Sieci komputerowe. Jak działa Internet?

Jacek Kobus

Instytut Fizyki UMK

Toruń 2-6/2006

„Komputery są wśród nas”

- Rozwój nauki i techniki $\longrightarrow$ przemiany cywilizacyjne
- Fizyka XX w. $\longrightarrow$ półprzewodniki, układy scalone, nanotechnologia
- Komputery: *mainframe*, minikomputery, stacje robocze, PC
- Sieci komputerowe: LAN i WAN $\longrightarrow$ Internet
- Technologie informatyczne składnikiem towarów, pracy, usług

W jakim stopniu nasze życie zależy od komputerów?

Jak komputery zmieniają funkcjonowanie państw i społeczeństw?

Prawo Moore'a (1965) (Gordon Moore – założyciel i wiceprezydent firmy Intel)

Liczba tranzystorów, które można zmieścić na jednym calu kwadratowym płytki krzemowej podwaja się co 12 miesięcy.

Sformułowanie poprawniejsze:
Liczba tranzystorów (na jednostce powierzchni płytki krzemowej), która prowadzi do najmniejszych kosztów na jeden tranzystor, podwaja się w przybliżeniu co 12 miesięcy.

Sformułowanie najczęściej spotykane:
Wydajność systemów komputerów ulega podwojeniu co około 18 miesięcy.

Jack J.Dongara *The Quest for Petascale Computing*, Computing in Science & Engineering (2001)

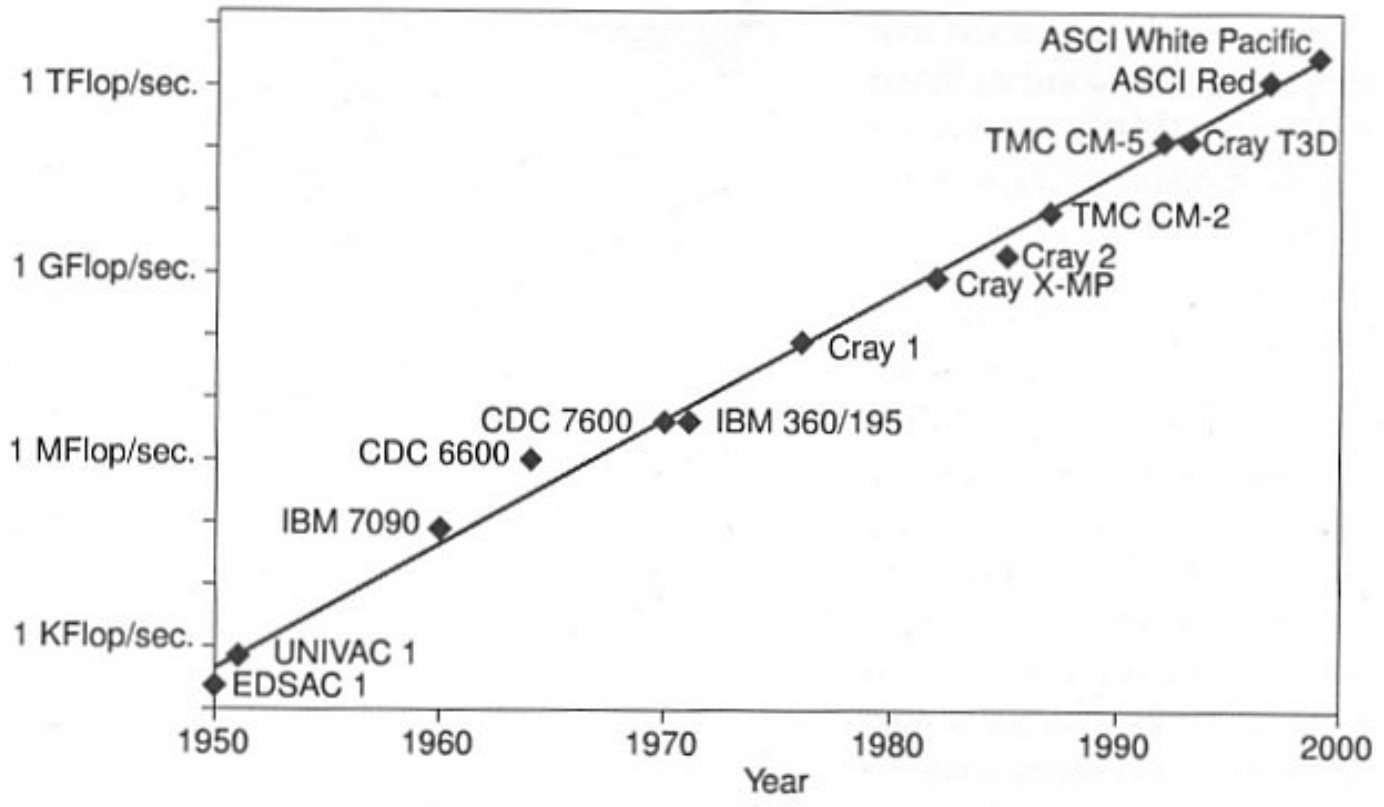


Figure 1. Moore's Law and the peak performance of various computers over time.

Historia Internetu w liczbach

(www.netvalley.com/intvalstat.html)

	# komputerów	# serwerów www
7/01	126 000 000	28 200 000
7/98	37 000 000	4 270 000
7/97	19 540 000	1 200 000
7/96	12 881 000	300 000
7/95	6 642 000	25 000
7/94	3 212 000	3 000
7/93	1 776 000	150
7/92	992 000	50
7/89	130 000	
7/81	210	
1969	4	

Ile osób korzysta z Internetu?

(wg szacunkowych danych, www.nua.ie/surveys/how_many_online)

8/2002	606 mln	(Nua Ltd)
8/2001	513 mln	(Nua Ltd)
8/2000	369 mln	(Nua Ltd)
8/1999	195 mln	(Nua Ltd)
9/1998	147 mln	(Nua Ltd)
11/1997	76 mln	(Reuters)
12/1996	36 mln	(IDC)
12/1995	16 mln	(IDC)

Wg Nielsen/NetRatings w 2002 r. było 580 milionów użytkowników Internetu. Szacunki International Telecommunications Union mówią o 665 milionach (http://www.sims.berkeley.edu/research/projects/how-much-info-2003/internet.htm).

Wg sondażu SMG/KRC z lutego 2004 r. 6.7 mln Polaków (22.3%) w wieku od 15 do 75 lat korzysta z Internetu (http://dziennik.pap.com.pl/)

Krótka historia powstania Internetu

- 1969 – Agencja Zaawansowanych Projektów Badawczych Departamentu Obrony Stanów Zjednoczonych (DARPA – *Defense Advanced Research Projects Agency*) sfinansowała prace badawcze i rozwojowe prowadzące do stworzenia sieci z komutacją pakietów (ARPANET).
- 1971 – R.Tomlinson tworzy program do przesyłania poczty elektronicznej (adres: *user@server*)
- 1973 – powstają sieci w W.Brytanii i Norwegii połączone z siecią ARPANET łączami satelitarnymi
- 1979 – powstają pierwsze grupy dyskusyjne
- 1981 – opracowanie protokołów komunikacyjnych TCP *Transmission Control Protocol*) oraz IP (*Internet Protocol*)
- 1983 – protokoły TCP/IP zostały przyjęte jako Standardy Wojskowe; implementacja TCP/IP w systemie operacyjnym UNIX BSD; ARPANET staje się siecią TCP/IP

Krótka historia powstania Internetu (cd)

- 1983 – ARPANET rozpada się na sieć MILNET (sieć Departamentu Obrony) oraz ARPANET (przestała istnieć w 1990 r.)

  Termin **Internet** służył do określenia obu tych sieci.

  Internet = Sieć

- 1984 – wprowadzenie usługi DNS (*Domain Name System*)
- 1986 – powstaje NSFNET (*Nationa Science Foundation NET*), amerykańska sieć szkieletowa o przepustowości 56 kb/s
- 1991 – T.Berners-Lee tworzy HTML (*Hyper-Text Markup Language*), co daje początek WWW (*World Wide Web*)
- 1995 – powstają przeglądarki Netscape Navigator i Internet Explorer (wojna na przeglądarki)

Cel wykładu:

Jak jest zbudowana i jak działa lokalna i rozległa sieć komputerowa, czyli jak działa Internet (Sieć, sieć sieci)?

Program wykładu

1. Wprowadzenie
2. Architektura protokołów sieciowych: model odniesienia OSI i TCP/IP
3. Charakterystyka protokołów modelu TCP/IP: Ethernet, ICMP, ARP, RARP, IP, TCP, UDP
4. Lokalna sieć komputerowa
   (a) topologia, media transmisyjne, urządzenia sieciowe, protokoły
   (b) zasady okablowania strukturalnego
5. Rozległa sieć komputerowa: topologia, media transmisyjne, urządzenia sieciowe, protokoły
6. Sieć Internet: protokoły warstwy aplikacji, usługi sieciowe
7. (Nie)bezpieczeństwo w sieci komputerowej

`http://www.phys.uni.torun.pl/~jkob/chemometria3-transp.pdf`

http://www.phys.uni.torun.pl/~jkob/wdi.pdf
http://www.phys.uni.torun.pl/~jkob/wdi-2005-transp.pdf
http://www.phys.uni.torun.pl/~jkob/sk-transp.pdf

Protokoły sieciowe

Komputery i inne urządzenia przyłączone do sieci (hosty) wymieniają informacje według ściśle ustalonych reguł zwanych **protokołami komunikacyjnymi**.

Umożliwia to budowę sieci heterogenicznych, w których mogą współpracować ze sobą komputery niezależnie od swojej architektury oraz systemu operacyjnego.

Internet – sieć z komutacją pakietów wykorzystująca rodzinę protokołów komunikacyjnych TCP/IP

TCP (*Transmission Control Protocol*) protokół sterowania transmisją
IP (*Internet Protocol*) protokół Internetu

Protokoły sieciowe (cd)

Cechy TCP/IP:

- standard otwartych protokołów, łatwo dostępnych i opracowywanych niezależnie od specyfiki sprzętu komputerowego lub systemu operacyjnego
- niezależność od fizycznych właściwości sieci, co pozwala na integrację różnego rodzaju sieci (łącza telefoniczne, światłowodowe, radiowe)
- wspólny system adresacji pozwalający dowolnemu urządzeniu korzystającemu z TCP/IP na jednoznaczne zaadresowanie innego urządzenia w sieci

Model OSI versus TCP/IP

model OSI		model TCP/IP	
warstwa aplikacji	(7)	(4)	warstwa aplikacji
warstwa prezentacji	(6)		
warstwa sesji	(5)		
warstwa transportowa	(4)	(3)	warstwa transportowa
warstwa sieciowa	(3)	(2)	warstwa Internet
warstwa łącza danych	(2)	(1)	warstwa dostępu do sieci
warstwa fizyczna	(1)		

ISO (*International Organization for Standardization*) ogłasza w 1984 specyfikację modelu odniesienia OSI (*Open System Interconnection*, otwarte połączenie systemów).

Model OSI i TCP/IP opisują sieci z przełączaniem pakietów.

Funkcje warstw modelu OSI

(warstwy protokołów aplikacji)

zastosowań (*application layer*) – oferuje usługi sieciowe użytkownikom lub programom, np. protokołowi realizującemu usługę poczty elektronicznej (nie dostarcza usług żadnej innej warstwie)

prezentacji (*presentation layer*) – zapewnia przekazywanie danych (tekstowych, graficznych, dźwiękowych) w odpowiednim (wspólnym) formacie, dokonuje ich kompresji oraz ew. szyfrowania

sesji (*session layer*) – ustanawia, zarządza i kończy połączeniami (sesjami) pomiędzy współpracującymi aplikacjami, m.in. ustala sposób wymiany danych (jednokierunkowy (*half-duplex*) lub dwukierunkowy (*full-duplex*))

Funkcje warstw modelu OSI (cd)

(warstwy protokołów przepływu danych)

transportowa (*transport layer*) – zapewnia bezbłędną komunikację pomiędzy komputerami w sieci (*host to host*), dzieli dane na fragmenty, kontroluje kolejność ich przesyłania, ustanawia wirtualne połączenia, utrzymuje je i likwiduje (TCP, UDP)

sieciowa (*network layer*) – definiuje datagramy, ustala drogę transmisji danych i przekazuje dane pomiędzy węzłami sieci (IP, IPX, ICMP, Apple Talk)

łącza danych (*data link layer*) – zapewnia niezawodne dostarczanie danych przez znajdującą się poniżej fizyczną sieć (IEEE 802.3, MAC, (R)ARP, PPP)

fizyczna (*physical layer*) – umożliwia przesyłanie poszczególnych bitów (ramek) przez dane fizyczne łącze, kontroluje przepływ bitów, powiadamia o błędach (Etherenet 802.3, RS232C, V.35)

Model OSI: komunikacja równorzędna i kapsułkowanie

Komunikacja równorzędna węzeł-węzeł (*host-host*, *host-to-host*)

- przepływ danych pomiędzy odpowiadającymi sobie warstwami sieci
- nagłówek i dane danej warstwy tworzą dane dla warstwy niższej: kapsułkowanie, enkapsulacja (*encapsulation*)

Sieci równorzędne (*peer-to-peer networks*)

Model OSI: komunikacja równorzędna (cd)

host A	komunikacja	host B
warstwa aplikacji	← strumień danych →	warstwa aplikacji
warstwa prezentacji	← strumień danych →	warstwa prezentacji
warstwa sesji	← strumień danych →	warstwa sesji
warstwa transportowa	← segmenty →	warstwa transportowa
warstwa sieciowa	← pakiety →	warstwa sieciowa
warstwa łącza danych	← ramki →	warstwa łącza danych
warstwa fizyczna	← bity →	warstwa fizyczna

Zalety modelu odniesienia OSI

- ułatwia zrozumienie działania komunikacji sieciowej
- standaryzuje elementy sieci pozwalając na ich rozwijanie przez wielu wytwórców
- pozwala na współdziałanie różnego typu urządzeń sieciowych i oprogramowania sieciowego
- przeciwdziała wpływowi zmian w jednej warstwie na funkcjonowanie innych warstw (szybszy rozwój)
- ułatwia uczenie i uczenie się działania sieci komputerowych

Warstwa dostępu do sieci (fizyczna + łącza danych)

Funkcje warstwy fizycznej:

- zamiana danych znajdujących się w ramkach na strumienie binarne
- stosowanie metody dostępu do nośnika, jakiej żąda warstwa łącza danych
- przesyłanie ramki danych szeregowo w postaci strumieni binarnych
- oczekiwanie na transmisje adresowane do danego hosta
- odbiór odpowiednio zaadresowanych strumieni
- przesyłanie binarnych strumieni do warstwy łącza danych, w celu złożenia ich w ramki

Sieci Ethernet/IEEE 802.3

- Lokalne sieci komputerowe są budowane w oparciu o normę IEEE 802.3 z roku 1985, która definiuje ramkę danych oraz określa sposób dostępu do nośnika.
- Norma ta uściśla i rozszerza specyfikację właściwą dla sieci Ethernet I (Ethernet PARC, *Palo Alto Research Center*) i Ethernet II (Ethernet DIX) i dlatego sieci wykorzystujące normę IEEE 802.3 zwane są sieciami ethernetowymi.
- Rodzaje ramek ethernetowych: PARC, DIX, 802.3, LLC (*Logical Link Control*), SNAP (*Sub-Network Access Protocol*)
- Materialnymi nośnikami transmisji są kabel koncentryczny, skrętka dwużyłowa, kabel światłowodowy. Ich fizyczne własności określają szerokość dostępnego pasma transmisyjnego, częstotliwości sygnałów i efektywną prędkość przesyłania danych.

IEEE *Institute of Electrical and Electronics Engineers*

Ramki Ethernet/IEEE 802.3

Ramka Ethernet II (Internet, DECNET, Novell)

7	1	6	6	2	46-1500	4
Preambuła	Ogranicznik początku ramki	Adres przezna-czenia	Adres źródłowy	Typ	Dane	Sekwencja kontrolna ramki

Ramka IEEE 802.3 (NETBEUI, SNA)

7	1	6	6	2	46-1500	4
Preambuła	Ogranicznik początku ramki	Adres przezna-czenia	Adres źródłowy	Długość	Nagłówek 802.2 i dane	Sekwencja kontrolna ramki

SFD (*Start of Frame Delimiter*) ogranicznik początku ramki
FCS (*Frame Check Sequence*) sekwencja kontrolna ramki
CRC (*Cyclic Redundancy Check*) cykliczna kontrola nadmiarowa
SNA (*Systems Network Architecture*) architektura sieci systemów

Struktura warstwy dostępu do sieci wg IEEE 802.3

Powiązanie warstwy łącza danych i warstwy fizycznej z warstwą sieciową (Internet) jest realizowane poprzez protokół LLC (*Logical Link Control*)

Warstwy OSI

<table>
<tr><td rowspan="2">Data Link Layer</td><td>LLC sublayer</td></tr>
<tr><td>MAC sublayer</td></tr>
<tr><td colspan="2">Physical Layer</td></tr>
</table>

Specyfikacja LAN

<table>
<tr><td rowspan="2">Ethernet</td><td colspan="4">IEEE 802.2</td></tr>
<tr><td>IEEE 802.3i
10Base-T</td><td>IEEE 802.3u
100Base-TX</td><td>IEEE 802.5
Token Ring</td><td>IEEE 802.8
FDDI</td></tr>
</table>

Warstwa dostępu do sieci (cd)

Funkcje warstwy łącza danych:

- sterowanie łączem logicznym (LLC *Logical Link Control*)

  Podwarstwa LLC izoluje protokoły wyższej warstwy od właściwej metody dostępu do nośnika, co zapewnia współoperacyjność różnych architektur sieciowych.

- sterowanie dostępem do nośnika (MAC *Media Access Control*)

  Podwarstwa MAC odpowiada za opakowanie danych z podwarstwy LLC w ramki, za testy integralności danych, za śledzenie stanu nośnika

  – używa płaskiej struktury adresowej (adresy MAC)
  – grupuje bity w ramki
  – używa MAC do określania, który komputer będzie transmitował dane (w sytuacji, gdy wiele komputerów chce nadawać równocześnie)

Ethernet II Type Element Codes:

```
Note   Hex       Definition
@    0000-05DC IEEE802.3 Length Field (0.:1500.)
+    0101-01FF Experimental
     0200 Xerox PUP (conflicts with 802.3 Length Field
          range) (see 0A00)
     0201 Xerox PUP Address Translation (conflicts ...)
          (see 0A01)
     0400 Nixdorf (conflicts with 802.3 Length Field)
+*   0600 Xerox NS IDP
     0601 XNS Address Translation (3Mb only)
+*   0800 DOD Internet Protocol (IP)
+    0801 X.75 Internet
+    0802 NBS Internet
+    0803 ECMA Internet
+    0804 CHAOSnet
+    0805 X.25 Level 3
```

```
+*    0806 Address Resolution Protocol (ARP) (for IP and for
           CHAOS)

      7031 Prime NTS (Network Terminal Service)
      7034 Cabletron
      8003 Cronus VLN
      803E DEC Distributed Time Service
      803F DEC LAN Traffic Monitor Protocol

+     809B EtherTalk (AppleTalk over Ethernet)
+     809C-809E Datability
+     809F Spider Systems Ltd.
+     80A3 Nixdorf Computers
+     80A4-80B3 Siemens Gammasonics Inc.
+     80C0-80C3 DCA (Digital Comm. Assoc.) Data Exchange
                Cluster
```

```
+     8137 Novell (old) NetWare IPX (ECONFIG E option)
+     8138 Novell, Inc.
+     8139-813D KTI
      813F M/MUMPS data sharing
      8145 Vrije Universiteit (NL)  Amoeba 4 RPC (obsolete)
      8146 Vrije Universiteit (NL)  FLIP (Fast Local
           Internet Protocol)
      8147 Vrije Universiteit (NL)  [reserved]
      814C SNMP over Ethernet (see RFC1089)
```

Warstwa dostępu do sieci (cd)

- Adres sprzętowy MAC (*Media Access Control*) składa się z 48 bitów.

  24 bity są przypisane producentowi sprzętu (OUI, *Organizational Unique Identifier*), a pozostałe 24 bity numerują kolejne karty. Np. numery kart sieciowych firmy Sun Microsystems są postaci 08:00:20:xx:xx:xx.

- Dostęp do nośnika: wielodostęp z wykrywaniem fali nośnej i wykrywaniem kolizji, CSMA/CD (*Carrier Sense-Multiple Access/Collision Detection*)

Warstwa Internet (sieciowa)

Funkcje warstwy sieciowej:

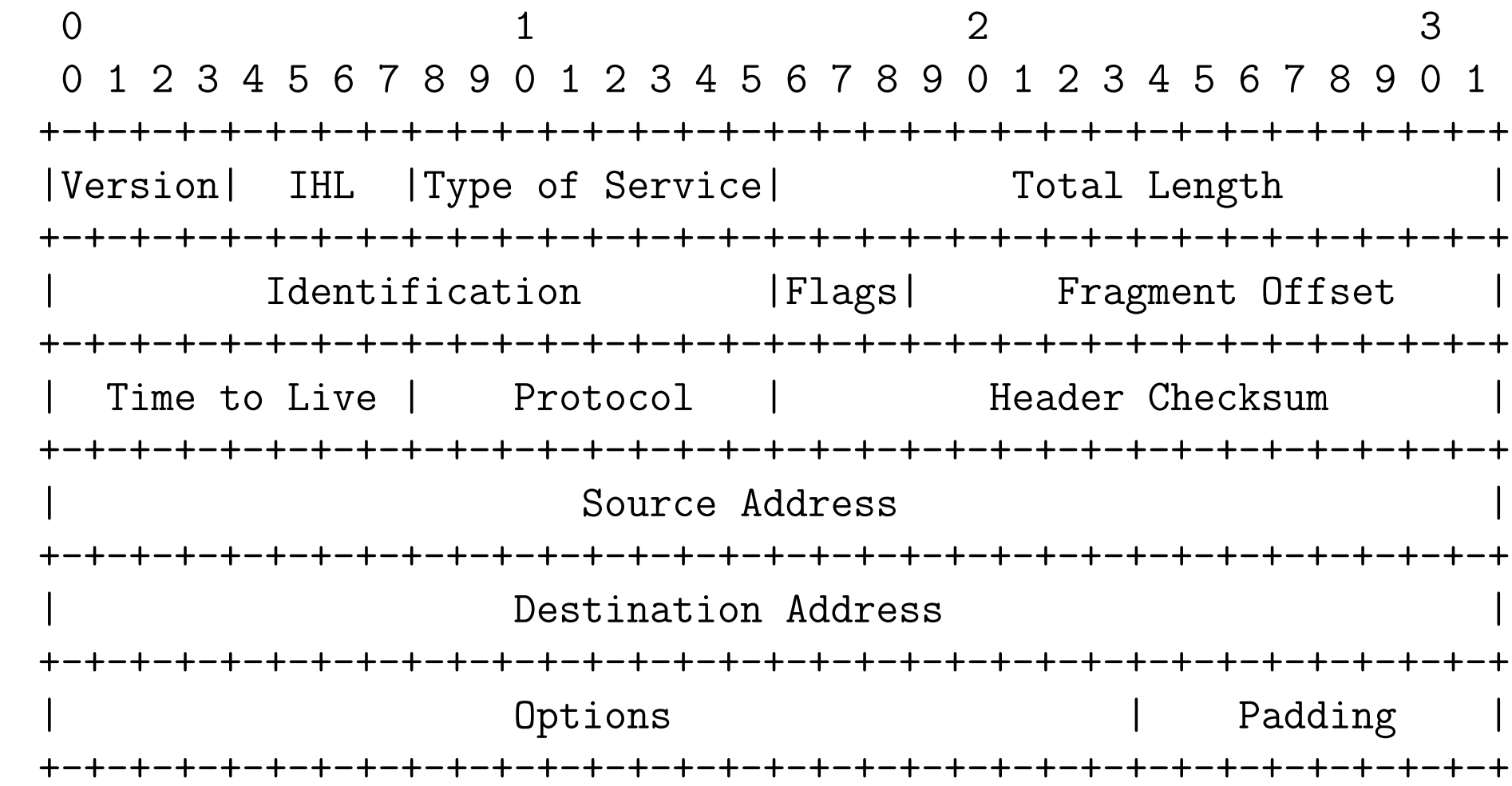
- definiowanie datagramów
- definiowanie schematu adresowania używanego w Internecie
- przekazywanie danych pomiędzy warstwą transportową i warstwą dostępu do sieci
- kierowanie datagramów do komputerów oddalonych
- dokonywanie fragmentacji i ponownego składania datagramów (MTU, *Maximum Transmission Unit*)

Internet Protocol (IP) protokół międzysieciowy, internetowy (RFC 791)

Własności IP:

- IP jest protokołem *bezpołączeniowym*
- *datagram* jest formatem pakietu zdefiniowanym przez protokół Internet.

  Dane są przekazane do właściwego protokołu warstwy transportowej na podstawie pola *Numer protokołu* w nagłówku datagramu.
- sieć Internet jest *siecią z przełączaniem pakietów* (routery, trasowanie)



IP Header Format (RFC 791)

Note that each tick mark represents one bit position.

Fragment pliku /etc/protocols:

```
# Internet (IP) protocols
#
# See also http://www.iana.org/assignments/protocol-numbers

ip          0       IP              # internet protocol, pseudo protoc
icmp        1       ICMP            # internet control message protocc
igmp        2       IGMP            # Internet Group Management
ggp         3       GGP             # gateway-gateway protocol
ipencap     4       IP-ENCAP        # IP encapsulated in IP (officiall
st          5       ST              # ST datagram mode
tcp         6       TCP             # transmission control protocol
egp         8       EGP             # exterior gateway protocol
pup         12      PUP             # PARC universal packet protocol
udp         17      UDP             # user datagram protocol
hmp         20      HMP             # host monitoring protocol
xns-idp     22      XNS-IDP         # Xerox NS IDP
```

```
rdp             27      RDP             # "reliable datagram" protocol
ipv6            41      IPv6            # IPv6
ipv6-crypt      50      IPv6-Crypt      # Encryption Header for IPv6
ipv6-auth       51      IPv6-Auth       # Authentication Header for IPv6
swipe           53      SWIPE           # IP with Encryption
tlsp            56      TLSP            # Transport Layer Security Protocc
ipv6-icmp       58      IPv6-ICMP       # ICMP for IPv6
ipv6-nonxt      59      IPv6-NoNxt      # No Next Header for IPv6
ipv6-opts       60      IPv6-Opts       # Destination Options for IPv6
```

Klasy adresów IP (RFC 1597)

Każdy komputer pracujący w sieci posiada unikatowy adres (tzw. adres IP) składający się z 32 bitów zapisywanych w postaci czterech oktetów, czyli czterech liczb z zakresu 0-255 oddzielonych kropkami, np. 158.75.5.47.

Przydzielaniem adresów zajmuje się NIC *Network Information Center*.

Adres IP składa się z części sieciowej i części hosta. Podział na te części jest określony przez klasę do której adres należy.

klasa A

IP	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
adresy	0.0.0.0 – 127.255.255.255
# sieci	128
# hostów	$\approx 17 \times 10^6$

adres sieci (*network address*): np. 127.0.0.0

adres rozgłoszeniowy (*broadcast address*): np. 127.255.255.255

Klasy adresów IP (cd)

klasa B

IP	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
adresy	128.0.0.0 – 191.255.255.255
# sieci	16384
# hostów	65536

klasa C

IP	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
adresy	192.0.0.0 – 223.255.255.255
# sieci	$\approx 2 \times 10^6$
# hostów	256

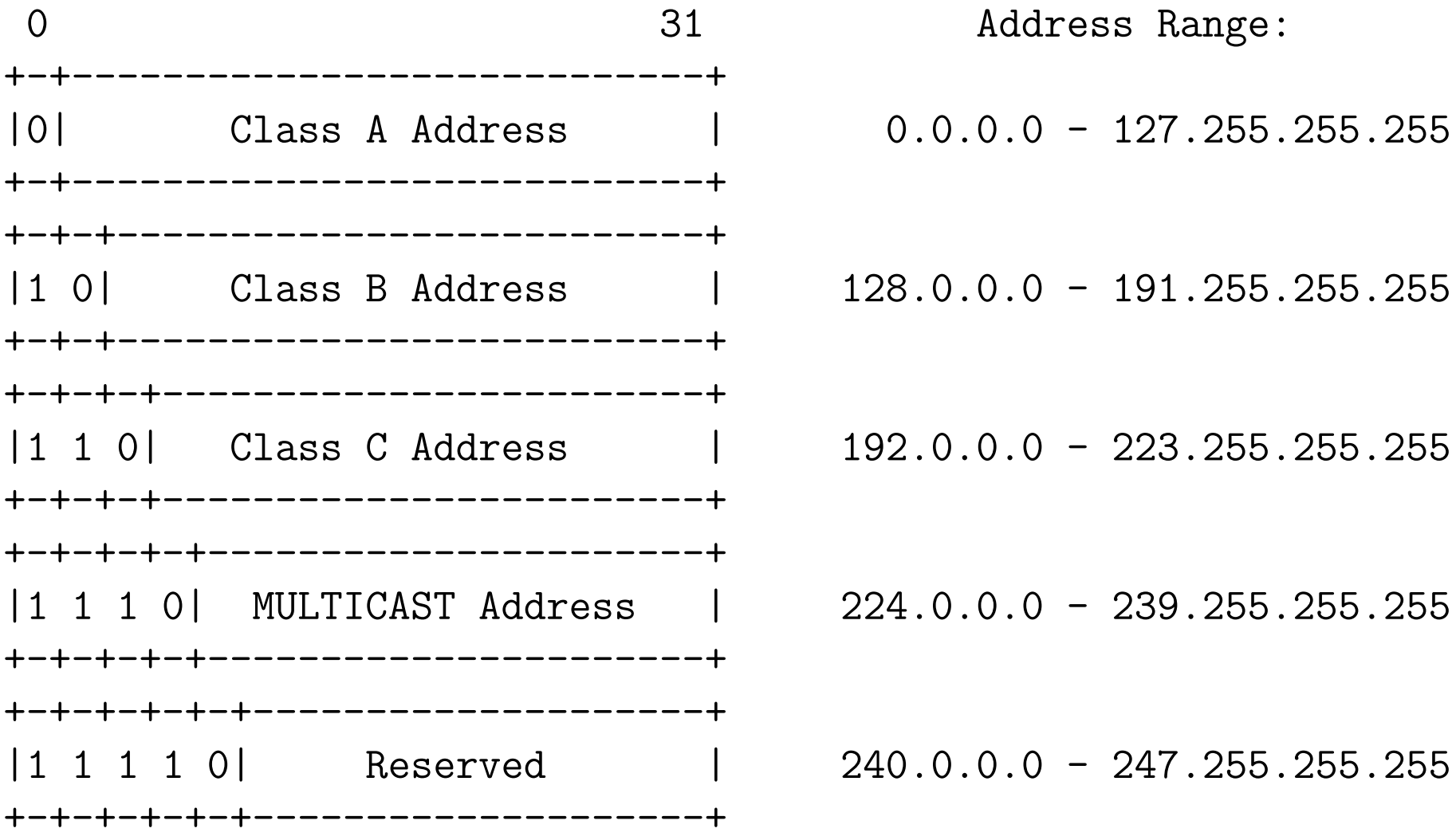
Klasy adresów IP (cd)

klasa D (adresy grupowe)

IP	1110bbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb
adresy	224.0.0.0 – 239.255.255.255

W trakcie transmisji multicastowej nadawca przesyła pojedynczą kopię wiadomości do *dostarczyciela usługi* (SP, *service provider*) w trakcie pojedynczej operacji. SP dostarcza kopię wiadomości do każdego odbiorcy transmisji multicastowej.

Klasy adresów IP (cd)



Adresy grupowe (multicast)

Niektóre adresy klasy D są zarezerwowane dla *dobrze znanych* grup multicastowych

- 224.0.0.1 – grupa wszystkich hostów akceptujących multicast; każdy host akceptujący multicasty zapisuje się do tej grupy przy uruchamianiu
- 224.0.0.2 – grupa wszystkich routerów multicastowych
- 224.0.0.4 – grupa routerów DVMRP (*Distance Vector MulticastRouting Protocol*)
- 224.0.0.5 – grupa routerów OSPF
- ...
- 224.0.0.0 - 224.0.0.255 są zarezerwowane na potrzeby lokalne (administrowanie i konserwowanie urządzeń i usług) i nie są nigdy przekazywane dalej przez routery multicastowe
- 239.0.0.0 - 239.255.255.255 zarezerwowane na potrzeby *administrative scoping*

Klasy adresów IP (cd)

Sieci prywatne

klasa A	10.1.1.1	–	10.254.254.254
klasa B	172.16.1.1	–	172.31.254.254
klasa C	192.168.1.1	–	192.168.254.254

Klasy adresów IP (cd)

Adres pętli zwrotnej (loopback address)

sieć	127.0.0.0
adresy	127.x.x.x

Fragment pliku `/etc/hosts`

```
127.0.0.1 localhost.localdomain scobie localhost
158.75.5.43 ameryk.phys.uni.torun.pl ameryk am
158.75.5.47 ferm.phys.uni.torun.pl ferm fm
158.75.5.51 tal.phys.uni.torun.pl tal tl
158.75.5.90 nobel.phys.uni.torun.pl nobel nb
158.75.28.35 enter.hpc.uni.torun.pl enter
```

Komenda: `ifconfig -a`

```
eth0 Link encap:Ethernet  HWaddr 00:10:A4:D2:52:55
     inet addr:158.75.5.95  Bcast:158.75.5.255  Mask:255.255.254.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:0 errors:0 dropped:0 overruns:0 frame:0
     TX packets:0 errors:102 dropped:0 overruns:0 carrier:102
     collisions:0 txqueuelen:100
     RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
     Interrupt:11 Base address:0x4800

lo   Link encap:Local Loopback
     inet addr:127.0.0.1  Mask:255.0.0.0
     UP LOOPBACK RUNNING  MTU:16436  Metric:1
     RX packets:675 errors:0 dropped:0 overruns:0 frame:0
     TX packets:675 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
     RX bytes:65654 (64.1 Kb)  TX bytes:65654 (64.1 Kb)
```

Sieci i podsieci. Maski podsieci

- standardowa struktura adresów IP może być lokalnie modyfikowana poprzez użycie bitów adresowych hostów jako dodatkowych bitów określających sieć
- podział sieci na podsieci (*subnets*) przy pomocy maski bitowej (maski podsieci (*netmask*)
  - bit 1 w masce wskazuję, że odpowiadający mu bit w adresie IP wskazuje na adres sieci
  - bit 0 w masce wskazuje, że odpowiadający mu bit adresu jest związany z adresem komputera w podsieci
- podsieć jest znana tylko lokalnie

Sieci i podsieci. Maski podsieci (cd)

Przykłady wielkości podsieci w zależności
od wyboru maski dla adresu klasy C.

liczba IP	maska (lbs)	liczba podsieci
2	255.255.255.254 (7)	128
4	255.255.255.252 (6)	64
8	255.255.255.248 (5)	32
16	255.255.255.240 (4)	16
32	255.255.255.224 (3)	8
64	255.255.255.192 (2)	4
128	255.255.255.128 (1)	2
maska podsieci = 256 - liczba IP w podsieci		

LAN Instytutu Fizyki wykorzystuje adresy od 158.75.4.0 do 158.75.5.255 wydzielone spośród adresów klasy B przy pomocy maski sieciowej 255.255.254.0.

Sieci i podsieci. Maski podsieci (cd)

Przykład: sieć=195.15.25.0, maska=255.255.255.224.

sieć	sieć	podsieć	numery hostów
195.15.25.0	11000011 00000111 00011001	000	0-31
195.15.25.32	11000011 00000111 00011001	001	32-63
195.15.25.64	11000011 00000111 00011001	010	64-95
195.15.25.96	11000011 00000111 00011001	011	96-127
195.15.25.128	11000011 00000111 00011001	100	128-159
195.15.25.160	11000011 00000111 00011001	101	160-191
195.15.25.192	11000011 00000111 00011001	110	192-223
195.15.25.224	11000011 00000111 00011001	111	224-255

	195.15.25.73	11000011 00000111	00011001	01001001
AND	255.255.255.224	11111111 11111111	11111111	11100000
=	195.15.25.64	11000011 00000111	00011001	01000000

Bezklasowe trasowanie międzydomenowe (CIDR *Classless InterDomain Routing*, RFC 1519)

Rozwój Internetu spowodował duże zapotrzebowanie na adresy. Przy rozdziale adresów wg klas wiele adresów się marnowało. CIDR umożliwia istnienie wielu mniejszych klas adresowych w ramach jednej, większej domeny trasowania (na poczatku lat 1990 było około 5000 tras w Internecie, a obecnie jest około 100000). Za pomocą adresu IP i maski można trasować dowolny datagram IP do miejsca przeznaczenia.

Bezklasowe trasowanie międzydomenowe (cd)

```
158.75.4.0      (10011110.01001011.00000100.00000000)  Class C subnet
158.75.5.0      (10011110.01001011.00000101.00000000)  Class C subnet
-----------------------------------------------------------------
158.75.4.0      (10011110.01001011.00000100.00000000)  Supernetted Sub
255.255.254.0   (11111111.11111111.11111110.00000000)  Subnet Mask
158.75.5.255    (10011110.01001011.00000101.11111111)  Broadcast addre
```

Grupowanie w nadsieci. Podsieć 158.75.4.0 zawiera wszystkie adresy od 158.75.4.0 do 158.75.5.255. Część sieciowa adresu ma długość 23 bitów, a część określająca hosty – 9.

Stosując notację CIDR taką podsieć zapisuje się jako 158.75.4.0/23.

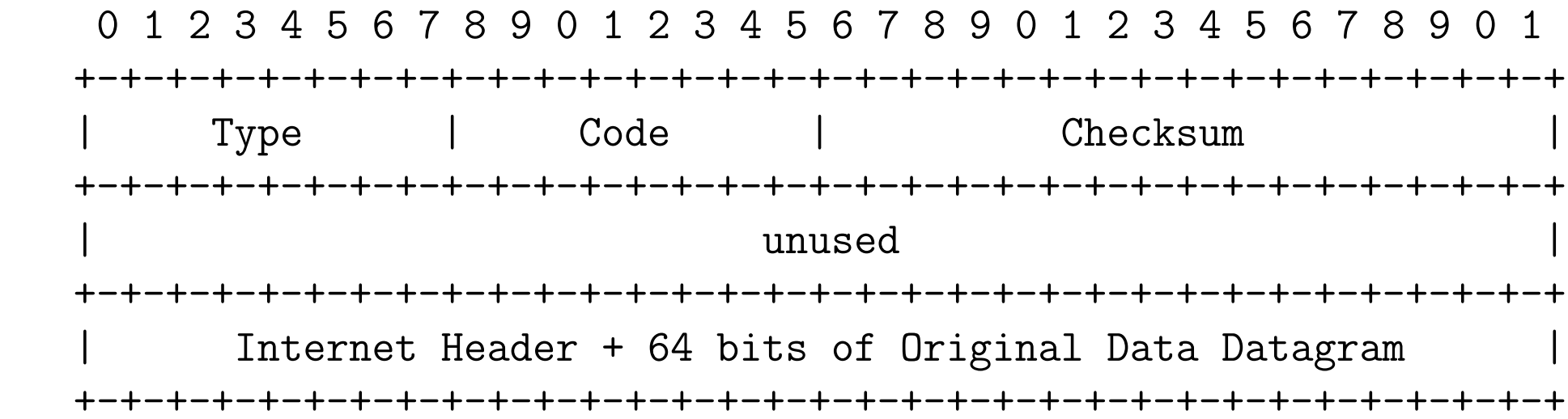
Adres klasy A można zapisac jako /8, klasy B – /16, klasy C – /24.

Internet Control Message Protocol (ICMP, RFC 792) – protokół sterowania wiadomością internetową

Funkcje ICMP:

- sterowanie przepływem datagramów
- wykrywanie nieosiągalnych miejsc przeznaczenia
- przekierunkowywanie marszrut (zmiana trasowania)
- sprawdzanie połączeń z komputerami oddalonymi

Internet Control Message Protocol (cd)



Message Types:

0	Echo Reply		
3	Destination Unreachable	4	Source Quench
5	Redirect	8	Echo
11	Time Exceeded	12	Parameter Problem
13	Timestamp	14	Timestamp Reply
15	Information Request	16	Information Reply

Internet Control Message Protocol (cd)

Komenda: `traceroute 158.75.1.4`

```
traceroute to 158.75.1.4 (158.75.1.4), 30 hops max, 38 byte packets
 1  158.75.5.190 (158.75.5.190)  0.301 ms  0.275 ms  0.227 ms
 2  172.16.3.5 (172.16.3.5)  1.141 ms  1.513 ms  0.998 ms
 3  centrum.man.torun.pl (158.75.33.140)  1.377 ms  1.135 ms  2.386 m
 4  158.75.1.253 (158.75.1.253)  1.923 ms  2.388 ms  2.628 ms
 5  koala.uci.uni.torun.pl (158.75.1.4)  1.674 ms  1.497 ms  2.013 ms
```

Komenda: `ping 158.75.1.4`

```
PING 158.75.1.4 (158.75.1.4) from 158.75.5.95 : 56(84) bytes of data.
64 bytes from 158.75.1.4: icmp_seq=1 ttl=251 time=1.84 ms
64 bytes from 158.75.1.4: icmp_seq=2 ttl=251 time=1.88 ms
64 bytes from 158.75.1.4: icmp_seq=3 ttl=251 time=1.21 ms
```

Internet Control Message Protocol (cd)

Komenda: `ping -f -c 1000 158.75.5.90`

```
PING 158.75.5.90 (158.75.5.90) from 158.75.5.95 : 56(84) bytes of dat

--- 158.75.5.90 ping statistics ---
1000 packets transmitted, 1000 received, 0% loss, time 252ms
rtt min/avg/max/mdev = 0.141/0.154/0.446/0.031 ms, ipg/ewma 0.252/0.1
```

Address Resolution Protocol (ARP RFC 826)

- ARP – protokół odwzorowywania adresów: zmiana adresów logicznych (IP) na adresy fizyczne (MAC)

  Zastosowania: działanie sieci ethernetowych

- RARP (*Reverse Address Resolution Protocol*) – protokół odwrotnego odwzorowywania adresów: zamiana adresów fizycznych (MAC) na adresy logiczne (IP)

  Zastosowania: bootowanie stacji bezdyskowych

Tablica ARP (komenda: **arp**)

```
158.75.4.198          ether   00:B0:D0:F4:83:CD   C     eth0
158.75.5.142          ether   00:50:04:03:9B:F1   C     eth0
158.75.5.54           ether   00:01:02:8A:4C:2D   C     eth0
158.75.5.129          ether   00:00:C0:12:55:6A   C     eth0
158.75.5.238          ether   00:80:AD:8A:0D:89   C     eth0
158.75.5.233          ether   00:10:5A:3C:15:4D   C     eth0
```

Jak powstaje tablica ARP?

Host A (158.75.5.90) próbuje przesłać dane do hosta B (158.75.5.47). Tablica ARP hosta A nie zawiera adresu MAC hosta B.

1. host A wysyła rozgłoszenie (*ARP request*):
   Who has 158.75.5.47? Tell 158.75.5.90.
2. host B odpowiada hostowi A (*ARP reply*):
   158.75.5.47 is at 00:30:48:21:A3:8B
3. host A uzupełnia tablicę ARP o kolejny wpis
4. host A wysyła ramki z adresem docelowym 00:30:48:21:A3:8B

ARP spoofing (podszywanie ARP): odpowiedzi uzyskiwane na zapytania ARP nie są weryfikowane, co pozwala „zatruwać" tablice ARP.

Ograniczenia IP

- zbyt mała liczba adresów ($2^{32} - 1 \approx 4.29 \times 10^9$), nieefektywne wykorzystywanie przestrzeni adresowej (klasy adresowe)
- dwupoziomowa hierarchia adresowania (host.domena), która uniemożliwia konstruowanie wydajnych hierarchii adresowych (nieefektywne trasowanie datagramów)
- słaba obsługa ruchu audio/wideo
- brak mechanizmów zapewniających bezpieczeństwo przekazywania datagramów

Internet Protocol version 6 (IPv6)

- ogromna przestrzeń adresowa ($2^{128} - 1 \approx 3.4 \times 10^{38}$)
- trzy rodzaje adresów (*unicast*, *multicast*, *anycast*)
- obsługa transmisji audio/wideo w czasie rzeczywistym
  - opcje są określone w rozszerzeniu do nagłówka, dzięki czemu mogą być badane po dotarciu pakietu do celu, co pozwala poprawić szybkość przekazywania pakietów od węzła do węzła sieci Internet
  - możliwość znaczenia pakietów (np. pakiety „multimedialne" mogą być przełączane z większym priorytetem)
- bezpieczeństwo (kodowanie i identyfikacja) – nagłówek zawiera rozszerzenie, które pozwala zaznaczyć używany w czasie połączenia mechanizm uwierzytelniania źródła pochodzenia pakietów (zapewnienie integralności i poufności danych)
- mobilność hostów, autokonfiguracja i autorekonfiguracja

Warstwa transportowa

Transmission Control Protocol (TCP, RFC 793) – protokół sterowania transmisją zapewnia usługi niezawodnie dostarczające dane, z wykrywaniem na obu końcach błędów i ich korekcją

Z TCP korzystają m.in. protokoły (warstwy aplikacji):

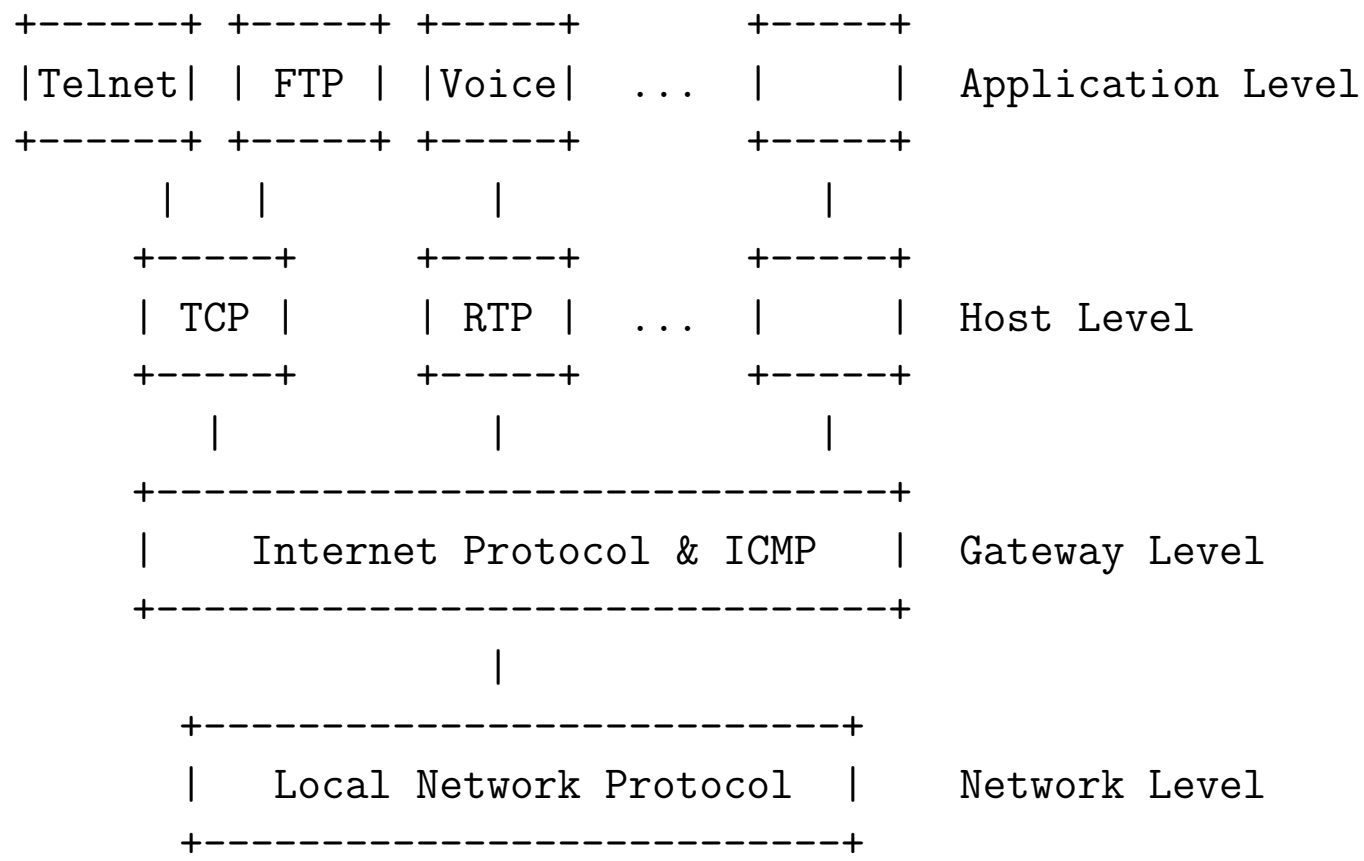
- HTTP (*HyperText Transport Protocol*) protokół przesyłania hipertekstu
- TELNET (*Network Terminal Protocol*) protokół końcówki sieciowej
- SSH (*Secure SHell*) bezpieczna powłoka
- FTP (*File Transfer Protocol*) protokół przesyłania plików

TCP (cd)

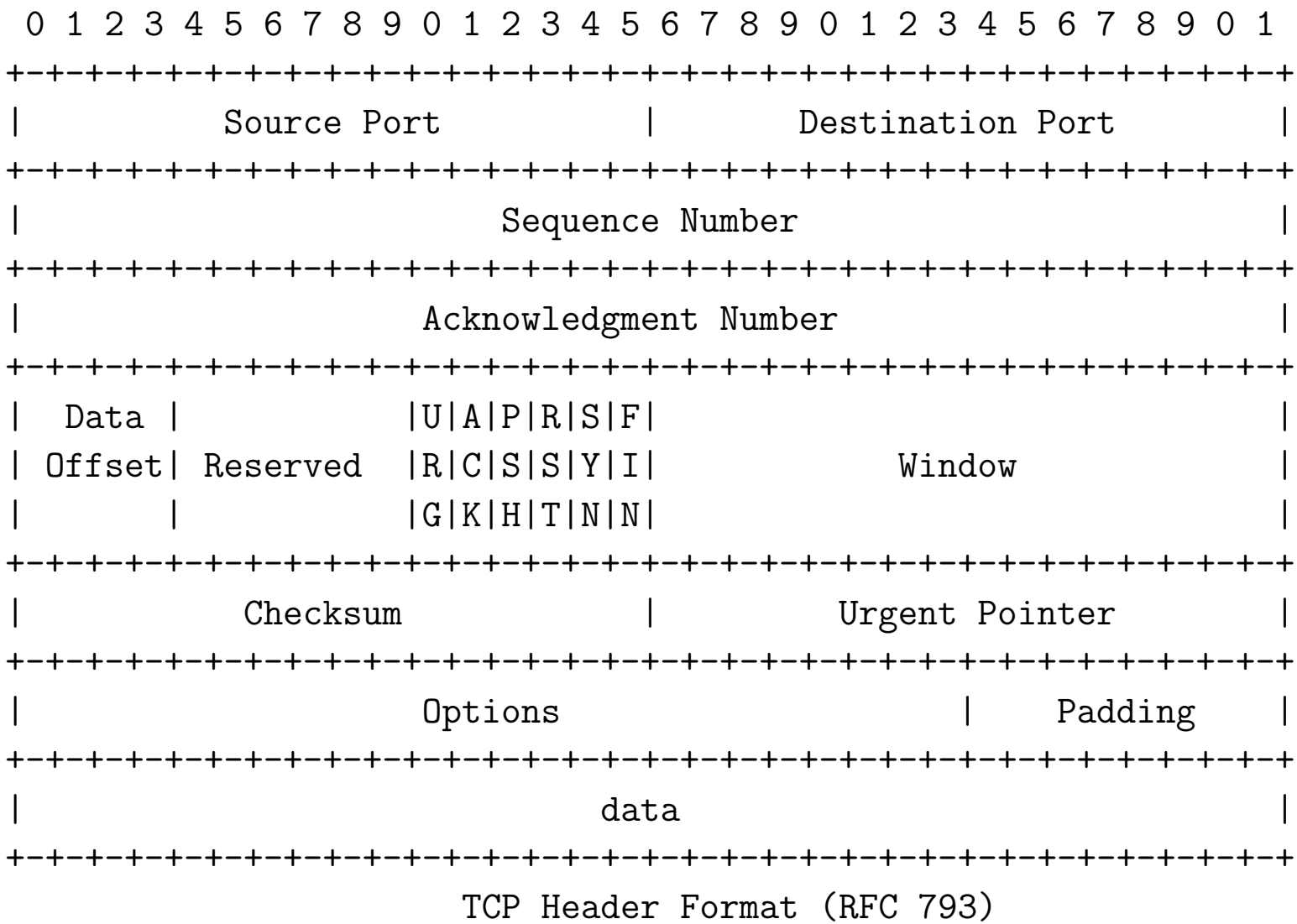
Wg RFC 793, 1.5. Operation:

> As noted above, the primary purpose of the TCP is to provide reliable, securable logical circuit or connection service between pairs of processes. To provide this service on top of a less reliable internet communication system requires facilities in the following areas:
>
> Basic Data Transfer
> Reliability
> Flow Control
> Multiplexing
> Connections
> Precedence and Security

TCP (cd)



Protocol Relationships



TCP Header Format (RFC 793)

TCP Header Format (RFC 793)

```
Control Bits:  6 bits (from left to right):

  URG:  Urgent Pointer field significant
  ACK:  Acknowledgment field significant
  PSH:  Push Function
  RST:  Reset the connection
  SYN:  Synchronize sequence numbers
  FIN:  No more data from sender
```

TCP: Three way handshake

The synchronization requires each side to send it's own initial sequence number and to receive a confirmation of it in acknowledgment from the other side. Each side must also receive the other side's initial sequence number and send a confirming acknowledgment.

```
1) A --> B  SYN my sequence number is X
2) A <-- B  ACK your sequence number is X
3) A <-- B  SYN my sequence number is Y
4) A --> B  ACK your sequence number is Y
```

Because steps 2 and 3 can be combined in a single message this is called the three way (or three message) handshake.

Trzystanowy *handshake* dla synchronizacji połączenia

host A	host B
wysyła SYN (seq=x)	
	odbiera SYN (seq=x)
	wysyła SYN (seq=y)
	wysyła ACK (ack=x+1)
odbiera SYN (seq=y)	
odbiera ACK (ack=x+1)	
wysyła ACK (ack=y+1)	
wysyła dane (seq=x+1)	
	odbiera ACK (ack=y+1)
	odbiera dane

TCP zapewnia niezawodność dostarczania danych za pomocą mechanizmu zwanego **pozytywne potwierdzenie z retransmisją** (*Positive Acknowledgement with Retransmission*, PAR).

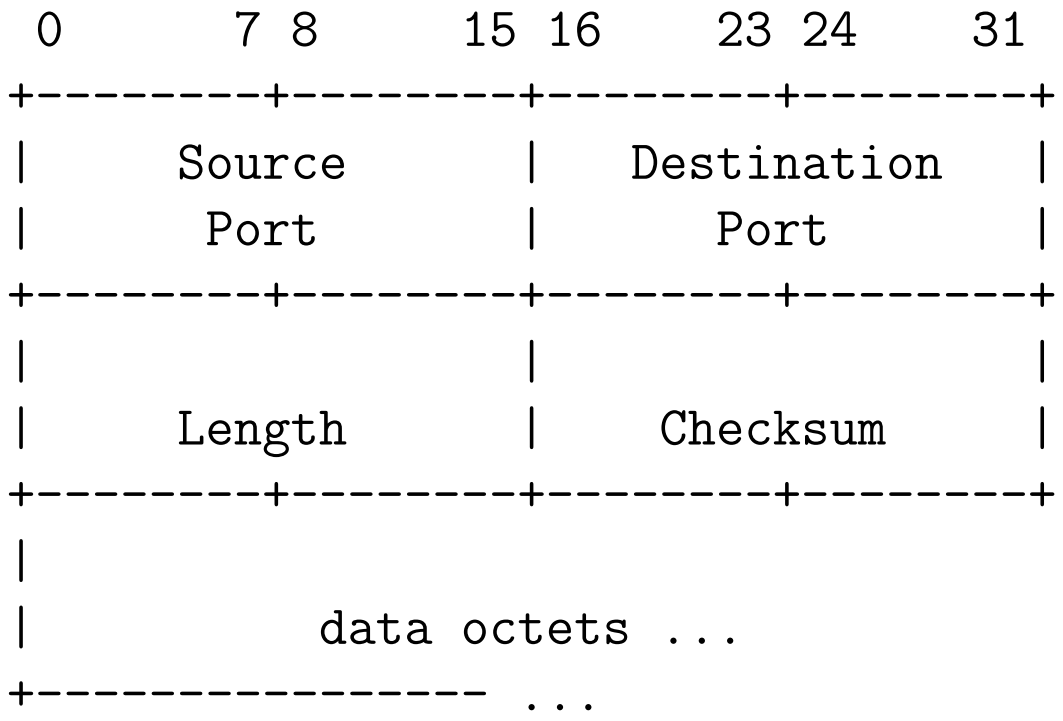
- Dane wysyłane są tak długo, aż nie nadejdzie potwierdzenie, że zostały poprawnie odebrane.
- Jeśli dane są poprawne, to odbiorca wysyła do nadawcy *pozytywne potwierdzenie*.
- Gdy odebrane dane są niepoprawne, to zostają zignorowane. Po określonym czasie moduł nadający powtórnie wysyła dane.
- Odbiorca wysyła nadawcy informację o maksymalnej liczbie bajtów, które wolno wysłać bez czekania na potwierdzenie. Wartość ta jest nazywana **rozmiarem okna** i jest podstawowym mechanizmem kontroli przepływu stosowanym w protokole TCP.

TCP: kontrola przepływu

- algorytm retransmisji z adaptacją ze zmiennym czasem oczekiwania (zależnym od rodzaju sieci i panujących w niej warunków)
- wartość czasu oczekiwania jest obliczana na podstawie bieżącej średniej czasu podróży w dwie strony dla dotychczas wysłanych pakietów
- jeśli odbiór pakietu nastąpi przed upływem czasu oczekiwania, to TCP aktualizuje średnią i stosuje ją przy oczekiwaniu na potwierdzenie kolejnego pakietu
- jeśli odbiór pakietu nie nastąpi przed upływem czasu oczekiwania, to TCP ponownie wysyła pakiet i czeka dwukrotnie dużej
- połączenie jest kontynuowane, jeśli nadejdzie potwierdzenie; przekroczenia maksymalnego czasu oczekiwania powoduje zerwanie połączenia

User Datagram Protocol (UDP, RFC 768)

UDP (protokół datagramów użytkownika) udostępnia usługi dostarczające datagramy z małym narzutem, metodą bezpołączeniową



User Datagram Protocol (cd)

Z UDP korzystają m.in. protokoły (warstwy aplikacji):

- TFTP (*Trivial File Transfer Protocol*) trywialny protokół przesyłania plików
- SNMP (*Simple Network Management Protocol*) prosty protokół zarządzania siecią
- DNS (*Domain Name System*) system nazw domenowych
- NFS (*Network File System*) sieciowy system plików
- DHCP (*Dynamic Host Configuration Protocol*) protokół dynamicznej konfiguracji hostów

Struktury danych protokołów TCP i UDP

warstwy TCP/IP	TCP	UDP
aplikacji	strumień (stream)	wiadomość (message)
transportowa	segment	pakiet
sieciowa	datagram	datagram
dostępu do sieci	ramka (frame)	ramka (frame)

Stream Control Transmission Protocol (SCTP, RFC2960)

Cechy protokołu SCTP:

- oferuje bezbłędne, potwierdzane dostarczanie (bez powtórzeń) datagramów (wiadomości)
- wsparcie dla węzłów o wielu adresach (*multi-homed nodes*)
- wiele strumieni w ramach jednego połączenia
- wbór zasadniczej ścieżki transmisji i sledzenie stanu sesji
- zawiera mechanizmy unikania tworzenia się zatorów
- zawiera mechanizmy uodparniające na ataki typu *flooding* oraz *masquerade*
- strumień SCTP reprezentuje ciąg wiadomości (strumień TCP to ciąg bajtów)
- pojedynczy pakiet składa się z nagówka i jednego lub więcej kawałków zawierających dane sterujące lub dane użytkownika

IANA (Internet Assigned Numbers Authority) i /etc/services

```
# /etc/services:
# $Id: services,v 1.22 2001/07/19 20:13:27 notting Exp $
#
# Network services, Internet style
#
# Note that it is presently the policy of IANA to assign a single well-known
# port number for both TCP and UDP; hence, most entries here have two entries
# even if the protocol doesn't support UDP operations.
# Updated from RFC 1700, ``Assigned Numbers'' (October 1994).  Not all ports
# are included, only the more common ones.
#
# The latest IANA port assignments can be gotten from
#       http://www.iana.org/assignments/port-numbers
# The Well Known Ports are those from 0 through 1023.
# The Registered Ports are those from 1024 through 49151
# The Dynamic and/or Private Ports are those from 49152 through 65535
#
# Each line describes one service, and is of the form:
#
# service-name  port/protocol  [aliases ...]   [# comment]
```

```
tcpmux          1/tcp                           # TCP port service multiplexer
tcpmux          1/udp                           # TCP port service multiplexer
rje             5/tcp                           # Remote Job Entry
rje             5/udp                           # Remote Job Entry
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
systat          11/udp          users
daytime         13/tcp
daytime         13/udp
qotd            17/tcp          quote
qotd            17/udp          quote
msp             18/tcp                          # message send protocol
msp             18/udp                          # message send protocol
chargen         19/tcp          ttytst source
chargen         19/udp          ttytst source
ftp-data        20/tcp
ftp-data        20/udp
ftp             21/tcp
ftp             21/udp
ssh             22/tcp                          # SSH Remote Login Protocol
ssh             22/udp                          # SSH Remote Login Protocol
```

```
telnet          23/tcp
telnet          23/udp
smtp            25/tcp          mail
smtp            25/udp          mail
time            37/tcp          timserver
time            37/udp          timserver
#...
nicname         43/tcp          whois
domain          53/tcp          nameserver      # name-domain server
domain          53/udp          nameserver
whois++         63/tcp
whois++         63/udp
bootps          67/tcp                          # BOOTP server
bootps          67/udp
bootpc          68/tcp                          # BOOTP client
bootpc          68/udp
tftp            69/tcp
tftp            69/udp
#...
finger          79/tcp
finger          79/udp
http            80/tcp          www www-http    # WorldWideWeb HTTP
http            80/udp          www www-http    # HyperText Transfer Protocol
kerberos        88/tcp          kerberos5 krb5  # Kerberos v5
```

```
kerberos        88/udp          kerberos5 krb5  # Kerberos v5
supdup          95/tcp
supdup          95/udp
hostname        101/tcp         hostnames       # usually from sri-nic
hostname        101/udp         hostnames       # usually from sri-nic
iso-tsap        102/tcp         tsap            # part of ISODE.
csnet-ns        105/tcp         cso             # also used by CSO name server
csnet-ns        105/udp         cso
pop3            110/tcp         pop-3           # POP version 3
pop3            110/udp         pop-3
#...
netbios-ns      137/tcp                         # NETBIOS Name Service
netbios-ns      137/udp
netbios-dgm     138/tcp                         # NETBIOS Datagram Service
netbios-dgm     138/udp
netbios-ssn     139/tcp                         # NETBIOS session service
netbios-ssn     139/udp
imap            143/tcp         imap2           # Interim Mail Access Proto v2
imap            143/udp         imap2
```

```
#>REGISTERED PORT NUMBERS
#>
#>The Registered Ports are listed by the IANA and on most systems can be
#>used by ordinary user processes or programs executed by ordinary
#>users.
socks           1080/tcp                        # socks proxy server
socks           1080/udp                        # socks proxy server
h323hostcallsc  1300/tcp                        # H323 Host Call Secure
h323hostcallsc  1300/udp                        # H323 Host Call Secure
ms-sql-s        1433/tcp                        # Microsoft-SQL-Server
ms-sql-s        1433/udp                        # Microsoft-SQL-Server
ms-sql-m        1434/tcp                        # Microsoft-SQL-Monitor
ms-sql-m        1434/udp                        # Microsoft-SQL-Monitor
ica             1494/tcp                        # Citrix ICA Client
ica             1494/udp                        # Citrix ICA Client
wins            1512/tcp                        # Microsoft's Windows Internet Name Service
wins            1512/udp                        # Microsoft's Windows Internet Name Service
```

Gniazda

Interfejs gniazd (*socket interface*) – mechanizm umożliwiający komunikowanie się procesów w tym samym systemie lub procesów różnych hostów w sieci.

Systemy Uniksowe/Linuksowe wspierają szereg klas gniazd łączonych w dziedziny (rodziny) gniazd.

System gniazd Linuxa jest rozszerzoną wersją systemu gniazd z Unixa 4.3 BSD i wspiera m.in. następujące dziedziny adresów:

- UNIX – gniazda domeny Unixowej
- INET – rodzina adresów internetowych wspierająca komunikację przy pomocy protokołów TCP/IP
- IPX – Novell IPX
- APPLETALK – Appletalk DDP (*Datagram Delivery Protocol*)
- X25 – gniazda dla komunikacji w ramach protokołu X25

Gniazda (cd)

Linux implementuje gniazda następujących typów:

- **Stream** – gniazda strumieniowe (zwane czasem obwodem wirtualnym) dostarczają niezawodnego, sekwencyjnego połączenia pomiędzy dwoma komunikującymi się hostami (protokół TCP)
- **Datagram** – gniazda tego typu nie gwarantują dotarcia wysłanej wiadomosci (protokół UDP)
- **Raw** – gniazda umożliwiające procesom bezpośredni, czyli „surowy" dostęp do niżej leżących protokołów; można otworzyć surowe gniazdo do urządzenia ethernetowego i oglądać ruch danych w sieci IP

Warstwa zastosowań (sesji+prezentacji+zastosowań)

- transfer plików – protokół FTP (*File Transfer Protocol*)
- zdalne rejestrowanie się – protokół TELNET (*Network Terminal Protocol*)
- poczta komputerowa – protokoły SMTP (*Simple Mail Transport Protocol*), POP3 (*Post Office Protocol*), IMAP (*Internet Message Access Protocol*)
- listy korespondencyjne i dyskusyjne – protokół NNTP (*Network News Transport Protocol*).
- www (*World Wide Web*) – protokół HTTP (*HyperText Transport Protocol*)
- DNS (*Domain Name Service*) – protokół UDP
- NFS (*Network File System*) – sieciowy system plików pozwalający na współdzielenie plików przez wiele komputerów w sieci (protokoły UDP, TCP)

Aktywny FTP

```
serwer          klient
------          ------
  21    <---    dowolny port
  21    --->    >1024   (odpowiedź serwera na inicjatywę klienta)
  20    --->    >1024   (serwer inicjuje połączenie do portu danych klienta)
  20    <---    >1024   (klient wysyła ACK)
```

Pasywny FTP

```
serwer           klient
------           ------
  21     <---    dowolny port
  21     --->    >1024   (odpowiedź serwera na inicjatywę klienta)
>1024    <---    >1024   (klient inicjuje połączenie na wskazany port serwera)
>1024    --->    >1024   (serwer wysyła ACK)
```

FTP wykorzystuje porty: 20 – port kontrolny, 21 – port danych

Monitorowanie usług i połączeń

Przykłady komend:

- netstat -np
- netstat -npl
- netstat -npl –inet|–ip
- netstat -npl –tcp
- netstat -npl –udp
- nmap -sS adresIP

Monitorowanie usług i połączeń

Komenda: `netstat -npl --tcp`

```
Active Internet connections (only servers)
Proto ... Local Address  Foreign Add   State       PID/Program name
tcp   ... 0.0.0.0:32768  0.0.0.0:*     LISTEN      487/rpc.statd
tcp   ... 0.0.0.0:32769  0.0.0.0:*     LISTEN      701/rpc.mountd
tcp   ... 0.0.0.0:111    0.0.0.0:*     LISTEN      468/portmap
tcp   ... 0.0.0.0:6000   0.0.0.0:*     LISTEN      922/X
tcp   ... 0.0.0.0:113    0.0.0.0:*     LISTEN      638/identd
tcp   ... 0.0.0.0:22     0.0.0.0:*     LISTEN      17456/sshd
tcp   ... 0.0.0.0:631    0.0.0.0:*     LISTEN      759/cupsd
tcp   ... 0.0.0.0:23     0.0.0.0:*     LISTEN      669/xinetd
tcp   ... 0.0.0.0:862    0.0.0.0:*     LISTEN      682/rpc.rquotad
```

Monitorowanie usług i połączeń (cd)

Komenda: `/etc/init.d/identd stop; netstat -npl --tcp`

```
Active Internet connections (only servers)
Proto ... Local Address  Foreign Add   State       PID/Program name
tcp   ... 0.0.0.0:32768  0.0.0.0:*     LISTEN      487/rpc.statd
tcp   ... 0.0.0.0:32769  0.0.0.0:*     LISTEN      701/rpc.mountd
tcp   ... 0.0.0.0:111    0.0.0.0:*     LISTEN      468/portmap
tcp   ... 0.0.0.0:6000   0.0.0.0:*     LISTEN      922/X
tcp   ... 0.0.0.0:22     0.0.0.0:*     LISTEN      17456/sshd
tcp   ... 0.0.0.0:631    0.0.0.0:*     LISTEN      759/cupsd
tcp   ... 0.0.0.0:23     0.0.0.0:*     LISTEN      669/xinetd
tcp   ... 0.0.0.0:862    0.0.0.0:*     LISTEN      682/rpc.rquotad
```

Monitorowanie usług i połączeń (cd)

Komenda: `netstat -np --tcp | grep '158.75.5.95'`

```
tcp ... 158.75.5.90:22  158.75.5.95:33445  ESTABLISHED 6204/sshd
tcp ... 158.75.5.90:22  158.75.5.95:33459  ESTABLISHED 7323/sshd
tcp ... 158.75.5.90:23  158.75.5.95:33494  ESTABLISHED 23272/in.telnetd: t
tcp ... 158.75.5.90:23  158.75.5.95:33496  ESTABLISHED 23643/in.teln
```

Monitorowanie usług i połączeń (cd)

Komenda: `netstat -nlp --udp | grep '158.75.5.95'`

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address    Foreign Add State  PID/Program name
udp        0      0 0.0.0.0:32768    0.0.0.0:*          487/rpc.statd
udp        0      0 0.0.0.0:32770    0.0.0.0:*           -
udp        0      0 0.0.0.0:32771    0.0.0.0:*          701/rpc.mountd
udp        0      0 0.0.0.0:859      0.0.0.0:*          682/rpc.rquotad
udp        0      0 0.0.0.0:111      0.0.0.0:*          468/portmap
udp        0      0 0.0.0.0:631      0.0.0.0:*          759/cupsd
```

Stany gniazda TCP: (`man netstat`)

Super demon sieciowy xinetd (`man xinetd.conf`)

`/etc/xinted.conf`:

```
# Simple configuration file for xinetd
defaults
{
        instances               = 60
        log_type                = SYSLOG authpriv
        log_on_success          = HOST PID
        log_on_failure          = HOST RECORD
        cps                     = 25 30
        enabled                 = telnet ftp
#       disabled                = telnet ftp
}
includedir /etc/xinetd.d
```

Super demon sieciowy xinetd (cd)

/etc/xinted.d/telnet

```
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        disable         = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
        banner_success = /etc/xinetd.d/banners/telnet
```

Super demon sieciowy xinetd (cd)

Plik `/etc/xinted.d/tftp`

```
# default: off
service tftp
{
        disable                 = no
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot
```

Super demon sieciowy xinetd (cd)

Komenda: `/etc/init.d/identd stop; netstat -nltp`

```
Active Internet connections (only servers)
Proto ...  Local Address    ...    State       PID/Program name
tcp   ...  0.0.0.0:32768    ...    LISTEN      484/rpc.statd
tcp   ...  0.0.0.0:515      ...    LISTEN      680/lpd Waiting
tcp   ...  0.0.0.0:111      ...    LISTEN      465/portmap
tcp   ...  0.0.0.0:6000     ...    LISTEN      932/X
tcp   ...  0.0.0.0:21       ...    LISTEN      31390/xinetd
tcp   ...  0.0.0.0:22       ...    LISTEN      651/sshd
tcp   ...  0.0.0.0:23       ...    LISTEN      32713/xinetd
tcp   ...  127.0.0.1:25     ...    LISTEN      702/sendmail: accept
```

Kontrola dostępu: TCP wrappers

- *TCP wrappers* są domyślnie instalowane na serwerach i pozwalają na kontrolę dostępu do szeregu usług internetowych (ssh, telnet, ftp, rsh, itp.)
- usługi sieciowe są „opakowane" w oprogramowanie kontrolujące do nich dostęp; jeśli kryteria dostępu są spełnione, to uruchamiana jest właściwa usługa sieciowa
- biblioteka `libwrap.a` dostarcza odpowiednich funkcji
- `ssh, portmap, xinetd` są kompilowane z biblioteką `libwrap.a`
- inne usługi sieciowe oraz oprogramowanie użytkowe mogą korzystać z `libwrap.a`

Kontrola dostępu: TCP wrappers (cd)

Zalety *TCP wrappers:*

- klient żądający usługi nie dostrzega działania „opakowywaczy”
- „opakowywacze” działają niezależnie od aplikacji, które chronią; wspólne pliki konfiguracyjne, łatwiejsze zarządzanie

Kontrola dostępu: TCP wrappers (cd)

Patrz: `man 5 hosts_access`, `man 5 hosts.allow`

Plik konfiguracyjny: `/etc/hosts.allow`

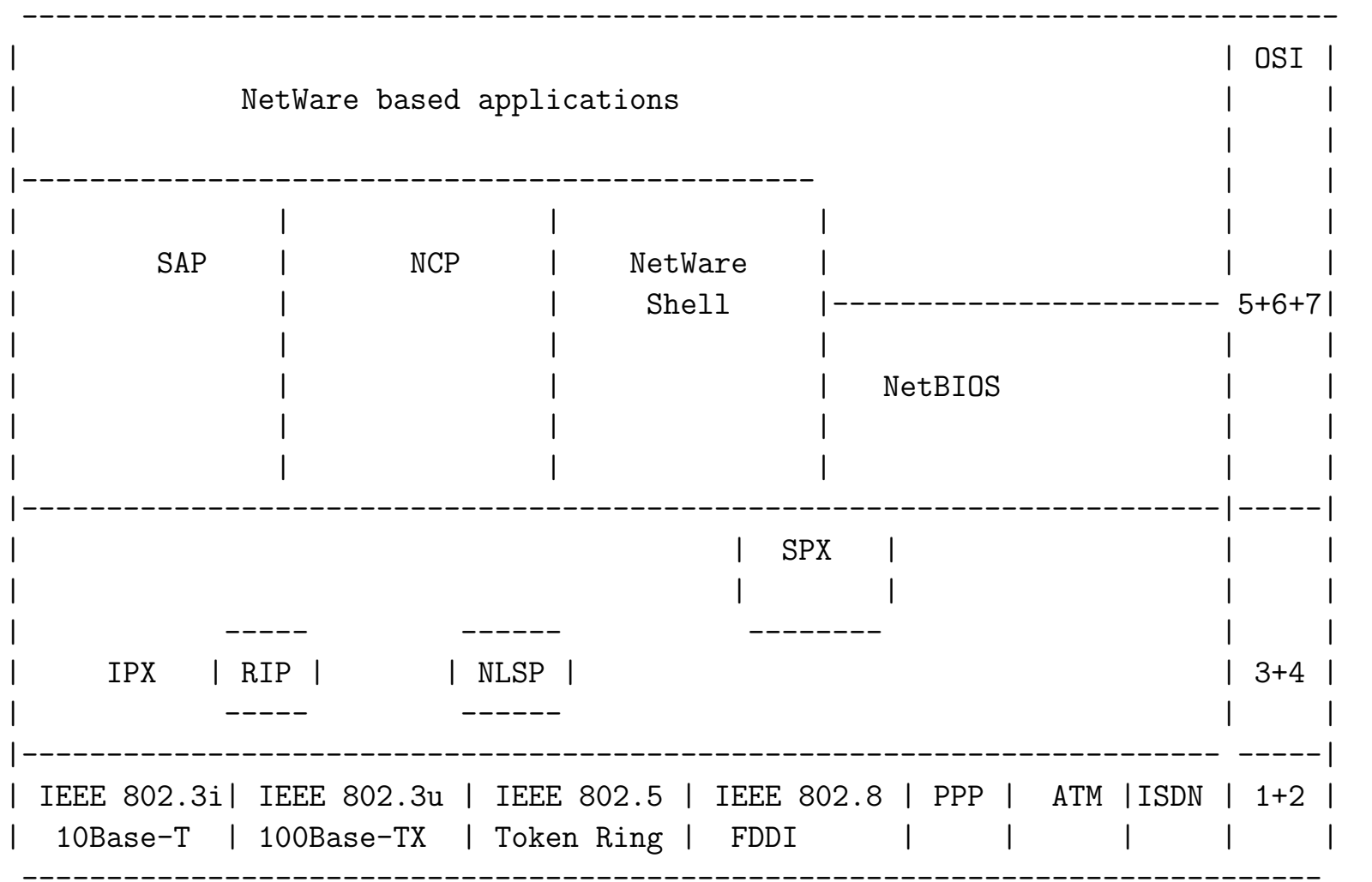
```
#
# hosts.allow This file describes the names of the hosts which are
# allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
#
ALL EXCEPT in.ftpd: 127.0.0.1 158.75.5.95
sshd: 158.75.5. 158.75.4.*
portmap: 158.75.5.51 158.75.5.90
in.telnetd: 158.75.5.1: spawn (/bin/echo `date` %c \
                                >> /var/log/telnet.log) &
```

Kontrola dostępu: TCP wrappers

Plik konfiguracyjny: `/etc/hosts.deny`

```
#
# hosts.deny This file describes the names of the hosts which are
# *not* allowed to use the local INET services, as decided
# by the '/usr/sbin/tcpd' server.
ALL: ALL@ALL, PARANOID : spawn ( /bin/echo `date`  "%d-%h" \
                                  >>/var/log/hosts.deny ) &
```

Rodzina protokołów NetWare firmy Novell



Rodzina protokołów NetWare firmy Novell (cd)

- **SAP** (*Service Advertisment Protocol*) rozgłasza (co 60 sek.) adres i usługi serwera w sieci (identyfikatory SAP: 4 – serwer plików, 7 – serwer drukarek)
- **NCP** (*NetWare Core Protocol*) dostarcza połączeń i aplikacji dla komunikacji klient-serwer (dostęp do plików, drukarek, zarządzanie nazwami, synchronizacja plików, bezpieczeństwo)
- **NetBIOS** (*Network Basic Input/Output System*) pozwala aplikacjom uruchamianym na różnych komputerach na wzajemną komunikację w ramach lokalnej sieci komputerowej (schemat opracowany przez IBM w początkowym okresie rozwoju sieci komputerowych opartych o komputery osobiste, który później został przejęty przez firmę Microsoft i stał się de facto standardem); NetWare dostarcza emulatora pozwalającego uruchamiać aplikacje korzystające z interfejsu NetBIOS

Rodzina protokołów NetWare firmy Novell (cd)

- **SPX** (*Sequenced Packet Exchange*) połączeniowy protokół sekwencyjnej wymiany pakietów wspomagający protokoły warstwy transportowej i służący do sprawdzania czy pakiety IPX docierają do miejsca przeznaczenia
- **IPX** (*Internetwork Packet Exchange*) międzysieciowa wymiana pakietów jest bezpołaczeniowym protokołem (warstwy sieciowej) służącym do łączenia komputerów używających oprogramowania NetWare firmy Novell (oprogramowanie NetWare od wersji 5.0 używa w warstwie sieciowej protokołu IP zamiast IPX)
- **RIP** (*(Novell's) Routing Information Protocol*) protokół routingu wykorzystujący algorytm wektora odległości do wymiany informacji o dostępnych trasach pomiędzy routerami sieci IPX
- **NLSP** (*NetWare Link Services Protocol*) protokół routingu wykorzystujący algorytm stanu łącza (najkrótszej ścieżki)

Cechy systemu NetWare

- 80-bitowy adres postaci network.node (32+48-bitów)
- adres MAC jest częścią adresu logicznego
- wiele rodzajów kapsułkowania na pojedynczym interfejsie
- domyślnym protokolem routingu jest Novell RIP
- usługi są rozgłaszane przez SAP
- klienci znajdują serwery poprzez pakiety GNS (*Get Nearest Server*)
- RIP i NLSP są implementowane jako protokoły warstw 5-7

Rodzaje kapsułkowania w NetWare

nazwa novellowa		struktura ramki
NetWare $\leqslant$ 3.11:	Ethernet_802.3	802.3 | IPX
NetWare $\geqslant$ 3.12:	Ethernet_802.2	802.3 | 802.2 LLC | IPX
TCP/IP:	Ethernet_II	Ethernet | IPX
TCP/IP+AppleTalk:	Ethernet_SNAP	802.3 | 802.2 LLC | SNAP | IPX

Struktura nagłówka pakietu IPX

- suma kontrolna (*checksum*, 2)
- długość pakietu (*packet length*, 2) – liczba oktetów nagłówka i danych
- sterowanie transportem (*transport control*, 1) – liczba routerów ($\leqslant$16), które pakiet może przejść zanim zostanie usunięty (każdy router zwiększa to pole o jeden)
- typ pakietu (*packet type*, 1) – numer usługi, która utworzyła pakiet (NCP(17), SAP, NetBIOS, SPX(5), RIP, NLSP)

Struktura nagłówka pakietu IPX (cd)

- numer sieci docelowej (*destination network*, 4) – numer sieci, w której znajduje się węzeł docelowy
- adres węzła docelowego (*destination node*, 6) – adres MAC węzła, w którym znajduje się docelowy komputer
- numer gniazda docelowego (*destination socket*, 2) – numer gniazda procesu odbierającego pakiety
- numer sieci źródłowej (*source network*, 4) – numer sieci, w której znajduje się węzeł źródłowy
- adres węzła źródłowego (*source node*, 6) – adres MAC węzła, w którym znajduje się komputer źródłowy
- numer gniazda źródłowego (*source socket*, 4) – numer gniazda procesu wysyłającego pakiety

NetBIOS i NetBEUI

- *NetBIOS Extended User Interface* (NetBEUI) –rozszerzony interfejs użytkownika podstawowego systemu wej/wyj jest rozbudowaną wersją protokołu NetBIOS używanego przez sieciowe systemy operacyjne takie jak LAN Manager, LAN Server, Windows for Workgroups, Windows NT, Samba.
- Interfejs NetBIOS został opracowany przez firmę Sytec Inc. dla IBM w 1983 r. na potrzeby sieci komputerów IBM PC (*PC Network*)
- NetBEUI został wprowadzony w 1985 r., aby aplikacje dla PC Network mogły pracować w sieci Token-Ring
- w 1987 r. Microsoft wprowadził LAN Managera, który wykorzystywał ramki NetBIOS-owe
- NetBIOS/NetBEUI są „protokołami" warstwy sesji i wykorzystują do transportu niższe warstwy (*NetBIOS over TCP/IP, NetBIOS over IPX/-SPX, NetBIOS over PPP*)

NetBIOS i NetBEUI (cd)

- NetBIOS nie jest protokołem, ale interfejsem do rodziny protokołów: *Name Management Protocol* (NMP), *Diagnostic and Monitoring Protocol* (DMP), *User Datagram Protocol* (UDP), *Session Management Protocol* (SMP).

  NetBIOS był zaprojektowany jako interfejs programów użytkowych (API, *Application Programming Interface*)

- NetBEUI jako rozszerzenie NetBIOS-u nie jest protokołem, lecz API

- **protokoł NetBIOS/NetBEUI** – rodzina protokołów używanych przez API NetBIOS/NetBEUI

- w trakcie rozwoju NetBEUI powstały nowe protokoły zwane *NetBIOS Frames* (NBF), czyli niekapsułkowana implementacja NetBIOS-u

- NetBIOS/NetBEUI = NetBIOS Frames Protocol for 802.2 Networks (oficjalna nazwa używana przez IBM)

Server Message Block Protocol (SMB)

- **Server Message Block Protocol**, blok komunikatów serwera, jest protokołem warstwy aplikacji
- SMB służy do implementowania sterowania sesjami sieciowymi, sieciowym systemem plików, dostępem do sieciowych drukarek i przekazywaniem komunikatów
- zapewnia podobną funkcjonalność jak ASP, AFP, NCP, NFS
- SMB wykorzystuje:
  - NetBIOS Frames Protocol (NBF)
  - NetBIOS over TCP/IP
  - NetBIOS over IPX

Rodzaje sieci

- **LAN** (*Local Area Network*) – lokalna sieć komunikacyjna obejmująca niewielki obszar geograficzny i umożliwiająca szybki i szerokopasmowy dostęp do lokalnych serwerów. LAN może także umożliwiać hostom dostęp do zasobów sieci rozległej (WAN).

  Urządzenia LAN: komputery, serwery, drukarki sieciowe, koncentratory, przełączniki, routery.

- **WAN** (*Wide Area Network*) – rozległa sieć komunikacyjna obejmująca swoim zasięgiem rozległy obszar geograficzny i umożliwiająca LAN-om łączność poprzez komutowane lub dedykowane łącza. Technologie WAN funkcjonują w trzech pierwszych warstwach modelu OSI.

  Urządzenia WAN: routery, przełączniki, serwery telekomunikacyjne (*dial-up*), modemy

Rodzaje topologii sieci

- **sieć z szyną wielodostępną** – pojedyncze łącze jest dzielone przez wszystkie stanowiska; szyna może mieć organizację linii prostej lub pierścienia
- **sieć w kształcie gwiazdy** – jedno ze stanowisk jest połączone ze wszystkimi pozostałymi
- **sieć w kształcie pierścienia** – każde stanowisko połączone z dwoma sąsiednimi; pierścień może być jedno- lub dwukierunkowy
- **sieć w pełni połączona** – każde stanowisko (węzeł) jest bezpośrednio połączony ze wszystkimi pozostałymi stanowiskami w systemie.
- **sieć częściowo połączona** – bezpośrednie łącza istnieją tylko między niektórymi (nie wszystkimi) parami stanowisk

Sieci Ethernet/IEEE 802.3

- Lokalne sieci komputerowe są budowane w oparciu o normę IEEE 802.3 z roku 1985, która definiuje ramkę danych oraz określa sposób dostępu do nośnika.
- Norma ta uściśla i rozszerza specyfikację właściwą dla sieci Ethernet I (Ethernet PARC) i Ethernet II (Ethernet DIX); sieci wykorzystujące normę IEEE 802.3 zwane są sieciami ethernetowymi.
- Rodzaje ramek ethernetowych: PARC, DIX, 802.3, LLC (*Logical Link Control*), SNAP (*Sub-Network Access Protocol*)
- Materialnymi nośnikami transmisji są kabel koncentryczny, skrętka dwużyłowa, kabel światłowodowy, pusta przestrzeń. Ich fizyczne własności określają szerokość dostępnego pasma transmisyjnego, częstotliwości sygnałów i efektywną prędkość przesyłania danych.

IEEE *Institute of Electrical and Electronics Engineers*

Dostęp do łącza:

wielodostęp do łącza z badaniem stanu kanału i wykrywaniem kolizji (CSMA/CD, *carrier-sense with multiple access/colission detection*)

- sprawdzanie stanu kanału przed wysłaniem komunikatu
- wykrywanie kolizji i wstrzymywanie nadawania
- wznawianie nadawania po losowo określonej (i stopniowo wydłużanej) przerwie

Taka forma dostępu do łącza jest wykorzystywana w sieciach typu Ethernet (IEEE 802.3).

Nośniki transmisji fizycznej:

- cienki kabel koncentryczny RG-58 (50 Ω)
- nieekranowana (czteroparowa) skrętka (UTP, *Unshielded Twisted Pair*)
  - kategoria 1,2: uznane za przestarzałe w 1995
  - kategoria 3 UTP: szerokość pasma 16 MHz, szybkość 10 Mb/s, maks. odległość 100 m
  - kategoria 4 UTP: szerokość pasma 20 MHz
  - kategoria 5 UTP: szerokość pasma 100 MHz, szybkość 10, 100, 256 Mb/s, maks. odległość 100 m.
- ekranowana skrętka (STP, *Shielded Twisted Pair*)
- światłowód
  - wielomodowy 62.5 μm (62.5/125), LED (*Light Emitting Diode*)
  - jednomodowy 8-10 μm (osłona 125μm) ILD (*Injection Laser Diode*)

LAN – rodzaje sieci Ethernet

- **10Base-5** – sieć z szyną wielodostępną w formie linii prostej wykorzystująca gruby kabel koncentryczny (tzw. gruby ethernet); zasięg do 500m, pasmo 10Mbs (IEEE 802.3)
- **10Base-2** – sieć z szyną wielodostępną w formie linii prostej wykorzystująca cienki kabel koncentryczny (tzw. cienki ethernet); zasięg do 185m, 30 hostów w segmencie; pasmo 10Mb/s (IEEE 802.3a)
- **10Base-T** – sieć w formie gwiazdy wykorzystująca nieekranowaną skrętkę (kategorii 3,4 lub 5); zasięg do 100m; pasmo 10Mb/s (IEEE 802.3i)
- **10Base-FL/FB** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca włókna światłowodowe; zasięg do 2km; pasmo 10Mb/s (IEEE 802.3j)
- **100Base-TX** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca 2 pary nieekranowanej skrętki (kategorii 5); zasięg do 100m, pasmo 100Mb/s (IEEE 802.3u)

- **100Base-T4** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca 4 pary nieekranowanej skrętki (kategorii 3,4,5); zasięg do 100m, pasmo 100Mb/s (IEEE 802.3u)
- **100Base-FX** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca włókna światłowodowe (wielomodowe); zasięg do 2km, pasmo 100Mb/s
- **1000Base-T** – sieć w formie gwiazdy wykorzystująca nieekranowaną skrętkę (kategorii 5, 4 pary); zasięg do 100m, pasmo 1Gb/s (IEEE 802.3ab)
- **1000Base-LX** – krótka sieć szkieletowa wykorzystująca włókna światłowodowe (jednomodowe); zasięg do 5km; pasmo 1Gb/s (IEEE 802.3z)
- **10GBase-ER/EW** – połączenie punkt-punkt wykorzystujące włókna światłowodowe (jednomodowe); zasięg do 40km; pasmo 10Gb/s (IEEE 802.3ae)

Topologie sieci ethernetowej

- topologia magistrali
- topologia gwiazdy
- topologia rozszerzonej gwiazdy
- topologia hierarchiczna gwiazdy
- topologia przełączana

Domena rozgłoszeniowa i domena kolizyjna.

Przy zastosowaniu topologii przełączanej następuje segmentacja domeny kolizyjnej (mikrosegmentacja).

Urządzenia sieciowe: regenerator, koncentrator

- Regenerator (wzmacniak) jest urządzeniem warstwy 1, które wzmacnia i regeneruje sygnał w sieci Ethernet. Dzięki temu możliwe staje się rozszerzenie sieci na większy obszar i obsłużenie większej liczby użytkowników.
- Zastosowanie regeneratorów powoduje zwiększenie domeny rozgłoszeniowej i domeny kolizyjnej.
- Koncentrator to wieloportowy wzmacniak (*multiport repeater, hub*).

Metody zwiększenia wydajności sieci Ethernet/802.3

- nadawanie dwukierunkowe (pełny dupleks)

  wymagania:

  – dwie pary przewodów

  – NIC i urządzenia sieciowe wyposażone w możliwość transmisji dwukierunkowej

- podział sieci LAN na segmenty

  wymagania:

  – mosty

  – routery

  – przełączniki

Urządzenia sieciowe: most

- Most (*bridge*) jest urządzeniem sieciowym warstwy 2 łączącym dwa segmenty sieci, które wykorzystuje adresy MAC do filtrowania ramek. Most tworzy tablicę adresów zawierającą wpisy typu interfejs-MAC, dzięki czemu możliwe staje się przekazywanie ramek tylko do właściwych segmentów.
- Most jest urządzeniem typu „przechowaj i przekaż" (*store and forward*).
- Most dzieli sieć LAN na dwie domeny kolizyjne (pozostaje jedna domena rozgłoszeniowa).

Urządzenia sieciowe: przełącznik ethernetowy

- Przełącznik ethernetowy (*Ethernet switch*) jest wieloportowym mostem, który dzieli sieć LAN na mikrosegmenty, które tworzą bezkolizyjne domeny.
- Jeśli przełącznik nie zna segmentu docelowego ramki, to przekazuje ją do wszystkich segmentów z wyjątkiem segmentu źródłowego.

  Pozostaje jedna domena rozgłoszeniowa!
- Sieć o topologii przełączanej zachowuje się tak, jakby miała tylko dwa węzły, które dzielą między siebie całe dostępne pasmo transmisyjne.
- Każde dwa komunikujące się węzły połączone są obwodem wirtualnym.
- Przełączanie symetryczne i asymetryczne.

Urządzenia sieciowe: przełącznik ethernetowy (cd)

Stosowane są dwie metody przełączania:

1. **Przechowaj i przekaż** (*store and forward*) – przed przekazaniem ramki do segmentu (portu) docelowego cała ramka jest odbierana, odczytywane są adresy źródła oraz przeznaczenia i stosowane reguły fitrowania.

   Cechy:

   – możliwość wykrywania błędów

   – im dłuższa ramka tym większe opóźnienie

Urządzenia sieciowe: przełącznik ethernetowy (cd)

2. **Przycinanie** (*cut-through*) – po odczytaniu adresu docelowego ramka jest kierowana do docelowego portu bez oczekiwania na odebranie jej pozostałej części.

   Przycinanie przyjmuje postać

   – przekazywania typu szybkie przełączanie (*fast forward*) – natychmiastowe przekazywanie ramki po otrzymaniu adresu docelowego (możliwość przekazywania błędnych ramek)
   – przełączania bez fragmentacji (*fragment free*) – przed przekazywaniem odfiltrowywane są fragmenty powodujące kolizje (krótsze niż 64 bajty)

   Cechy:

   – słaba wykrywalność błędów
   – zmniejszone opóźnienia transmisji

Urządzenia sieciowe: router

- Router jest urządzeniem sieciowym warstwy 3 łączącym dwa lub więcej segmentów lokalnej sieci komputerowej, kilka sieci LAN (lub WAN). Router przekazuje (trasuje) pakiety wykorzystując adresy warstwy 3. i tablicę routingu. Tabela routingu jest budowana w oparciu o jedną lub wiele metryk w celu ustalenia optymalnej ścieżki dla ruchu sieciowego.
- Router dzieli sieć LAN na oddzielne domeny kolizyjne i rozgłoszeniowe.
- Router wprowadza większe opóźnienia w ruchu pakietów niż koncentratory i przełączniki.

Urządzenia sieciowe: router (cd)

- Router tworzy tablicę routing dzięki wymianie informacji z innymi routerami przy wykorzystaniu protokołów trasowania.

Protokół trasowany/routowalny (*routed protocol*) to dowolny protokół sieciowy, który może być trasowany/routowany przez router i który dostarcza schematu adresowania pozwalającego na dostarczanie pakietów od jednego hosta do drugiego. Protokóły IP i IPX są przykładami protokołów trasowanych/routowalnych.

Protokół trasowania/routingu (*routing protocol*) to protokół obsługujacy protokoły trasowane poprzez dostarczanie mechanizmów umożliwiających wymianę informacji między routerami i wybór trasy pakietów. Do protokołów routing zaliczamy takie protokoły jak *Routing Information Protocol* (RIP), *Interior Gateway Routing Protocol* (IGRP), *Enhanced IGRP*, *Open Shortest Path First (OSPF)*.

Urządzenia sieciowe: przełącznik warstwy 3.

W 1992 roku firma 3Com rozpoczęła scalanie produkowanych przez siebie przełączników i routerów (cel: zmniejszenie liczby urządzeń sieciowych, którymi trzeba zarządzać i obniżenie kosztów).

Generation	Technology	Product	Routing Performance
First	Software	LANplex(R) 5000 switch	50K pps
Second	ISE ASIC	CoreBuilder 2500, 6000 switch	100K-1.1Mpps
Third (1997)	FIRE ASIC	CoreBuilder 3500, 9000 switch	3.5M-64M pps

wg R.Ciampa, *Layer 3 switching*, 3Com documentation

ASIC *Application Specific Integrated Circuit*

FIRE *Flexible Intelligent Routing Engine*

ISE *Intelligent Switching Engine*

Współczesny model sieci versus OSI i TCP/IP

<table>
<tr><th>model współczesny</th><th colspan="2">model OSI</th><th colspan="2">model TCP/IP</th></tr>
<tr><td rowspan="3">aplikacji</td><td>warstwa aplikacji (7)</td><td rowspan="3"></td><td rowspan="3">(4)</td><td rowspan="3">aplikacji</td></tr>
<tr><td>warstwa prezentacji (6)</td></tr>
<tr><td>warstwa sesji (5)</td></tr>
<tr><td>transportowa</td><td>warstwa transportowa (4)</td><td>(3)</td><td>transportowa</td></tr>
<tr><td>routowania</td><td>warstwa sieciowa (3)</td><td>(2)</td><td>Internet</td></tr>
<tr><td rowspan="2">przełączania
interfejsu</td><td>warstwa łącza danych (2)</td><td rowspan="2"></td><td rowspan="2">(1)</td><td rowspan="2">dostępu do sieci</td></tr>
<tr><td>warstwa fizyczna (1)</td></tr>
</table>

Urządzenia sieciowe: przełącznik ethernetowy 3Com 3300

- obsługa kilkunastu tysięcy adresów MAC
- automatyczny wybór prędkości transmisji (*auto-sensing*) portu w zależności od rodzaju przyłączonego urządzenia sieciowego
- możliwość tworzenia wirtualnych LAN-ów (*Virtual LAN*) oraz wykorzystanie *FastIP* do przyspieszenia komunikacji pomiędzy VLAN-ami.
- możliwość traktowania wielu równoległych połączeń jako jednego (*port trunking*)
- możliwość tworzenia zapasowych połączeń (*resilient links*) i podwójnych ścieżek w ramach protokołu częściowego drzewa (STP, *Spanning Tree Protocol*, IEEE 802.1d)
- sterowanie przepływem poprzez zastosowanie trybu pełnego dupleksu (IEEE 802.3x) oraz zastosownie *Intelligent Flow Managment* dla trybu półdupleksowego.
- obsługa znakowania wg IEEE 802.1q

Urządzenia LAN: przełącznik ethernetowy 3Com 3300 (cd)

- możliwość priorytetyzowania ruchu poprzez zastosowanie ośmiu kolejek (IEEE 802.1p); poprawa wydajność sieci multimedialnych
- filtrowanie pakietów multicastowych w oparciu o system IEEE 802.1p, który korzysta z GMRP (*GARP Muticast Registration Protocol*) oraz IGMP (*Internet Group Management Protocol*)
- zarządzanie kilkoma przełącznikami zestawionymi w stos jak pojedynczym urządzeniem
- zarządzanie i kontrolowanie całej sieci z jednego stanowiska
- kontrolowanie i konfigurowanie urządzenia za pomocą CLI, przeglądarki www, protokołu SNMP (*Simple Network Management Protocol*) oraz RMON-u (*Remote Monitoring*)

Wirtualne sieci lokalne (VLAN)

W typowej sieci LAN użytkownicy są grupowani w oparciu o ich położenie względem koncentratora. Użytkownicy (zwykle) różnych kategorii walczą o pasmo, dostęp do routera i sieci szkieletowej.

- Wirtualne sieci lokalne (*Virtual LANs*) pozwalają na grupowanie użytkowników podług ich przynależności organizacyjnej, pełnionej funkcji, wydziału, potrzeb, itp. niezależnie od położenia ich segmentu fizycznego.
- Sieci VLAN dokonują logicznego podziału fizycznej infrastruktury sieci lokalnej na różne podsieci (domeny rozgłoszeniowe).
- Sieci VLAN działają na poziomie warstwy 2 i 3 modelu OSI.
- Komunikacja między sieciami VLAN zapewniona jest prze routing warstwy 3.
- Użytkownicy są przypisywani do sieci VLAN przez administratora.

Wirtualne sieci lokalne (cd)

- Przekazywanie ramek poprzez sieć szkieletową wymaga ich znakowania poprzez umieszczenie w nagłówku ramki unikatowego identyfikatora (IEEE 802.1q)
- Rodzaje sieci VLAN:
  1. bazujące na portach – wszystkie węzły tej samej sieci VLAN przypisane są do jednego portu przełącznika
  2. statyczne – porty przełącznika są ręcznie przypisywane do określonych sieci VLAN
  3. dynamiczne – porty przełącznika dokonują automatycznego wyboru sieci VLAN w oparciu o adres MAC, adres logiczny lub typ protokołu wykorzystywanego przez pakiety danych.

Wirtualne sieci lokalne (cd)

Zalety sieci VLAN:

- ograniczenie domen rozgłoszeniowych
- zwiększenie bezpieczeństwa poprzez separację użytkowników
- łatwość obsługi przemieszczających się użytkowników
  - mniej zmian w okablowaniu i konfiguracji
  - brak konieczności rekonfiguracji routerów

Konfiguracja urządzeń sieciowych

Komenda: `ifconfig`

```
eth0      Link encap:Ethernet  HWaddr 00:30:48:21:A3:8B
          inet addr:158.75.5.47  Bcast:158.75.5.255  Mask:255.255.254.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84502524 errors:0 dropped:0 overruns:36 frame:0
          TX packets:109005454 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1377116795 (1313.3 Mb)  TX bytes:3059594632 (2917.8 Mb)
          Interrupt:16 Base address:0xf000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:340138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:340138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:152325113 (145.2 Mb)  TX bytes:152325113 (145.2 Mb)
```

Konfiguracja urządzeń sieciowych (cd)

wartości MTU: 576 (wartość domyślna), 1500 (PPP, Ethernet), 1006 (SLIP)

netstat -s

```
Ip:
    86788548 total packets received
    10797 with invalid headers
    1190614 forwarded
    ...

Icmp:
    229379 ICMP messages received
    256 input ICMP message failed.
    ...

Tcp:
    34830 active connections openings
    1144833 passive connection openings
```

```
    80 failed connection attempts
    34841 connection resets received
    ...

Udp:
    17397316 packets received
    74955 packets to unknown port received.
    481739 packet receive errors
    12428262 packets sent
TcpExt:
    7852 resets received for embryonic SYN_RECV sockets
    4775 packets pruned from receive queue because of socket buffer overrun
    105 ICMP packets dropped because they were out-of-window
    290 ICMP packets dropped because socket was locked
    ...
```

Konfiguracja urządzeń sieciowych (cd)

Komenda: `netstat -nr`
`route -ne`

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.20.0.2      0.0.0.0         255.255.255.255 UH        0 0          0 tun0
158.75.4.0      0.0.0.0         255.255.254.0   U         0 0          0 eth3
172.20.0.0      172.20.0.2      255.255.128.0   UG        0 0          0 tun0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth3
0.0.0.0         158.75.5.190    0.0.0.0         UG        0 0          0 eth3
```

Konfiguracja urządzeń sieciowych (cd)

Komenda: `route -ee`

```
Kernel IP routing table
Destination  Gateway       Genmask         Flags Metric Ref Use Iface  MSS  Window
172.20.0.2   0.0.0.0       255.255.255.255 UH    0      0     0 tun0   0    0
158.75.4.0   0.0.0.0       255.255.254.0   U     0      0     0 eth3   0    0
172.20.0.0   172.20.0.2    255.255.128.0   UG    0      0     0 tun0   0    0
169.254.0.0  0.0.0.0       255.255.0.0     U     0      0     0 eth3   0    0
0.0.0.0      158.75.5.190  0.0.0.0         UG    0      0     0 eth3   0    0
```

Analiza ruchu sieciowego: tcpdump

```
NAME
       tcpdump - dump traffic on a network

SYNOPSIS
       tcpdump [ -adeflnNOpqRStuvxX ] [ -c count ] [ -F file ]
               [ -i interface ] [ -m module ] [ -r file ]
               [ -s snaplen ] [ -T type ] [ -U user ] [ -w file ]
               [ -E algo:secret ] [ expression ]

DESCRIPTION
       Tcpdump prints out the headers of packets on a network
       interface that match the boolean expression.
```

Analiza ruchu sieciowego: ethereal

```
NAME
       ethereal - Interactively browse network traffic

SYNOPSYS
       ethereal [ -a capture autostop condition ] ...  [ -b num-
       ber of ring buffer files ] [ -B byte view height ] [ -c count ]
       ...

DESCRIPTION
       Ethereal is a GUI network protocol analyzer.  It lets you
       interactively browse packet data from a live network or from a
       previously saved cap- ture file.  Ethereal's native capture
       file format is libpcap format,
```

Standardy EIA/TIA-568B

Instalacja sieciowa powinno być wykonane zgodnie z normami EIA/TIA-568B, które określają sposób wykonania okablowania:

- poziomego
- węzłów dystrybucyjnych
- szkieletowego
- pomieszczeń zawierających urządzenia sieciowe
- miejsc pracy i urządzeń wejściowych

EIA *Electronics Industry Association* Towarzystwo Przemysłu Elektronicznego
TIA *Telecommunications Industry Association* Towarzystwo Przemysłu Telekomunikacyjnego

Okablowanie poziome łączy każde gniazdo telekomunikacyjne z poziomym punktem dystrybucyjnym (krosownicą).

Rodzaje przewodów:

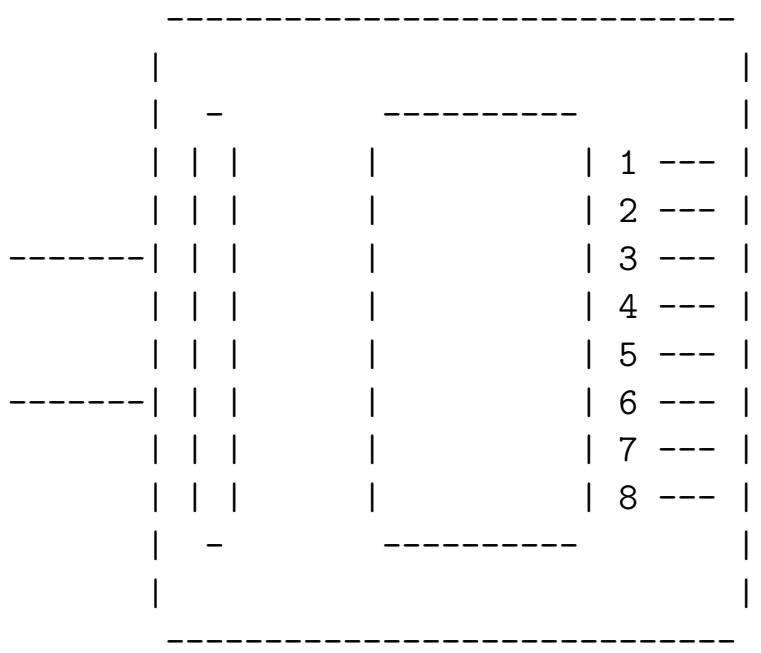
- UTP (*Unshielded Twisted Pair*): max. długość segmentu 3+90+6 (3m kabel od urządzenia sieciowego do gniazda, 90m od gniazda telekomunikacyjnego do krosownicy, 6m kable połączeniowe w węźle dystrybucyjnym)

  4 pary przewodów:

para #1	biało-niebieska/niebieska
para #2	biało-pomarańczowa/pomarańczowa
para #3	biało-zielona/zielona
para #4	biało-brązowa/brązowa

- RG58A/U (kabel koncentryczny): 50 Ω, max. długość segmentu 185m, max. liczba węzłów 30
- kabel światłowodowy wielomodowy (62.4/125 μm)

Wtyk RJ-45



Uwaga: złote styki u góry, języczek u dołu

Kabel prosty

	DTE	568B (RJ-45)		568B (RJ-45)	DCE	
1	N+	biało-pomarańczowy	1 ⟶ 1	biało-pomarańczowy	O+	1
2	N–	pomarańczowy	2 ⟶ 2	pomarańczowy	O–	2
3	O+	biało-zielony	3 ⟶ 3	biało-zielony	N+	3
4		niebieski	4 ⟶ 4	niebieski		4
5		biało-niebieski	5 ⟶ 5	biało-niebieski		5
6	O–	zielony	6 ⟶ 6	zielony	N–	6
7		biało-brązowy	7 ⟶ 7	biało-brązowy		7
8		brązowy	8 ⟶ 8	brązowy		8

DCE (*Data Communications Equipment*) urządzenie końcowe łącza teleinformatycznego

DTE (*Data Terminal Equipment*) terminal teleinformatyczny

DCE vs DTE

- DCE (*Data Communications Equipment, Data Circuit-terminating Equipment*) urządzenie końcowe łącza teleinformatycznego, czyli urządzenie teleinformatyczne, które przekazuje („komunikuje") sygnały wytwarzane przez inne urządzenia (modemy, routery, porty MDI-X koncentratora)

  odpowiednikiem ethernetowym DCE jest IEA/TIA 568A

- DTE (*Data Terminal Equipment*) terminal teleinformatyczny – urządzenie teleinformatyczne, które samo generuje lub otrzymuje przekazywane do niego sygnały (interfejsy sieciowe komputerów, routery, porty MDI koncentratora)

  odpowiednikiem ethernetowym DTE jest IEA/TIA 568B

MDI (*Media Dependent Interface*)
MDI-X (*Media Dependent Interface Cross-over*)

Kabel skrośny

	DTE	568B (RJ-45)		568A (RJ-45)	DTE	
1	N+	biało-pomarańczowy	1 ⟶ 3	biało-zielony	N+	1
2	N–	pomarańczowy	2 ⟶ 6	zielony	N–	2
3	O+	biało-zielony	3 ⟶ 1	biało-pomarańczowy	O+	3
4		niebieski	4 ⟶ 4	niebieski		4
5		biało-niebieski	5 ⟶ 5	biało-niebieski		5
6	O–	zielony	6 ⟶ 2	pomarańczowy	O–	6
7		biało-brązowy	7 ⟶ 7	biało-brązowy		7
8		brązowy	8 ⟶ 8	brązowy		8

Kabel skrośny (*null modem cable*) – kabel potrzebny do połączenia dwóch identycznych urządzeń ze sobą

Węzeł dystrybucyjny (*wiring closet*):

- wydzielone miejscem w budynku, które służy do łączenia okablowania przenoszącego dane i głos
- centralny punkt łączący urządzenia sieci LAN w topologii gwiazdy
- ściany wyłożone sklejką o grubości 20mm (w odległości 30mm od ściany) i pokryte farbą ognioodporną
- wyposażenie: panele montażowe (*patch panel*), koncentratory, przełączniki, routery, POP (*Point of Presence*)
- liczba: na każde 1000m^2 powierzchni przypada jeden węzeł dystrybucyjny

Sieć o topologii rozszerzonej gwiazdy wymaga

- głównego węzeła dystrybucyjnego (MDF, *Main Distribution Facility*)
- pośrednich węzłów dystrybucyjnych (IDF, *Intermediate Distribution Facility*)

Zalety okablowania UTP

- łatwość instalacji (korytka, gniazdka i wtyki RJ45, panele montażowe, szafy dystrybucyjne)
- łatwość rozbudowy
- odporność na zakłócenia
- łatwość lokalizowania i usuwania awarii sieci

Zasada 5-4-3-2-1 łączenia urządzeń sieci Ethernet 10Base-T:

1. jest tylko 5 segmentów pomiędzy każdymi dwoma węzłami
2. są tylko 4 wzmacniaki pomiędzy każdymi dwoma węzłami
3. są tylko 3 segmenty, które służą do podłączania węzłów
4. są dwa segmenty, które nie mogą służyć do podłączania węzłów
5. jest jedna domena kolizyjna, w której mogą być co najwyżej 1024 węzły

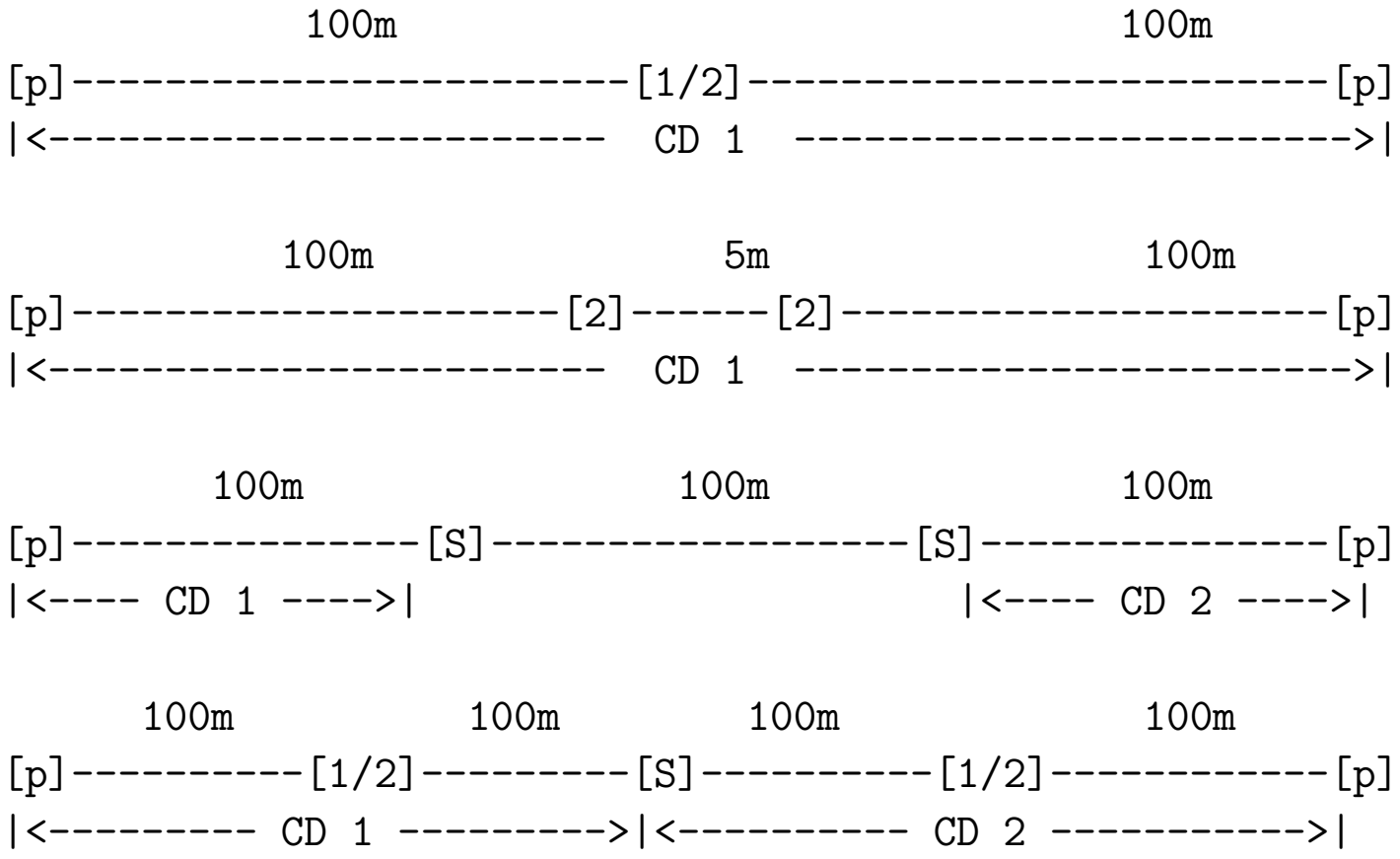
Zasady łączenia urządzeń Fast Ethernet 100Base-TX

Legenda:

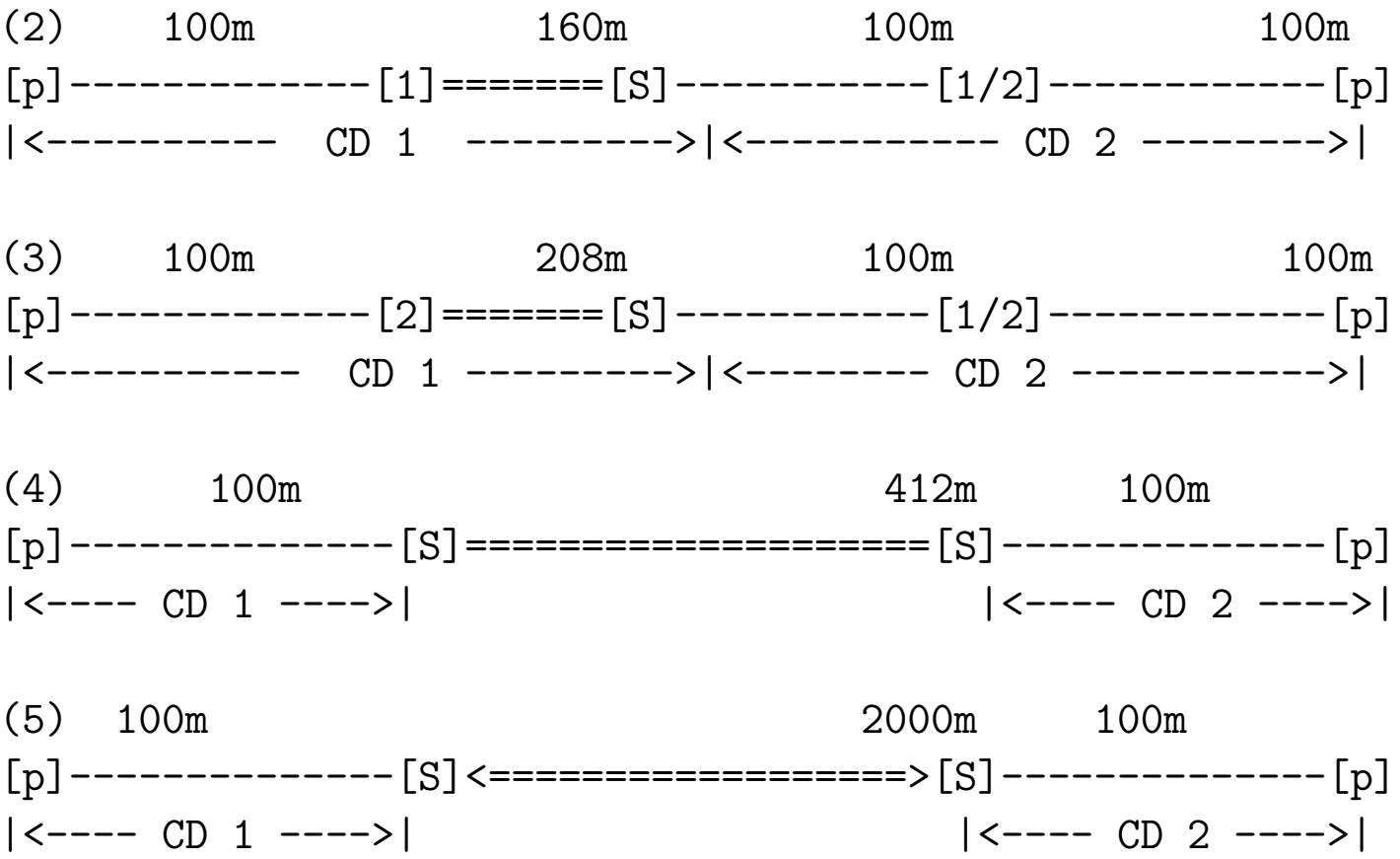
```
[p] : PC; the terminal nodes
[1] : 100 Base-TX Class I Repeater
[2] : 100 Base-TX Class II Repeater
[1/2] : 100 Base-TX Class I or Class II Repeater
[S] : 10 Base-T/100 Base-TX Switch
----- : TX cable (Twisted Pairs cable)
        (Cat. 5 UTP/STP cable for 100 Base-TX,
         Cat. 3, 4, or 5 UTP/STP cable for 10 Base-T.)
===== : FX cable (Half Duplex),
<===> : FX cable (Full Duplex)  Multi-mode Fiber cable (62.5/125)

<- CD ->: Collision Domain
```

Zasady łączenia urządzeń Fast Ethernet 100Base-TX



Zasady łączenia urządzeń 100Base-TX i 100Base-FX



Słownik skrótów

API *Application Programming Interface* interfejs programów użytkowych
ARP *Address Resolution Protokol* protokół odwzorowywania adresów
ASCII *American Standard Code for Information Interchange* standardowy amerykański kod wymiany informacji
ASIC *Application Specific Integrated Circuit* układ scalony właściwy aplikacji
ATM *Asynchronous Transfer Mode* tryb przesyłania asynchronicznego
B8ZS *Bipolar with 8-Zeros Substitution* bipolarna substytucja ośmiozerowa
BECN *Backward Explicit Congestion Notification* jawne powiadomienie o zatorze wysyłane w kierunku nadawcy
bps *bits per second* bity na sekundę
BRA *Base Rate User Access* tryb podstawowy dostępu użytkownika
CHAP *Challenge Handshake Authentication Protocol* protokół wymiany wyzwania uwierzytelniającego (protokół uwierzytelniania przez uzgodnienie)
CIDR *Classless InterDomain Routing* bezklasowy routing międzydomenowy

CIR *Committed Information Rate* zagwarantowany poziom transmisji
CoS *Class Of Service* klasa usługi
CSMA/CD *Carrier Sense-Multiple Access/Collision Detection* wielodostęp z wykrywaniem fali nośnej i wykrywaniem kolizji
CRC *Cyclic Redundancy Check* cykliczna kontrola nadmiarowa
DCE *Data Communications Equipment* urządzenie końcowe łącza teleinformatycznego
DDP *Datagram Delivery Protocol* protolół dostarczania datagramów
DES *Data Encription Standard* standard szyfrowania danych
DHCP *Dynamic Host Configuration Protocol* protokół dynamicznej konfiguracji hosta
DLCI *Data Link Connection Identifier* jednoznaczny identyfikator łącza danych
DNS *Domain Name System* system nazw domenowych
DSAP *Destination Service Access Point* punkt dostępu usługi docelowej
DSH *Digital Sygnal Hierarchy* hierarchia sygnałów cyfrowych (standard ANSI)

DSL *Digital Subscriber Line* cyfrowa linia abonencka
DTE *Data Terminal Equipment* terminal teleinformatyczny
DWDM *Dense Wavelength Division Multiplexing* multipleksacja z gęstym podziałem falowym
EBCDIC *extended binary coded decimal interchange code* rozszerzony kod znakowy
EIA *Electronics Industry Association* Towarzystwo Przemysłu Elektronicznego
FDDI *Fiber Distributed Data Interface* złącze danych w sieciach optycznych o dużych przepustowościach
FCS *Frame Check Sequence* sekwencja kontrolna ramki
FECN *Forward Explicit Congestion Notification* jawne powiadomienie o zatorze wysyłane w kierunku odbiorcy
FR *Frame Relay* przekaz ramek
FTP *File Transfer Protocol* protokół przesyłania plików
Gb *gigabit* gigabit
GB *gigabyte* gigabajt

GNS *Get Nearest Server* uzyskaj dostęp do najbliższego serwera
HDLC *High-level Data Link Control* wysokopoziomowe sterowanie łączem danych
HTML *Hypertext Markup Language* język hipertekstowego znakowania informacji
HTTP *Hypertext Transfer Protocol* protokół przesyłania hipertekstu
IANA *Internet Assigned Numbers Authority* urząd internetowy odpowiedzialny za przydział numerów
ICMP *Internet Message Control Protocol* protokół sterowania wiadomością internetową
IDEA *International Data Encription Algorithm* międzynarodowy algorytm szyfrowania danych
IDF *Intermediate Distribution Facility* pośredni węzeł dystrybucyjny
IEEE *Institute of Electrical and Electronics Engineers* Instytut Inżynierów Elektryków i Elektroników
IGRP *Interior Gateway Routing Protocol*
ILD *Injection Laser Diode* iniekcyjna dioda laserowa

IMAP *Internet Mail Access Protocol* protokół dostępu do poczty internetowej
IP *Internet Protocol* protokół internetowy
IPX *Internetwork Packet eXchange* protokół wymiany pakietów sieci firmy Novell
ISDN *Integrated Services Digital Network* sieć cyfrowa usług zintegrowanych
ISO *International Organization for Standardization* Międzynarodowa Organizacja Normalizacyjna
ISO *International Standards Organization* Organizacja Standardów Międzynarodowych
ISP *Internet Service Provider* dostawca usług internetowych
Kb *kilobit* kilobit
KB *kilobyte* kilobajt
LAN *Local Area Network* lokalna sieć komputerowa
LAPB *Link Access Procedure Balanced* zrównoważona procedura dostępu do łącza

LED *Light Emitting Diode* dioda emitująca światło
LLC *Logical Link Control* sterowanie łączem logicznym
MAC *Media Access Control* sterowanie dostępem do nośnika
MAN *Municipal Area Network* miejska sieć komputerowa
Mb *megabit* megabit
MB *megabyte* megabajt
MD5 *Message Digest 5* skrót wiadomości 5
MDF *Main Distribution Facility* główny węzeł dystrybucyjny
MIB *Management Information Base* baza informacji zarządzania
MIME *Multipurpose Internet Mail Extension* uniwersalne rozszerzenie poczty internetowej
MDI *Media Dependent Interface* interfejs zależny od medium
MDI-X *Media Dependent Interface Cross-over* skrośny interfejs zależny od medium
NCP *NetWare Core Protocol* protokół rdzeniowy systemu Netware
NetBIOS *Network Basic Input/Output System* system podstawowych procedur wejścia/wyjścia

NetBEUI *NetBIOS Extended User Interface* rozszerzony interfejs użytkownika podstawowego systemu wejścia/wyjścia
NEXT *Near-End CrossTalk* poziom przesłuchu zbliżnego
NFS *Network File System* sieciowy system plików
NIC *Network Information Center (1)* sieciowe centrum informacyjne
NIC *Network Interface Card (2)* karta interfejsu sieci
NLSP *NetWare Link Services Protocol* protokół usług łącza danych firmy Netware
NNTP *Network News Transfer Protocol* (protokół przesyłania wiadomości w sieci Internet)
OC *Optical Carrier* system nośników optycznych
OSI *Open Systems Interconnection* otwarte połączenie systemów
OSPF *Open Shortest Path First*
OUI *Organizational Unique Identifier* unikatowy identyfikator organizacji
PAD *Packet Assembler/Disassembler* asembler/disasembler pakietów
PAP *Password Authentication Protocol* protokół uwierzytelniania hasła
PAR *Positive Acknowledgement with Retransmission* pozytywne potwier-

dzenie z retransmisją
PCM *Pulse Coded Modulation* modulacja impulsowa
PDN *Privite Data Networks* cyfrowe sieci publiczne
PLC *PowerLine Communications* komunikacja wykorzystująca linie energetyczne
PLP *Packet Level Protocol* protokół warstwy sieci w stosie protokołów X.25
POP *Post Office Protocol (1)* protokoł urzędu pocztowego
POP *Point of Presence (2)* miejsce przyłączenia (urządzeń sieciowych odbiorcy z urządzeniami komunikacyjnymi firmy telefonicznejobecności)
POTS *Plain Old Telephone Service* tradycyjna telefonia
PPP *Point-to-Point Protocol* protokół transmisji bezpośredniej (protokół dwupunktowy)
PRA *Primary Rate User Access* pierwotny tryb dostępu użytkownika (tryb rozszerzony)
PVC *Permanent Virtual Circuit* stałe łącze wirtualne
QoS *Quality Of Service* jakość usługi

RARP *Reverse Address Resolution Protokol* protokół odwrotnego odwzorowywania adresów
RIP *Routing Information Protocol* protokół informacji routingu
RMON *Remote Monitoring* zdalny nadzór
SAP *Service Advertisment Protocol* protokół rozgłaszania usługi
SMDS *Switched Multimegabit Data Service*
SDH *Synchronous Digital Hierarchy* hierarchia cyfrowych sygnałów synchronicznych (standard ITU)
SDLC *Synchronous Data Link Control*) sterowanie synchronicznym łączem danych
SFD *Start of Frame Delimiter* ogranicznik początku ramki
SMB *Server Message Block Protocol* protokół bloków komunikatów serwera
SMIME *Secure Multipurpose Internet Mail Extension* bezpieczne i uniwersalne rozszerzenie poczty internetowej
SMTP *Simple Mail Transport Protocol* prosty protokół przesyłania poczty
SNA *Systems Network Architecture* architektura sieci systemów

SNAP *Sub-Network Access Protocol* protokół dostępu podsieci
SNMP *Simple Network Management Protocol* prosty protokół zarządzania siecią
SONET *Synchronous Optical NETwork* synchroniczna sieć optyczna
SPX *Sequenced Packet Exchange* protokół sekwencyjnej wymiany pakietów
SSAP *Source Service Access Point* punkt dostępu usługi źródłowej
SSH *Secure SHell* bezpieczna powłoka
STM *Synchronous Transport Module* moduł transportu synchronicznego
STS *Synchronous Transport Signal* system sygnałów transportu synchronicznego
STP *Spanning Tree Protocol (1)* protokół częściowego drzewa
STP *Shielded Twisted Pair (2)* ekranowana skrętka
SVC *Switched Virtual Circuit* komutowany obwód wirtualny
TCP *Transmission Control Protocol* protokół sterowania transmisją
TELNET *Network Terminal Protocol* protokół końcówki sieciowej
TFTP *Trivial File Transfer Protocol* trywialny protokół przesyłania plików
TIA *Telecommunications Industry Association* Towarzystwo Przemysłu Te-

lekomunikacyjnego

TORMAN *Torun Municipal Area Network* toruńska miejska sieć komputerowa

UDP *User Datagram Protocol* protokół datagramów użytkownika

URL *Universal Resource Locator* ujednolicony lokalizator zasobów

UTP *Unshielded Twisted Pair* nieekranowana skrętka

VLAN *Virtual LAN* wirtualna lokalna sieć komputerowa

WAN *Wide Area Network* rozległa sieć komputerowa

WLAN *Wireless Local Area Network* lokalna bezprzewodowa sieć komputerowa

WWW *World Wide Web* światowa pajęczyna