sposób wygodny do analizy:

- wyodrębnia każdą z przechwytanych ramek i przedstawia je w formie listy (1., górna część okna),
- dla każdej przechwyconej ramki analizuje zawartość nagłówka na każdej warstwie modelu OSI (2., środkowa część okna) — można rozwinąć (klikając + lub >) interesującą nas warstwę, po czym każde pole z nagłówka protokołu na tej warstwie przedstawione jest w czytelny i zrozumiały sposób (Nazwa pola: Wartość),

- po kliknięciu interesującego nas pola, Wireshark zaznacza na granatowo, które bity przechwyconej ramki przenosiły akurat to pole (3., dolna część okna).



- a) Wybierz pierwszą ramkę (powinna to być wiadomość *Echo (ping) request*). Rozwiń sekcję dotyczącą nagłówka protokołu z warstwy łącza danych (Ethernet) i sprawdź wartości następujących pól (zweryfikuj je za pomocą komendy *ipconfig* w Wierszu polecenia):

- **Destination** — adres MAC urządzenia, na które wysłany był ping (osoby siedzącej obok),
- **Source** — adres MAC urządzenia, z którego wysłany był ping (Twojego komputera),
- **Type** — określa protokół, którego pakiet stanowi zawartość (dane) ramki ethernetowej (jest enkapsulowany w ramkę ethernetową) — powinno wskazywać na protokół IP.

Zwróć uwagę, że na warstwie 2. sieć rozpoznaje urządzenia na podstawie ich adresu MAC.

- b) Rozwiń sekcję dotyczącą nagłówka protokołu z warstwy sieciowej (IP) i sprawdź wartości następujących pól:

- **Protocol** — tak, jak w polu Type w nagłówku protokołu Ethernet, określa, z jakiego protokołu są dane stanowiące zawartość przechwy-

conego pakietu IP — powinno przyjąć wartość 1 (wskazującą na to, że enkapsulowane do pakietu IP były dane z protokołu ICMP),

- **Source Address** — adres IP urządzenia, z którego wysłany był ping,
- **Destination Address** — adres IP urządzenia, na które wysłany był ping.

Zwróć uwagę, że na warstwie 3. sieć rozpoznaje urządzenia na podstawie ich adresu IP.

- Rozwiń sekcję dotyczącą zawartości ramki (danych z protokołu ICMP) i sprawdź zawartość pola **Type** — powinno zawierać wartość 8, a więc wskazywać na to, że przechwycona ramka zawiera prośbę o odpowiedź na wysłany ping (*Echo request*).
- Kliknij na drugą przechwyconą ramkę na liście (powinna to być wiadomość *Echo (ping) reply* — odpowiedź komputera sąsiada na wysłany przez Ciebie ping). Przekonaj się, jakie nastąpiły zmiany w obserwowanych wartościach pól:
 - adresy docelowe zostały zamienione ze źródłowymi (w przypadku tej ramki, Twój komputer jest odbiorcą, a sąsiada — nadawcą),
 - w polu Type protokołu ICMP pojawiła się wartość 0 (*Echo reply*).

1.4 Powtórz ćwiczenie dla innego rodzaju ruchu sieciowego.

Na każdym z komputerów w laboratorium powinno być zainstalowane oprogramowanie Apache, za pomocą którego każdy z komputerów staje się serwerem www. Możesz zwrócić się do komputera sąsiada z prośbą o udostępnienie zasobu (jego strony internetowej) i przeanalizować wygenerowany w ten sposób ruch HTTP.

- Uruchom na nowo przechwytywanie danych w programie Wireshark, nie zapisując uprzednio przechwyconych danych: *Capture (Przechwytyuj)* ⇒ *Start* ⇒ „*Continue without saving*” („*Kontynuuj bez zapisywania*”).
- Wejdź w przeglądarkę internetową i w polu adresu wpisz adres IP komputera osoby siedzącej obok. Powinna wyświetlić Ci się prosta strona informująca o tym, że na tym komputerze uruchomione jest oprogramowanie Apache: **It works!**
- Wróć do okna Wiresharka, zatrzymaj przechwytywanie danych i przefiltruj przechwycone dane tak, by wyświetlał się jedynie ruch wygenerowany przez protokół HTTP.
- Przeanalizuj przechwycony ruch sieciowy:

- Wybierz pierwszą przechwyconą ramkę (HTTP GET). Ponownie sprawdź adresy źródłowe i docelowe na warstwie 2. oraz 3. Kto tym razem jest nadawcą, a kto odbiorcą?
- HTTP jest protokołem działającym na warstwie najwyższej, aplikacyjnej, w związku z tym widoczne są nagłówki także wyższych warstw modelu OSI. Rozwiń sekcję dotyczącą nagłówka protokołu na warstwie transportowej (TCP, *Transmission Control Protocol*) i sprawdź zawartość pola **Destination Port** — powinno przyjąć wartość 80, wskazującą na to, że przechwycony ruch jest skierowany do usługi www na komputerze sąsiada.
- Kliknij na drugą przechwyconą ramkę (odpowiedź na Twoją prośbę o udostępnienie zasobów, HTTP/1.1 200 OK). Jeszcze raz sprawdź adresy źródłowe i docelowe na obu warstwach. Sprawdź, który z portów (docelowy czy źródłowy) teraz przyjął wartość 80.

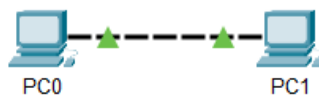
Podsumowując tę część ćwiczenia, nauczyłeś się korzystać z programu Wireshark, aby przechwytywać i analizować ruch sieciowy — w tym przypadku, przyjrzałeś się procesowi enkapsulacji danych (zamykania danych z najwyższej warstwy modelu OSI w jednostki coraz niższych warstw poprzez dodawanie dedykowanych nagłówków) i przyjrzałeś się, jakiego rodzaju dane dodawane są w nagłówkach na poszczególnych warstwach modelu OSI.

2 Budowa i konfiguracja prostej sieci laboratoryjnej

Druga część ćwiczenia pozwoli na zapoznanie się z budową i konfiguracją sieci. Należy odpowiednio połączyć urządzenia, dobierając właściwe okablowanie (co należy do warstwy fizycznej), a także zadbać o poprawną adresację IP (co jest konfiguracją na warstwie sieciowej).

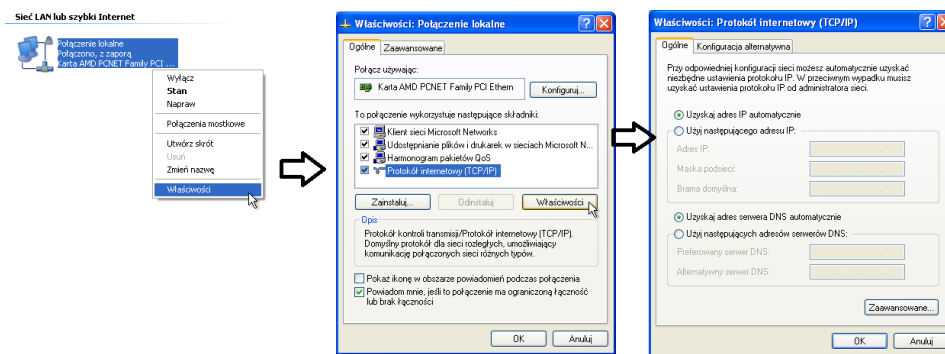
2.1 Zbuduj prostą sieć, łącząc 2 sąsiednie komputery.

- Wyjmij wtyczkę z żółtego gniazda, znajdującego się na ścianie za Twoim komputerem. Poproś prowadzącego o złączkę, po czym do jednej strony złączki wepnij kabel od swojego komputera, a do drugiej — od komputera sąsiada.



Wskazówka. Do połączenia dwóch komputerów zwyczajowo używa się kabla z przeplotem (zamienia od na jednym końcu żyły odbierające z nadającymi). W dzisiejszych czasach jednak, gdy istnieje system auto MDI-X wykrywający typ kabla i odpowiednio zamieniający żyły, dobór kabla nie jest aż tak istotny jak kiedyś.

- b) Skonfiguruj adres IP na komputerze. Wejdź w ustawienia karty sieciowej LAB na swoim komputerze (*Start* \Rightarrow *Ustawienia* \Rightarrow *Połączenia sieciowe*; kliknij prawym klawiszem na kartę sieciową LAB i wybierz *Właściwości*, zaznacz *Protokół internetowy (TCP/IP)* i wybierz *Właściwości*).



Wybierz „Użyj następującego adresu IP” i wpisz, po uzgodnieniu z sąsiadem, następujące ustawienia:

- **Adres IP** na pierwszym komputerze: 192.168.0.1
- **Adres IP** na drugim komputerze: 192.168.0.2
- **Maska podsieci** na obu komputerach: 255.255.255.0

- c) Sprawdź poprawność komunikacji pomiędzy dwoma komputerami, wysyłając ze swojego komputera ping na adres komputera sąsiada. W razie niepowodzenia sprawdź poprawność podłączenia oraz adresacji IP, a następnie skonsultuj się z prowadzącym.

2.2 Zasymuluj niektóre błędy, mogące pojawić się podczas budowania sieci.

- a) Zasymuluj błąd w okablowaniu, tj. na warstwie fizycznej, poprzez odpięcie od złączki kabla od jednego z komputerów. Zaobserwuj, jak system Windows na odpiętym komputerze informuje o błędzie komunikatem „Kabel sieciowy jest odłączony”. Czy na drugim (nieodpiętym) komputerze pojawił się jakikolwiek komunikat o błędzie? Spróbuj wysłać ping na sąsiedni komputer (powinien zakończyć się niepowodzeniem). Napraw błąd, podłączając właściwie kabel.

Zapamiętaj. Błędy, które mogą wystąpić na warstwie fizycznej:

- źle podłączone okablowanie (w niewłaściwy port, niewłaściwy rodzaj kabla),
- uszkodzony lub wypięty kabel sieciowy,
- uszkodzona karta sieciowa lub port na urządzeniu pośredniczącym,
- wyłączona administracyjnie karta sieciowa lub port na urządzeniu pośredniczącym,
- uszkodzone/wyłączone urządzenie pośredniczące.

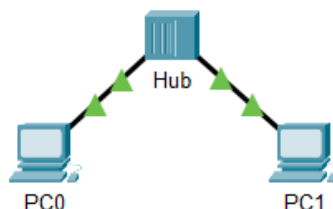
b) Zasymuluj kilka rodzajów błędów w adresacji IP, tj. na warstwie sieciowej.

- Na jednym z komputerów ustaw adres IP taki sam, jak na drugim komputerze. Zaobserwuj, jak system Windows informuje o tym komunikatem „*Konflikt adresów IP*”. Przywróć właściwą adresację.
- Na jednym z komputerów ustaw adres IP, który jest spoza sieci, która skonfigurowana jest na drugim z komputerów. Przykładowo, zachowując maskę podsieci 255.255.255.0, na jednym z komputerów zostaw adres IP 192.168.0.1, a na drugim ustaw adres IP 192.168.1.1. Czy system Windows poinformował o błędzie? Spróbuj wysłać ping na adres sąsiedniego komputera. Jaki komunikat pojawia się przy oczekiwaniu na odpowiedź? Przywróć właściwą adresację.

Zapamiętaj. Aby dwa komputery mające adresy IP z różnych posieci mogły się ze sobą komunikować, musiałyby być podłączone przez router.

2.3 Powtórz ćwiczenie, łącząc komputery za pomocą koncentratora sieciowego.

a) Poproś prowadzącego o koncentrator, podłącz urządzenie do prądu. Odłącz oba komputery od złączki, podłącz końce kabli pochodzących od obu komputerów do dwóch portów koncentratora. Tradycyjnie, powinien być tu użyty kabel prosty.



- b) Powtórz symulację błędu na warstwie fizycznej, odłączając jeden z komputerów. Na ilu komputerach tym razem pojawił się komunikat systemu Windows o odłączonym kablu sieciowym?
- c) Powtórz symulację błędów na warstwie sieciowej. Czy koncentrator wystarczy, aby komputery z dwóch podsieci mogły się ze sobą skomunikować?
- d) Przywróć stanowisko do stanu początkowego:
 - odłącz komputery od koncentratora i podłącz je z powrotem do żółtych gniazd,
 - ustaw automatyczne pobieranie adresu IP.

V. Pytania kontrolne

1. Z jakich warstw składa się sieć komputerowa według modelu OSI?
2. Czym jest enkapsulacja w sieciach komputerowych?
3. Wymień, jakie błędy mogą pojawić się podczas budowania i konfiguracji sieci na warstwie:
 - fizycznej,
 - sieciowej.