Część teoretyczna

**Model OSI** – (Open Systems Interconnection) opublikowany w 1984 roku przez ISO (International Organization for Standarization) jest jednym z powszechnie wykorzystywanych standardów komunikacji między komputerami. Struktura modelu opiera się na wielowarstwowości. Każda warstwa ma zapewniać podzbiór powiązanych ze sobą funkcji. Niższe warstwy wykonują bardziej prymitywne zadania i ukrywają szczegóły działania przed wyższymi.

W sytuacji idealnej zakłada się, że warstwy są niezależne i dokonanie zmian w jednej nie wymaga zmian w pozostałych.

Główną funkcją modelu jest zdefiniowanie zestawu warstw i ustalenie usługi świadczonej przez każdą z nich. Dodatkowo podział grupuje funkcje zgodnie z ich zastosowaniem i zapewnia liczbę warstw wygodną do zarządzania. Liczbą ustaloną przez ISO jest 7.

**Warstwy modelu OSI/ISO**

|  |
| --- |
| **7. Warstwa aplikacji**  Zawiera protokoły wykorzystywane przez użytkownika końcowego (np. HTTP). |
| **6. Warstwa prezentacji**  Odpowiada za kodowanie (enkodowanie i dekodowanie) danych w zależności od kierunku przechodzenia przez model. |
| **5. Warstwa sesji**  Pozwala użytkownikom różnych komputerów nawiązywać sesje. Sesja steruje kierunkiem nadawania i synchronizuje (przywraca transmisję w postawionym punkcie kontrolnym). |
| **4. Warstwa transportowa**  Dzieli dane z wyższych warstw na mniejsze jednostki i zapewnia, że wszystkie fragmenty dotrą bezbłędnie do miejsca przeznaczenia. Izoluje wyższe warstwy od zmian technologii sprzętu. Określa typy usług świadczonych warstwie sesji (np. dwupunktowy „host-to-host” kanał, przekazujący dane sekwencyjnie, przesył izolowanych wiadomości bez gwarancji doręczenia, rozgłaszanie wiadomości pod wiele adresów). Ta warstwa jest w pełni dwupunktowa. |
| **3. Warstwa sieciowa**  Steruje działaniem podsieci. Zawiera funkcje obsługujące trasowanie. Kontrola przepływu (usuwanie zatorów), odpowiada za jakość usług. Powinna zapewnić łączenie niejednakowych sieci, różniących się np. Adresowaniem, czy wielkością akceptowanych pakietów. |
| **2. Warstwa łącza danych**  Podział przychodzących bitów na ramki (od kilkuset do kilku tysięcy bajtów) i sekwencyjna transmisja ramek. Sterowanie przepływem danych i obsługa błędów. |
| **1. Warstwa fizyczna**  Transmisja bitów kanałem komunikacyjnym. Zagadnienia projektowe wiążą się głównie z interfejsami mechniacznymi, elektrycznymi i zależnościami czasowaymi oraz z fizycznym nośnikiem transmisyjnym, który znajduje się pod wastwą fizyczną. |

**Architektura TCP/IP** – architektura protokołów stworzona w ramach eksperymentalnego projektu ARPANET finansowanego przez DARPA. Protokoły należące do architektury TCP/IP uznawane są przez IAB (Internet Architecture Board) za standardy Internetowe. Podobnie jak model OSI/ISO koncept architektury opiera się na warstwach. TCP/IP jest dużo bardziej przejrzysty od OSI/ISO i łatwiejszy w implementacji.

**Warstwy TCP/IP**

|  |
| --- |
| **4. Warstwa aplikacji**  Pozwala użytkownikom różnych komputerów nawiżywać sesje. Sesja steruje kierunkiem nadawania i synchronizuje (przywraca transmisję w postawionym punkcie kontrolnym). |
| **3. Warstwa transportowa**  Głównymi protokołami w tej warstwie są TCP i UDP. |
| **2. Warstwa Internetu**  Definiuje oficjalny format pakietu i Internet Protocol. Zadaniem tej warstwy jest dostarzenie pakietów IP w przewidziane miejsce, zajmuje się ona routingiem i unikaniem zatorów. |
| 1. **Warstwa host-sieć/fizyczna/dostepu do sieci**   Zajmuje się przekazywaniem danych przez fizyczne połączenia między urządzeniami sieciowymi. Najczęściej są to karty sieciowe lub modemy. Dodatkowo warstwa ta jest czasami wyposażona w protokoły do dynamicznego określania adresów IP. |

**Pakiet** – jednostka informacji składająca się z nagłówka i obszaru danych. Nagłówek zawiera między innymi informacje o adresowaniu, sumę kontrolną, długość pakietu, informacje o protokole. Obszar danych zawiera dane od wyższych warstw. W modelu OSI/ISO jest on skojarzony z warstwą sieciową, a w TCP/IP.

**Datagram** jest odpowiednikiem pakietu w protokołach zawodnych.

**Kapsułkowanie (encapsulation)** - polega na dodaniu nagłówka z dodatkowymi informacjami z wyższej warstwy przed przesłaniem do warstwy niższej danego protokołu po stronie nadawczej.

**Dekapsułkowanie (de-encapsulation)** – proces odwrotny do kapsułkowania, nagłóweki zostają usunięte po odczytaniu przed przesłaniem do wyższej warstwy.

**Fragmentacja** – dzielenie datagramów na fragmenty, które mieszczą się w ramce fizycznej. Procesem odwrotnym jest defragmentacja.

Część praktyczna

*1. Za pomocą programów ping, pathping, tracert, traceroute zbadać dostępność systemów i trasy do nich: a) z sieci laboratoryjnej, b) z sieci ZSK poza laboratorium, c) w dowolnym miejscu w Polsce, d) w dowolnym miejscu poza Polską. Ustalić zarządców tych adresów. Podać przynajmniej jeden przykład dostępności systemu i trasy dla sieci IPv6 (lokalizacja dowolna).*

Opis poleceń:

Ping - do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami. Dostępne w MS Windows i Linux.

Pathping - łączy funkcjonalność polecenia ping oraz tracert. Na początku ustalana jest trasa między hostami, a następnie pingowany jest każdy z węzłów na tej trasie. Dostępne w MS Windows.

Traceroute – ustala trasę między hostami. Dostępne w Linux, odpowiednikiem w systemach z rodziny MS Windows jes tracert.

Zadanie wykonano na systemie Linux

a) > ping -6 10.18.130.6

|  |
| --- |
| PING 10.18.130.6 (10.18.130.6) 56(84) bytes of data. 64 bytes from 10.18.130.6: icmp\_seq=1 ttl=64 time=0.307 ms 64 bytes from 10.18.130.6: icmp\_seq=2 ttl=64 time=0.280 ms 64 bytes from 10.18.130.6: icmp\_seq=3 ttl=64 time=0.278 ms 64 bytes from 10.18.130.6: icmp\_seq=4 ttl=64 time=0.283 ms 64 bytes from 10.18.130.6: icmp\_seq=5 ttl=64 time=0.253 ms 64 bytes from 10.18.130.6: icmp\_seq=6 ttl=64 time=0.257 ms  --- 10.18.130.6 ping statistics --- 6 packets transmitted, 6 received, 0% packet loss, time 5000ms rtt min/avg/max/mdev = 0.253/0.276/0.307/0.022 ms |

> traceroute 10.18.130.6

|  |
| --- |
| traceroute to 10.18.130.6 (10.18.130.6), 30 hops max, 60 byte packets  1 10.18.130.6 (10.18.130.6) 0.192 ms !X 0.168 ms !X 0.156 ms !X |

b) > ping -6 212.51.220.1

|  |
| --- |
| PING 212.51.220.1 (212.51.220.1) 56(84) bytes of data.  64 bytes from 212.51.220.1: icmp\_seq=1 ttl=255 time=2.69 ms  64 bytes from 212.51.220.1: icmp\_seq=2 ttl=255 time=0.793 ms  64 bytes from 212.51.220.1: icmp\_seq=3 ttl=255 time=0.920 ms  64 bytes from 212.51.220.1: icmp\_seq=4 ttl=255 time=0.810 ms  64 bytes from 212.51.220.1: icmp\_seq=5 ttl=255 time=1.30 ms  64 bytes from 212.51.220.1: icmp\_seq=6 ttl=255 time=0.823 ms |

> traceroute 212.51.220.1

|  |
| --- |
| traceroute to 212.51.220.1 (212.51.220.1), 30 hops max, 60 byte packets  1 pc-212-51-220-1.p.lodz.pl (212.51.220.1) 18.223 ms \* \* |

c) > ping -6 wp.pl

|  |
| --- |
| PING wp.pl (212.77.100.101) 56(84) bytes of data.  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=1 ttl=246 time=13.4 ms  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=2 ttl=246 time=11.7 ms  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=3 ttl=246 time=11.6 ms  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=4 ttl=246 time=11.9 ms  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=5 ttl=246 time=11.7 ms  64 bytes from www.wp.pl (212.77.100.101): icmp\_seq=6 ttl=246 time=11.6 ms  --- wp.pl ping statistics ---  6 packets transmitted, 6 received, 0% packet loss, time 5020ms  rtt min/avg/max/mdev = 11.665/12.026/13.451/0.654 ms |

> traceroute wp.pl

|  |
| --- |
| traceroute to wp.pl (212.77.100.101), 30 hops max, 60 byte packets  1 pc-212-51-220-1.p.lodz.pl (212.51.220.1) 19.180 ms 19.359 ms 19.503 ms  2 ckmx-uss.p.lodz.pl (212.51.207.91) 20.004 ms 20.174 ms 20.330 ms  3 pl-cke-gw-0-0-0.man.lodz.pl (212.191.9.193) 20.828 ms 21.021 ms 21.172 ms  4 e-gw1-0-2-0.man.lodz.pl (212.191.9.13) 21.654 ms 21.844 ms 21.998 ms  5 z-lodmana.poznan-gw3.10Gb.rtr.pionier.gov.pl (212.191.224.5) 25.915 ms 26.110 ms 26.280 ms  6 z-poznan-gw3.gdansk.10Gb.rtr.pionier.gov.pl (212.191.224.206) 31.965 ms 13.633 ms 17.722 ms  7 wp-jro4.10ge.task.gda.pl (153.19.102.6) 18.218 ms 18.396 ms 18.552 ms  8 rtr2.rtr-int-2.adm.wp-sa.pl (212.77.96.69) 20.571 ms rtr2.rtr-int-1.adm.wp-sa.pl (212.77.96.65) 24.755 ms rtr2.rtr-int-2.adm.wp-sa.pl (212.77.96.69) 20.749 ms  9 www.wp.pl (212.77.100.101) 25.108 ms 25.100 ms 25.205 ms |

d) > ping -6 www.usa.gov

|  |
| --- |
| PING a386.dscb.akamai.net (212.191.241.25) 56(84) bytes of data.  64 bytes from 212.191.241.25: icmp\_seq=1 ttl=59 time=7.57 ms  64 bytes from 212.191.241.25: icmp\_seq=2 ttl=59 time=5.78 ms  64 bytes from 212.191.241.25: icmp\_seq=3 ttl=59 time=5.78 ms  64 bytes from 212.191.241.25: icmp\_seq=4 ttl=59 time=5.75 ms  64 bytes from 212.191.241.25: icmp\_seq=5 ttl=59 time=5.76 ms  64 bytes from 212.191.241.25: icmp\_seq=6 ttl=59 time=5.75 ms  --- a386.dscb.akamai.net ping statistics ---  6 packets transmitted, 6 received, 0% packet loss, time 5014ms  rtt min/avg/max/mdev = 5.751/6.067/7.570/0.677 ms |

> traceroute www.usa.gov

|  |
| --- |
| traceroute to www.usa.gov (212.191.241.9), 30 hops max, 60 byte packets  1 pc-212-51-220-1.p.lodz.pl (212.51.220.1) 18.263 ms 21.891 ms 22.122 ms  2 ckmx-uss.p.lodz.pl (212.51.207.91) 22.604 ms 22.794 ms 22.970 ms  3 pl-cke-gw-0-0-0.man.lodz.pl (212.191.9.193) 23.428 ms 23.623 ms 23.774 ms  4 e-gw1-0-2-0.man.lodz.pl (212.191.9.13) 24.257 ms 24.427 ms 24.597 ms  5 z-lodmana.poznan-gw3.10Gb.rtr.pionier.gov.pl (212.191.224.5) 25.075 ms 28.979 ms 29.127 ms  6 a212-191-241-009.deploy.akamaitechnologies.com (212.191.241.9) 29.528 ms 8.937 ms 14.223 ms |

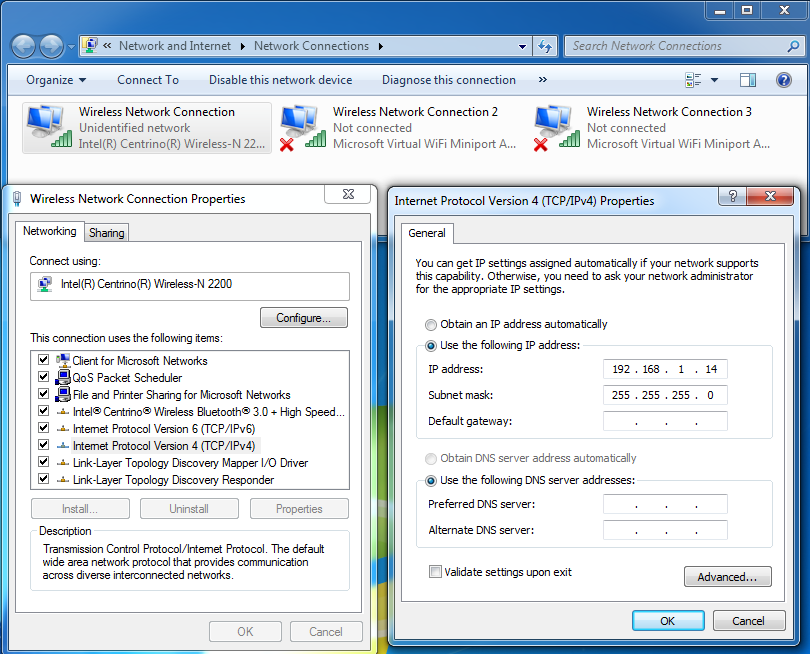
*2. Zbadać i zmodyfikować ustawienia protokołu IP na własnym stanowisku korzystając zarówno z narzędzi Panelu Sterowania Windows, jak i polecenia ipconfig oraz w systemie Linux (polecenia ip, ifconfig)*

**ipconfig** – służy do wyświetlania konfiguracji interfejsów sieciowych. Dostępne w MS Windows, odpowiednikiem w systemie Linux jest **ifconfig**.

Zadanie wykonane w systemie MS Windows

> ipconfig /all

|  |
| --- |
| Windows IP Configuration  Host Name . . . . . . . . . . . . : test1-PC  Primary Dns Suffix . . . . . . . :  Node Type . . . . . . . . . . . . : Hybrid  IP Routing Enabled. . . . . . . . : No  WINS Proxy Enabled. . . . . . . . : No  DNS Suffix Search List. . . . . . : home  Wireless LAN adapter Wireless Network Connection 3:  Media State . . . . . . . . . . . : Media disconnected  Connection-specific DNS Suffix . :  Description . . . . . . . . . . . : Microsoft Virtual WiFi Miniport Adapter #2  Physical Address. . . . . . . . . : 9C-4E-36-8A-39-59  DHCP Enabled. . . . . . . . . . . : Yes  Autoconfiguration Enabled . . . . : Yes  Wireless LAN adapter Wireless Network Connection 2:  Media State . . . . . . . . . . . : Media disconnected  Connection-specific DNS Suffix . :  Description . . . . . . . . . . . : Microsoft Virtual WiFi Miniport Adapter  Physical Address. . . . . . . . . : 9C-4E-36-8A-39-59  DHCP Enabled. . . . . . . . . . . : Yes  Autoconfiguration Enabled . . . . : Yes  Wireless LAN adapter Wireless Network Connection:  Connection-specific DNS Suffix . : home  Description . . . . . . . . . . . : Intel(R) Centrino(R) Wireless-N 2200  Physical Address. . . . . . . . . : 9C-4E-36-8A-39-58  DHCP Enabled. . . . . . . . . . . : Yes  Autoconfiguration Enabled . . . . : Yes  Link-local IPv6 Address . . . . . : fe80::4d0d:ef49:ce6e:6dd7%11(Preferred)  IPv4 Address. . . . . . . . . . . : 192.168.1.16(Preferred)  Subnet Mask . . . . . . . . . . . : 255.255.255.0  Lease Obtained. . . . . . . . . . : Sunday, October 20, 2013 4:51:28 PM  Lease Expires . . . . . . . . . . : Monday, October 21, 2013 4:51:28 PM  Default Gateway . . . . . . . . . : 192.168.1.254  DHCP Server . . . . . . . . . . . : 192.168.1.254  DHCPv6 IAID . . . . . . . . . . . : 245124662  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-19-A3-29-3B-9C-4E-36-8A-39-58  DNS Servers . . . . . . . . . . . : 192.168.1.254  NetBIOS over Tcpip. . . . . . . . : Enabled  Tunnel adapter isatap.home:  Media State . . . . . . . . . . . : Media disconnected  Connection-specific DNS Suffix . : home  Description . . . . . . . . . . . : Microsoft ISATAP Adapter  Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0  DHCP Enabled. . . . . . . . . . . : No  Autoconfiguration Enabled . . . . : Yes  Tunnel adapter Teredo Tunneling Pseudo-Interface:  Connection-specific DNS Suffix . :  Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface  Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0  DHCP Enabled. . . . . . . . . . . : No  Autoconfiguration Enabled . . . . : Yes  IPv6 Address. . . . . . . . . . . : 2001:0:5ef5:79fb:14b1:14de:3f57:feef(Preferred)  Link-local IPv6 Address . . . . . : fe80::14b1:14de:3f57:feef%14(Preferred)  Default Gateway . . . . . . . . . : ::  NetBIOS over Tcpip. . . . . . . . : Disabled |

Zmiana adresu IP.  


> ipconfig

|  |
| --- |
| Windows IP Configuration  […]  IPv4 Address. . . . . . . . . . . : 192.168.1.14  […] |

*3. Zbadać tablicę routingu (w szczególności bramę domyślną) na własnym stanowisku korzystając np. z polecenia route.*

**route** – służy do wyświetlania i modyfikacji wpisów w tabeli routingu

|  |
| --- |
| ===========================================================================  Interface List  13...9c 4e 36 8a 39 59 ......Microsoft Virtual WiFi Miniport Adapter #2  12...9c 4e 36 8a 39 59 ......Microsoft Virtual WiFi Miniport Adapter  11...9c 4e 36 8a 39 58 ......Intel(R) Centrino(R) Wireless-N 2200  1...........................Software Loopback Interface 1  15...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter  14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface  ===========================================================================  IPv4 Route Table  ===========================================================================  Active Routes:  Network Destination Netmask Gateway Interface Metric  0.0.0.0 0.0.0.0 192.168.1.254 192.168.1.16 25  127.0.0.0 255.0.0.0 On-link 127.0.0.1 306  127.0.0.1 255.255.255.255 On-link 127.0.0.1 306  127.255.255.255 255.255.255.255 On-link 127.0.0.1 306  192.168.1.0 255.255.255.0 On-link 192.168.1.16 281  192.168.1.16 255.255.255.255 On-link 192.168.1.16 281  192.168.1.255 255.255.255.255 On-link 192.168.1.16 281  224.0.0.0 240.0.0.0 On-link 127.0.0.1 306  224.0.0.0 240.0.0.0 On-link 192.168.1.16 281  255.255.255.255 255.255.255.255 On-link 127.0.0.1 306  255.255.255.255 255.255.255.255 On-link 192.168.1.16 281  ===========================================================================  Persistent Routes:  None  IPv6 Route Table  ===========================================================================  Active Routes:  If Metric Network Destination Gateway  14 58 ::/0 On-link  1 306 ::1/128 On-link  14 58 2001::/32 On-link  14 306 2001:0:5ef5:79fd:28fb:3c99:3f57:feef/128  On-link  11 281 fe80::/64 On-link  14 306 fe80::/64 On-link  14 306 fe80::28fb:3c99:3f57:feef/128  On-link  11 281 fe80::4d0d:ef49:ce6e:6dd7/128  On-link  1 306 ff00::/8 On-link  14 306 ff00::/8 On-link  11 281 ff00::/8 On-link  ===========================================================================  Persistent Routes:  None |

*4. Zbadać nasłuchujące porty TCP i UDP oraz nawiązane połączenia TCP wykorzystując polecenie netstat. Utworzyć połączenie TCP (np. przeglądarką WWW, klientem poczty, telnet czy ssh) i wykazać jego obecność poleceniem netstat.*

> netstat

|  |
| --- |
| Active Connections  Proto Local Address Foreign Address State  TCP 0.0.0.0:135 test1-PC:0 LISTENING  TCP 0.0.0.0:445 test1-PC:0 LISTENING  TCP 0.0.0.0:1025 test1-PC:0 LISTENING  TCP 0.0.0.0:1026 test1-PC:0 LISTENING  TCP 0.0.0.0:1027 test1-PC:0 LISTENING  TCP 0.0.0.0:1028 test1-PC:0 LISTENING  TCP 0.0.0.0:1029 test1-PC:0 LISTENING  TCP 0.0.0.0:7520 test1-PC:0 LISTENING  TCP 192.168.1.16:139 test1-PC:0 LISTENING  TCP [::]:135 test1-PC:0 LISTENING  TCP [::]:445 test1-PC:0 LISTENING  TCP [::]:1025 test1-PC:0 LISTENING  TCP [::]:1026 test1-PC:0 LISTENING  TCP [::]:1027 test1-PC:0 LISTENING  TCP [::]:1028 test1-PC:0 LISTENING  TCP [::]:1029 test1-PC:0 LISTENING  TCP [::]:7520 test1-PC:0 LISTENING  UDP 0.0.0.0:68 \*:\*  UDP 0.0.0.0:5355 \*:\*  UDP 127.0.0.1:1900 \*:\*  UDP 127.0.0.1:55350 \*:\*  UDP 192.168.1.16:137 \*:\*  UDP 192.168.1.16:138 \*:\*  UDP 192.168.1.16:1900 \*:\*  UDP [::]:5355 \*:\*  UDP [::1]:1900 \*:\*  UDP [::1]:55349 \*:\*  UDP [fe80::4d0d:ef49:ce6e:6dd7%11]:546 \*:\*  UDP [fe80::4d0d:ef49:ce6e:6dd7%11]:1900 \*:\* |

Uruchomiono program korzystający z sieci (steam.exe).  
> netstat

|  |
| --- |
| Active Connections  Proto Local Address Foreign Address State  […]  TCP 192.168.1.16:139 test1-PC:0 LISTENING  **TCP 192.168.1.16:3441 208-64-202-69:http TIME\_WAIT**  **TCP 192.168.1.16:3446 fa-in-f138:http ESTABLISHED**  TCP [::]:135 test1-PC:0 LISTENING  TCP [::]:445 test1-PC:0 LISTENING  […] |

**Bibliografia:**

- A. S. Tannenbaum “*Sieci komputerowe*”, 2004 Helion- W. Stallings “*Data And Computer Communications*”, 2004 Pearson Education, Inc.  
- <http://www.wikipedia.org/>