KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

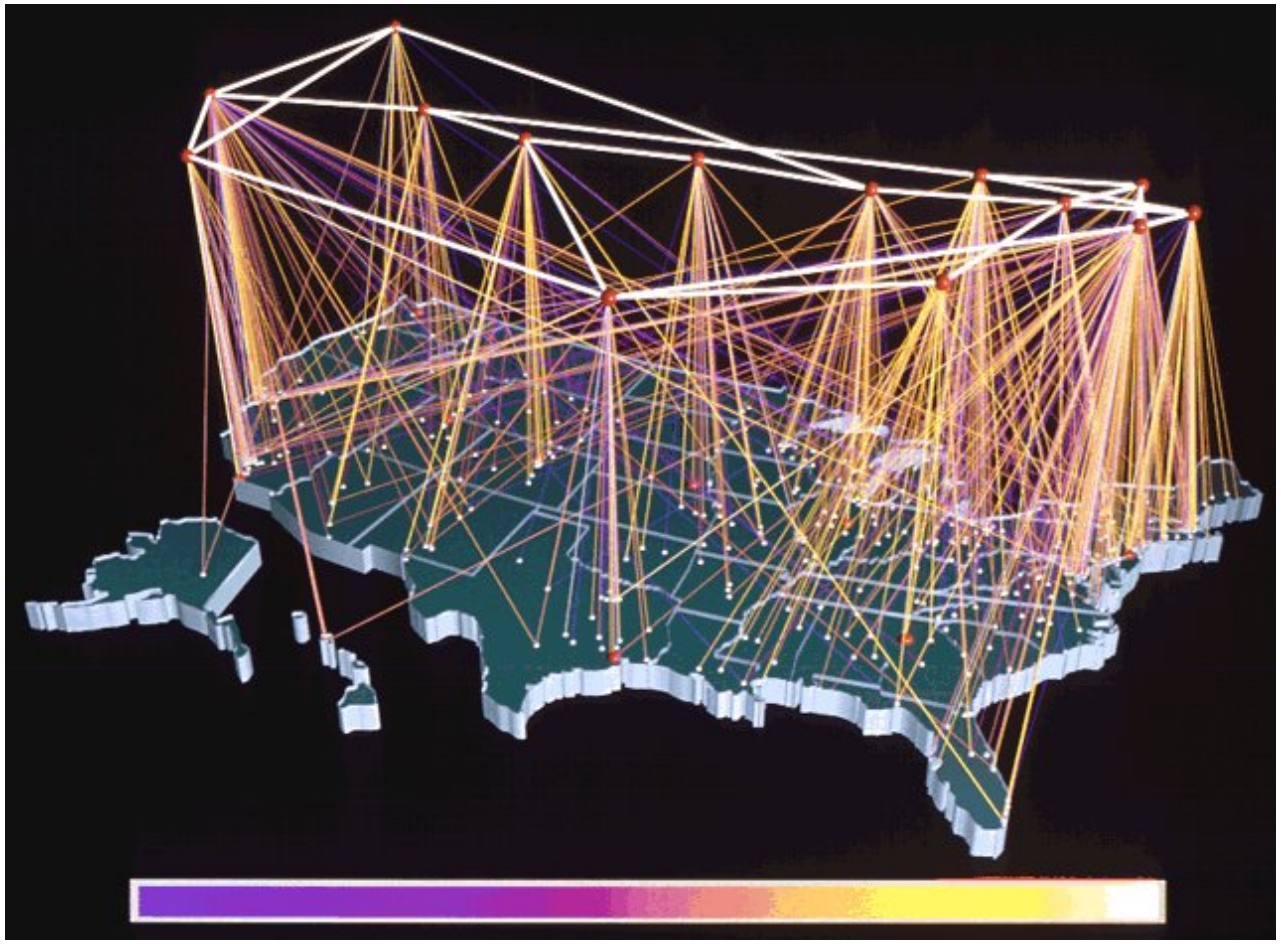
Sieci komputerowe

Jacek Kobus

Wydział Fizyki, Astronomii i Informatyki Stosowanej UMK (2023/2024)

`https://jkob.fizyka.umk.pl/students/notes/notes.html (sk.pdf)`
`git clone ssh://<user>@ameryk.fizyka.umk.pl/git/tm-docs`
`git clone ssh://<user>@ameryk.fizyka.umk.pl/git/tm-scripts`

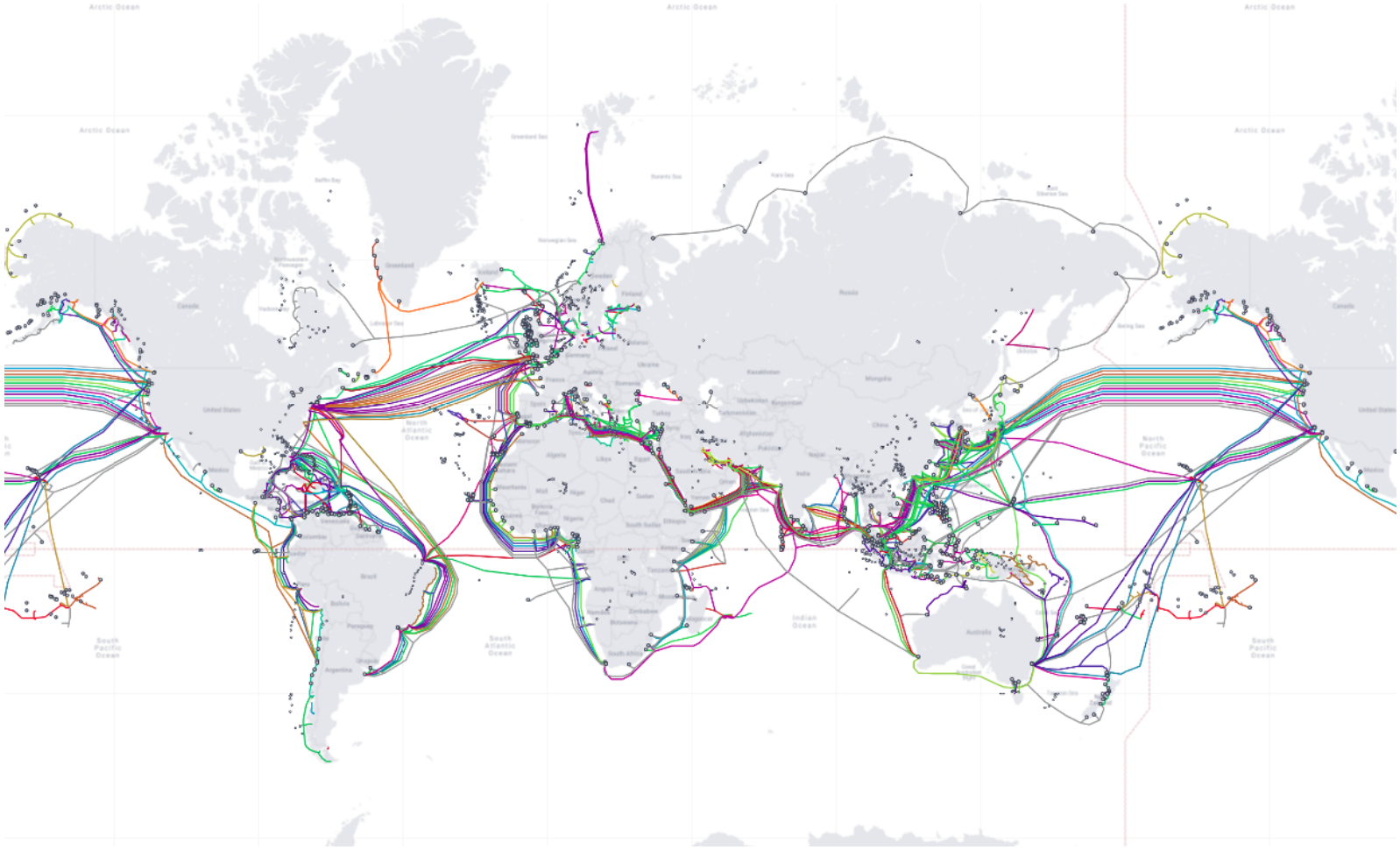
ostatnia aktualizacja: 22-04-2024



NSFNET 9/1991 – traffic visualization

People think that the data is in the cloud, but it's not. It's in the ocean.

Internet cables in oceans



Submarine Cable Map, 02-2022

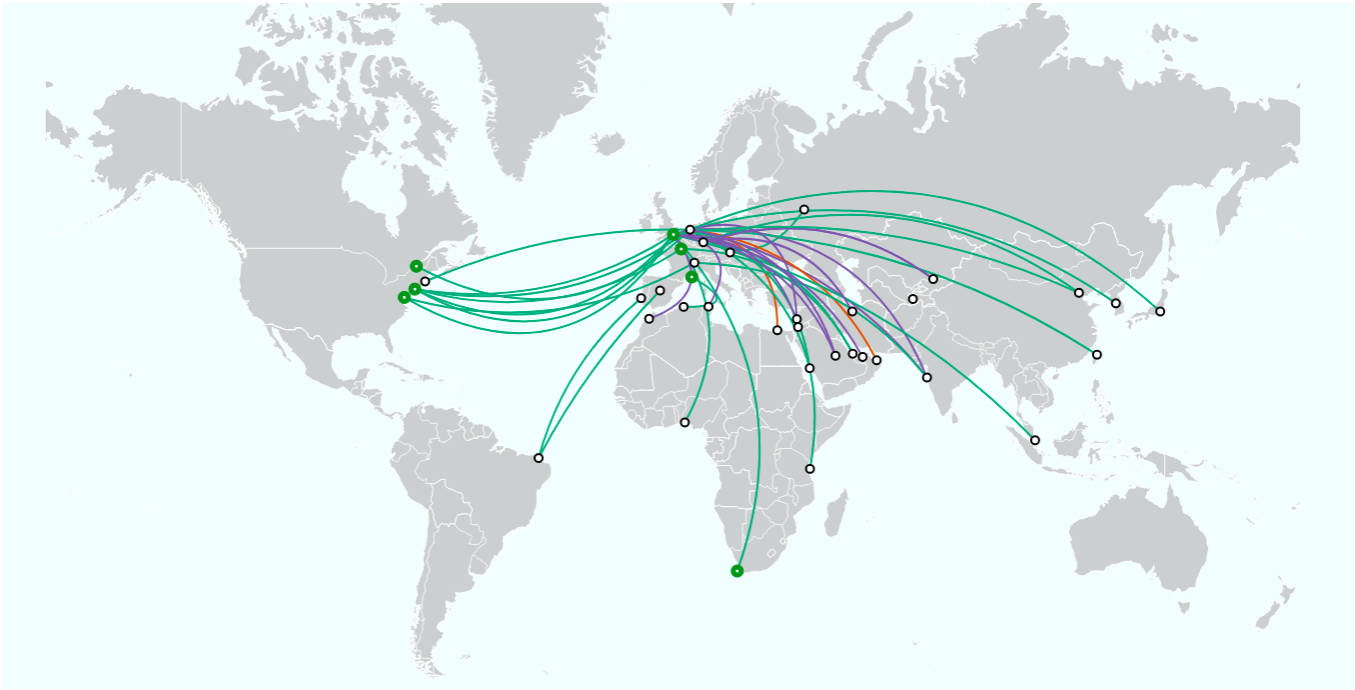
Czy zostaliśmy złapani w Sieć?

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

W jakim stopniu nasze życie zależy od komputerów i sieci komputerowych?

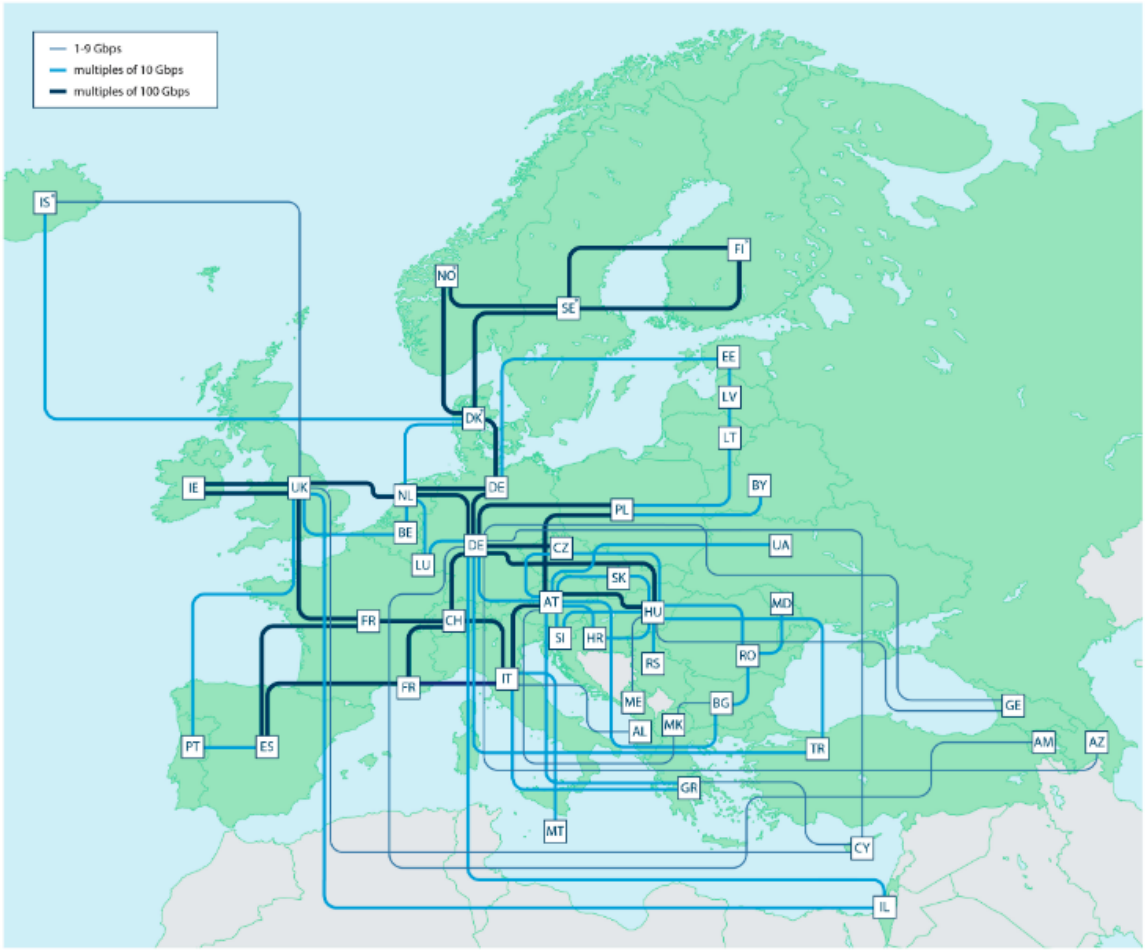
Jak komputery i sieci komputerowe wpływają na funkcjonowanie państw i społeczeństw?

... jednym z niezbitych faktów jest dzisiaj to, że systemy i sieci informatyczne stanowią część „krytycznej infrastruktury" kraju ... kontrolują one tak zwany „żelazny trójkąt" telekomunikacji, bankowości i zasilania w energię elektryczną. (E.Yourdon *Wojny na bity*)



Geant 2022 – połączenia z innymi sieciami

Data carried: 7 PB/d, Backbone capacity: up to 8 Tb/s, Traffic growth: 30% (avg annual over 5 years)



Geant: European Topology Map (Dec 2018)

TORUŃ

Uniwersytet Mikołaja Kopernika

Uniwersyteckie Centrum Informatyczne

Miejska Sieć Komputerowa TORMAN

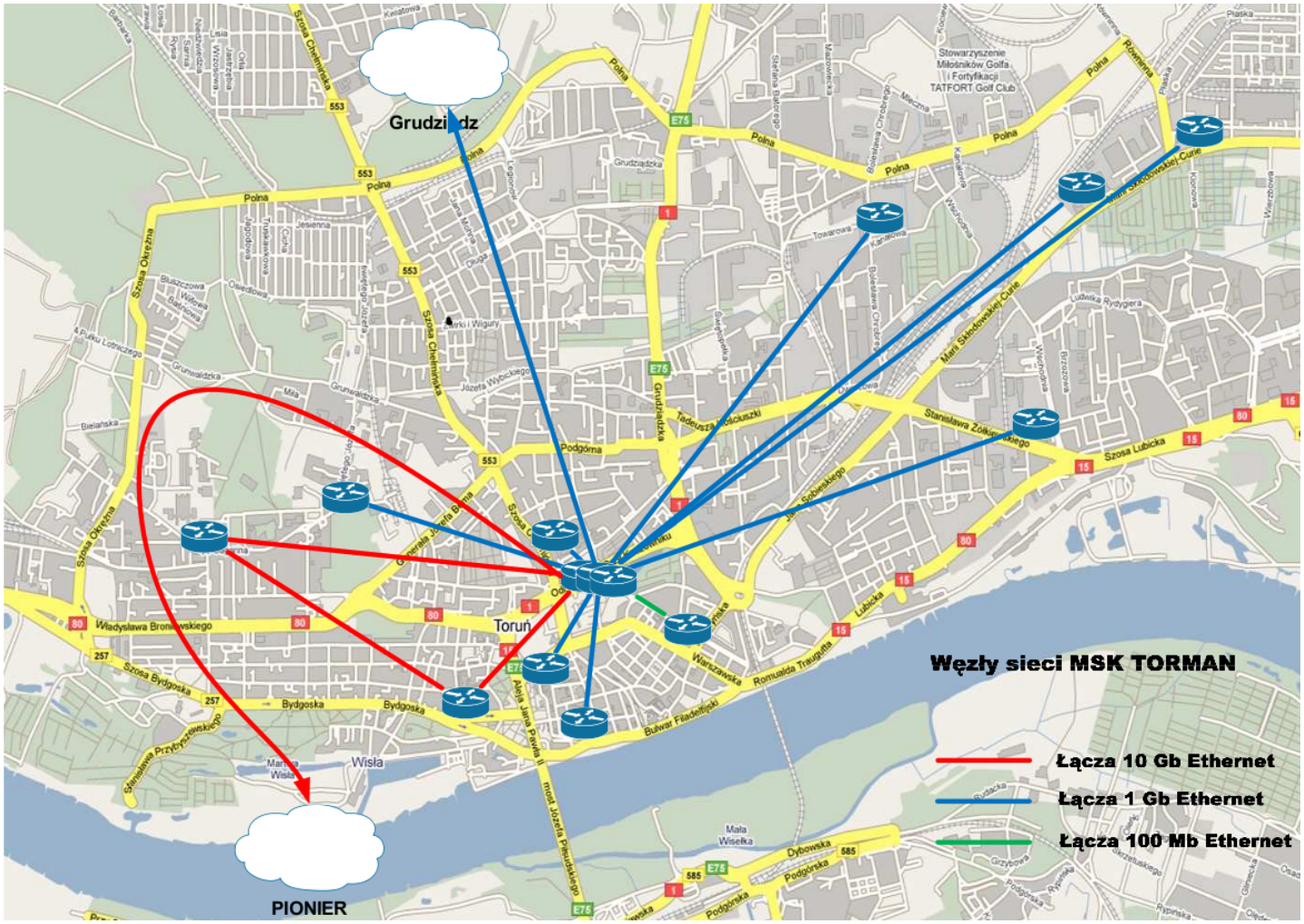
Interfejsy dostępowe:

- **n×10Gb/s**
- **100Gb/s**

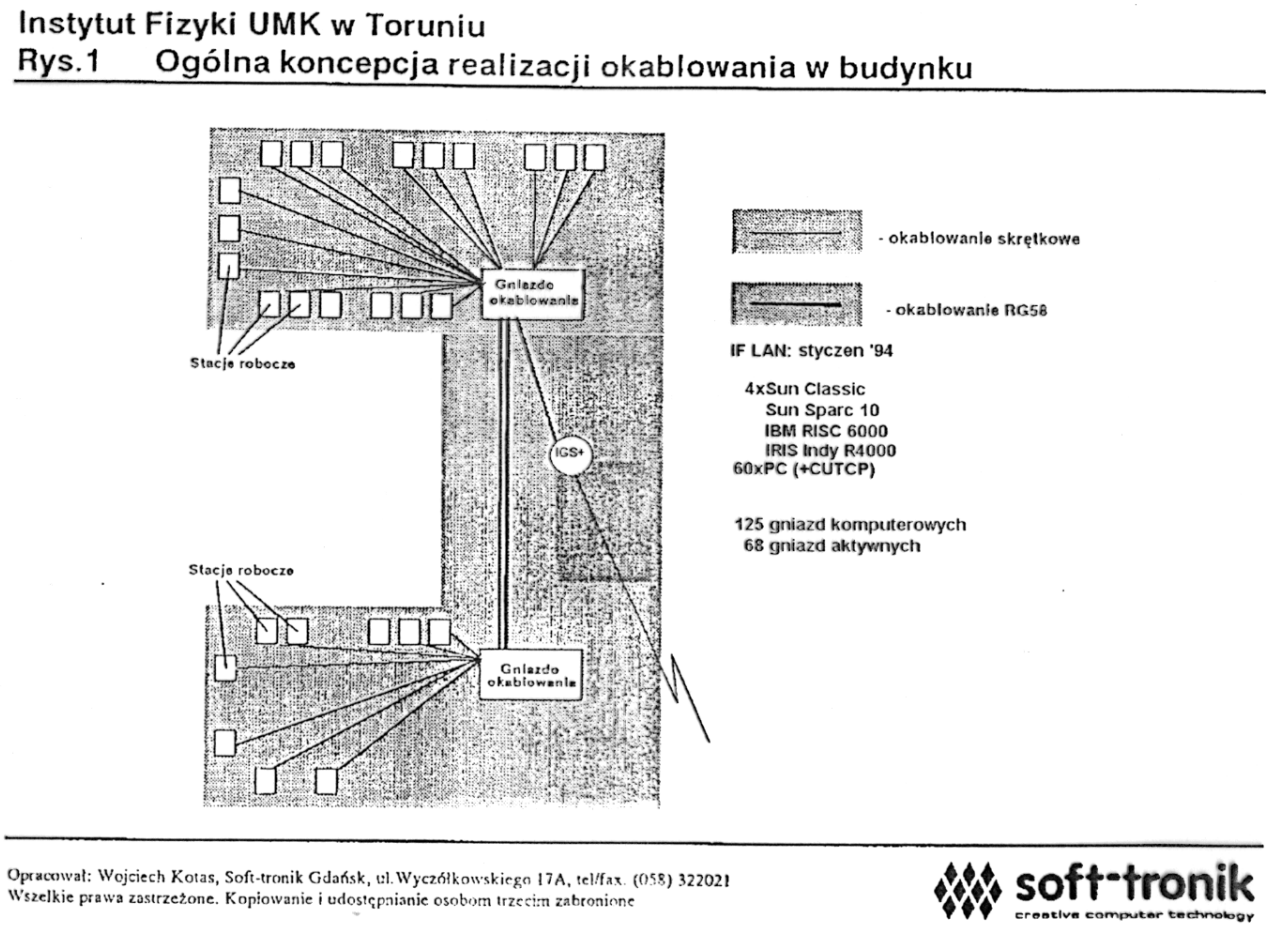
LEGENDA

- Węzeł sieci PIONIER, ośrodek MAN i KDM
- Węzeł sieci PIONIER, ośrodek MAN
- Punkty styku na granicy
- Punkt wymiany ruchu zagranicznego
- Linie światłowodowe sieci PIONIER

Sieć optyczna Pionier (2024)

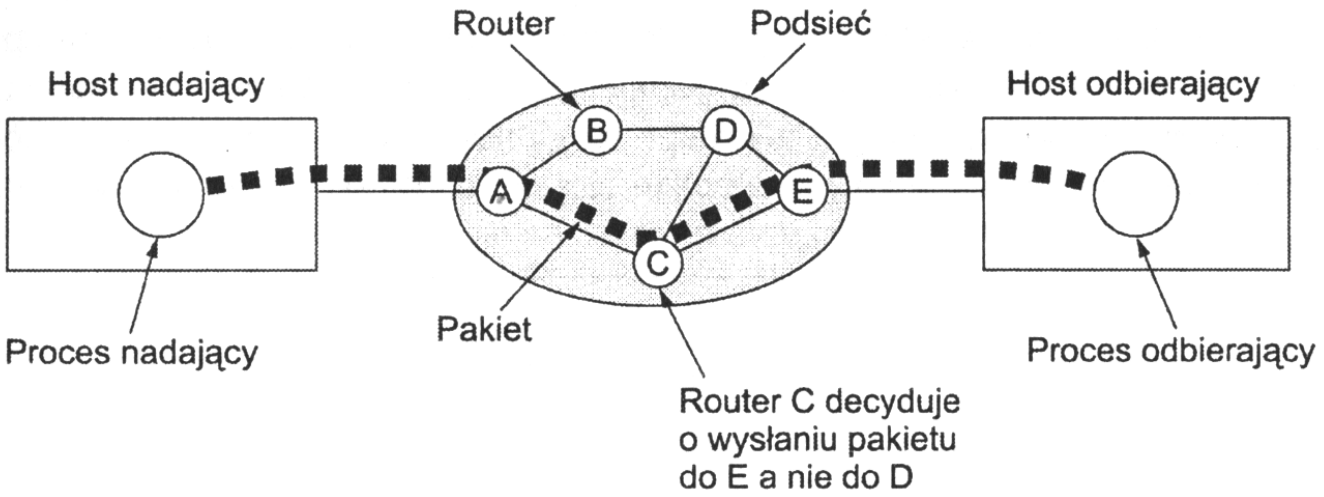


Schemat miejskiej sieci TORMAN, 2009

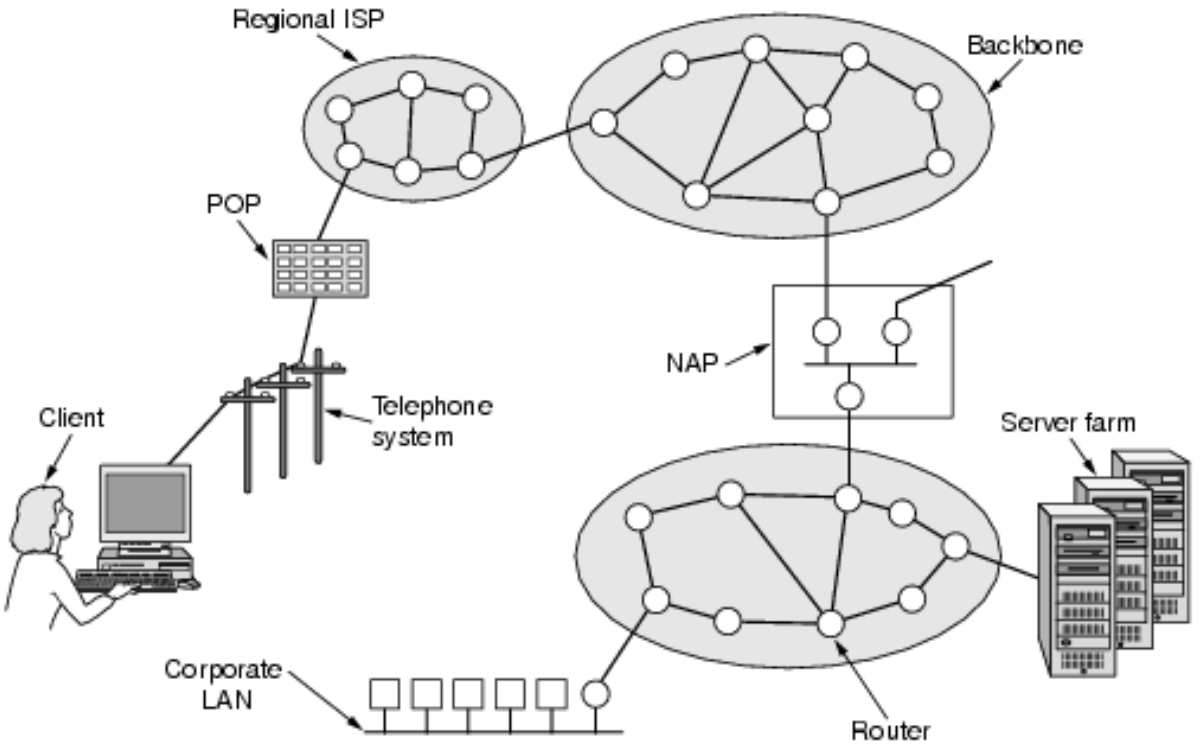


Schemat sieci LAN w budynku Instytutu Fizyki UMK (styczeń 1994)

Internet: komunikacja poprzez wymianę pakietów



Internet: zbiór połączonych sieci



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).

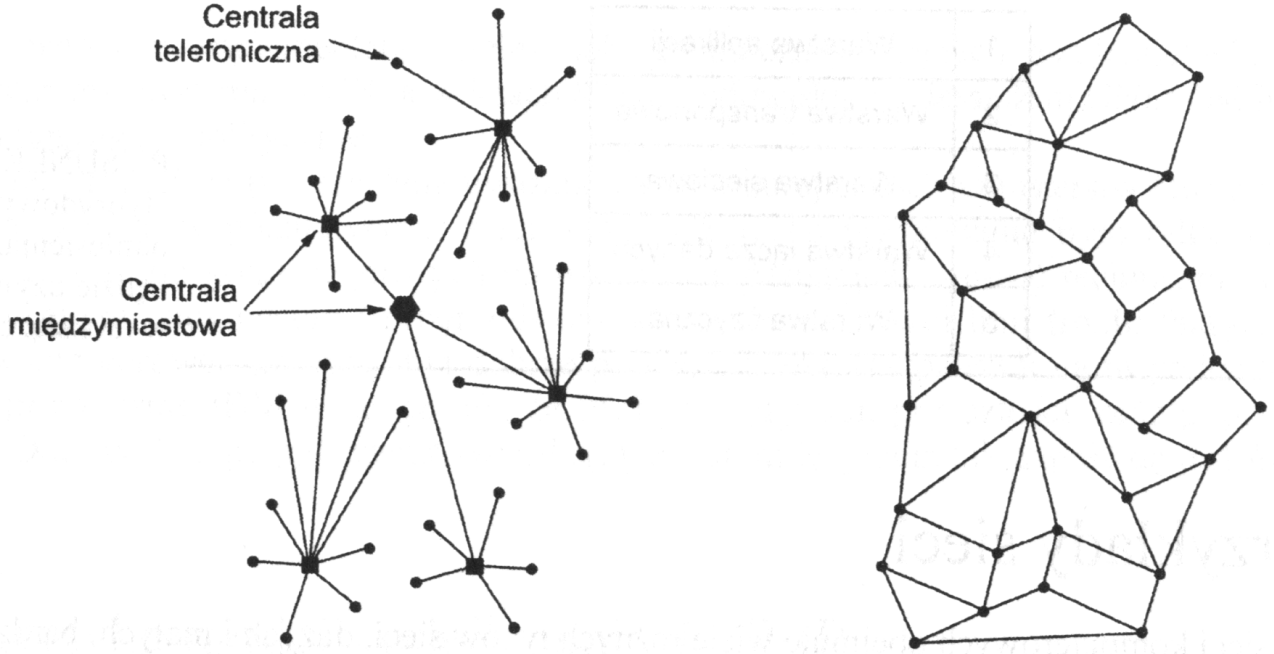
  Urządzenia: komputery, serwery, drukarki sieciowe, koncentratory, mosty, przełączniki, routery.

- **WAN** (*Wide Area Network*) – rozległa sieć komunikacyjna obejmująca swoim zasięgiem duży obszar geograficzny i umożliwiająca LAN-om łączność poprzez komutowane lub stałe łącza. Technologie WAN funkcjonują w warstwach 1-3 modelu OSI.

  Urządzenia: routery, przełączniki, serwery telekomunikacyjne (*dial-up*), modemy, urządzenia CSU/DSU

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).



Krótka historia powstania Internetu

- 1971 – R.Tomlinson tworzy pierwszy 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; wdrożenie TCP/IP w systemie operacyjnym UNIX BSD; ARPANET staje się siecią TCP/IP

Krótka historia powstania Internetu

- 1983 – ARPANET rozpada się na sieć MILNET oraz ARPANET
  Termin **Internet**[1] służył do określenia obu tych sieci.
  Internet = Sieć
- 1983 – powstaje EARN (*European Academic and Research Network*)
- 1984 – wprowadzenie usługi DNS (*Domain Name System*); w sieci około 1000 serwerów
- 1986 – powstaje NSFNET (*National 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 – NSFNET przekształca się w sieć badawczą, Internet się komercjalizuje; *wojna* przeglądarek (Netscape Navigator kontra Internet Explorer)

[1] Termin *internet* pojawił się w RFC 675 z 1974 r.

ARPANET, 1973

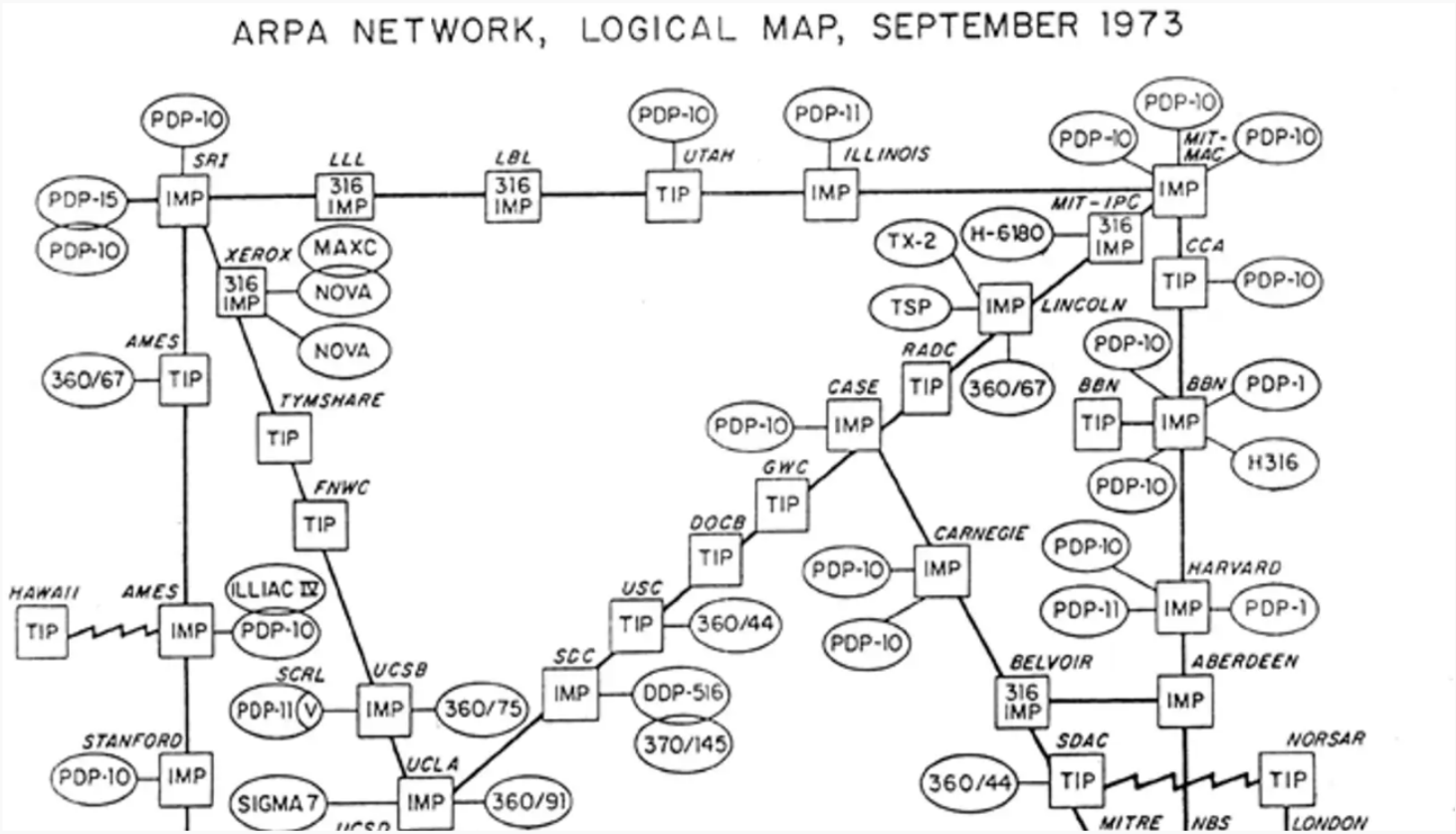


Image: ARPA/ARPAnet Completion Report

Back in the days.

ARPANET, 1973

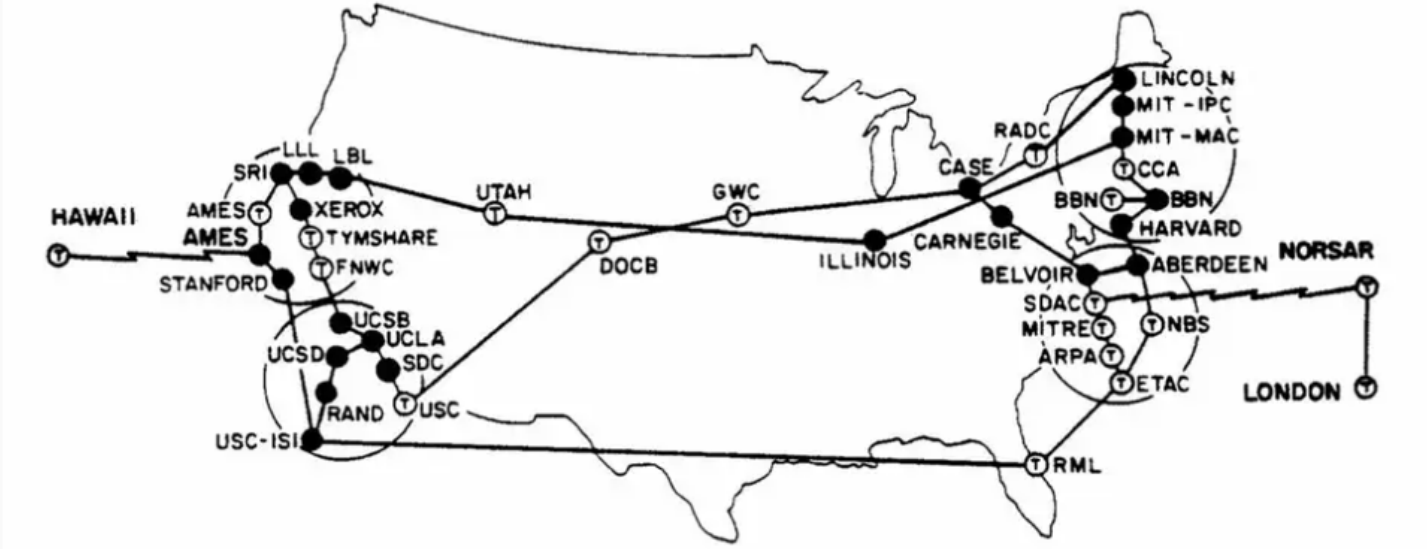


Image: ARPA/ARPAnet Completion Report

ARPANET Geographic Map, September 1973.

Historia Internetu w liczbach

	# komputerów	# serwerów www
7-2001	126×10^6	28.2×10^6
7-1998	37×10^6	4.27×10^6
7-1997	19.54×10^6	1.2×10^6
7-1996	12.88×10^6	3×10^5
7-1995	6.64×10^6	25×10^3
7-1994	3.21×10^6	3×10^3
7-1993	1.78×10^6	1.5×10^2
7-1992	99×10^5	5×10^1
7-1989	1.3×10^5	
7-1981	2.1×10^2	
5-1973	4.2×10^1	
1969	4×10^0	

Pierwsza strona WWW

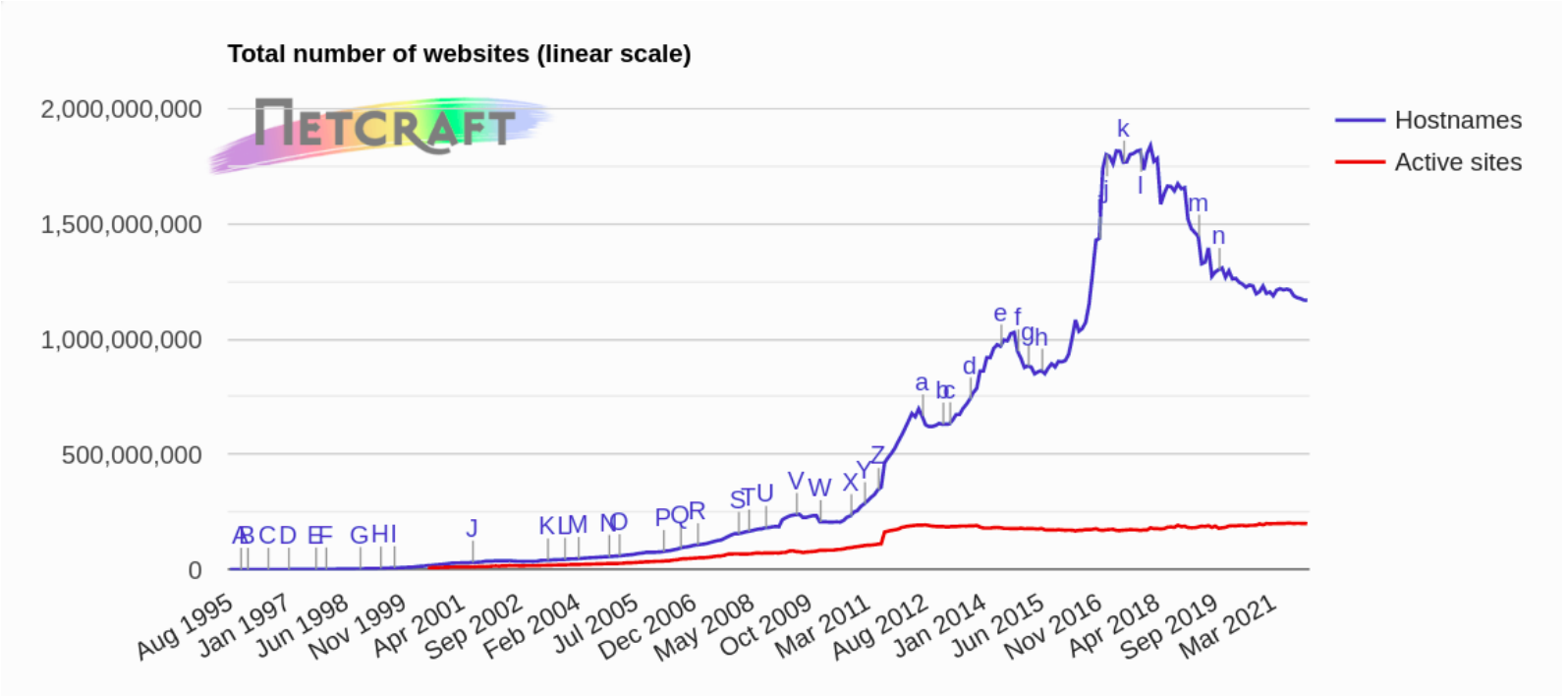
World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

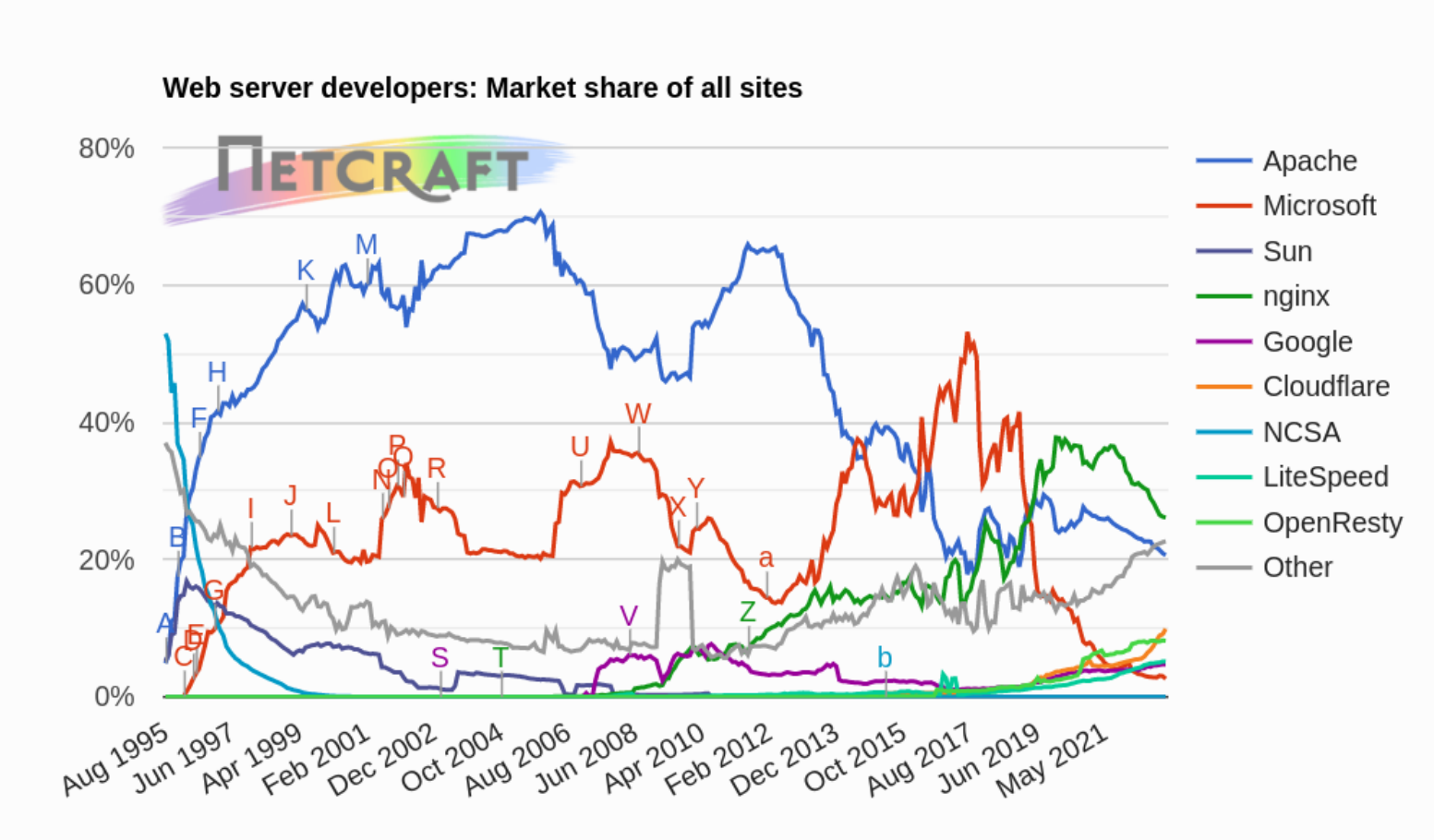
Całkowita liczba stron WWW (websites)[2]



In the January 2022 survey we received responses from 1,167,715,133 sites across 269,835,071 unique domains and 11,700,892 web-facing computers. This reflects a loss of 1.15 million sites, but a gain of 1.51 million domains and 31,100 computers.

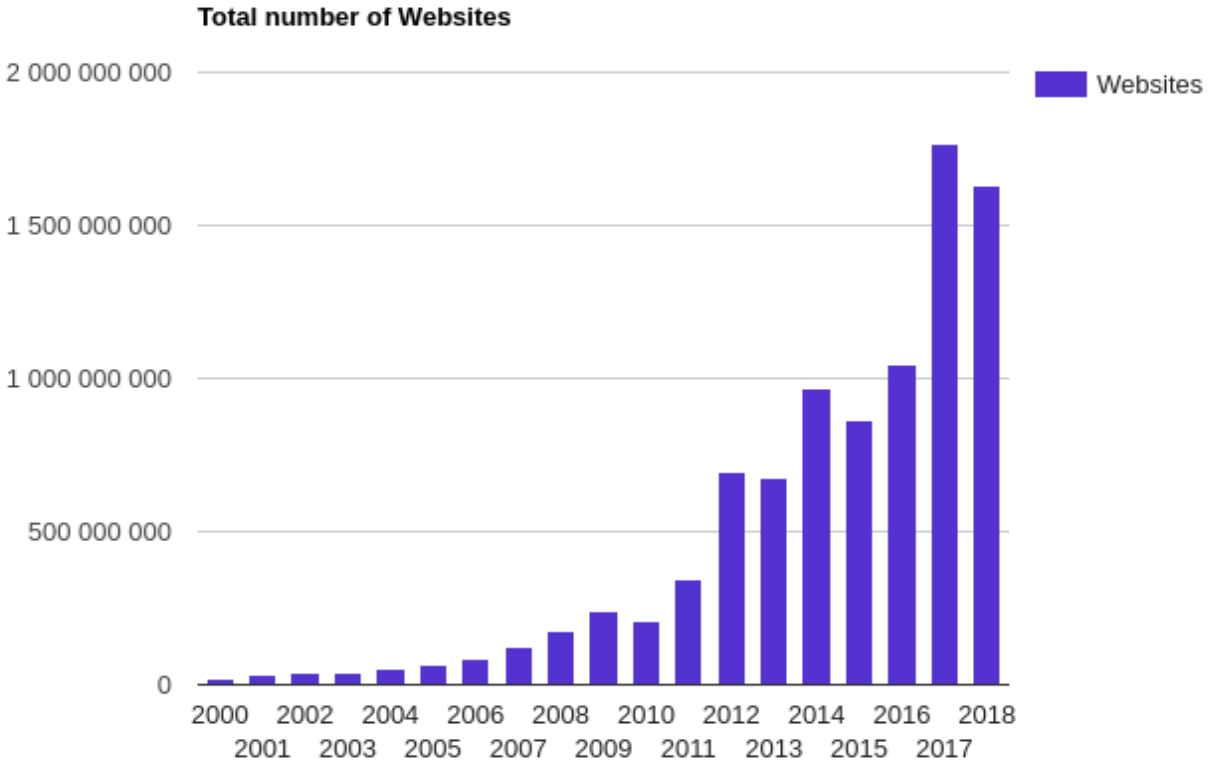
[2] https://news.netcraft.com/

Jakiego oprogramowania używają sewery WWW?[3]



[3] https://news.netcraft.com/

Jak szybko przybywa stron WWW (websites)?[4]



[4] *Website* oznacza unikatową nazwę hosta, której odpowiada określony przez DNS adres IP. Zob. internet live stats/.

Jak szybko przybywa stron WWW?[5]

Year (June)	Websites	Change	Internet Users	Users per Website	Websites launched
2018	**1,630,322,579**	-8%			
2017	**1,766,926,408**	69%			
2016	**1,045,534,808**	21%			
2015	**863,105,652**	-11%	3,185,996,155*	3.7	
2014	**968,882,453**	44%	2,925,249,355	3.0	
2013	**672,985,183**	-3%	2,756,198,420	4.1	
2012	**697,089,489**	101%	2,518,453,530	3.6	
2011	**346,004,403**	67%	2,282,955,130	6.6	
2010	**206,956,723**	-13%	2,045,865,660	9.9	Pinterest, Instagram
2009	**238,027,855**	38%	1,766,206,240	7.4	
2008	**172,338,726**	41%	1,571,601,630	9.1	Dropbox
2007	**121,892,559**	43%	1,373,327,790	11.3	Tumblr
2006	**85,507,314**	32%	1,160,335,280	13.6	Twttr
2005	**64,780,617**	26%	1,027,580,990	16	YouTube, Reddit
2004	**51,611,646**	26%	910,060,180	18	Thefacebook, Flickr
2003	**40,912,332**	6%	778,555,680	19	WordPress, LinkedIn
2002	**38,760,373**	32%	662,663,600	17	
2001	**29,254,370**	71%	500,609,240	17	Wikipedia
2000	**17,087,182**	438%	413,425,190	24	Baidu

[5] Total number of websites

Internet AD 2020[6]

- 4.484 mld– liczba użytkowników
- 109.6 mld – liczba wysyłanych listów dziennie
- 2.96 mld – liczba kwerend wysyłanch do wyszukiwarki Goggle'a dziennie (80.9 tys./s)
- 2.8 mln – liczna postów tworzonych dziennie
- 326 mln – liczba tweetów tworzonych dziennie (8.86/s)
- 3.05 mld – liczba wideo odtwarzanych dziennie (YouTube, 35.3 tys./s)
- 35.9 mln – liczba zdjęć umieszczanych dziennie (Instagram, 973/s)
- 2.435 mld – liczba aktywnych użytkowników Facebooka
- 795 mln – liczba aktywnych użytkowników Google'a
- 357 mln – liczba aktywnych użytkowników Twittera

[6] https://www.internetlivestats.com

Internet AD 2020

- 165 mln – liczba połączeń Skype'a dziennie (4.45 tys./s)
- 63.3 tys. – liczba przejętych przez hackerów stron WWW
- 3.258 EB – dzienna wielkość ruchu w Internecie (87.7 GB/s)
- 1.78 mln MWh – dzienne zużycie prądu na potrzeby Internetu
- 1.6 mln ton – dzienna emisja CO_2 przez użytkowników Internetu

Internet AD 2017

- 1.8 mld – liczba aktywnych użytkowników Facebooka
- 300 mln – liczba aktywnych użytkowników Twittera
- 59 tys./s – liczba kwerend kierowanych do wyszukiwarki Google
- 7.2 tys./s – liczba tweetów
- 2.5 tys./s – liczba rozmów via Skype
- 770/s – liczba zdjęć ładowanych (Instagram)
- 68 tys./s – liczba filmów oglądanych na platformie YouTube

Cel wykładu

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

Program wykładu

1. Wprowadzenie
2. Architektura protokołów sieciowych: model odniesienia OSI i TCP/IP
3. Protokoły modelu TCP/IP
   (a) IPv4 (adresacja, sieci/podsieci), ARP/RARP, ICMP, IPv6
   (b) TCP, UDP, SCTP; interfejs gniazd, dobrze znane usługi
   (c) FTP (aktywny/pasywny), HTTP, SSH, DHCP, DNS, NFS, etc
   (d) Porównanie modelu odniesienia OSI i TCP/IP
4. Protokoły modelu Netware oraz AppleTalk. NetBIOS/NetBEUI
5. Lokalne sieci komputerowe
   (a) Ethernet, Token Ring, Wi-Fi, PLC
   (b) media transmisyjne
   (c) urządzenia sieciowe: koncentratory, mosty, przełączniki, routery
   (d) sieci wirtualne
   (e) konfiguracja i stan interfejsów sieciowych
   (f) okablowanie strukturalne (standardy EIA/TIA-568B)

6. Monitorowanie połączeń i usług, analiza ruchu sieciowego
7. Rozległa sieć komputerowa
   (a) technologie, standardy sygnałów cyfrowych, modemy (linie analogowe i cyfrowe), modemy kablowe
   (b) protokoły warstwy łącza danych (HDLC, PPP)
   (c) obwody datagramowe i wirtualne
   (d) protokoły obsługi obwodów wirtualnych (ISDN, X.25, Frame Relay)
8. Problemy routingu/trasowania
   (a) algorytm wektora odległości (RIP)
   (b) algorytm stanu łącza (OSPF)
   (c) routing hierarchiczny (AS, BGP)
   (d) routing dla hostów mobilnych, routing w sieciach ad hoc
   (e) sieci złożone (tunelowanie), sieci skalowalne

Literatura

[1] V. Amato, editor. *Akademia Sieci Cisco. Pierwszy rok nauki*. Wydawnictwo MIKOM, Warszawa, 2001.

[2] V. Amato, editor. *Akademia Sieci Cisco. Drugi rok nauki*. Wydawnictwo MIKOM, Warszawa, 2001.

[3] Iljitsch van Beijnum. *Running IPv6*. Apress, 2006.

[4] J. Glenn Brookshear and Denis Brylow. *Informatyka w ogólnym zarysie*. Wydawnictwo Naukowe PWN, Warszawa, 2022.

[5] D. E. Comer. *Sieci komputerowe TCP/IP*. Wydawnictwo Naukowo-Techniczne, Warszawa, 1999.

[6] D. E. Comer. *Sieci komputerowe i intersieci*. Wydawnictwo Naukowo-Techniczne, Warszawa, 2000.

[7] F. J. Derfler. *Poznaj sieci*. Wydawnictwo Mikom, Warszawa, 1999.

[8] C. Hunt. *TCP/IP – Administracja sieci*. Wydawnictwo READ ME, Warszawa, 1996.

[9] Charles M. Kozierok. *The TCP/IP Guide*. http://www.tcpipguide.com/.

[10] M. McGregor. *Akademia Sieci Cisco. Piąty semestr*. Wydawnictwo MIKOM, Warszawa, 2002.

[11] B. Pfaffenberger. *Słownik terminów komputerowych*. Prószyński i S-ka, Warszawa, 1999.

[12] *Requests For Comments*. http://www.freesoft.org/CIE/RFC/index.htm.

[13] *The Shaldon's Linktionary*. http://www.linktionary.com.

[14] A. Silberschatz i P. B. Galvin. *Podstawy systemów operacyjnych*. Wydawnictwo Naukowo-Techniczne, wyd.5, Warszawa, 2002.

[15] M. Sportack. *Sieci komputerowe - Księga eksperta*. Wydawnictwo Helion, Gliwice, 1999.

[16] A. S. Tanenbaum. *Sieci komputerowe*. Wydawnictwo Helion, Gliwice, 2004.

[17] A. S. Tanenbaum. *Computer Networks*. Prentice Hall PTR, http://authors.phptr.com/tanenbaumcn4/, 2002.

[18] E. Yourdon. *Wojny na bity*. Wydawnictwo Naukowo-Techniczne, Warszawa, 2004.

Protokoły komunikacyjne/sieciowe

Wg słownika języka polskiego protokół to:

- pisemne sprawozdanie z obrad, posiedzenia, sesji, zebrania zawierające streszczenie przemówień, wniosków i uchwał (*protokół posiedzenia*)
- akt sporządzony przez urzędnika zawierający spis dokonanych przez niego czynności i stwierdzonych faktów (*protokół powypadkowy, zdawczo-odbiorczy*)

Protokół dyplomatyczny: ogół prawideł i zasad postępowania i zachowania się przyjęty w stosunkach międzynarodowych; ceremoniał dyplomatyczny.

Protokół komunikacyjny/sieciowy: system formatów wiadomości cyfrowych i reguł ich wymiany w systemach komputerowych i telekomunikacyjnych oraz między nimi.

Protokoły te stwarzają możliwość budowy heterogenicznych sieci komputerowych, w których hosty mogą ze sobą współpracować niezależnie od swojej architektury oraz używanego systemu operacyjnego.

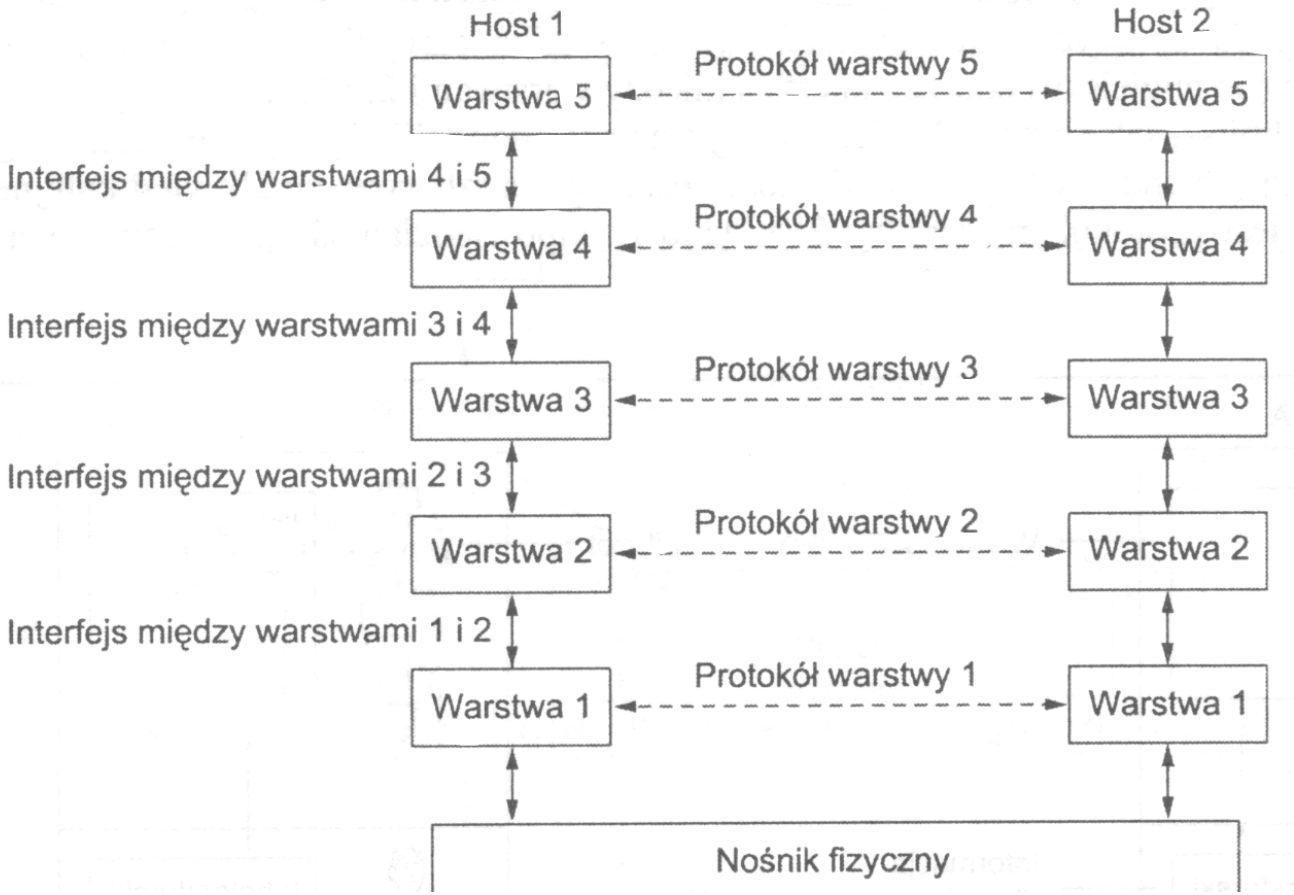
Rodziny protokołów komunikacyjnych

- TCP/IP: BOOTP, DHCP, HTTP, FTP, TFTP, IMAP, POP, NNTP, NTP, SMTP, SNMP, RMON, **TCP, UDP, SCTP, ICMP, IPv4, IPv6, IP NAT**, IP Sec, **RIP, OSPF, EGP, BGP, MPLS, ARP, RARP, PPP**, SLIP
- Security/VPN
  - AAA (Authentication, Authorization, Accounting): Kerberos, RADIUS, SSH
  - Tunneling: L2TP, PPTP, OpenVPN
  - Secured Routing: DiffServ, GRE, IPsec, IKE, AH, ESP, TLS
- Mobile/Wireless: GPRS, CDMA, GSM, LTE (UMTS)
- VOIP/IPTV
  - Signalling: H.323, H.225, H.235, H.245
  - Codec: G.7xx, H.261, H.263, H.264/MPEG-4

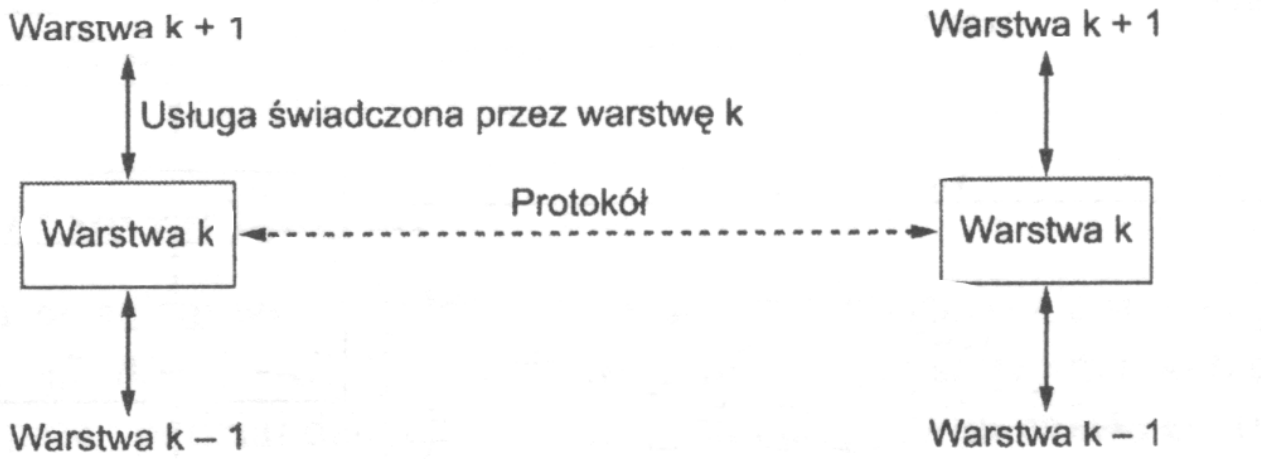
Rodziny protokołów komunikacyjnych

- LAN:
  - Ethernet: IEEE 802.3 suite
  - Wireless LAN: IEEE 802.11a/b/g/n, Bluetooth, IEEE 802.15, IEEE 802.11i, IEEE 802.1X
  - VLAN: IEEE 802.1Q, GARP, GMRP, GVRP, VTP
- WAN: ATM, SONET/SDH, Frame Relay, PPP, X.25
- SS7/C7: BISUP, DUP, ISUP, MAP, MTP, TUP
- Apple – AppleTalk: AFP, PAP, ATP, NBP, DDP, EtherTalk, TokenTalk
- IBM – SNA: SMB, NetBIOS, NetBEUI
- Microsoft: CIFS, SOAP
- Novell – Netware: IPX, SPX, NCP
- Sun: NFS, RPC

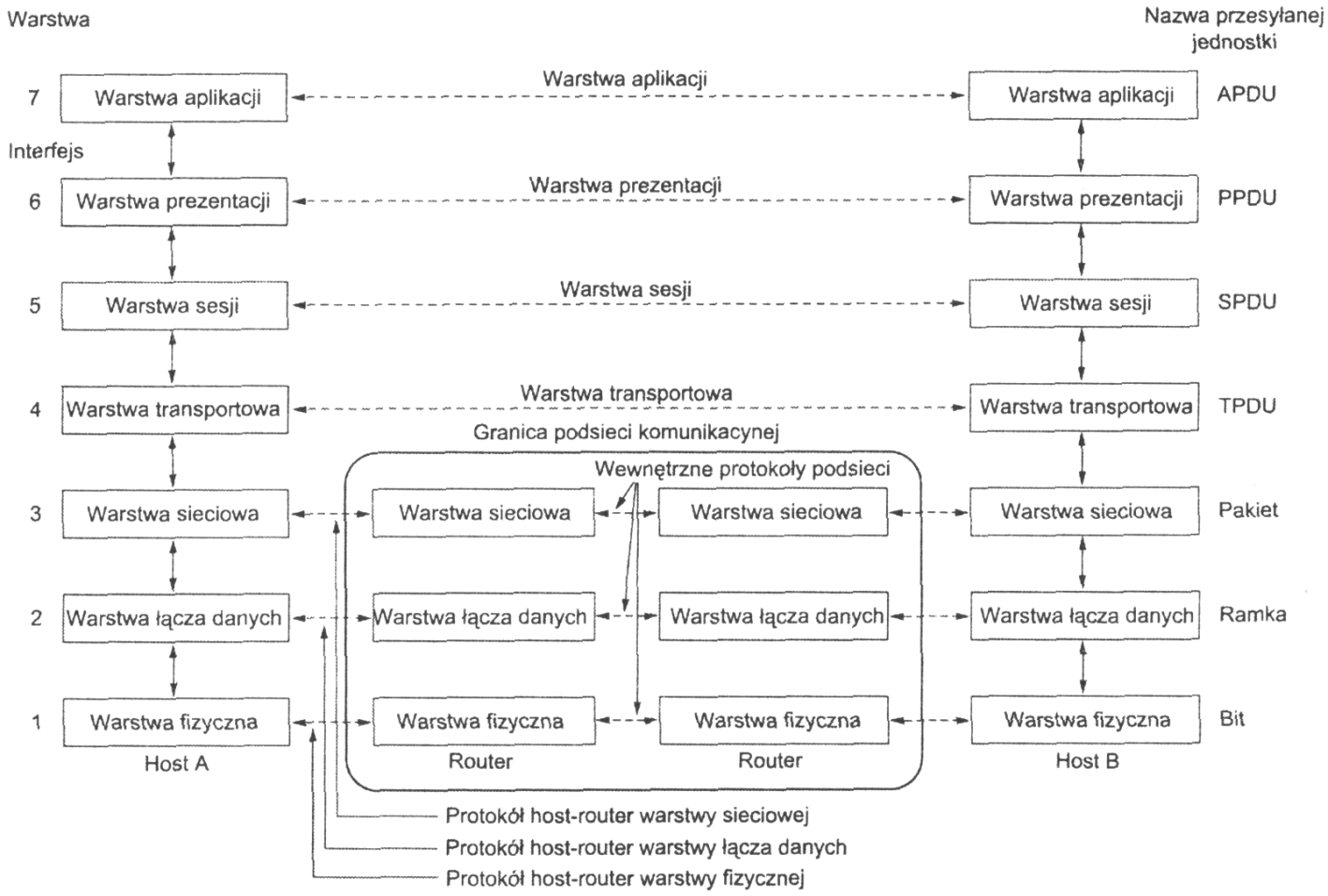
Model warstwowy sieci



Związek między usługą i protokołem



Model odniesienia OSI



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 (w-wy 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, SCTP)

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

łącza danych (*data link layer*) – zapewnia niezawodne dostarczanie danych przez znajdującą się poniżej fizyczną sieć (MAC/LLC, PPP, ATM, Frame Relay, HDLC, 802.1q, 802.3, 802.11a/b/g/n MAC/LLC)

fizyczna (*physical layer*) – umożliwia przesyłanie poszczególnych bitów (ramek) przez dane fizyczne łącze, kontroluje przepływ bitów, powiadamia o błędach (RS232C, V.35, RJ45, 802.11 a/b/g/n PHY, 10BASE-T, 100BASE-TX, 1000BASE-T, T1, E1, SONET, SDH, DWDM)

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

Specyfikacja modelu OSI (*Open System Interconnection) Reference Model*), tj. modelu odniesienia łączenia systemów otwartych, została ogłoszona w 1984 przez Międzynarodową Organizację Normalizacyjną (ISO, *International Organization for Standardization*).

Protokoły sieciowe: TCP/IP

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

Specyfikacje protokołów TCP/IP są opracowywane przez grupy specjalistów skupionych w IETF (*The Internet Engineering Task Force*) i dostępne via dokumenty RFC (*Request For Calls*); zob. IETF.

David D. Clark (główny architekt TCP/IP w latach 1981-89):

We reject presidents, kings and voting, we believe in rough consensus and running code.

Model OSI versus TCP/IP

model OSI	model TCP/IP
warstwa aplikacji (7) warstwa prezentacji (6) warstwa sesji (5)	(4) warstwa aplikacji
warstwa transportowa (4)	(3) warstwa transportowa
warstwa sieciowa (3)	(2) warstwa internetowa
warstwa łącza danych (2) warstwa fizyczna (1)	(1) warstwa dostępu do sieci (host-sieć) wg AT *wielkie nic*

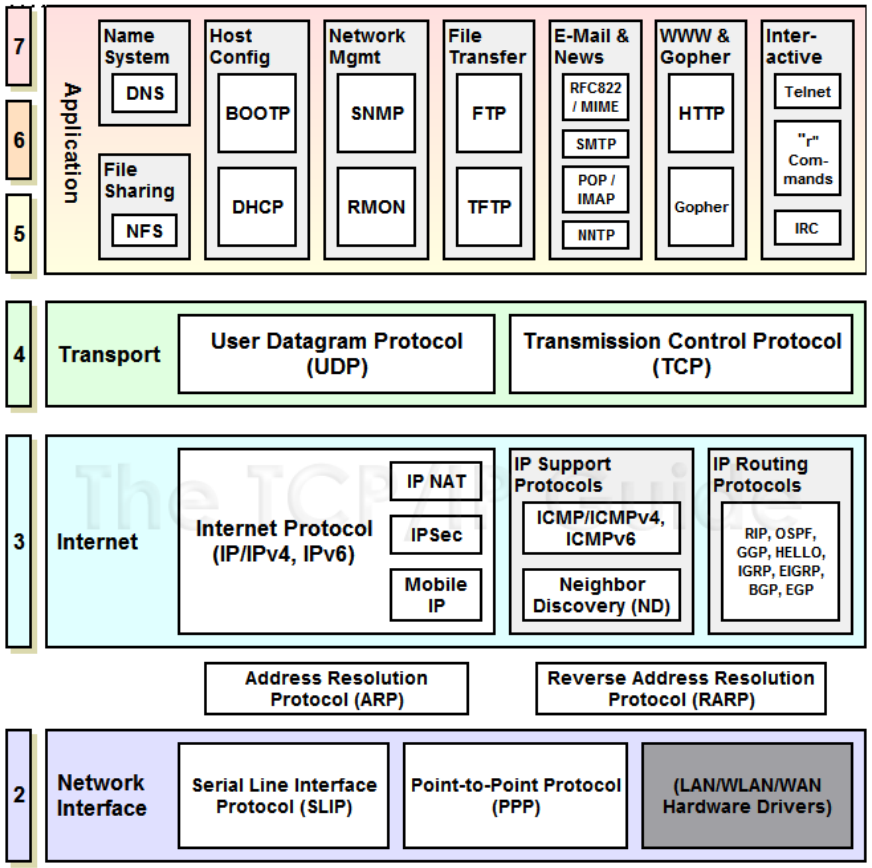
Model TCP/IP bywa przedstawiany jako model 5-cio warstwowy z warstwą dostępu do sieci rozbitą na warstwę łącza danych i fizyczną.

Warstwy OSI i rodziny protokołów[7]

Layer		Misc. examples	TCP/IP suite	SS7	AppleTalk suite	OSI suite	IPX suite	SNA	UMTS
#	Name								
7	Application	HL7, Modbus, CDP	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, DHCP, SMPP, SMTP, SNMP, Telnet,	ISUP, INAP, MAP, TUP, TCAP,	AFP, ZIP, RTMP, NBP	FTAM, X.400, X.500, DAP	RIP, SAP	APPC	
6	Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG	MIME, XDR, SSL, TLS (Not a separate layer)		AFP	ISO 8823, X.226			
5	Session	Named Pipes, NetBIOS, SAP, SDP	Sockets. Session establishment in TCP. SIP. (Not a separate layer with standardized API.)		ASP, ADSP, PAP	ISO 8327, X.225	NWLink	DLC?	
4	Transport	NBF, nanoTCP, nanoUDP	TCP, UDP, IPsec, PPTP, L2TP	SCTP, SCCP, RTP	DDP	TP0, TP1, TP2, TP3, TP4	SPX		
3	Network	NBF, Q.931	IP, ARP, ICMP, RIP, OSPF, BGP, IGMP, IS-IS	MTP-3	ATP (TokenTalk or EtherTalk)	X.25 (PLP), CLNP	IPX		RRC (Radio Resource Control) PDCP (Packet Data Convergence Protocol) and Broadcast/Multicast Control (BMC)
2	Data Link	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, HDP, FDDI, Fibre Channel, Frame Relay, HDLC, ISL, PPP, Q.921, Token Ring	PPP, SLIP	MTP-2	LocalTalk,AppleTalk Remote Access, PPP	X.25 (LAPB), Token Bus	IEEE 802.3 framing, Ethernet II framing	SDLC	LLC (Logical Link Control), MAC (Media Access Control)
1	Physical	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, DSL, 802.11a/b/g/n PHY		MTP-1	RS-232, RS-422, STP, PhoneNet	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)		Twinax	UMTS L1 (UMTS Physical Layer)

[7] OSI model. Layer 1: Physical layer

Warstwy TCP/IP i ich protokoły[8]

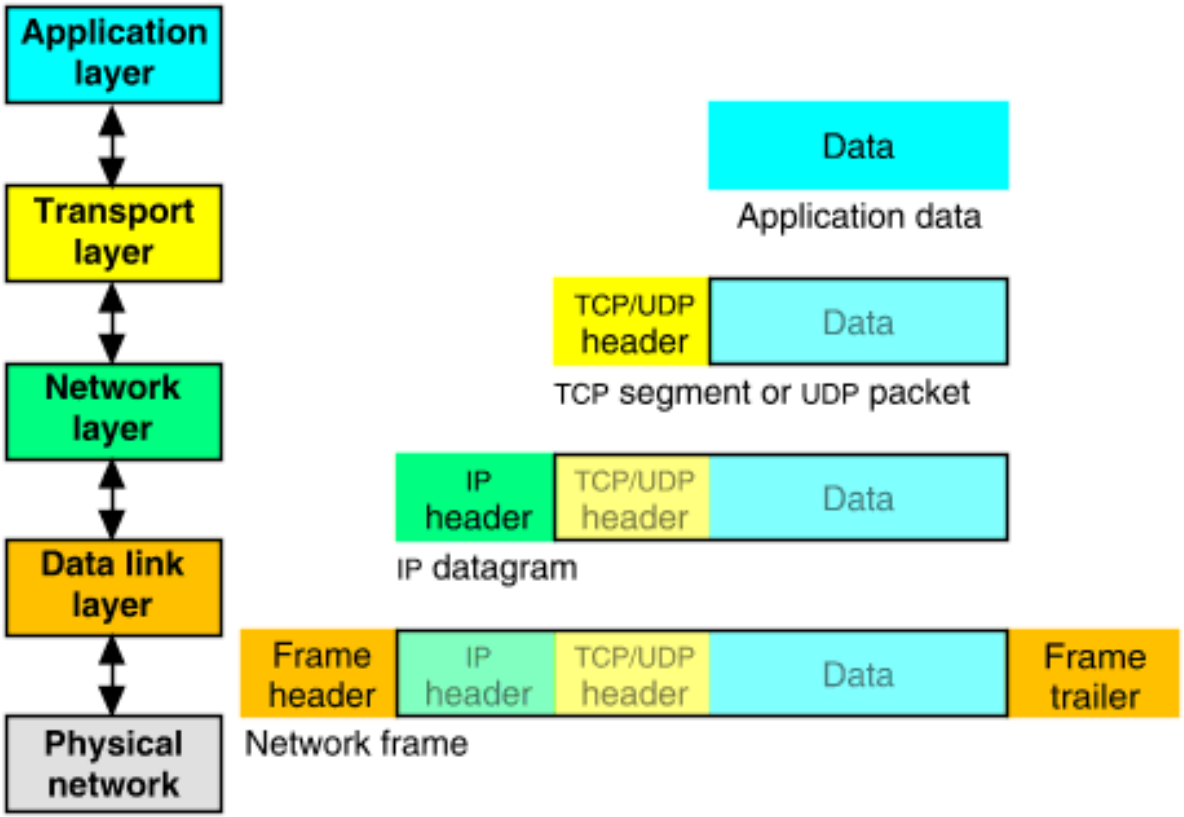


[8] TCP/IP Guide. TCP/IP Protocols

Kapsułkowanie i komunikacja równorzędna

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

TCP/IP: kapsułkowanie[9]



[9] TCP/IP stack

Komunikacja równorzędna

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

Model OSI: podsumowanie[10]

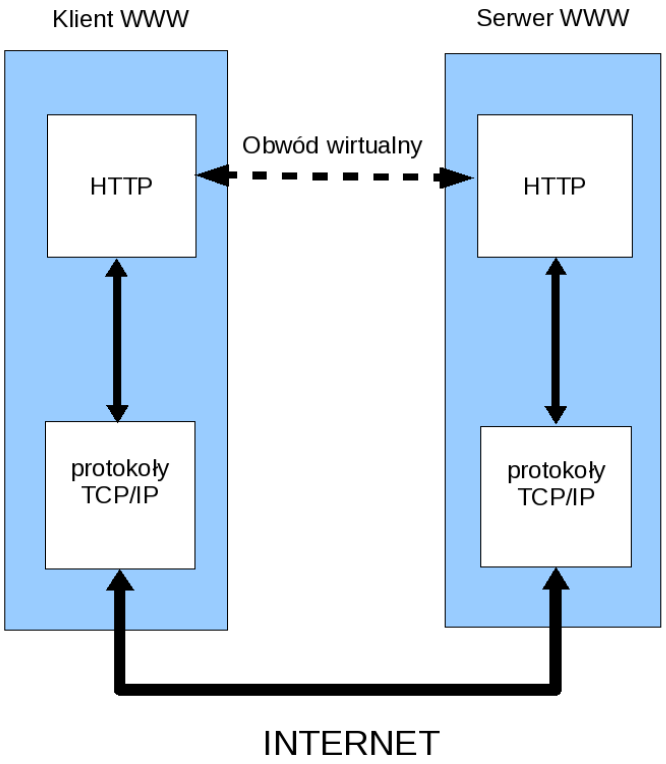
OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of packets between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams between points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.

[10] OSI model

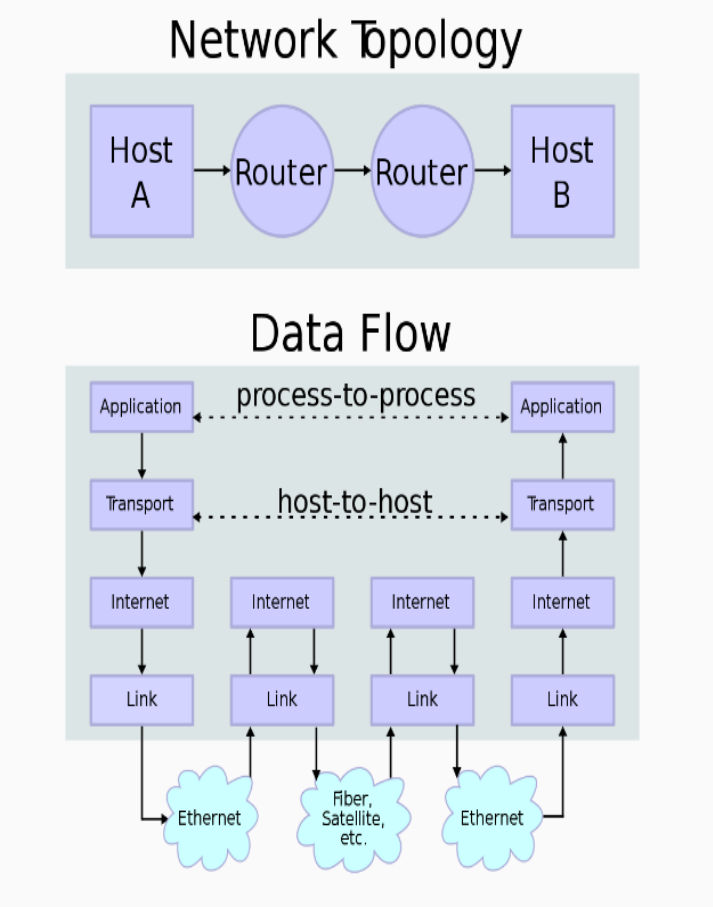
Komunikacja w sieci Internet

Komunikacja równorzędna węzeł-węzeł (*host-host*).

Sieci równorzędne (*peer-to-peer*, *P2P*).



Komunikacja w sieci Internet[11]



[11] TCP/IP model

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 (1983+), która definiuje ramki 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 (unifikacja Ethernet II i 802.3: IEEE 802.3x-1997).
- 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, przestrzeń. 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 docelowy	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 docelowy	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="5">IEEE 802.2</td></tr>
<tr><td>IEEE 802.3i
10Base-T</td><td>IEEE 802.3u
100Base-TX</td><td>IEEE 802.3ab
1000Base-T</td><td>IEEE 802.5
Token Ring</td><td>IEEE 802.8
FDDI</td></tr>
</table>

Warstwa dostępu do sieci

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: (a) opakowanie danych z podwarstwy LLC w ramki, (b) testy integralności danych, (c) śledzenie stanu nośnika

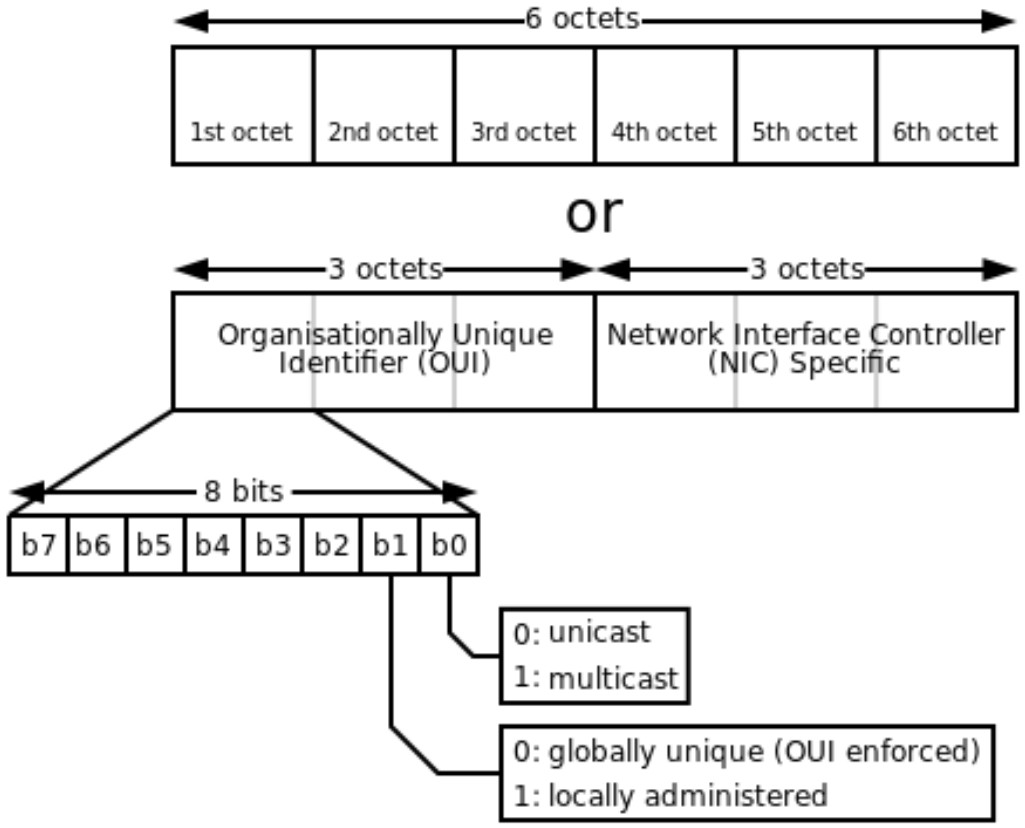
  – używa płaskiej struktury adresowej (adresy MAC)
  – grupuje bity w ramki
  – używa MAC do określania, który komputer będzie transmitował dane (w sytuacji, gdy wiele komputerów chce nadawać równocześnie)

Podwarstwa MAC

Adres sprzętowy MAC składa się z 48 bitów:

- 22 bity są przypisane producentowi sprzętu (OUI, *Organizational Unique Identifier*)
- 2 bity służą do określenia, czy adres jest globalnie jednoznaczny (*U/L bit*) i czy jest adresem grupowym (rozgłoszenia grupowego)
- 24 bity numerują kolejne karty

Podwarstwa MAC[12]



[12] MAC address

Usługi sterowania LLC:

- niepotwierdzona usługa bezpołączeniowa (*unacknowledged connectionless mode; uni-, multi-, broadcast*),
- potwierdzona usługa bezpołączeniowa (*acknowledged connectionless mode*),
- usługa połączeniowa (punkt-punkt)

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)
     6001 DEC MOP (Dump/Load)
     6002 DEC MOP (Remote Console)
```

```
      6003 DECNET Phase 4
      6004 DEC LAT
      6005 DEC
      6006 DEC
+     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)
-------------------------------------------------------------
```

\+ protokoły, którym przyznano publiczne numery

∗ protoły wykorzystujące Ethernet z rozgłoszeniem

@ jeśli wartość typu $<$0x600 – Ethernet 802.3, $\geqslant$0x600 – Ethernet II

Typy ramek ethernetowych

```
$ cat /etc/ethertypes
#
# Ethernet frame types
# This file describes some of the various Ethernet
# protocol types that are used on Ethernet networks.
#
...
IPv4   0800   ip ip4  # Internet IP (IPv4)
X25 0805
ARP 0806 ether-arp #
FR_ARP 0808     # Frame Relay ARP        [RFC1701]
BPQ 08FF # G8BPQ AX.25 Ethernet Packet
...
RARP 8035 # Reverse ARP            [RFC903]
AARP 80F3 # Appletalk AARP
ATALK 809B # Appletalk
802_1Q 8100 8021q 1q 802.1q dot1q # 802.1Q Virtual LAN tagged frame
IPX 8137 # Novell IPX
NetBEUI 8191 # NetBEUI
IPv6 86DD ip6  # IP version 6
PPP 880B # PPP
...
```

Struktura ramki Ethernet LLC

Nagłówek 802.2:

- 1-oktetowe pole punktu dostępu do usługi docelowej (pole DSAP) identyfikujące punkt dostępu do usługi LLC urządzenia docelowego
- 1-oktetowe pole punktu dostępu do usługi źródłowej (pole SSAP) identyfikujące punkt dostępu do usługi LLC urządzenia źródłowego
- 1- lub 2-oktetowe pole kontroli, wskazujące typ przenoszonej ramki LLC

Długość pola danych: 43-1497 lub 42-1496

Jeśli bajt DSAP ma wartość 0xAA, to ramka jest interpretowana jako SNAP; każda inna wartość oznacza ramkę LLC.

SSAP (*Source Service Access Point*) punkt dostępu usługi źródłowej

DSAP (*Destination Service Access Point*) punkt dostępu usługi docelowej

Struktura ramki Ethernet SNAP (*Sub-Network Access Protocol*)

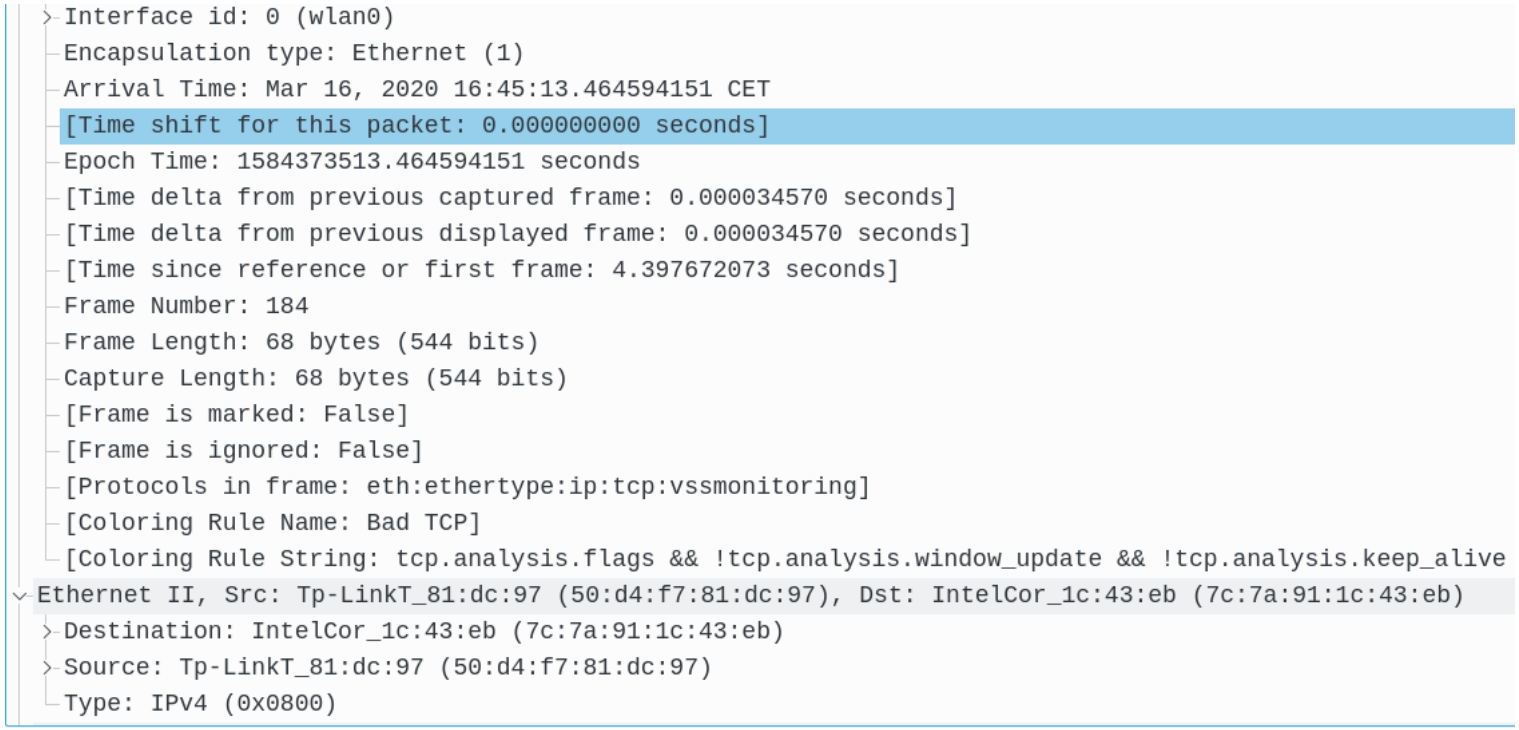
Nagłówek 802.2:

- 1-oktetowe pole punktu dostępu do usługi docelowej (pole DSAP) identyfikujące punkt dostępu do usługi LLC urządzenia docelowego
- 1-oktetowe pole punktu dostępu do usługi źródłowej (pole SSAP) identyfikujące punkt dostępu do usługi LLC urządzenia źródłowego
- 1- lub 2-oktetowe pole kontroli, wskazujące typ przenoszonej ramki LLC
- 5-oktetowa podramka SNAP zawierająca 3-oktetowe pole jednoznacznego identyfikatora organizacji (*Organizationally Unique Identifier* OUI) i 2-oktetowe pole Typ protokołu (identyfikacja protokołu warstwy wyższej)

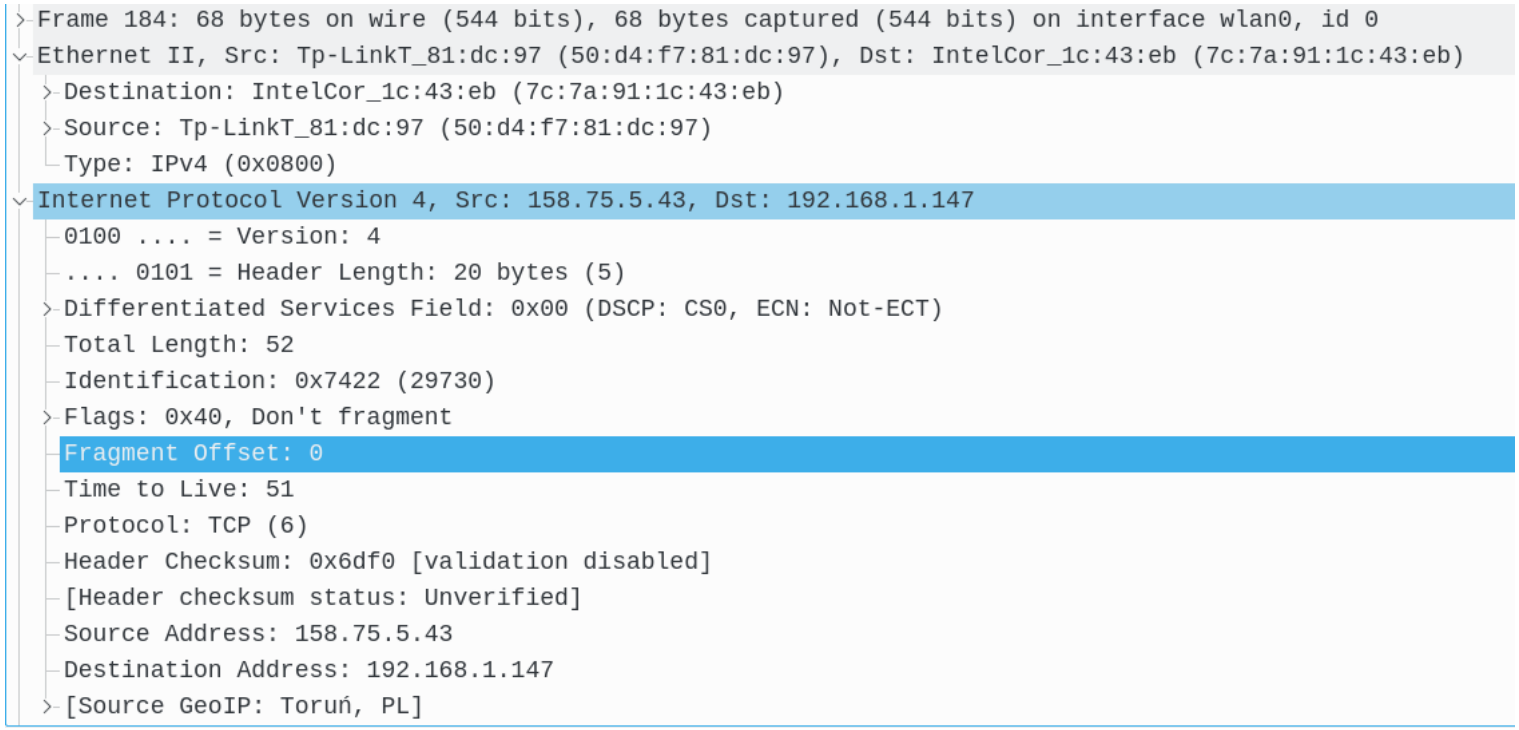
Długość pola danych: 38-1492 lub 37-1491

Ramka Ethernet SNAP umożliwia identyfikacje protokołów wyższego poziomu i zapewnia wsteczną kompatybilność z wcześniejszymi wersjami Ethernetu.

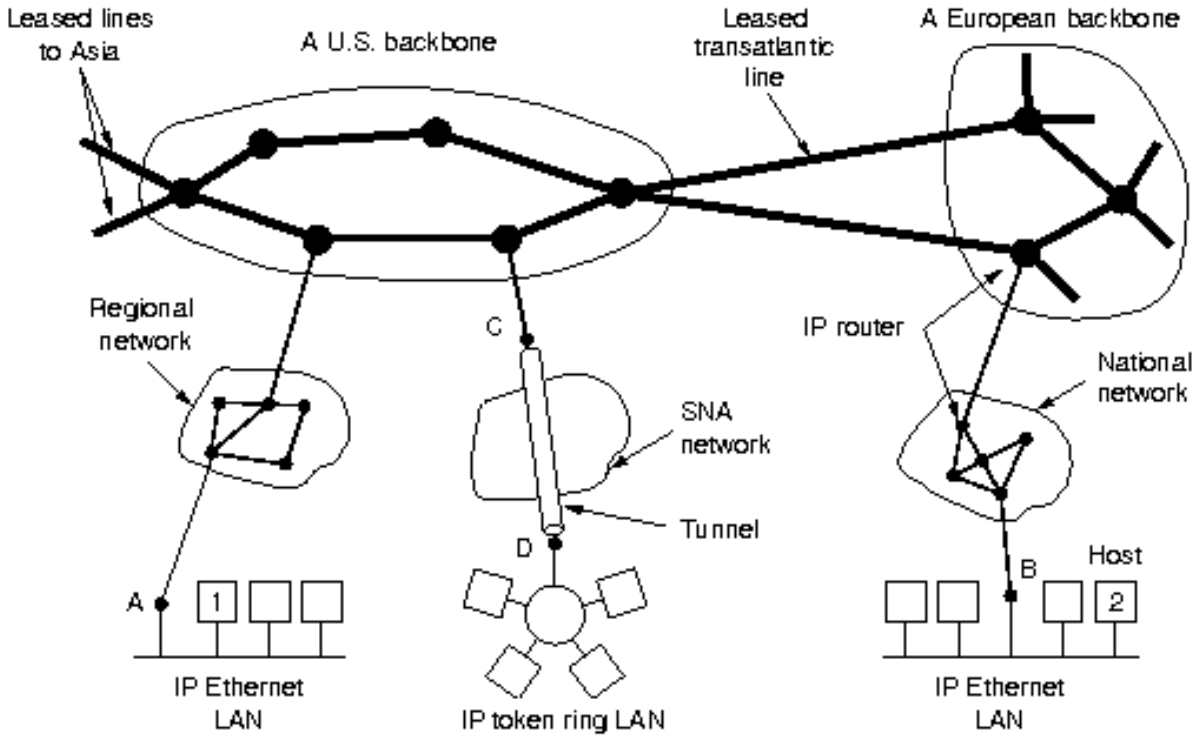
wireshark: Frame + Ethernet II



wireshark: Frame + Ethernet II + Internet Protocol



Internet jako zbiór połączonych sieci



Warstwa Internet (sieciowa)

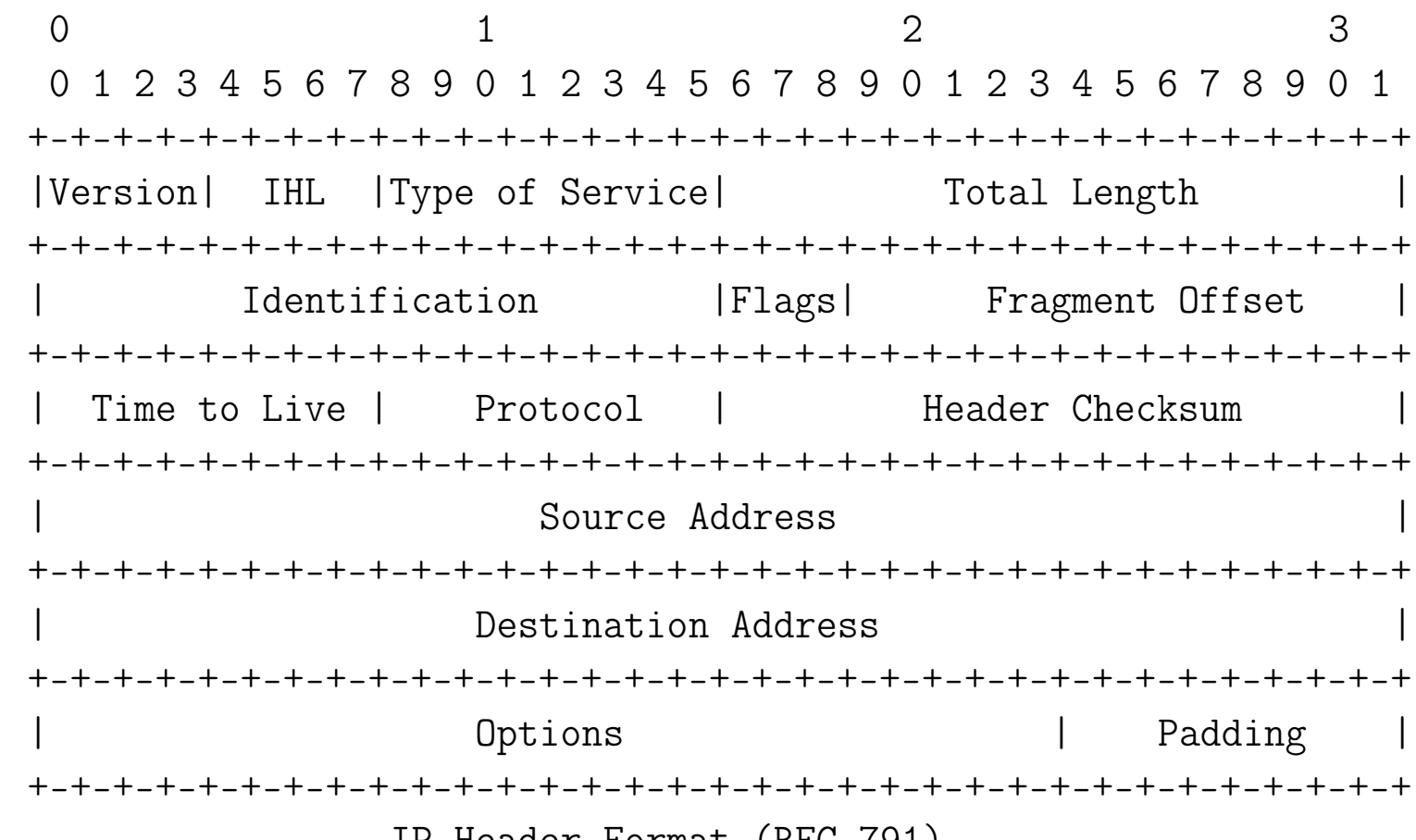
Funkcje warstwy sieciowej:

- 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 (przez host odbierający datagramy) (MTU, *Maximum Transmission Unit*); minimalna wartość MTU wynosi 576 dla IPv4 i 1280 dla IPv6

Internet Protocol protokół międzysieciowy, internetowy (RFC 791)

Własności IP:

- IP jest protokołem bezpołączeniowym, bez potwierdzenia i niepewnym
- *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.

Internet Assigned Numbers Authority (IANA)

IP TIME TO LIVE PARAMETER: The current recommended default time to live (TTL) for the Internet Protocol (IP) is 64 [RFC791, RFC1122]

IP TOS PARAMETERS: This documents the default Type-of-Service values

TOS Value	Description	Reference
0000	Default	[Obsoleted by RFC2474]
0001	Minimize Monetary Cost	[Obsoleted by RFC2474]
0010	Maximize Reliability	[Obsoleted by RFC2474]
0100	Maximize Throughput	[Obsoleted by RFC2474]
1000	Minimize Delay	[Obsoleted by RFC2474]
1111	Maximize Security	[Obsoleted by RFC2474]

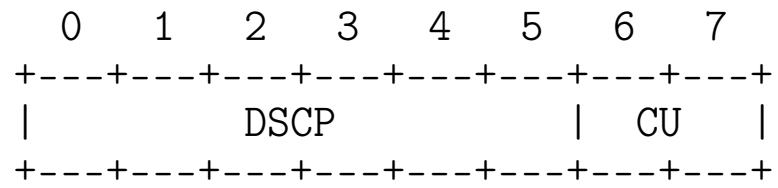
Generally, protocols which are involved in direct interaction with a human should select low delay, while data transfers which may involve large blocks of data are need high throughput. Finally, high reliability is most important for datagram-based Internet management functions.

TOS: zalecane wartości

Protocol	TOS Value	
TELNET (1)	1000	(minimize delay)
FTP		
Control	1000	(minimize delay)
Data (2)	0100	(maximize throughput)
TFTP	1000	(minimize delay)
SMTP (3)		
Command phase	1000	(minimize delay)
DATA phase	0100	(maximize throughput)
Domain Name Service		
UDP Query	1000	(minimize delay)
TCP Query	0000	
Zone Transfer	0100	(maximize throughput)
NNTP	0001	(minimize monetary cost)

TOS/Traffic Class

Dokument RFC 2474 określa nowe wykorzystanie pola TOS (IPv4) oraz oktetu *Traffic Class* (IPv6), który przyjmuje nazwę usług zróżnicowanych (DS, *Differentiated Services*):

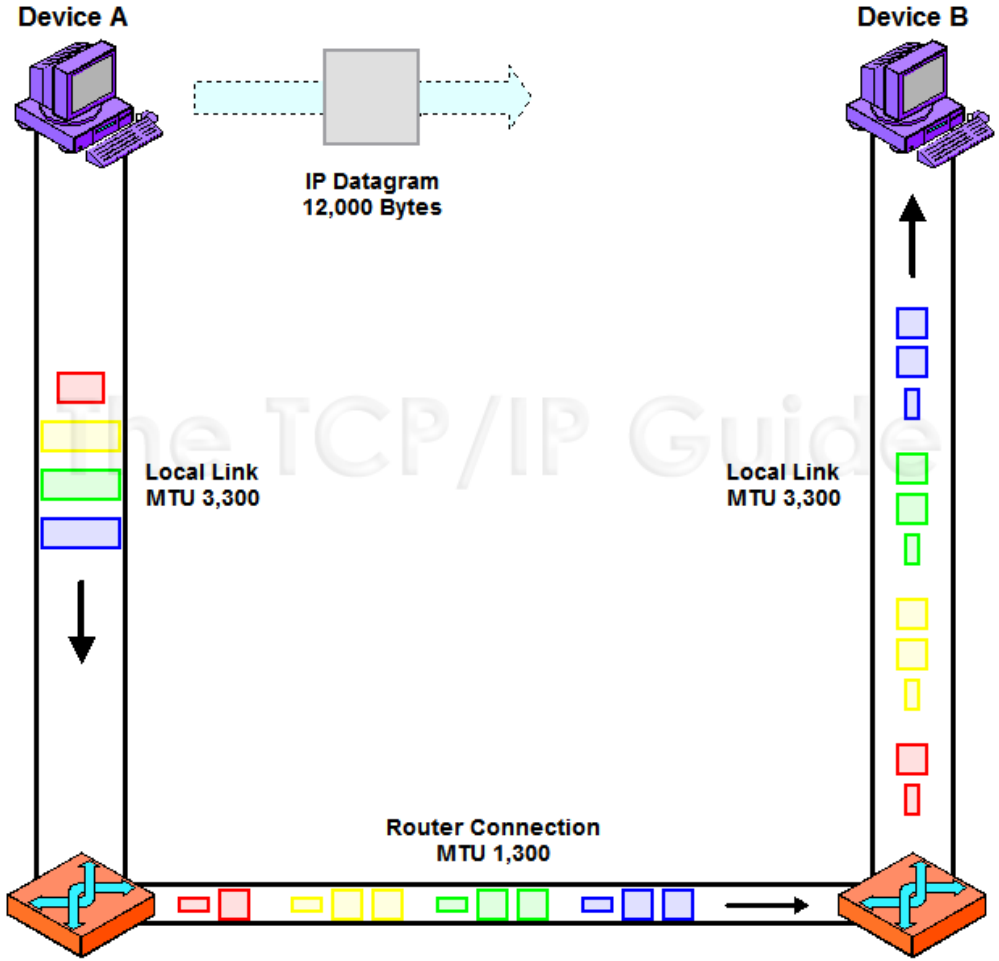



```
In the packet forwarding path, differentiated services are realized by mapping
the codepoint contained in a field in the IP packet header to a particular
forwarding treatment, or per-hop behavior (PHB), at each network node along its
path. The codepoints may be chosen from a set of mandatory values defined later
in this document, from a set of recommended values to be defined in future
documents, or may have purely local meaning.
```

IP: fragmentacja datagramów

```
Flags:  3 bits

    Various Control Flags.

      Bit 0: reserved, must be zero
      Bit 1: (DF) 0 = May Fragment,  1 = Don't Fragment.
      Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.

         0   1   2
       +---+---+---+
       |   | D | M |
       | 0 | F | F |
       +---+---+---+
```

IP: fragmentacja datagramów[13]



[13] C.M.Kozierok, TCP/IP Guide

IP: opcje

CLASS	NUMBER	LENGTH	DESCRIPTION
0	0	-	End of Option list. This option occupies only 1 octet; it has no length octet.
0	1	-	No Operation. This option occupies only 1 octet; it has no length octet.
0	2	11	Security. Used to carry Security, Compartmentation, User Group (TCC), and Handling Restriction Codes compatible with DOD requirements.
0	3	var.	Loose Source Routing. Used to route the internet datagram based on information supplied by the source.
0	9	var.	Strict Source Routing. Used to route the internet datagram based on information supplied by the source.
0	7	var.	Record Route. Used to trace the route an internet datagram takes.
0	8	4	Stream ID. Used to carry the stream identifier.
2	4	var.	Internet Timestamp.

Fragment pliku /etc/protocols[14]

```
# Internet (IP) protocols
ip          0       IP              # internet protocol, pseudo protocol number
icmp        1       ICMP            # internet control message protocol
igmp        2       IGMP            # Internet Group Management
ggp         3       GGP             # gateway-gateway protocol
ipencap     4       IP-ENCAP        # IP encapsulated in IP (officially ``IP'')
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 Protocol
ipv6-icmp   58      IPv6-ICMP       # ICMP for IPv6
ipv6-nonxt  59      IPv6-NoNxt      # No Next Header for IPv6
```

[14] Protocol Numbers

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.[15]

Adres IP składa się z części sieciowej i części hosta. Podział na te części był pierwotnie, tj. do czasu opracowania RFC 1519, określany przez klasę, do której adres należał.

klasa A	
IP	0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh
adresy	0.0.0.0 – 127.255.255.255
# sieci	126
# hostów	$\approx 17 \times 10^6$

adres sieci (*network address*): np. 127.0.0.0
adres rozgłoszeniowy (*broadcast address*): np. 127.255.255.255

[15] Przydzielaniem adresów zajmuje się ICANN (*Internet Corporation for Assigned Names and Numbers*).

Klasy adresów IP

klasa B	
IP	10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh
adresy	128.0.0.0 – 191.255.255.255
# sieci	16384
# hostów	65534

klasa C	
IP	110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh
adresy	192.0.0.0 – 223.255.255.255
# sieci	$\approx 2 \times 10^6$
# hostów	254

Klasy adresów IP

klasa D	
IP	1110bbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb
adresy	224.0.0.0 – 239.255.255.255
# grup	$2^{28} = 268435456$

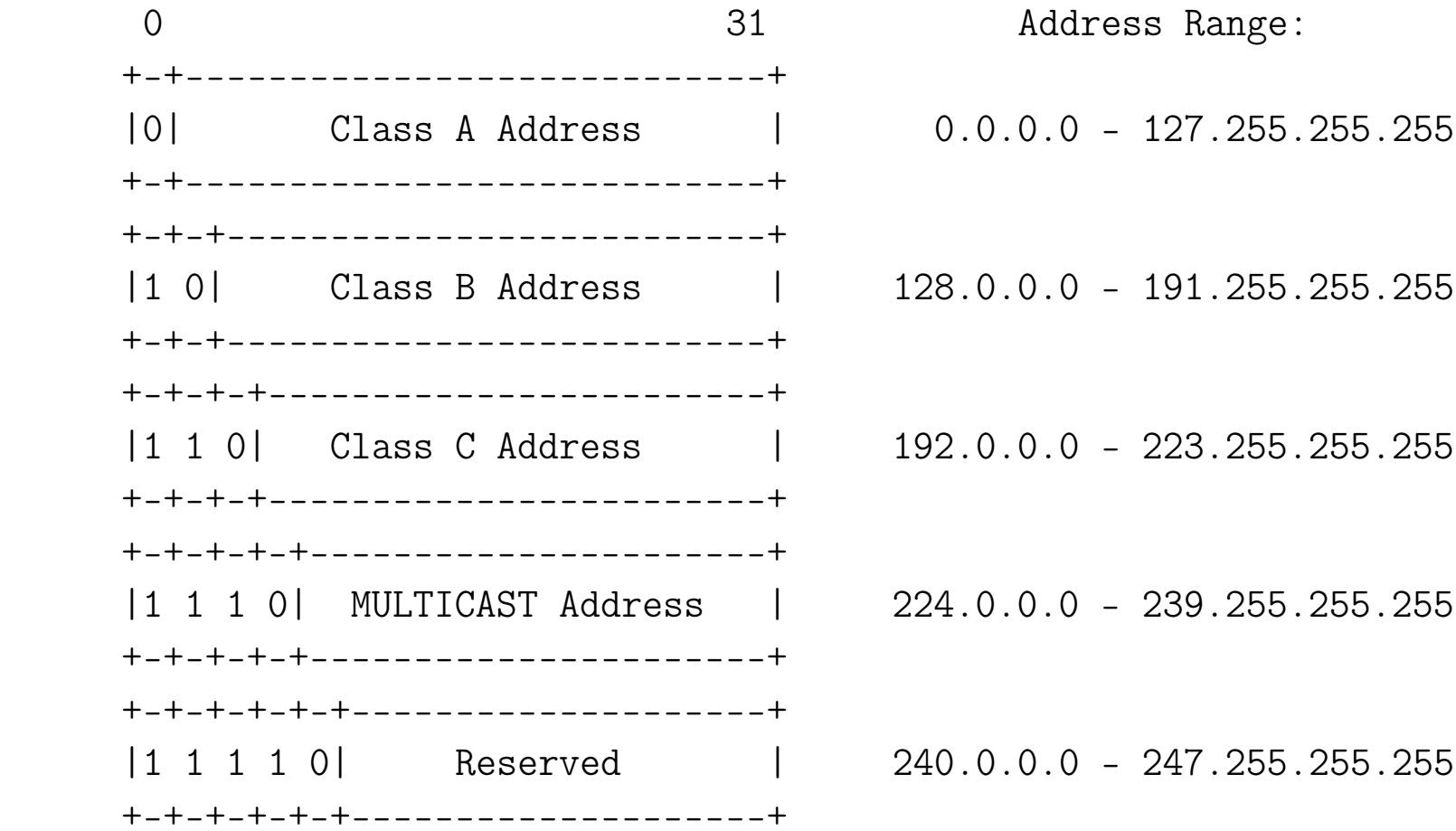
W trakcie rozgłaszania grupowego (transmisji multicastowej) nadawca przesyła pojedynczą kopię wiadomości do *dostarczyciela usługi* (SP, *service provider*) w trakcie pojedynczej operacji. SP dostarcza kopię wiadomości do każdego odbiorcy transmisji multicastowej.

Adresy grupowe (multicast)

Wyróżnia się trzy grupy adresów multicastowych:

1. 224.0.0.0-224.0.0.255 są zarezerwowane dla *dobrze znanych* grup multicastowych, m.in.
   - 224.0.0.1 – grupa wszystkich hostów z lokalnej sieci akceptujących multicast; każdy host akceptujący multicasty zapisuje się do tej grupy przy uruchamianiu
   - 224.0.0.2 – grupa wszystkich routerów multicastowych w sieci lokalnej
   - 224.0.0.5 – grupa wszystkich routerów OSPF rozsyłających pakiety *Hello*
   - 224.0.0.6 – grupa wszystkich routerów desygnowanych OSPF
   - 224.0.0.251 – adress usługi mDNS (*Multicast DNS*)
   - 224.0.0.252 – adress usługi LLMNR (*Link-local Multicast Name Resolution*)
2. 224.0.1.0–238.255.255.255 adresy o zasięgu globalnym (*Globally-scoped (Internet-wide) multicast addresses*
3. 239.0.0.0–239.255.255.255 zarezerwowane na lokalne potrzeby organizacji (*Administratively-scoped (local) multicast addresses*)

Klasy adresów IP (cd)



Wydzielone/zarezerwowane bloki adresów IP

- Dokument RFC 1918 definiuje adresy prywatne, które mogą być wykorzystywane na potrzeby sieci domowej, biurowej lub sieci całego przedsiębiorstwa.

klasa A	10.0.0.0–10.255.255.254	10.0.0.0/8
klasa B	172.16.0.0–172.31.255.254	172.16.0.0/12
klasa C	192.168.0.0–192.168.255.254	192.168.0.0/16

- 169.254.0.0–169.254.255.255: autokonfiguracja (Zeroconf)
- 127.0.0.0–127.255.255.255: pętla zwrotna
- Inne bloki adresów zarezerwowanych: 0.0.0.0-0.255.255.255, 198.18.0.0/15, ...

Klasy adresów IP: pętla zwrotna

Adresy 127.0.0.0/8 zostały zarezerwowane dla wirtualnego (realizowanego programowo) interfejsu (lo, lo0). Jest to tzw. interfejs pętli zwrotnej, gdyż każdy pakiet wysłany na ten interfejs pojawia się na nim jako pakiet wchodzący.

Zwyczajowo przypisuje się interfejsowi pętli zwrotnej adres 127.0.0.1.

Fragment pliku `/etc/hosts`:

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
158.75.5.43 ameryk.fizyka.umk.pl ameryk am
...
```

Bezklasowe trasowanie międzydomenowe (RFC 1519)

Przyczyny opracowania CIDR (*Classless InterDomain Routing*):

- wzrost zapotrzebowania na nowe adresy (adresy klasy B na wyczerpaniu)
- klasowy podział adresów prowadzi do marnowania sporej ich części
- wzrost obciążenia routerów/wzrost liczby tras w Internecie:[16]
  - 1990: $\approx 5 \times 10^3$
  - 2022: $\approx 1048 \times 10^3$ (IPv4)
  - 2022: $\approx 131 \times 10^3$ (IPv6)

[16] CIDR Report, What will happen when the routing table hits 1024k?

Sieci i podsieci. Maski podsieci

Za pomocą adresu IP i maski można trasować dowolny datagram IP do miejsca przeznaczenia.

- 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 urządzenia sieciowego (hosta) w podsieci
- podsieć jest znana tylko lokalnie

Sieci i podsieci. Maski podsieci[17]

Wielkości podsieci w zależności wyboru maski (klasa C)

liczba IP	liczba podsieci	maska	/maska|prefix	*wildcard*
2	128	255.255.255.254 (1111 1110)	/31	0.0.0.1
4	64	255.255.255.252 (1111 1100)	/30	0.0.0.3
8	32	255.255.255.248 (1111 1000)	/29	0.0.0.7
16	16	255.255.255.240 (1111 0000)	/28	0.0.0.15
32	8	255.255.255.224 (1110 0000)	/27	0.0.0.31
64	4	255.255.255.192 (1100 0000)	/26	0.0.0.63
128	2	255.255.255.128 (1000 0000)	/25	0.0.0.127

maska podsieci = 256 - <liczba IP w podsieci (zawsze 2^n)>
/maska = /<długość prefiksu>

[17] Understanding IP Addressing

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
	195.15.25.64	11000011	00000111	00011001	01000000
OR	0.0.0.31	00000000	00000000	00000000	00011111
=	195.15.25.95	11000011	00000111	00011001	01011111

Sieci i podsieci. Grupowanie w nadsieci

```
158.75.4.0     (10011110.01001011.0000010 0.00000000)  Class C subnet address
158.75.5.0     (10011110.01001011.0000010 1.00000000)  Class C subnet address
-------------------------------------------------------------------------
158.75.4.0     (10011110.01001011.0000010 0.00000000)  Supernetted Subnet address
255.255.254.0  (11111111.11111111.1111111 0.00000000)  Subnet Mask
158.75.5.255   (10011110.01001011.0000010 1.11111111)  Broadcast address

$ ipcalculator 158.75.4.0/23
Address:   158.75.4.0           10011110.01001011.0000010 0.00000000
Netmask:   255.255.254.0 = 23   11111111.11111111.1111111 0.00000000
Wildcard:  0.0.1.255            00000000.00000000.0000000 1.11111111
=>
Network:   158.75.4.0/23        10011110.01001011.0000010 0.00000000
HostMin:   158.75.4.1           10011110.01001011.0000010 0.00000001
HostMax:   158.75.5.254         10011110.01001011.0000010 1.11111110
Broadcast: 158.75.5.255         10011110.01001011.0000010 1.11111111
Hosts/Net: 510                   Class B
```

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

Klasy adresów IP: sieci prywatne (cd)

```
$ sipcalc 10.0.0.0/8
-[ipv4 : 10.0.0.0/8] - 0

[CIDR]
Host address            - 10.0.0.0
Host address (decimal)  - 167772160
Host address (hex)      - A000000
Network address         - 10.0.0.0
Network mask            - 255.0.0.0
Network mask (bits)     - 8
Network mask (hex)      - FF000000
Broadcast address       - 10.255.255.255
Cisco wildcard          - 0.255.255.255
Addresses in network    - 16777216
Network range           - 10.0.0.0 - 10.255.255.255
Usable range            - 10.0.0.1 - 10.255.255.254
```

Klasy adresów IP: sieci prywatne (cd)

```
$ sipcalc  172.16.0.0/12
-[ipv4 : 172.16.0.0/12] - 0

[CIDR]
Host address            - 172.16.0.0
Host address (decimal)  - 2886729728
Host address (hex)      - AC100000
Network address         - 172.16.0.0
Network mask            - 255.240.0.0
Network mask (bits)     - 12
Network mask (hex)      - FFF00000
Broadcast address       - 172.31.255.255
Cisco wildcard          - 0.15.255.255
Addresses in network    - 1048576
Network range           - 172.16.0.0 - 172.31.255.255
Usable range            - 172.16.0.1 - 172.31.255.254
```

Klasy adresów IP: sieci prywatne (cd)

```
$ sipcalc 192.168.0.0/16
-[ipv4 : 192.168.0.0/16] - 0

[CIDR]
Host address            - 192.168.0.0
Host address (decimal)  - 3232235520
Host address (hex)      - C0A80000
Network address         - 192.168.0.0
Network mask            - 255.255.0.0
Network mask (bits)     - 16
Network mask (hex)      - FFFF0000
Broadcast address       - 192.168.255.255
Cisco wildcard          - 0.0.255.255
Addresses in network    - 65536
Network range           - 192.168.0.0 - 192.168.255.255
Usable range            - 192.168.0.1 - 192.168.255.254
```

Konfiguracja interfejsów sieciowych: ifconfig[18]

```
# ifconfig -a
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 15723  bytes 1960492 (1.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15723  bytes 1960492 (1.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.103  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::2fd3:ef24:ebb3:99fc  prefixlen 64  scopeid 0x20<link>
        ether 7c:7a:91:1c:43:eb  txqueuelen 1000  (Ethernet)
        RX packets 1024386  bytes 778178815 (742.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 741353  bytes 194591753 (185.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

[18] Windows: `ipconfig /all`

Konfiguracja interfejsów sieciowych: ip

```
# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN \
                                        mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: em1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN \
                                        mode DEFAULT group default qlen 1000
    link/ether 28:d2:44:56:0f:d5 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP \
                                        mode DORMANT group default qlen 1000
    link/ether 7c:7a:91:1c:43:eb brd ff:ff:ff:ff:ff:ff
```

Konfiguracja interfejsów sieciowych: ip

```
# ip address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qle
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
...
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default
    link/ether 7c:7a:91:1c:43:eb brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.103/24 brd 192.168.2.255 scope global dynamic wlan0
       valid_lft 83756sec preferred_lft 83756sec
    inet6 fe80::2fd3:ef24:ebb3:99fc/64 scope link
       valid_lft forever preferred_lft forever

# ip route show
default via 192.168.2.1 dev wlan0 proto static metric 600
158.75.4.0/23 via 172.20.1.26 dev tun0
158.75.104.0/23 via 172.20.1.26 dev tun0
172.20.0.1 via 172.20.1.26 dev tun0
172.20.1.26 dev tun0 proto kernel scope link src 172.20.1.25
192.168.2.0/24 dev wlan0 proto kernel scope link src 192.168.2.103 metric 600
```

Konfiguracja interfejsów sieciowych: ip

```
# ip -4 maddress show
1:      lo
        inet  224.0.0.251
        inet  224.0.0.1
3:      eth0
        inet  224.0.0.1
4:      wlan0
        inet  224.0.0.252
        inet  224.0.0.1
        inet  224.0.0.251 users 3
5:      virbr0
```

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); teraz tę rolę pełni DHCP (*Dynamic Host Configuration Protocol*)

  Zastosowania: bootowanie stacji bezdyskowych

```
# arp -n
158.75.4.26              ether   70:85:c2:a9:39:ca   C           eth0
158.75.5.101                     (incomplete)                    eth0
...
# ip neighbor show
158.75.4.26 dev eth0 lladdr 70:85:c2:a9:39:ca DELAY
158.75.5.240 dev eth0 lladdr 0c:c4:7a:4c:89:d7 REACHABLE
158.75.5.101 dev eth0  FAILED
158.75.4.243 dev eth0 lladdr aa:bb:6d:7e:e1:bd STALE
...
```

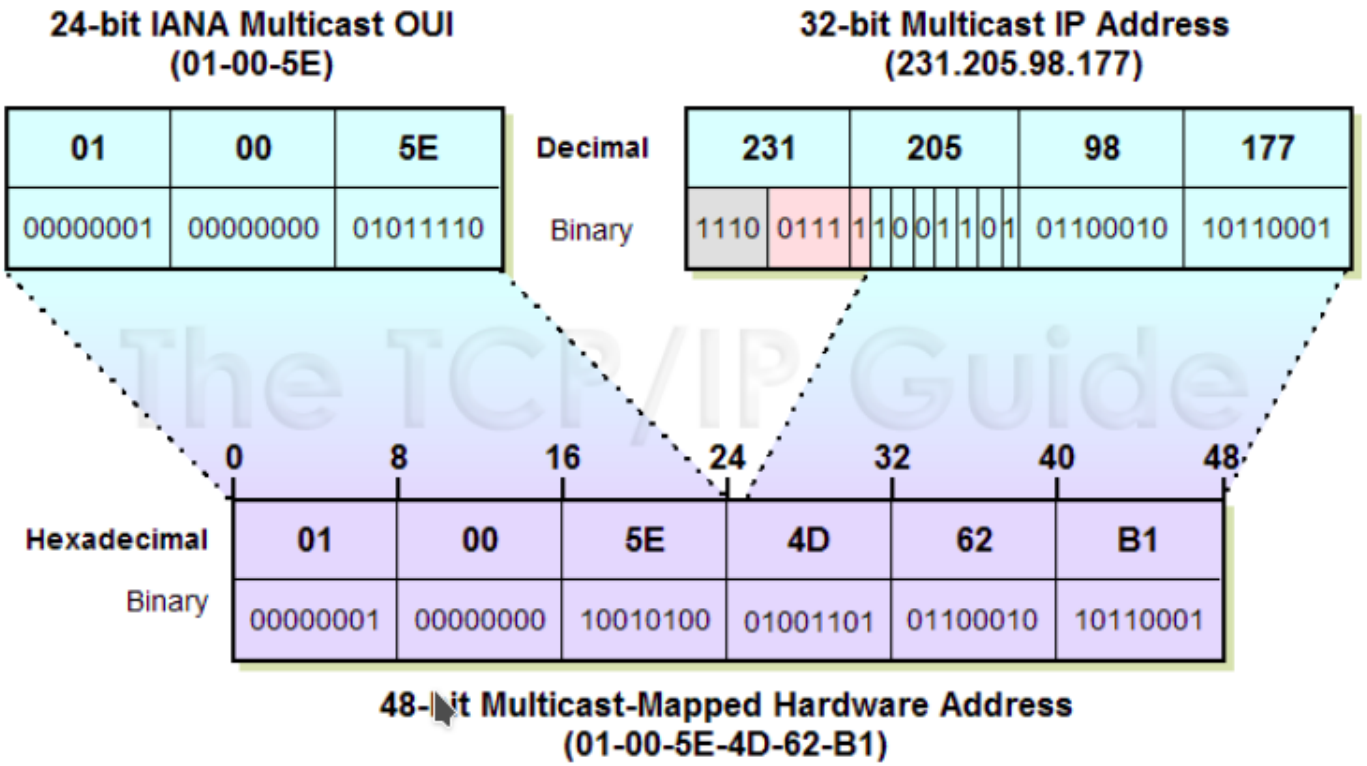
Jak powstaje tablica ARP?

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.

Jak mapować adresy klasy D na IEEE 802.2?[19]



[19] TCP/IP Address Resolution For IP Multicast Addresses

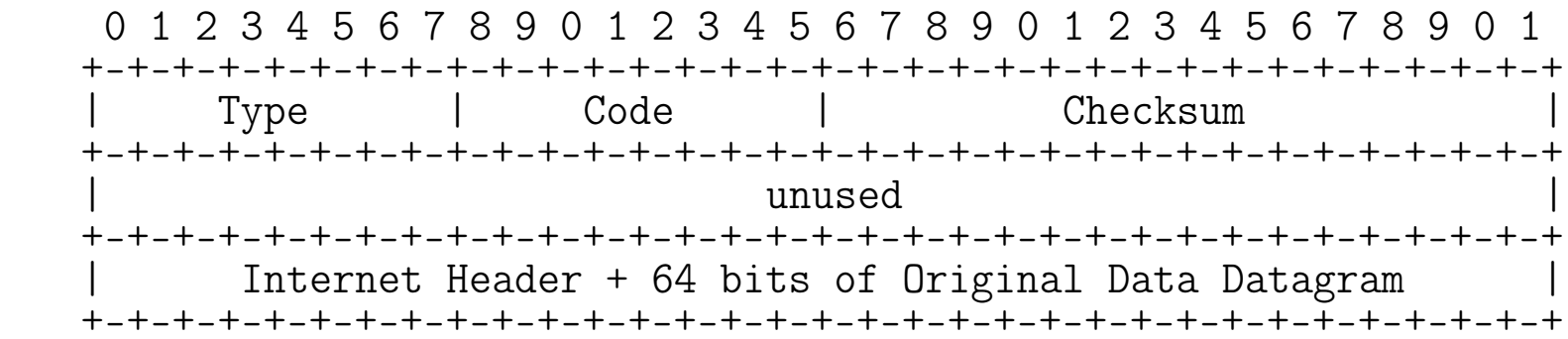
Internet Control Message Protocol (ICMP, RFC 792)

ICMP – protokół sterowania wiadomością internetową

Funkcje:

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

Internet Control Message Protocol[20]



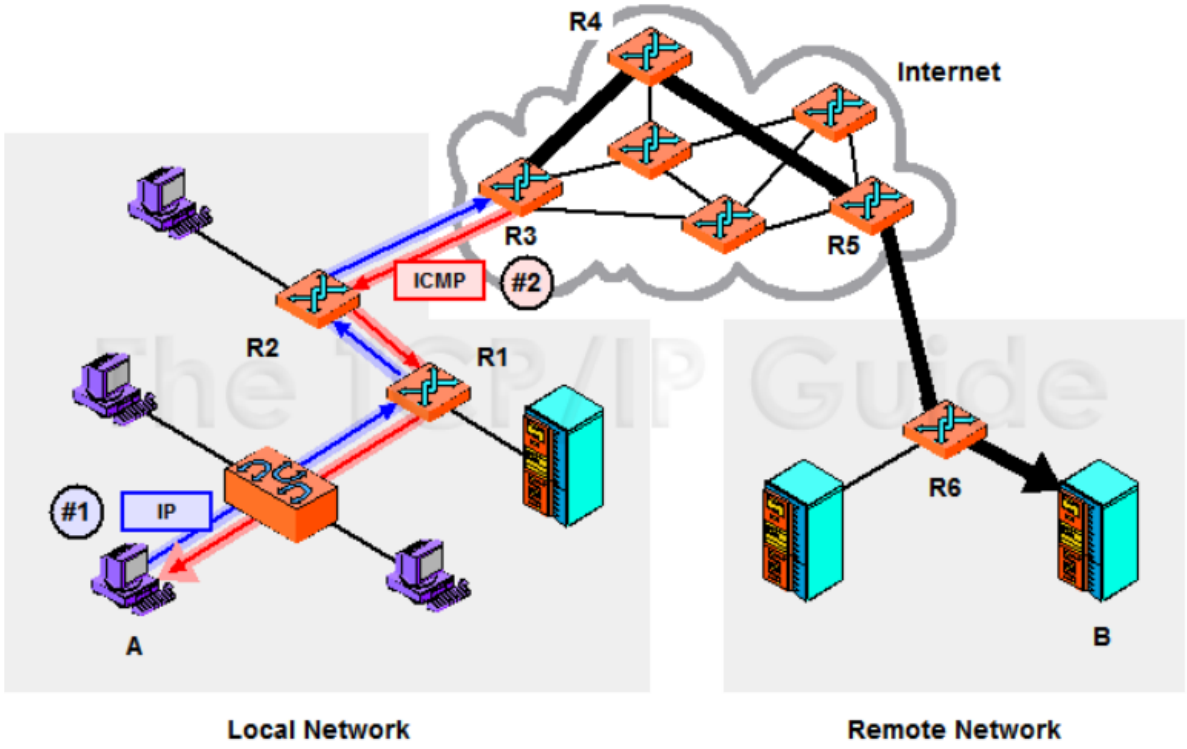
Message Types:

0	Echo Reply		
3	Destination Unreachable	4	Source Quench
5	Redirect	8	Echo (Request)
9	Router Advertisement	10	Router Solicitation
11	Time Exceeded	12	Parameter Problem
13	Timestamp (Request)	14	Timestamp Reply
15	Information Request	16	Information Reply

Type=3 Code: 0 = net unreachable; 1 = host unreachable; 2 = protocol unreachable;
3 = port unreachable; 4 = fragmentation needed and DF set;
5 = source route failed.

[20] C.M.Kozierok, TCP/IP Guide: ICMP Message Classes, Types and Codes

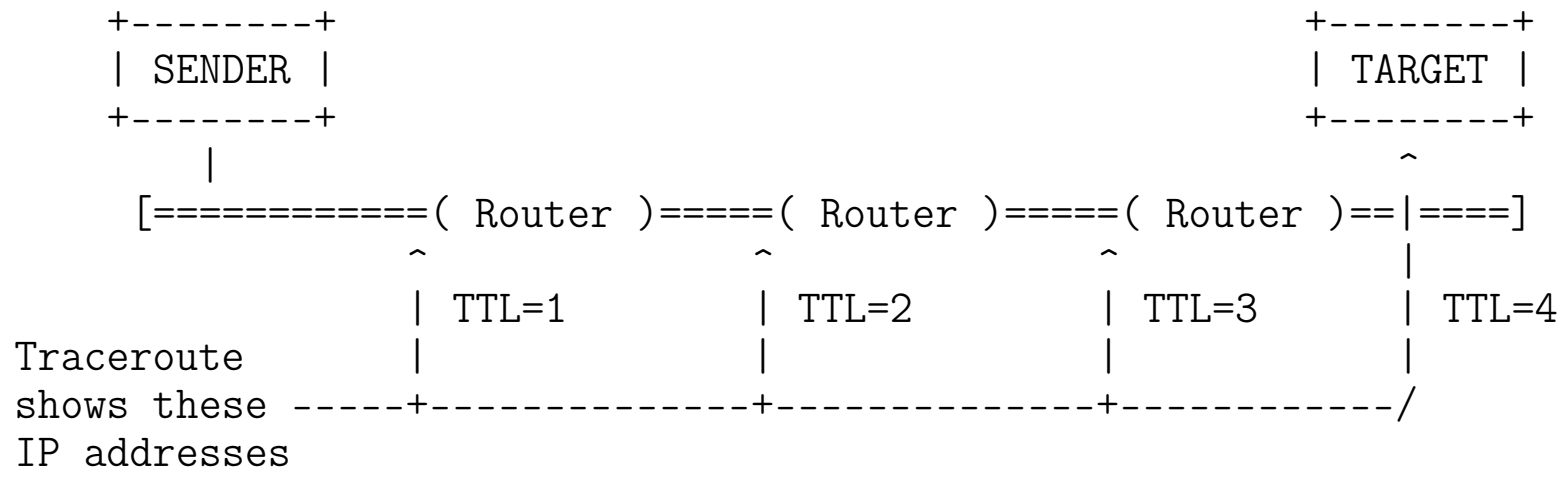
ICMP – działanie[21]



[21] C.M.Kozierok, TCP/IP Guide

ICMP – traceroute

```
# traceroute 158.75.1.4
traceroute to 158.75.1.4 (158.75.1.4), 30 hops max, 60 byte packets
 1  158.75.5.254 (158.75.5.254)  19.664 ms  19.839 ms  20.530 ms
 2  158.75.64.105 (158.75.64.105)  0.594 ms  0.902 ms  1.051 ms
 3  ucirt.man.torun.pl (158.75.33.33)  0.497 ms  0.493 ms  0.485 ms
 4  158.75.64.22 (158.75.64.22)  0.425 ms  0.390 ms  0.349 ms
 5  158.75.64.22 (158.75.64.22)  0.307 ms  0.399 ms  0.876 ms
```



ICMP – ping

```
# 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


# 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 data.

--- 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 0.252/0.147 ms
```

Internet Protocol Version 6 (IPv6 RFC 2460)

Ograniczenia IPv4:

- zbyt mała liczba adresów ($2^{32} - 1 \approx 4.29 \times 10^9$), nieefektywne wykorzystywanie przestrzeni adresowej
- dwupoziomowa hierarchia adresowania (host.domena), która uniemożliwia konstruowanie wydajnych hierarchii adresowych (utrudniona agregacja tras)
- słaba obsługa ruchu audio/wideo
- brak mechanizmów zapewniających poufność i integralność datagramów oraz uwierzytelnianie nadawców i odbiorców pakietów

Internet Protocol Version 6

Własności:

- ogromna przestrzeń adresowa ($2^{128} - 1 \approx 3.4 \times 10^{38}$)

  ..., this is 2^{52} ($\approx 4.5 \times 10^{15}$) addresses for every star in the known universe – a million times as many addresses per star than IPv4 supported for our single planet.[22]

- 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 (*Flow label*), np. pakiety „multimedialne" mogą być przełączane z większym priorytetem

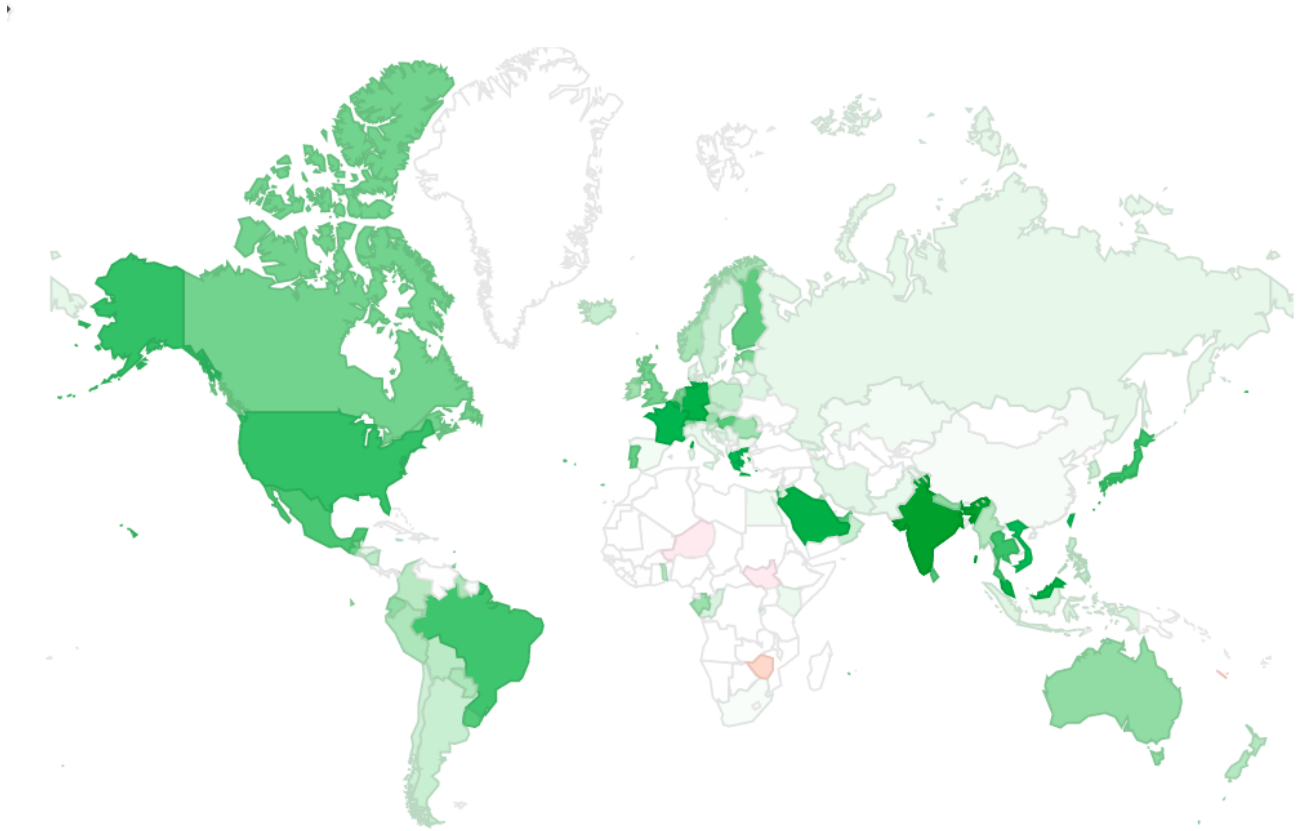
[22] http://en.wikipedia.org/wiki/IPv6

Internet Protocol Version 6

- bezpieczeństwo (kodowanie i identyfikacja) – nagłówek zawiera rozszerzenie, które pozwala zaznaczyć używany w czasie połączenia mechanizm uwierzytelniania źródła pochodzenia pakietów (plus zapewnienie integralności i poufności danych); IPv4 został uzupełniony o protokół IPsec
- mobilność hostów, auto(re)konfiguracja (stanowa i bezstanowa, stałe adresy)
- wydajność – stała długość nagłówka (tylko 40 oktetów), zoptymalizowane przetwarzanie nagłówka, brak sumy kontrolnej, brak fragmentacji, rozgłoszenia zastąpione rozgłoszeniami grupowymi

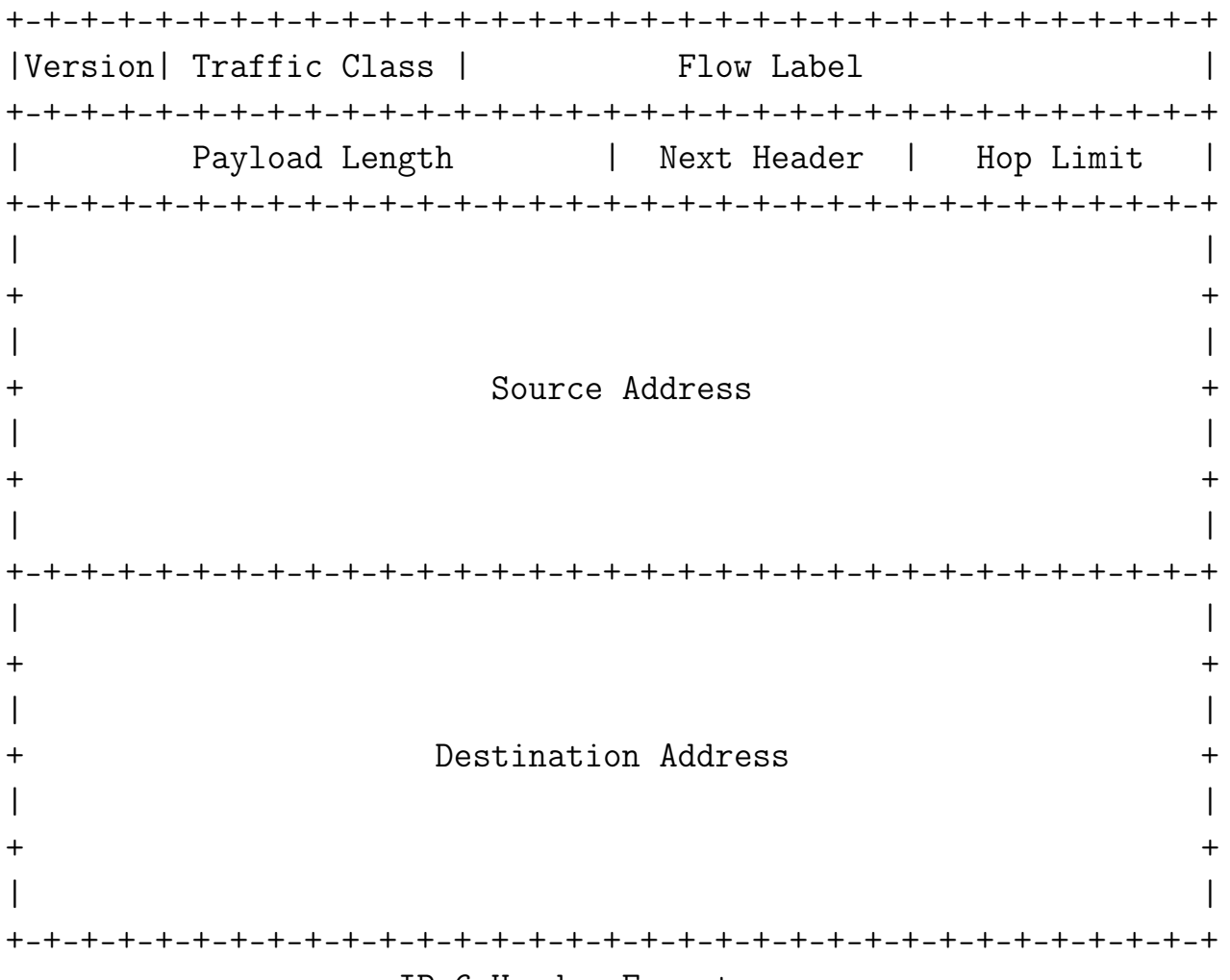
Działanie IPv6 jest wspomagane przez ICMPv6 (RFC 4443) oraz protokół *Neighbor Discovery* (RFC 4861, uaktualniony przez 5942, 6980, 7048, 7527, 7559, 8028).

Poziom wykorzystania IPv6[23]



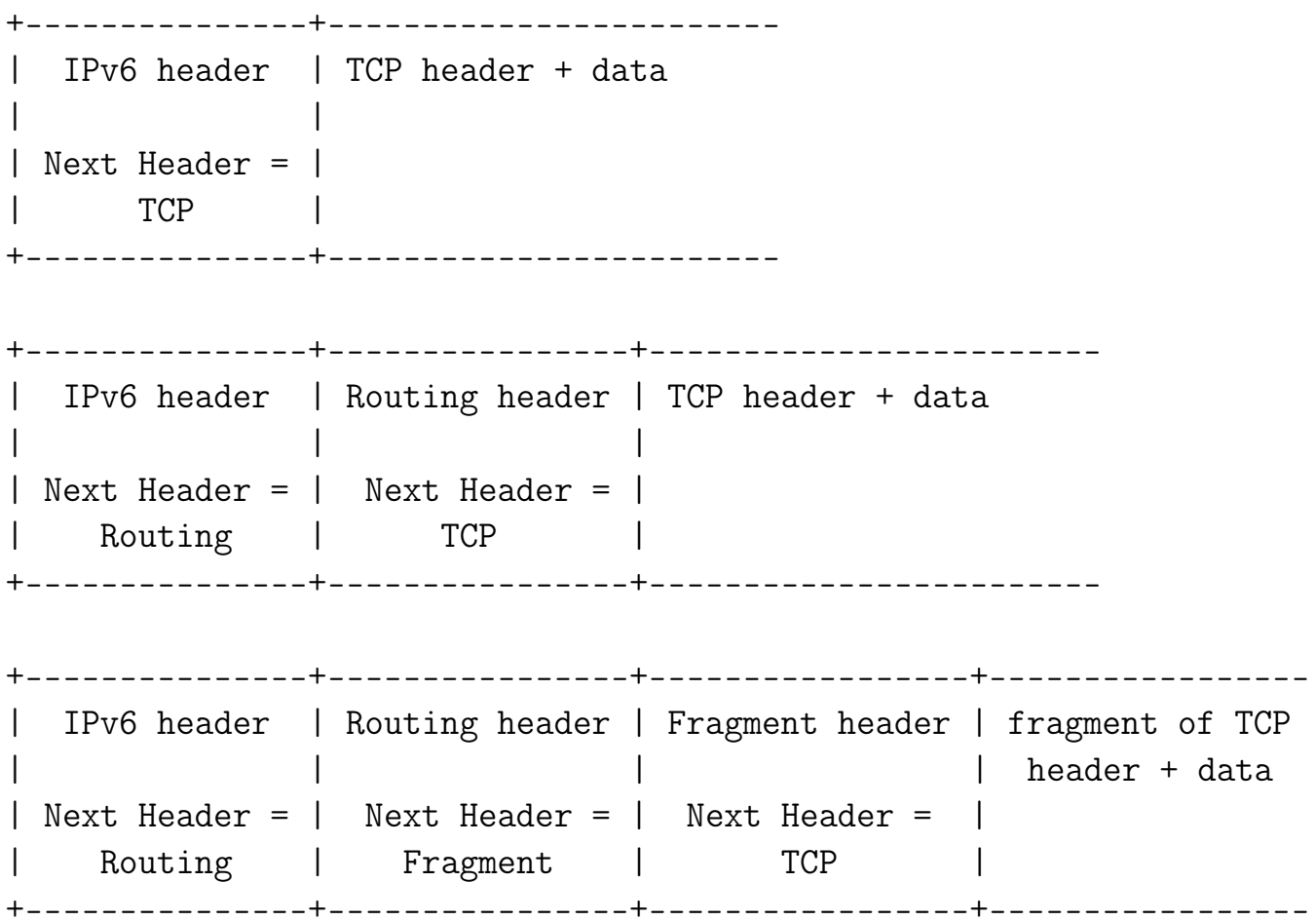
[23] Per-country IPv6 adoption, zob. także IPv6 Launch: measurements

Internet Protocol Version 6

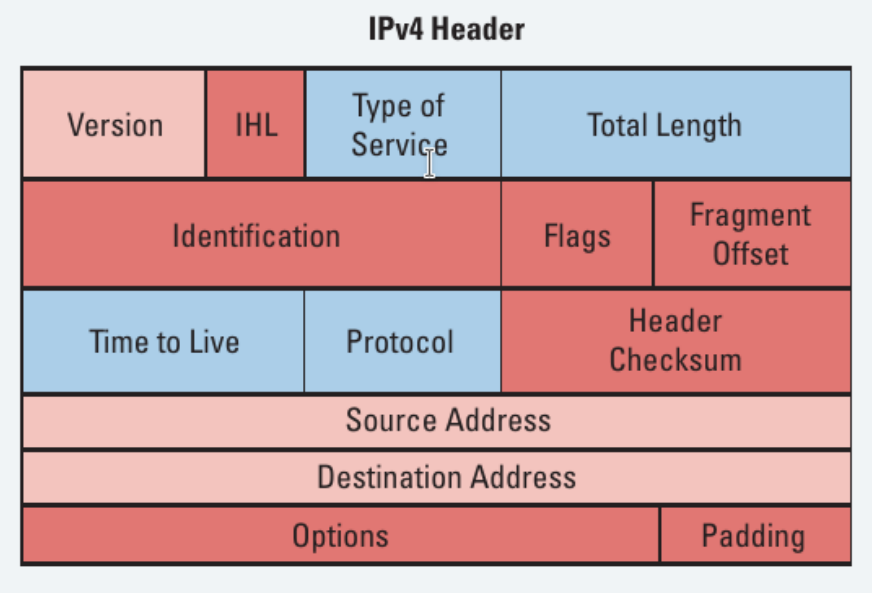


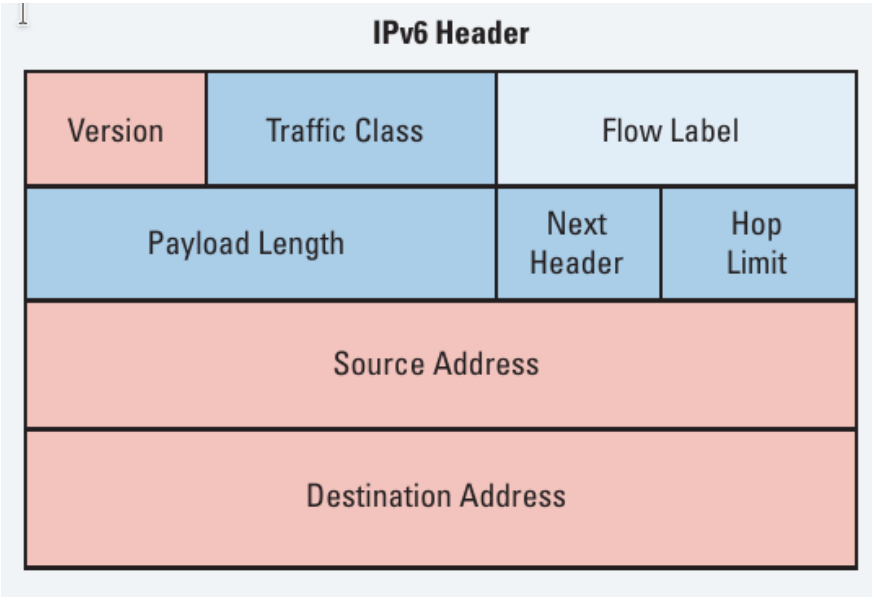
IPv6 Header Format

Internet Protocol Version 6



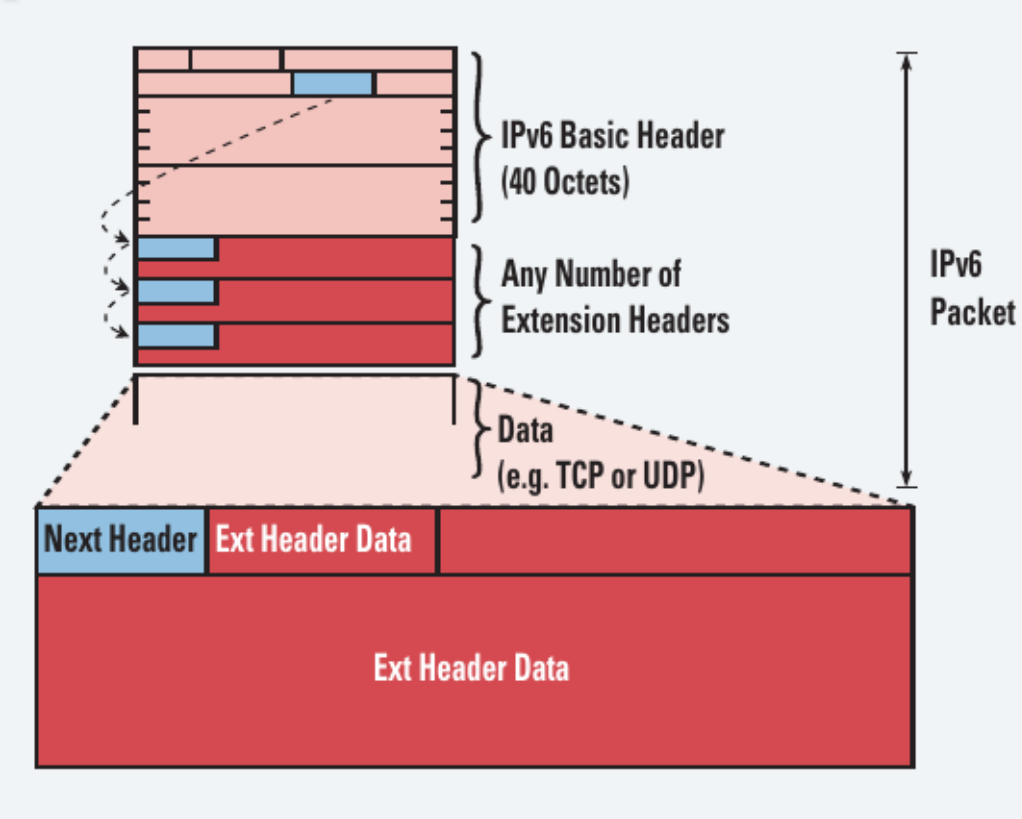
IPv4 *versus* IPv6[24]





[24] Cisco IPv6 headers at a glance

IPv6 – struktura pakietu[25]



[25] Cisco IPv6 headers at a glance

Adresy IPv6

- *unicast* (adres pojedynczej emisji, adres jednostkowy):
  - adres dostawcy usług internetowych (ISP, *Internet Service Provider*)
  - adres użytku lokalnego dla łącza przeznaczony dla pojedynczego łącza (*link-local unicast address*)
  - adresy użytku lokalnego dla miejsca przeznaczone do stosowania w miejscach i organizacjach, które nie są przyłączone do globalnego Internetu (*site-local unicast address*); RFC 3879 *Deprecating Site Local Addresses*; RFC 4193 zaleca stosowanie adresów typu *Unique Local Address* (FD00::/8)
  - adres IPv6 zgodny z IPv4 niezbędny z uwagi na tunelowanie IPv6 przez sieć IPv4
  - adres IPv6 wzorowany na IPv4 niezbędny z uwagi na tunelowanie IPv4 przez sieć IPv6 (adresy tymczasowe tylko dla routerów)

Adresy IPv6

- *anycast* (adres dowolnej emisji, adres grona)

  Pojedyncza wartość przypisana do więcej niż jednego interfejsu (zwykle różnych urządzeń). Pakiet wysłany na adres anycast jest trasowany tylko do jednego urządzenia najbliższego wg pewnej miary odległości. Jeśli dwaj użytkownicy wysyłają z różnych miejsc sieci datagramy pod ten sam adres, to mogą one docierać i być jednocześnie obsługiwane przez różne urządzenia sieciowe.

  Adres tego typu jest składniowo identyczny z adresem *unicast*.

- *multicast* (adres rozgłoszenia grupowego)

  Udostępnia ogromną liczbę adresów grup multicastowych. Adresy te mogą mieć zasięg globalny, mogą być powiązane z danym miejscem lub łączem sieciowym dzięki obecności 4 bitów określających tzw. *multicast scoping*. Są m.in. wykorzystywane do autokonfiguracji hostów oraz wykrywania najlepszych tras (wykrywania routerów).

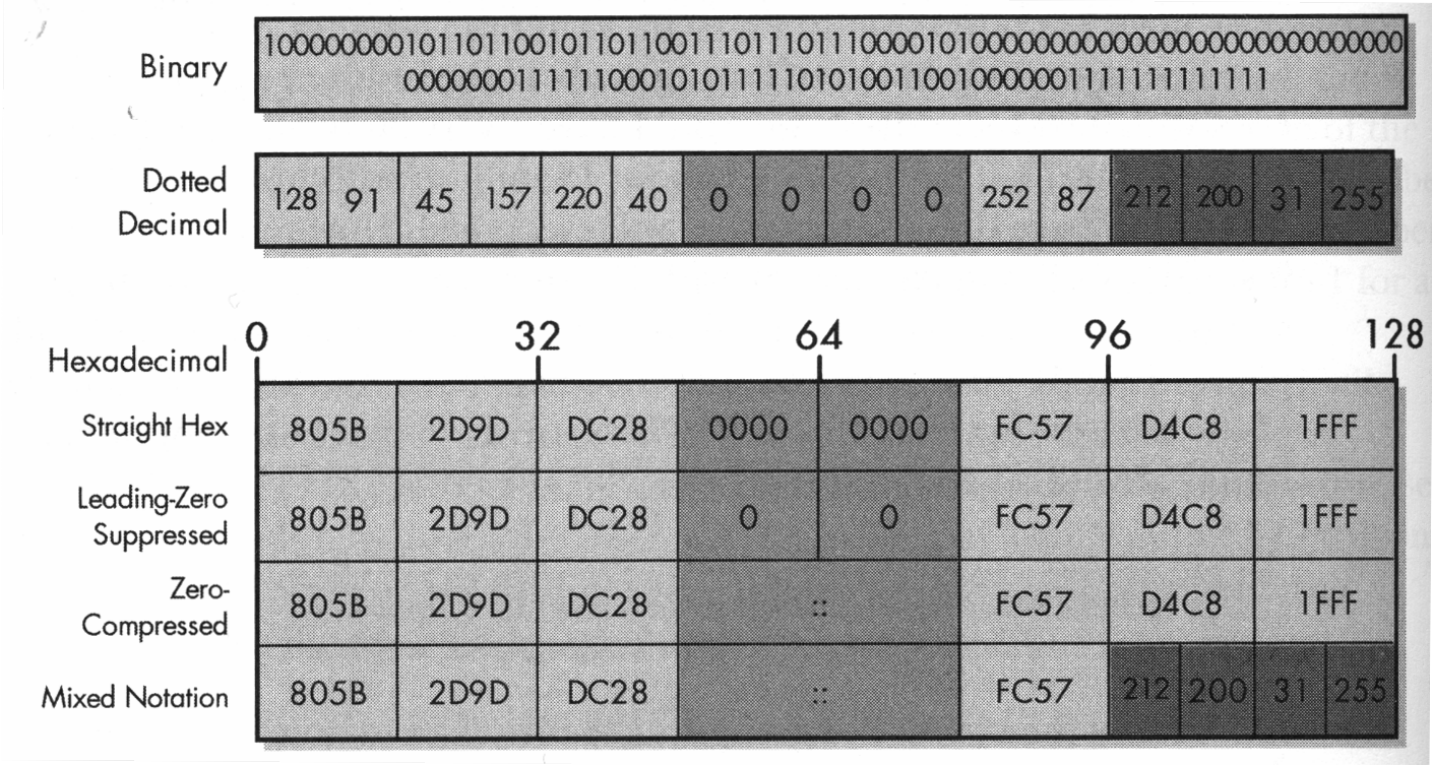
Adresy IPv6

128-bitowy adres IPv6 (16 oktetów) zapisuje się jako 8 liczb całkowitych bez znaku, gdzie każda liczba składa się z 4 cyfr szestnastkowych, np.: 1060:0000:0000:0000:0004:0400:200C:617B.

Zapis adresu można uprościć pomijając początkowe zera, np.: 1060::4:400:200C:617B.

Podsieci określa sie poprzez podanie prefiksu, który określa liczbę bitów przeznaczoną na numer podsieci, np.: 1060:0:0:abcd:001e:0400:200C:617B/60.

IPv6 – format zapisu adresów[26]



[26] C.M.Kozierok, TCP/IP Guide

Adresy IPv6: struktura przestrzeni adresowej[27]

0000::/8	zarezerwowane przez IETF
0100::/8	zarezerwowane przez IETF
0200::/7	zarezerwowane przez IETF
0400::/6	zarezerwowane przez IETF
0800::/5	zarezerwowane przez IETF
1000::/4	zarezerwowane przez IETF
2000::/3	przydzielone adresy globalne pojedynczej emisji (0010:: - 0011 1111 1111 1111)
2001:0DB8::/32	dokumentacja i przykłady (także testowanie)
2002::/16	adresy 6to4
4000::/2	zarezerwowane adresy globalne
...	...
FD00::/8	unikatowe, lokalne adresy pojedynczej emisji (*unique local unicast*); zamiast *site-local*
FE80::/10	adresy pojedynczej emisji lokalnego łącza (*link-local*)
FF00::/8	adresy rozgłoszenia grupowego

[27] Internet Protocol Version 6 Address Space, TCP/IP Guide: IPv6 Address Space Allocation

Adresy IPv6 rozgłoszeń grupowych[28]

Node-Local Scope Multicast Addresses	
FF01:0:0:0:0:0:0:1	All Nodes Address
FF01:0:0:0:0:0:0:2	All Routers Address
FF01:0:0:0:0:0:0:C	variable scope allocation
FF01:0:0:0:0:0:0:FB	mDNSv6

Link-Local Scope Multicast Addresses	
FF02:0:0:0:0:0:0:1	All Nodes Address
FF02:0:0:0:0:0:0:2	All Routers Address
FF02:0:0:0:0:0:0:3	Unassigned
FF02:0:0:0:0:0:0:4	DVMRP Routers
FF02:0:0:0:0:0:0:5	OSPFIGP
FF02:0:0:0:0:0:0:6	OSPFIGP Designated Routers
FF02:0:0:0:0:0:0:7	ST Routers
FF02:0:0:0:0:0:0:8	ST Hosts
FF02:0:0:0:0:0:0:9	RIP Routers
FF02:0:0:0:0:0:0:A	EIGRP Routers

[28] IPv6 Multicast Address Space Registry

Adresy IPv6 pojedynczej emisji

Pierwszych 48 bitów określa adres sieci, kolejnych 16 – adres podsieci, a ostatnie 64 bity są związane z identyfikatorem interfejsu.

Jest to tzw. adres łącza (*link address*).

Adres łącza może być generowany w trybie

- EUI-64 (*Extended Unique Identifier*)

  Np. adres 00:16:3e:00:00:02 przechodzi w 00:16:3e:ff:fe:00:00:02, a po zmianie bitu 6-go (numeracja 0..7) w adres 02:16:3e:ff:fe:00:00:02.

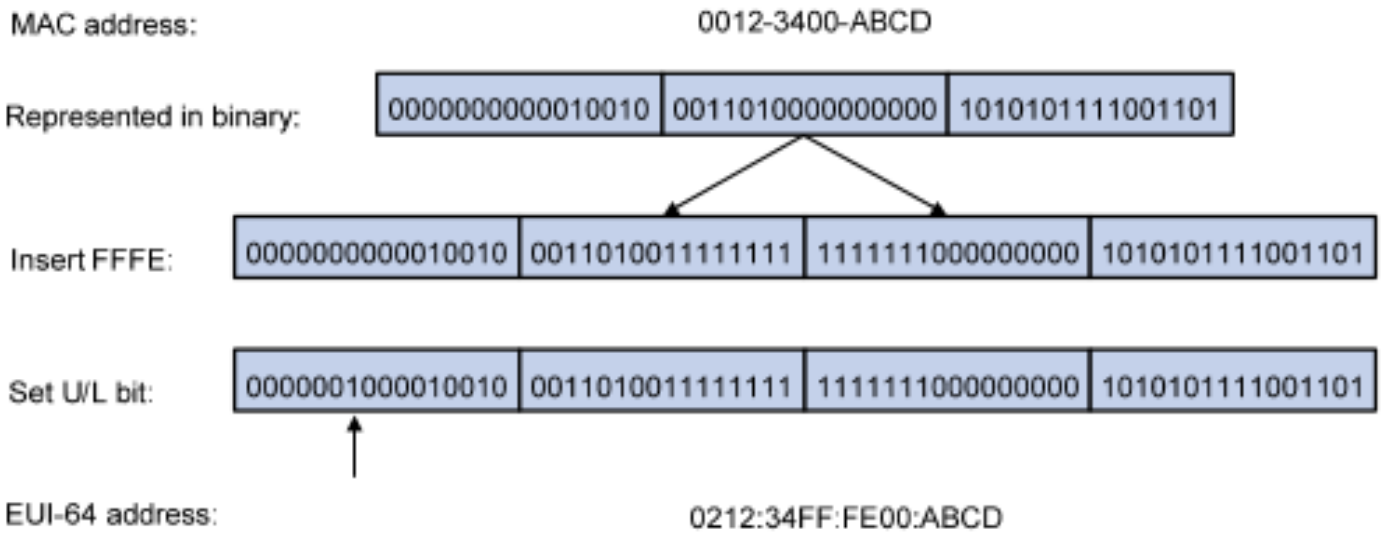
  Po dodaniu prefiksu FE80 otrzymujemy adres pojedynczej emisji dla łącza lokalnego: fe80::0216:3eff:fe00:0002 (fe80::216:3eff:fe00:2).

```
$ ipv6calc --in mac --action geneui64 --out eui64 00:16:3e:00:00:02
216:3eff:fe00:2
```

- STABLE_PRIVACY, adres hosta pozostaje niezależny od sprzętu, czyli adresu MAC

Adresy IPv6

Zamiana adresu MAC na (zmodyfikowany) adres EUI-64



Adresy IPv6: EUI-64 vs STABLE-PRIVACY

```
[root@hel ~]# ip add show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
    link/ether 54:52:00:05:00:90 brd ff:ff:ff:ff:ff:ff
    inet 158.75.5.90/23 brd 158.75.5.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 2001:470:617a:1111:5652:ff:fe05:90/64 scope global mngtmpaddr dynamic
       valid_lft 40sec preferred_lft 40sec
    inet6 fe80::5652:ff:fe05:90/64 scope link
       valid_lft forever preferred_lft forever
root@tor7 ~/bin]# ip add show eth0

[root@tor7 ~]# ip add show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group d
    link/ether 54:52:00:05:00:91 brd ff:ff:ff:ff:ff:ff
    inet 158.75.5.91/23 brd 158.75.5.255 scope global noprefixroute dynamic eth0
       valid_lft 62617sec preferred_lft 62617sec
    inet6 2001:470:617a:1111:c3e0:3db0:ad95:3073/64 scope global noprefixroute dynami
       valid_lft 12sec preferred_lft 12sec
    inet6 fe80::5344:46b9:c984:6b7c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Adresy IPv6: konfiguracja

Fazy bezstanowej konfiguracji urządzenia sieciowego w IPv6:

1. generowanie adresu typu *link-local*
2. sprawdzanie, czy adres nie jest używany przez inne urządzenia (unikatowość adresu)
3. przypisanie unikatowego adresu do interfejsu; możliwa komunikacja w ramach lokalnej sieci
4. urządzenie sieciowe komunikuje się z routerem (*router solicit*), żeby otrzymać instrukcję, co do dalszego sposobu autokonfiguracji
5. urządzenie sieciowe otrzymuje od routera instrukcję (*router advertisement*), co do dalszego sposobu autokonfiguracji
6. urządzenie sieciowe konfiguruje się z adresem globalnie jednoznacznym, który składa się z prefiksu sieciowego dostarczonego przez router oraz identyfikatora urządzenia

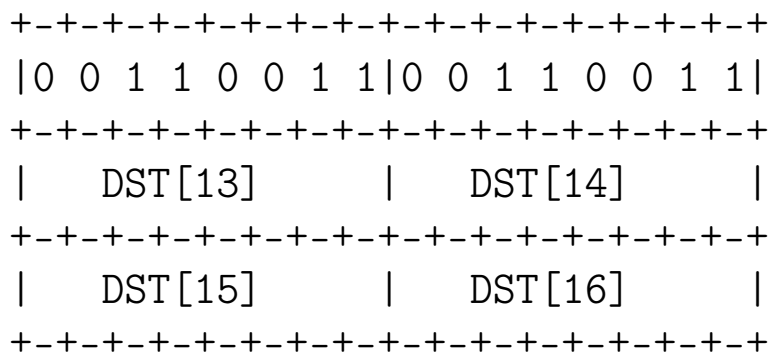
Adresy IPv6: NDP

Network Discovery Protocol (NDP) jest oparty o ICMPv6 i jest używany w procesie autokonfiguracji urządzenia sieciowego. Wykorzystuje do tego adresy typu *unicast* oraz *multicast* oraz 9 funkcji:

- wykrywania routera, prefiksu (sieciowej porcji adresu IPv6), parametrów sieci (MTU) i routera (*Hop Limit*), autokonfiguracja adresu
- odwzorowywania adresu, określanie adresu następnego routera, wykrywanie nieosiągalnego sąsiada i podwójnego adresu
- przekierowywania

Jak mapować adresy IPv6 na IEEE 802.2?[29]

An IPv6 packet with a multicast destination address DST, consisting of the sixteen octets DST[1] through DST[16], is transmitted to the Ethernet multicast address whose first two octets are the value 3333 hexadecimal and whose last four octets are the last four octets of DST.



[29] Transmission of IPv6 Packets over Ethernet Networks

Konfiguracja interfejsów sieciowych: adresy multicast

```
# ip -6 maddress show
1: lo
inet6 ff12::8384
inet6 ff02::fb
inet6 ff02::1
inet6 ff01::1
2: eth0
inet6 ff12::8384
inet6 ff02::1
inet6 ff01::1
3: wlan0
inet6 ff02::1:3
inet6 ff02::fb
inet6 ff02::1:ff7b:1565
inet6 ff12::8384
inet6 ff02::1
inet6 ff01::1
```

`ff01::1` – *interface-local scope address (loopback address)*

`ff02::1` – *all hosts multicast address*

`ff02::fb` – *multicast DNS IPv6*

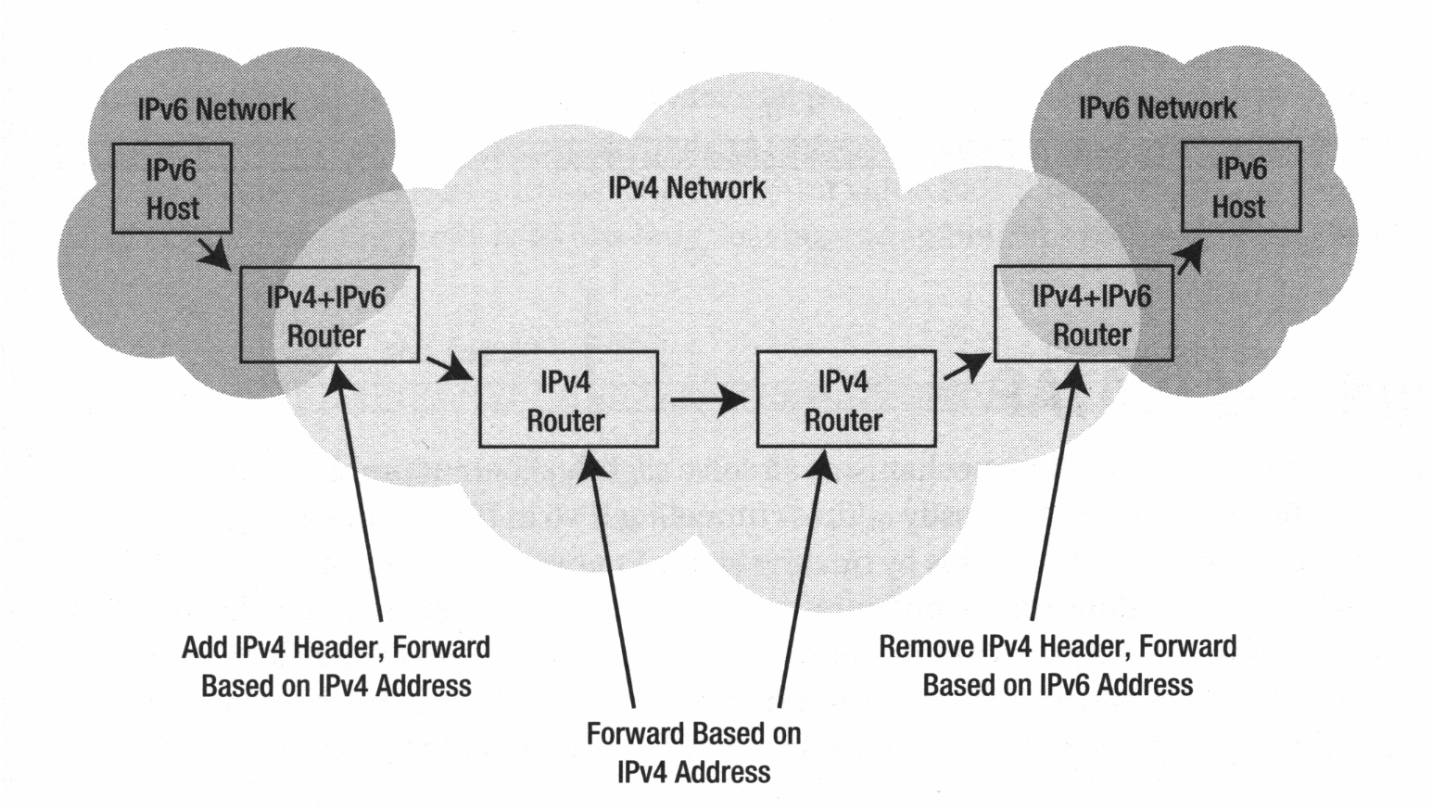
Konfiguracja interfejsów sieciowych: adresy multicast

```
# ip -6 maddress show # router wyłączony
...
4:      br0
        inet6 ff02::1:ff80:a0e4
        inet6 ff02::1
        inet6 ff01::1
...

# ip -6 maddress show # router włączony
...
4:      br0
        inet6 ff02::1:ff00:0 users 2
        inet6 ff05::2
        inet6 ff01::2
        inet6 ff02::2 users 2
        inet6 ff02::1:ff80:a0e4 users 2
        inet6 ff02::1
        inet6 ff01::1
...
```

`ff02::2` – *all routers multicast address*

`ff05::2` – *site-local scope multicast address*

Tunelowanie ruchu IPv6[30]




```
ip tunnel add he-ipv6 mode sit remote $remoteIPv4 local $localIPv4
```

[30] Iljitsch van Beijnum, *Running Ipv6*, Apress, 2006, s.33

Adresy IPv6: użycie

```
$ ipcalc 2001:470:70:110b:5652:ff:fe05:226/64
$ sipcalc -t 2001:470:70:110b:5652:ff:fe05:226/64

$ ipv6calc -qi 2001:470:70:110b:500b:d309:7170:d5ae/64
$ ipv6calc -qi 2001:470:70:110b:5652:ff:fe05:226/64

$ ipv6calc -qi fe80::0216:3eff:fe00:0002
$ ipv6calc -qi fe80::5344:46b9:c984:6b7c

$ ipv6calc --showinfo [-m] 2002:9e4b:5fe:0:204:23ff:fed0:2032/64
$ ipv6calc --in mac --action geneui64 --out eui64 00:16:3e:00:00:02
$ ipv6calc --in ipv4addr 158.75.5.254 --action conv6to4 --out ipv6addr

$ ping6         fe80::204:23ff:fed0:2032%eth0
$ ping6 -I eth0 fe80::204:23ff:fed0:2032
$ tracepath6    fe80::204:23ff:fed0:2032
$ ssh [-6]      2002:9e4b:5fe:0:215:c5ff:feb1:9a8a
```

Adresy IPv6: użycie

```
ipv6calc -qi 2001:470:617a:1111:a236:9fff:fe80:a0e4/64
Address type: unicast, global-unicast, productive, iid, iid-global, iid-eui48
Country Code: US
Registry for address: ARIN
Address type has SLA: 1111
Interface identifier: a236:9fff:fe80:a0e4
EUI-48/MAC address: a0:36:9f:80:a0:e4
MAC is a global unique one
MAC is an unicast one
OUI is: Intel Corporate
GeoIP (MaxMindDB) reports Continent Code: NA
GeoIP (MaxMindDB) reports Continent Name: North America
GeoIP (MaxMindDB) reports Country Code: US
GeoIP (MaxMindDB) reports Country Name: United States
GeoIP (MaxMindDB) reports Latitude: 37.751000
GeoIP (MaxMindDB) reports Longitude: -97.822000
GeoIP (MaxMindDB) reports Accuracy Radius: 100
GeoIP (MaxMindDB) reports Time Zone Name: America/Chicago
GeoIP (MaxMindDB) reports Geoname ID of Country: 6252001
GeoIP (MaxMindDB) reports Geoname ID of Continent: 6255149
GeoIP database:(MaxMindDB) GeoLite2-City Copyright (c) 2019 MaxMind All Rights Reserv
Built-In database: IPv6-REG:AFRINIC/20221204 APNIC/20221202 ARIN/20221203 IANA/201911
```

Adresy IPv6: użycie

```
$ ipv6calc -qi 2a00:1450:401b:80d::2004
Address type: unicast, global-unicast, productive, iid, iid-local
Country Code: IE
Registry for address: RIPENCC
Address type has SLA: 080d
Interface identifier: 0000:0000:0000:2004
Interface identifier is probably manual set
GeoIP (MaxMindDB) reports Continent Code: EU
GeoIP (MaxMindDB) reports Continent Name: Europe
GeoIP (MaxMindDB) reports Country Code: IE
GeoIP (MaxMindDB) reports Country Name: Ireland
GeoIP (MaxMindDB) reports Latitude: 53.000000
GeoIP (MaxMindDB) reports Longitude: -8.000000
GeoIP (MaxMindDB) reports Accuracy Radius: 100
GeoIP (MaxMindDB) reports Time Zone Name: Europe/Dublin
GeoIP (MaxMindDB) reports Geoname ID of Country: 2963597
GeoIP (MaxMindDB) reports Geoname ID of Continent: 6255148
GeoIP database:(MaxMindDB) GeoLite2-City Copyright (c) 2019 MaxMind All Rights Reserv
Built-In database: IPv6-REG:AFRINIC/20211019 APNIC/20211019 ARIN/20211019 IANA/201911
```

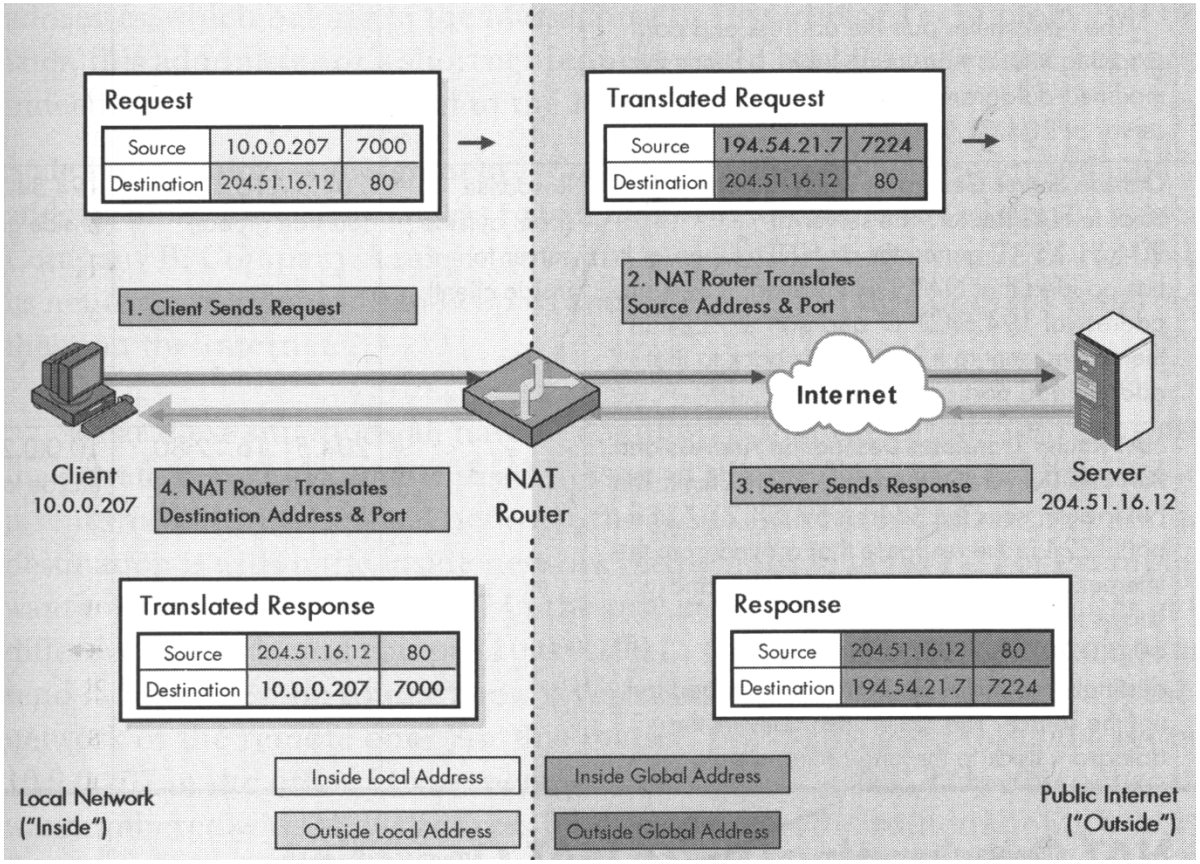
NAT – translacja adresów sieciowych

Adresy IPv4 są towarem deficytowym. W niektórych częściach Internetu ich pula się wyczerpała. Braki są skutkiem wzrostu zapotrzebowania na adresy IP oraz przydzielania użytkownikom (ISP) klas B zamiast C, co powoduje marnowanie się adresów (ponad połowa klas B korzysta z mniej niż 50 adresów!).

Rozwiązaniem jest przejście na adresację IPv6, ale migracja następuje powoli. Jako rozwiązanie tymczasowe zaproponowano translację adresów sieciowych (NAT, *Network Address Translation*) opisaną w RFC 3022.

W ramach tego rozwiązania użytkownik (firma, ISP, etc) otrzymuje jeden, ew. kilka publicznych numerów IP, pod którymi widoczny jest cały ruch generowany przez jego komputery pracujące w wydzielonej, wewnętrznej sieci i wykorzystujące do komunikacji sieciowej adresy prywatne. Wszystkie pakiety wychodzące z sieci wewnętrznej do Internetu muszą być poddawane operacji zamiany adresów źródłowych (z prywatnych na publiczne) przez tzw. konwerter NAT.

NAT – translacja adresów sieciowych[31]



[31] C.M.Kozierok, TCP/IP Guide

NAT – translacja adresów sieciowych

Wady:

- poważne naruszenie architektury IP: każdy adres odpowiada w skali globalnej powinien odpowiadać pojedynczemu komputerowi
- komunikacja w ramach protokołu bezpołączeniowego nabiera charakteru połączeniowego (konwerter NAT przechowuje informacje o połączeniach)
- pogwałcenie reguły warstwowości: funkcjonowanie jednej warstwy nie może zależeć od zmian w nagłówku innej warstwy
- zależność działania usług od protokołów TCP i UDP
- niektóre aplikacje wstawiają adres IP do ładunku pakietu, np. FTP (NAT nic o tym nie wie!)

IPv6 oferuje IPv6-to-IPv6 Network Prefix Translation (NPTv6) w celu zamiany jednoznacznych (unikatowych) adresów lokalnych (ULA) na adresy globalnie jednoznaczne (GUA).

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):

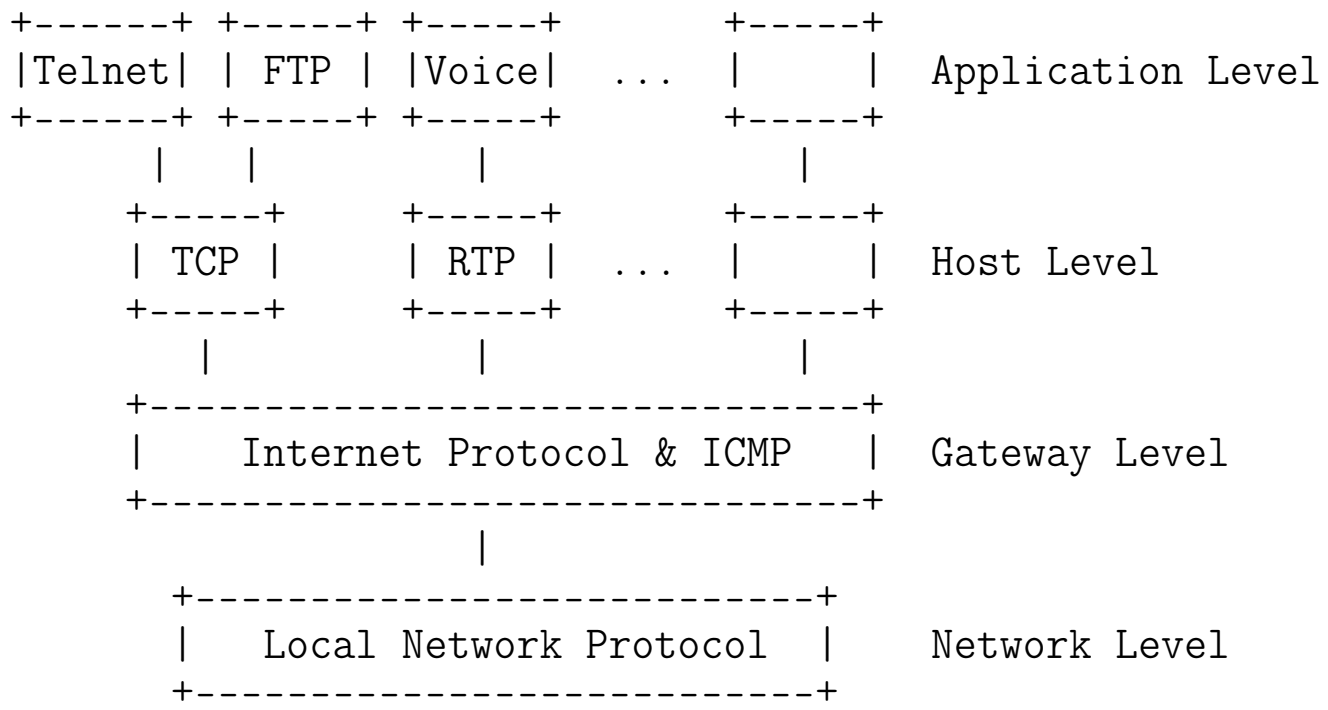
- HTTP (*HyperText Transport Protocol*) protokół przesyłania hipertekstu
- TELNET (*Network Terminal Protocol*) protokół końcówki sieciowej (wirtualnego terminala)
- SSH (*Secure SHell*) bezpieczna powłoka
- FTP (*File Transfer Protocol*) protokół przesyłania plików
- NFS (*Network File System*) sieciowy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

TCP

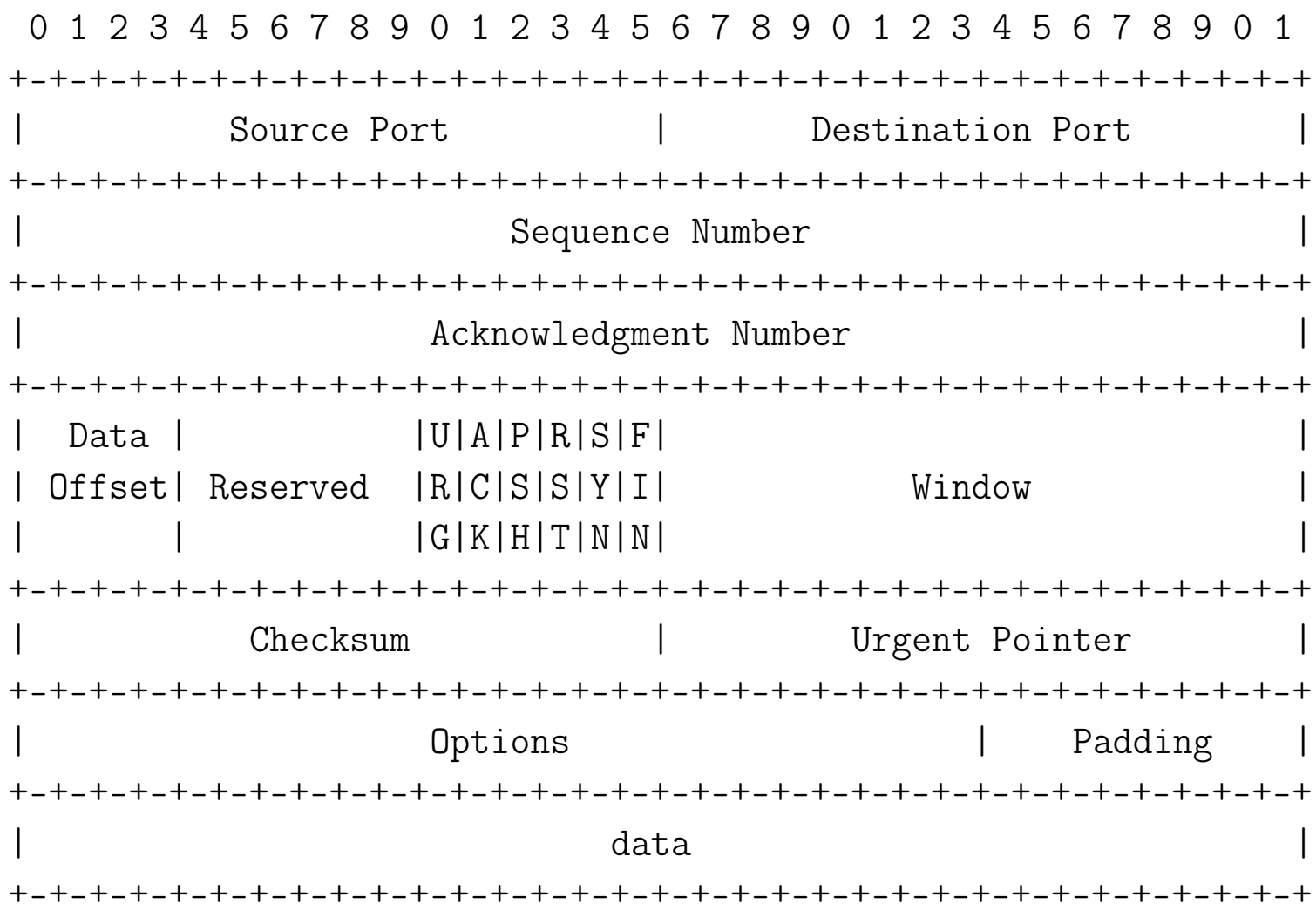
Wg RFC 793, 1.5. Operation:

```
... 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



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.

TCP: trójetapowa synchronizacja 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: trójetapowa synchronizacja połączenia

```
    TCP A                                                TCP B

1.  CLOSED                                               LISTEN

2.  SYN-SENT    --> <SEQ=100><CTL=SYN>               --> SYN-RECEIVED

3.  ESTABLISHED <-- <SEQ=300><ACK=101><CTL=SYN,ACK>  <-- SYN-RECEIVED

4.  ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK>       --> ESTABLISHED

5.  ESTABLISHED --> <SEQ=101><ACK=301><CTL=ACK><DATA> --> ESTABLISHED
```

Basic 3-Way Handshake for Connection Synchronization

TCP: pozytywne potwierdzenie z retransmisją

Niezawodność dostarczania danych – mechanizm pozytywnego potwierdzenia z retransmisją (*Positive Acknowledgement with Retransmission*, PAR).

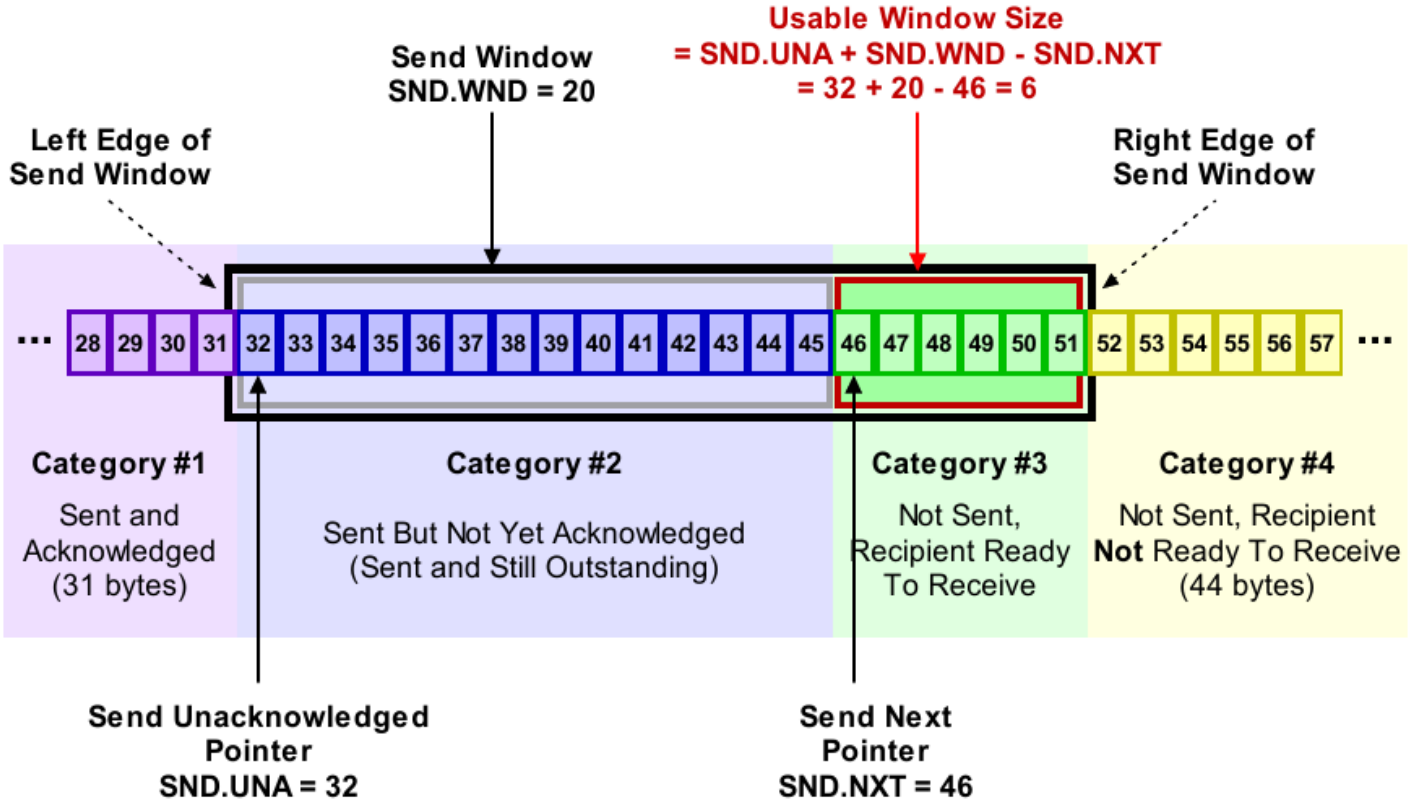
- Dane wysyłane są tak długo, aż nie nadejdzie potwierdzenie, że zostały poprawnie odebrane.
- Jeśli dane są poprawne, to odbiorca wysyła do nadawcy *pozytywne potwierdzenie*.
- Gdy odebrane dane są niepoprawne, to zostają zignorowane. Po określonym (jak?) czasie moduł nadający powtórnie wysyła dane.
- Odbiorca wysyła nadawcy informację o maksymalnej liczbie bajtów, które wolno wysłać bez czekania na potwierdzenie (**rozmiar okna**). Wartość 0 wstrzymuje nadawanie, a nadawca ustawia wartość czasomierza „nie ustępuj" (*Persist Timer*).[32]

[32] RFC 1323 wprowadza opcję *Scale Window*, która pozwala na wynegocjowanie przez strony połączenia 30. bitowego rozmiaru okna, czyli ustalenia wielkości bufora rzędu 1 GB. Wskutek tego pasmo zmienia się z 2^{16}/RTT do 2^{30}/RTT, czyli $2^{14} = 16384$ razy.

TCP: sterowanie przepływem

- 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

TCP: przesuwne okna[33]



[33] C.M.Kozierok, TCP/IP Guide

TCP: maksymalna wielkość segmentu

TCP został zaprojektowany w taki sposób, aby można było ograniczyć wielkość segmentu do rozmiaru pozwalającego uniknąć fragmentacji pakietu na poziomie warstwy sieciowej. Parametr MSS (*Maximum Segment Size*) określa maksymalną liczbę bajtów w polu danych segmentu TCP. Ponieważ domyślną wartością MTU jest 576 bajtów, więc przy założeniu, że nagłówki TCP i IP mają po 20 bajtów każdy, domyslnie MSS wynosi 536 bajtów (MTU-40).

Zmiana domyślnej wartości MSS może zostać wymuszona przez każdą z komunikujących się stron poprzez zastosowanie w segmencie SYN opcji *Maximum Segment Size*. Każda ze stron może używać innej wartości MSS.

Stream Control Transmission Protocol (SCTP, RFC2960)

Cechy strumieniowego protokołu sterowania transmisją:

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

SCTP: struktura pakietu[34]

Bits	Bits 0 - 7	8 - 15	16 - 23	24 - 31
+0	Source port		Destination port	
32	Verification tag			
64	Checksum			
96	Chunk 1 type	Chunk 1 flags	Chunk 1 length	
128	Chunk 1 data			
...	...			
...	Chunk N type	Chunk N flags	Chunk N length	
...	Chunk N data			

[34] SCTP packet structure

Sterowanie zatorami w TCP/IP[35]

Problem: Jeśli węzeł jest przeciążony, pojawiają się zatory i router zaczyna porzucać pakiety.

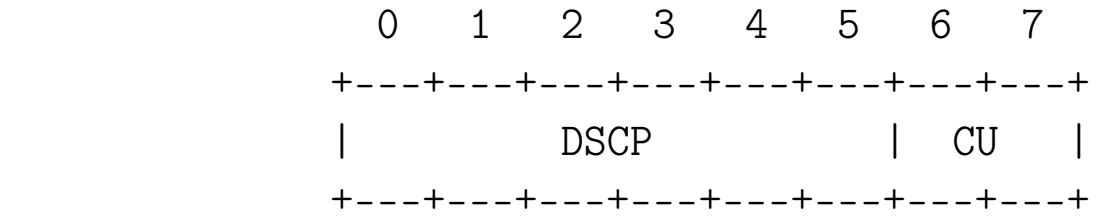
Rozwiązanie: Wykorzystać nieużywane bity nagłówków protokółów IP i TCP do przekazania wiadomości od routera do nadawcy pakietów poprzez odbiorcę pakietów:

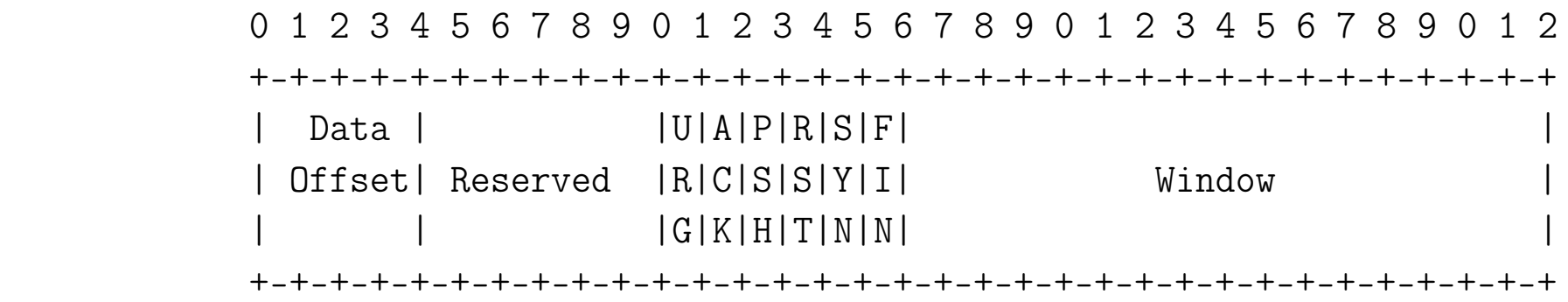
- nagłówek TCP: pole *Reserved*
  - bit 8 - CWR *Congestion Window Reduced*
  - bit 9 - ECE *Explicit Congestion Notification (ECN) Echo*
- nagłówek IP: pole *Traffic Class*
  - bit 6: ECN *Capable Transport*
  - bit 7: Congestion Experienced (CE)

Pakiety nie są porzucane, ale nadawca zmniejsza dwukrotnie tzw. okno zatorów, co powoduje zmniejszenie tempa wysyłania pakietów.

[35] TCP congestion control

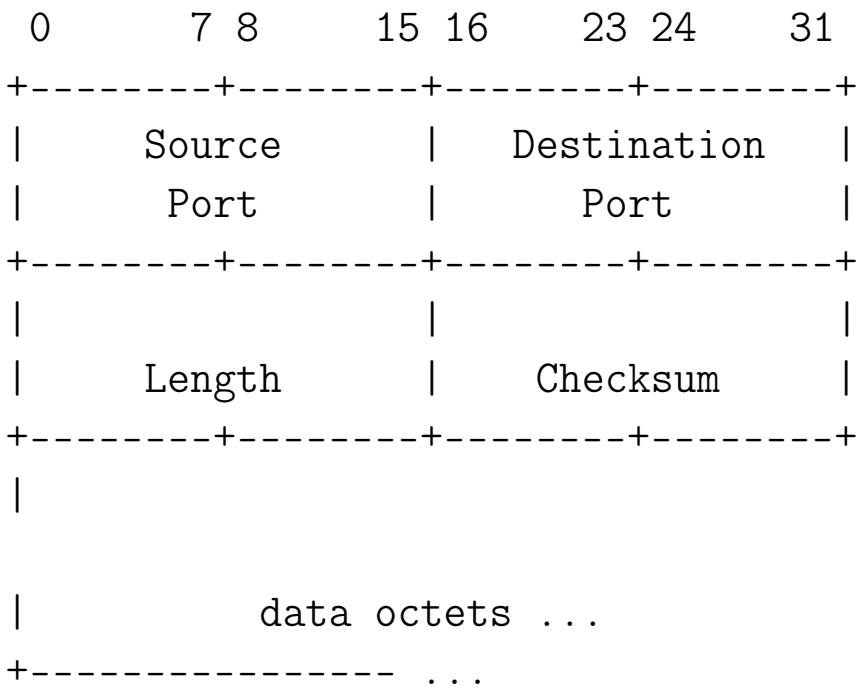
Sterowanie zatorami w TCP/IP





User Datagram Protocol (UDP, RFC 768)

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



User Datagram Protocol

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

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

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)

Gniazda

Interfejs gniazd (*socket interface*) – mechanizm umożliwiający komunikowanie się procesów w tym samym systemie lub procesów działających na różnych hostach w sieci.
System gniazd Linuxa jest rozszerzoną wersją systemu gniazd z Unixa 4.3 BSD i wspiera m.in. następujące dziedziny adresów (*Address Family*):

- AF_UNIX/AF_LOCAL – komunikacja lokalna
- AF_INET/AF_INET6 – protokoły internetowe IPv4/IPv6
- AF_NETLINK – *kernel user interface device*
- AF_IPX – Novell IPX
- AF_APPLETALK – Appletalk DDP (*Datagram Delivery Protocol*)
- AF_X25 – protokoły ITU-T X.25
- AF_AX25 – protokół AX.25 dla radia amatorskiego
- AF_PACKET – interfejs niskiego poziomu dla pakietów
- AF_ALG – interface do API podsystemu szyfrowania

Rodzaje gniazd (man socket)

SOCK_STREAM
: Provides sequenced, reliable, two-way, connection-based byte streams. An out-of-band data transmission mechanism may be supported.

SOCK_DGRAM
: Supports datagrams (connectionless, unreliable messages of a fixed maximum length).

SOCK_SEQPACKET
: Provides a sequenced, reliable, two-way connection-based data transmission path for datagrams of fixed maximum length; a consumer is required to read an entire packet with each read system call.

SOCK_RAW
: Provides raw network protocol access.

SOCK_RDM
: Provides a reliable datagram layer that does not guarantee ordering.

IANA i /etc/services

```
# /etc/services:
# $Id: services,v 1.49 2017/08/18 12:43:23 ovasik Exp $
#
# Network services, Internet style
# IANA services version: last updated 2016-07-08
#
# 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
```

```
http            80/sctp                         # HyperText Transfer Protocol
...
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
```

```
#>The Registered Ports are listed by the IANA and on most systems can be used by ordi
#>user processes or programs executed by ordinary users.
socks           1080/tcp                        # socks proxy server
socks           1080/udp                        # socks proxy server
...
openvpn         1194/tcp                        # OpenVPN
openvpn         1194/udp                        # OpenVPN
...
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 S
wins            1512/udp                        # Microsoft's Windows Internet Name S
...
x11             6000/tcp        X               # the X Window System
```

Zob.: Service Name and Transport Protocol Port Number Registry

Jak działa serwer sieciowy?[36]

```
...
int main( int argc, char *argv[] )
{ ...
  /* First call to socket() function */
  sockfd = socket(AF_INET, SOCK_STREAM, 0);
  if (sockfd < 0) {perror("ERROR opening socket"); exit(1);}

  /* Initialize socket structure */
  bzero((char *) &serv_addr, sizeof(serv_addr));
  portno = 51001;
  serv_addr.sin_family = AF_INET;
  serv_addr.sin_addr.s_addr = INADDR_ANY;
  serv_addr.sin_port = htons(portno);

  /* Now bind the host address using bind() call.*/
  if (bind(sockfd, (struct sockaddr *) &serv_addr, sizeof(serv_addr)) < 0)
    { perror("ERROR on binding"); exit(1); }

  /* Now start listening for the clients, here process will go in sleep mode */
  /* and will wait for the incoming connection  */
```

[36] `/git/tm-scripts`, Unix Socket - Server Examples

```
  listen(sockfd,5);
  clilen = sizeof(cli_addr);

  /* Accept actual connection from the client */
  newsockfd = accept(sockfd, (struct sockaddr *)&cli_addr, &clilen);
  if (newsockfd < 0) {perror("ERROR on accept"); exit(1);}

  /* If connection is established then start communicating */
  bzero(buffer,256);
  n = read( newsockfd,buffer,255 );
  if (n < 0) {perror("ERROR reading from socket"); exit(1);}

  printf("Here is the message: %s\n",buffer);

  /* Write a response to the client */
  n = write(newsockfd,"I got your message.\n",21);

  if (n < 0) {perror("ERROR writing to socket"); exit(1);}
  return 0;
}
```

Gniazda i połączenia: skrypt `ncatctl`[37]

```
...
host=localhost
port=51001
nmesg=1000

mesg="server: message #"                    |    mesg="client: message #"
if [[ $1 == server-send ]]                  |    if [[ $1 == "client-send" ]]
then                                        |    then
    (                                       |        (
        for i in $(seq $nmesg)              |            for i in $(seq $nmesg)
        do                                  |            do
            sleep 1                         |                sleep 1
            echo "$mesg $i"                 |                echo "$mesg $i"
        done |ncat -k -l $host $port        |            done |ncat $host $port
    )&                                      |        )
    exit                                    |        exit
fi                                          |    fi
...
```

[37] /git/tm-scripts

Monitorowanie usług i połączeń[38]

```
# ss -np                                |   # ss -u [-a]
# ss -npt                               |   # ss -t [-a]
# ss -npu                               |   # ss -tap [-n]
# ss -npl                               |   # ss -s
# ss -nptl                              |   # ss -tn -o
# ss -npul                              |   # ss -nl4 [-f inet]
# ss -4 -t state time-wait              |   # ss -t  dst 158.75.5.226
# ss -4|6 -t state established          |   # ss -nt dst :443 or dst :80
# ss -o state established '( dport = :443 or sport = :443 )'
```

[38]Komenda `ss` zastąpiła przestarzałą komendę `netstat`.

Monitorowanie usług i połączeń

```
#  ss -tap
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
LISTEN     0      3          *:tinc               *:*                    users:(("tincd",pid=22885,
LISTEN     0      128        *:sunrpc             *:*                    users:(("rpcbind",pid=2401
LISTEN     0      10     127.0.0.1:domain         *:*                    users:(("named",pid=4159,f
LISTEN     0      128        *:ssh                *:*                    users:(("sshd",pid=1309,fd
LISTEN     0      5      127.0.0.1:ipp            *:*                    users:(("cupsd",pid=1307,f
LISTEN     0      128    127.0.0.1:rndc           *:*                    users:(("named",pid=4159,f
LISTEN     0      100    127.0.0.1:smtp           *:*                    users:(("master",pid=1887,
LISTEN     0      128        *:db-lsp             *:*                    users:(("dropbox",pid=3334
LISTEN     0      128    127.0.0.1:17600          *:*                    users:(("dropbox",pid=3334
CLOSE-WAIT 32     0      192.168.2.103:32848      162.125.66.3:https     users:(("dropbox",pid=3334
CLOSE-WAIT 1      0      192.168.2.103:35440      52.73.106.131:https    users:(("dropbox",pid=3334
ESTAB      0      0      192.168.2.103:51264      172.217.20.206:https   users:(("opera",pid=5314,f
CLOSE-WAIT 32     0      192.168.2.103:52444      108.160.172.204:https  users:(("dropbox",pid=3334
ESTAB      0      0      192.168.2.103:41252      162.125.18.133:https   users:(("dropbox",pid=3334
CLOSE-WAIT 32     0      192.168.2.103:39118      108.160.172.225:https  users:(("dropbox",pid=3334
LISTEN     0      10        :::domain             :::*                   users:(("named",pid=4159,f
LISTEN     0      128       :::ssh                :::*                   users:(("sshd",pid=1309,fd
ESTAB      0      0      172.20.1.25:35498        158.75.5.226:ssh       users:(("ssh",pid=5025,fd=
 ...
```

Monitorowanie usług i połączeń

```
# ss -nt -o
State      Recv-Q Send-Q Local Address:Port      Peer Address:Port
CLOSE-WAIT 1      0      192.168.2.103:41130     54.239.31.63:443       timer:(keepalive,8.852ms,0)
ESTAB      0      0      192.168.2.103:50092     199.16.156.120:443     timer:(keepalive,32sec,0)
CLOSE-WAIT 32     0      192.168.2.103:52444     108.160.172.204:443
ESTAB      0      0      192.168.2.103:58416     173.194.73.189:443     timer:(keepalive,7.209ms,0)
ESTAB      0      0      172.20.1.25:35498       158.75.5.226:22        timer:(keepalive,104min,0)
CLOSE-WAIT 1      0      192.168.2.103:58356     34.196.150.80:443
ESTAB      0      0      192.168.2.103:41252     162.125.18.133:443
```

```
# 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
```

Stany gniazda TCP (man ss|netstat)

ESTABLISHED The socket has an established connection
(normalny stan transmisji danych).

SYN_SENT The socket is actively attempting to establish a connection
(proces rozpoczyna nawiązywanie połączenia).

SYN_RECV A connection request has been received from the network
(otrzymano żądanie połączenia; oczekiwanie na ACK).

FIN_WAIT1 The socket is closed, and the connection is shutting down
(proces sygnalizuje zakończenie wysyłania danych).

FIN_WAIT2 Connection is closed, and the socket is waiting for a shutdown
from the remote end (druga strona zgadza się na zwolnienie połączenia).

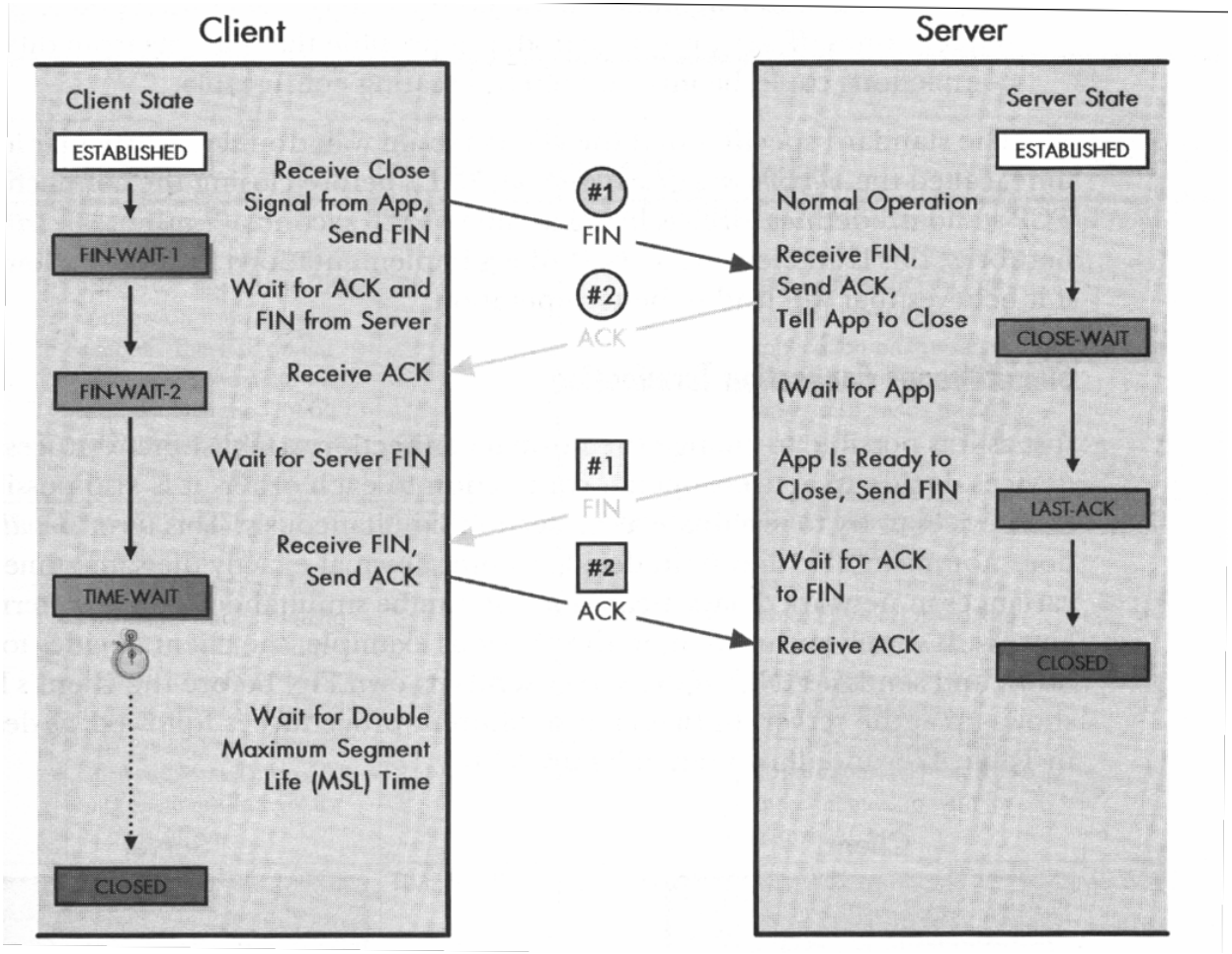
TIME_WAIT The socket is waiting after close to handle packets still
in the network (oczekiwanie na wygaśnięcie wszystkich pakietów).

LISTEN The socket is listening for incoming connections
(serwer oczekuje na żądanie połączenia).

CLOSED The socket is not being used
(brak aktywnych połączeń i nieobsłużonych żądań połączenia).

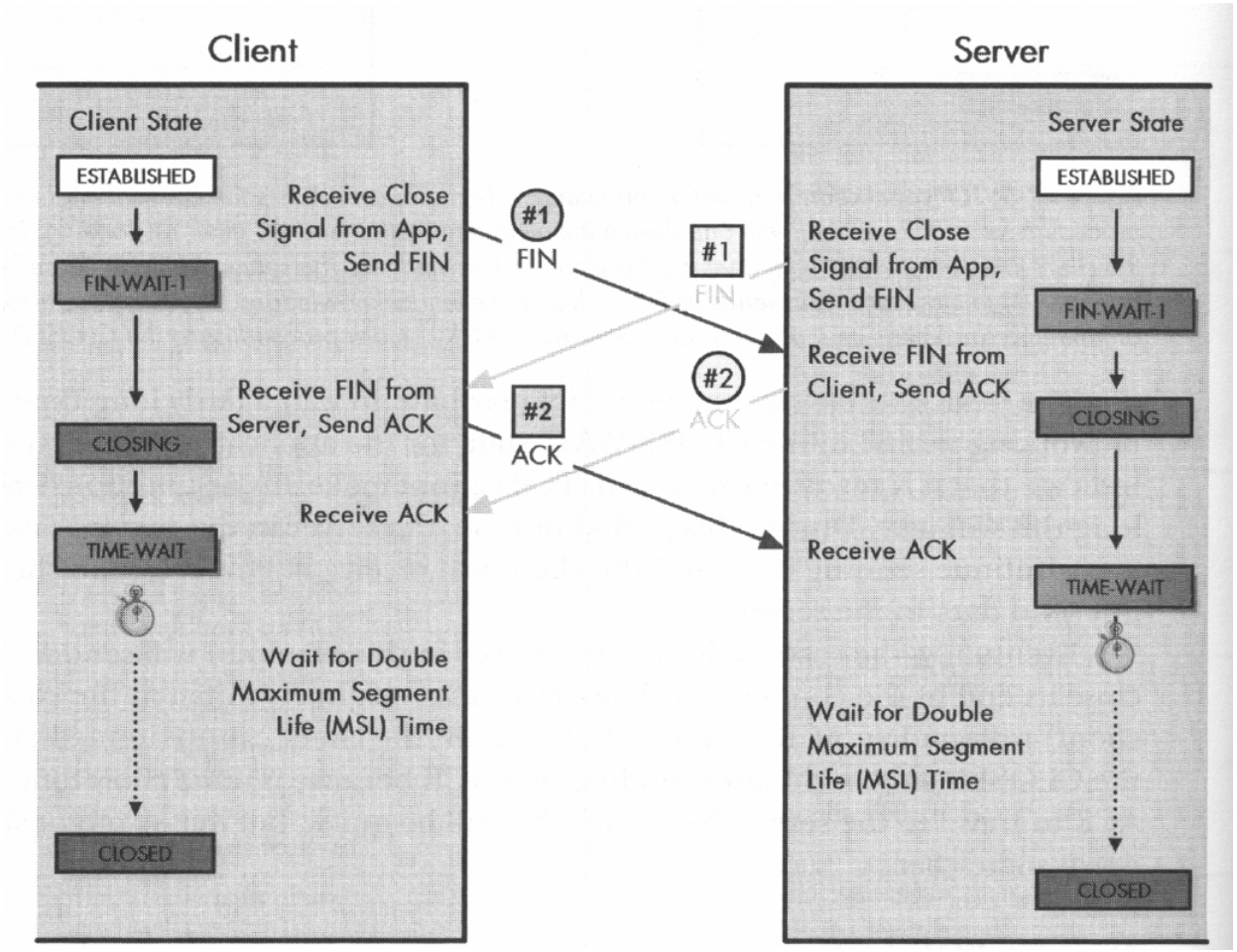
CLOSE_WAIT The remote end has shut down, waiting for the socket to close
(druga strona połączenia zainicjowała jego zwolnienie).

TCP: procedura zamykania połączenia[39]



[39] C.M.Kozierok, TCP/IP Guide

TCP: procedura równoczesnego zamykania połączenia[40]



[40] C.M.Kozierok, TCP/IP Guide

Warstwa zastosowań (sesji+prezentacji+zastosowań)

- transfer plików – FTP (*File Transfer Protocol*)
- zdalne rejestrowanie się – SSH (*Secure SHell*), TELNET (*Network Terminal Protocol*)
- poczta elektroniczna – SMTP (*Simple Mail Transport Protocol*), POP3 (*Post Office Protocol*), IMAP (*Internet Message Access Protocol*)
- listy korespondencyjne i dyskusyjne – NNTP (*Network News Transport Protocol*).
- www (*World Wide Web*) – HTTP (*HyperText Transport Protocol*)
- dynamiczna konfiguracja hostów w sieci – DHCP (*Dynamic Host Configuration Protocol*)
- usługa nazw domenowych – DNS (*Domain Name Service*)
- sieciowy system plików – NFS (*Network File System*)

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 – danych, 21 – sterujący

Super demon sieciowy xinetd[41]

/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
```

[41] Jak działa serwer sieciowy obsługujący jedno lub wiele połączeń? Zobacz `/git/tm-scripts`.

Super demon sieciowy xinetd

/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

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
```

Porównanie modeli odniesienia OSI i TCP/IP

Wg A.Tanenbauma znaczenie modelu OSI bierze się z wyraźnego rozróżnienia trzech idei, które są podstawą tego modelu:

- usługi warstwy: co warstwa robi (semantyka warstwy)
- interfejs warstwy: sposób dostępu do niej dla procesów położonych wyżej
- protokoły (równorzędne) warstwy: sposób wymiany danych między równorzędnymi warstwami, który zapewnia wypełnianie przez warstwę jej funkcji

Warstwę można traktować jak obiekt, który wyposażony jest w zbiór metod, które mogą być wykonywane przez procesy z zewnątrz obiektu.

Semantyka tych metod definiuje zbiór usług oferowanych przez obiekt. Parametry i wyniki tworzą wraz z metodą interfejs obiektu.

Wewnętrzny kod obiektu jest jego protokołem (nie jest widoczny z zewnątrz).

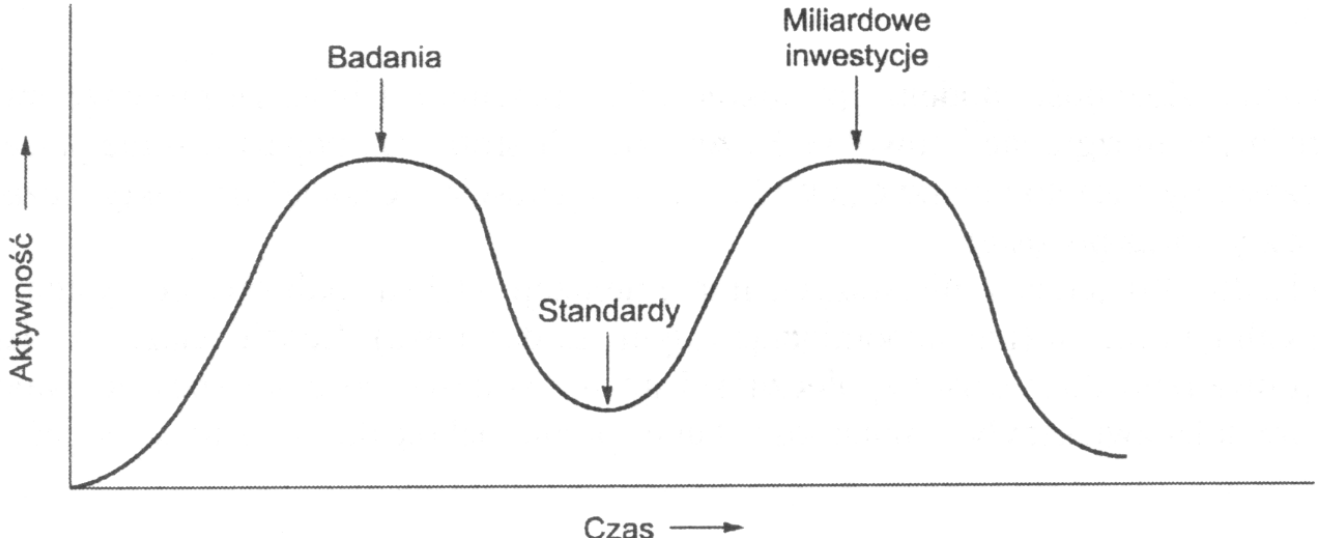
Porównanie modeli odniesienia OSI i TCP/IP

- Model odniesienia OSI powstał przed określeniem odpowiadających mu protokołów! Próby jego implementacji wymusiły konieczność wprowadzenia modyfikacji.
- W przypadku TCP/IP najpierw powstały protokoły. Model jest tylko ich opisem.
- Model OSI przewiduje komunikację połączeniową i bezpołączeniową w warstwie sieciowej, ale jedynie połączeniową w warstwie transportowej. TCP/IP obsługuje oba typu w warstwie transportowej (co daje użytkownikowi możliwość wyboru), ale tylko komunikację bezpołączeniową w warstwie sieciowej.

Porównanie modeli odniesienia OSI i TCP/IP

Przyczyny porażki modelu OSI:

- zły moment wprowadzenia standardu (*apokalipsa dwóch słoni* D.Clarka[42])



[42] The Apocalypse of Two Elephants, or "what I really said"

Porównanie modeli odniesienia OSI i TCP/IP

Przyczyny porażki modelu OSI:

- zła technologia (wady modelu i protokołów; złożoność)

  Niektóre funkcje (adresowanie, sterowanie przepływem, kontrola błędów) pojawiają się w każdej warstwie.

- zła implementacja (spowodowana złożonością modelu i protokołów)

- zła polityka

  TCP/IP uważano za składnik UNIX-a, a model OSI za twór ministerstw telekomunikacji krajów Unii Europejskiej (potem także rządu USA)

Porównanie modeli odniesienia OSI i TCP/IP

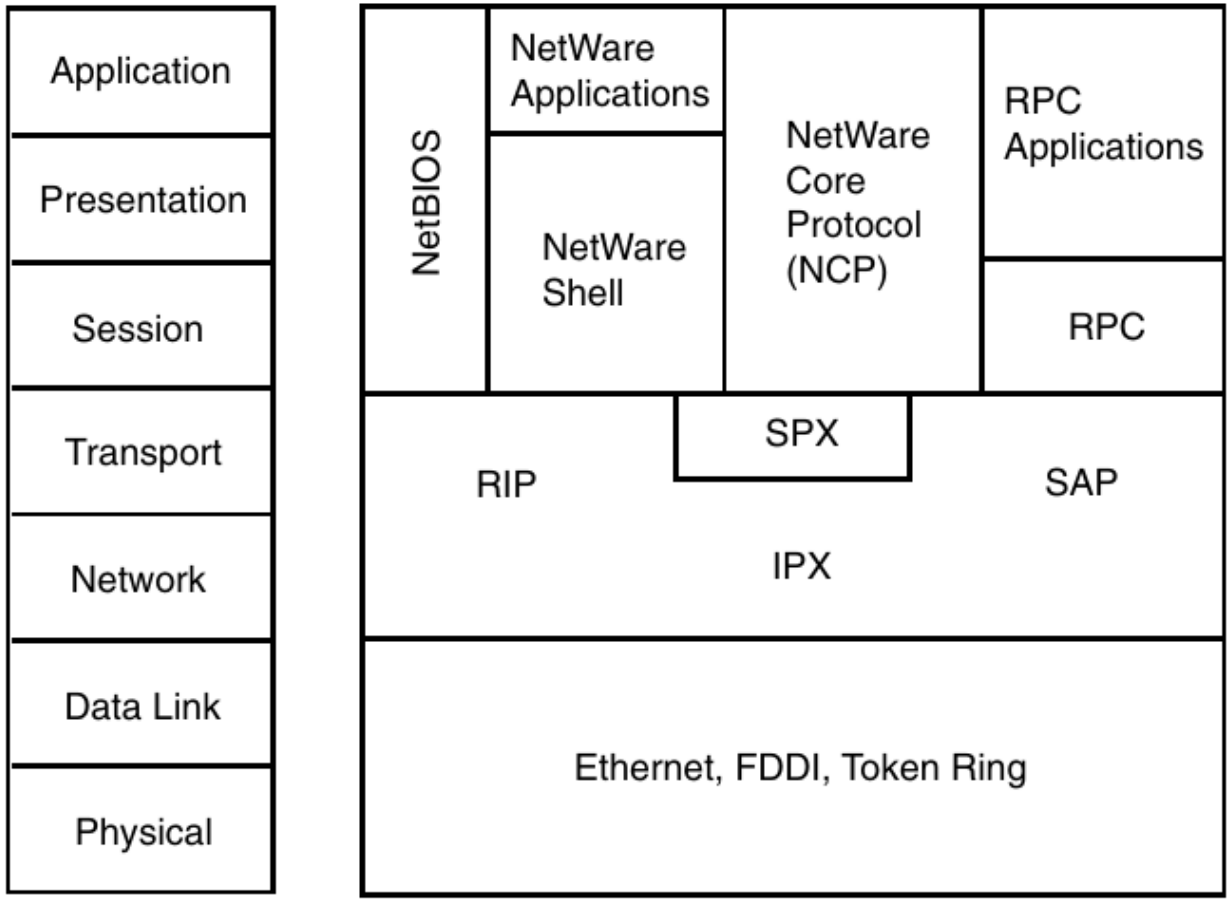
Problemy modelu i protokołów TCP/IP:

- brak rozróżnienia idei usługi, interfejsu i protokołu (także specyfikacji od implementacji)
- brak ogólności (trudność w użyciu tego modelu do opisania innych stosów protokołów)
- warstwa host-sieć nie jest warstwą w sensie ścisłym, ale interfejsem pomiędzy siecią, a warstwą łącza danych
- brak rozróżnienia na warstwę fizyczną i warstwę łącza danych
- brak jednolitej jakości protokołów

Model OSI jest przydatny do omawiania działania sieci komputerowych, ale protokoły OSI nie zdobyły popularności.

Model TCP/IP praktycznie nie istnieje, ale protokoły są powszechnie używane.

Rodzina protokołów NetWare firmy Novell[43]



[43] The Network's Guide to AppleTalk, IPX and NetBIOS

Rodzina protokołów NetWare firmy Novell

- **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;[44] NetWare dostarcza emulatora pozwalającego uruchamiać aplikacje korzystające z interfejsu NetBIOS

[44] Schemat komunikacji sieciowej 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.

Rodzina protokołów NetWare firmy Novell

- **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 bezpołączeniowym 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 wdrażane 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:	802.3/Novel_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

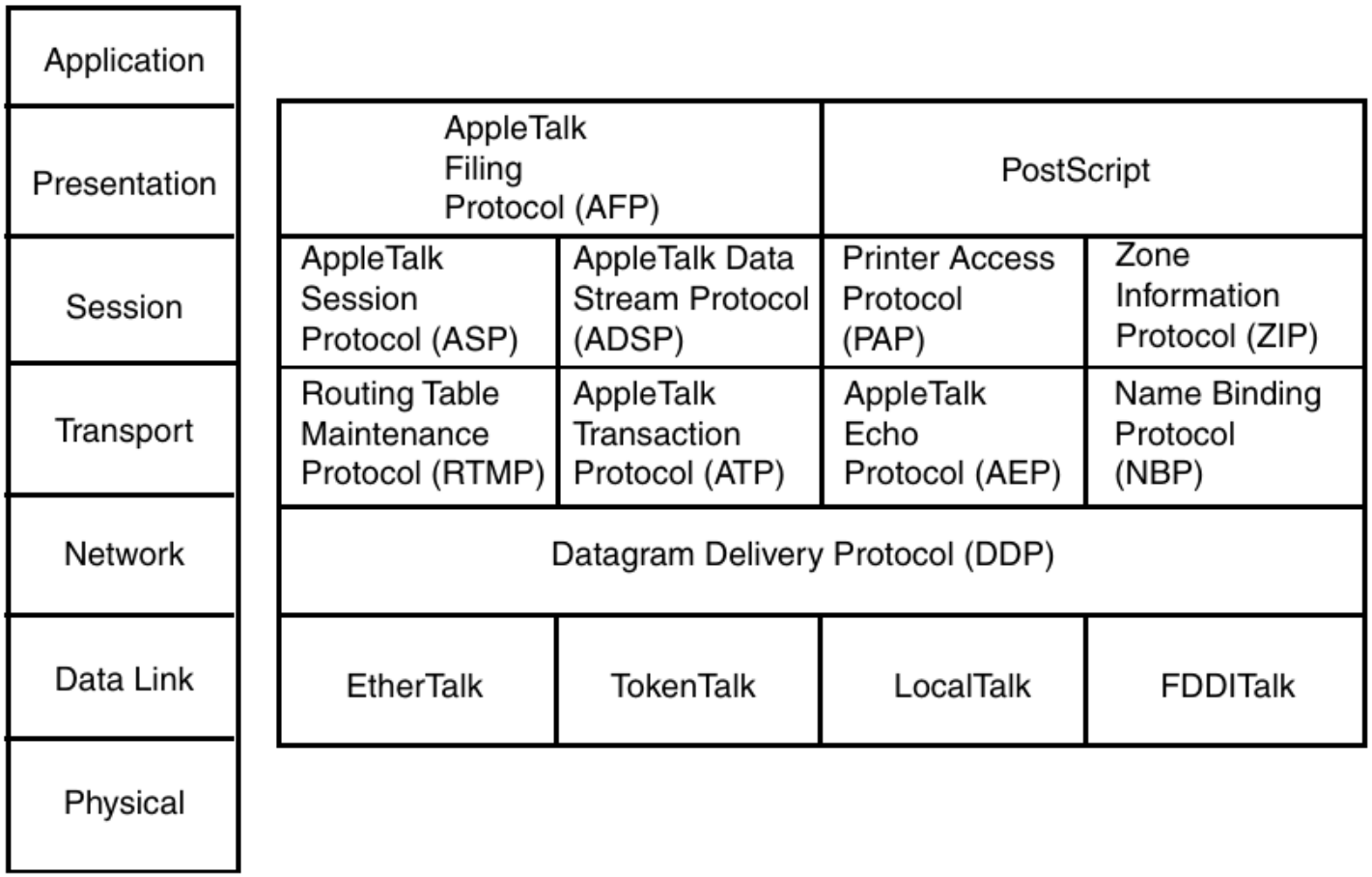
Struktura nagłówka pakietu IPX

- 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 zmniejsza 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

- 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

Rodzina protokołów AppleTalk[45]



[45] The Network's Guide to AppleTalk, IPX and NetBIOS

Rodzina protokołów AppleTalk

- **AFP** (*AppleTalk Filing Protocol*) – protokół warstwy aplikacji dostarcza usługi plików sieciowych (wszystkim) aplikacjom istniejącym niezależnie od stosu protokołów
- **ADSP** (*AppleTalk Data Stream Protocol*) – protokół strumienia danych sieci dostarcza w niezawodny sposób pełnodupleksowe usługi połączeniowe poprzez ustanowienie logicznego połączenia (sesji) pomiędzy komunikującymi się komputerami (wykorzystuje gniazda)
- **ASP** (*AppleTalk Session Protocol*) – protokoł sesji zapewnia niezawodne dostarczanie danych poprzez sekwencyjne zarządzanie sesją
- **PAP** (*Printer Access Protocol*) – protokół dostępu do drukarki umożliwiający zarządzanie drukarkami (wymianę innych danych)
- **ZIP** (*Zone Information Protocol*) – protokół informacji o strefach zapewnia mechanizm logicznego grupowania urządzeń sieciowych (tworzenia stref)

Rodzina protokołów AppleTalk

- **ATP** (*AppleTalk Transport Protocol*) – protokoł transportu
- **AURP** (*AppleTalk Update-Based Routing Protocol*) – protokoł trasowania
- **DDP** (*Datagram Delivery Protocol*) – protokół warstwy datagramowej odpowiedzialny za dostarczanie danych metodą bezpołączeniową
- **ELAP** (*Ether Talk Link Access Protocol*) – protokół warstwy łącza danych zapewniający opakowywanie danych w ramkach 802.3
- **TLAP** (*Token Talk Link Access Protocol*) – protokół warstwy łącza danych zapewniający opakowywanie danych w ramkach sieci Token Ring
- **LLAP** (*Local Talk Link Access Protocol*) – protokół warstwy dostępu do sieci firmy Apple (skrętka dwużyłowa, 230Kb/s)

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

- 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
- **protokół NetBIOS/NetBEUI** – rodzina protokołów używanych przez API NetBIOS/NetBEUI
- w trakcie rozwoju NetBEUI powstały nowe protokoły zwane *NetBIOS Frames* (NBF)
- NetBEUI = NetBIOS Frames Protocol for 802.2 Networks (oficjalna nazwa używana przez IBM)[46]

[46] Usługi nazwowe wykorzystują tryb 802.2 typ 1 (*unacknowledged connectionless mode*), a usługi sesyjne – tryb 802.2 typ 2 (*connection-oriented operational mode*)

Common Internet File System (CIFS)[47]

- **Common Internet File System** (dialekt **Server Message Block Protocol**, protokół bloków komunikatów serwera), jest protokołem (wg modelu OSI) warstwy aplikacji/prezentacji używany przez systemy operacyjne firmy Microsoft
- CIFS/SMB służy do realizowania sterowania sesjami sieciowymi, sieciowym systemem plików, dostępem do sieciowych drukarek i przekazywaniem komunikatów, wykrywaniem serwerów sieciowych, uwierzytelniania i autoryzacji
- zapewnia podobną funkcjonalność jak ASP, AFP, NCP, NFS
- CIFS/SMB wykorzystuje: NetBIOS Frames Protocol (NBF), NetBIOS over TCP/IP (NBT), NetBIOS over IPX
- systemy Unix/Linux realizują komunikację klient/serwer protokołu CIFS poprzez program Samba

[47] Timothy D. Evans, *NetBIOS, NetBEUI, NBF, NBT, NBIPX, SMB, CIFS Networking*

tcpdump

```
# tcpdump  -i tun0 host 158.75.5.90
tcpdump: WARNING: arptype 65534 not supported by libpcap - falling back to cooked soc
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tun0, link-type LINUX_SLL (Linux cooked), capture size 96 bytes
21:06:19.162460 IP 172.20.1.25.53928 > hel.fizyka.umk.pl.ssh: S 932535202:932535202(0
21:06:19.176748 IP hel.fizyka.umk.pl.ssh > 172.20.1.25.53928: S 2860128732:2860128732
21:06:19.176779 IP 172.20.1.25.53928 > hel.fizyka.umk.pl.ssh: . ack 1 win 92
21:06:19.199486 IP hel.fizyka.umk.pl.ssh > 172.20.1.25.53928: P 1:21(20) ack 1 win 12
21:06:19.199519 IP 172.20.1.25.53928 > hel.fizyka.umk.pl.ssh: . ack 21 win 92
21:06:19.199621 IP 172.20.1.25.53928 > hel.fizyka.umk.pl.ssh: P 1:22(21) ack 21 win 9
21:06:19.219481 IP hel.fizyka.umk.pl.ssh > 172.20.1.25.53928: . ack 22 win 12
21:06:19.219510 IP 172.20.1.25.53928 > hel.fizyka.umk.pl.ssh: P 22:814(792) ack 21 wi
```

ngrep

```
# ngrep -Nq -d tun0 -c 70 host 158.75.5.90 | head -50
interface: tun0 (172.20.1.25/255.255.255.255)
filter: (ip or ip6) and ( host 158.75.5.90 )

T(6) 172.20.1.25:46809 -> 158.75.5.90:80 [AP]
  GET /wfaiis/ HTTP/1.1..User-Agent: Opera/9.50 (X11; Linux i686; U
  ; en)..Host: www.fizyka.umk.pl..Accept: text/html, application/xm
  ....

# ngrep -Nq -d tun0 -c 70 Werner host 158.75.5.90 and port 80
interface: tun0 (172.20.1.25/255.255.255.255)
filter: (ip or ip6) and ( host 158.75.5.90 and port 80 )
match: Werner

T(6) 158.75.5.90:80 -> 172.20.1.25:48230 [AP]
  ions</a>.</big></h4>.<hr width="100%">.<h4><big><font color="#000
  000"><font size="+0"><big>Teaching/Materia..y.pomocnicze do zaj..
  ..</big></font></font></big></h4>.<ul type="">.<li><span style="f
```

wireshark

```
NAME
       wireshark - Interactively dump and analyze network traffic
DESCRIPTION
       Wireshark is a GUI network protocol analyzer.  It lets you interactively brows
       packet data from a live network or from a previously saved capture file.
       Wireshark's native capture file format is pcap format, which is also the forma
       used by tcpdump and various other tools.

       Wireshark can read / import the following file formats:
       o   pcap - captures from Wireshark/TShark/dumpcap, tcpdump, and various other
           using libpcap's/Npcap's/WinPcap's/tcpdump's/WinDump's capture format
       o   pcapng - "next-generation" successor to pcap format
       o   snoop and atmsnoop captures
       o   Shomiti/Finisar Surveyor captures
       o   Novell LANalyzer captures
       o   Microsoft Network Monitor captures
       o   AIX's iptrace captures
       o   Cinco Networks NetXRay captures
       o   Network Associates Windows-based Sniffer captures
       ...
```

Zob. /git/tm-scripts, plik socket/smtp.pcapng

tshark

```
NAME
    tshark - Dump and analyze network traffic
DESCRIPTION
    TShark is a network protocol analyzer. It lets you capture packet data from a
    live network, or read packets from a previously saved capture file, either
    printing a decoded form of those packets to the standard output or writing the
    packets to a file.  TShark's native capture file format is pcapng format,
    which is also the format used by wireshark and various other tools.
```

```
$ tshark -r smtp.pcapng
    1 0.000000000  172.20.1.25 -> 158.75.5.252 TCP 60 37042 -> 25 [SYN] Seq=0 Win=642
    2 0.065629165 158.75.5.252 -> 172.20.1.25  TCP 60 25 -> 37042 [SYN, ACK] Seq=0 Ac
    3 0.065667426  172.20.1.25 -> 158.75.5.252 TCP 52 37042 -> 25 [ACK] Seq=1 Ack=1 W
    4 0.171884635 158.75.5.252 -> 172.20.1.25  SMTP 90 S: 220 mail.fizyka.umk.pl ESMT
    5 0.171936070  172.20.1.25 -> 158.75.5.252 TCP 52 37042 -> 25 [ACK] Seq=1 Ack=39
    6 11.199918660  172.20.1.25 -> 158.75.5.252 SMTP 65 C: HELO scobie
    7 11.265847362 158.75.5.252 -> 172.20.1.25  TCP 52 25 -> 37042 [ACK] Seq=39 Ack=1
    ...
```

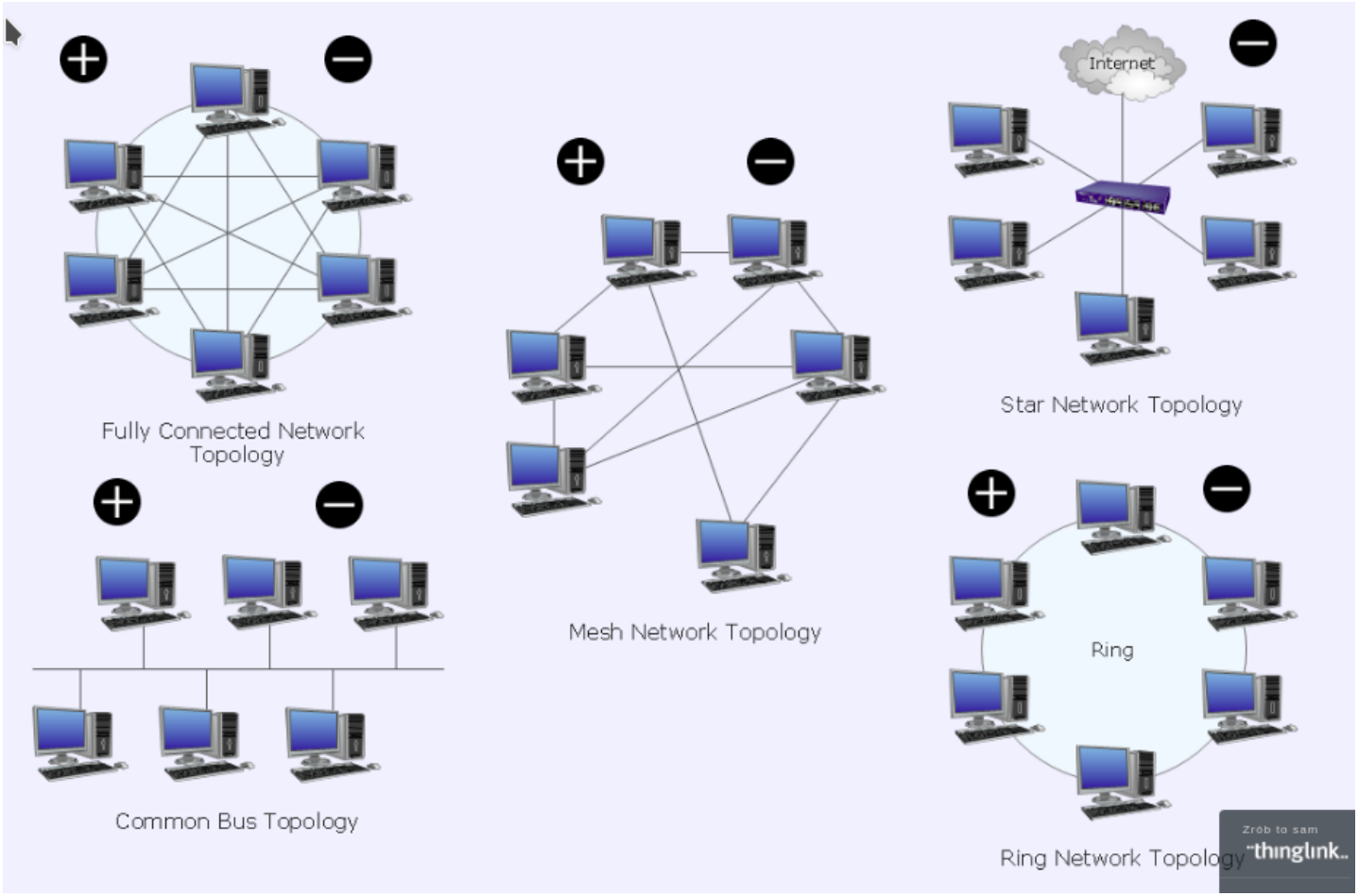
Zob. także inne komendy z pakietu wireshark-cli, np. `capinfos`, `editcap`.

Lokalna sieć komputerowa

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

Urządzenia LAN: komputery PC, stacje robocze, serwery, drukarki sieciowe, koncentratory, mosty, przełączniki, routery

LAN: rodzaje topologii[48]



[48] https://www.thinglink.com/scene/702756142819835906

LAN: rodzaje topologii

- 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
- sieci w kształcie kraty – część lub wszystkie stanowiska są połączone z dwoma lub większą liczbą innych stanowisk

Technologie LAN i model OSI

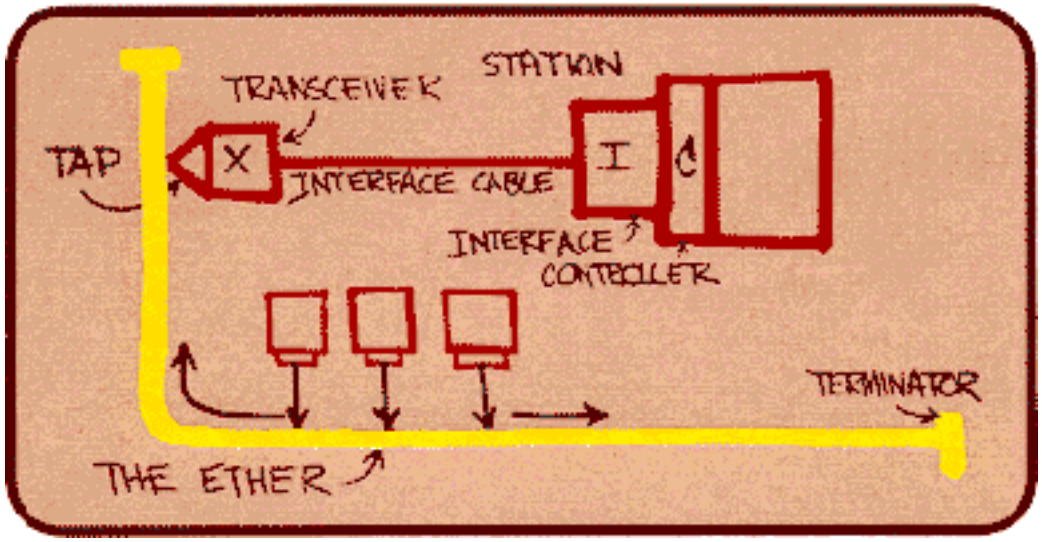
Powiązanie warstwy łącza danych i warstwy fizycznej z warstwą sieciową (Internet) jest realizowane poprzez protokół LLC (*Logical Link Control*)

<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>

<table>
<tr><td colspan="6">LAN protocols</td><td>OSI layers</td></tr>
<tr><td colspan="6">IEEE 802.2</td><td>LLC sublayer</td></tr>
<tr><td>IEEE 802.3
10Base-T</td><td>IEEE 802.3u
100Base-TX</td><td>802.3[ab|z]
1000Base-T|[SL]X</td><td>802.3ae
10GBase-[S|L]R</td><td>IEEE 802.5
Token Ring</td><td>IEEE 802.11
Wi-Fi</td><td>MAC sublayer
Physical layer</td></tr>
</table>

Sieci typu Ethernet

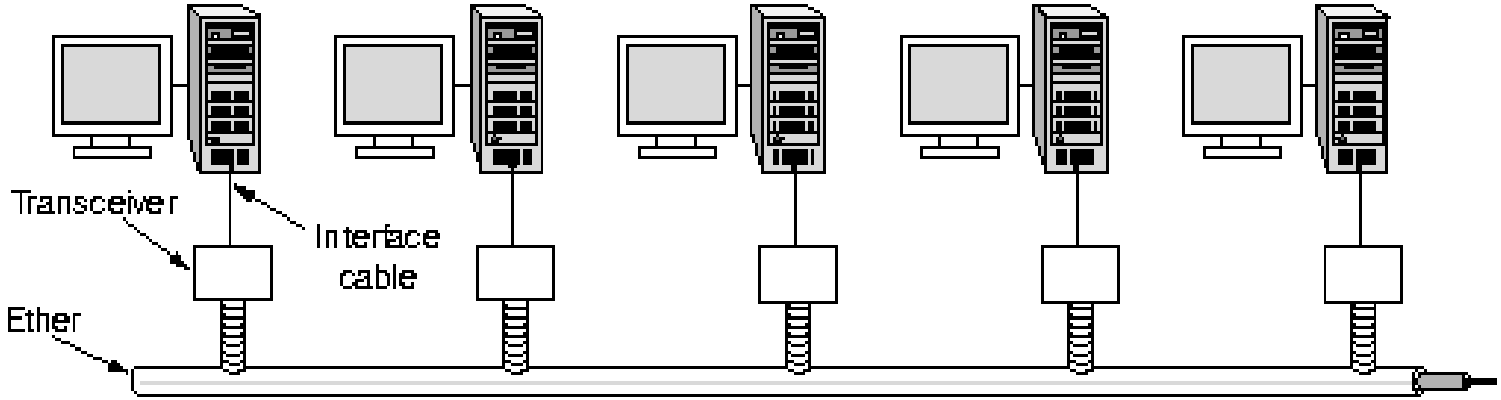
- maj 1973 – Robert Metcalfe publikuje notatkę opisującą *X-Wire*, czyli sieć biurową opartą o szynę wielodostępną o przepustowości 3 Mb/s
- 1973 – w Palo Alto Research Center (PARC) firmy Xerox powstaje pierwsza sieć (*Alto Aloha Network*)
- sieć może zapewnić komunikację dowolnym komputerom – zmiana nazwy na Ethernet



Sieci typu Ethernet

- 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 IEEE 802.3 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.
- komputer przyłączany jest do sieci poprzez interfejs ethernetowy (adapter sieciowy, kontroler, kartę sieciową)

Oryginalna sieć Ethernet



- MAU (*Medium Attachment Unit*) – urządzenie przyłączające do medium, transceiver – nadbiornik, nadajnik/odbiornik
- AUI (*Attachment Unit Interface*) – interfejs urządzenia przyłączającego, 10 Mb/s
- MII (*Media Independent Interface*) – interfejs niezależny od medium, 100 Mb/s
- GBIC, GMII (*Giga Bit Interface Converter*) – konwerter interfejsu gigabitowego, 1000 Mb/s; także mini GBIC lub SFP (*Small Form-factor Pluggable*)
- XAUI, XGMII – 10 Gb/s
- NIC (*Network Interface Card*) – karta sieciowa

Jak działa Ethernet?[49]

Dlaczego sieci ethernetowe działają dobrze pomimo braku

- potwierdzania otrzymywanych ramek
- zgłaszania nieudanych transmisji
- zegara sieciowego do wyznaczania pulsów danych
- kontroli współdzielenia sieci
- przewidywalności zachowania się sieci (indywidualne transmisje mogą być wstrzymywane)
- sterowania przepływem (brak priorytetowania)

[49] Jean-Yves Le Boudec, The MAC Layer

Jak działa Ethernet?

- każda ramka rozpoczyna się 96 bitową zwłoką (9.6 μs dla sieci 10 Mb/s)[50]
- 64 bity preambuły ramki ethernetowej służą synchronizacji zegara odbiorcy
- synchronizacja jest wymagana przez następnych 1518 oktetów (12144 bitów, 1.2 msek); możliwość tworzenia prostych urządzeń sieciowych
- wielkość danych: od 46 do 1500 oktetów
  efektywność/narzut: od 2.5% ($\frac{12+26}{1500}$) do 82.6% ($\frac{12+26}{46}$)

[50] Odpowiednio 0.96μs/96ns dla sieci 100/1000 Mb/s.

Jak działa Ethernet?

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

1. sprawdzanie stanu kanału przed wysłaniem ramki (*carrier sense*)
2. zwłoka 9.6 μs. przed rozpoczęciem nadawania
3. w razie wykrycia kolizji (*collision*) nadawca wysyła przez 32 bity czasu sygnał „tłok" (*jam*) i wstrzymuje nadawanie
4. wznawianie nadawania (powrot do pkt. 1) po losowo określonej (i stopniowo wydłużanej) przerwie wg algorytmu binarnego odczekiwania wykładniczego (*binary exponential backoff algorithm*)
5. porzucenie ramki po 16 nieudanych próbach wysłania (około 0.5 s; początkowa zwłoka 8 μs, więc $2^{16} \times 8 \times 10^{-6} \approx 0.5$ s)

Forma dostępu do łącza wykorzystywana w sieciach typu Ethernet (IEEE 802.3).

Jak działa Ethernet?

- CD wymaga, aby długość sieci nie przekraczała $\frac{1}{2}c_c t_{64}$=5760 m (Ethernet 10 MHz)
  - c_c prędkość rozchodzenia się sygnału elektrycznego w miedzi ($\approx$ 2.25×10^8m/s)
  - t_{64} czas transmisji najmniejszej ramki ($8 \times 64 \times 1/10^7 = 51.2$ μs)
- DIX Ethernet (gruby kabel koncentryczny): 3 segmenty po 500 m plus dwa wzmacniaki
- 10Base-5 (gruby kabel koncentryczny): maksymalny zasięg 2800 m (5×500, 4 wzmacniaki, 2 AUI)
- 10Base-2 (cienki kabel koncentryczny): maksymalny zasięg 925 m (5×185)
- 10Base-T (UTP): maksymalny zasięg 500 m (5×100, 4 wzmacniaki)

Nośniki transmisji fizycznej

- cienki kabel koncentryczny RG-58 (50 Ω)
- nieekranowana/ekranowana (czteroparowa) skrętka (UTP/STP, *Unshielded/Shielded Twisted Pair*)
  - kategoria 1,2 UTP: uznane za przestarzałe w 1995
  - kategoria 3 UTP: 10 Mb/s, $\leqslant$ 100 m
  - kategoria 5, 5e UTP: 10/100 Mb/s, $\leqslant$ 100 m.
  - kategoria 6 (class E): 10/100/1000 Mb/s, $\leqslant$ 100 m (10000 Mb/s $\leqslant$ 37 m)
  - kategoria 6A (class E_A): 10/100/1000/10000 Mb/s
  - kategoria 7/7A (class F/F_A): 10/100/1000/10000 Mb/s
  - kategoria 8: 25/40 Gb/s, $\leqslant$ 30 m
- światłowód wielomodowy 50/62.5 μm (50/125, 62.5/125), LED
- światłowód jednomodowy 9 μm (9/125) ILD

Nośniki transmisji fizycznej[51]

Category	Max. Data Rate	Bandwidth	Max. Distance	Usage
Category 1	1 Mbps	0.4 MHz		Telephone and modem lines
Category 2	4 Mbps	4 MHz		LocalTalk & Telephone
Category 3	10 Mbps	16 MHz	100 m (328 ft.)	10BaseT Ethernet
Category 4	16 Mbps	20 MHz	100 m (328 ft.)	Token Ring
Category 5	100 Mbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet
Category 5e	1 Gbps	100 MHz	100 m (328 ft.)	100BaseT Ethernet, residential homes
Category 6	1 Gbps	250 MHz	100 m (328 ft.) 10Gb at 37 m (121 ft.)	Gigabit Ethernet, commercial buildings
Category 6a	10 Gbps	500 MHz	100 m (328 ft.)	Gigabit Ethernet in data centers and commercial buildings
Category 7	10 Gbps	600 MHz	100 m (328 ft.)	10 Gbps Core Infrastructure
Category 7a	10 Gbps	1000 MHz	100 m (328 ft.) 40Gb at 50 m (164 ft.)	10 Gbps Core Infrastructure
Category 8	25 Gbps (Cat8.1) 40 Gbps (Cat8.2)	2000 MHz	30 m (98 ft.)	25 Gbps/40 Gbps Core Infrastructure

[51] Ethernet Cables Explained

LAN – rodzaje sieci Ethernet[52]

- **10Base-5** – sieć z szyną wielodostępną w formie linii prostej wykorzystująca gruby kabel koncentryczny (tzw. gruby ethernet); zasięg do 500 m, pasmo 10 Mbs (IEEE 802.3)
- **10Base-2** – sieć z szyną wielodostępną w formie linii prostej wykorzystująca cienki kabel koncentryczny (tzw. cienki ethernet); zasięg do 185 m, 30 hostów w segmencie; pasmo 10 Mb/s (IEEE 802.3a)
- **10Base-T** – sieć w formie gwiazdy wykorzystująca nieekranowaną skrętkę (kategorii 3,4 lub 5); zasięg do 100m; pasmo 10 Mb/s (IEEE 802.3i)
- **10Base-FL/FB** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca włókna światłowodowe; zasięg do 2000 m; pasmo 10 Mb/s (IEEE 802.3j)
- **100Base-TX** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca 2 pary nieekranowanej skrętki (kategorii 5); zasięg do 100 m, pasmo 100 Mb/s (IEEE 802.3u)
- **100Base-FX** – sieć w formie gwiazdy bądź szkieletowa wykorzystująca wielomodowe włókna światłowodowe (MMF); zasięg do 2000 m, pasmo 100 Mb/s
- **1000Base-T** – sieć w formie gwiazdy wykorzystująca nieekranowaną skrętkę (4 pary, kabel kategorii 5/5e/6); zasięg do 100 m, pasmo 1 Gb/s (IEEE 802.3ab)

[52] http://en.wikipedia.org/wiki/IEEE_802.3

LAN – rodzaje sieci Ethernet

- **1000Base-SX** – sieć szkieletowa wykorzystująca MMF; zasięg do 550 m; pasmo 1 Gb/s (IEEE 802.3z)
- **1000Base-LX** – sieć szkieletowa wykorzystująca włókna światłowodowe jednomodowe (SMF) lub MMF, zasięg do 5000 m (SMF); pasmo 1 Gb/s (IEEE 802.3z)
- **10GBase-USR** – połączenie punkt-punkt via MMF; zasięg do 100/150 m pasmo 10 Gb/s
- **10GBase-SR** – połączenie punkt-punkt via MMF; zasięg do 300/400m; pasmo 10 Gb/s (IEEE 802.3ae)
- **10GBase-LR/ER** – połączenie punkt-punkt via SMF; zasięg do 25000/40000 m; pasmo 10 Gb/s (IEEE 802.3ae)
- **10GBase-T** – połączenia punkt-punkt 55/100 m, kabel STP/UTP klasa E kat.6/klasa E_A kat. 6A lub kat. 7 (IEEE 802.3a)
- **40/100GbE** – połączenia punkt-punkt, 100 m – OM3 MMF, 2/10/40 km – SMF (IEEE 802.3ba-2010, 802.3bg-2011, 802.3bj-2014, 802.3bm-2015)

Ramki IEEE 802.3z

7	1	6	6	2	46-1500	4	
Pre	SFD	DA	SA	Type	Data	FCS	Ext

- przedłużenie nośnika (*carrier extension*) – sprzęt uzupełnia ramkę do 416 B (1000Base-X) lub 520 B (512 bez Pre+SFD, 1000Base-T).
- przesyłanie ramek wiązkami (*frame/packet bursting*) – w jednej transmisji (półdupleksowej) jest przesyłanych wiele ramek, nie więcej jednak niż około 5.4 razy najdłuższa ramka)

```
| MAC Frame w/ Extension | Interframe Gap | MAC Frame | Interframe Gap | ... | MAC Frame |
|---------------------------------- Burst Limit ---------------------------|
|---------------------------- Duration of Carrier Event ------------------------------|
```

- *jumbo frames* – ramki przenoszące do 9000/9216 B danych (pełen dupleks)

Ramki IEEE 802.3z + VLAN

7	1	6	6	4	2	46-1500	4	
Pre	SFD	DA	SA	VLAN Tag	Type	Data	FCS	Ext

Topologie sieci ethernetowej

- topologia magistrali
- topologia gwiazdy
- topologia rozszerzonej gwiazdy/hierarchicznej gwiazdy
- topologia przełączana

Domena rozgłoszeniowa i domena kolizyjna.

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

Czynniki wpływające na wydajność lokalnej sieci Ethernet/802.3

- rozgłaszanie ramek (rozmiar sieci, liczba hostów)
- metoda dostępu CSMA/CD ograniczająca transmisję do jednej stacji
- zatory w sieci spowodowane zapotrzebowaniem na większe pasmo aplikacji multimedialnych
- opóźnienia wynikające ze skończonego czasu propagacji i przechodzenia ramek przez urządzenia sieciowe

rozmiar pakietu (B)	czas transmisji (μs)
64	51
512	410
1000	800
1518	1214

Dla sieci 10Base-T czas transmisji 1 b wynosi 100 ns

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

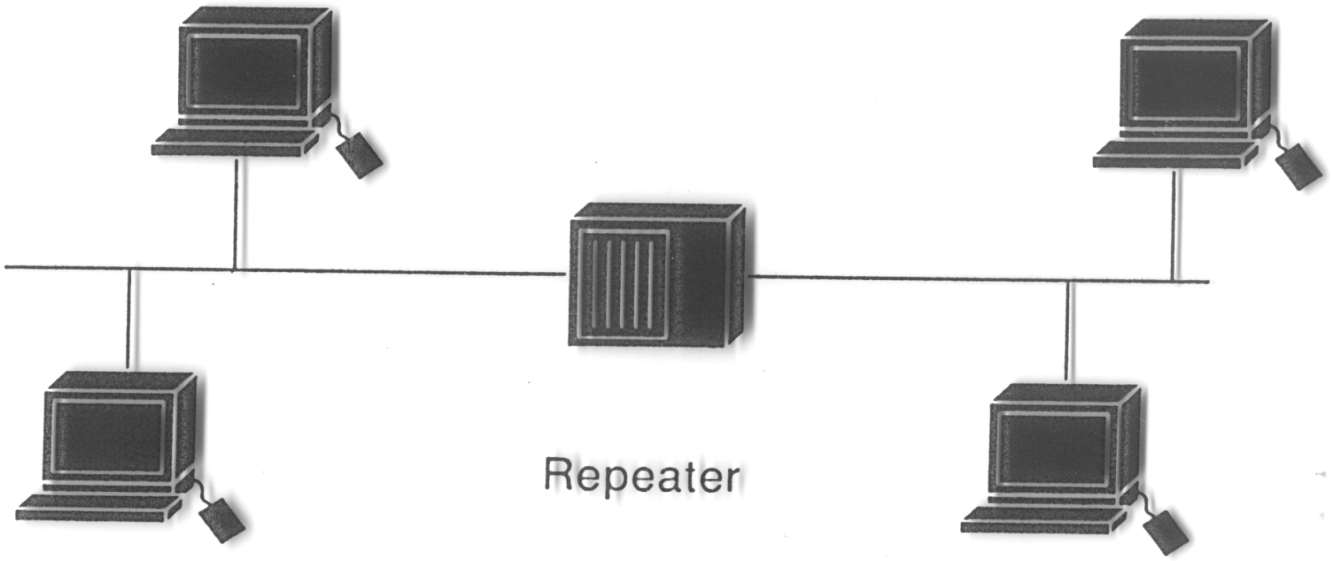
  wymagania:

  – mosty
  – routery
  – przełączniki

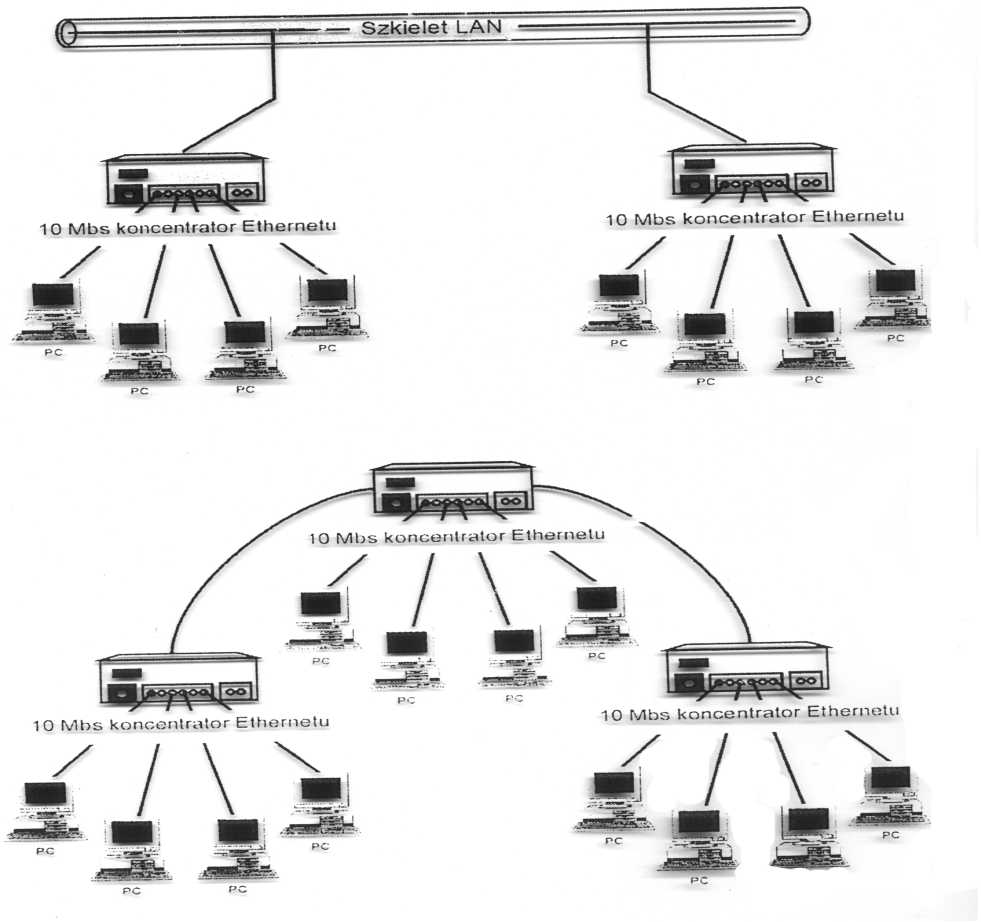
Urządzenia sieciowe: regenerator, koncentrator

- 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*).

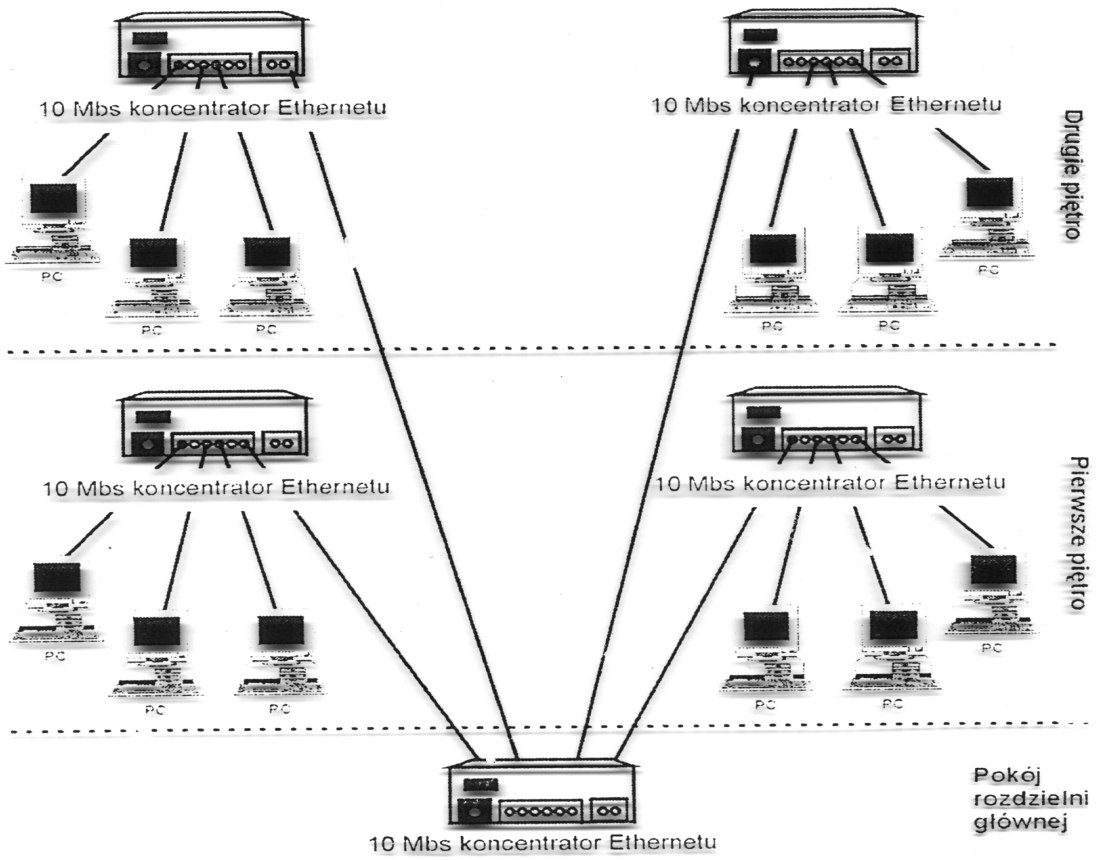
LAN: wzmacniak



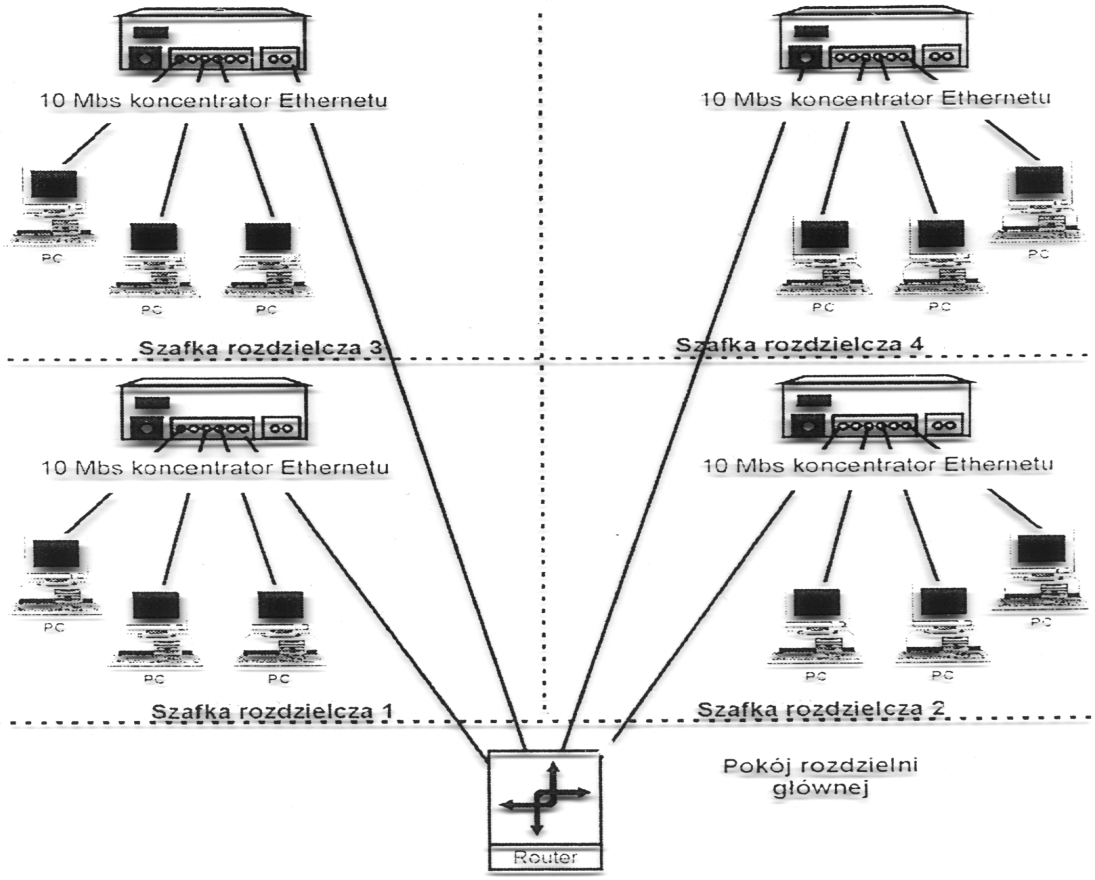
LAN: koncentratory



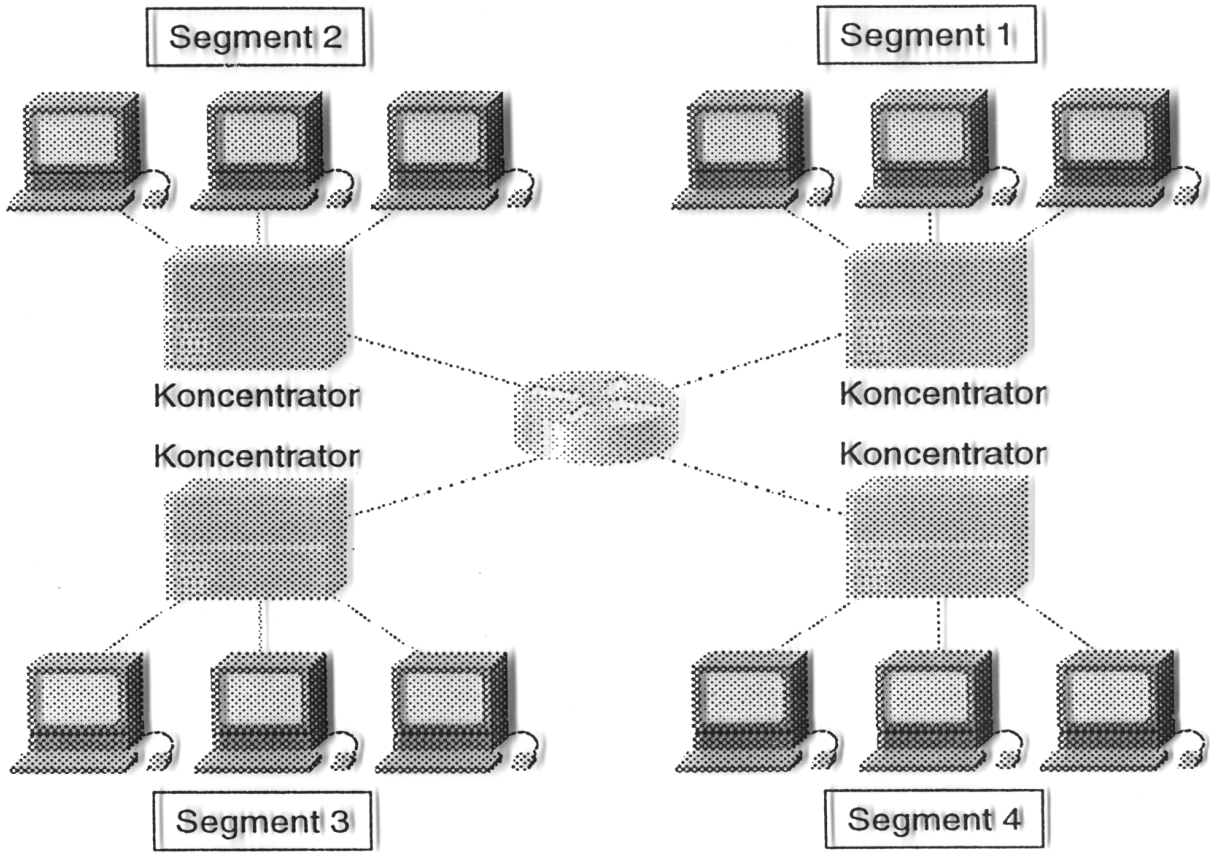
LAN: koncentratory



LAN: koncentratory i router



LAN: koncentratory i router



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

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

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)*.

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.

Urządzenia sieciowe: most

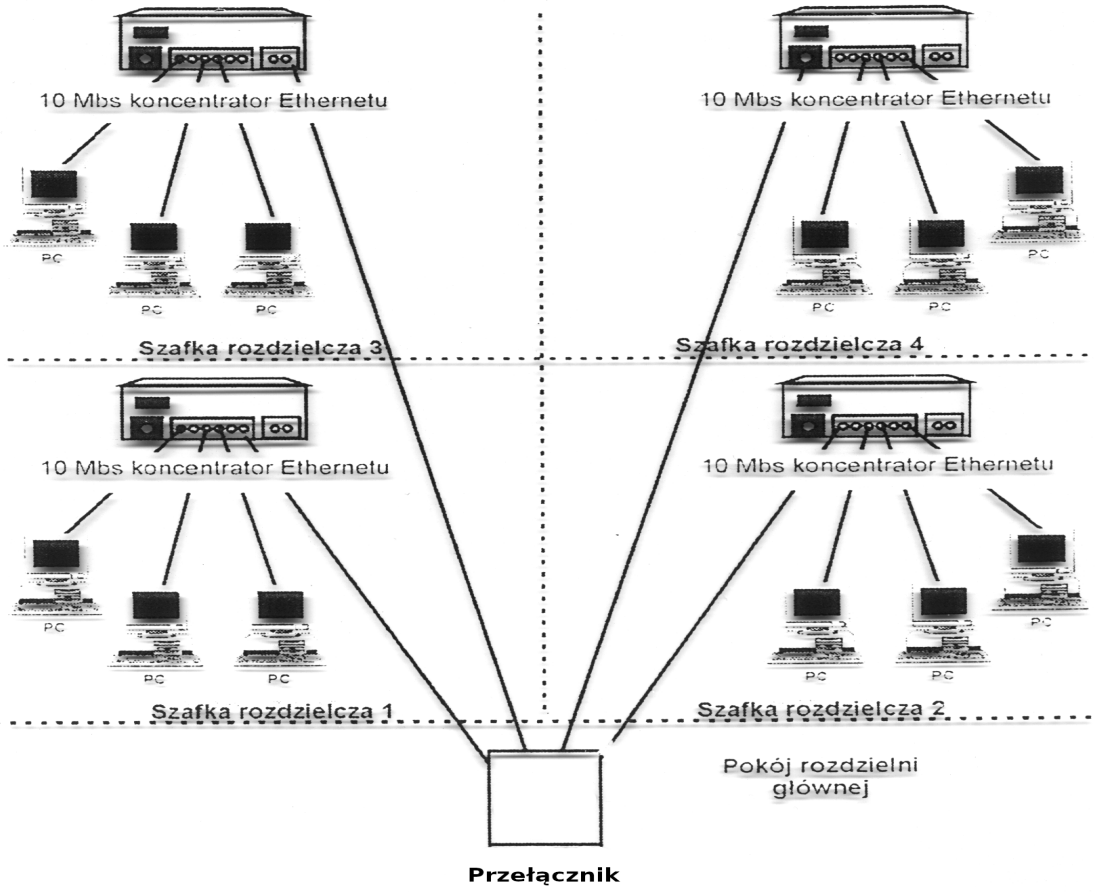
- Most (*bridge*) jest urządzeniem sieciowym warstwy 2 łączącym dwa segmenty sieci, które wykorzystuje adresy MAC do filtrowania ramek. Most tworzy tablicę adresów zawierającą wpisy typu interfejs-MAC, dzięki czemu możliwe staje się przekazywanie ramek tylko do właściwych segmentów.
- Most jest urządzeniem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

Urządzenia sieciowe: przełącznik ethernetowy

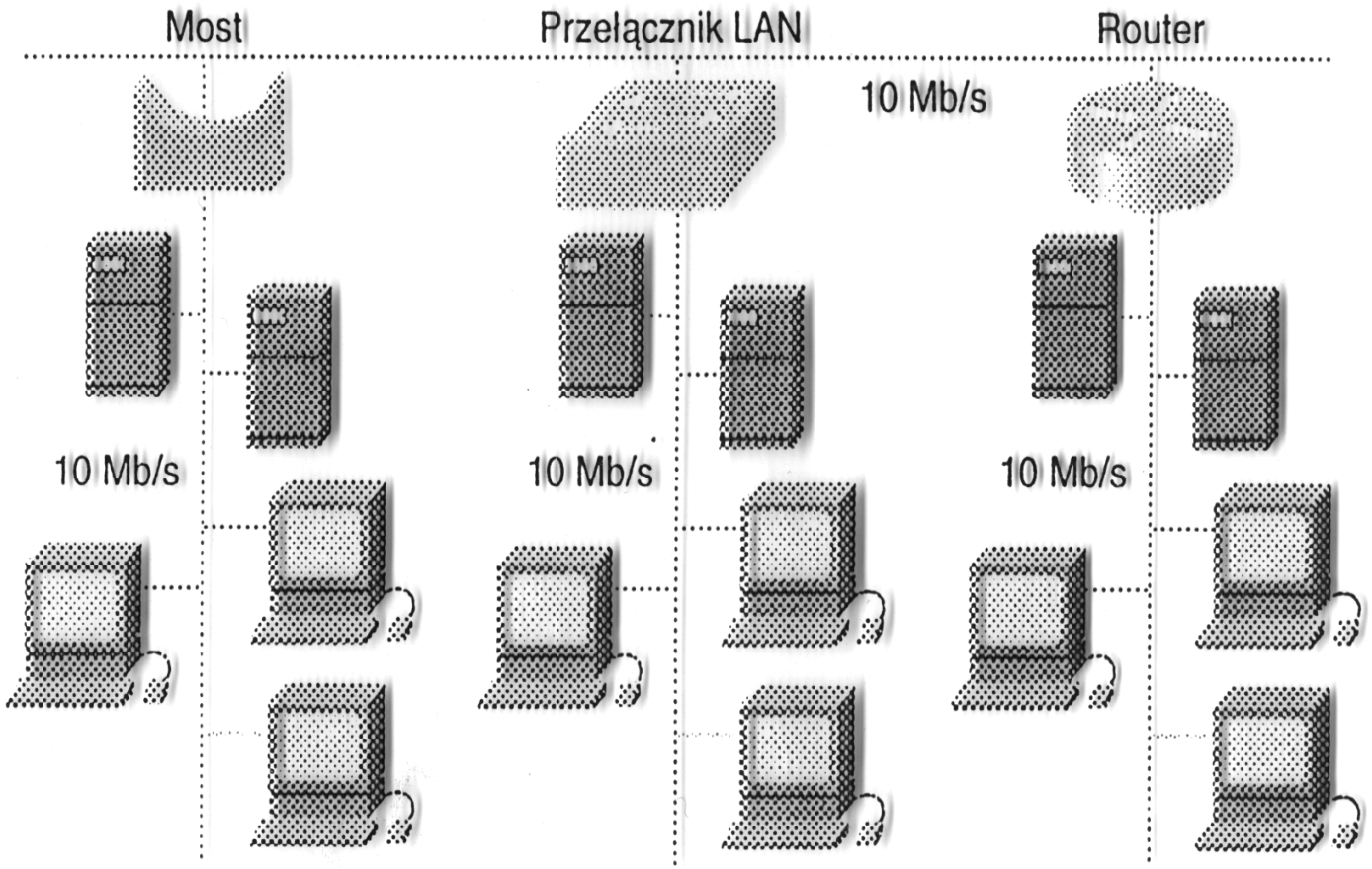
- Przełącznik ethernetowy (*Ethernet switch*) jest wieloportowym mostem, który dzieli sieć LAN na mikrosegmenty, które tworzą bezkolizyjne domeny.
- Jeśli przełącznik nie zna segmentu docelowego ramki, to przekazuje ją do wszystkich segmentów z wyjątkiem segmentu źródłowego.

  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.

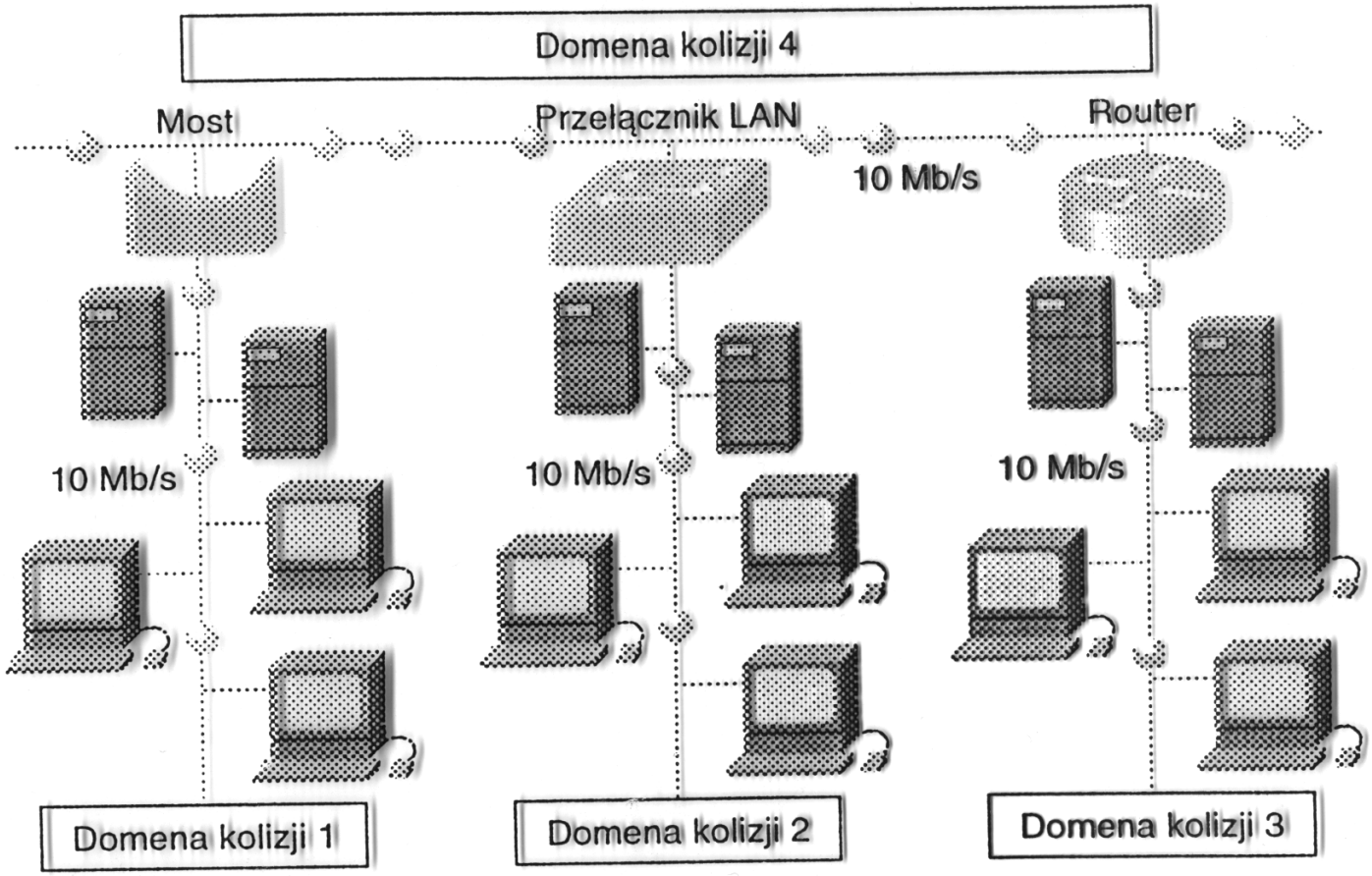
LAN: koncentratory i przełącznik $\longrightarrow$ przełączniki



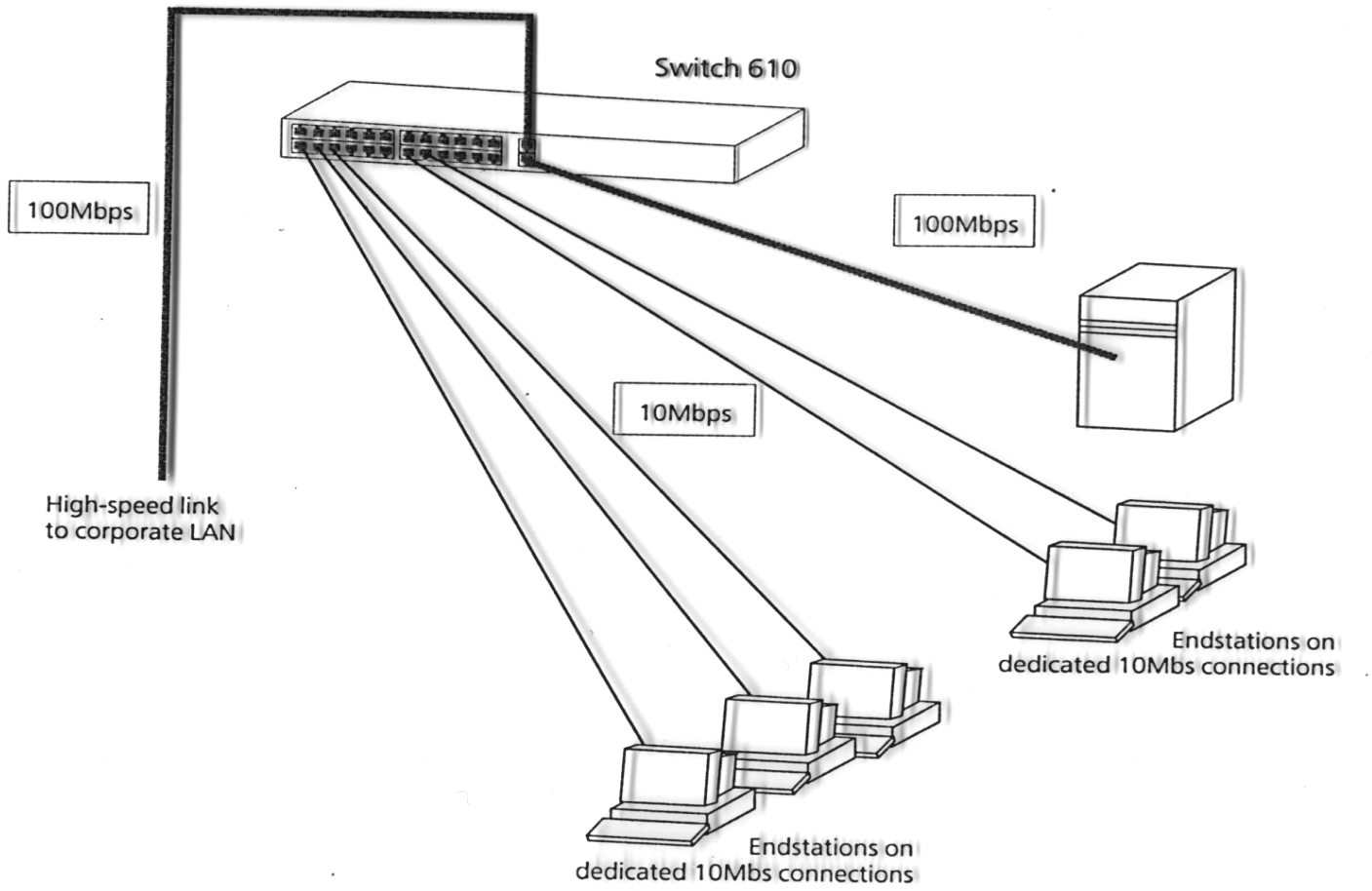
LAN: koncentratory, przełączniki i routery



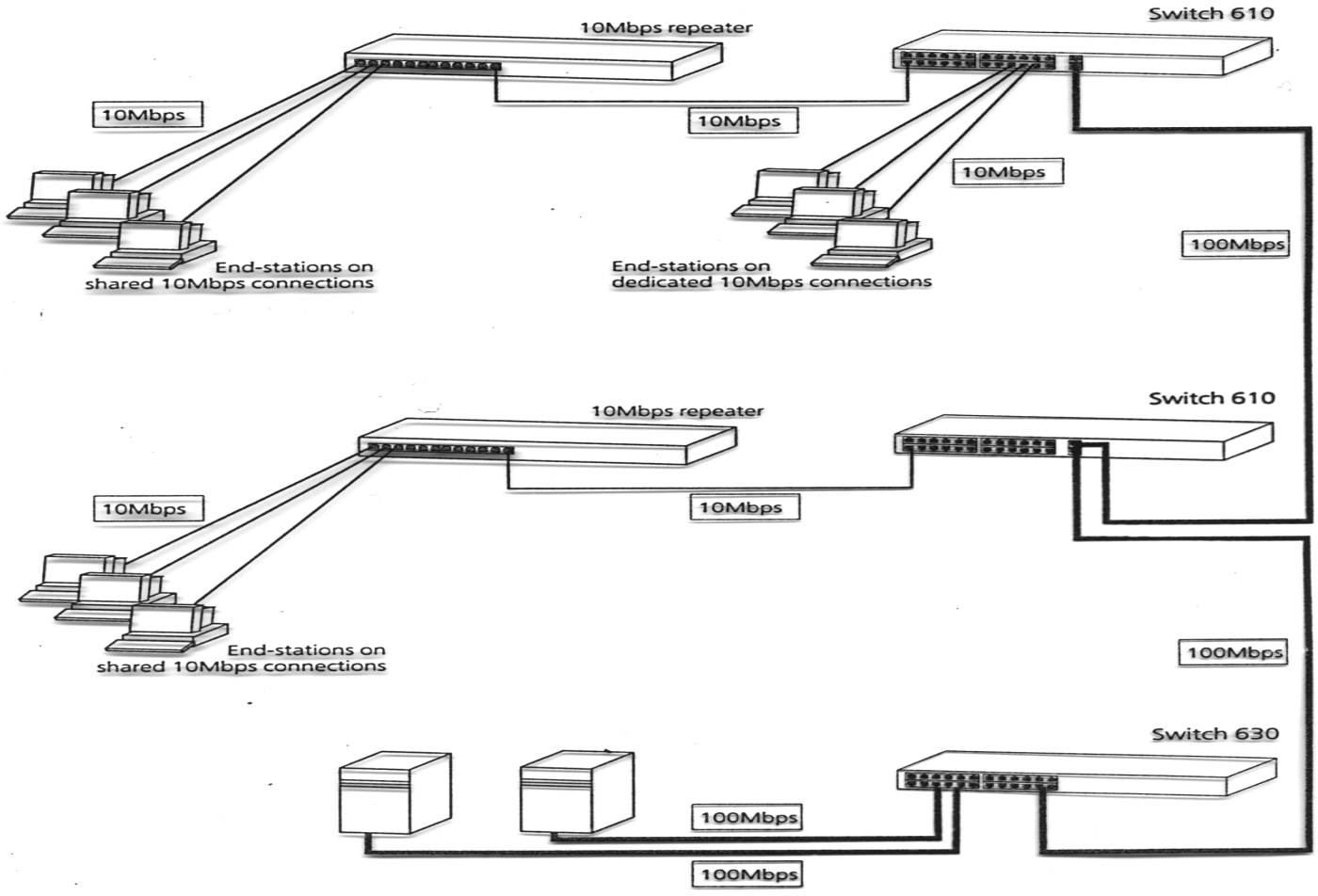
LAN: koncentratory, przełączniki i routery



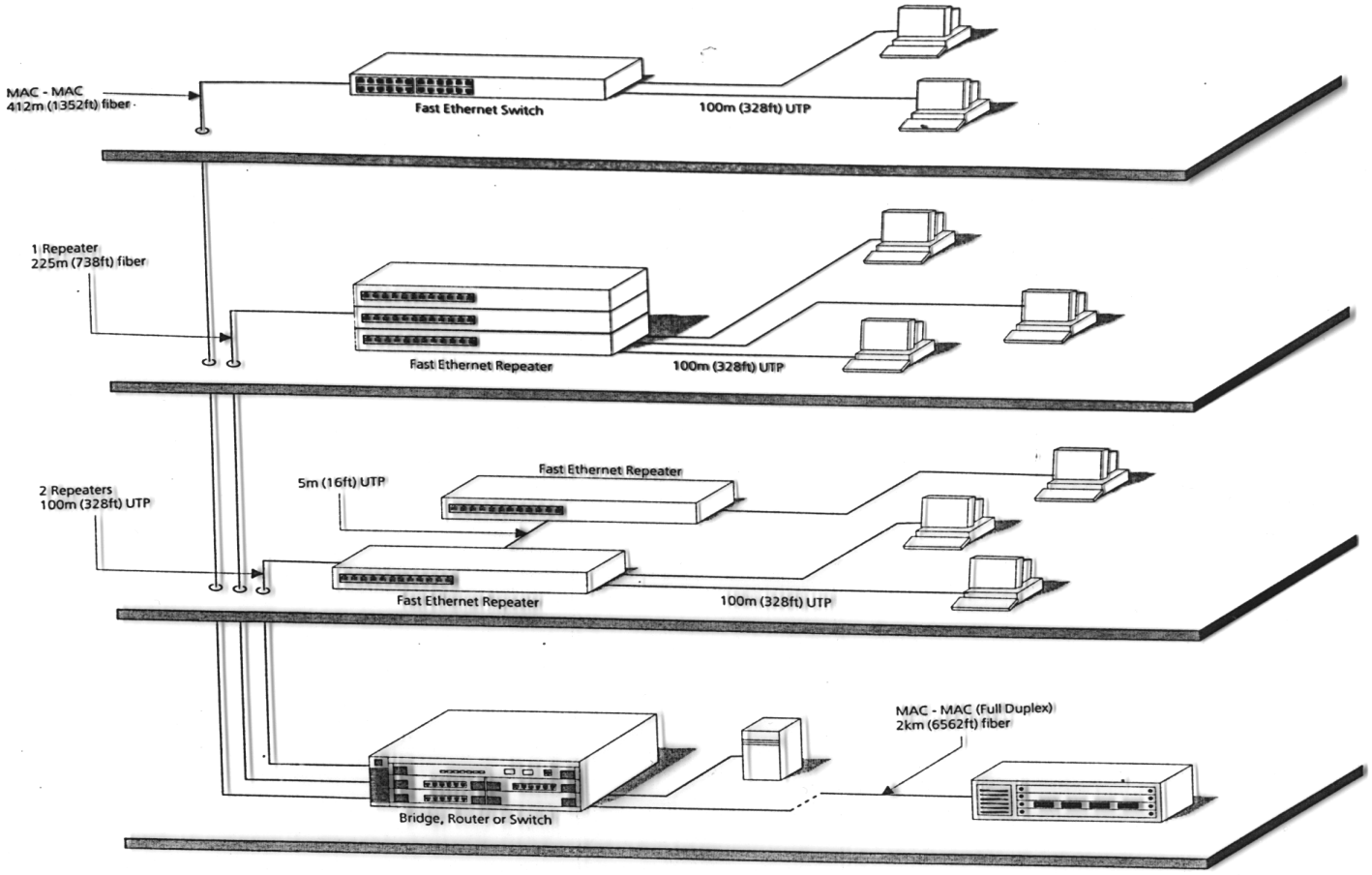
LAN: koncentratory, przełączniki i routery



LAN: koncentratory, przełączniki i routery



LAN: koncentratory, przełączniki i routery



Urządzenia sieciowe: przełącznik warstwy 3

Przełącznik warstwy 3. (*brouter*) wykonuje swoje funkcje przekazywania pakietów na poziomie warstwy 2 i 3, pakietów uni- i multicastowych oraz rozgłoszeniowych sprzętowo, a nie programowo (jak tradycyjne routery).

Programowo obsługiwane jest administrowanie siecią, zarządzanie tabelami, obsługa wyjątków.

Sprzętowo realizowana jest polityka przekazywania pakietów pod względem:

- bezpieczeństwa
- równoważenia obciążenia
- rodzaju protokołów
- przydziału pasma i sterowanie przepływem (QoS, *Quality Of Service*)
- priorytetyzowania pakietów (CoS, *Class Of Service*)
- numerów portów protokołów TCP/UDP (*Layer 4 switching*)

Urządzenia sieciowe: przełącznik warstwy 3

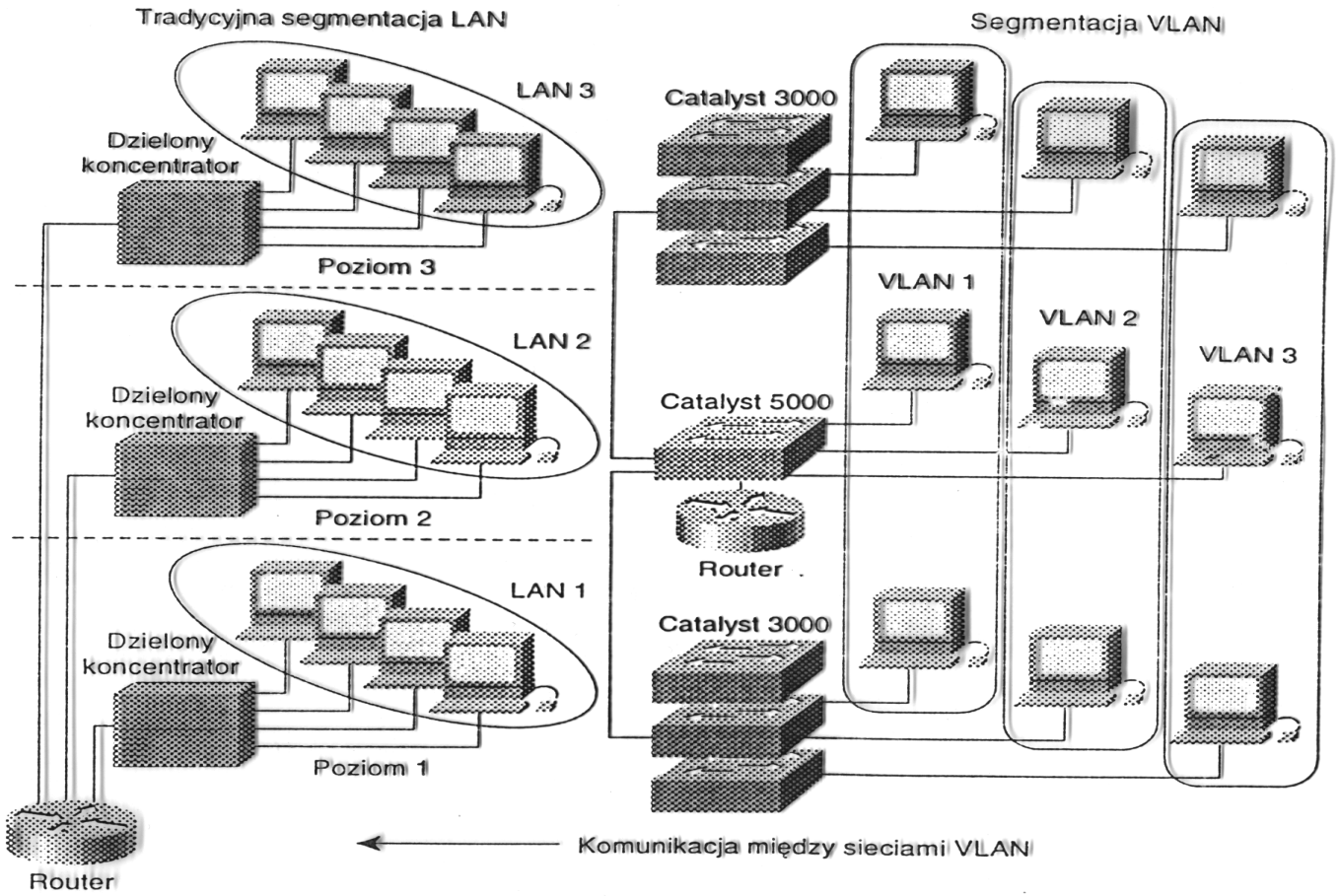
Przełącznik warstwy 3. jest routerem, gdyż:

- wyznacza trasę w oparciu o informację z nagłówka pakietu warstwy 3
- potwierdza ważność pakietu warstwy 3. w oparciu o sumę kontrolną nagłówka
- sprawdza i aktualizuje pole TTL
- odczytuje i reaguje na zawarte w nagłówku pakietu opcje
- uaktualnia statystyki przekazywanych pakietów w bazie informacji zarządzania (MIB, *Management Information Base*)
- komunikuje się z innymi routerami poprzez protokoły RIP, OSPF, itp.

Przełączniki warstwy 3. nadają się dobrze do jednoczesnego przekazywania zwykłych danych oraz strumieni audio/wideo.

Routery są niezbędne do podłączenia sieci korporacyjnej do sieci WAN.

Wirtualne sieci lokalne

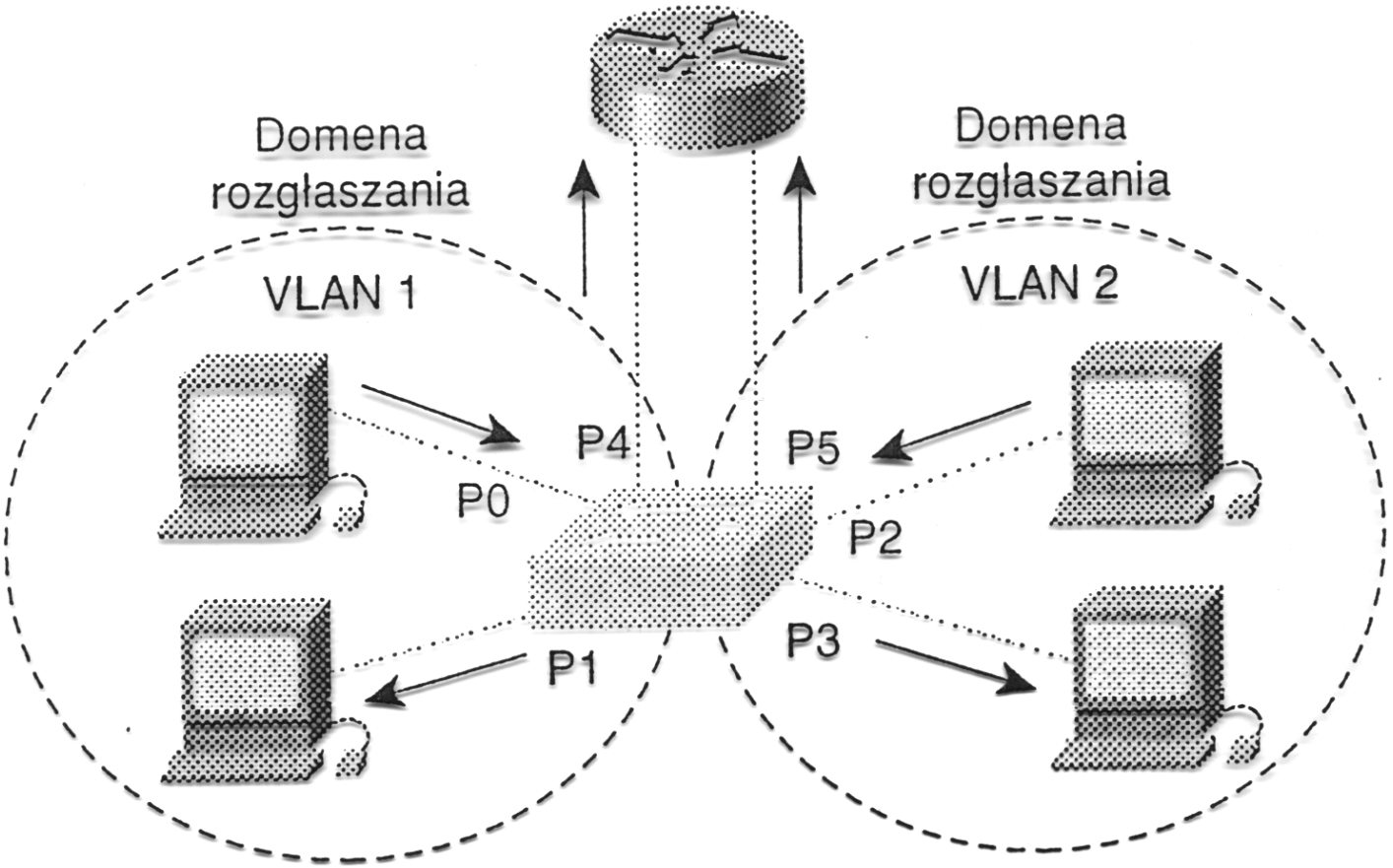


Wirtualne sieci lokalne

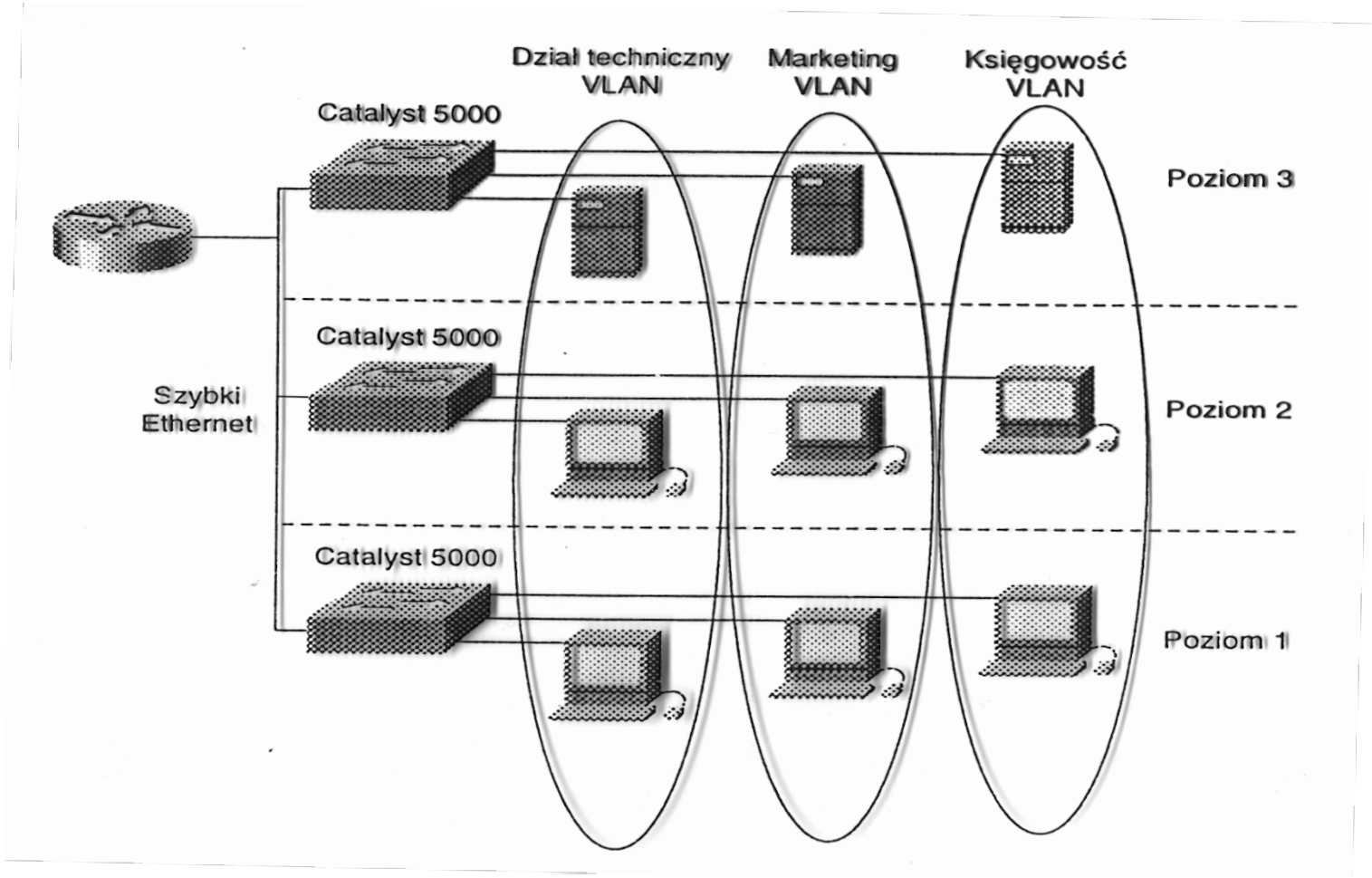
W typowej sieci LAN użytkownicy są grupowani w oparciu o ich położenie względem koncentratora/przełącznika. Użytkownicy (zwykle) różnych kategorii walczą o pasmo, dostęp do routera i sieci szkieletowej.

- 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 przez routing warstwy 3.
- Użytkownicy są przypisywani do sieci VLAN przez administratora.

Wirtualne sieci lokalne



Wirtualne sieci lokalne



Wirtualne sieci lokalne

- 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.

IEEE 802.1q dopuszcza 4094 VLAN-ów; 1. (VID=0) i 4096. (VID=4095) są zarezerwowane.[53]

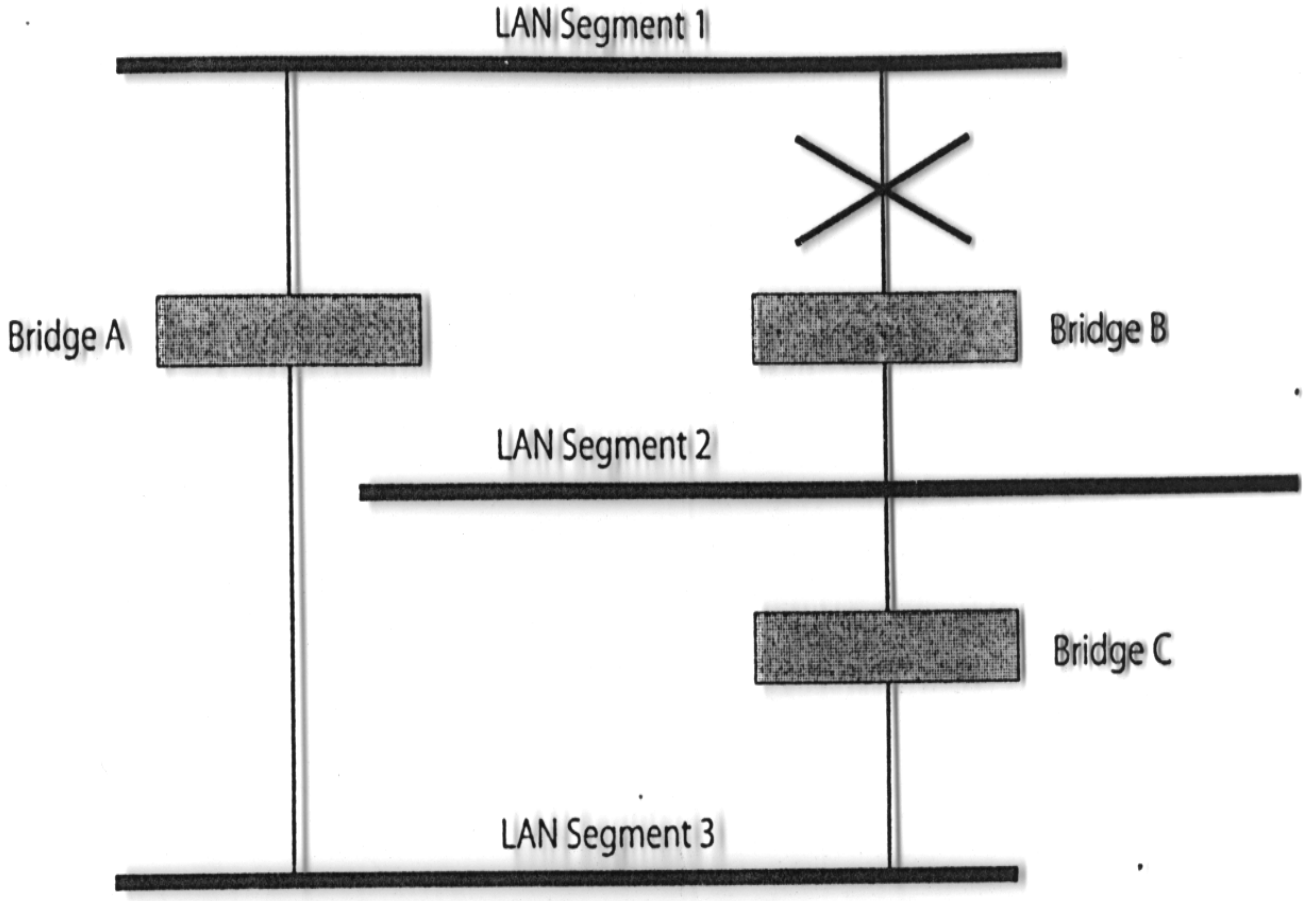
[53] PVID i *native* VLAN, zob. What is PVID?

Wirtualne sieci lokalne

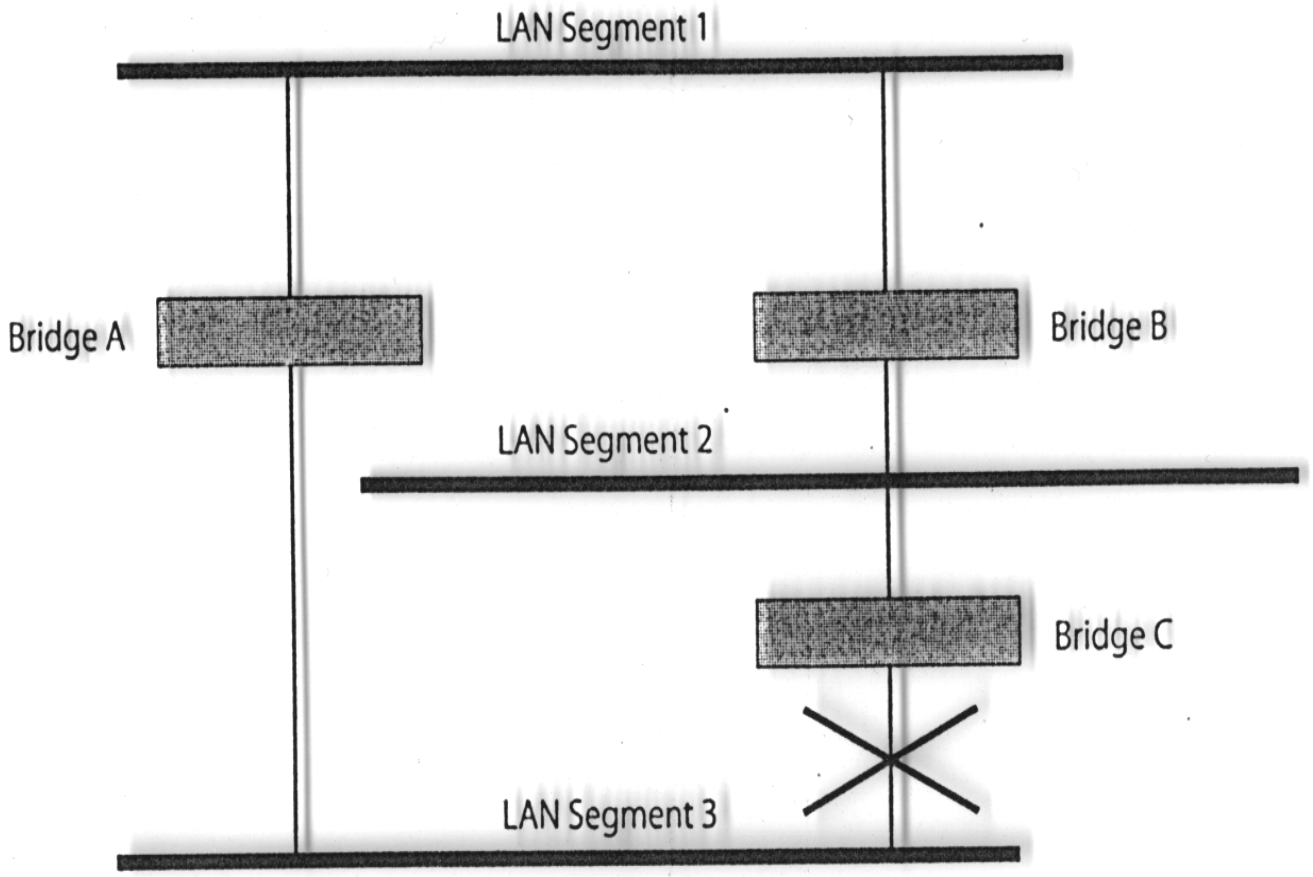
Zalety sieci VLAN:

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

Jak zapewnić nadmiarowe połączenia między segmentami?



Jak zapewnić nadmiarowe połączenia między segmentami?



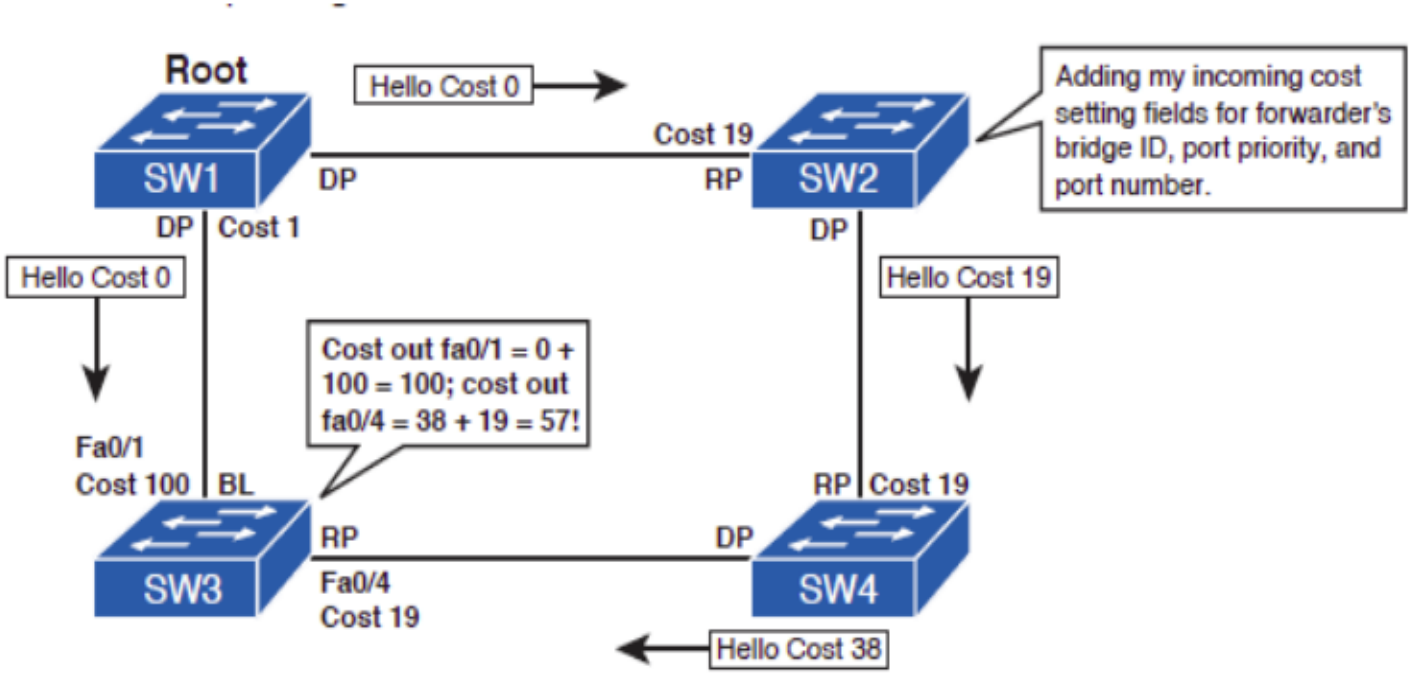
Protokół częściowego drzewa (STP, *Spanning Tree Protocol*)

STP umożliwia użycie podwójnych dróg na potrzeby ruchu sieciowego i wykorzystuje schemat wykrywania pętli w sieci w celu:

- wyznaczenia efektywności każdej z dróg
- uaktywnienia najlepszej drogi
- zdezaktywowania wszystkich mniej efektywnych połączeń
- uaktywnienie jednej z mniej efektywnych dróg, w przypadku awarii najlepszego połączenia
- komunikacja pomiędzy przełącznikami odbywa się poprzez wymianę BPDU (*Bridge Protocol Data Unit*)

RSTP (*Rapid STP*) oraz MSTP (*Multiple STP*) są nowszymi wersjami STP zapewniającymi szybszą zbieżność oraz lepsze działanie w przypadku wielu VLAN-ów.

Protokół częściowego drzewa[54]



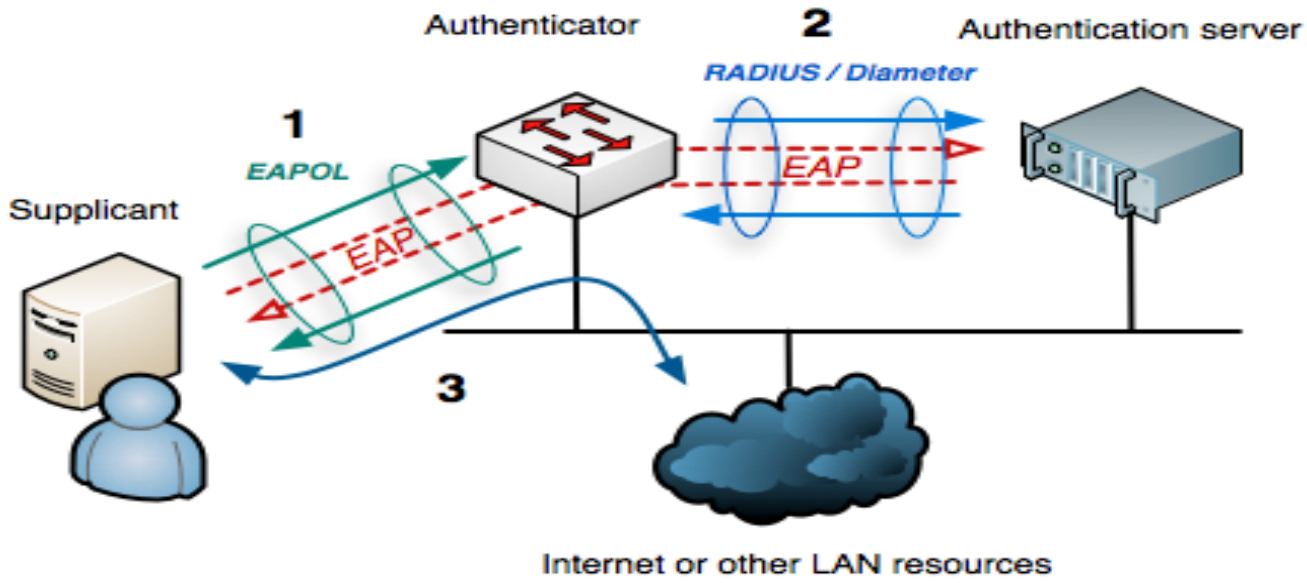
[54] Spanning Tree Protocol: Root Port Cost

Urządzenia sieciowe: Cisco/Linksys SRW2048[55]

- segmentacja via wirtualne LAN-y (*Virtual LAN*) wg IEEE 802.1Q
- możliwość traktowania wielu równoległych połączeń jako jednego (agregacja połączeń, *port trunking, link aggregation*)
- możliwość tworzenia zapasowych połączeń i podwójnych ścieżek w ramach protokołu częściowego drzewa (STP, *Spanning Tree Protocol*, IEEE 802.1d; MSTP *Multiple Spanning Tree Protocol* IEEE 802.1s, IEEE 802.1Q-2003)
- ograniczanie pasma (*ingress rate limit, policing*), kształtowanie ruchu wyjściowego (shaping, *egress shaping rates* (CIR, CBS)), IGMP Snooping (*Internet Group Management Protocol*), sterowanie sztormami
- wsparcie dla protokołów GARP, GVRP, GMRP[56]
- bezpieczne zarządzanie via SSH/SSL, uwierzytelnianie użytkownika via 802.1x oraz filtrowanie MAC
- kontrolowanie i konfigurowanie urządzenia za pomocą CLI, przeglądarki WWW, protokołu SNMP (*Simple Network Management Protocol*) oraz RMON-u (*Remote network MONitoring*)

[55] http://www.linksys.com/
[56] *The Generic Attribute Registration Protocol*, *GARP VLAN Registration Protocol*, *GARP Muticast Registration Protocol*

IEEE 802.1x[57]



EAPOL – EAP (*Extensible Authentication Protocol*) over LAN

[57] IEEE_802.1X

HP E4510G (3COM 4510G)[58]

- Layer 2 switching
  - VLAN support and tagging – support IEEE 802.1Q, with 4094 simultaneous VLAN IDs
  - GARP VLAN Registration Protocol (GVRP) – allows automatic learning and dynamic assignment of VLANs
  - IP multicast snooping and data-driven IGMP – automatically prevents flooding of IP multicast traffic
  - Jumbo packet support – supports up to 9220-byte frame size to improve performance of large data transfers
  - IEEE 802.1ad QinQ – increases the scalability of an Ethernet network by providing a hierarchical structure; connects multiple LANs on a high-speed campus or metro network
- Layer 3 routing
  - Static IP routing – provides manually configured routing; includes ECMP (*Equal-Cost Multi-Path*) routing capability
  - Routing Information Protocol (RIP) – provides RIPv1 and RIPv2 routing

[58] http://h17007.www1.hp.com/us/en/products/switches/HP_E4510G_Switch_Series/

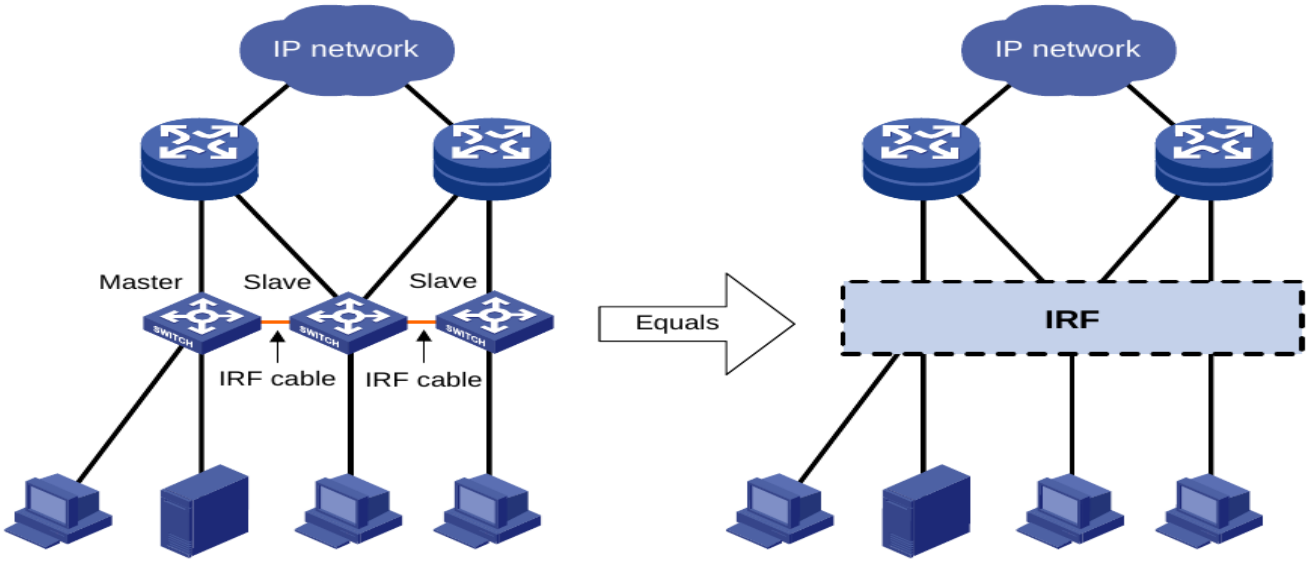
HP E4510G (3COM 4510G)

- Quality of Service (QoS)
  - Layer 4 prioritization – enables prioritization based on TCP/UDP port numbers
  - Traffic prioritization (IEEE 802.1p) – allows real-time traffic classification into eight priority levels mapped to eight queues
  - Class of service (CoS) – sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
  - Rate limiting – sets per-port ingress enforced maximums and per-port, per-queue guaranteed minimums
  - Bandwidth shaping
    * Rate limiting – provides per-port, ingress-based enforced bandwidth maximums
    * Guaranteed minimums – provides per-port, per-queue egress-based guaranteed bandwidth minimums
  - Broadcast control – allows limitation of broadcast traffic rate to cut down on unwanted broadcast traffic on the network

HP E4510G (3COM 4510G)

- Security
  - Access control lists (ACLs) – provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number
  - RADIUS/TACACS+ – eases switch management security administration by using a password authentication server
  - Secure Shell (SSHv2) – encrypts all transmitted data for secure, remote command-line interface (CLI) access over IP networks
  - Secure Web management with HTTPS and SSL – encrypts all HTTP traffic, allowing secure access to the browser-based management GUI in the switch
  - Port security – allows access only to specified MAC addresses, which can be learned or specified by the administrator
  - Secure management access – securely encrypts all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
  - Automatic VLAN assignment – automatically assigns users to the appropriate VLAN based on their identity and location and the time of day

Intelligent Resilient Framework[59]



Producenci sprzętu sieciowego określają takie łączenie przełączników mianem stosu.

[59] HP E4510G Configuration Guide

Współczesny model sieci versus OSI i TCP/IP

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

Standardy EIA/TIA-568A i EIA/TIA-568B[60]

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

[60] EIA, *Electronics Industry Association* – Towarzystwo Przemysłu Elektronicznego, TIA, *Telecommunications Industry Association* – Towarzystwo Przemysłu Telekomunikacyjnego

Standardy EIA/TIA-568B

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); wtyk RJ-45

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 jedno/wielomodowy

Schematy łączenia T568A i T568B[61]

8P8C Wiring (TIA/EIA-568-A T568A)

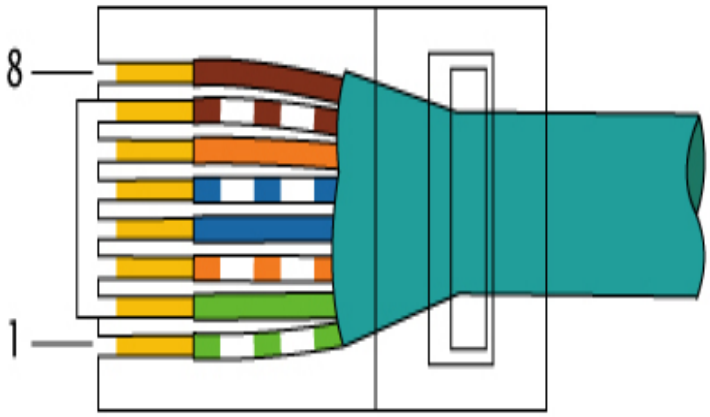
Pin	Pair	Wire	Color
1	3	1	white/green
2	3	2	green
3	2	1	white/orange
4	1	2	blue
5	1	1	white/blue
6	2	2	orange
7	4	1	white/brown
8	4	2	brown

8P8C Wiring (TIA/EIA-568-B T568B)

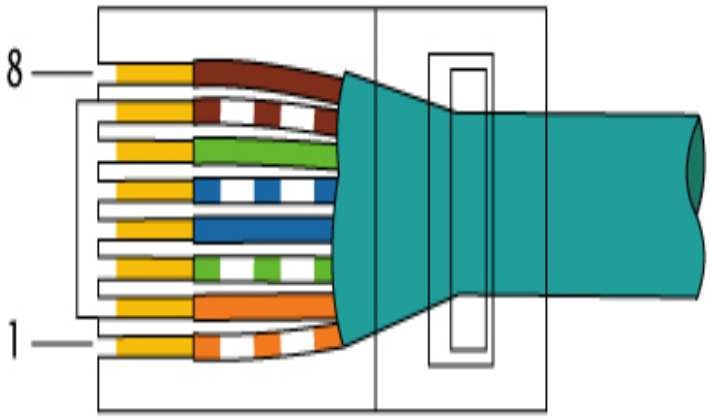
Pin	Pair	Wire	Color
1	2	1	white/orange
2	2	2	orange
3	3	1	white/green
4	1	2	blue
5	1	1	white/blue
6	3	2	green
7	4	1	white/brown
8	4	2	brown

[61] http://en.wikipedia.org/wiki/Category_6_cable

Schematy łączenia T568A i T568B[62]



EIA/TIA-568A



EIA/TIA-568B

[62] Modular connector

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

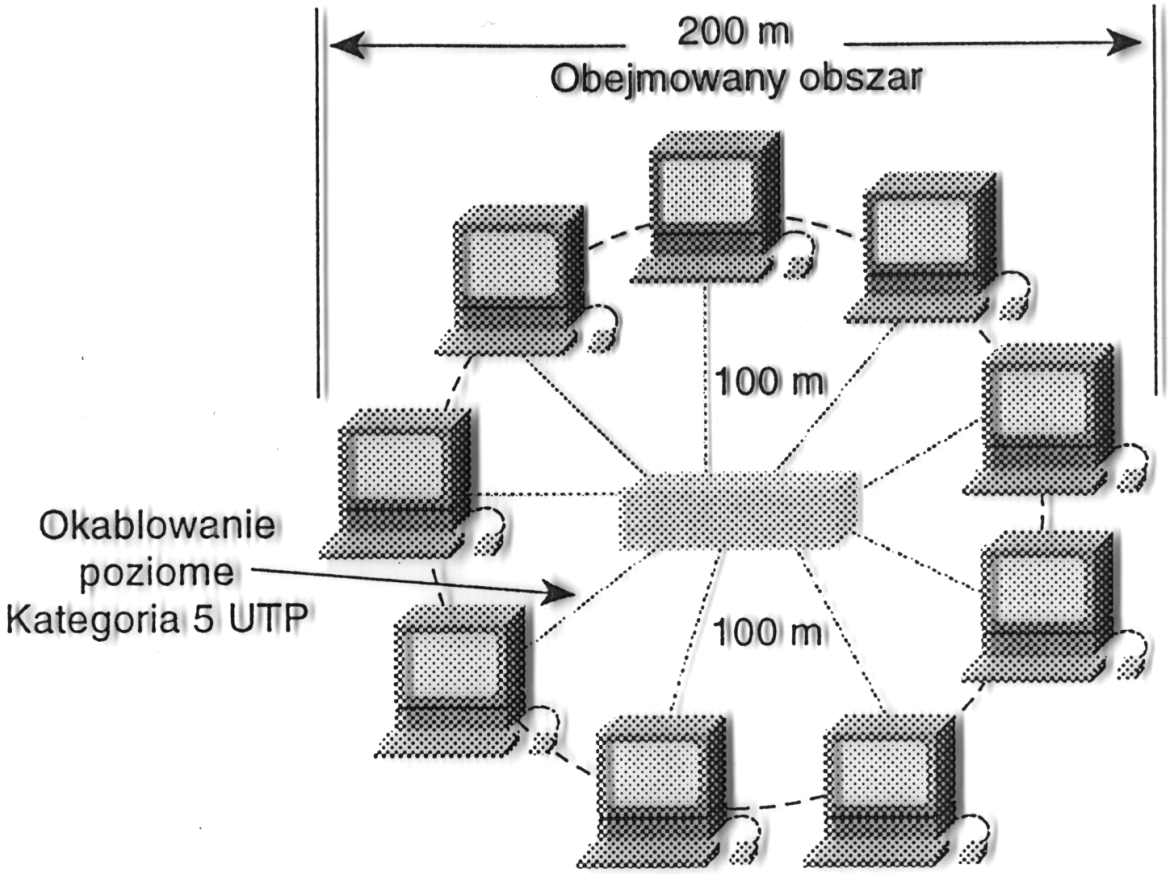
MDI (*Media Dependent Interface*)
MDI-X (*Media Dependent Interface Cross-over*)

Kabel skrośny

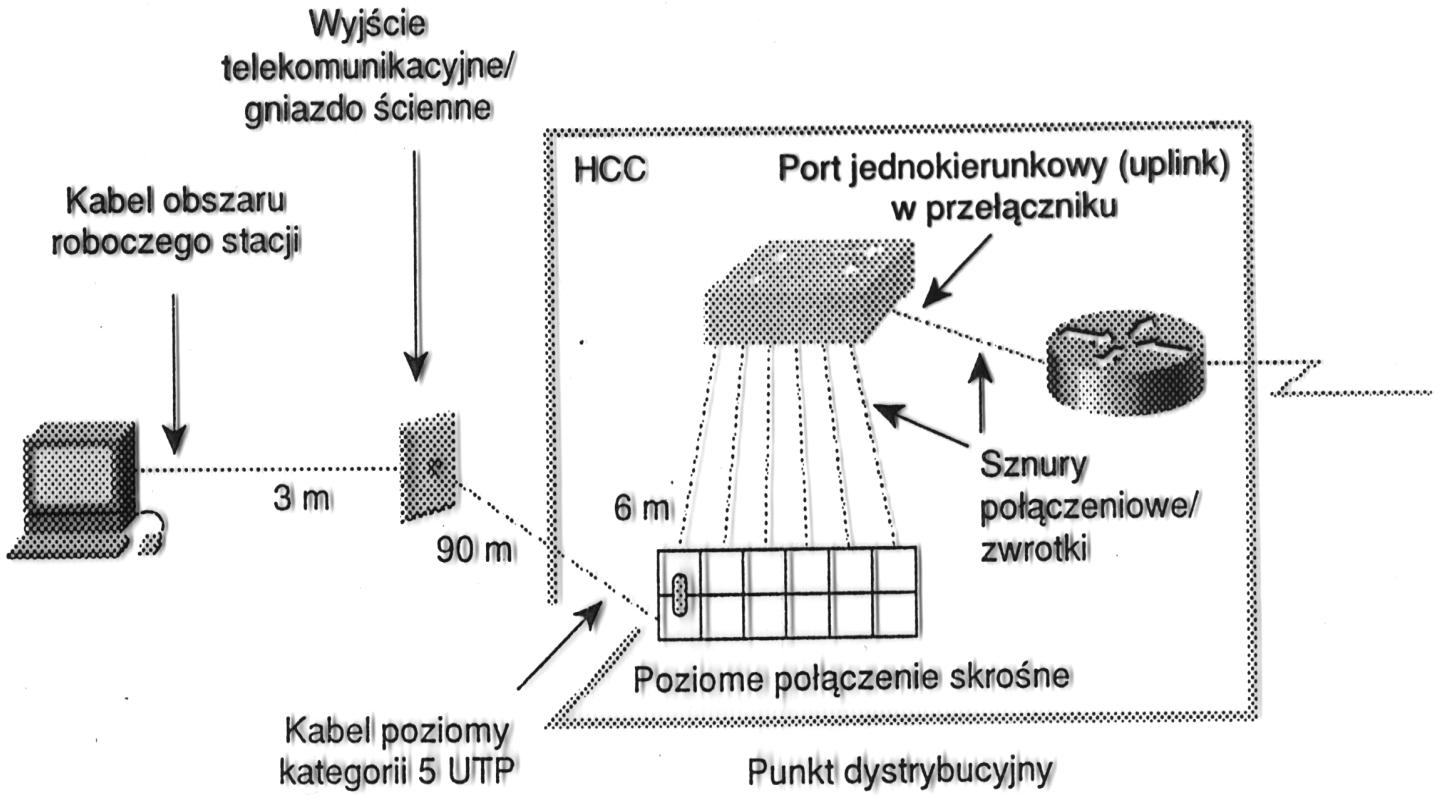
	DTE	568B (RJ-45)		568A (RJ-45)	DTE	
1	N+	biało-pomarańczowy	1 ⟶ 3	biało-zielony	N+	1
2	N–	pomarańczowy	2 ⟶ 6	zielony	N–	2
3	O+	biało-zielony	3 ⟶ 1	biało-pomarańczowy	O+	3
4		niebieski	4 ⟶ 4	niebieski		4
5		biało-niebieski	5 ⟶ 5	biało-niebieski		5
6	O–	zielony	6 ⟶ 2	pomarańczowy	O–	6
7		biało-brązowy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

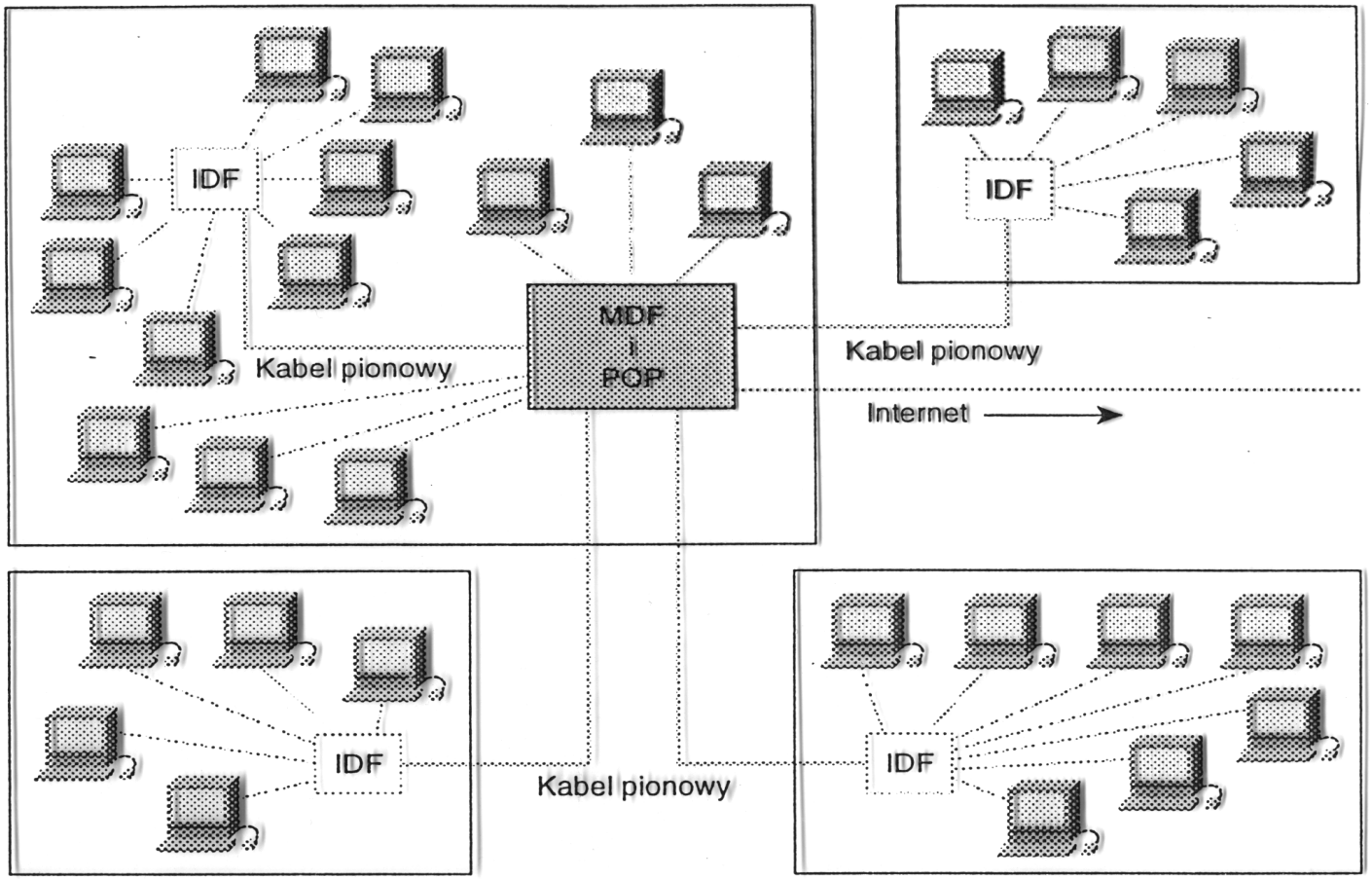
Okablowanie strukturalne



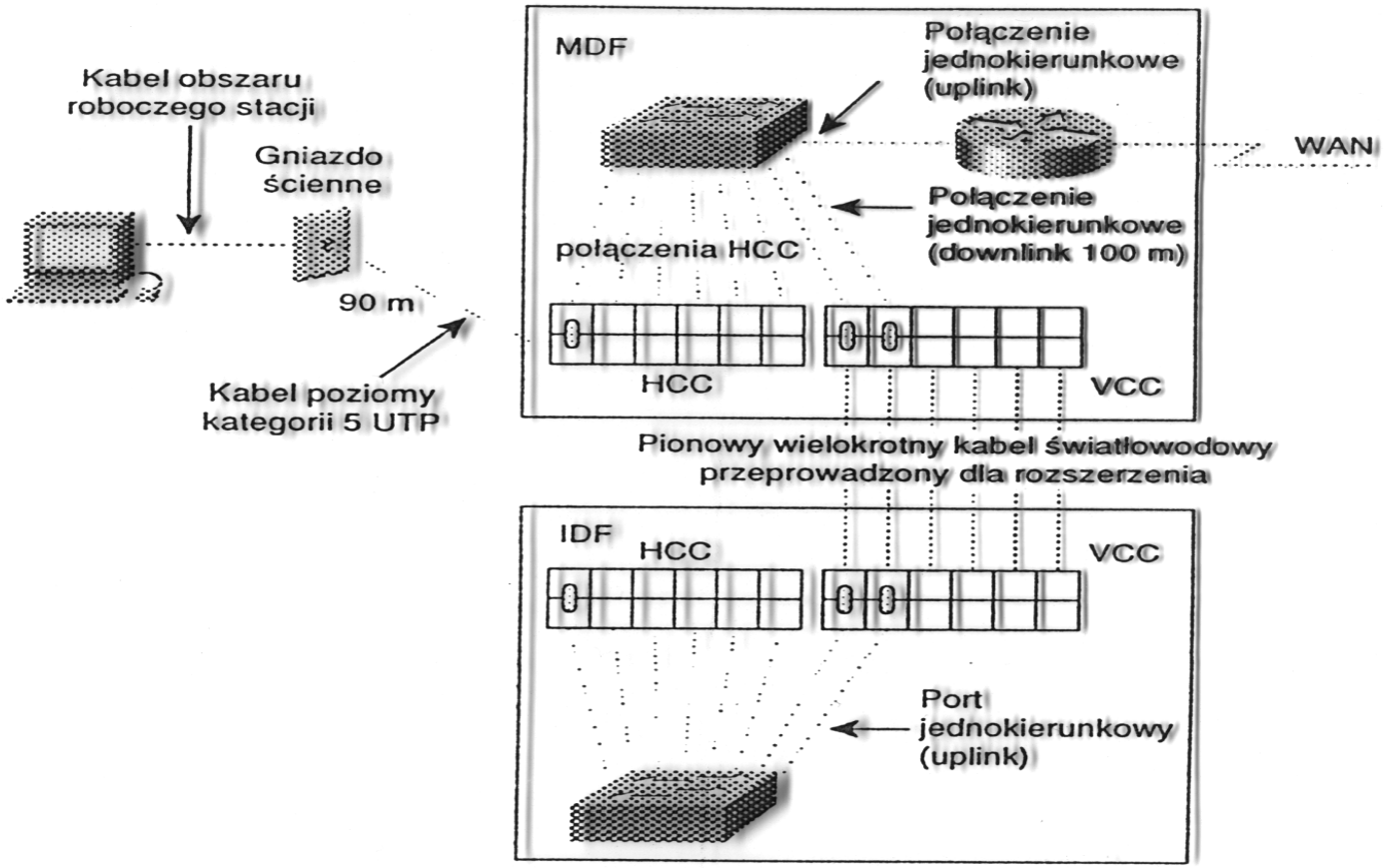
Okablowanie strukturalne



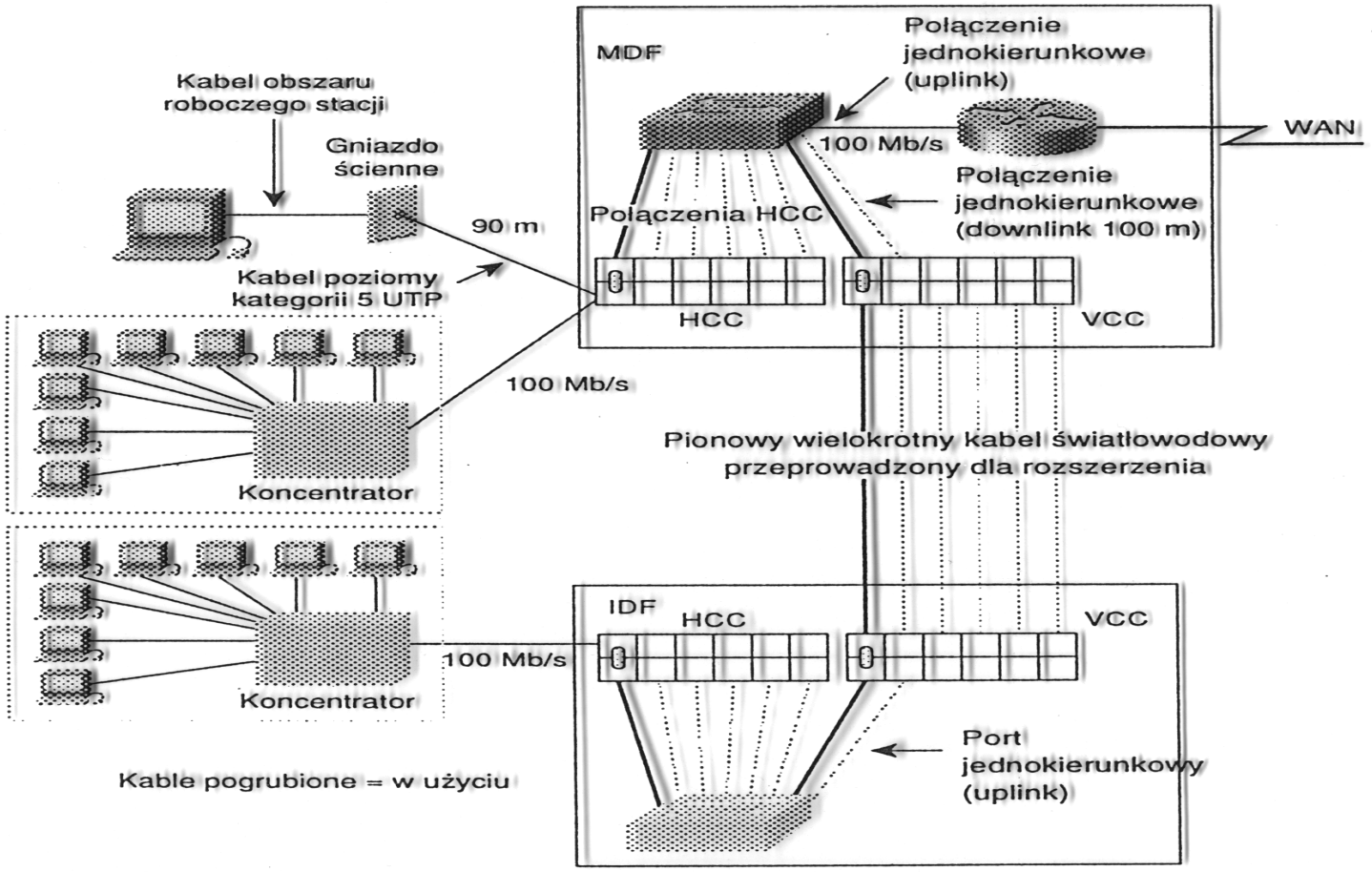
Okablowanie strukturalne



Okablowanie strukturalne



Okablowanie strukturalne



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

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
- 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*)

Okablowanie szkieletowe łączy węzły dystrybucyjne w topologii rozszerzonej gwiazdy i obejmuje

- okablowanie pionowe (pomiędzy węzłami na różnych piętrach)
- okablowanie pomiędzy MDF i POP,
- okablowanie pomiędzy budynkami

Typy mediów sieciowych:

- UTP 100 Ω
- STP 150 Ω
- światłowód wielomodowy 50/125 μm
- światłowód jednomodowy 9/125 μm

Jakość wykonania instalacji

Standardy IEEE i EIA/TIA-568B określają sposób testowania sieci po zakończeniu instalacji.

Testery okablowania wyznaczają:

- długość okablowania
- położenie wadliwych połączeń (skrzyżowane pary)
- poziomy tłumienności
- poziomy przesłuchu zbliżnego (NEXT, *Near-End CrossTalk*)
- poziomy zakłóceń
- położenie kabli w ścianach

Jakość wykonania instalacji (tester połączeń)

Tester okablowania wyznacza tzw. mapę połączeń. Połączenia mogą być

- otwarte – brak połączeń pomiędzy pinami na obu końcach kabla
- zwarte – pomiędzy dwiema lub większą liczbą linii występuje zwarcie
- skrzyżowana para – para podłączona do dwóch różnych pinów na obu końcach (np. para pierwsza jest podłączona do pinów 4/5 z jednej strony i 1/2 z drugiej)
- odwrócona para (odwrócona polaryzacja) – dwie linie pary są podłączone do odwrotnych pinów z każdej strony kabla (linia podłączona do pinu 1 na jednym końcu jest przyłączona do pinu 2 na drugim końcu kabla)
- rozszczepiona para – jedna linia z każdej z dwóch par jest podłączona tak, jakby stanowiła część jednej pary przewodów

Zasady łączenia urządzeń 10Base-T[63]

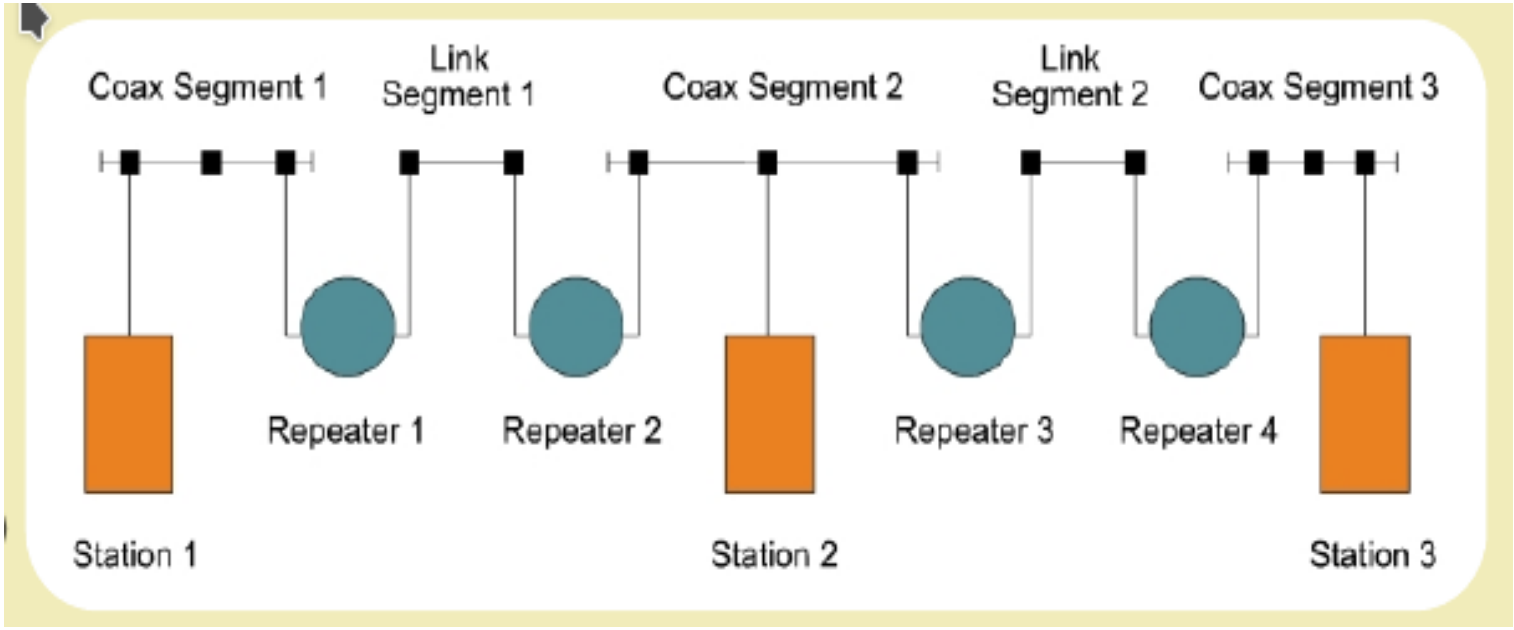
Zasada 5-4-3-2-1:

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

Maksymalna wielkość sieci jest ograniczona czasem propagacji sygnału. Czas propagacji sygnału pomiędzy dwoma najbardziej odległymi węzłami nie może przekroczyć $\frac{1}{2} \times 51.2\mu$s.

[63] TechBrief1_P1.pdf

10Base-T: zasada 5-4-3-2-1[64]



[64] TechBrief1_P1.pdf

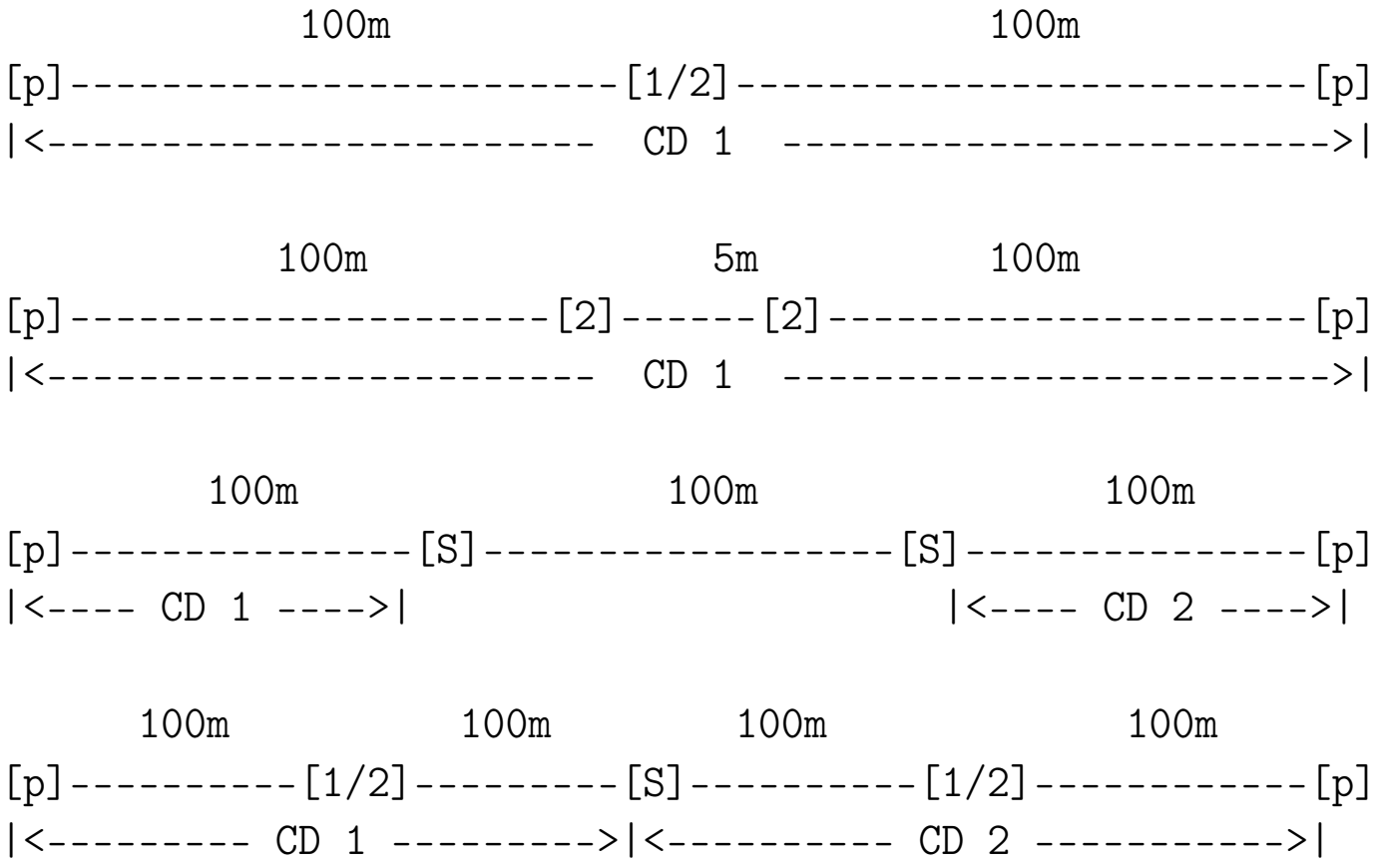
Zasady łączenia urządzeń Fast Ethernet 100Base-TX[65]

Legenda:

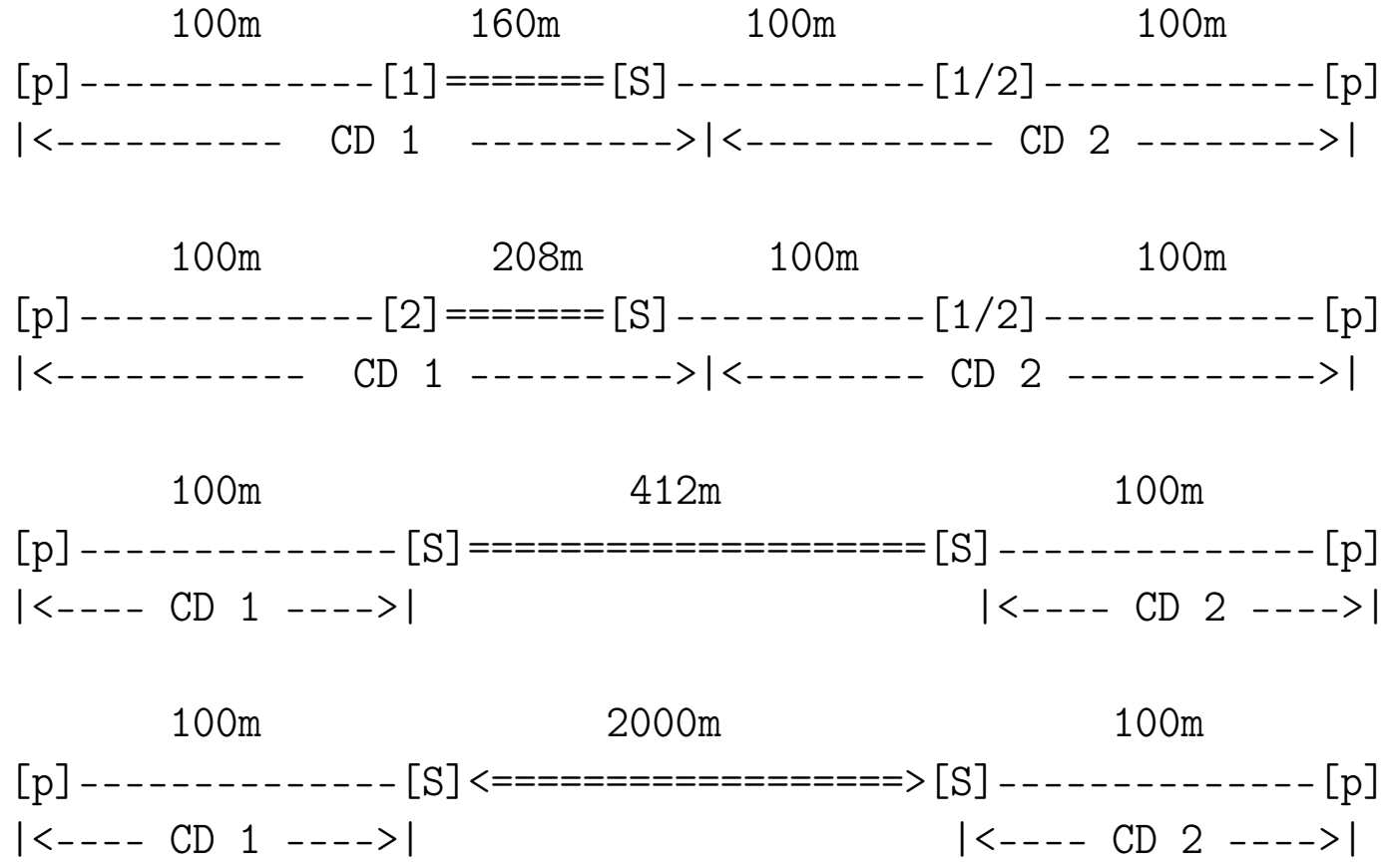
```
[p] : PC; the terminal nodes
[1] : 100 Base-TX Class I Repeater
[2] : 100 Base-TX Class II Repeater
[1/2] : 100 Base-TX Class I or Class II Repeater
[S] : 10 Base-T/100 Base-TX Switch
----- : TX cable (Twisted Pairs cable)
        (Cat. 5 UTP/STP cable for 100 Base-TX,
         Cat. 3, 4, or 5 UTP/STP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

<- CD ->: Collision Domain
```

[65] TechBrief1_P1.pdf

Zasady łączenia urządzeń 100Base-TX



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



Zasady łączenia urządzeń Fast Ethernet

Maksymalna wielkość sieci jest ograniczona czasem propagacji sygnału. Czas propagacji sygnału pomiędzy dwoma najbardziej odległymi węzłami nie może przekroczyć $\frac{1}{2} \times \frac{1}{10} \times 51.2$ μs. Opóźnienia można wyznaczyć wg danych z poniższej tabeli:

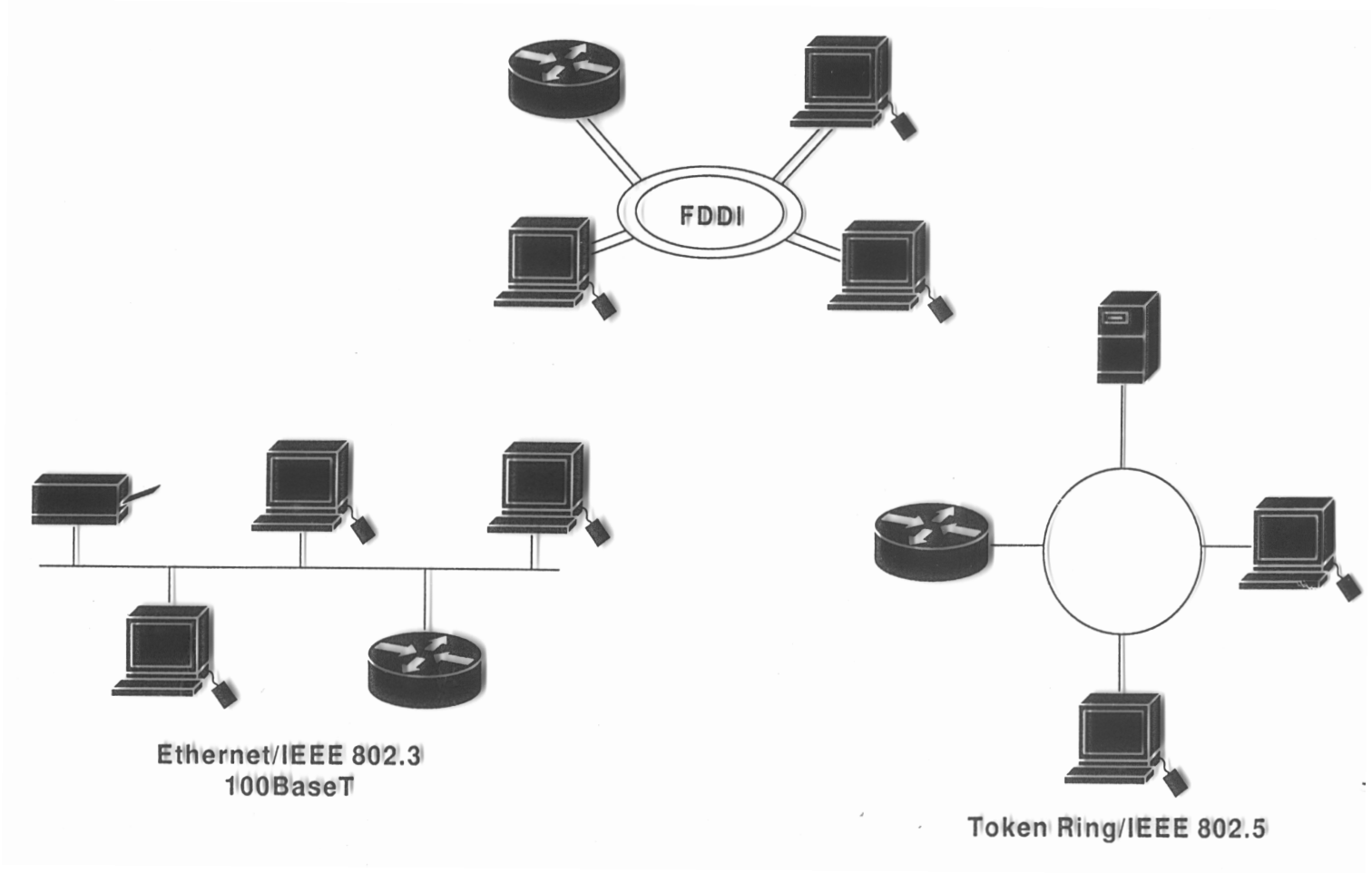
Element	Opóźnienie (w μs)
karta sieciowa	0.25
port przełącznika	0.25
koncentrator klasy I	0.70
koncentrator klasy II	0.46
kabel UTP (100 m)	0.55
światłowód wielomodowy (100 m)	0.50

Zasady łączenia urządzeń Gigabit Ethernet[66]

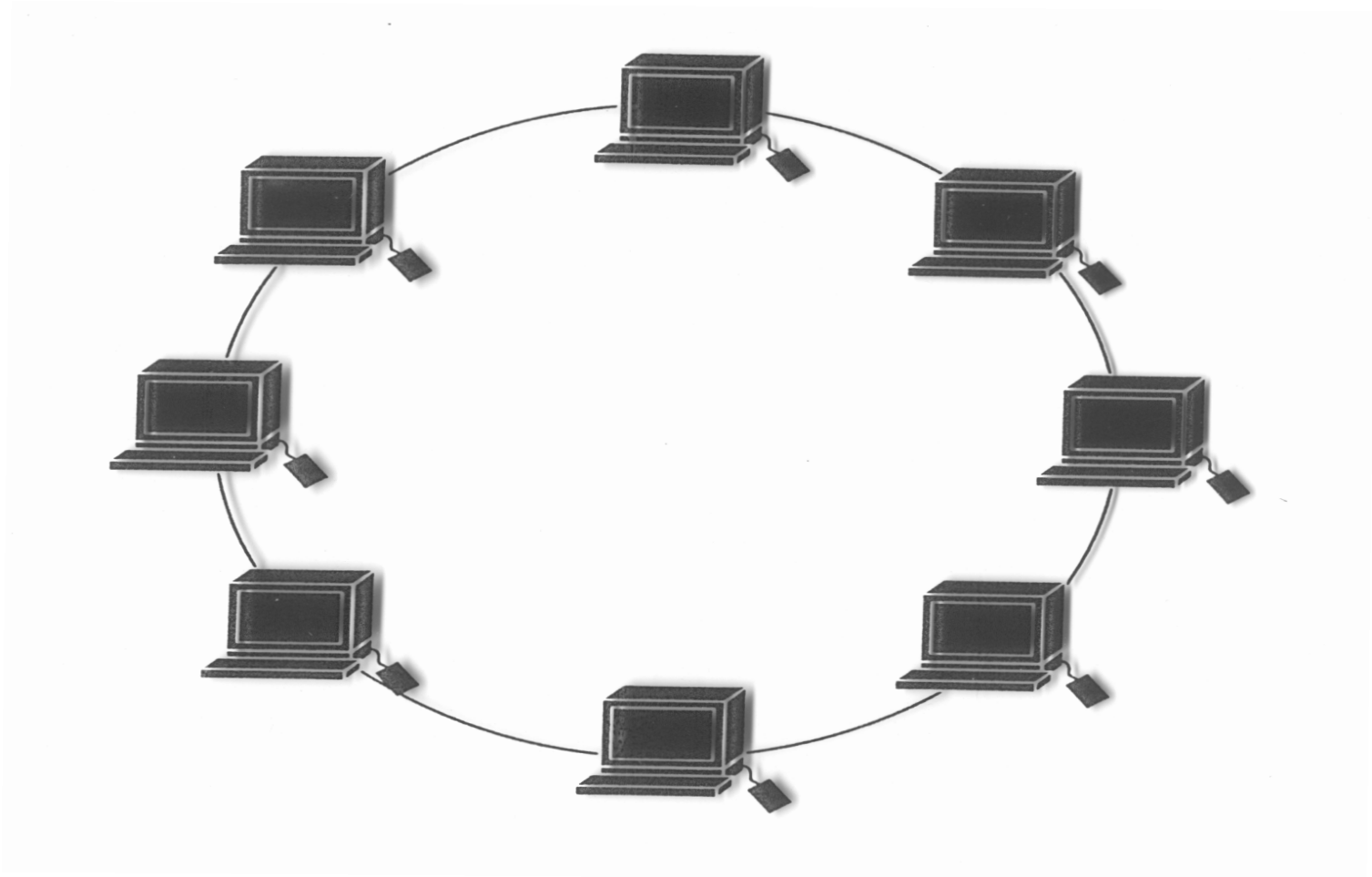
- kolizje muszą zostać wykryte w czasie potrzebnym do nadania ramki o długości 512 B (=4096 bitów), czyli w czasie 4.096 μs; czas propagacji sygnału od nadawcy do odbiorcy nie może przekroczyć 2.048 μs
- sieci budowane są (w praktyce) wyłącznie w oparciu o przełączniki
- dowolna liczba przełączników pomiędzy skrajnymi punktami sieci (ale STP wprowadza ograniczenie do 7. skoków!)
- rosnąca liczba przełączników powiększa domenę rozgłoszeniową, zmniejsza dostępne pasmo i może prowadzić do przepełniania tablic adresów MAC

[66] TechBrief1_P2.pdf

Sieć Token Ring



Sieć Token Ring



Sieć Token Ring

System komunikacji wykorzystywany w sieciach lokalnych wykorzystujących protokoły *Token Ring* (IEEE 802.5) oraz FDDI (*Fiber Distributed Data Interface*, IEEE 802.8).

- szybkość: 4/16/100 Mb/s
- nośniki: TP, kabel koncentryczny, światłowód
- dostęp do łącza: przekazywanie żetonu
  - w systemie ciągle krążą puste, pozbawione informacji ramki
  - komputer-nadawca umieszcza w ramce wiadomość, adres przeznaczenie i żeton (*token*) (zmieniając ustalony bit w ramce z 0 na 1)
  - komputer-odbiorca kopiuje wiadomość i usuwa żeton
  - komputer-nadawca stwierdza brak żetonu i usuwa wiadomość
  - jeśli ramka zginie, to wytwarza się nową

Techniki PLC (*PowerLine Communications*)

Prąd elektryczny jest przesyłany liniami wysokiego, średniego i niskiego napięcia. Dla każdego z tych systemów rozprowadzania energii elektrycznej opracowano techniki przesyłania sygnałów cyfrowych poprzez wykorzystywanie odpowiednio dobranego (modulowanego) sygnału wysokiej częstotliwości.

- zalety: nie trzeba inwestować w budowę okablowania
- wady: wysoki stopień zakłóceń w przewodach, emitowanie zakłóceń do środowiska i niedokończony proces normalizacyjny

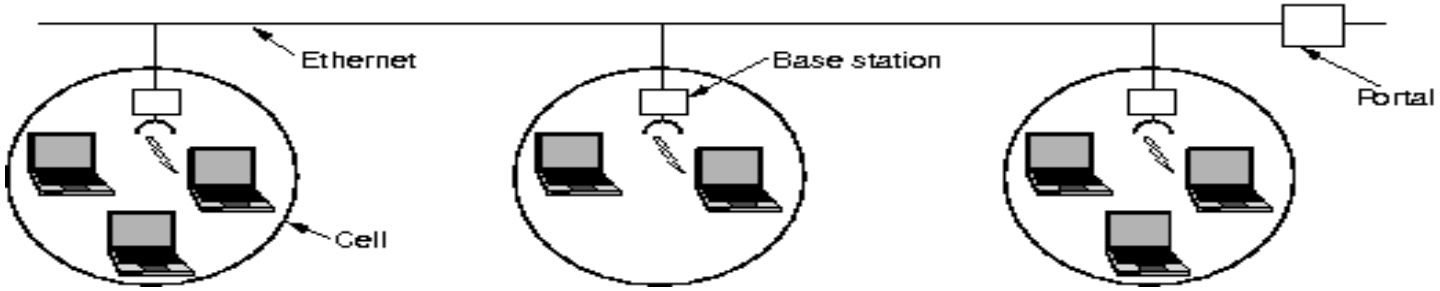
Techniki PLC

Typy technologii PLC:

- samochodowe: instalacja elektryczna (DC) pojazdu służy do przekazywania w sposób cyfrowy danych, głosu, muzyki, wideo
- krótkozasięgowe/średniozasięgowe:
  - modemy PLC używają sygnałów o częstotliwościach 1.6-80 MHz, szybkość asymetryczna (od 256 Kb/s do 2.7 Mb/s)
  - koncentratory (*repeatery*) pracują z szybkością do 45 Mb/s
  - podłączenie do Internetu o szybkości do 135 Mb/s (przy transmisji od stacji transformatorowej do Internetu)
- długozasięgowe: sygnał o częstotliwości poniżej 1 kHz, odczytywanie wskazań liczników, sterowanie urządzeniami pomiarowymi

Zestawy *powerline* pozwalają na transmisję z prędkościami rzędu 100/1000 Mb/s w oparciu o typową instalację elektryczną (zasięg do 300 m).

Sieci bezprzewodowe WLAN (*Wireless LAN*)



- topologia: magistrala, gwiazda
- zasięg: od kilku do kilkuset metrów
- nośnik
  - podczerwień
  - pasma 2.4, 3.65, 5 GHz
- własności: szybkość, zasięg, interferencja

Pasma 2.4 i 5 GHz są pasmami nielicencjonowanymi, przeznaczonymi dla zastosowań przemysłowych, naukowych i medycznych (ISM).

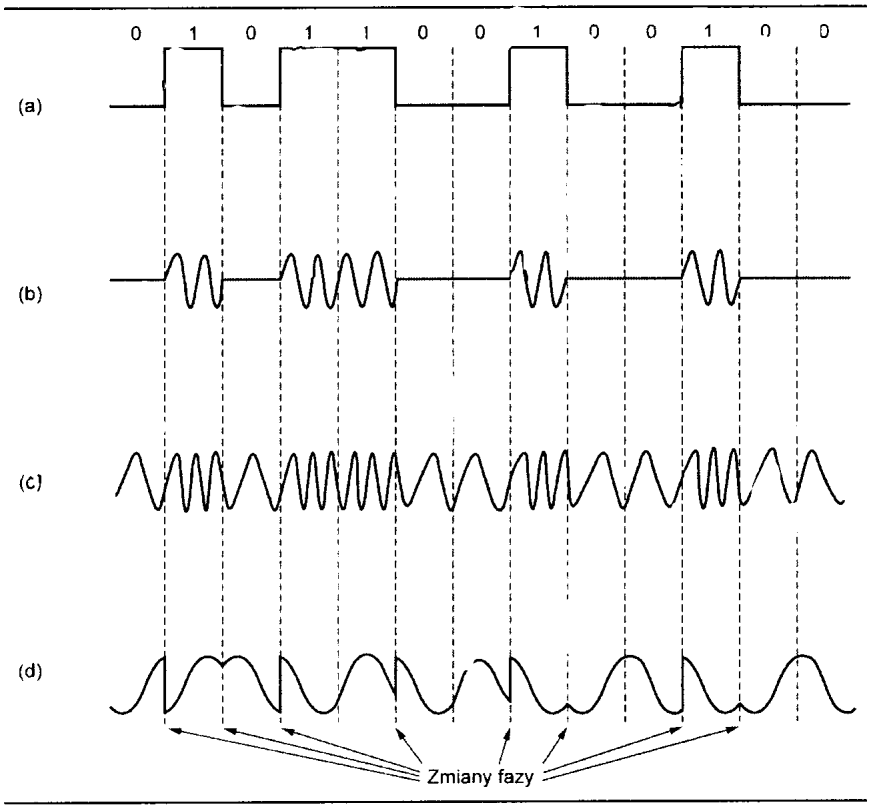
Sieci bezprzewodowe (WLAN)

LAN protocols									OSI layers
									LLC sublayer
802.11 IR	802.11 FHSS	802.11 DSSS	802.11a OFDM	802.11b HR-DSSS	802.11g OFDM	802.11n OFDM	802.11ac OFDM	802.11ax OFDMA	MAC sublayer
									Physical layer

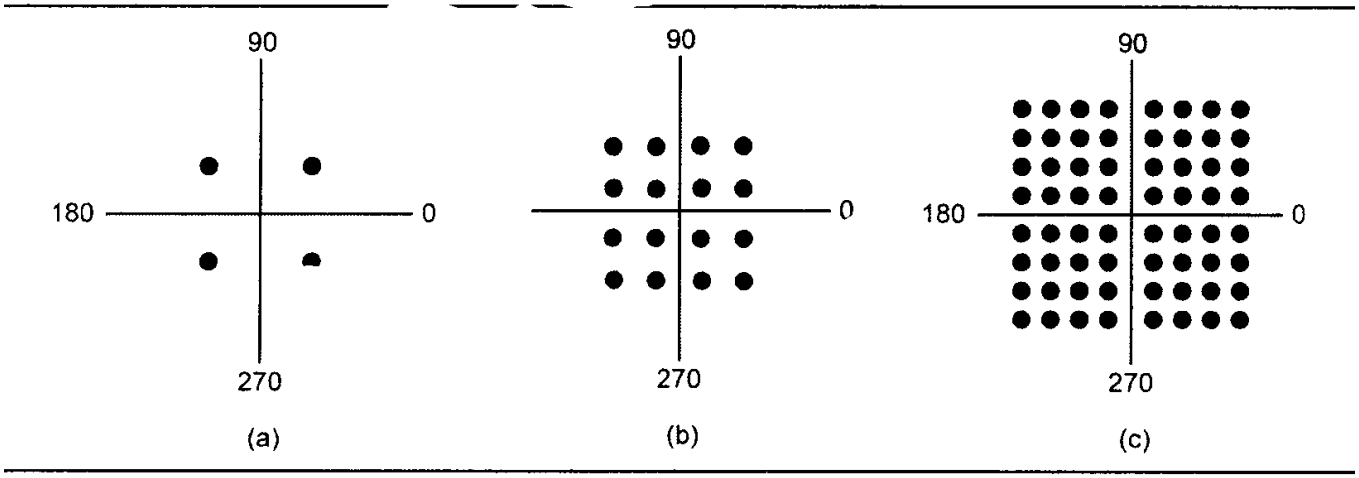
- FHSS (*Frequency Hopping Spread Spectrum*) – modulacja w widmie rozproszonym ze skokową zmianą kanału; szybkość 1, 2 Mb/s w paśmie 2.4 GHz, 79 kanałów o szerokości 1 MHz, odporność na zakłócenia[67]
- DSSS (*Direct Sequence Spread Spectrum*) – rozpraszanie widma z wykorzystaniem sekwencji bezpośredniej; szybkość 1, 2 Mb/s w paśmie 2.4 GHz, modulacja fazowa, podatność na zakłócenia
- HR DSSS (*High Rate DSSS*) – szybkość 1, 2, 5.5, 11 Mb/s w pasmie 2.4 GHz, modulacja fazowa
- OFDM (*Orthogonal Frequency Division Multiplexing*) – zwielokrotnianie z ortogonalnym podziałem częstotliwości; szybkość 54 Mb/s w pasmie 5 GHz, 52 różne częstotliwości, dobra odporność na zakłócenia, modulacja fazowa (<18 Mb/s) lub QAM
- OFDMA (*Orthogonal Frequency Division Multiple Access*) – wielodostęp z ortogonalnym podziałem częstotliwości

[67] Pomysł tej techniki komunikacji pochodzi od aktorki Hedy Lamarr i muzyka George'a Antheila, zob. Hedy Lamarr.

Sygnały – modulacja



Sygnały – kodowanie[68]



(a) kwadraturowa modulacja fazy (QPSK, *Quadrature Phase Shift Keying*)

(b) QAM-16 (*Quadrature Amplitude Modulation*)

(c) QAM-64

[68] Signal Encoding Techniques

Sieci przewodowe i bezprzewodowe – podobieństwa

- przekazywanie ramek pomiędzy kartami sieciowymi rozróżnianymi przez adres MAC
- przekazywanie danych pomiędzy urządzeniami rozróżnianymi przez adres IP
- ograniczone pasmo, powstawania zatorów
- wpływ sieci szkieletowej na jakość komunikacji
- zależność od tych samych protokołów i usług

Sieci przewodowe i bezprzewodowe – różnice

Sieci przewodowe:

- jedna droga, którą pokonują dane (przewód)
- przełączniki
- stała szybkość transmisji
- sygnał chroniony fizycznie
- proste nawiązywanie połączenia

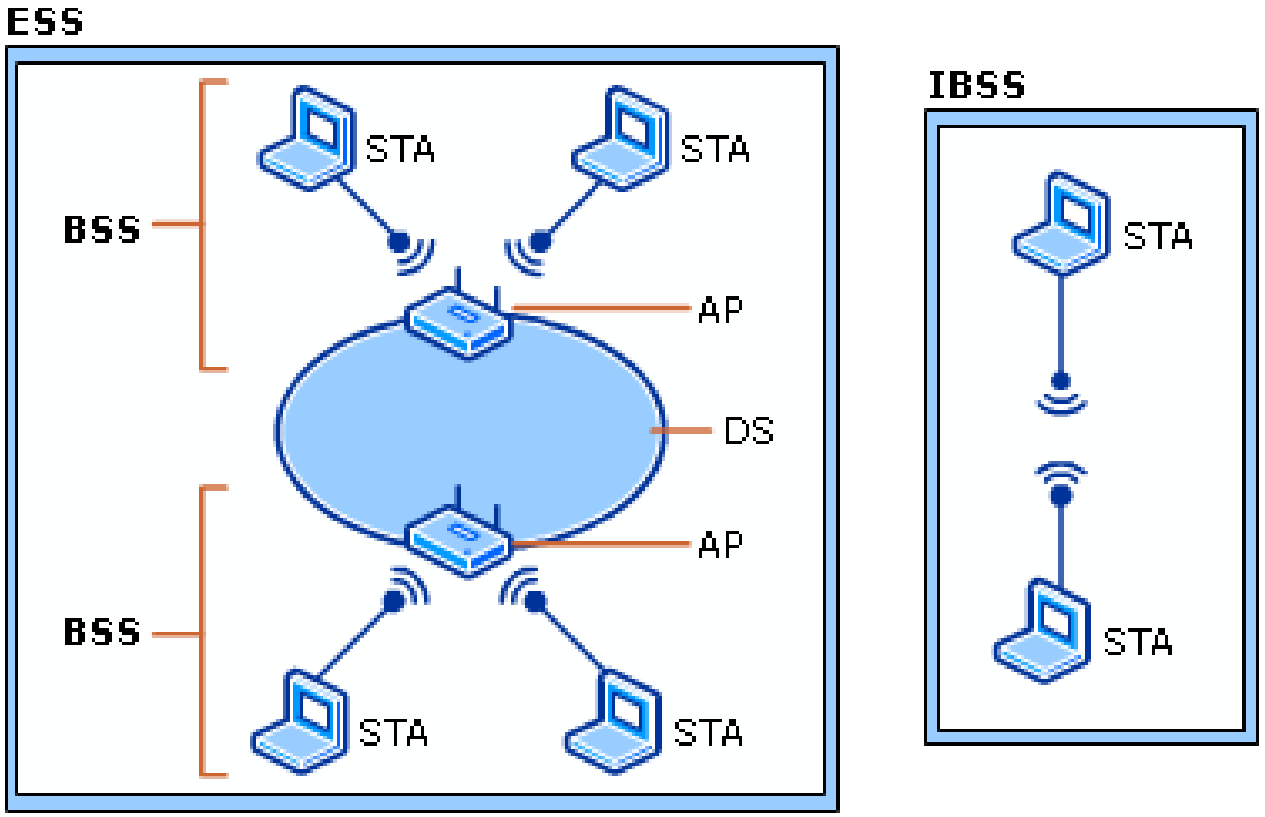
Sieci bezprzewodowe:

- wiele dróg dla danych (kanały)
- wspólnie używane medium (jak koncentrator)
- szybkość transmisji danych zależna od odległości
- transmisja dostępna dla każdego
- złożony proces nawiązywania połączenia

Jak działa sieć 802.11?

- CSMA/CA (*Collision Avoidance*)
- warstwa 2: komunikacja MAC-MAC, transmisja odbywa się jednocześnie w wielu kanałach („indywidualne przewody")
- kanały realizowane w medium współdzielonym (jak koncentrator)
  - walka o dostęp do medium
  - komunikacja w półdupleksie
  - pasmo jest dzielone przez wszystkie urządzenia bezprzewodowe (czas na nadawanie jest bardzo cenny: 1 Mbs – 36ms/beacon, 11 Mbs – 3.5 ms/beacon, 24 Mbs – 1.5 ms/beacon)
- siła sygnału maleje z odległością (jak $1/r^2$)
- sygnał podatny na zakłócenia radiowe (*RF interference*)

Architektura 802.11: BSS, EBSS i IBSS[69]



[69] How 802.11 Wireless Works

Architektura 802.11: BSS, EBSS i IBSS

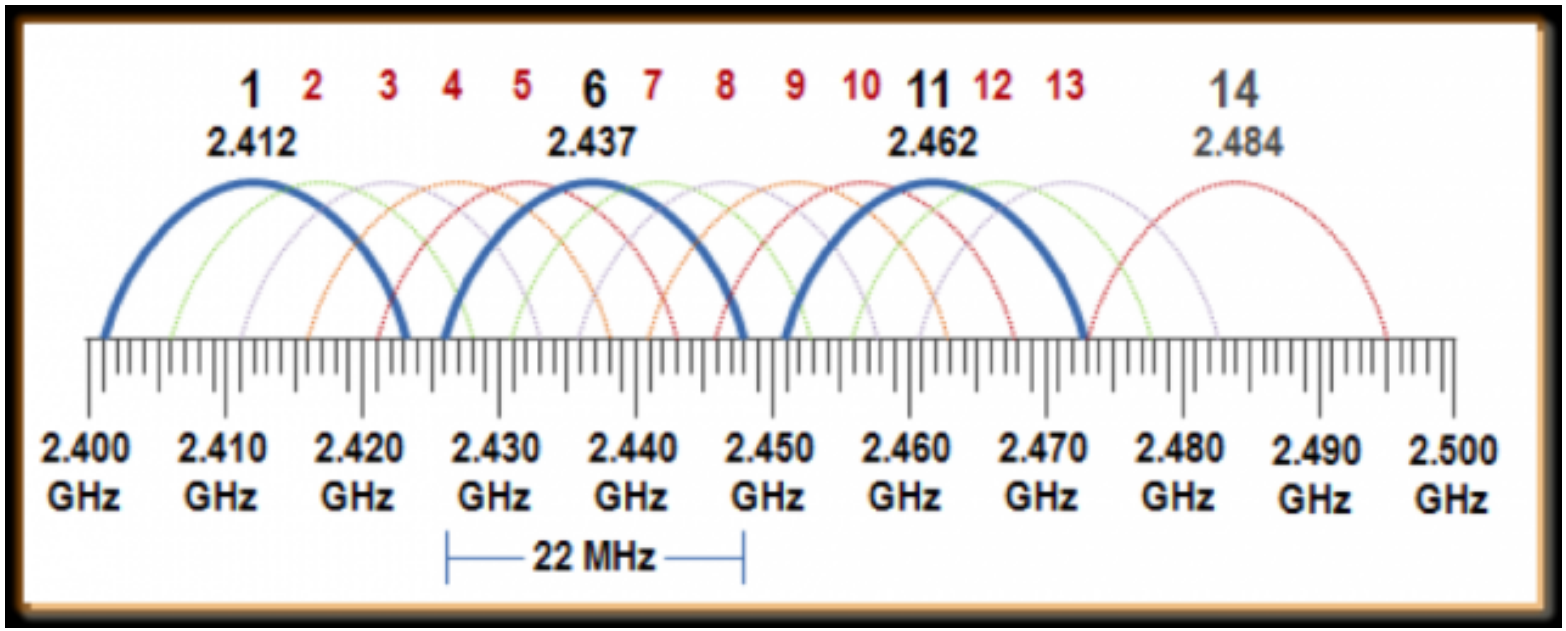
- STA (Station) – stacja
- Access-Point (AP) – punkt dostępowy
- Independent Basic Service Set (IBSS) – niezależny podstawowy zestaw usługowy
- Basic Service Set (BSS) – podstawowy zestaw usługowy
- Extended Service Set (ESS) – rozszerzony zestaw usługowy
- Distribution System (DS) – zestaw rozproszony (*main/relay/remote base station*)

Podłączenie stacji do AP może wymagać uwierzytelnienia: WEP (*Wired Equivalent Privacy*), WPA/WPA2/WPA2 Personal (*Wi-Fi Protected Access*), WPA2 Enterprise (802.1x, RADIUS).

Przepustowość i zasięg

- 802.11: 1, 2 Mb/s (FHSS, 1997)
- 802.11b: 1, 2, 5.5, 11 Mb/s, 2.4 GHz (HR-DSSS), przepustowość: ≈4.3Mb/s, zasięg: ≈140 m (1999)
- 802.11g: 11, 54 Mb/s, 2.4 GHz (OFDM); przepustowość: ≈25 Mb/s, zasięg: ≈140 m
- 802.11n: 600 Mb/s (dla kanału 40 MHz, 4 strumieni), 2.4, 5 GHz, 4 MIMO/SDM (*Multiple-Input Multiple-Output/Spatial Division Multiplexing*), przepustowość ≈160 Mb/s, zasięg: ≈250 m
- 802.11a: 54 Mb/s, 5 GHz (OFDM), przepustowość ≈23 Mb/s, zasięg: ≈120 m
- 802.11ac: 5 GHz, przepustowość ≈500 Mb/s, do 8. strumieni, kanały 20/40/80/160 MHz
- 802.11ad: 60 GHz (WiGig), przepustowość ≈7 Gb/s

Rozkład kanałów w paśmie 2.4 GHz[70]

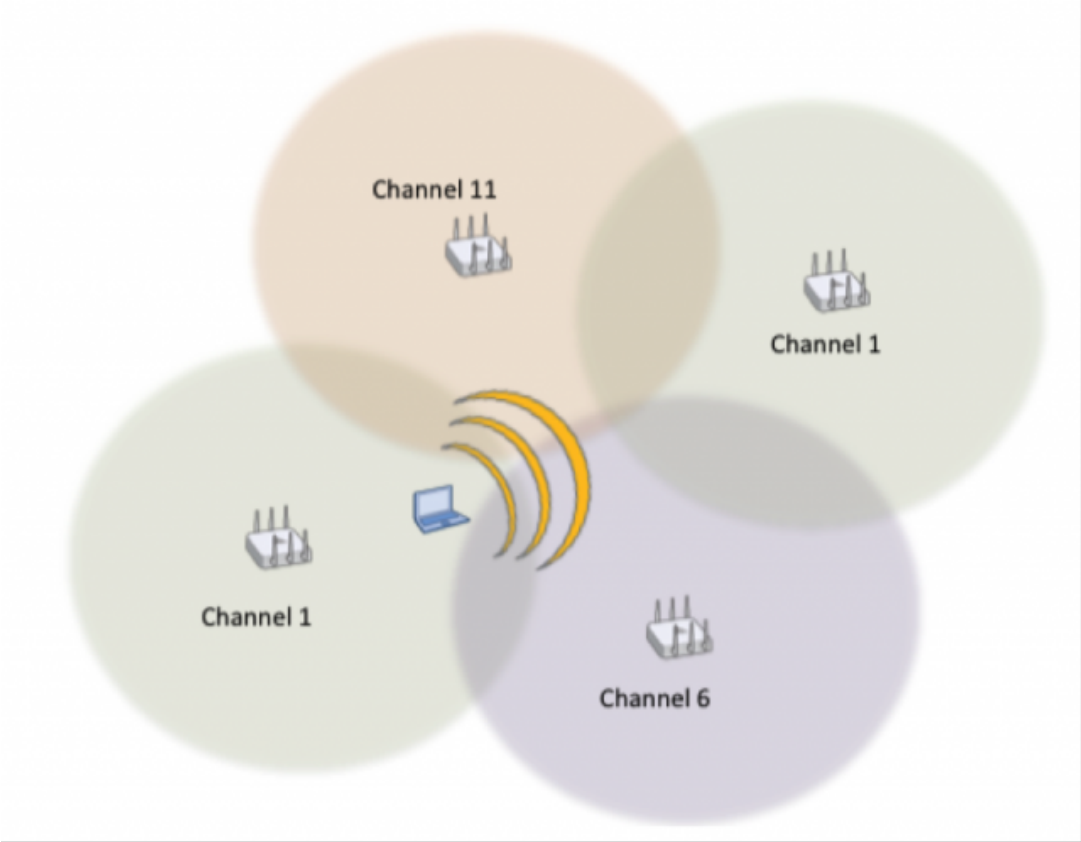


W paśmie 5 GHz dostępnych jest 24 (rozdzielonych) kanałów o szerokości 20 MHz: 36, 40, 44, 48 (indoor), 52, 56, 60, 64 (indoor/DFS/TPC), 100-140 (DFS/TPC).

Dynamic Frequency Selection/Transmision Power Control są określone przez standard 802.11h.

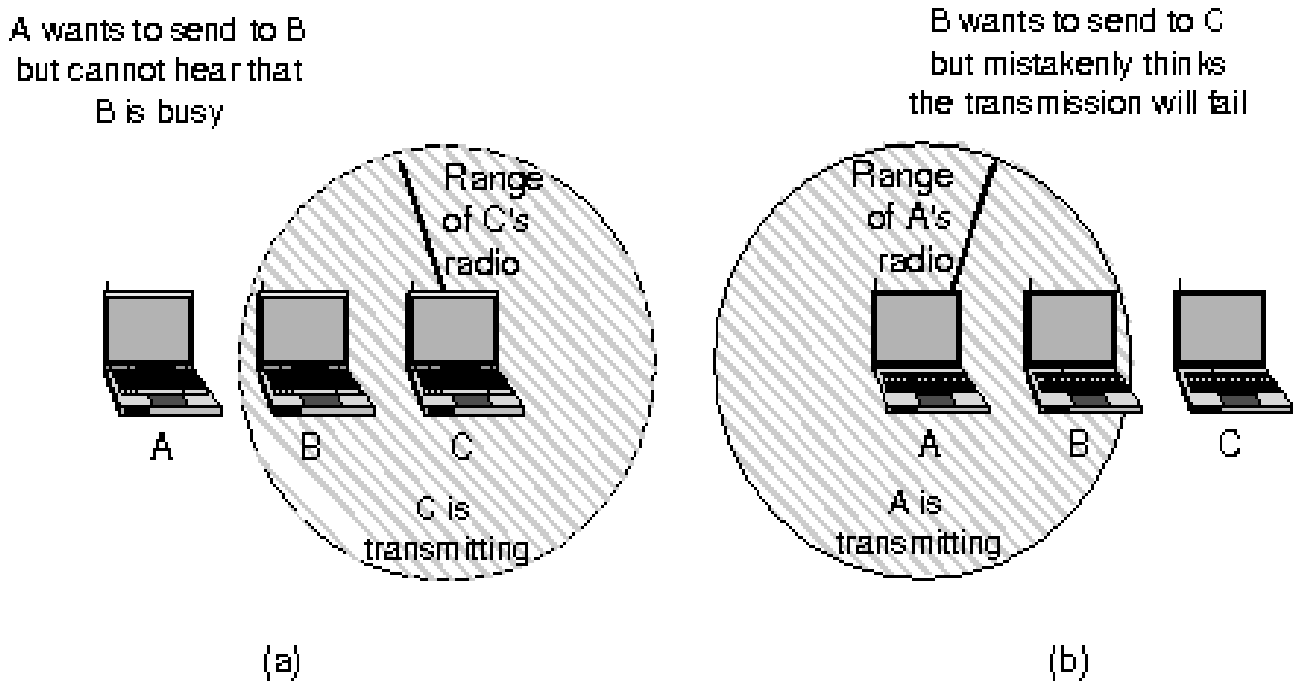
[70] 2.4 GHz Channel Planning

Komórki i kanały[71]

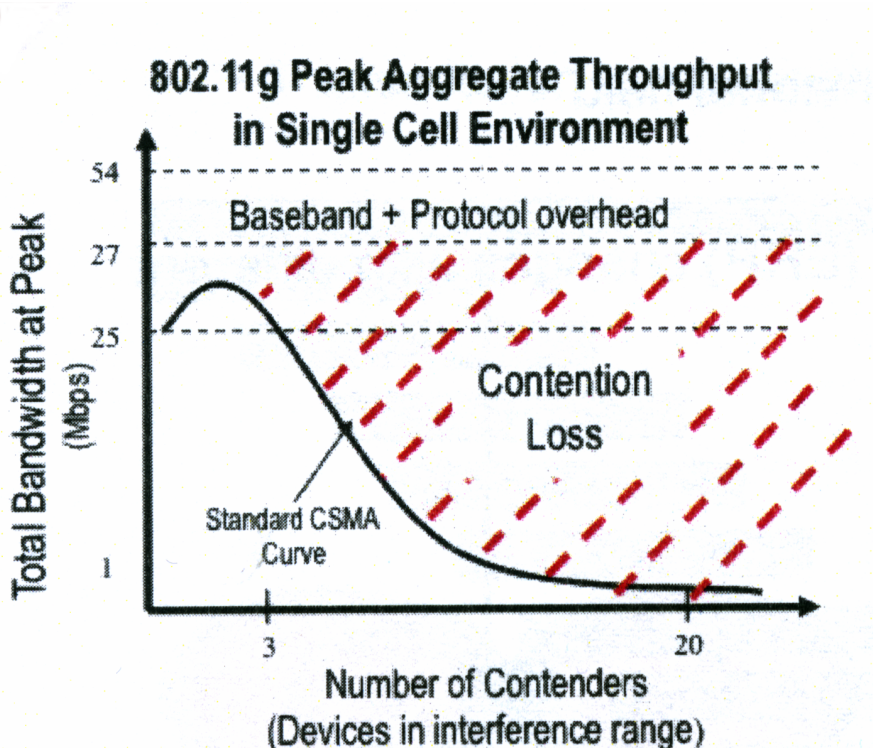


[71] 2.4 GHz Channel Planning

Problem ukrytej/odkrytej stacji



802.11 – przepustowość[72]



[72] Meru Networks, materiały szkoleniowe

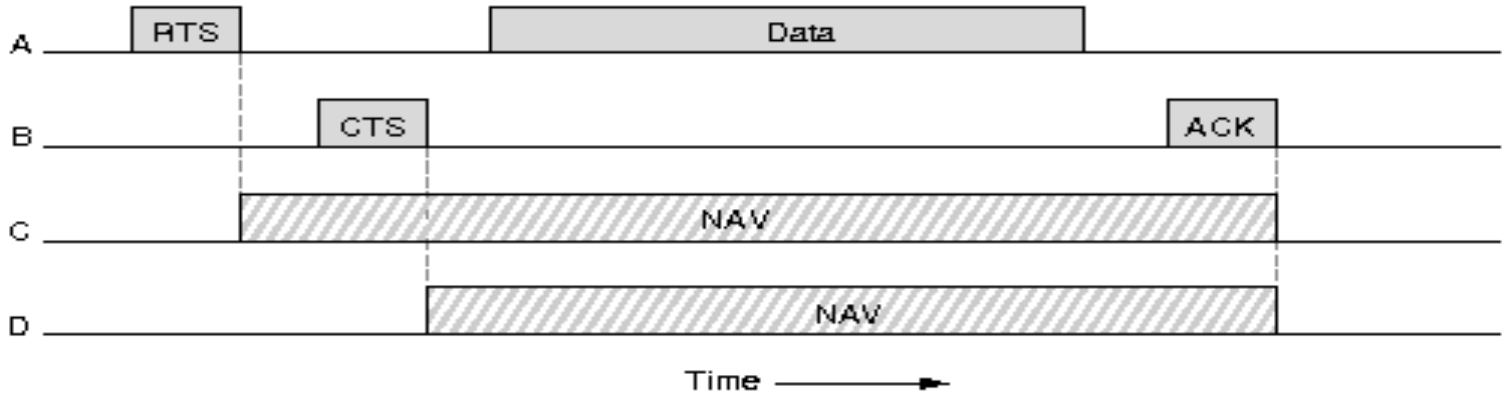
WLAN – działanie

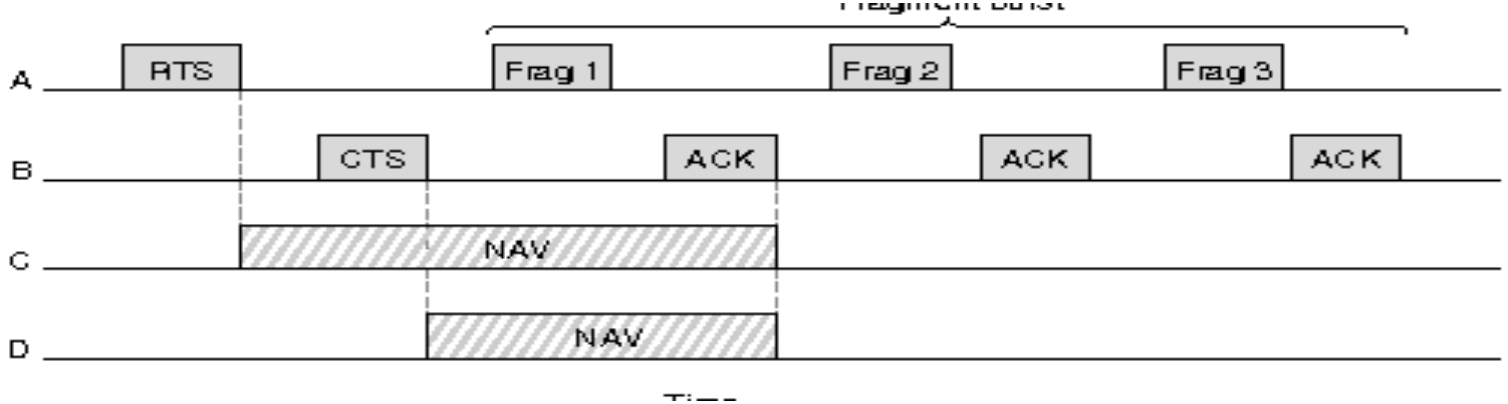
- DCF (*Distributed Coordination Function*): funkcja kordynacji rozproszonej używa dostępu do nośnika CSMA/CA (*CSMA/Collision Avoidance*), czyli CSMA z unikaniem kolizji i ma dwa tryby działania:
  - CSMA/CA: sprawdzanie stanu nośnika, losowy odstęp antykolizyjny pomiędzy dwiema wysyłanymi ramkami
  - CSMA/CA + MACAW[73]: sprawdzanie stanu nośnika, oznaczanie zajętości kanału wirtualnego (NAV, *Network Allocation Vector*)

  Ramka może być przesyłana w postaci wiązki jej fragmentów, gdyż (zwykle) duży poziom zakłóceń powoduje, że łatwiej jest bezbłędnie przesyłać mniejsze fragmenty.
- PCF (*Point Coordinated Function*): funkcja koordynacji punktowej, w której stacja bazowa odpytuje inne stacje, czy mają ramki do wysłania (brak kolizji); standard definiuje mechanizm odpytywania, ale nie częstotliwość i porządek.

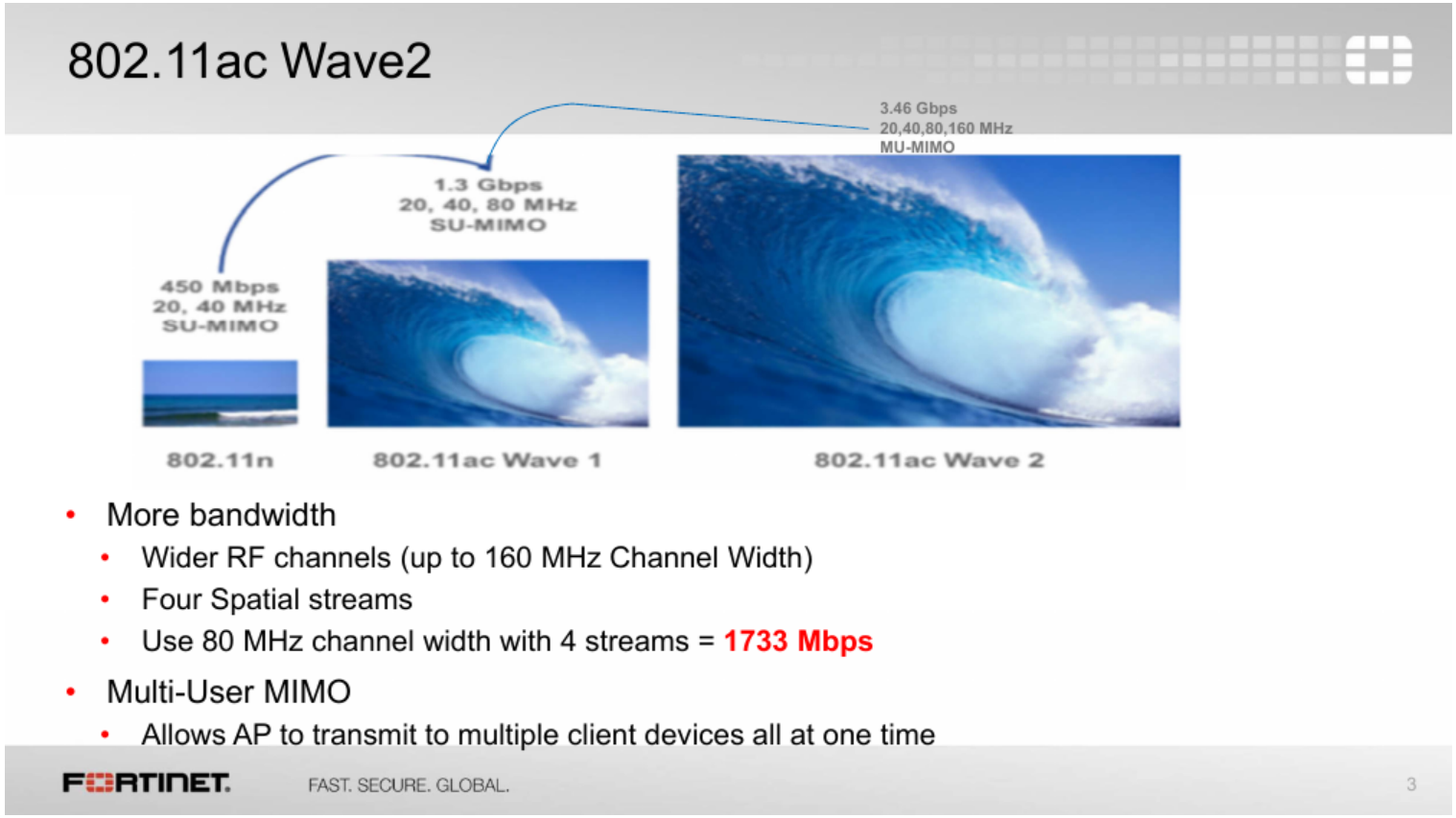
[73] *Multiple Access, Collision Avoidance, Wireless*

WLAN – działanie





Wi-Fi wg Fortinet[74]



[74] Opracowano w oparciu o materiały promocyjne firmy FORTINET: http://www.fortinet.com, 802.11ac Wave 2 - Impact on Enterprises.

Wi-Fi wg Fortinet

Wave-2 Data Rates

	1 SS	2 SS	3 SS	4 SS
256-QAM 80 MHZ	433	867	1300	1733
256-QAM 160 MHz	867	1733	2340	3467

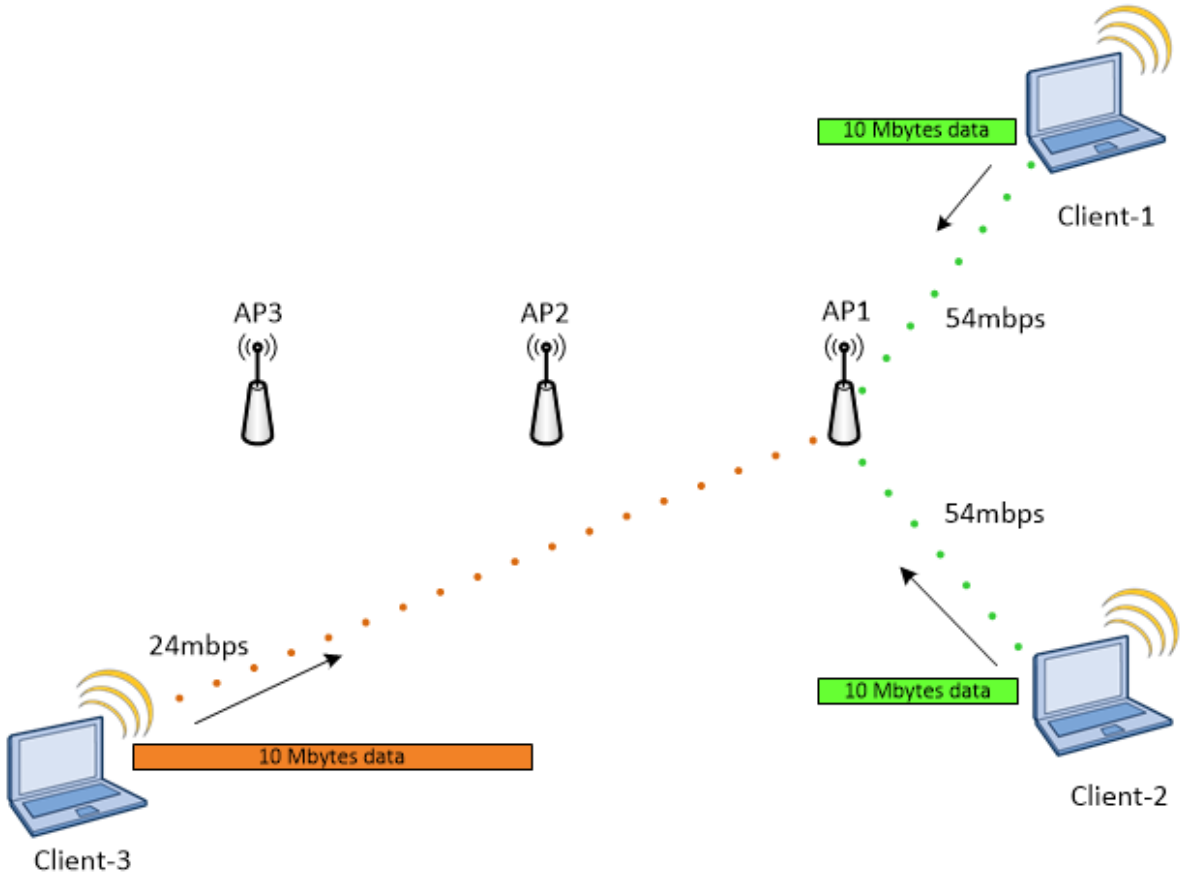
- 70 % of data rate is best case Throughput for TCP traffic
- LACP support on AP is needed
- Free wider spectrum is required for the usage of 160 MHz channels
  - Virtual Cell might make the difference

FORTINET. FAST. SECURE. GLOBAL. 4

LACP – *Link Aggregation Control Protocol*

Wi-Fi wg Fortinet

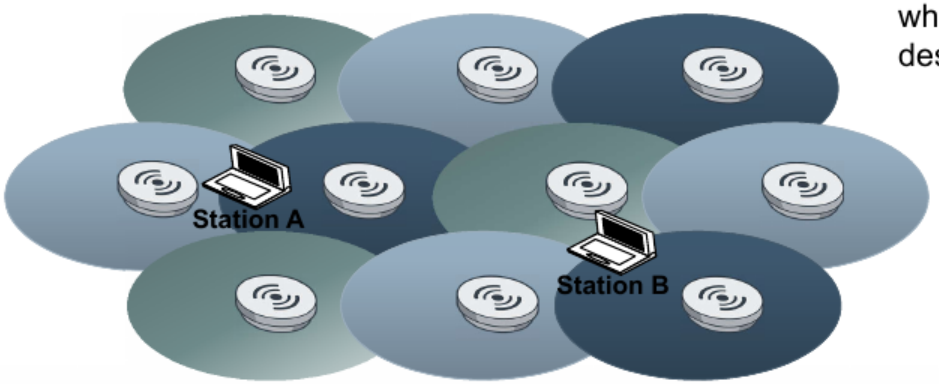
Wi-Fi sticky clients[75]



[75] What are sticky-clients?

Wi-Fi wg Fortinet: Multi Channel Architecture (MCA)

Traditional WiFi

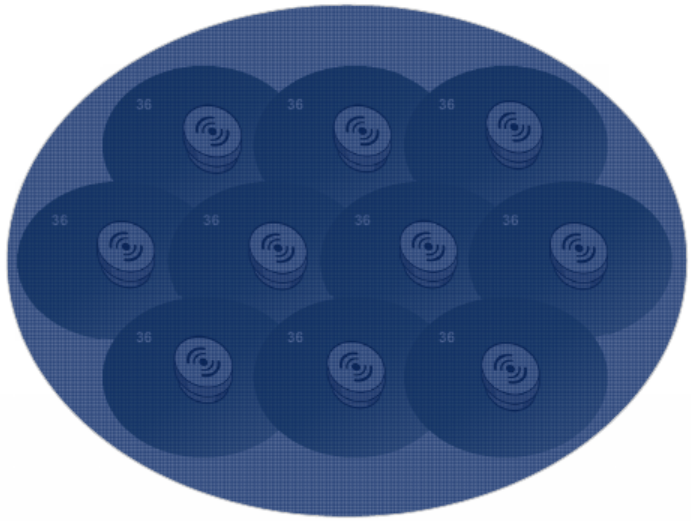


There will be 10 x AP's here, which eqauls 20 x BSSID (2xradio design)

Wi-Fi wg Fortinet: Single Channel Architecture (SCA)

Network in control

✓Virtual Cell technology



The system creates a virtual AP (bssid), which hides the actual AP from the clients, so clients only ”hear” one AP. So all connection control is in the infrastructure, not the client.

For voice devices and all other where the handoff between the actual AP’s are importent, this technique is a perfect match.

Controlled handoffs means greater scalability in high density enviroments.

FORTINET. FAST. SECURE. GLOBAL. 17

Wi-Fi wg Fortinet

Single Channel

One single channel with coverage all over the location

FORTINET. FAST. SECURE. GLOBAL. 23

Wi-Fi wg Fortinet

Channel Layering all over (more than 2 layer)

Multiple single channels with coverage all over the location

FORTINET FAST. SECURE. GLOBAL. 24

Wi-Fi wg Fortinet

Channel Striping

Two single channels, each channel with own coverage area

FORTINET FAST. SECURE. GLOBAL. 25

Wi-Fi wg Fortinet

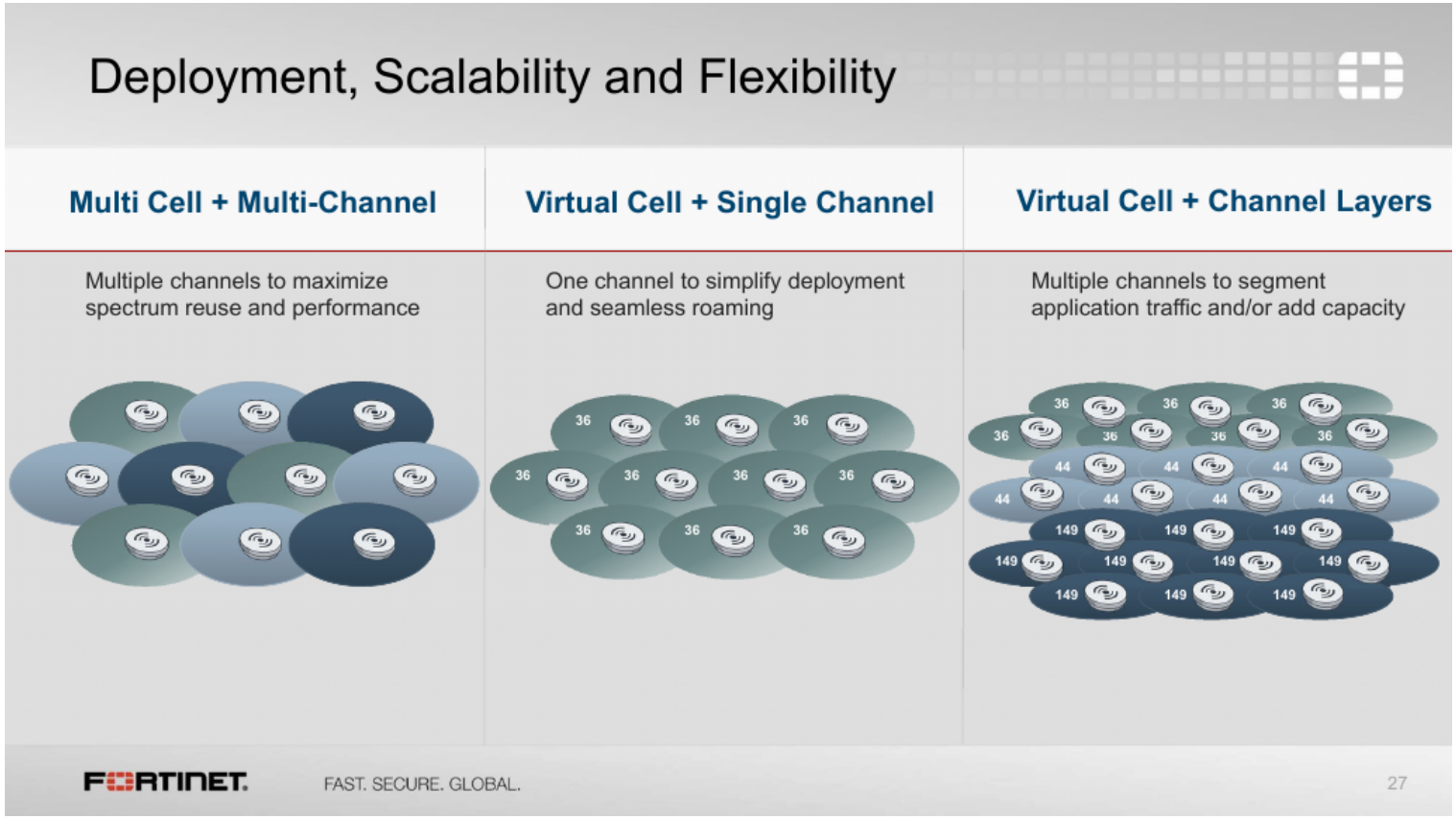
Channel Striping and Channel layering

In each area there will be two single channels. So in total we then use 5 single channels here.

We can then add multiple single channels, for instance at certain parts of the location. Could be areas like lobby for hotels ☺

FORTINET. FAST. SECURE. GLOBAL. 26

Wi-Fi wg Fortinet



Fortinet: architektura jednego kanału (?)

```
# nmcli dev wifi
IN-USE  BSSID              SSID                    MODE   CHAN  RATE        SIGNAL  BARS  SECURITY
        00:0C:E6:02:11:15  eduroam                 Infra  6     195 Mbit/s  100     ****  WPA2 802.1
        00:0C:E6:02:42:01  konferencja             Infra  6     195 Mbit/s  100     ****  --
        00:0C:E6:02:35:E9  konferencja             Infra  36    405 Mbit/s  100     ****  --
*       00:0C:E6:02:1E:13  eduroam                 Infra  36    405 Mbit/s  55      **    WPA2 802.1
        18:9E:2C:86:01:56  --                      Infra  100   270 Mbit/s  55      **    WPA2
        40:9B:CD:A2:3E:5C  JestemElektronem        Infra  6     130 Mbit/s  47      **    WPA1 WPA2
        18:9E:2C:86:01:54  KIS_2                   Infra  100   270 Mbit/s  45      **    WPA2
        6E:5C:51:CE:30:3B  Galaxy S20 FE 5G950A    Infra  1     130 Mbit/s  44      **    WPA2
        86:87:8F:14:FA:E1  rmax's Galaxy M52 5G    Infra  1     117 Mbit/s  40      **    WPA2
        7A:69:7F:A8:6D:6B  Szymon's Galaxy S21 5G  Infra  11    130 Mbit/s  34      **    WPA2
        6A:8C:46:31:40:4B  Majid?s MacBook Air     Infra  11    130 Mbit/s  30      *     WPA2 WPA3
        B6:41:45:52:DF:DE  Fffff                   Infra  48    270 Mbit/s  27      *     WPA2
        18:9E:2C:86:01:55  --                      Infra  6     270 Mbit/s  24      *     WPA2
        18:9E:2C:86:01:50  KIS_2                   Infra  6     270 Mbit/s  22      *     WPA2
        86:25:19:23:83:75  DIRECT-CFM288x Series   Infra  11    54 Mbit/s   19      *     WPA2
        AA:0B:57:0C:2D:54  Marta?s Mac mini        Infra  11    130 Mbit/s  10      *     WPA2 WPA3
```

Fortinet: architektura jednego kanału (?)

```
# iwlist wlan0 scan
wlan0     Scan completed :
          Cell 01 - Address: 00:0C:E6:02:11:15
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=68/70  Signal level=-42 dBm
                    ...
                    ESSID:"eduroam"
                    ...
                    Mode:Master
    ...
          Cell 06 - Address: 18:9E:2C:86:01:50
                    Channel:6
                    ...
                    ESSID:"KIS_2"
    ...
          Cell 09 - Address: 00:0C:E6:02:42:01
                    Channel:6
                    Frequency:2.437 GHz (Channel 6)
                    Quality=68/70  Signal level=-42 dBm
                    ...
                    ESSID:"konferencja"
```

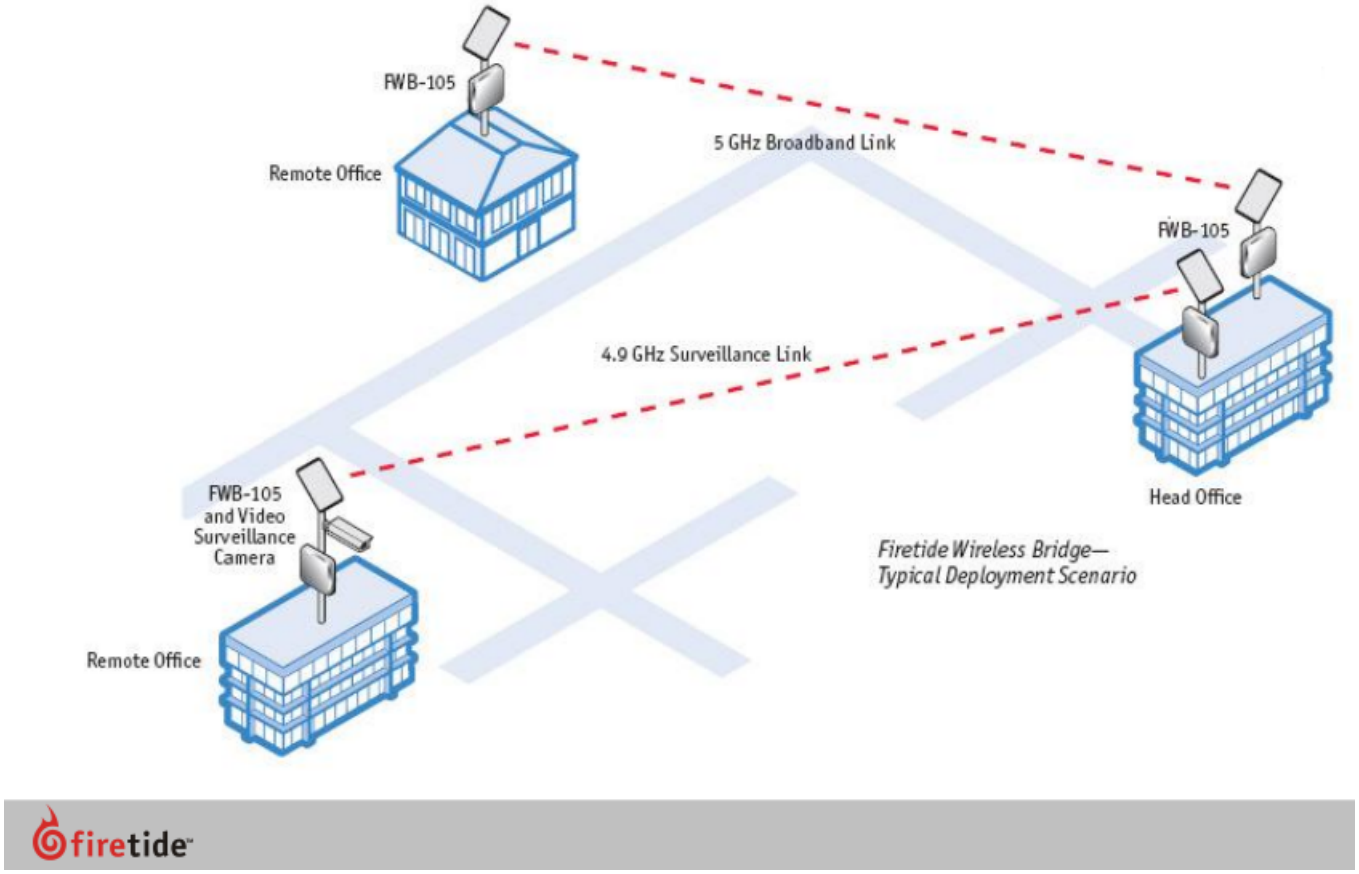
Topologia punkt-punkt (point-to-point)[76]

- Dedykowane połączenie
- Najwyższa możliwa przepływność dla szkieletu
- Ograniczona skalowalność i elastyczność
- Pojedynczy punkt awarii

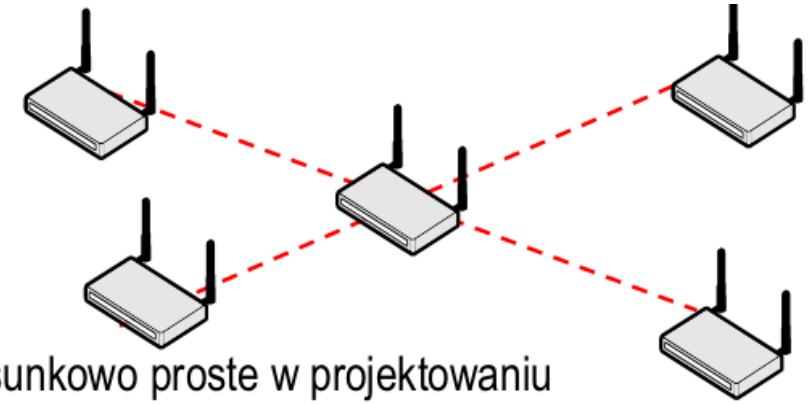
firetide

[76] Te i następne plansze zostały udostępnione przez organizatorów Meru Summit Poland 2012

Topologia punkt-punkt

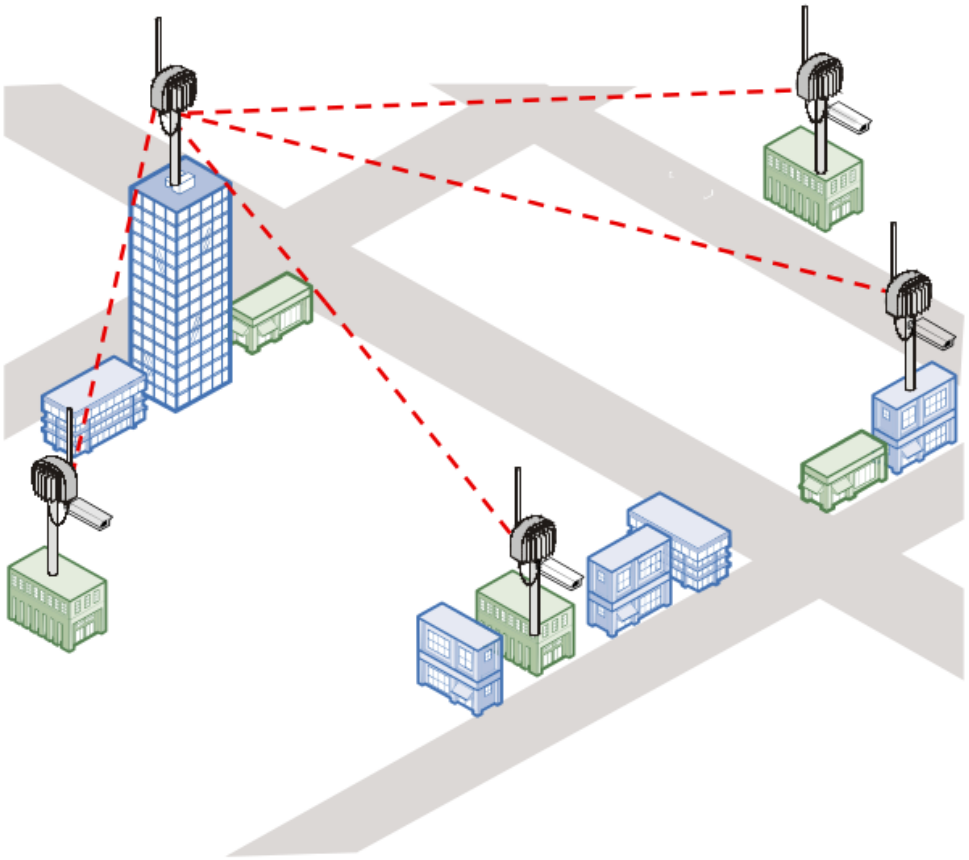


Topologia punkt-wielopunkt (point-to-multipoint)

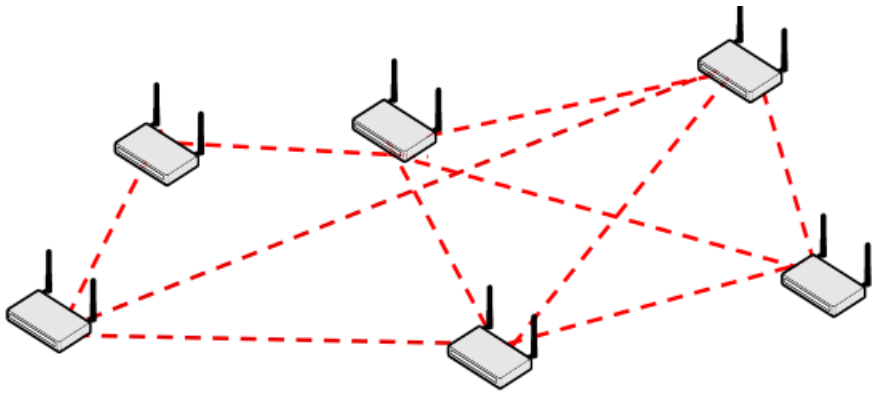


- Stosunkowo proste w projektowaniu
- Wydajne kosztowo, zastosowanie pojedyn czych punktów zbiorczych
- Ograniczona skalowalność: pasmo współdzielone pomiędzy wszystkie punkty zdalne
- LOS – widoczność wymagana bezpośrednio od każdego punktu zdalnego
- Stacja bazowa stanowi pojedynczy punkt awarii

Topologia punkt-wielopunkt

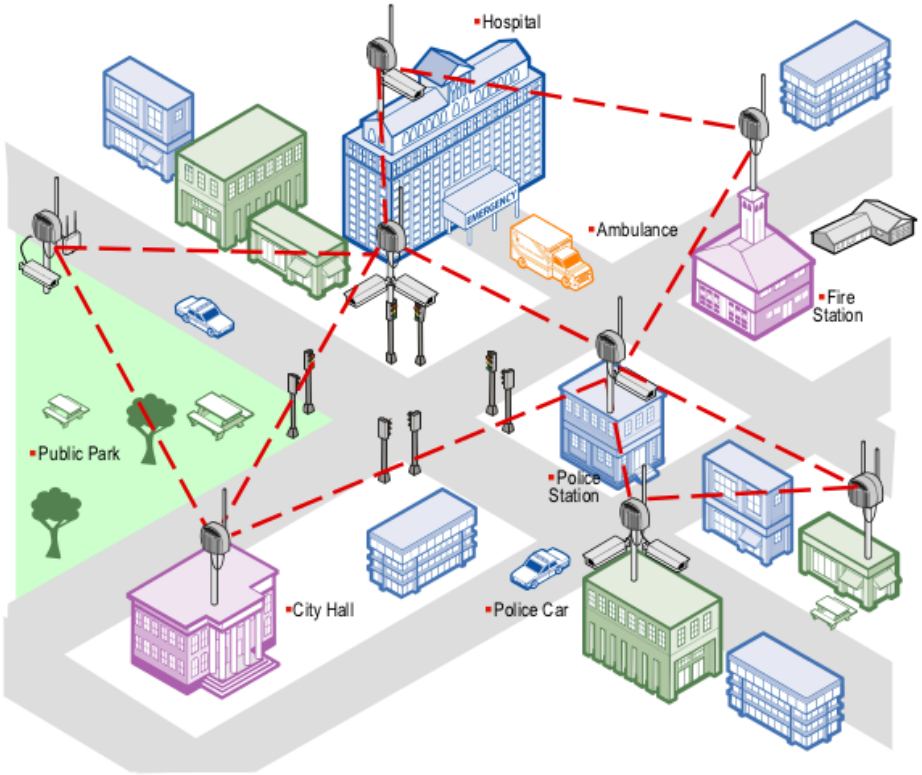


Topologia kraty (mesh, mp2mp)

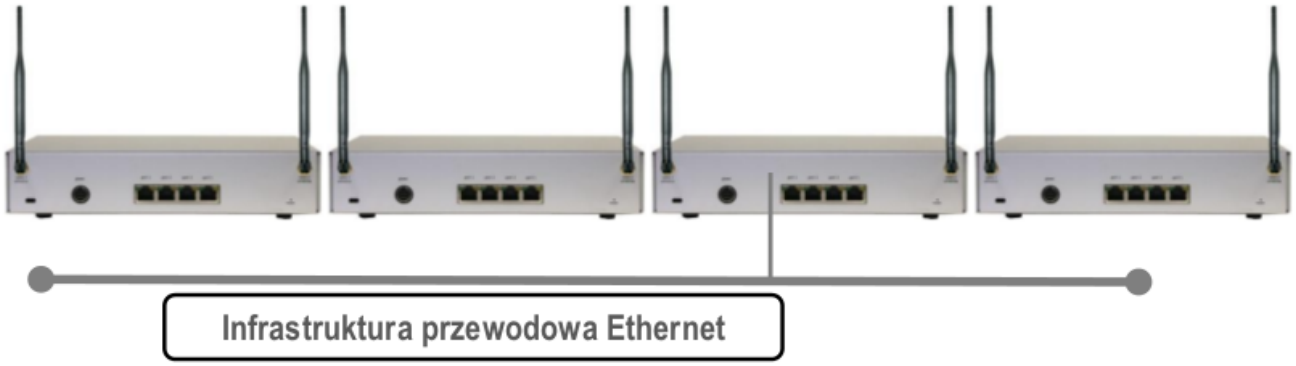


- Dostępność i skalowalność, dzięki połączeniom wiele do wielu
- Połączenia redundantne
- Możliwość realizowania połączeń wokół przeszkód
- Większa elastyczność możliwość łączenia topologii PtP, PtMP lub MtP to MtP

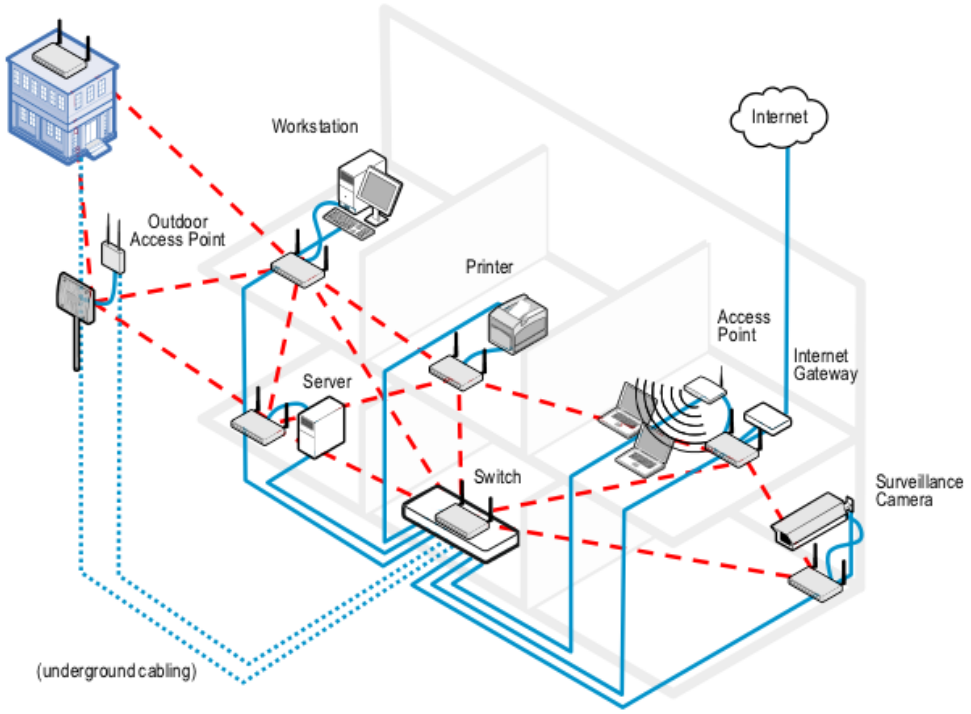
Topologia kraty



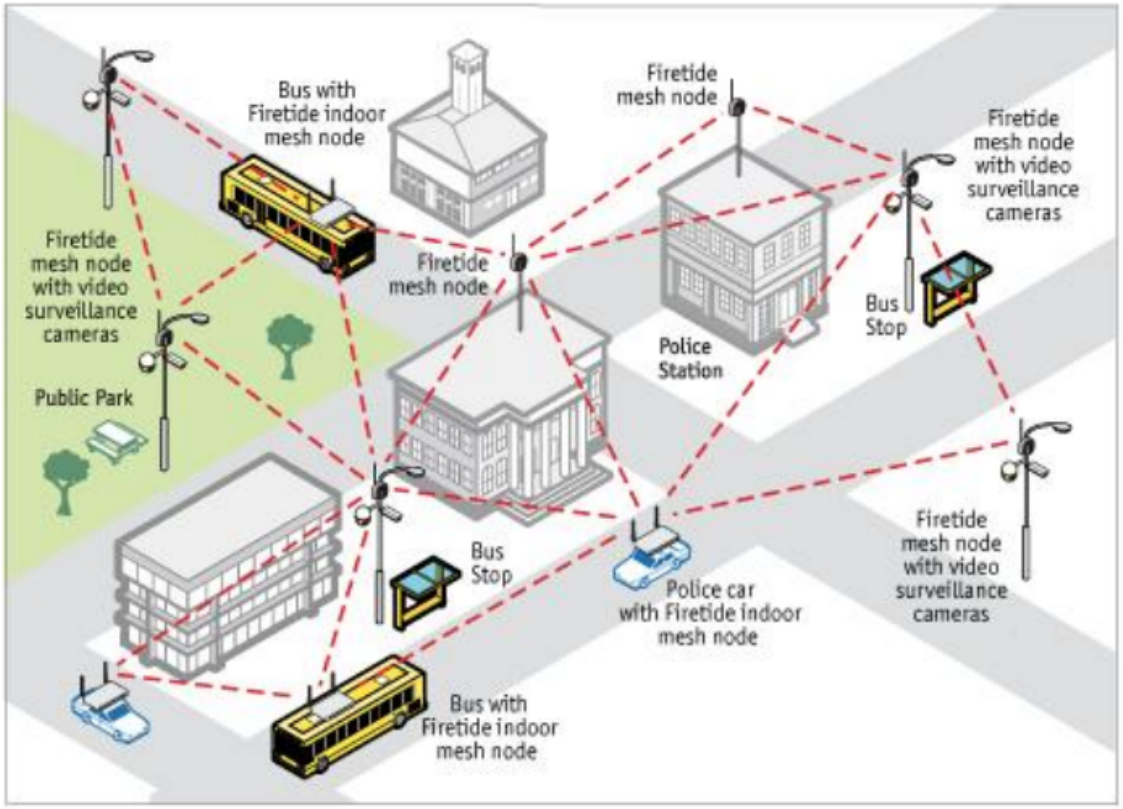
Topologia rozproszonego przełącznika



Topologia rozproszonego przełącznika

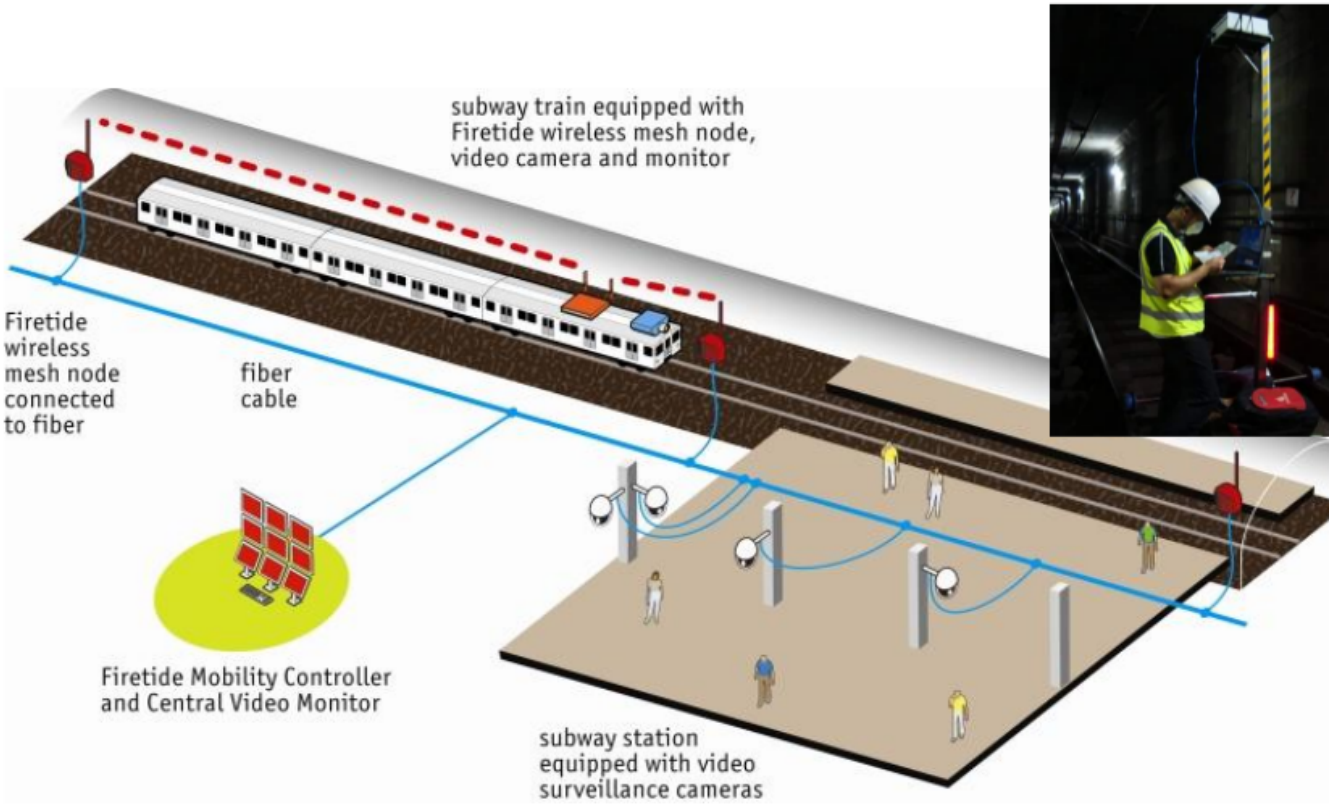


Zastosowania



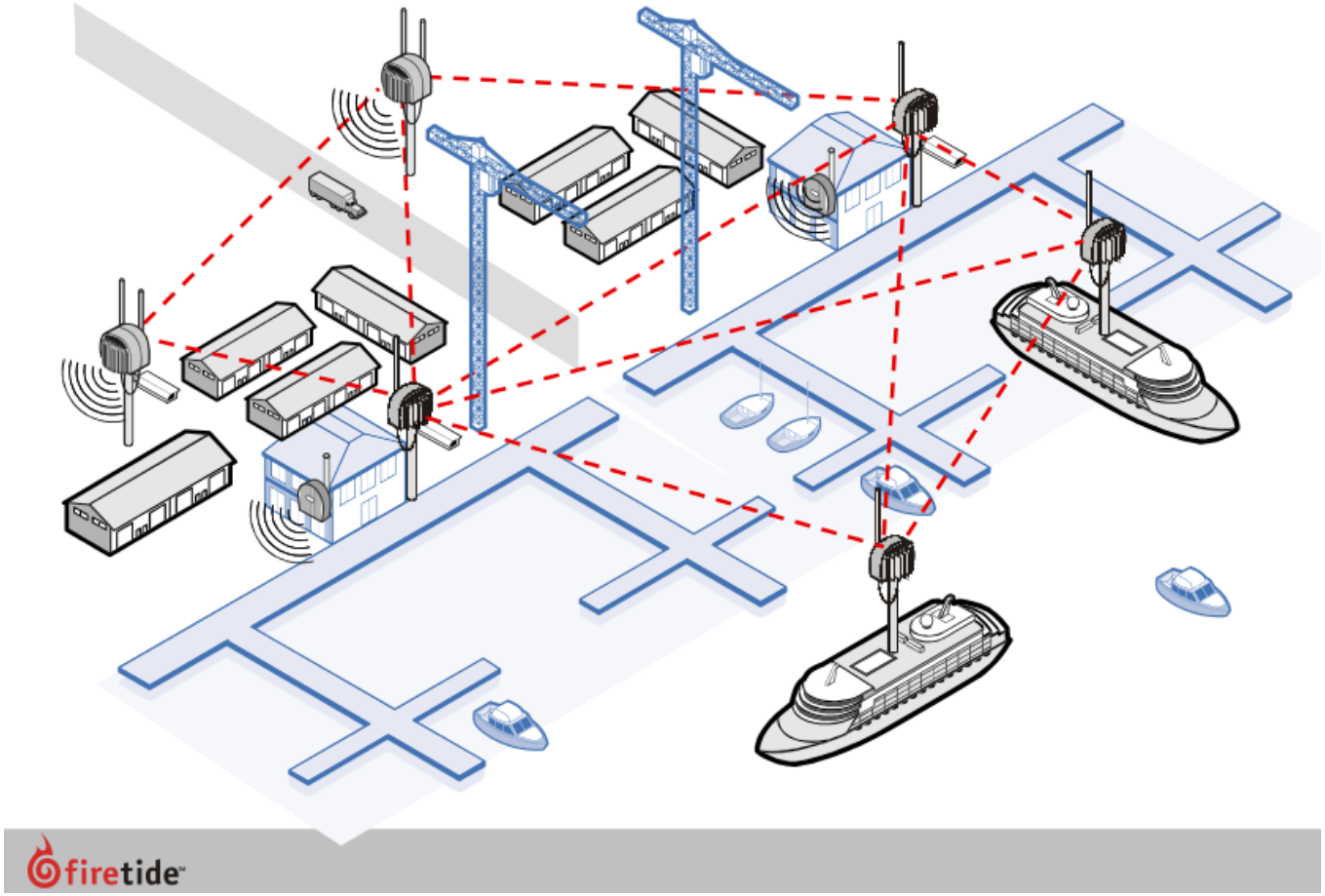
firetide

Zastosowania

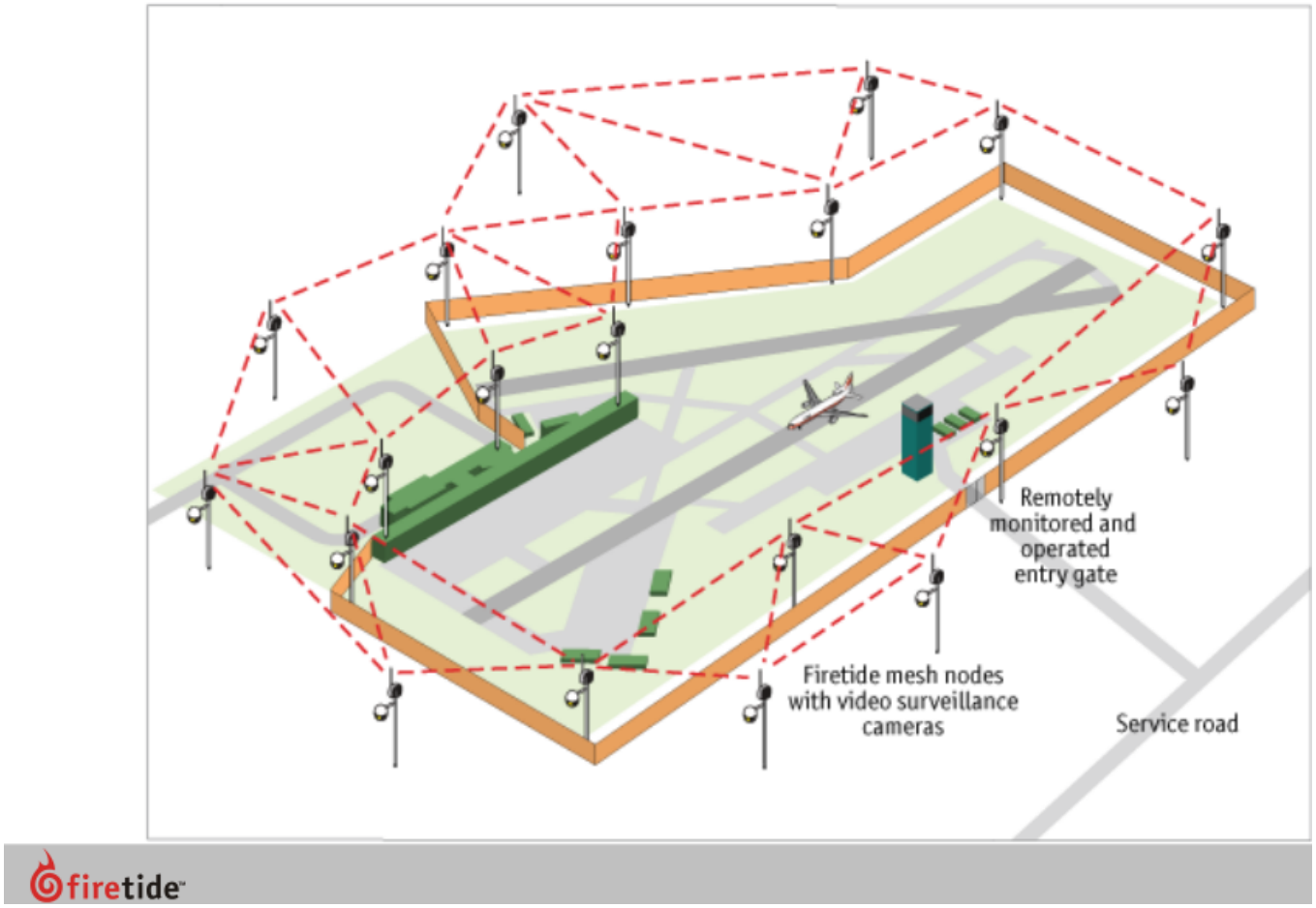


firetide

Zastosowania



Zastosowania



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: komputery, serwery, drukarki sieciowe, koncentratory, mosty, przełączniki, routery.

- **WAN** (*Wide Area Network*) – rozległa sieć komunikacyjna obejmująca swoim zasięgiem duży obszar geograficzny i umożliwiająca LAN-om łączność poprzez komutowane lub stałe łącza. Technologie WAN funkcjonują w warstwach 1-3 modelu OSI.

  Urządzenia: routery, przełączniki, serwery telekomunikacyjne (*dial-up*), modemy, urządzenia CSU/DSU

CSU (*Channel Service Unit*) jednostka obsługi kanału

DSU (*Data Service Unit*) jednostka obsługi danych

Technologie WAN i model OSI

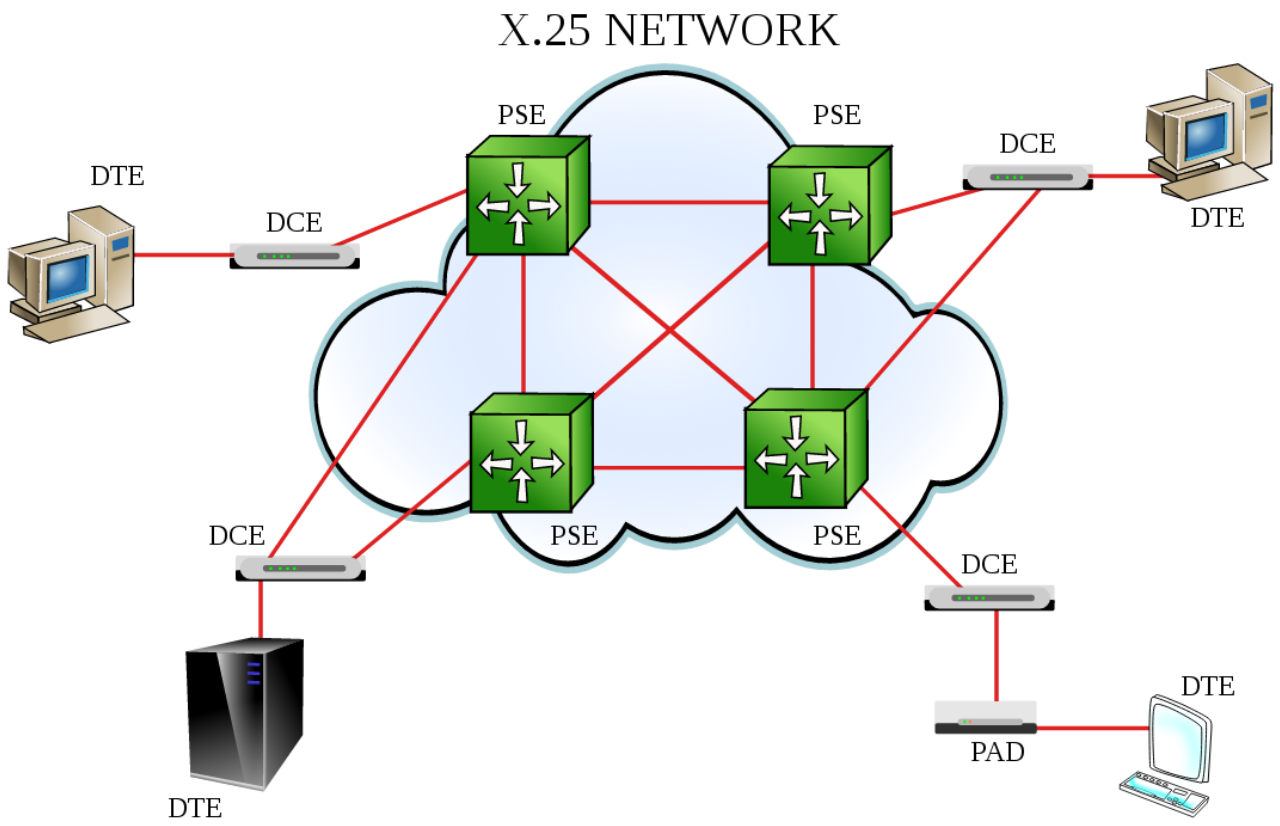
<table>
<tr><th colspan="5">WAN protocols</th><th>OSI layers</th></tr>
<tr><td>X.25 PLP</td><td colspan="4"></td><td>Network layer</td></tr>
<tr><td>LAPB</td><td>Frame Relay</td><td>HDLC</td><td>PPP</td><td>SDLC</td><td>Data Link layer</td></tr>
<tr><td>X.21bis</td><td colspan="4">EIA/TIA-232
EIA/TIA-449
V24, V25
HSSI, G.703, G.707, G.708
EIA-530</td><td>Physical layer</td></tr>
</table>

HDLC (*High-level Data Link Control*) wysokopoziomowe sterowanie łączem danych
PPP (*Point-to-Point Protocol*) protokół transmisji bezpośredniej
LAPB (*Link Access Procedure Balanced*)
PLP (*Packet Level Protocol*)
SDLC (*Synchronous Data Link Control*) sterowanie synchronicznym łączem danych
Frame Relay tranzyt (przekazywanie) ramek

Technlogie WAN

- komutowanie obwodów (*Circuit Switching*)
  - tradycyjna telefonia (POTS, *Plain Old Telephone Service*)
  - ISDN (*Integrated Services Digital Network*) cyfrowa sieć usług zintegrowanych
  - sieci Switched 56
- komutowanie pakietów (*Packet Switching*)
  - X.25
  - *Frame-Relay* tranzyt ramek
- komutowanie komórek (*Cell Switching*)
  - ATM (*Asynchronous Transfer Mode*) tryb przesyłania asynchronicznego
  - SMDS (*Switched Multimegabit Data Service*)
- komutowanie etykiet (MPLS, *Multi-Protocol Label Switching*)

Sieć X.25[77]



[77] Rodzina protokołów X.25

Standardy sygnałów cyfrowych

Linie dzierżawione umożliwiają przesyłanie danych w zgodzie ze standardowymi schematami transmisyjnymi. Schematy te określają szybkość transmisji i rodzaje nośników, formaty ramek i metody multipleksowania.

Standardy sygnałów cyfrowych ANSI (DSH *Digital Signal Hierarchy*)

St. sygnałów cyfr.	Szerokość pasma	Liczba kanałów głosowych
DS-0	64 Kb/s	1
DS-1	1.544 Mb/s	24
DS-1C	3.152 Mb/s	48
DS-2	6.312 Mb/s	96
DS-3	44.736 Mb/s	672
DS-4	274.176 Mb/s	4032

Standardy DS zostały zastosowane w systemach telefonicznych pod nazwą *systemu T-Carrier.* Standardowi DS-1 odpowiadają obwody transmisyjne T-1, a DS-3 – T3.

Standardy sygnałów cyfrowych (cd)

Standardy sygnałów cyfrowych ITU

St. sygnałów cyfr.	Szerokość pasma	Liczba kanałów głosowych
CEPT-1	2.048 Mb/s	30
CEPT-2	8.448 Mb/s	120
CEPT-3	34.368 Mb/s	480
CEPT-4	139.264 Mb/s	1920
CEPT-5	565.148 Mb/s	7680

Standard CEPT-1 realizują urządzenia transmisyjne E-1, a CEPT-3 – E-3.

Szerokość CEPT-1 wynosi 32 kanały głosowe. 2 wolne kanały są wykorzystywane do celów synchronizacji i sygnalizowania. ANSI narzuca umieszczanie impulsów czasowych i ramek w każdym kanale, redukując dostępną szerokość pasma w stosunku do podawanej szybkości transmisji.

Systemy przenoszenia sygnałów

T-1 i T-3 – schemat transmisji danych w sieciach rozległych odpowiadające standardom DS-1 i DS-3; wprowadzony przez Bell System w latach 1960.

- przenoszenie dźwięku (100 Hz-4 kHz) w postaci cyfrowej; nośniki – skrętka dwuparowa, włókna światłowodowe, fale radiowe
- modulacja impulsowa (PCM *Pulse Code Modulation*) i multipleksacja z podziałem czasowym (TDM, *Time Division Multiplexing*)
- linia T-1 o przepustowości 1.544Mb/s składa się z 24 kanałów 64 kb/s; format ramki – D-4 (także ESF, *Extended Super Frame*); kodowanie B8ZS (*Bipolar/Binary with 8-Zeros Substitution* bipolarna substytucja ośmiozerowa)

  maksymalna przepustowość wynika z częstotliwości próbkowania: 24 kanały są próbkowane 8000 razy na sekundę (każdy przy pomocy 8. bitowego słowa) i przesyłane w ramce o długości 192 bitów plus jeden bit rozdzielający ramki ($24\times8\times8000+8000=1544000$)

Systemy przenoszenia sygnałów

E-1 i E-3

- schemat transmisji danych w sieciach rozległych używany poza USA i Japonią
- dane przenoszone z szybkością 2.048 i 34.368 Mb/s (wg CEPT-1 i CEPT-3)
- odpowiednik schematów T-1 i T-3

Standardy sygnałów cyfrowych

SONET (*Synchronous Optical NETwork*) synchroniczna sieć optyczna, czyli szereg systemów transmisyjnych opartych na technologii optycznej, które zapewniają współpracę między systemami przyłączania różnych producentów oraz systemów o różnej pojemności i szybkości działania (norma ANSI). Standard SONET obsługuje dwa systemy transmisji:

- system nośników optycznych (OC *Optical Carrier*)
- system sygnałów transportu synchronicznego (STS *Synchronous Transport Signal*) na nośnikach miedzianych (zachodzi odpowiedniość: OC-n – STS-n); podstawową szybkością jest STS-1 równy 51.840 Mb/s

Ramka STS-1 ma długość 810 B i jest transmitowana w ciągu 125 μs przez obwód optyczny OC-1. Multipleksowanie TDM umożliwia przesyłanie np. trzech ramek STS-1 poprzez obwód OC-3.

Standard SONET jest używany w USA i Kanadzie.

Standardy sygnałów cyfrowych

SDH (*Synchronous Digital Hierarchy*) – standard ITU (G.706, rozszerzenie G.707), który definiuje szybkości i formaty danych przesyłanych przez włókna światłowodowe. STM-1 (*Synchronous Transport Module*) jest podstawową szybkością równą 155.52 Mb/s.

Standard SDH jest używany poza USA i Kanadą (SONET jest traktowany jako wariant SDH).

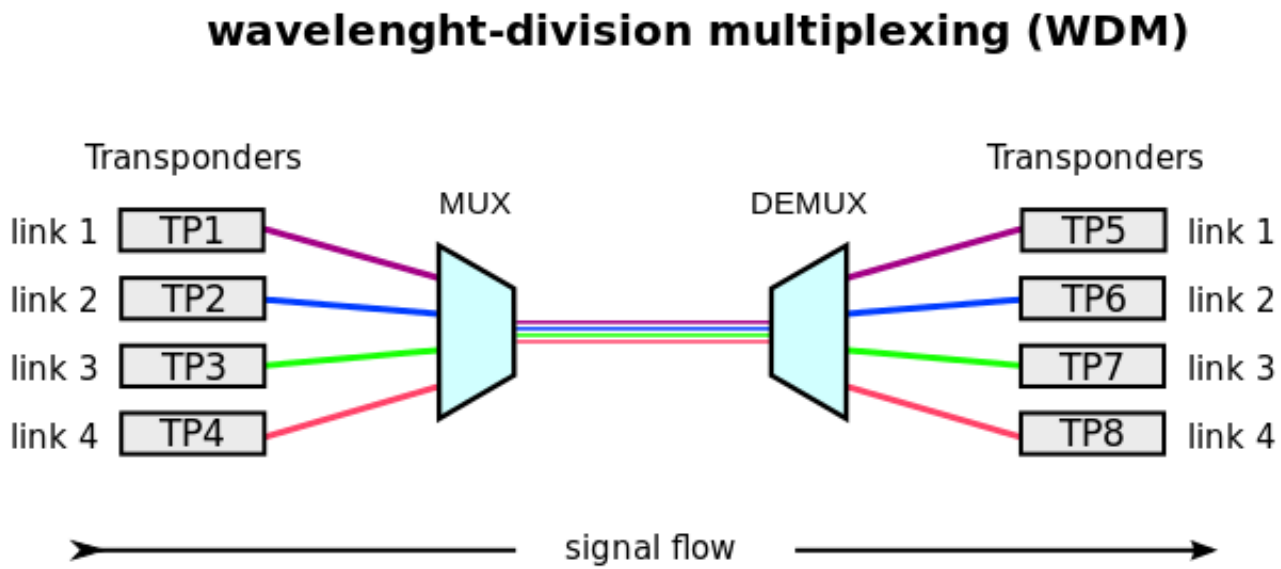
Tempo przesyłania danych jest ściśle synchronizowane w obrębie całych sieci (np. krajowych) dzięki zastosowaniu zegarów atomowych. Pozwala to na zmniejszenie buforowania przesyłanych danych pomiędzy elementami sieci.

Standardy sygnałów cyfrowych

Linia nośnika opt.	Szerokość pasma	ramka SONET	ramka SDH
OC-1	51.84 Mb/s	STS-1	
OC-3	155.52 Mb/s	STS-3	STM-1
OC-12	622.08 Mb/s	STS-12	STM-4
OC-48	2.488 Gb/s	STS-48	STM-16
OC-192	9.952 Gb/s	STS-192	STM-64
OC-768	39.813 Gb/s	STS-768	STM-256
OC-3072	159.252 Gb/s	STS-3072	STM-1024

Multipleksacja z podziałem falowym[78]

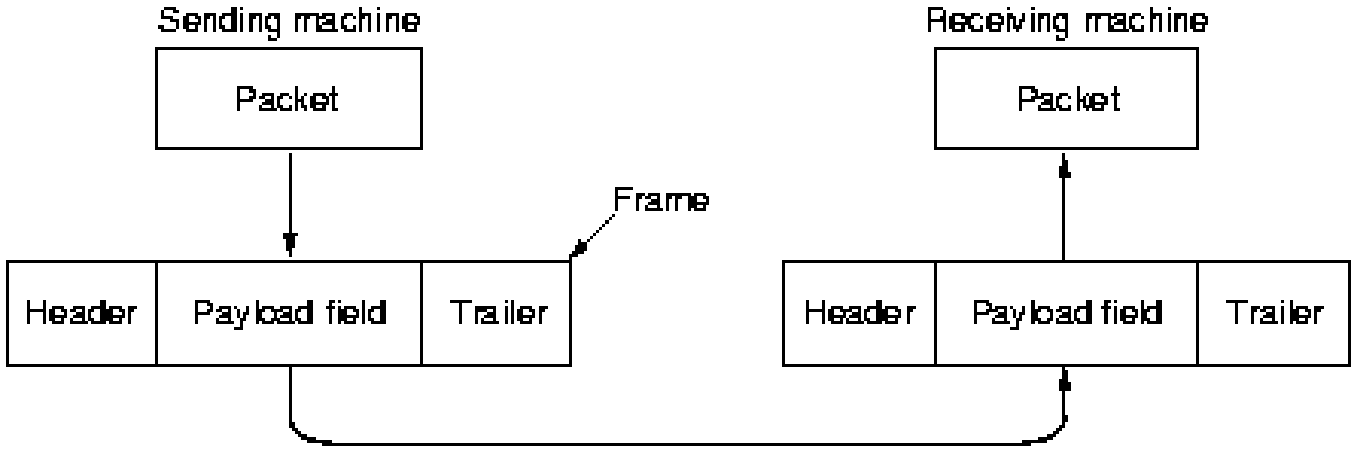
(C/D)WDM (*Coarse/Dense Wavelength-Division Multiplexing*) – multipleksacja z rzadkim/gęstym podziałem falowym, technika umożliwiająca utworzenie w obrębie jednego włókna światłowodowego wielu odrębnych kanałów transmisji danych. Ponieważ ta technologia jest niezależna od protokołu i szybkości transmisji, więc może wspierać przenoszenie ruchu IP, ATM, SONET/SDH, Ethernet.



[78] Wavelength division multiplexing

Problemy warstwy łącza danych

Pakiety i ramki

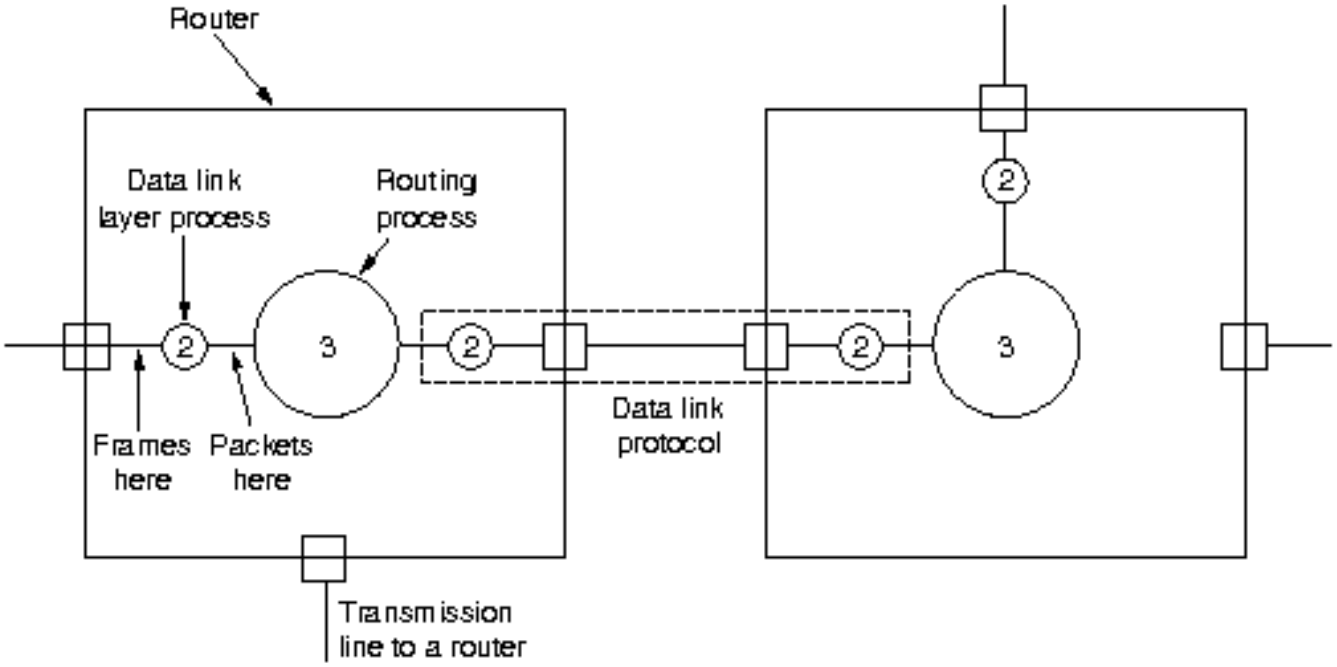


Funkcje warstwy łącza danych:

- udostępnianie interfejsu warstwie sieciowej
- obsługiwanie błędów transmisji
- sterowanie przepływem danych (szybki nadajnik, wolny odbiornik)

Problemy warstwy łącza danych

Miejsce protokołu łącza danych



Problemy warstwy łącza danych

Rodzaje usług warstwy łącza danych:

1. usługa bezpołączeniowa bez potwierdzeń
2. usługa bezpołączeniowa z potwierdzeniami (przyspieszenie przesyłania pakietów poprzez kanały o wysokiej stopie błędów)
3. usługa połączeniowa z potwierdzeniami

Problemy warstwy łącza danych

Warstwa fizyczna przyjmuje od warstwy łącza danych strumień bitów, które zwykle dzieli się na oddzielne porcje (ramki). Poprawność przesłania ramki określa się w oparciu o sumę kontrolną wyliczaną przez nadawcę i odbiorcę danych. Ramki można rozdzielać poprzez wstawienie przerwy czasowej, ale wymaga to utrzymania w sieci dobrych zależności czasowych.

Problem komunikacji cyfrowej: odbiorca musi znać początek i czas trwania pojedynczego bitu

Transmisja asynchroniczna: każdy znak (bajt) jest traktowany oddzielnie na potrzeby synchronizacji na poziomie bitu lub znaku; synchronizacja następuje na początku każdego znaku

Transmisja synchroniczna: cała ramka jest przesyłana jako ciągły strumień bitów, odbiornik jest odpowiedzialny za utrzymanie synchronizacji w czasie odbierania całej ramki

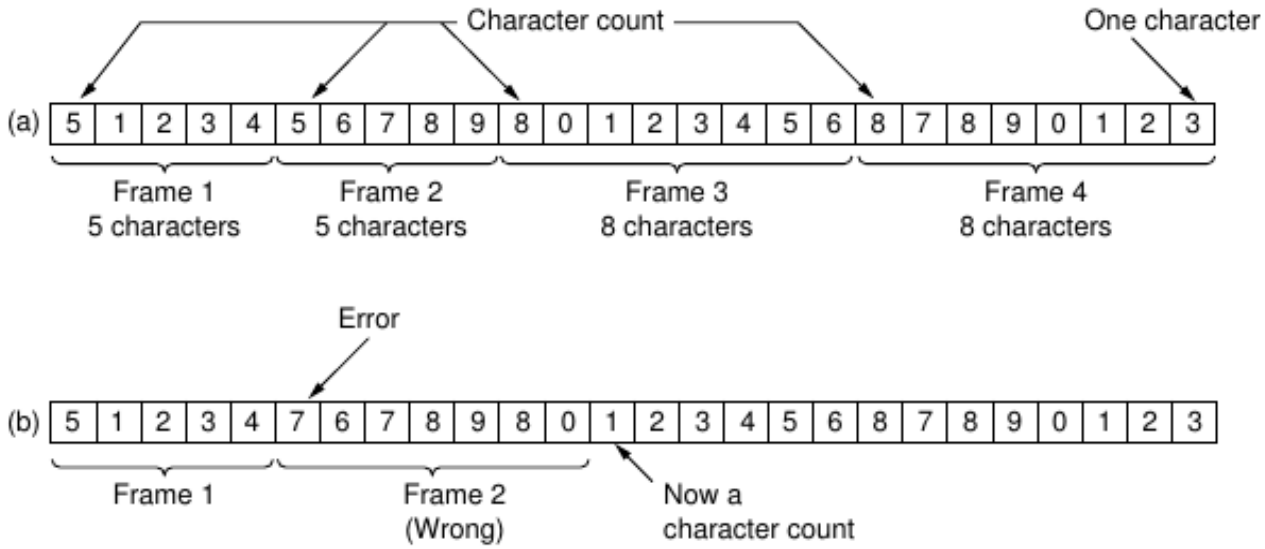
Problemy warstwy łącza danych

Metody wyznaczania początku ramki:

1. zliczanie znaków
2. bajty znacznikowe z napełnianiem bajtami
3. znaczniki początku i końca z napełnianiem bitami
4. zmiany kodowania w warstwie fizycznej (bit „1” reprezentowany przez parę wysoki-niski, a „0” – niski-wysoki)

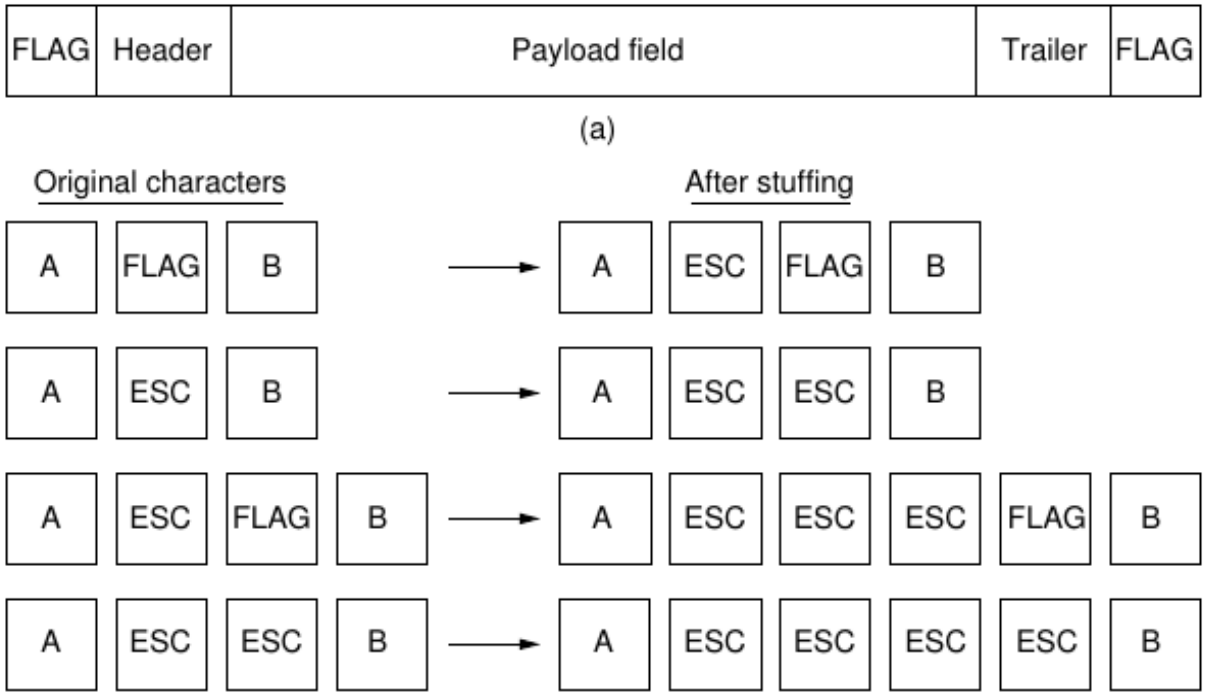
Problemy warstwy łącza danych

Zliczanie znaków

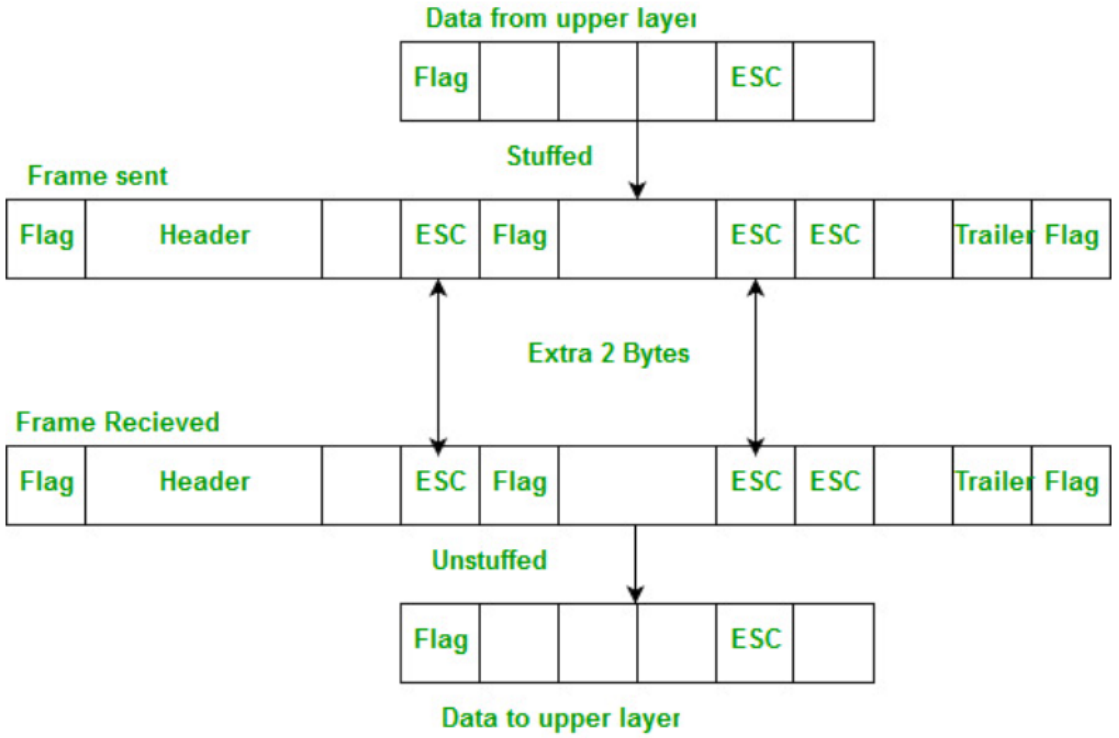


Problemy warstwy łącza danych

Ramka z bajtami znacznikowymi



Problemy warstwy łącza danych: napełnianie bajtami[79]

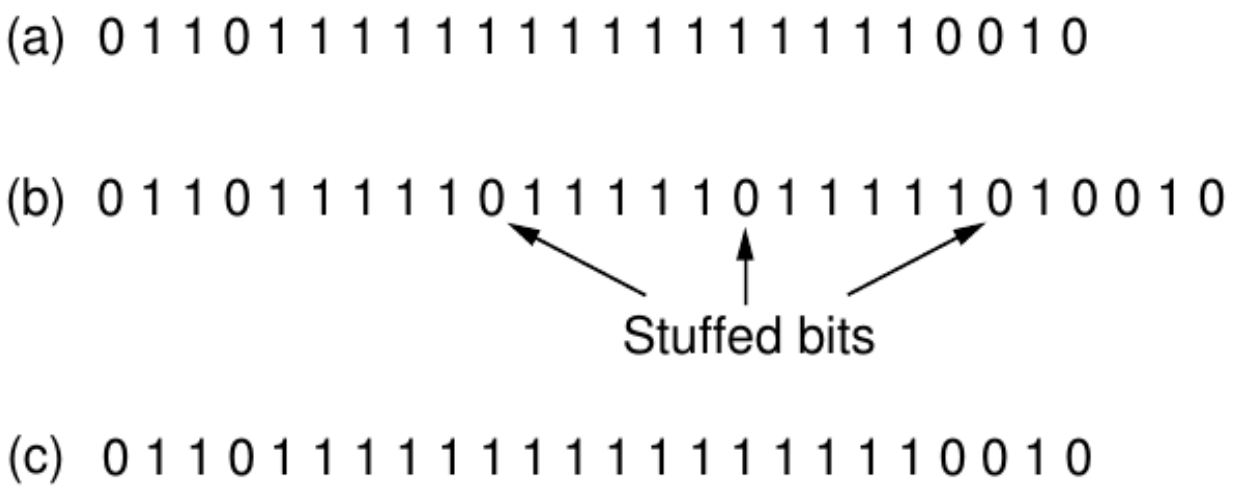


[79] Bit and bte stuffing

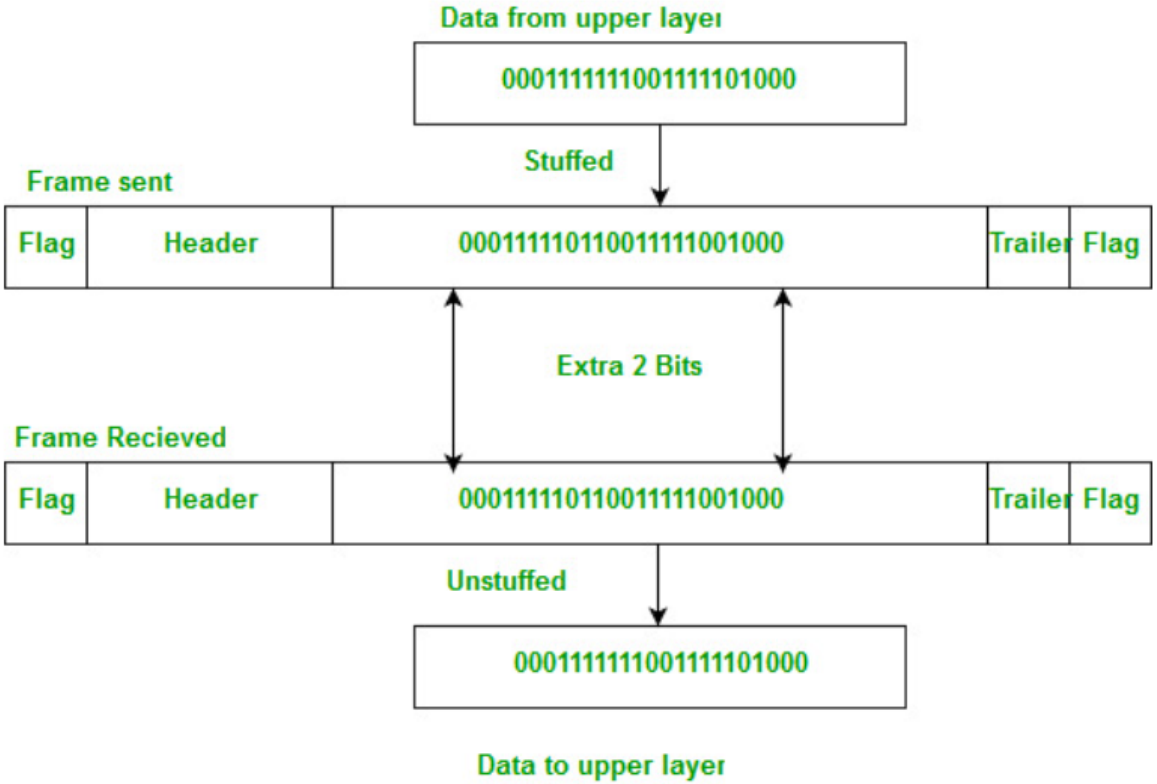
Problemy warstwy łącza danych

Sekwencja rozdzielająca ramki: 01111110

Napełnianie bitami



Problemy warstwy łącza danych: napełnianie bitami[80]



[80] Bit and byte stuffing

Problemy warstwy łącza danych

Kontrola błędów

W jaki sposób zapewnić dostarczanie przez warstwę drugą do warstwy sieciowej wszystkich pakietów bez błędów i w odpowiedniej kolejności?

Niezawodne dostarcznie danych wymaga wprowadzenia mechanizmu potwierdzania przez odbiorcę odebranych ramek. Z uwagi na zawodność kanału komunikacyjnego ramka z potwierdzeniem może zaginąć. Dlatego nadawca przy wysyłaniu ramki włącza czasomierz i ustawia czas oczekiwania na taką wartość, która powinna wystarczyć na dotarcie ramki do odbiorcy, jej przetworzenie i nadejście ramki potwierdzenia.

Jeśli ramka potwierdzenia nie nadchodzi w określonym czasie, to nadawca ponownie wysyła ramkę. Jeśli zakłócenia w kanale komunikacyjnym spowodowały zaginięcie potwierdzenia, to ponowne wysłanie ramki grozi tym, że odbiorca przekaże do warstwy sieciowej dwa identyczne pakiety. Można tego uniknąć wprowadzając numery sekwencyjne ramek.

Problemy warstwy łącza danych

Wykrywanie i korekcja błędów

Nowoczesne systemy telefoniczne: systemy cyfrowe (centrale, łącza między centralami) – mała stopa błędów, lokalna pętla – dużą stopa błędów

Zaburzenia w kanale komunikacyjnym mogą objawiać się jako przypadkowe uszkodzenia pojedynczych bitów lub błędy mogą pojawiać się seriami (np. w nośniku radiowym).

Problemy warstwy łącza danych

Sposoby obsługi błędów

- kody korekcyjne (*error correcting code*)

  Każdy wysyłany blok danych zawiera dostateczną ilość nadmiarowej informacji, która pozwala odbiorcy na odtworzenie oryginalnych danych. Tę technikę stosuje się w kanałach od dużej stopie błędów (kod Hamminga).

- kody detekcyjne (*error detecting code*)

  Każdy blok danych jest uzupełniany informacją (sumą kontrolną) pozwalającą odbiorcy na sprawdzenie integralności odebranych danych. Błędne ramki są porzucane i przesyłane ponownie. Takie podejście jest korzystne w kanałach charakteryzujących się małą stopą błędów (kod wielomianowy znany jako cykliczna kontrola nadmiarowa (CRC), bit parzystości).

Kody korekcyjne

symbol	słowo kodowe	symbol	slowo kodowe
A	00	A	000
	01		100
	10		010
B	11		001
			110
			101
			011
		B	111

- odległość Hamminga – liczba pozycji, na których różnią się słowa kodowe; dwa słowa odległe o $\mathbf{d}$ bitów wymagają $\mathbf{d}$ jednobitowych błędów, żeby przekształcić jedno w drugie
- w celu wykrycia $\mathbf{d}$ błędów trzeba posłużyć się kodem o odległości $\mathbf{d}+1$ ($\mathbf{d}$ błędów nie przekształca jednego słowa kodowego w inne poprawne słowo kodowe)
- w celu naprawienia $\mathbf{d}$ błędów potrzeba kodu o odległości $2\mathbf{d}+1$

Kody korekcyjne

symbol	słowo kodowe	odległość 010100 XOR słowo kodowe
A	000000	2
B	001111	4
C	010011	3
D	011100	1
E	100110	3
F	101001	5
G	110101	2
H	111010	4

Przykładowe protokoły warstwy łącza danych

1. Nieograniczony protokół simpleksowy
   (a) dane przesyłane są tylko w jednym kierunku
   (b) warstwy sieciowe nadająca i odbierająca są zawsze gotowe
   (c) czas przetwarzania można pominąć
   (d) dostępne jest nieograniczone miejsce w buforach
   (e) kanał komunikacyjny nie uszkadza i nie traci ramek
2. Simpleksowy protokół stop-and-wait

   Jeśli zrezygnować z założenia (b), to pojawia się problem jak zabezpieczyć odbiornik przez zalewaniem ramkami przez nadajnik. Jeśli w odbiorniku nie następuje automatyczne, sprzętowe buforowanie i kolejkowanie ramek, to nie można nadać kolejnej ramki bez potwierdzenia, że poprzednia została poprawnie przekazana do warstwy sieciowej odbiornika. Po wysłaniu ramki nadajnik czeka na nadejście potwierdzenia (pusta ramka). Do komunikacji wystarcza kanał półdupleksowy.

Przykładowe protokoły warstwy łącza danych

3. Simpleksowy protokół dla kanału z zakłóceniami

   Jeśli nie jest spełnione założenie (e), to sprzęt odbiornika wykrywa uszkodzone ramki i je porzuca. W przypadku, kiedy nadajnik używa czasomierza, to może ponownie przesłać utraconą ramkę.

   Co się dzieje, jeśli do nadawcy nie dociera ramka potwierdzająca?

   Nadanie ponownie ramki może spowodować, że warstwa sieciowa odbiorcy otrzyma dwie identyczne ramki. Rozwiązanie polega na dodaniu do każdej wysyłanej ramki numeru sekwencyjnego.

   Protokoły, w których nadajnik czeka na pozytywne potwierdzenie przed wysłaniem kolejnej porcji danych zwane są PAR (*Positive Acknowledgment with Retransmission*).

Przykładowe protokoły warstwy łącza danych

4. Protokół z oknem przesuwnym

   Jeśli nie jest spełnione założenie (a), tj. dane nie są przesyłane tylko w jednym kierunku, to dla zapewnienia komunikacji pełnodupleksowej trzeba zastosować dwa oddzielne kanały. W każdym z nich kanał „zwrotny" jest jednak słabo wykorzystywany (przesyłane są tylko potwierdzenia).

   Kanał „zwrotny" można wykorzystać do transmisji danych od odbiorcy do nadawcy dołączając pakiety potwierdzeń do pakietów z danymi. Oznacza to, że odbiorca czeka z odesłaniem ramki potwierdzenia do czasu nadejścia pakietu danych z warstwy sieciowej; jeśli brak jest odpowiednich pakietów, to potwierdzenie jest wysyłane osobno.

   Ta technika nosi nazwę „jazdy na barana" (*piggybacking*).

Zalety:

- lepsze wykorzystanie dostępnego pasma kanału (pole ACK w nagłówku kosztuje mniej niż osobna ramka).
- mniejsza liczba wysłanych ramek oznacza mniej przerwań „przybycie ramki”

Wady:

- Jak długo warstwa łącza danych powinna czekać na pakiet umożliwiający przesłanie do nadawcy potwierdzenia?

  Jeśli czas oczekiwania będzie dłuższy niż czas oczekiwania nadajnika, to nadawca wyśle ponownie ramkę (i wysyłanie potwierdzenia traci sens). Ponieważ warstwa łącza danych nie potrafi przewidzieć zachowania warstwy sieciowej, więc wysyła potwierdzenie, jeśli w określonym czasie oczekiwania nie pojawi się nowy pakiet.

Rozwiązanie (protokół z oknem przesuwnym):

- wszystkie ramki są numerowane
- nadajnik pamięta zbiór numerów sekwencyjnych ramek, które ma prawo wysłać (są to ramki mieszczące się w tzw. oknie nadawczym)
- odbiornik utrzymuje okno odbiorcze, które zawiera numery sekwencyjne ramek, które ma prawo odebrać
- ramki związane z oknem nadawczym są buforowane, żeby mogły być w razie potrzeby ponownie przesłane
- ramki nie muszą być przekazywane do warstwy sieciowej w kolejności nadejścia

Przykładowe protokoły warstwy łącza danych

5. Protokoły używające techniki *go to n* i powtórzeń selektywnych

   Jeśli nie jest spełnione założenie (c), tj. nie można pominąć czasu przetwarzania sygnału, to długi czas podróży w obie strony może mieć poważny (negatywny) wpływ na skuteczność wykorzystanie pasma.

   Kanał satelitarny: szybkość 50 kb/s, opóźnienie 500 ms.

   Wysłanie ramki długości 1000 bitów trwa 20 ms. Dociera ona do odbiornika po 270 ms. Potwierdzenie dociera do nadajnika po 520 ms. Zastosowanie protokołu z oknem przesuwnym oznacza, że nadajnik był zablokowany przez 500/520=96% czasu.

   Połączenie długiego czasu przejścia, wysokiej przepustowości i małej wielkości ramek jest bardzo niekorzystne dla wydajności kanału.

Rozwiązanie: przesyłanie ramek techniką potokową (*pipelining*); ramki są przesyłane jedna za drugą przez czas potrzebny na dotarcie pierwszej ramki do odbiornika i nadejście potwierdzenia.

Problem: Co się dzieje, kiedy ramka ze środka strumienia dociera do odbiornika uszkodzona?

Rozwiązanie:

- Protokół z techniką „wróć do n" (*go to n*)
  Ramka uszkodzona i wszystkie następne są porzucane przez odbiornik i odbiornik czeka, aż nadajnik powtórnie zacznie nadawać ramki począwszy od uszkodzonej.
- Protokół z techniką powtórzeń selektywnych
  Odebrana błędna ramka jest odrzucana, ale pozostałe odebrane ramki są buforowane do czasu ponownego przesłania przez nadajnik poprawnej ramki. Warstwa sieciowa otrzymuje wszystkie ramki z zachowaniem kolejności. Wymuszenie retransmisji odbywa się poprzez wysłanie potwierdzenia negatywnego (NAK).

Weryfikacja protokołów

Poprawność protokołów bada się stosując

- automaty skończone (automaty o skończonej liczbie stanów)

  Nadajnik i odbiornik modeluje się jako automat o określonej (skończonej) liczbie możliwych stanów, które są określone przez wszystkie wartości zmiennych. Z każdego stanu istnieje zero lub więcej możliwych przejść (zmian stanów) do innych stanów. Przejścia zachodzą, gdy występuje jakieś zdarzenie (wysłanie ramki, odebranie ramki, upłynięcie czasu oczekiwania, itp). Stosując techniki z teorii grafów można ustalić, które stany są dostępne, a które nie (analiza osiągalności), co pozwala ustalić, czy protokół jest poprawny.

- modele sieci Petriego (miejsca, przejścia, łuki i żetony)

Protokół HDLC

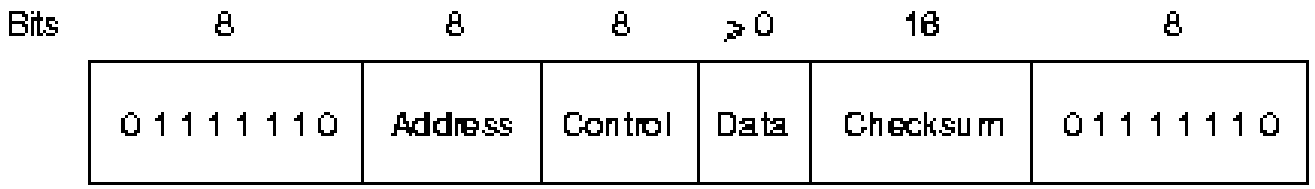
Historia protokołu HDLC (*High-level Data Link Control*):

- protokół SDLC (*Synchronous Data Link Control*) firmy IBM będący częścią SNA (*System Network Architekture*) zgłoszony do standaryzacji do ANSI i ISO
- ANSI: SDLC przekształcony w ADCCP (*Advanced Data Communication Control Procedure*)
- ISO: SDLC przekształcony w HDLC
- CCITT (od 1992 r. ITU-T (*ITU Telecommunication Standardization Sector*) przyjął i zmodyfikował HDLC do LAP (*Link Access Procedure*) jako element standardu X.25
- LAP ulega przekształceniu w LAPB (*LAP Balanced*), aby zapewnić większą zgodność z późniejszymi wersjami HDLC[81]

[81] Tanenbaum pisze: *Miło mieć tak dużo standardów do wyboru, nieprawdaż? Co więcej, jeśli żaden z nich nam się nie podoba, możemy po prostu zaczekać rok na nowszy model.*

Protokół HDLC

Wszystkie te protokoły mają organizację bitową i stosują wypełnianie bitami.
Format ramki:



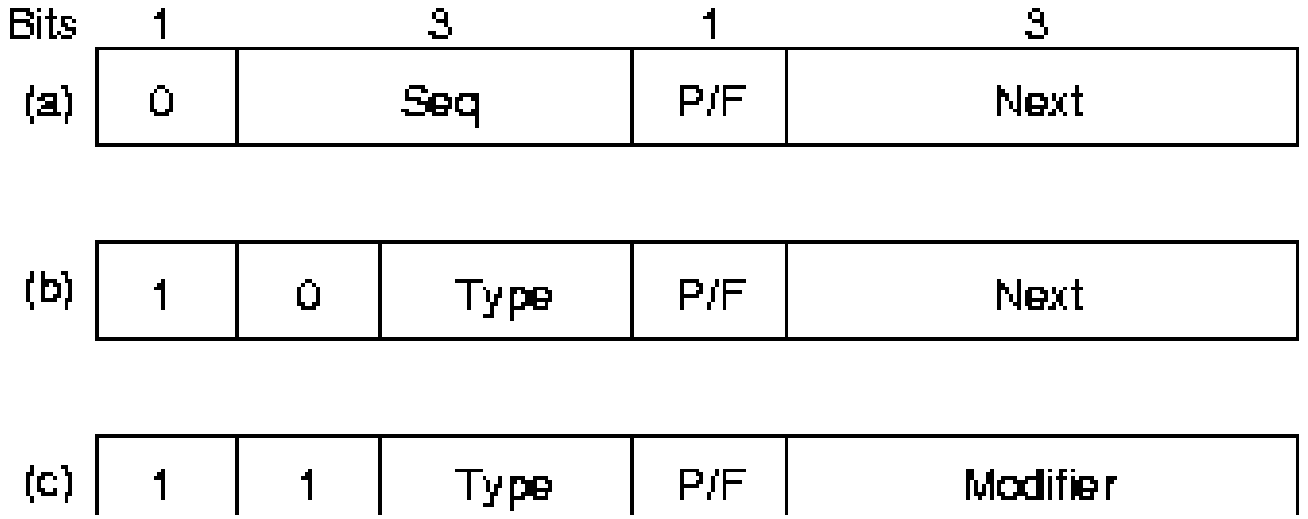
- minimalna długość ramki wynosi 32 bity
- pole *Address* jest wykorzystywane do identyfikowania terminali (na liniach z wieloma terminalami)
- pole *Control* jest wykorzystywane na numery sekwencyjne, potwierdzenia, itp.
- pole *Data* może zawierać dowolne informacje i być dowolnej długości
- pole *Checksum* zawiera kod CRC

Protokół HDLC

Rodzaje ramek:

- *Information* – ramka danych
- *Supervisory* – ramka nadzorcza
- *Unnumbered* – ramka nienumerowana

Pola sterujące poszczególnych ramek:



Protokół HDLC

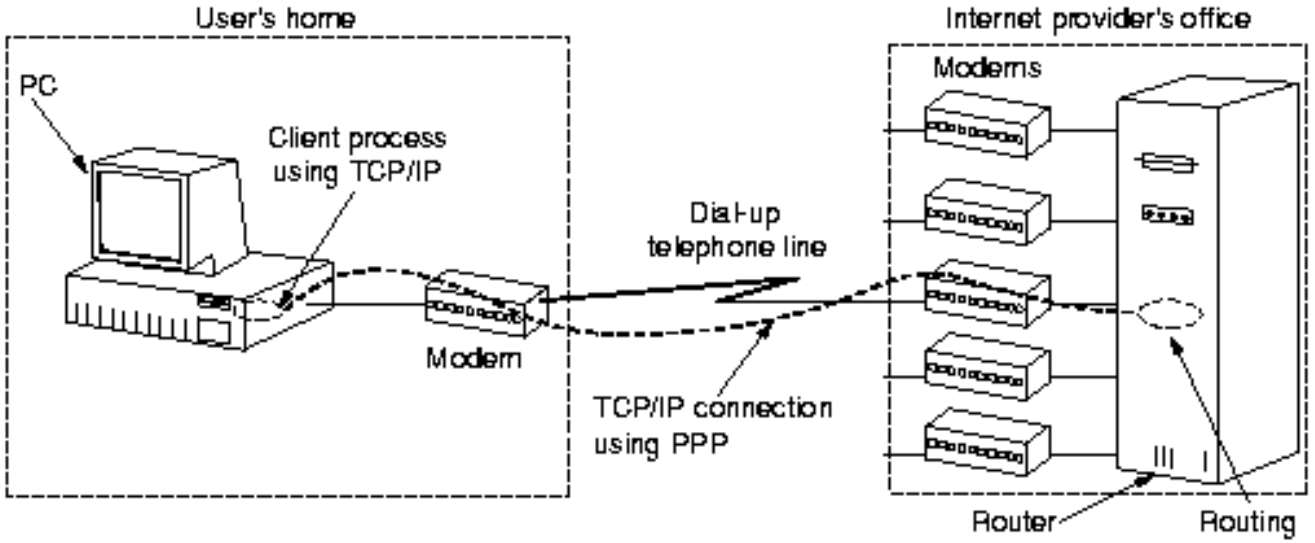
Typy ramek nadzorczych:

- ramka potwierdzająca (*RECEIVE READY*)
- ramka potwierdzenia negatywnego (*REJECT*); Next wskazuje na numer ramki do retransmisji
- *RECEIVE NOT READY* potwierdza ramki $<$ Next i nakazuje wstrzymanie nadawania
- *SELECTIVE REJECT* żąda retransmisji podanej ramki

- Ramki nienumerowane są używane do sterowania, ale mogą także przenosić dane.
- Jeśli ramki nie są transmitowane, to wysyłane są ciągle sekwencje ograniczające 7E (01111110), które są wykorzystywane przez modemy do synchronizacji zegarów.
- Na łączach synchronicznych stosuje się wypełnianie bitami, a na łączach asynchronicznych – bajtami.

Protokół PPP (*Point-to-Point Protocol*)

W Internecie do transmisji dwupunktowej między routerami oraz pomiędzy użytkownikiem domowym a ISP (*Internet Service Provider*) używa się protokołu PPP (RFC 1662, 1663).



Protokół PPP

PPP wykrywa błędy, obsługuje różne protokoły, pozwala na negocjację adresów IP w momencie podłączenia, umożliwia uwierzytelnianie.

PPP udostępnia funkcje:

- metodę ramkowania (początek, koniec, wykrywanie błędów)
- protokół LCP (*Link Control Protocol*) sterowania łączem do uruchamiania i testownia linii, negocjowania opcji (wielkość ładunku, włączanie i wybór protokołu uwierzytelniania, kompresja nagłówka); LCP obsługuje łącza synchroniczne i asynchroniczne, kodowanie bitowe i bajtowe
- sposób negocjacji opcji warstwy sieciowej niezależny od protokołu warstwy sieciowej, który będzie użyty dzięki protokołowi sterowania siecią (NCP, *Network Control Protocol*)

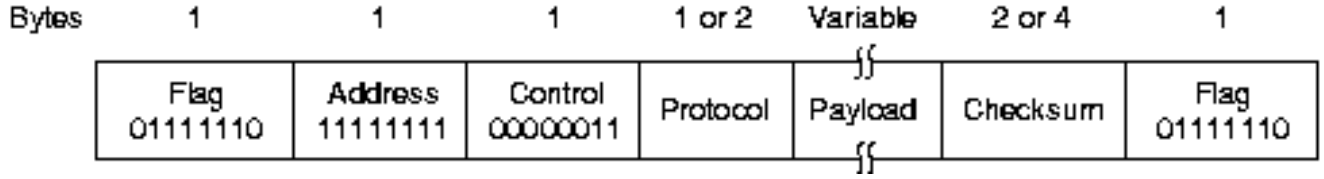
Protokół PPP

Działanie PPP: host domowy łączy się z ISP

1. komputer PC łączy się poprzez modem z routerem ISP
2. komputer PC wysyła serię pakietów LCP w polu ładunku ramek PPP w celu uzgodnienia parametrów PPP
3. komputer PC wysyła serię pakietów NCP do skonfigurowania warstwy sieciowej; jeśli jest nią TCP/IP, to trzeba pobrać IP, nazwę bramy, itd.
4. komputer PC działa jak host w sieci IP
5. użytkownik kończy pracę, to NCP zrywa połączenie w warstwie sieciowej i zwalnia IP; LCP zamyka połączenie w warstwie łącza danych; komputer nakazuje modemowi rozłączyć linię telefoniczną (następuje zamknięcie połączenia w warstwie fizycznej)

Protokół PPP

Format ramki PPP dla pracy w trybie nienumerowanym



PPP domyślnie nie zapewnia niezawodnej transmisji z użyciem numerów sekwencyjnych i potwierdzeń. Opcje PPP są negocjowane przez LCP.

Pole protokołu informuje jaki protokół jest w polu ładunku. Zostały zdefiniowane kody dla m.in. LCP, NCP, IP, IPX, AppleTalk, CLNP (*ConnectinLess Network Service*), XNS (*Xerox Network Services*).

Pole ładunku ma negocjowaną wartość (domyślnie 1500 bajtów).

Urządzenia WAN: modemy[82]

- Modem jest urządzeniem, które przekształca sygnały cyfrowe generowane przez komputer na sygnały analogowe, które mogą być przesyłane po linii telefonicznej oraz przekształca docierające sygnały analogowe na ich cyfrowe odpowiedniki (*MOdulator/DEModulator*).
- Przekształcanie sygnałów odbywa się zgodnie z protokołami modulacyjnymi i one decydują o surowej (bez kompresji) prędkości przesyłania danych.
- Organizacja ITU (*International Telecommunications Union*, wcześniej CCITT) zajmuje się standaryzacją protokołów komunikacyjnych wykorzystywanych w urządzeniach telekomunikacyjnych.

[82] Modems

Najpopularniejsze protokoły modemowe

Protokół	Maksymalna szybkość (b/s)	Sposób modulacji
V.22	1200 (600 b)	full-dupleks, PSK
V.22bis (1985)	2400 (600 b)	full-dupleks, QAM
V.32 (1987)	4800/9600 (2400 b)	asynch/synch, QAM
V.32bis (1992)	14400	asynch/synch, TCM
V.34 (1994)	28800	TCM
V.34+	33600	TCM
V.42 (1988)		V.32 + korekcja błędów
V.42bis		V.42 + kompresja danych (Lempel Ziv)
V.44 (2000)		standard kompresji danych dla V.92
V.90	31200(u)/56000(d)	PCM jednostronna
V.92 (2003)	48000(u)/56600(d)	PCM dwustronna

MNP (*Microcom Networking Protocol*)

MNP 4 + korekcja błędów oraz poprawiona szybkość transmisji (odp. V.42)

MNP 5 + korekcja błędów oraz podstawowa kompresja danych (odp. V.42bis)

PSK (*Phase Shift Keying*), QAM (*Quadrature Amplitude Modulation*), PCM (*Pulse Code Modulation*)

TCM (*Trellis Coded Modulation*)

Urządzenia WAN: modemy

- Nowoczesne modemy są wyposażone w możliwości kompresji i korekcji przesyłanych danych
- Modemy pracujące z korekcją błędów potrafią odfiltrowywać szumy oraz ponownie przesyłać uszkodzone dane.
- Modemy nawiązujące łączność potrafią uzgodnić najwyższą możliwą prędkość przesyłania danych i stosowaną korekcję błędów.

Urządzenia WAN: cyfrowe linie abonenckie

xDSL (*Digital Subscriber Line*) – cyfrowa linia abonencka (CLA) wykorzystująca stałe połączenie pomiędzy siedzibą klienta, a centralą operatora sieci telefonicznej, wymaga modemów z obu stron; szybkości od 16 Kb/s do 52 Mb/s zależy od odległości od centrali telefonicznej

- ISDN DSL (IDSL) – BRA (2B+D), zasięg do 6 km, Frame Relay
- Single Line DSL (SDSL) – CLA oparta na jednej parze przewodów, szybkość 768 Kb/s, zasięg 3 km, szybkość taka sama w obu kierunkach (symetryczy DSL)
- High speed DSL (HDSL) – CLA o szybkiej transmisji danych, dwie pary przewodów, szybkość od 384 Kb/s do 2 Mb/s, zasięg 4 km (1.544 Mb/s, zasięg 3.6 km)
- Symmetric DSL (SDSL) – HDSL wykorzystująca jedną parę przewodów

Urządzenia WAN: cyfrowe linie abonenckie

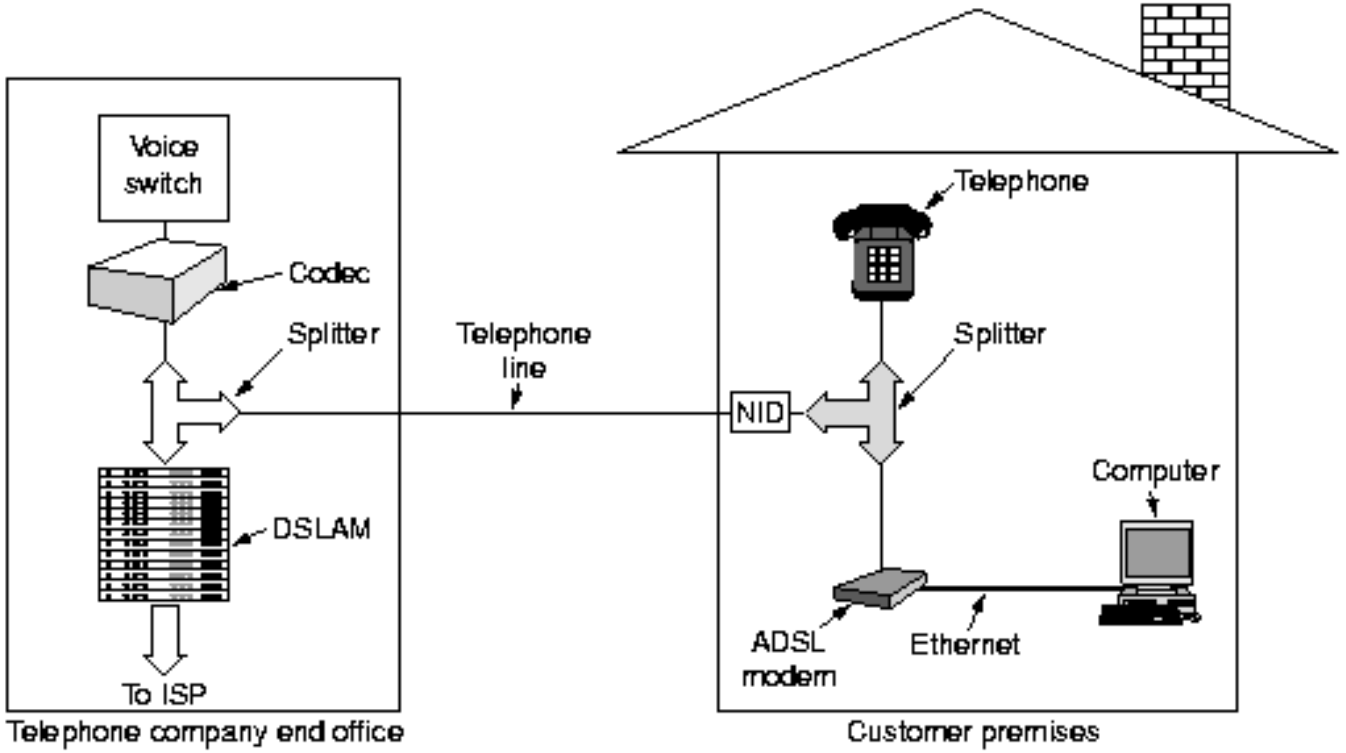
- Asymmetric DSL (ADSL) – asymetryczna CLA, para przewodów, zasięg do 6 km, szybkość do 8 Mb/s z centrali do klienta (zależna od odległości), 640 Kb/s od klienta do centrali

szybkość (w dół)	odległość
1.544 Mb/s	5.5 km
2.048 Mb/s	4.8 km
6.312 Mb/s	3.6 km
8.448 Mb/s	2.7 km

- Rate Adaptive DSL (RADSL) – CLA o adaptacyjnej szybkości transmisji (rozszerzenie ADSL), która potrafi dostosować szybkość przesyłania danych do stanu łącza
- Very high data rate DSL (VDSL) – bardzo szybka CLA, zasięg 1.5 km, szybkość do 52 Mb/s z centrali do klienta, 1.5-2.3 Mb/s od klienta do centrali

Urządzenia WAN: cyfrowe linie abonenckie

Konfiguracja sprzętowa ADSL



NID (*Network Interface Device*) – urządzenie interfejsu sieciowego

DSLAM (*Digital Subscriber Line Access Multiplexer* – multiplekser dostępowy cyfrowej linii klienta

Modemy kablowe

Infrastruktura kablowa CATV[83] może być wykorzystana do transmisji dwukierunkowej (tzw. kanał zwrotny); tani i szybki dostęp do Internetu.

Na system transmitowania danych przez sieć telewizji kablowej składa się centralny system nadawczo-odbiorczy CMTS[84] oraz modemy kablowe instalowane w mieszkaniach abonentów.

Parametry techniczne określają standardy DOCSIS[85] oraz EuroDOCSIS (odmiana europejska): wersja 1.0 (1997), 1.1 (1999), . . . 3.1 (2013), Full Duplex DOCSIS 3.1 (2016), DOCSIS 4.0 (2017):

- transmisja danych w sieci jest pakietowa i kodowana
- współistnienie różnych usług w sieci kablowej
- bezpieczeństwo przesyłania danych
- autoryzowany dostęp

[83] *Community Antenna TeleVision,CAble TV*
[84] *Cable Modem Termination System*
[85] *Data Over Cable Service Interface Specification*

Modemy kablowe

Do transmisji modem wykorzystuje kanały:

- „W dół" (*downstream*), tj. od centrali do modemu; tym kanałem o szerokości 6 MHz (8 MHz wg EuroDOCSIS) płyną stale dane od stacji nadawczej (kodowanie QAM64 lub QAM256); przepustowość do 42.88 Mbit/s (55.62 Mbit/s) na kanał.

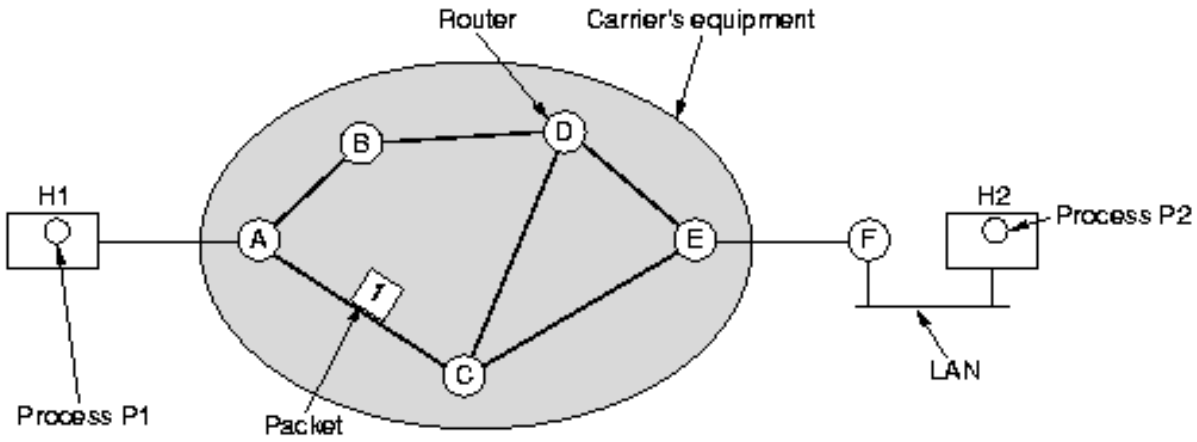
  Dla wersji 3.1/4.0 szybkości rzędu 10/10 Gb/s.

- „W górę" (*upstream*), tj. od modemu do stacji centralnej (kanał zwrotny); tym kanałem (200 kHz, 3.2 MHz, 6.4 MHz) wysyłane są dane porcjami (TDMA[86]) z pełną prędkością kanału zwrotnego lub w sposób ciągły w wydzielonej części pasma kanału zwrotnego (FDMA[87]); przepustowość: 30.72 Mbit/s dla kanału o szerokości 6.4 MHz.

  Dla wersji 3.1/4.0 szybkości rzędu 1-2/6 Gb/s.

[86] *Time Division Multiple Access*
[87] *Frequency Division Multiple Access*

Obwody datagramowe i wirtualne



Warstwa sieciowa świadczy usługi na rzecz warstwy transportowej.
Oczekuje się, że:

- usługi warstwy sieciowej powinny być niezależne od technologii routerów
- warstwa transportowa powinna być izolowana od liczby, typu i topologii routerów
- adresy sieciowe powinny być jednolite w obrębie sieci lokalnych i rozległych

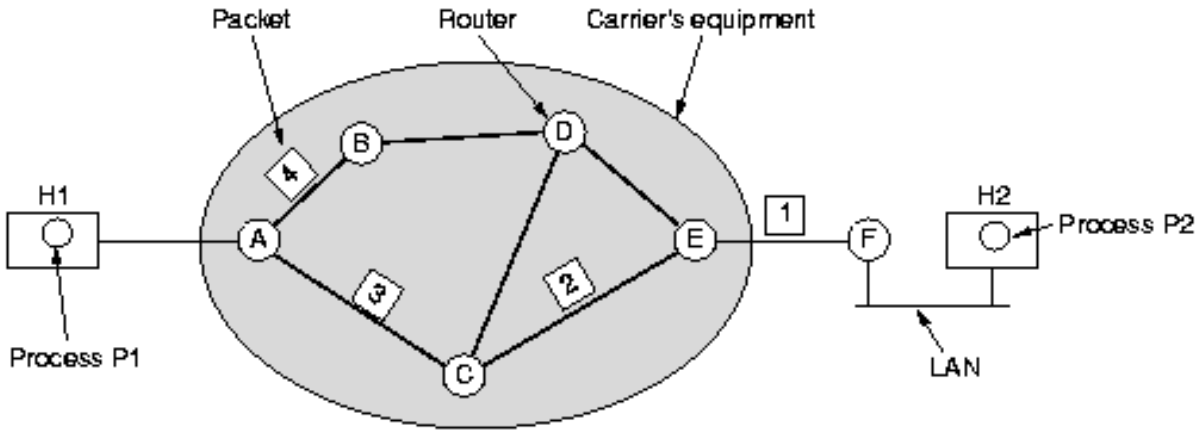
Obwody datagramowe i wirtualne

Warstwa sieciowa może świadczyć usługi

- bezpołączeniowe (Internet)
  - wysoka niezawodność
  - hosty zajmują się kontrolą błędów i kontrolą przepływu
  - każdy wysłany pakiet wysyłany jest niezależnie i wędruje trasą wyznaczaną (na bieżąco) przez kolejne routery w sieci
- połączeniowe (tradycyjna telefonia, X.25, FR, ATM)
  - wysoka jakość usług (przenoszenie sygnałów głosowych i wideo)
  - przed wysłaniem pakietu jest zestawiane połączenie pomiędzy routerem źródłowym i docelowym; tworzony jest tzw. obwód wirtualny (z takich obwodów powstaje podsieć obwodów wirtualnych)

Obwody datagramowe i wirtualne

Usługi bezpołączeniowe



A's table

initially		later	
A	–	A	–
B	B	B	B
C	C	C	C
D	B	D	B
E	C	E	B
F	C	F	B

Dest. Line

C's table

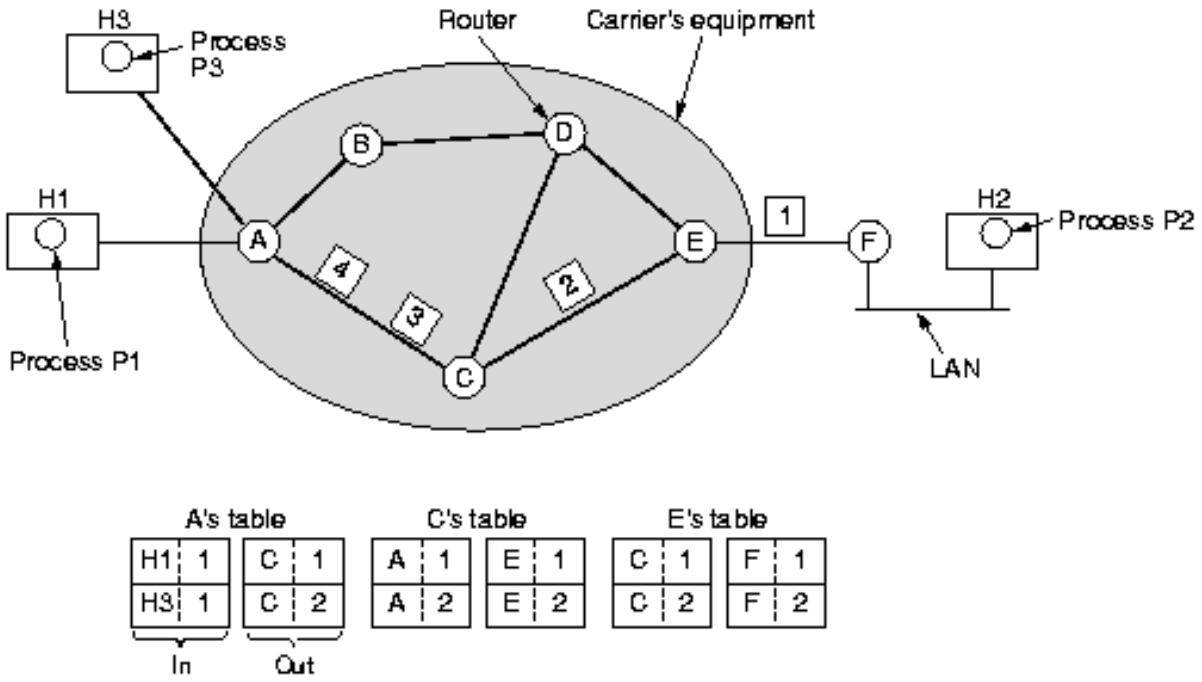
A	A
B	A
C	–
D	D
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	–
F	F

Obwody datagramowe i wirtualne

Usługi połączeniowe



Wszystkie pakiety (związane z komunikacją jakiejś pary hostów) wędrują poprzez jeden obwód wirtualny!

Porównanie podsieci datagramowej i obwodów wirtualnych

cecha	podsieci datagramowe	podsieci obwodów wirtualnych
zestawianie obwodu	niepotrzebne	wymagane
adresowanie	każdy pakiet zawiera adres globalny	każdy pakiet zawiera krótki numer VC
informacje o stanie	routery nie pamiętają stanów połączeń	każdy VC wymaga wpisu w tablicy routingu
routing	każdy pakiet trasowany niezależnie	trasa wybierana przy tworzeniu VC; jedna dla wszystkich pakietów
skutki wadliwego routingu	pakiety tracone w chwili awarii	wszystkie VC danego routera są zrywane
zapewnienie jakości usługi	trudne	łatwe, jeśli można dla każdego VC przydzielić potrzebne zasoby
kontrola przeciążeń	trudna	łatwa, jeśli można dla każdego VC przydzielić potrzebne zasoby

Obwody datagramowe i wirtualne

Porównanie:

- stosunek długość adresu do wielkości danych przenoszonych przez pakiet (wykorzystanie pasma)
- obsługa obwodów wirtualnych wymaga (zwykle) więcej pamięci w routerach
- obwody wirtualne: stosunkowo długi czas nawiązywania połączenia, krótki czas przełączania
- obwody datagramowe: złożona analiza adresu i wyboru trasy

Komutowanie obwodów (*Circuit Switching*)

POTS:

- połączeniowo zorientowane; przed przesłaniem danych musi nastąpić nawiązanie połączenia (zestawienie kanału)
- zestawiony kanał pozostaje niezmieniony w czasie trwania połączenia (stałe pasmo)
- sygnał jest przesyłany z szybkością „drutów”
- brak korekcji błędów

Komutowanie obwodów

ISDN (*Integrated Services Digital Network*) – sieć cyfrowa usług zintegrowanych

- tryb podstawowy BRA 2B+D (*Base Rate User Access*):
  - dwa kanały B (*Bearer Channel*) po 64 Kb/s do transmisji danych; dwa kanały B mogą być używane jako jeden kanał o przepustowości 128 Kb/s
  - kanał D (16 Kb/s) do przesyłania informacji sterujących

  Całkowita przepustowość łącza podstawowego wynosi 144 Kb/s.
- tryb rozszerzony PRA 30B+D (*Primary Rate User Access*)
  - 30 kanałów B (64 Kb/s)
  - jeden kanał D (64 Kb/s)

  Całkowita przepustowość 1920 Kb/s.

Do łącza ISDN można podłączyć maksymalnie 8 urządzeń abonenckich (terminali), czyli telefonów, faksów, komputerów.

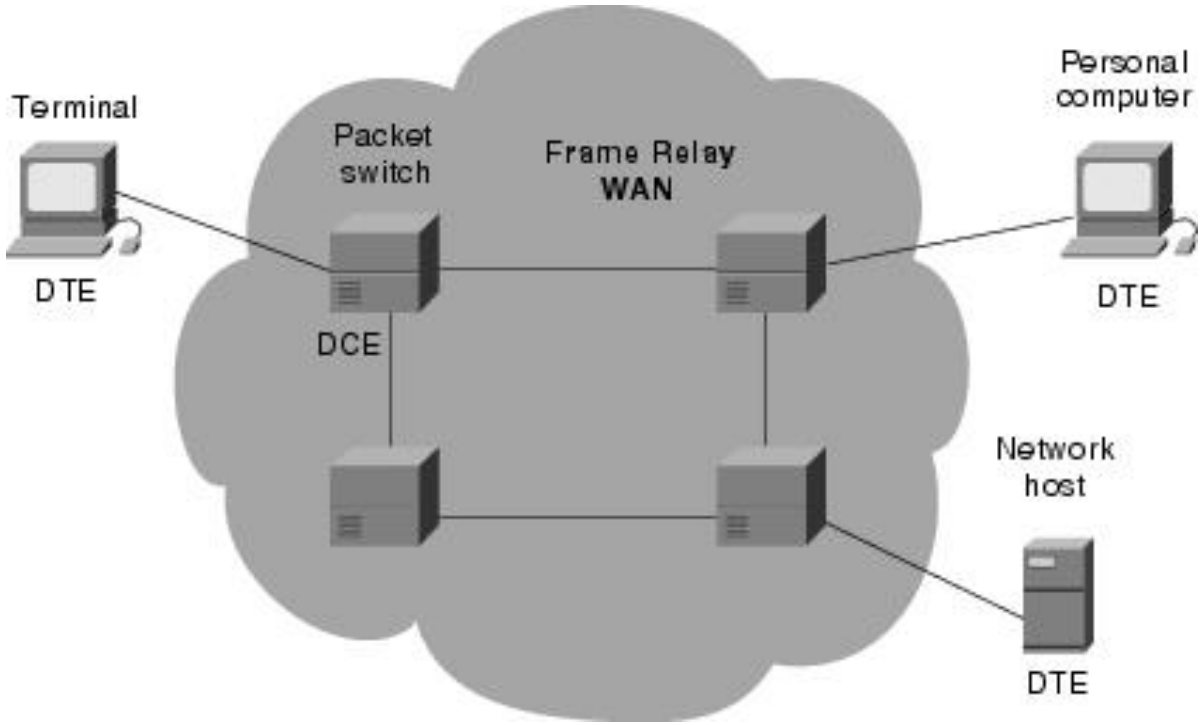
Komutowanie pakietów (*Packet Switching*)

X.25:

- standard ITU-T określający sposób podłączania terminali do cyfrowych sieci publicznych typu PDN (*Public Data Networks*)
- standard określający protokół warstwy łącza danych (HDLC) LAPB (*Link Access Procedure, Balanced*) oraz protokół warstwy sieci PLP (*Packet Level Protocol*); trasa pakietu jest wyznaczana dynamicznie przez urządzenia (przełączniki) sieciowe
- mechanizmy kontroli błędów (linie telefoniczne nie zapewniają wysokiej jakości przesyłania sygnałów)
- podłączenie wymaga urządzeń DTE (po stronie użytkownika) i DCE (po stronie dostawcy) oraz urządzeń PAD (*Packet Assembler/Disassembler*)
- szybkość 64 Kb/s (nowsze wersje – do 2 Mb/s)

Komutowanie pakietów

Frame-Relay[88]



[88] Comprehensive Guide to Configuring and Troubleshooting Frame Relay

Komutowanie pakietów

Frame-Relay

- standard określający protokół warstwy łącza danych pozwalający tworzyć sieci wykorzystujące komutowanie pakietów zmiennej długości
- umożliwia tworzenie wielu wirtualnych obwodów przy wykorzystaniu enkapsulacji HDLC pomiędzy połączonymi urządzeniami
- wykorzystuje PVC (*Permanent Virtual Circuits*) – stałe, logiczne połączenie pomiędzy urządzeniami sieciowymi użytkownika o określonej przepustowości (CIR, *Committed Information Rate*); brak fragmentacji i routingu (odpada wybór najlepszej trasy); gwarantowana jakość usługi (QoS)
- wykorzystuje SVC (*Switched Virtual Circuits*) – komutowane obwody wirtualne pomiędzy urządzeniami sieciowymi użytkownika; zmienna charakterystyka wydajności (opóźnienia, fluktuacje)

Frame-Relay

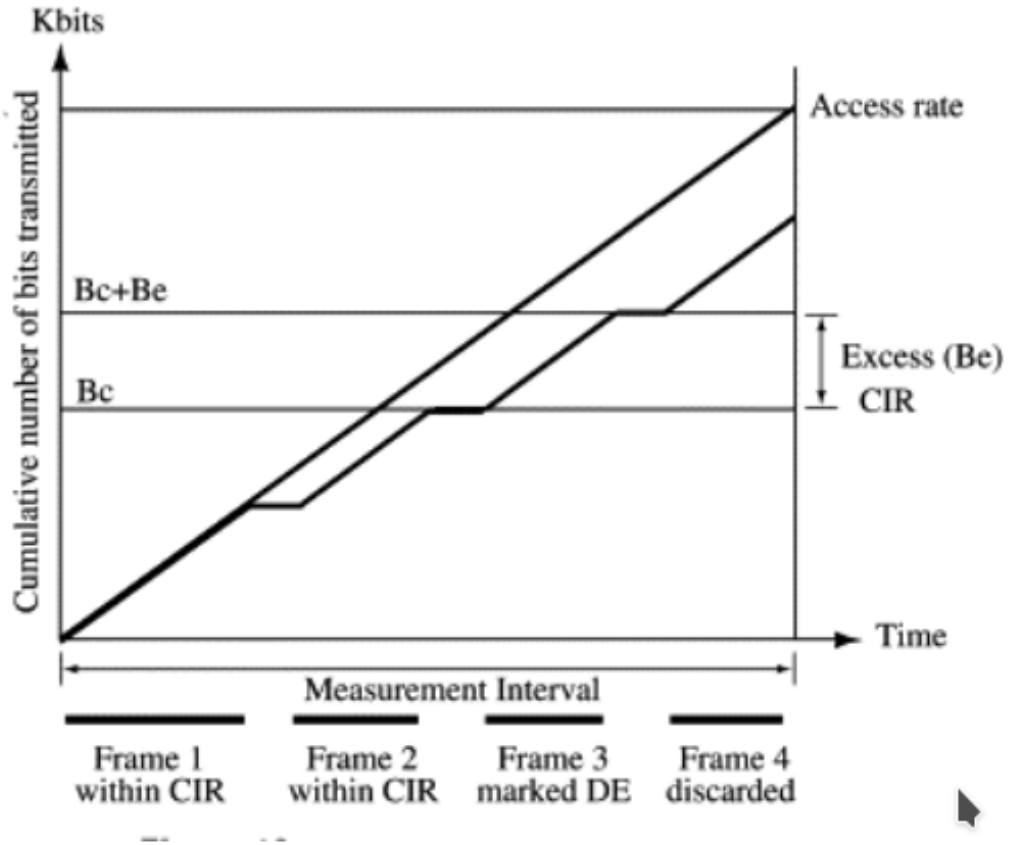
- przełączniki stosują metodę *store-and-forward* do przekazywania pakietów; możliwe priorytetowanie pakietów (CoS)
- kontrola przepływu w oparciu o bity nagłówka: DE (*Discard Eligible*), FECN (*Forward Explicit Congestion Notification*), BECN (*Backward Explicit Congestion Notification*)

  możliwość przekraczania ustalonych szybkości przekazywania informacji

  $$\text{CIR} \longrightarrow \text{Bc} \ (\textit{Committed Burst Rate}) \longrightarrow \text{Be} \ (\textit{Excess Burst Rate})$$

  Bc umowny wskaźnik pakietów, Be nadmiarowy wskaźnik pakietów
- wymaga użycia urządzeń CSU/DSU w celu stworzenia fizycznego połączenia z siecią WAN w oparciu o dzierżawione linie cyfrowe (tradycyjne i optyczne)
- wymaga zastosowania routerów do połączenia sieci LAN z WAN
- opłaty stałe (PVC) lub za przesłane pakiety (SVC)

Frame Relay: CIR+Bc+Ec[89]

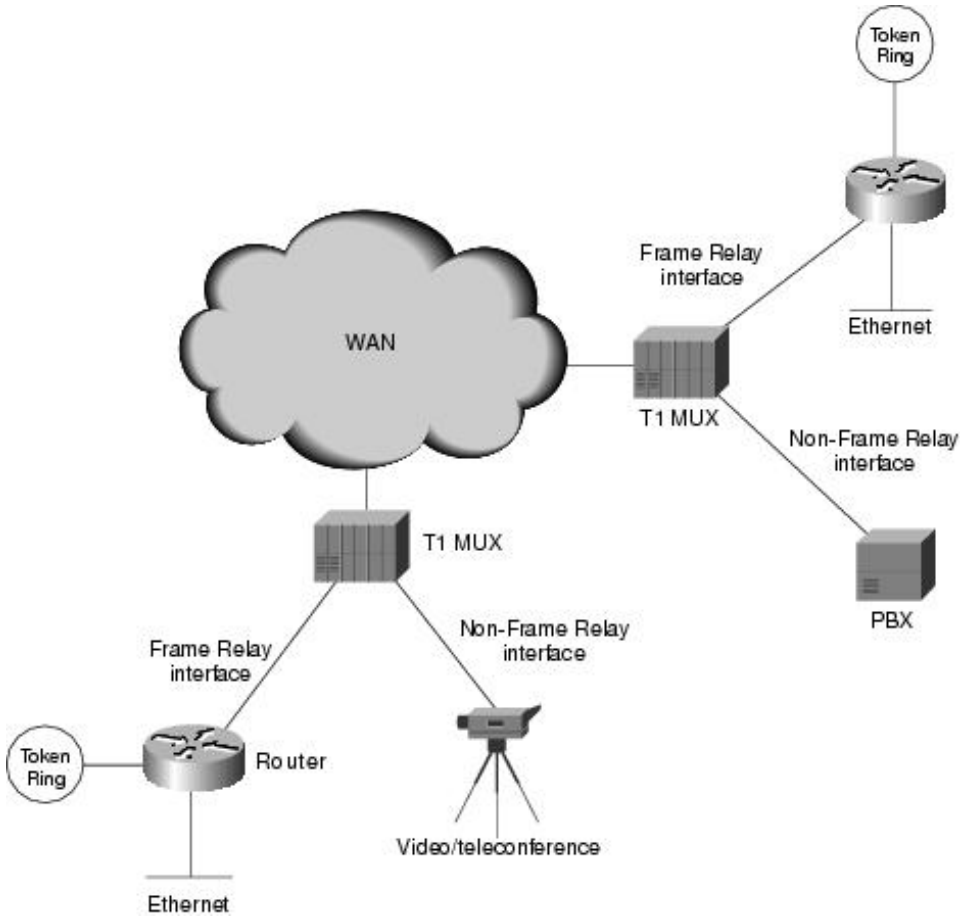


[89] CIR+Bc+Ec

Frame-Relay:

- rozszerzonie Frame Relay o LMI (*Local Management Interface*) pozwala na stosowanie adresowania globalnego, tj. jednoznacznych identyfikatorów łącza danych (DLCI, *Data Link Connection Identifier*) w obrębie globalnej „chmury Frame Relay"; LMI pozwala także na stosowanie transmisji rozgłoszeniowych
- wydajniejszy od X.25, ograniczona kontrola poprawności przesyłanych danych; brak mechanizmów retransmisji ramek, błędne ramki są porzucane, punkty końcowe łącza są odpowiedzialne za powtórne przesłanie danych
- traktowany jako następca X.25

Frame Relay


Token Ring
Frame Relay interface
WAN
Ethernet
T1 MUX
Non-Frame Relay interface
T1 MUX
PBX
Non-Frame Relay interface
Frame Relay interface
Token Ring
Router
Video/teleconference
Ethernet

Porównanie linii dzierżawionych i Frame Relay

Linie dzierżawione	Frame Relay
Architektura oczek pełnych wymaga n(n−1)/2 łączy fizycznych	Architektura oczek pełnych wymaga n(n−1)/2 stałych lub komutowanych obwodów wirtualnych, ale n łączy fizycznych
Trudne i drogie dodawanie oraz usuwanie nowych linii	Dodawanie/usuwanie nowych połączeń wymaga tylko dodania/usunięcia obwodu wirtualnego
Mniejsza niezawodność, brak połączeń zapasowych	Większa niezawodność, połączenia zapasowe
Słabe wykorzystanie pasma	Dobre wykorzystanie pasma

Zalety sieci Frame Relay

Prywatne sieci Frame Relay:

- wykorzystanie istniejącego sprzętu sieciowego (ochrona inwestycji)
- dzięki współdzieleniu pasma lepsze wykorzystanie istniejących obwodów
- większa elastyczność i kontrola nad siecią

Publiczne sieci Frame Relay:

- zmniejszenie kosztów własności (szkieletem sieci zarządza dostawca usługi)
- duży zasięg geograficzny, tanie połączenia wielu oddalonych miejsc, możliwość dostępu wdzwanianego (*dial-in*)
- ułatwione współdziałanie z niezależnymi organizacjami

Komutowanie komórek (*Cell Switching*)

ATM (*Asynchronous Transfer Mode*):

- usługa bezpołączeniowa (przed przesłaniem danych nie musi następować nawiązanie połączenia, bo każda komórka zawiera adres docelowy) wykorzystująca komórki o stałej długości 53 bajtów (48 bajtów danych i 5 bajtów nagłówka)
  - SVC (*Switched Virtual Circuits*) – komórki są routowane dynamicznie,
  - PVC (*Permanent Virtual Circuits*) – połączenia są zestawiane ręcznie
- logiczny routing pozwala na dobre wykorzystanie zasobów sieci i dostępnej przepustowości
- logiczne obwody pozwalają na zagwarantowanie jakości usługi (QoS)

Komutowanie komórek

- przełączniki komórek używają metody *store-and-forward* do przekazywania danych; możliwość wykrywania błędów i priorytetowania pakietów (CoS)
- komórki przesyłane poprzez sieci LAN oraz WAN pracujące w trybie podstawowym (*baseband*) oraz szerokopasmowym (*broadband*); szybkość 155 Mb/s (C-3), 622 Mb/s (C-12) lub więcej
- możliwość przesyłania głosu, obrazów, danych, sygnału wideo w czasie rzeczywistym, sygnałów audio wysokiej jakości
- wszystkie rodzaje danych są umieszczane w identycznych komórkach, co czyni transmisję prostą, jednorodną i przewidywalną

Komutacja komórek łączy zalety sieci z komutacją łączy (gwarantowana przepustowość) z zaletami sieci z komutacją pakietów (wydajne wykorzystaniem pasma i możliwość priorytetowania danych).

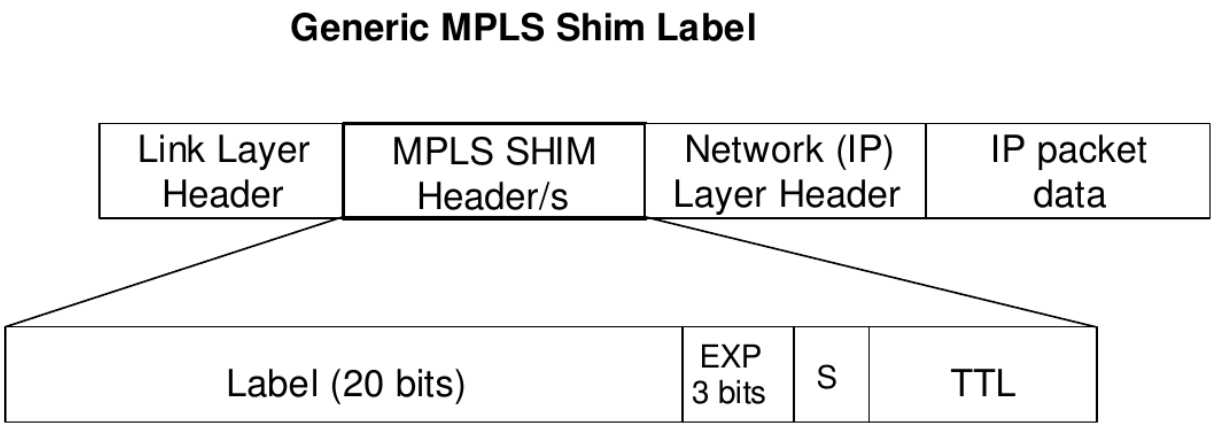
Komutowanie etykiet[90]

MPLS (*Multi-Protocol Label Switching*) – wieloprotokołowe przełączanie etykiet (protokół warstwy 2.5!)

- opracowany przez IETF w oparciu o rozwiązania komercyjne
  - *Cisco's Tag Switching*
  - *IBM's Aggregate Route-based IP Switching*
  - *IP Switching* (*Ipsilon Networks*, potem część Nokii)
  - *IP Navigator* (Lucent/Ascend)
- efektywne i uproszczone szybkie przekazywanie pakietów IP
- tworzenie skalowalnych sieci, możliwość zapewnienia QoS
- inżynieria ruchu i sterowanie routingiem (*Label Switched Paths*, *Resource ReSerVation Protocol-Traffic Engineering*, *Label Distribution Protocol*); wybór najkrótszej trasy, która zapewnia określoną przepustowość

[90] Frame Relay + MPL, MPLS for Dummies

Ogólna etykieta MPLS



- etykieta jest dodawana, jeśli protokół warstwy 2. jej nie posiada (PPP, Ethernet)
- hierarchia etykiet, tylko najbliższa nagłówkowi warstwy 2 się liczy, pole S (1 bit) do oznaczenia ostatniej etykiety w stosie
- pole Exp (*Traffic Class*) – wskazuje na inną zasadę przekazywania pakietów (np. *Differential Services*)

Komutowanie etykiet

Przełączanie etykiet wg MPLS:

- pierwsze urządzenie (*ingress node*) wyszukuje całą trasę, aż do routera końcowego (*egress node*)
- cała trasa jest oznaczana etykietą (powstaje tunel)
- routery (*transit nodes*) używają tej etykiety do routowania pakietów
- ostatni router (*egress node*) usuwa etykietę
- pakiet jest dostarczany wg zwykłego routingu IP

Komutowanie etykiet

```
root@hel ~]# traceroute -e www.nyse.com
traceroute to www.nyse.com (104.16.104.50), 30 hops max, 60 byte packets
 1  gateway (158.75.5.254)  0.883 ms  1.277 ms  1.772 ms
 2  158.75.64.105 (158.75.64.105)  0.455 ms  1.040 ms  1.185 ms
 3  pionier-GW.man.torun.pl (158.75.33.34)  0.397 ms  0.341 ms  0.361 ms
 4  z-torunia.poznan-gw3.10Gb.rtr.pionier.gov.pl (212.191.224.161) \
                                                    3.700 ms 3.662 ms  3.696 ms
 5  pionier-ias-geant-gw-1.poz.pl.geant.net (83.97.88.121) \
                                                    3.761 ms  3.704 ms 3.717 ms
 6  ae3.mx1.fra.de.geant.net (62.40.98.130) <MPLS:L=537799,E=0,S=1,T=1>
                                                  20.484 ms 20.657 ms  20.595 ms
 7  de-cix-frankfurt.as13335.net (80.81.194.180)  21.682 ms  21.640 ms  21.581 ms
 8  104.16.104.50 (104.16.104.50)  20.535 ms  20.505 ms  20.497 ms
```

Jaką rolę w sieci pełnią routery?

- Router jest urządzeniem sieciowym warstwy 3 łączącym dwa lub więcej segmentów lokalnej sieci komputerowej, sieci LAN lub WAN.
- Router przekazuje (komutuje, trasuje) pakiety wykorzystując adresy warstwy 3. i tabelę routingu (*forwarding*).

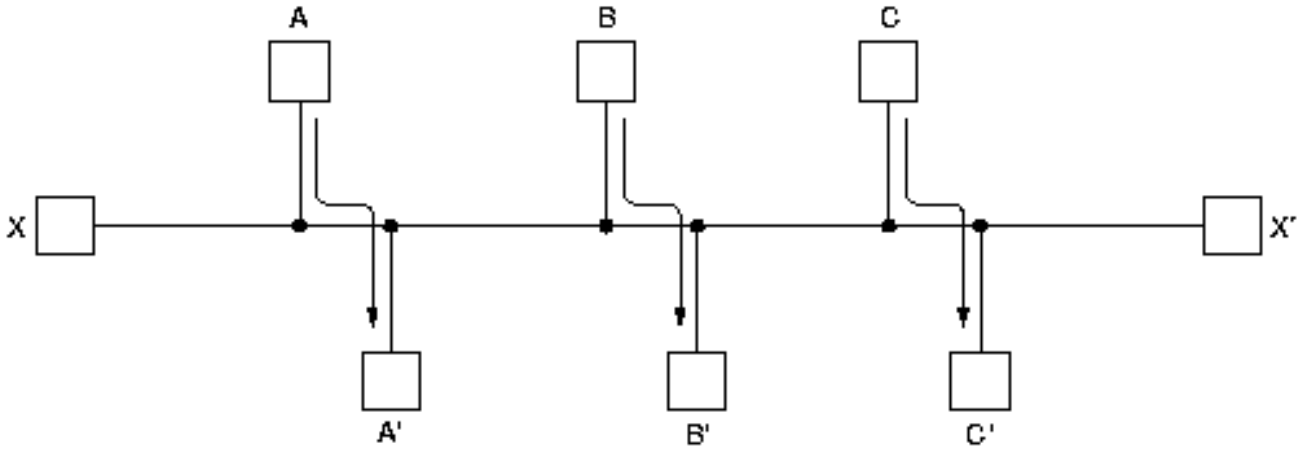
  Dla protokołów bezpołączeniowych decyzja o wyborze trasy jest podejmowana dla każdego przychodzącego pakietu.

  Dla protokołów połączeniowych wybór trasy dokonuje się w czasie tworzenia obwodu wirtualnego (routing sesji).
- Tabela routingu jest budowana w oparciu o jedną lub wiele metryk w celu ustalenia optymalnej ścieżki dla ruchu sieciowego. Za budowę tabeli routingu jest odpowiedzialny algortym routingu.

  Algorytm routingu musi być prosty, poprawny, odporny, stabilny, sprawiedliwy i optymalny.

Jaką rolę w sieci pełnią routery?

Konflikt między optymalnością i sprawiedliwością



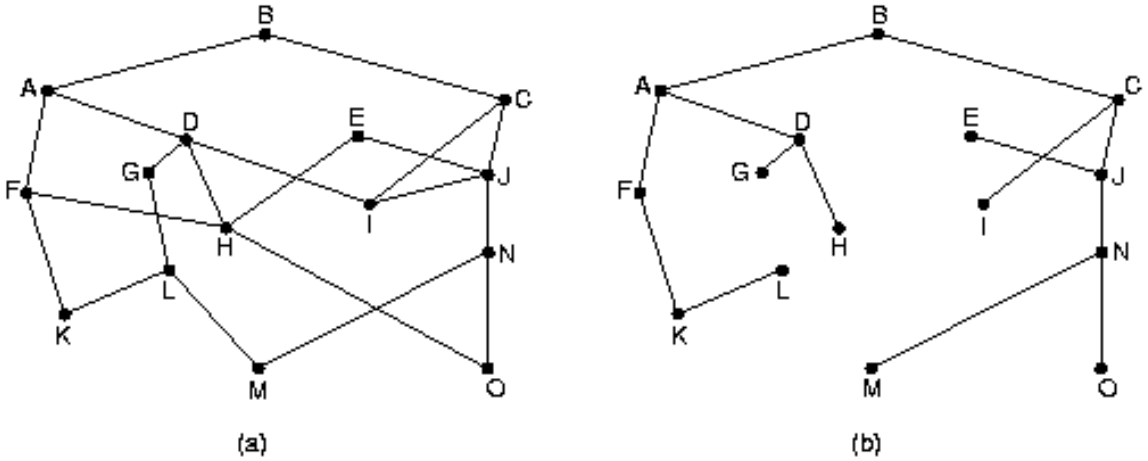
Zastosowanie systemu kolejkowania w celu sprawiedliwego przekazywania pakietów może prowadzić do dużych opóźnień w ruchu pakietów.

Wyróżnia się algorytmy nieadaptacyjne (routing statyczny) i adaptacyjne (routing dynamiczny).

Algorytmy (protokoły) routingu

Zasada optymalności: jeśli router J znajduje się na optymalnej trasie od routera I do routera K, to optymalna ścieżka od J do K przebiega tą samą trasą.

Z zasady optymalności wynika, że zbiór optymalnych tras z wszystkich źródeł do jednego celu tworzy drzewo z korzeniem w węźle docelowym (tzw. drzewo ujścia).



Zadaniem algorytmów routingu jest wykrycie i stosowanie drzew ujścia dla wszystkich routerów.

Protokół trasowania/routingu (*routing protocol*) to protokół obsługujacy protokoły trasowane poprzez dostarczanie mechanizmów umożliwiających wymianę informacji między routerami i wybór trasy pakietów. Do protokołów routingu zaliczamy takie protokoły jak:

- APPN (*Advanced Peer-to-Peer Networking*)
- BGP (*Border Gateway Protocol*) protokół bramy granicznej
- EGP (*Exterior Gateway Protocol*) protokół zewnętrznej bramy
- EIGRP (*Enhanced IGRP*)
- IGRP (*Interior Gateway Routing Protocol*) protokół routingu wewnętrznej bramy
- IS-IS (*Intermediate System-to-Intermediate System*)
- NLSP (*Netware Link Services Protocol*)
- OSPF (*Open Shortest Path First*) otwarty z wybieraniem najpierw najkrótszej ścieżki
- RIP (*Routing Information Protocol*)

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.

Protokoły routingu dzielą się na tzw. protokoły:

- wewnętrzne – wykorzystywane do trasowania wspólnie zarządzanych sieci (tzw. systemy autonomiczne), np. RIP, IGRP, OSPF
- zewnętrzne – wykorzystywane do wymiany informacji o trasach między sieciami, które nie są wspólnie zarządzane, np. EGP, BGP

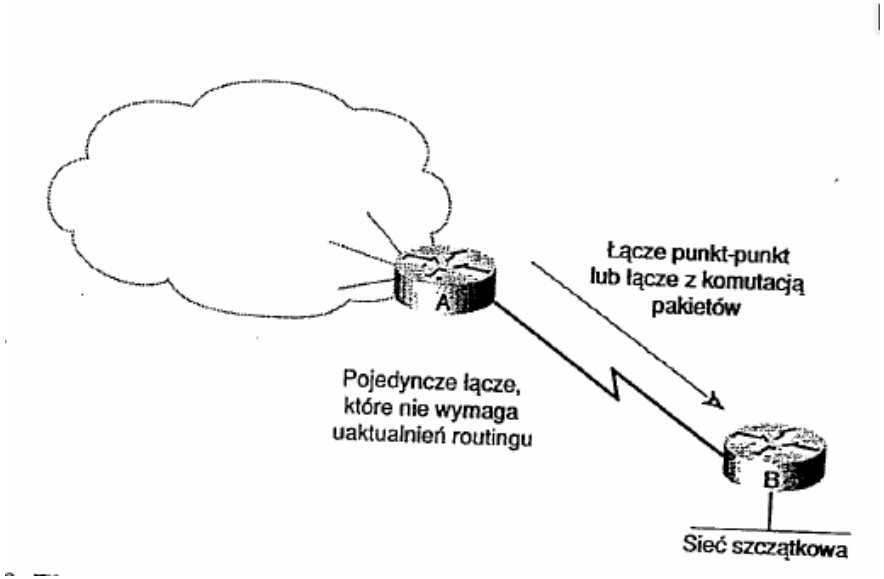
Od protokołów routingu wymaga się, aby były proste i wydajne, odporne na różne zachowanie sieci, elastyczne (szybko dostosowywać się do zmieniających się warunków w sieci) oraz pozwalające na uzyskanie szybkiej zbieżności.

Zbieżność to zdolność urządzeń obsługujących sieć do przekazywania sobie informacji o zmianie topologii sieci i ponownego wyliczenia optymalnych tras.

Kiedy o sieci złożonej z wielu routerów mówimy, że osiągnęła zbieżność?

Routing może być

- statyczny – tabela routingu jest tworzona przez administratora sieci, który ustala ręcznie trasy pakietów, np. w odniesieniu do sieci szczątkowych/końcowych (*stub networks*)



- dynamiczny – tabela routingu jest tworzona i modyfikowana w oparciu o informacje wymieniane przez routery w oparciu o różne protokoły routingu

Protokoły routingu stosują różne metryki do ustalania najlepszej ścieżki. Metryki wykorzystują takie charakterystyki ścieżek jak:

- Liczba skoków – liczba routerów, przez które musi przejść pakiet, zanim osiągnie miejsce przeznaczenia (ścieżka jest tym lepsza im liczy mniej skoków)
- Pasmo – przepustowość/pojemność łącza (np. łącze T3 jest lepsze niż T1)
- Opóźnienie – czas potrzebny na dotarcie pakietu ze źródła do miejsca przeznaczenia
- Niezawodność – częstotliwość występowania błędów na poszczególnych odcinkach łącza
- Takty – opóźnienie w warstwie łącza danych (wyrażane w taktach zegara IBM PC, czyli około 55 milisekund)
- Koszt – arbitralna wartość powiązana z szerokością pasma, kosztem dzierżawy łącza, itp.

```
# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         158.75.52.1     0.0.0.0         UG    600    0        0 wlan0
158.75.4.0      172.20.1.26     255.255.254.0   UG    0      0        0 tun0
158.75.52.0     0.0.0.0         255.255.254.0   U     600    0        0 wlan0
158.75.104.0    172.20.1.26     255.255.254.0   UG    0      0        0 tun0
172.20.0.1      172.20.1.26     255.255.255.255 UGH   0      0        0 tun0
172.20.1.26     0.0.0.0         255.255.255.255 UH    0      0        0 tun0
192.168.35.0    172.20.1.26     255.255.255.0   UG    0      0        0 tun0
192.168.100.0   172.20.1.26     255.255.255.0   UG    0      0        0 tun0

# ip route show
default via 158.75.52.1 dev wlan0 proto static metric 600
158.75.4.0/23 via 172.20.1.26 dev tun0
158.75.52.0/23 dev wlan0 proto kernel scope link src 158.75.53.9 metric 600
158.75.104.0/23 via 172.20.1.26 dev tun0
172.20.0.1 via 172.20.1.26 dev tun0
172.20.1.26 dev tun0 proto kernel scope link src 172.20.1.25
192.168.35.0/24 via 172.20.1.26 dev tun0
192.168.100.0/24 via 172.20.1.26 dev tun0

  U (route is up)                                 D (dynamically installed by daemon or redirect)
  H (target is a host)                            M (modified from routing daemon or redirect)
  G (use gateway)                                 A (installed by addrconf)
  R (reinstate route for dynamic routing)         C (cache entry)
                                                  ! (reject route)
```

```
BGP table version is 962513, local router ID is 10.1.2.5
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop                 Metric LocPrf Weight Path
*  4.17.250.0/24    12.123.45.252              0 7018 1239 13716 i
*>                  12.123.1.236               0 7018 1239 13716 i
*                   12.123.5.240               0 7018 1239 13716 i
*                   12.123.17.244              0 7018 1239 13716 i
*  4.23.84.0/22     12.123.45.252              0 7018 6461 20171 i
*>                  12.123.1.236               0 7018 6461 20171 i
*                   12.123.17.244              0 7018 6461 20171 i
*                   12.123.5.240               0 7018 6461 20171 i
*  4.23.112.0/24    12.123.45.252              0 7018 174  21889 i
*>                  12.123.1.236               0 7018 174  21889 i
*                   12.123.5.240               0 7018 174  21889 i
*                   12.123.17.244              0 7018 174  21889 i
```

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

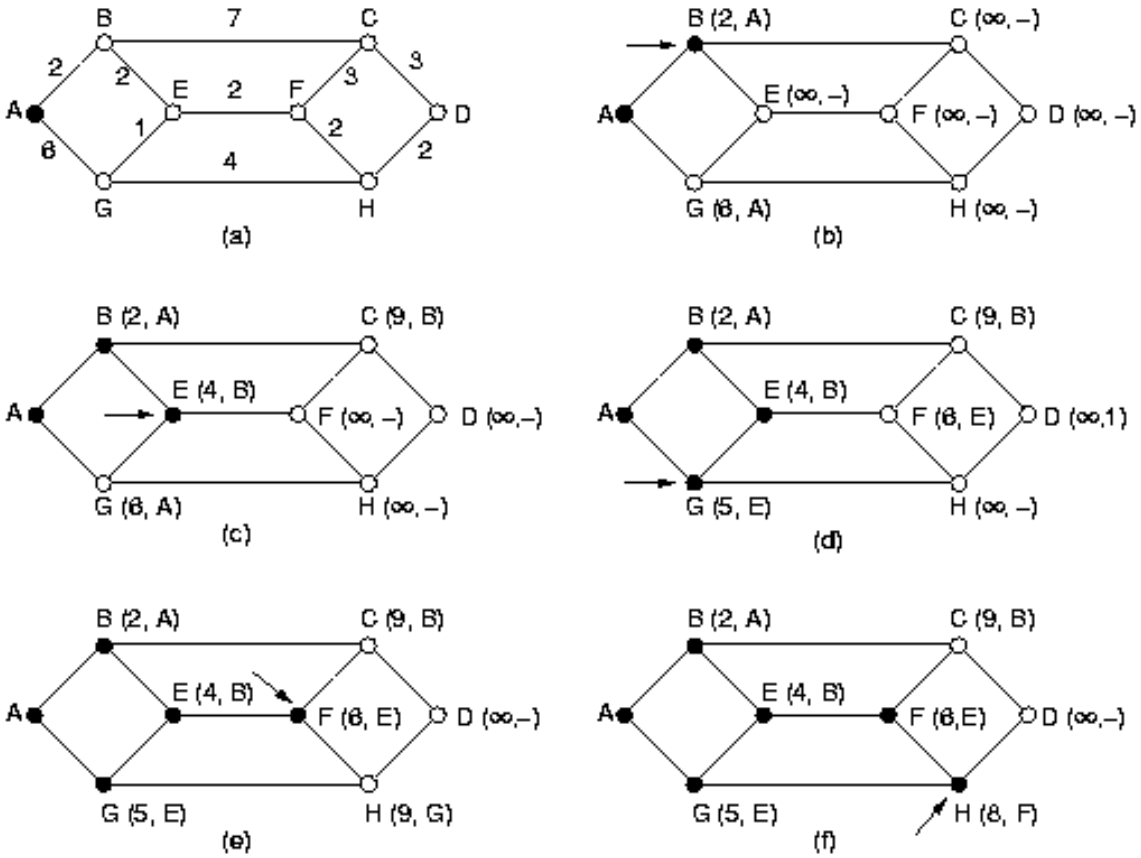
Routing z wyborem najkrótszej ścieżki

Sieć złożona z routerów jest reprezentowana przez graf, którego węzłami są routery, a łukami są linie komunikacyjne łączące węzły.

- Każdy węzeł jest oznaczany odległością od węzła źródłowego wzdłuż najlepszej znanej ścieżki.
- Etykiety mogą ulegać zmianą w miarę postępu algorytmu i znajdowania nowych ścieżek. Etykieta może być tymczasowa lub trwała. Na początku wszystkie etykiety są tymczasowe.

Do wyznaczania najkrótszej ścieżki służy algorytm Dijkstry (algorytm STP, *Shortest Path First*)

Algorytm Dijkstry wyznaczania najkrótszej ścieżki od A do D



Routing rozpływowy

Routing rozpływowy (*flooding*) jest algorytmem statycznym, w którym każdy przychodzący pakiet jest rozsyłany na każdą linię wyjściową (z wyjątkiem tej, z której nadszedł).

Algorytm ten generuje ogromne liczby pakietów, które trzeba ograniczać przez mechanizm postarzania pakietów lub stosowania numerów sekwencyjnych, żeby dany pakiet przechodził przez węzeł tylko raz.

Selektywny routing rozpływowy rozsyła pakiety w kierunku zgodnym z węzłem docelowym i dla każdego pakietu znajduje najlepszą ścieżkę, bo wszystkie możliwości są sprawdzane.

Routing wg wektora odległości

Algorytmy routingu wg wektora odległości powodują, że każdy z routerów okresowo rozsyła kopię swojej tabeli routingu do sąsiadujących routerów. Algorytm ten pozwala modyfikować informację o topologii sieci, ale żaden z routerów nie posiada informacji o topologii całej sieci.

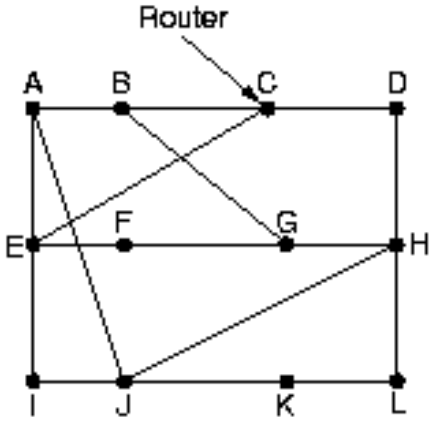
Stosowanie tego algorytmu może prowadzić do powstawaniu tzw. pętli routingu. Można temu zapobiegać przez określenie maksymalnej liczby skoków (po jej osiągnięciu sieć jest uznawana za niedostępną), zastosowaniu metody podzielonego horyzontu, ew. z zatruciem wstecz (*split horizon*, *split horizon with poisoned reverse*) lub liczników wstrzymywania (*hold down timers*).

Tablice routingu są rozsyłane regularnie przy pomocy (grupowych) rozgłoszeń lub przy zmianie topologii (*triggered updates*).

Przykładowe protokoły: RIP, IGRP

Inne nazwy: algorytm routingu Bellmana-Forda lub Forda-Fulkersona.

Routing wg wektora odległości



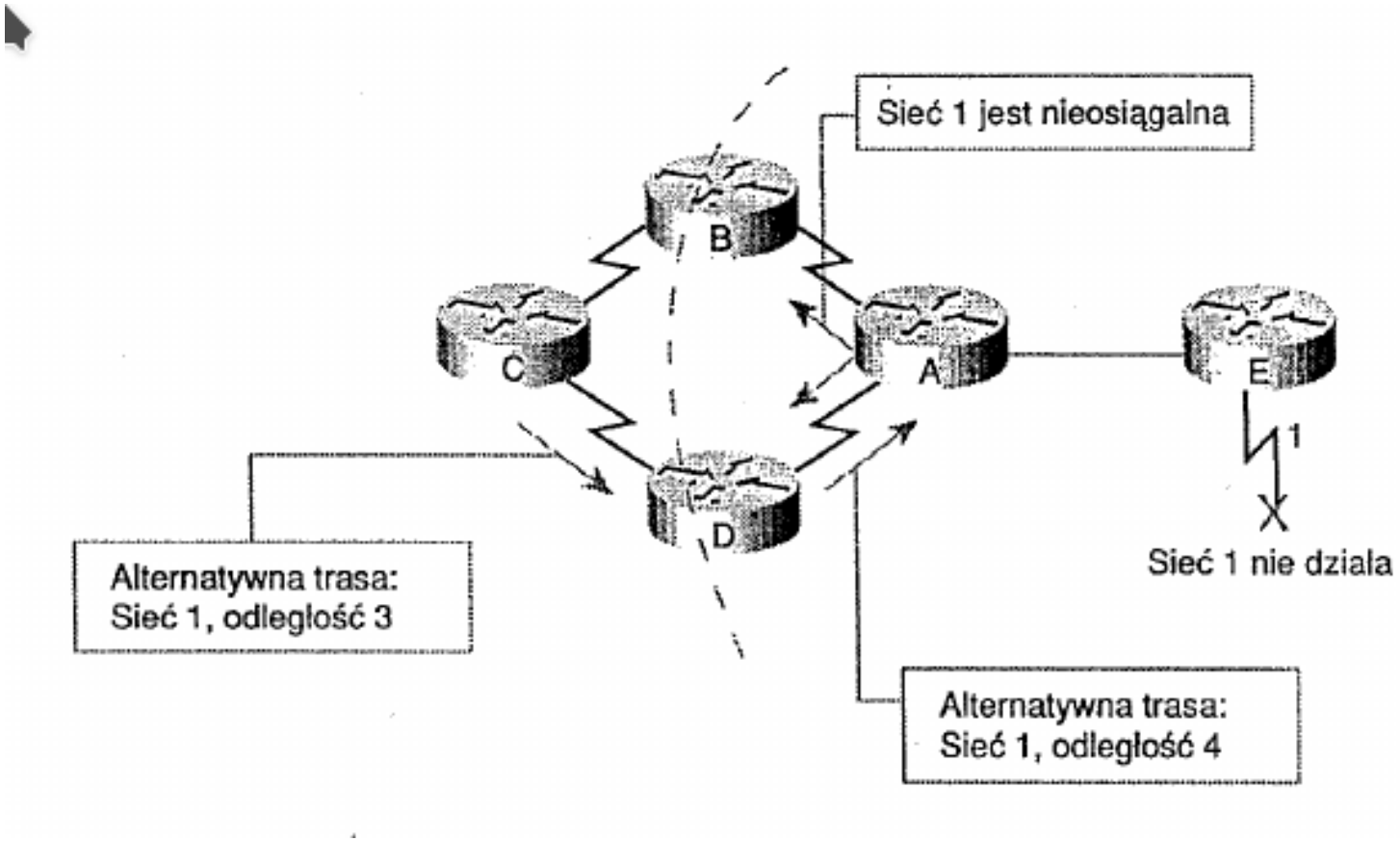
(a)

To	A	I	H	K	New estimated delay from J	Line
A	0	24	20	21	8	A
B	12	36	31	28	20	A
C	25	18	19	36	28	I
D	40	27	8	24	20	H
E	14	7	30	22	17	I
F	23	20	19	40	30	I
G	18	31	6	31	18	H
H	17	20	0	19	12	H
I	21	0	14	22	10	I
J	9	11	7	10	0	–
K	24	22	22	0	6	K
L	29	33	9	9	15	K
	JA delay is 8	JI delay is 10	JH delay is 12	JK delay is 6	New routing table for J	

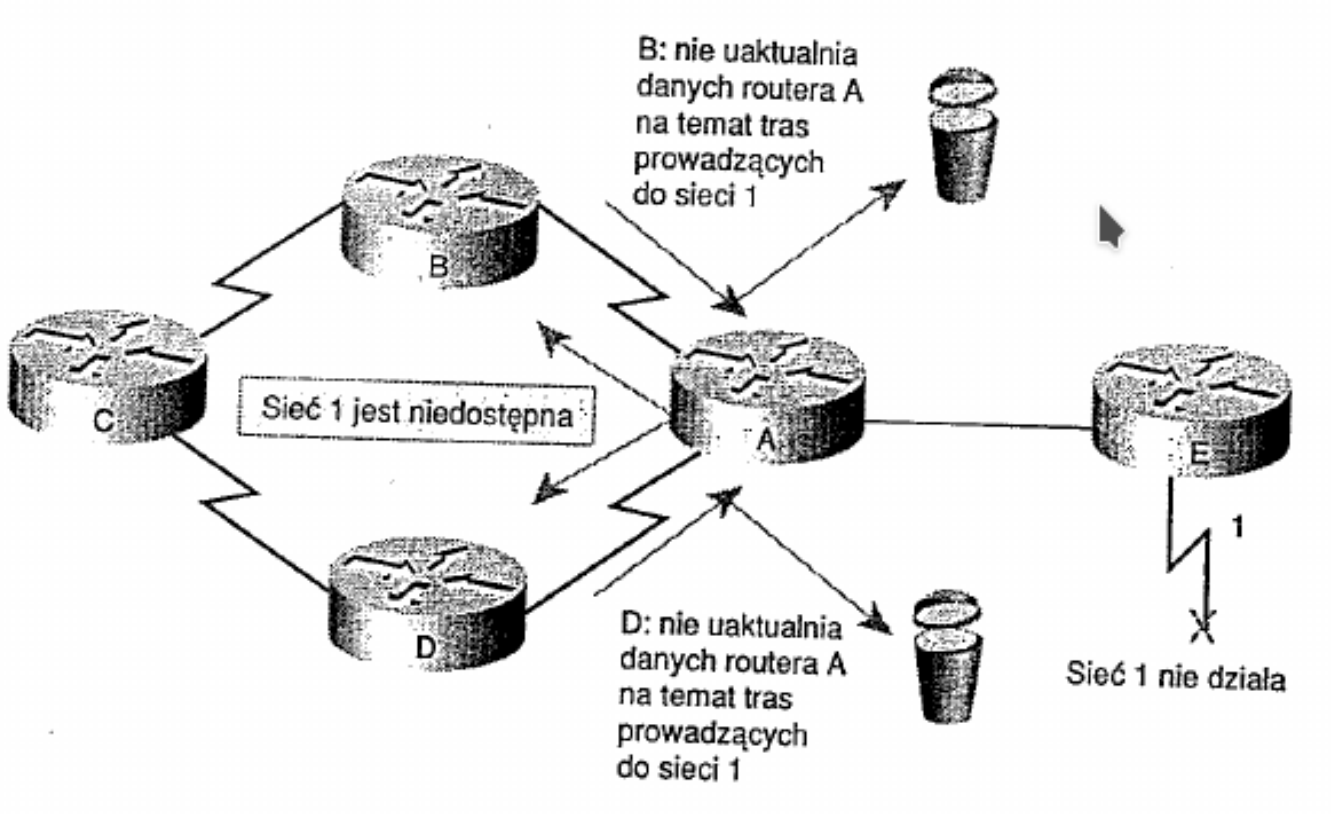
Vectors received from J's four neighbors

(b)

Routing wg wektora odległości

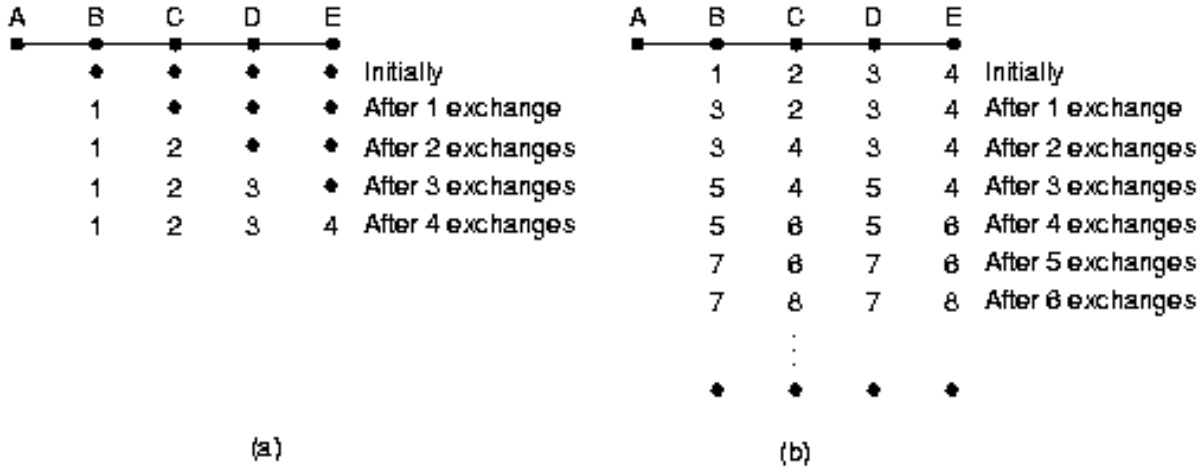


Routing wg wektora odległości



Routing wg wektora odległości

- dobre wiadomości rozchodzą się szybko
- złe wiadomości prowadzą do problemu naliczania do nieskończoności



- *RIP Request, RIP Response*
- *RIP timers*: *update (30 s)*, *invalid (90 s)*, *holddown (90)*, *flush (240 s)*
- *triggered updates*

Algorytmy stanu łącza

Algorytmy stanu łącza, zwane także algorytmami najkrótszej ścieżki (SPF, *Shortest Path First*) tworzą i uaktualniają stale bazy danych dotyczące topologii sieci.

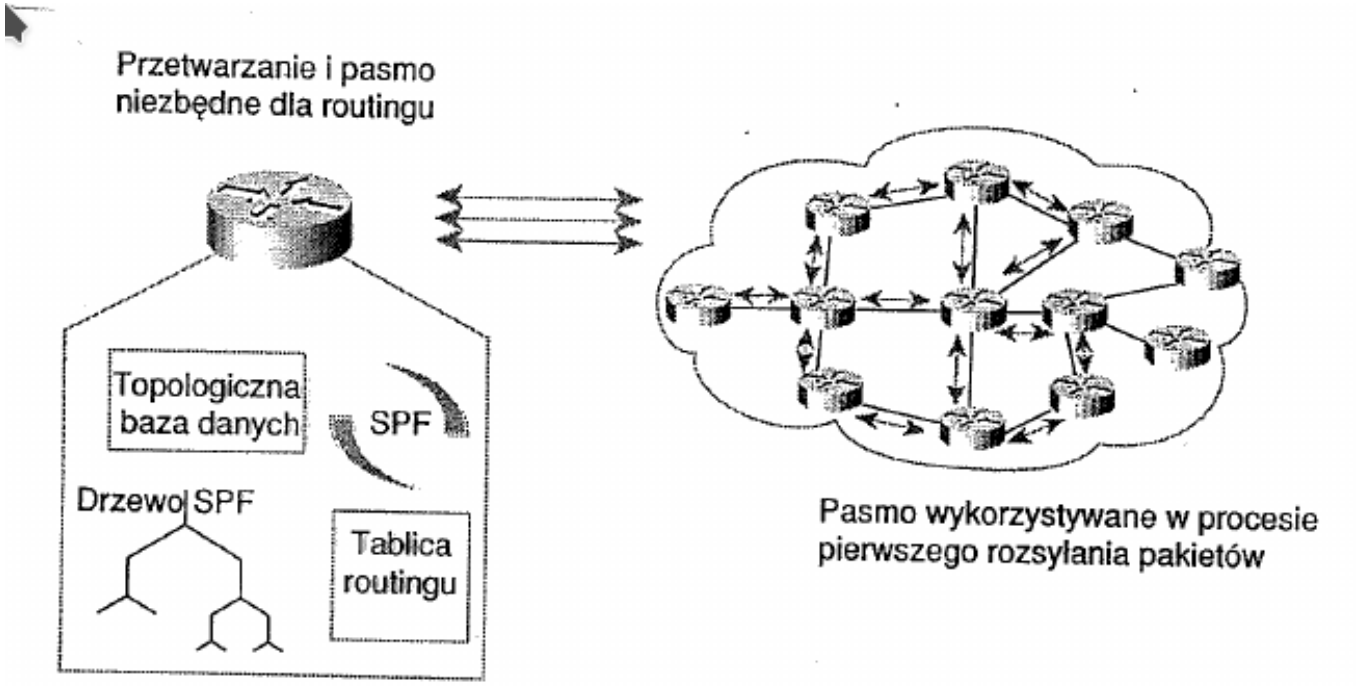
Każdy z routerów rozsyła ogłoszenia o stanie łącza (LSA, *Link State Advertisement*) do sieci, z którymi jest bezpośrednio połączony (via rozgłoszenie grupowe). Te informacje są podstawą tworzenia przez każdy z routerów drzewa najkrótszych ścieżek od danego routera do wszystkich punktów docelowych.

Drzewo SPF jest podstawą tworzenia i uaktualniania tabeli routingu.

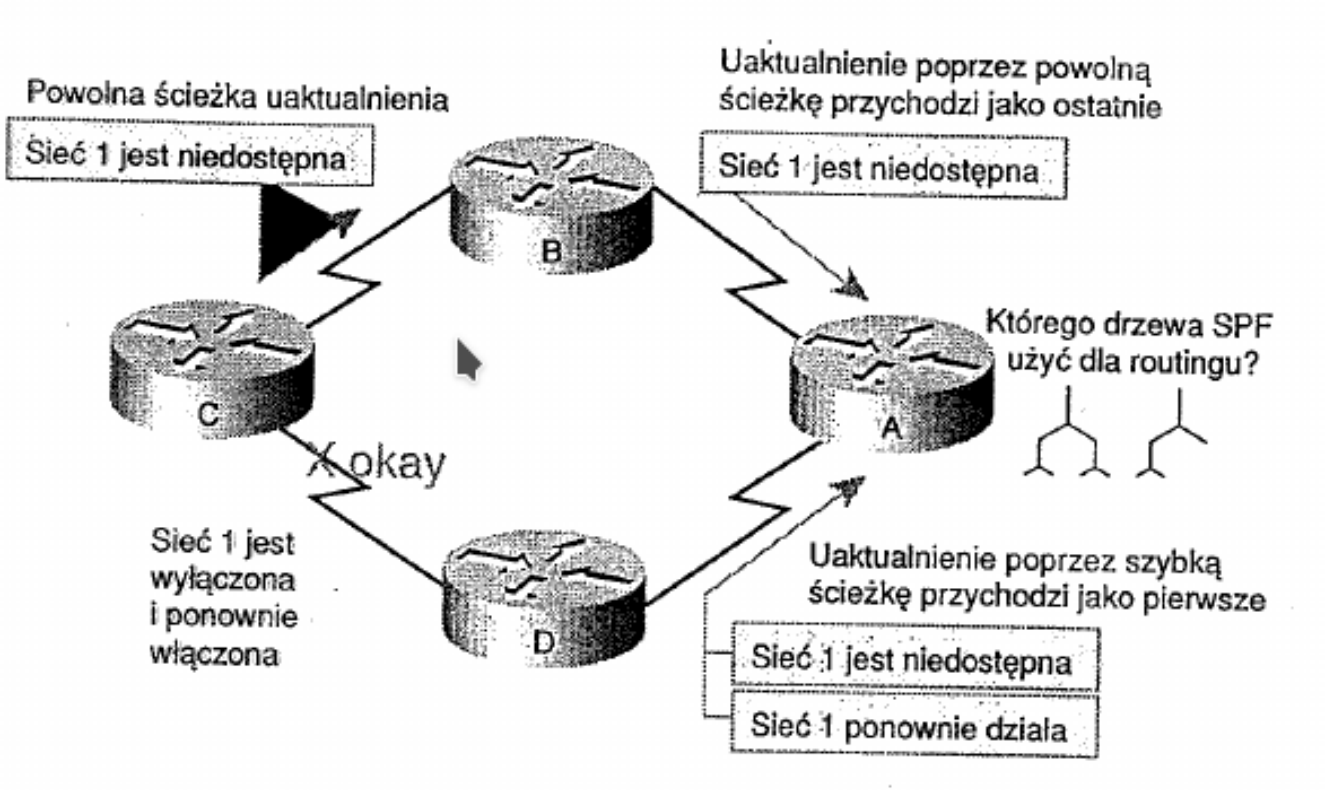
Algorytm SPF jest uruchamiany za każdym razem, kiedy router otrzymuje ogłoszenie o zmianie topologii sieci (nowy sąsiad, zmiana kosztu łącza, awaria łącza).

Przykładowe protokoły: OSPF, IS-IS, NLSP

Algorytmy stanu łącza: problemy



Algorytmy stanu łącza: problemy



Algorytmy stanu łącza: problemy

Routing stanu łącza działa poprawnie, jeśli wszystkie routery otrzymują właściwe pakiety LSA. W przeciwnym razie routery wyznaczają trasy w oparciu o różne dane o topologii sieci.

Problem niewłaściwej dystrybucji pakietów LSA wzrasta wraz z powiększaniem się sieci złożonej.

Rozwiązania:

- numery sekwencyjne LSP, znaczniki czasu, mechanizmy starzenia
- uaktualnienia wysyłane są do desygnowanego routera (grup routerów)
- budowa struktur hierarchicznych, tak aby routery w wydzielonych obszarach sieci przyjmowały uaktualnienia LSP tylko od routerów z danego obszaru

Algorytmy routingu: porównanie

Wektor odległości	Stan łącza
Topologia sieci w oparciu o dane sąsiadujących routerów	Topologia sieci w oparciu o LSA
Dodaje odległości między kolejnymi routerami	Oblicza najkrótszą ścieżkę do innych routerów
Okresowe uaktualnienia, wolna zbieżność	Uaktualnienia wywołane zmianami, szybka zbieżność
Przenosi kopie tabeli routingu do sąsiadujących routerów	Przekazuje uaktualnienia o stanie łączy do innych routerów

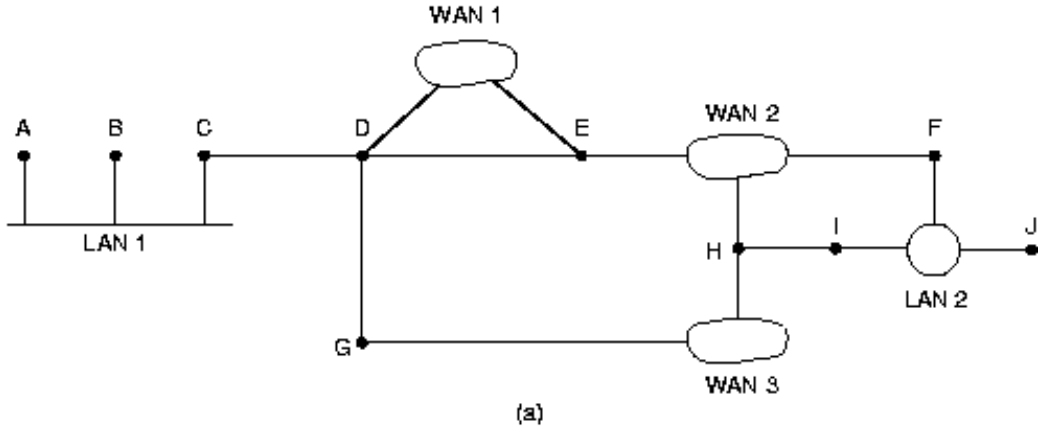
Zrównoważony protokół hybrydowy (*balanced hybrid routing*) łączy zalety routingu wektora odległości i stanu łącza. Oblicza on najkrótszą scieżkę wg wektora odległości, ale uaktualnienia bazy danych są powodowane przez zmiany topologii sieci. Przykłady: EIGRP.

OSPF: powstanie

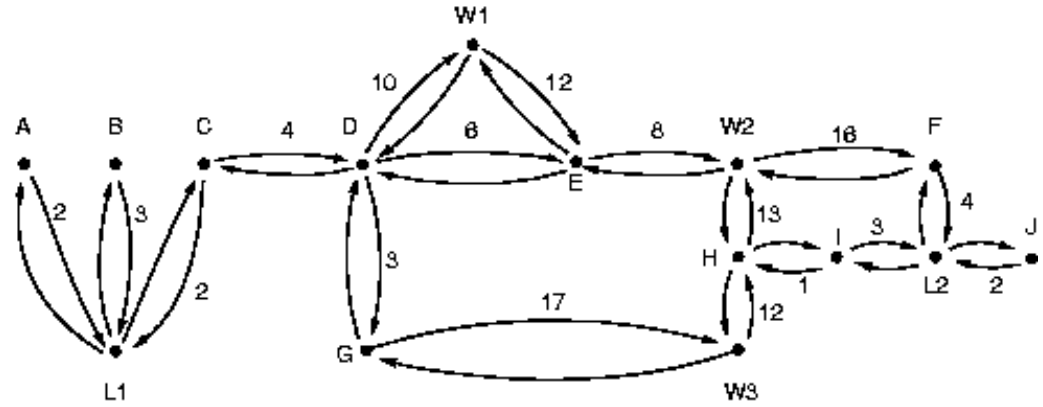
- przez 20 lat używano w Internecie oryginalnego protokołu bram wewnętrzynych (odziedziczonego po sieci ARPANET) opartego o wektor odległości (algorytm Bellmana-Forda), który nadaje się dobrze do małych sieci
- w 1988 r. IETF (*Internet Engineering Task Force*) rozpoczęła pracę nad protokołem OSPF; pierwszy dokument RFC ukazał się we wrześniu 1989 (RFC 1131); RFC 1247 (1991) opisywał wersje 2 protokołu OSPF, a dokumenty RFC 1583, 2178 i 2328 kolejne zmiany tej wersji standardu.

OSPF: własności

1. protokół otwarty
2. protokół obsługujący wiele miar odległości
3. routing dynamiczny
4. obsługa trzech typów adresacji
5. równoważenie obciążenia (routing wydajniejszy, niż oparty o przesyłanie pakietów najlepszą trasą)
6. obsługa systemów hierarchicznych (Internet stał się za duży, żeby pojedynczy router mógł znać topologię całej sieci)
7. obsługa tuneli
8. protokół z zabezpieczeniami przed niewłaściwym wykorzystaniem (uwierzytelnianie)


WAN 1
A
B
C
D
E
WAN 2
F
LAN 1
H
I
J
LAN 2
G
WAN 3

(a)


W1
10
12
A
B
C
4
D
6
8
W2
16
F
E
2
3
13
4
3
J
H
I
3
2
1
L2
2
17
12
G
L1
W3

(b)

OSPF: własności

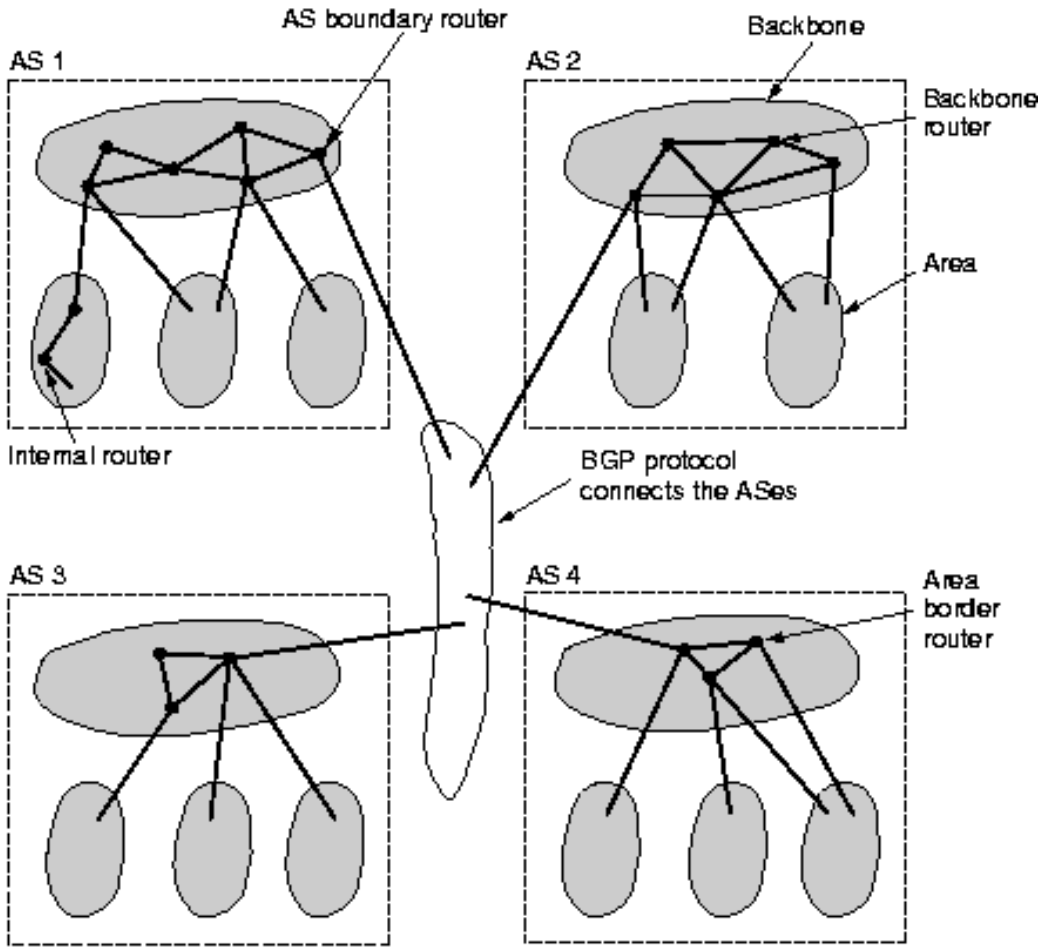
OSPF obsługuje następujące typy sieci i połączeń

1. linie dwupunktowe pomiędzy dwoma routerami
2. sieci wielodostępne z rozgłoszeniami (np. sieci lokalne)
3. sieci wielodostępne bez rozgłoszeń (większość sieci rozległych z komutacją pakietów)

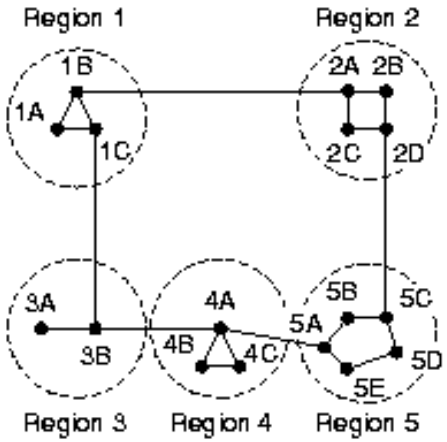
OSPF reprezentuje rzeczywistą sieć w postaci grafu skierowanego i oblicza najkrótsze ścieżki od danego węzła do wszystkich pozostałych.

OSPF pozwala na podział systemu autonomicznego (AS, *Autonomous System*) na ponumerowane obszary (sieć lub zbiór spójnych sieci). Każdy AS ma obszar szkieletu (*backbone*), z którym są połączone wszystkie pozostałe obszary.

W obrębie obszaru każdy router ma tę samą bazę stanów łączy i używa tego samego algorytmu najkrótszej ścieżki.


AS boundary router
Backbone
AS 1
AS 2
Backbone router
Area
Internal router
BGP protocol connects the ASes
AS 3
AS 4
Area border router

Routing hierarchiczny



(a)

Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

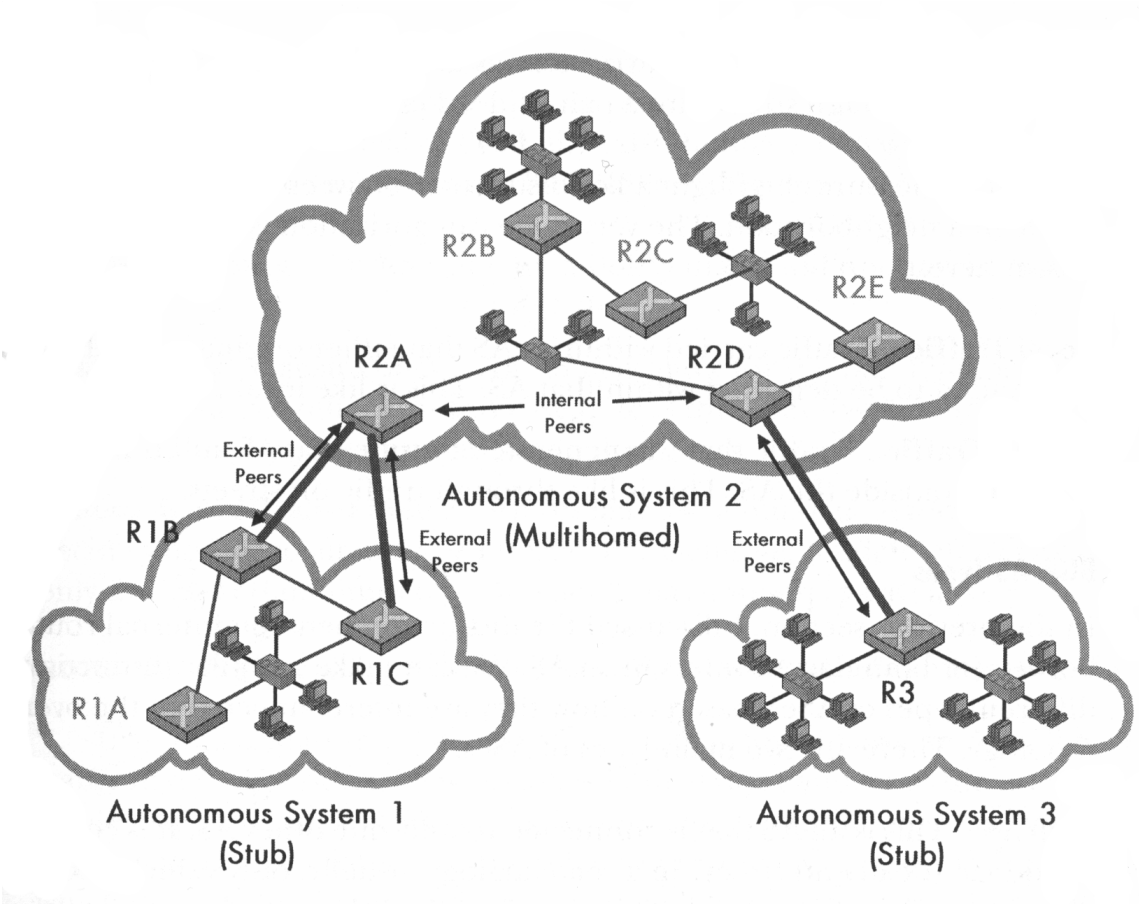
Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Routing hierarchiczny: BGP

- Wewnątrz systemów autonomicznych zaleca się stosowanie protokołu routingu OSPF. Pomiędzy takimi systemami protokołem routingu jest protokół bram granicznych (BGP).
- Zadaniem OSPF jest optymalne przenoszenie pakietów między węzłami systemu autonomicznego.
- Zadaniem BGP jest zapewnienie dostępu do innych AS-ów oraz regulowanie przekazywania pakietów pomiędzy zagranicznymi AS-mi.
- BGP został zaprojektowany tak, aby w ruchu między AS-mi można było egzekwować różne zasady (polityki) routingu.

BGP: przykładowa topologia[91]



[91] C.M.Kozierok, TCP/IP Guide

Routing hierarchiczny: BGP

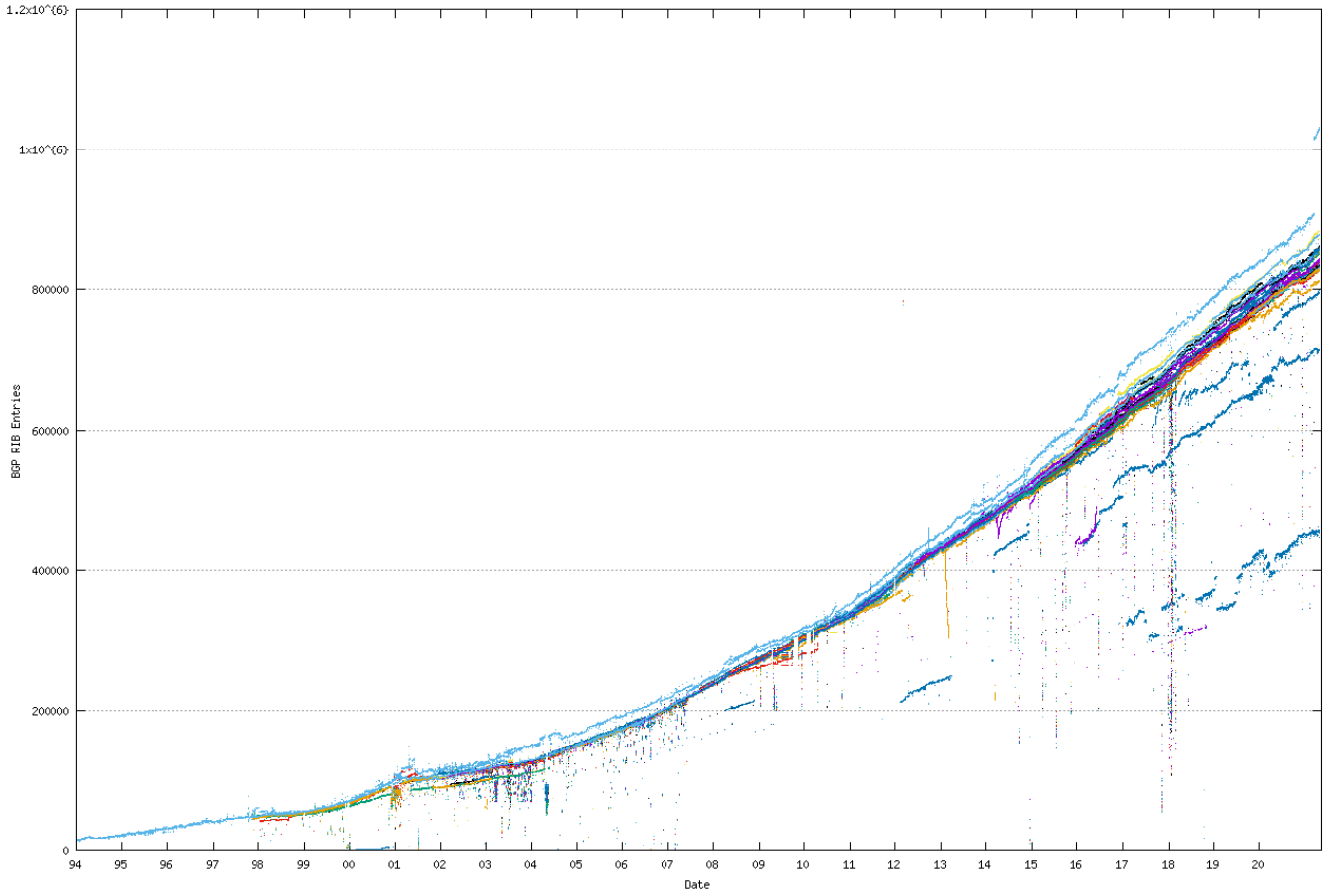
Z punktu widzenia BGP sieci dzieli się na

- sieci końcowe (*stub networks*)
- sieci wielopołączeniowe (*multiconnected networks*)
- sieci tranzytowe

Routery BGP

- komunikują się między sobą tworząc połączenia TCP
- wykorzystują protokół wektora odległości gromadząc i przekazując innym routerom pełną informację o używanych trasach (a nie koszcie tras)
- najlepsza trasa jest wyznaczana przez administratora

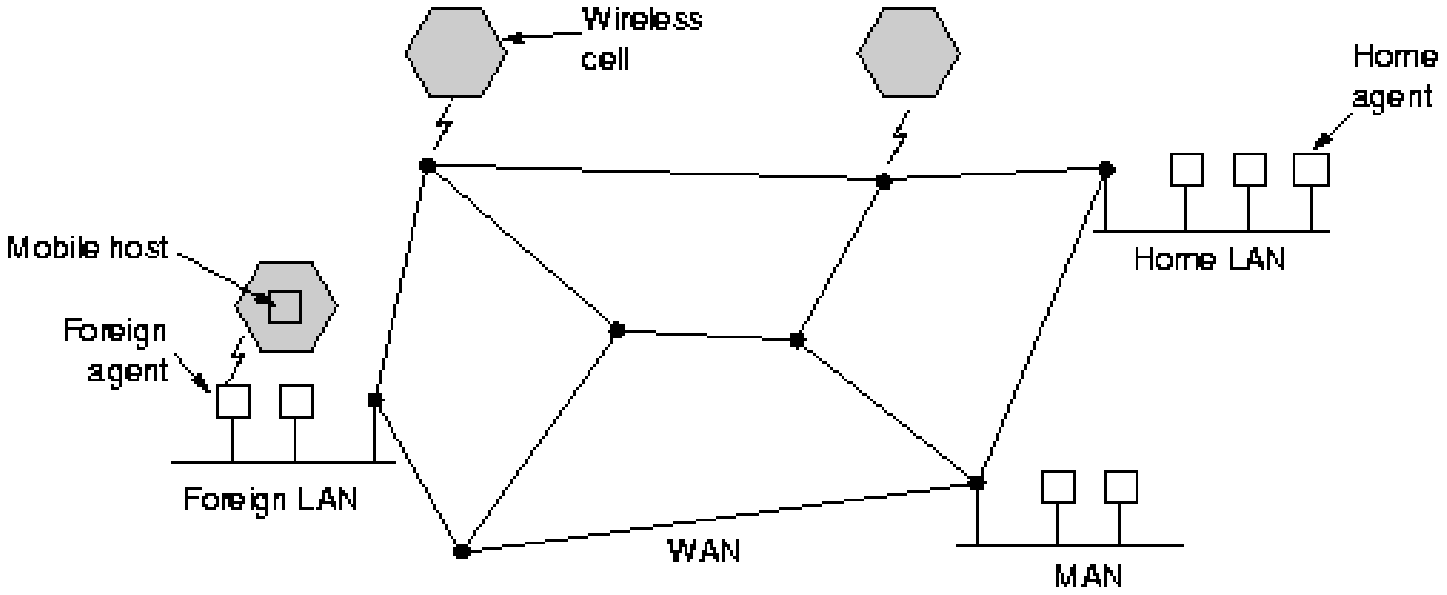
Zmiana wielkości tablic BGP[92]



[92] http://bgp.potaroo.net/

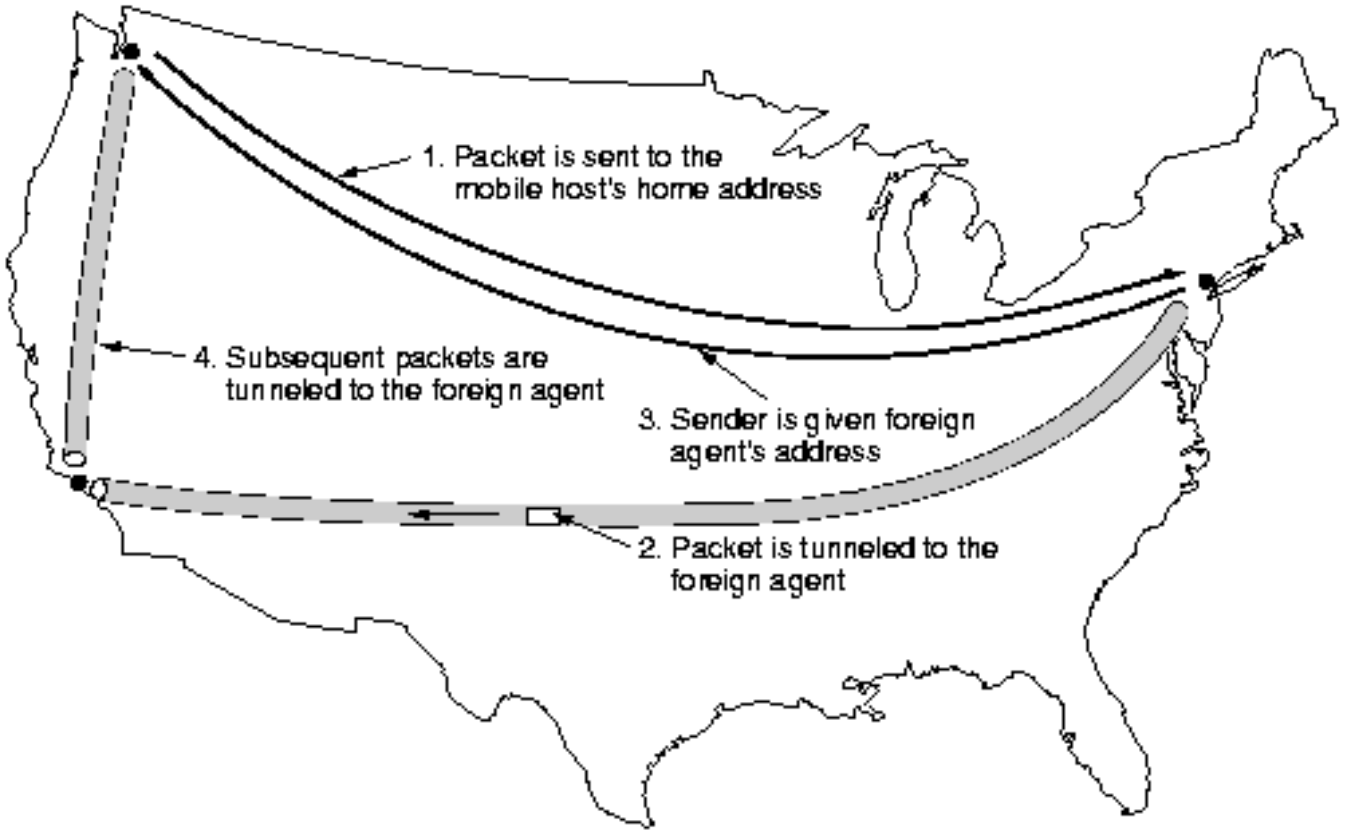
Routing dla hostów mobilnych

Problem: routery stacjonarne, host ruchomy



Routing dla hostów mobilnych

Host mobilny z sieci NY znajduje się w LA. Jak wygląda jego komunikacja z hostem z Seattle?



Routing w sieciach ad hoc

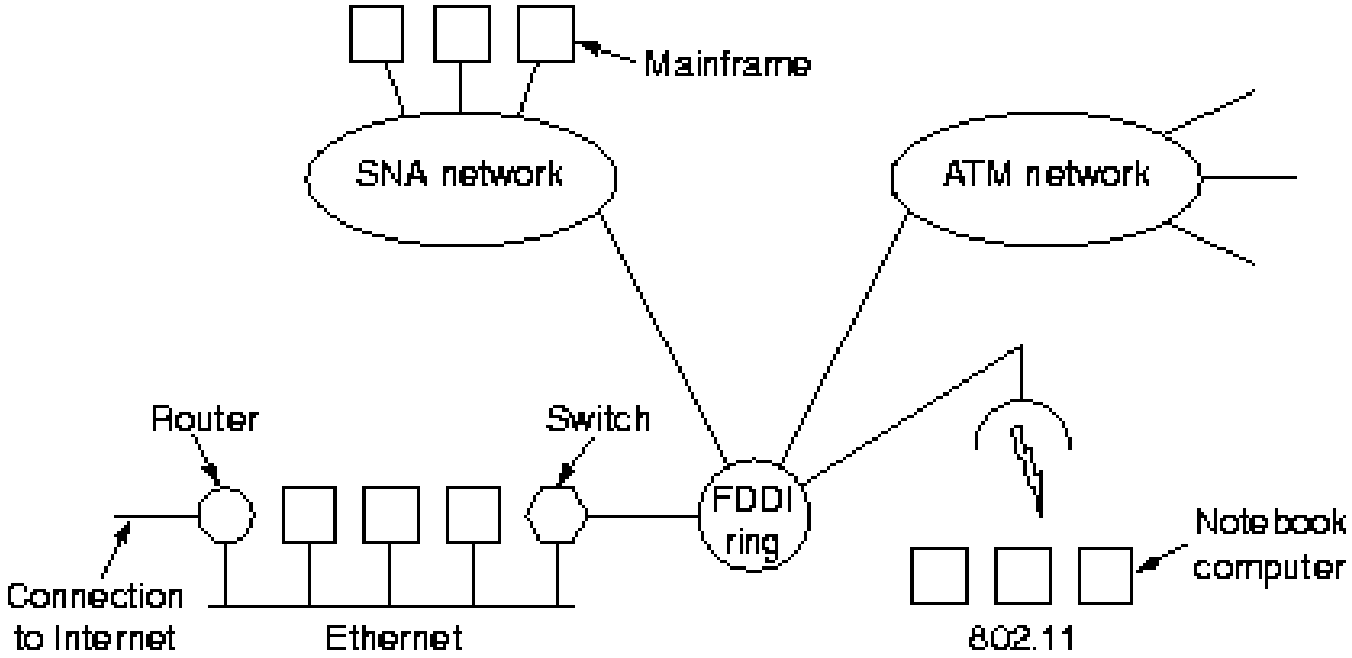
Problem: routery/hosty (zwykle ten sam komputer) ruchome

- pojazdy wojskowe na polu bitwy bez istniejącej infrastruktury
- flota na morzu
- ekipy ratunkowe w miejscu dotkniętym kataklizmem
- zgromadzenie z notebookami w obszarze bez 802.11

Sieci węzłów, które znalazły się koło siebie określa się jako **sieci ad hoc** lub MANET (*Mobile Ad hoc NETworks*). Jednym z algorytmów routingu stosowanych w takich sieciach jest AODV (*Ad hoc On-demand Distance Vector*), który pozwala na ustalanie trasy dopiero, kiedy pojawia się żądanie wysłania pakietu do jakiegoś celu.

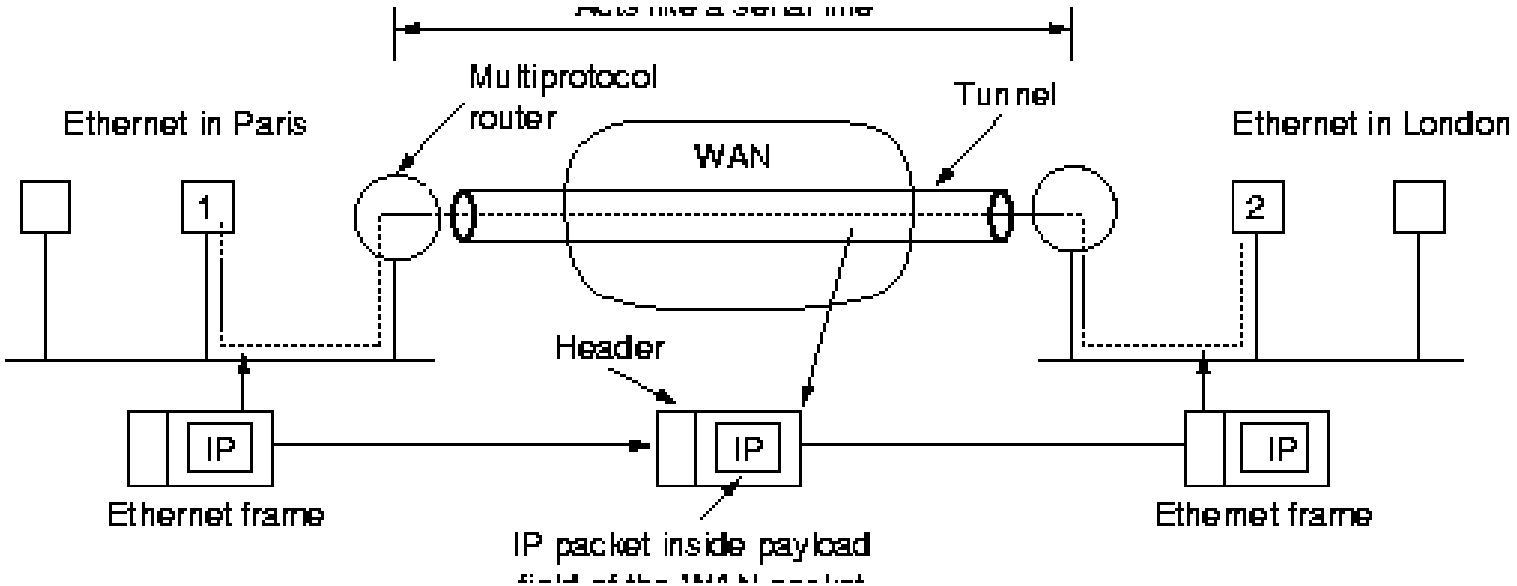
Sieci złożone

Istnieje wiele typów sieci lokalnych, miejskich i rozległych, w których w danej warstwie sieciowej używane są różne protokoły.



Łączenie ich tworzy sieć złożoną, czyli internet pisany z małej litery. Budowa internetu jest możliwa dzięki routerom wieloprotokołowym.

Sieci złożone: tunelowanie



Sieci skalowalne

Własności rozległej sieci skalowalnej:

1. Pewność i dostępność

   Sieć jest stale dostępna (24x7), awarie niewidoczne dla końcowych użytkowników, konieczność utrzymywania nadmiarowych połączeń. *Sieć silna* szybko radzi sobie z awariami.

   Funkcje IOS Cisco zwiększające niezawodność i dostępność:

   - skalowalne protokoły routingu (OSPF, EIGRP)
   - ścieżki zapasowe
   - równoważenie obciążenia
   - tunele protokołów
   - kopia zapasowa połączeń

Sieci skalowalne

2. Zdolność szybkiej reakcji (QoS dla aplikacji i protokołów)

   Kolejkowanie:

   - FIFO
   - priorytetowe (4 kolejki)
   - niestandardowe (rezerwowanie minimalnej ilości pasma dla każdego rodzaju ruchu; 16 kolejek)
   - równomierne (dynamiczna strategia kolejkowania stosowana domyślnie przez routery Cisco dla wszystkich interfejsów E1 i wolniejszych)

Sieci skalowalne

3. Wydajność (wykorzystanie pasma, redukcja zbędnego ruchu):
   - listy sterowania dostępem (ACL, *Access Control List*)
   - routing migawkowy (z RIP, IGRP)
   - kompresja
   - routing połączeń na żądanie (DDR, *Dial-on-Demand Routing*)
   - podsumowywanie tras
   - narastające uaktualnienia (np. OSPF i EIGRP wysyłają informacje tylko o trasach, które uległy zmianie)

Sieci skalowalne

4. Łatwość przystosowania (różne protokoły, aplikacje, technologie)

   EIGRP jest przykładem protokołu dobrze przystosowującego się (obsługuje informacje o routingu dla protokołów IP, IPX i AppleTalk).

   System IOS Cisco oferuje *redystrybucję tras* (przekazywania danych zgromadzonych w tablicach jednego protokołu routingu do innego).

5. Dostępność i bezpieczeństwo

   - możliwość łączenia się przy wykorzystaniu różnych technologii i typów połączeń (wdzwaniane, stałe, komutowane).
   - protokoły uwierzytelniania takie jak PAP lub CHAP (*Password Authentication Protocol*, *Challenge Handshake Authentication Protocol*)

Słownik skrótów

AH *Authentication Header* nagłowek uwierzytelniania

API *Application Programming Interface* interfejs programów użytkowych

ARP *Address Resolution Protocol* protokół odwzorowywania adresów

ASCII *American Standard Code for Information Interchange* standardowy amerykański kod wymiany informacji

ASIC *Application Specific Integrated Circuit* układ scalony właściwy aplikacji

AS *Autonomous System* system autonomiczny

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 *Basic Rate Access* dostęp w trybie podstawowym

BPDU *Bridge Protocol Data Unit* jednostka danych protokołu mostu

CIR *Committed Information Rate* przepustowość (średnia) gwarantowana umową

CBR *Committed Burst Rate* przepustowość chwilowa gwarantowana umową

CHAP *Challenge Handshake Authentication Protocol* protokół wymiany wyzwania uwierzytelniającego (protokół uwierzytelniania przez uzgodnienie)

CIDR *Classless InterDomain Routing* bezklasowy routing międzydomenowy

CIFS *Common Internet File System* powszechny internetowy system plików

CIR *Committed Information Rate* zagwarantowany poziom transmisji

CoS *Class Of Service* klasa usługi

CPE *Customer-premises Equipment* zakończenie sieci telekomunikacyjnej znajdujące się u klienta, terminal

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* protokół dostarczania datagramów

DES *Data Encription Standard* standard szyfrowania danych

DFS *Dynamic Frequency Selection* dynamiczny wybór częstotliwości

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 Signal 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

ESP *Encapsulating Security Payload* enkapsulowanie ładunku bezpieczeństwa

FDDI *Fiber Distributed Data Interface* światłowodowy interfejs danych rozproszonych

FCS *Frame Check Sequence* sekwencja kontrolna ramki

FECN *Forward Explicit Congestion Notification* jawne powiadomienie o zatorze wysyłane w kierunku odbiorcy

FR *Frame Relay* przekazywanie ramek

FTP *File Transfer Protocol* protokół przesyłania plików

GARP *Generic Attribute Registration Protocol*

Gb *gigabit* gigabit

GB *gigabyte* gigabajt

GMRP *GARP Multicast Registration Protocol*

GNS *Get Nearest Server* uzyskaj dostęp do najbliższego serwera

GRE *Generic Routing Encapsulation* ogólna enkapsulacja dla routingu

GVRP *GARP VLAN Registration Protocol*

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 Control Message 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* protokół routingu wewnętrznej bramy

IKE *Internet Key Exchange* internetowa wymiana klucza

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

MPLS *Multi-Protocol Label Switching* wieloprotokołowe przełączanie etykiet

NAP *Network Access Point* punkt dostępu do sieci

NAT *Network Address Translation* translacja adresów sieciowych

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* (model odniesienia) łączenia systemów otwartych

OSPF *Open Shortest Path First* otwarty protokół najkrótszej ścieżki

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 potwierdzenie 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)

PSE *Packet Switching Exchange* centrala komutacji pakietów

PVC *Permanent Virtual Circuit* stałe łącze wirtualne

QoS *Quality Of Service* jakość usługi

RARP *Reverse Address Resolution Protocol* protokół odwrotnego odwzorowywania adresów

RIP *Routing Information Protocol* protokół informacji routingu

RMON *Remote Monitoring* zdalny nadzór

RTP *Real-time Transport Protocol* protokól transportowy czasu rzeczywistego

SAP *Service Advertisment Protocol* protokół rozgłaszania usługi

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

SIP *Session Initialization Protocol* protokół inicjacji sesji

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

SOAP *Simple Object Access Protocol*

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 Telekomunikacyjnego

TORMAN *TORun Municipal Area Network* toruńska miejska sieć komputerowa

TPC *Transmission Power Control* sterowanie mocą sygnału

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