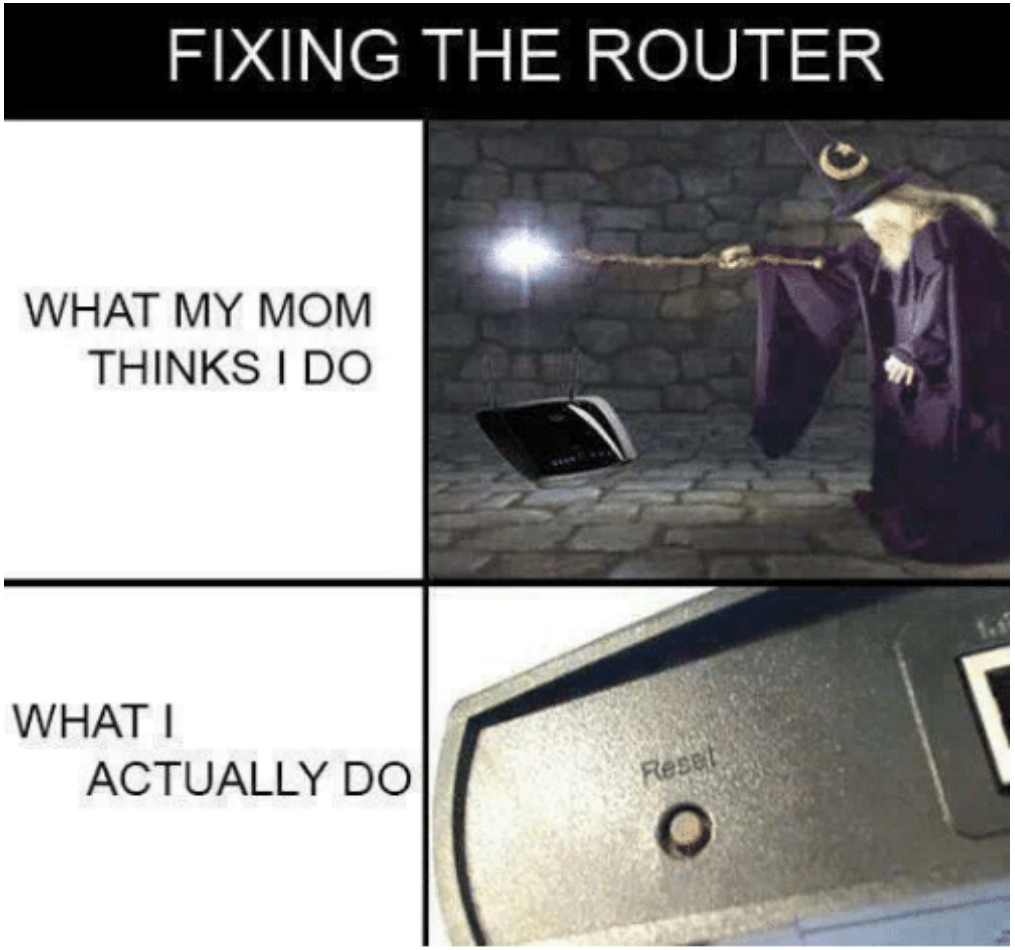
Sieci komputerowe

Wykład podsumowujący
27.05.2020

dr inż. Łukasz Graczykowski
lukasz.graczykowski@pw.edu.pl

Semestr letni 2019/2020

Po co nam to wszystko?

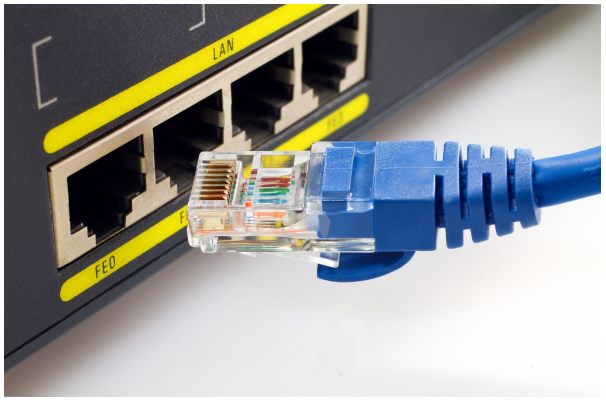


źródło: https://me.me/i/fixing-the-router-what-my-mom-thinks-i-do-what-3800420

Co to jest **sieć komputerowa**?

- **Sieć komputerowa** to:
  - zespół **urządzeń transmisyjnych** (np. komputer z kartą sieciową, router, switch, koncentrator, itp.)
  - które są połączone ze sobą za pomocą **medium transmisyjnego** (np. kabel, światłowód, technologie bezprzewodowe – podczerwień, radiowe, itp.)
  - pracujących pod kontrolą **zaawansowanego oprogramowania**
  - w celu przesyłania między sobą danych (informacji) za pomocą **protokołu transimisyjnego** (np. TCP/IP)

źródło: simply-ip.net



źródło: digitaltrends.com

Krótka historia Internetu

Vague but exciting ...

CERN DD/OC

Tim Berners-Lee, CERN/DD

Information Management: A Proposal

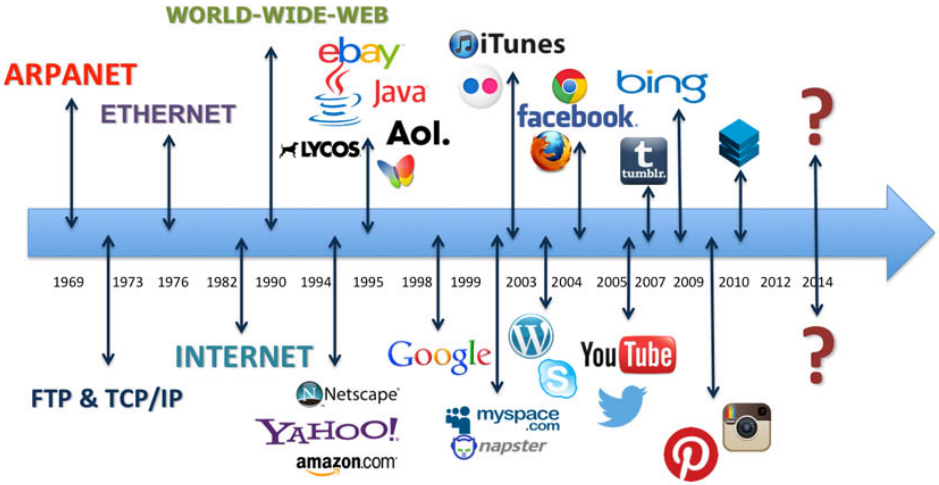
March 1989

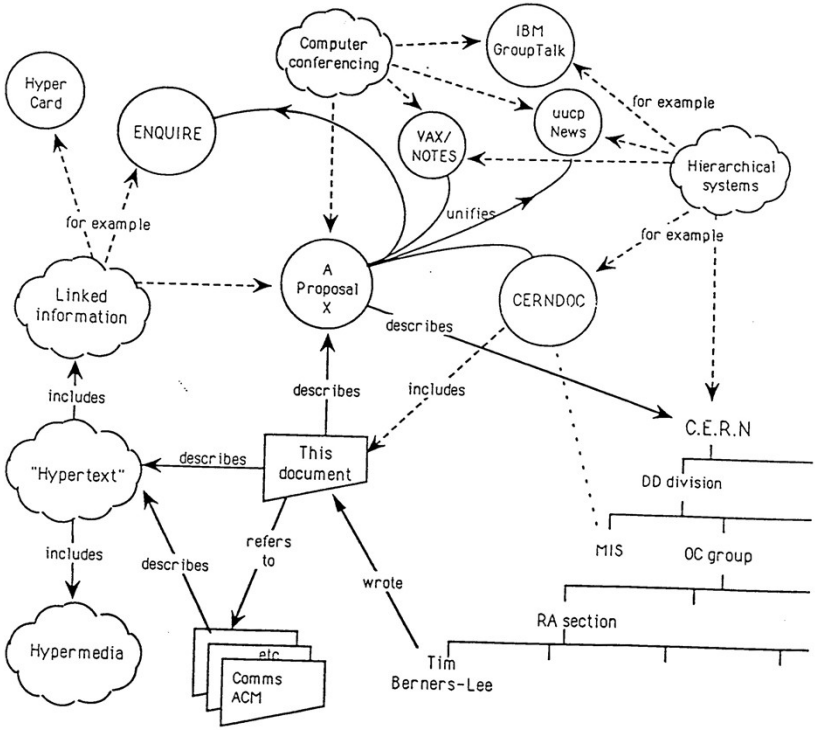
Information Management: A Proposal

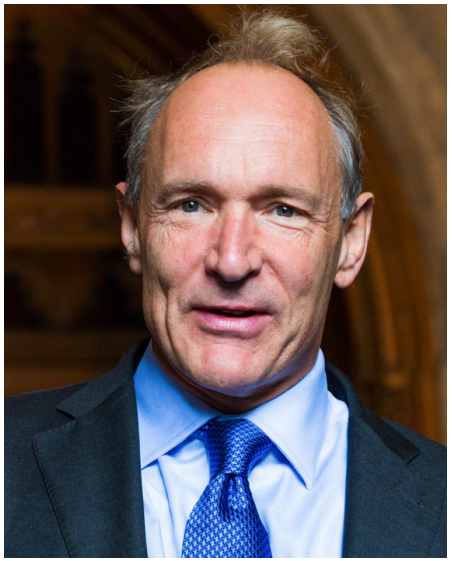
Abstract

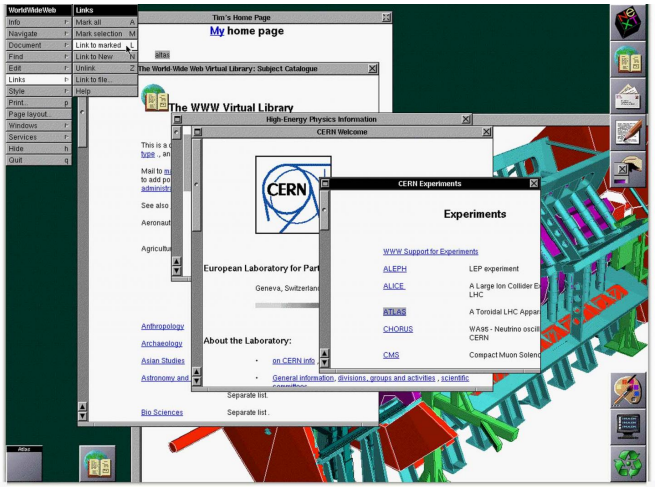
This proposal concerns the management of general information about accelerators and experiments at CERN. It discusses the problems of loss of information about complex evolving systems and derives a solution based on a distributed hypertext sytstem.

Keywords: Hypertext, Computer conferencing, Document retrieval, Information management, Project control



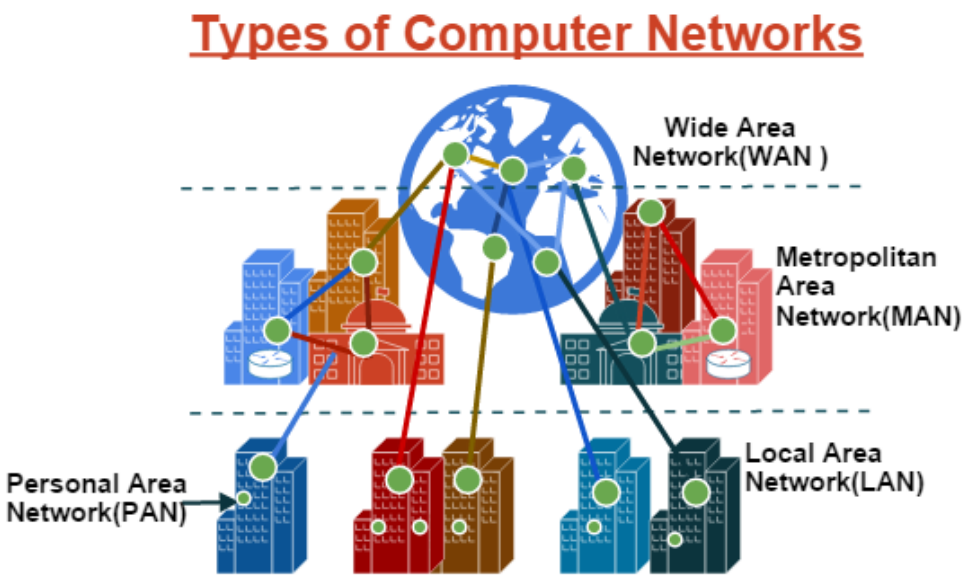






Podział sieci komputerowych

Podział sieci komputerowych



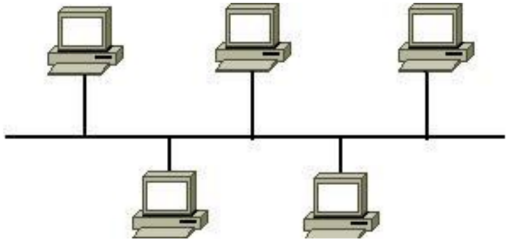
LAN (PAN) > MAN > WAN

Internet to też sieć WAN, tylko dostępna publicznie i zdecentralizowana

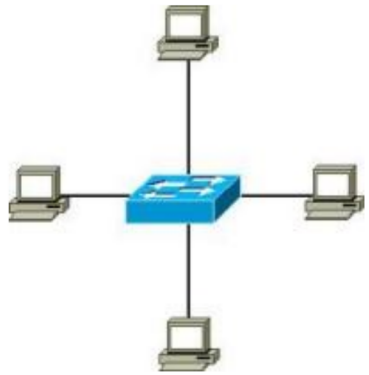
Intranet to sieć podobna do Internetu (te same usługi), tylko ograniczona do np. jednej organizacji, czy kraju (Korea Płn.)

Topologia sieci

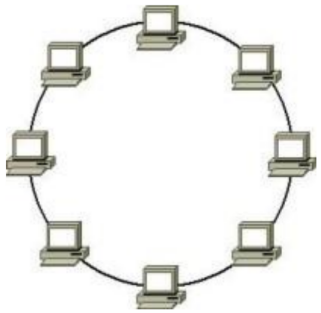
magistrala



gwiazda

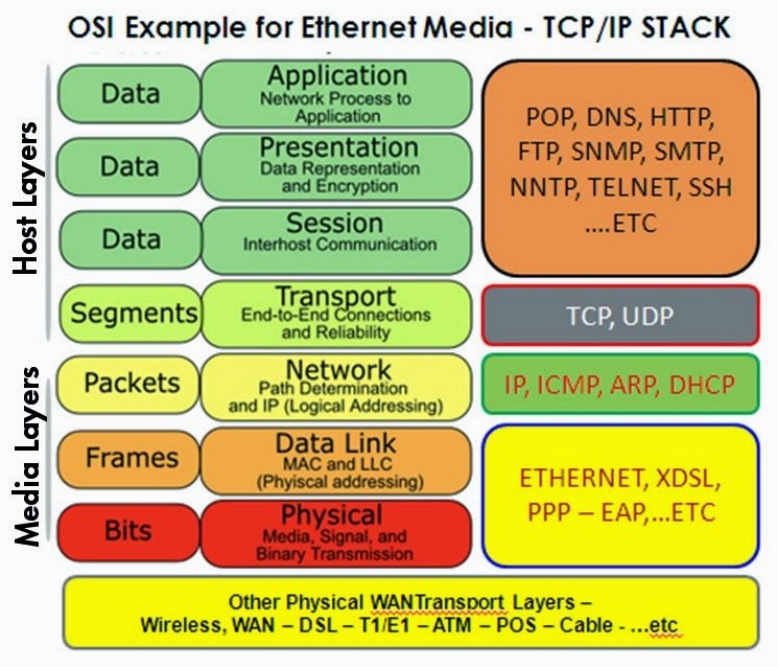


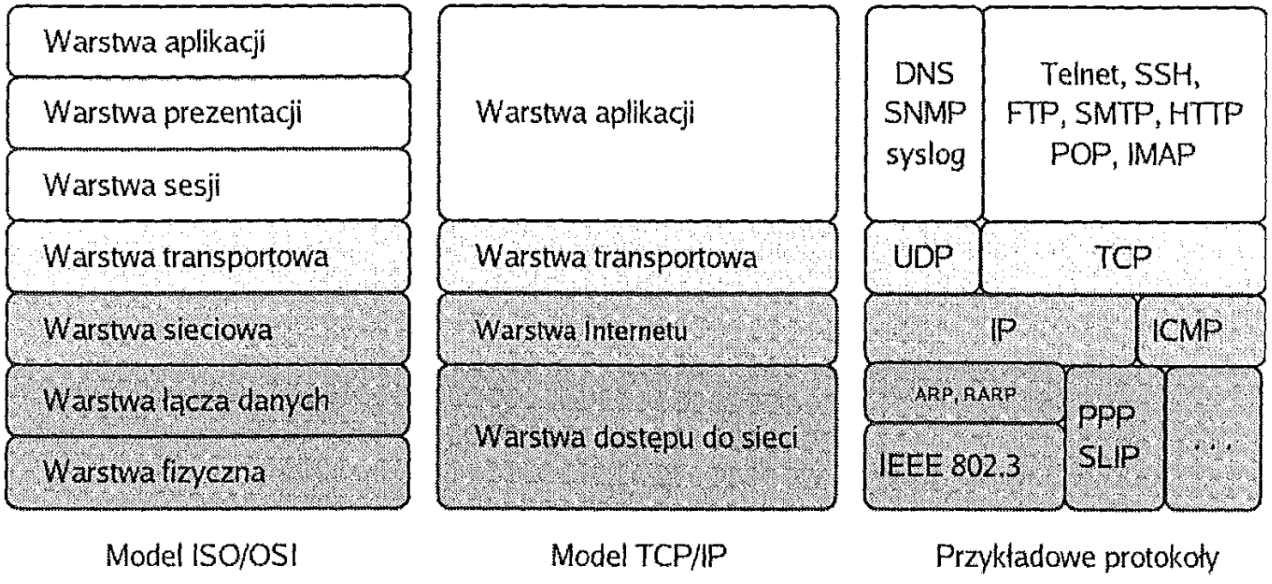
pierścień



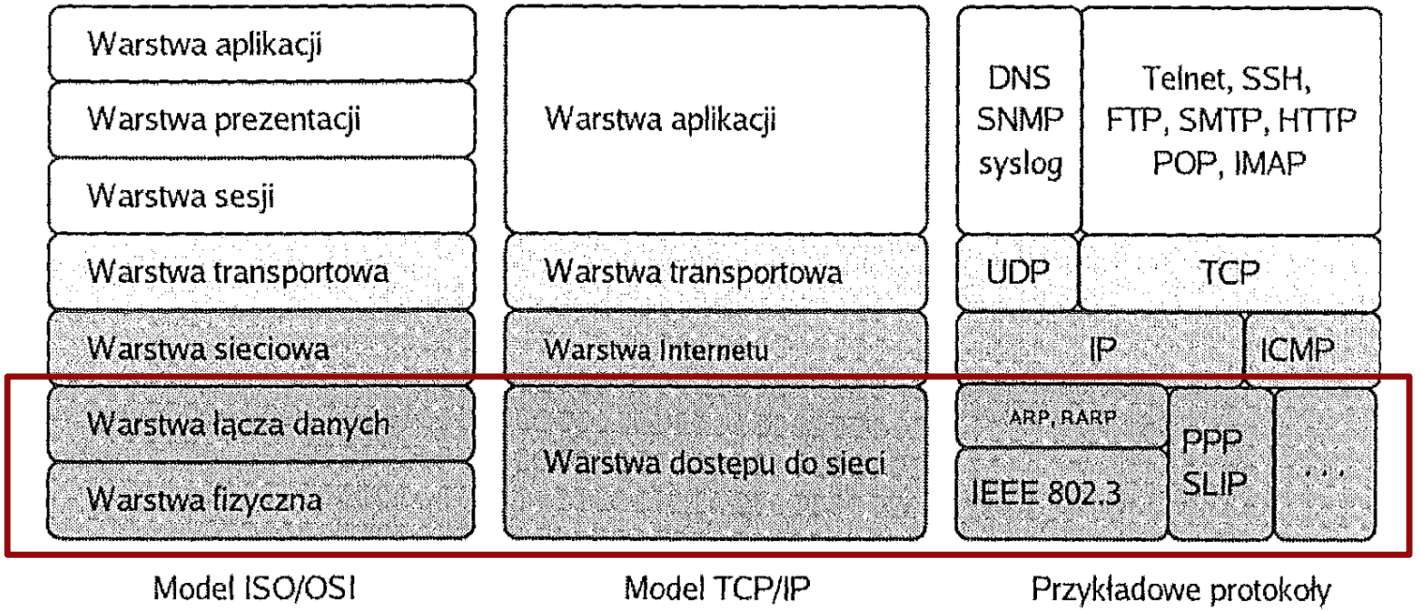
Podział sieci komputerowych

- W 1977 roku ISO (International Standard Organization) opracowało model “łączenia systemów otwartych” (Open System Interconnection – OSI)
- **Model ISO/OSI** dzieli proces transmisji danych na 7 etapów, zwanych ***warstwami***
- **W modelu TCP/IP wyróżniamy 4 warstwy** (poprzez łączenie funkcjonalności pozostałych)





Warstwa dostępu do sieci



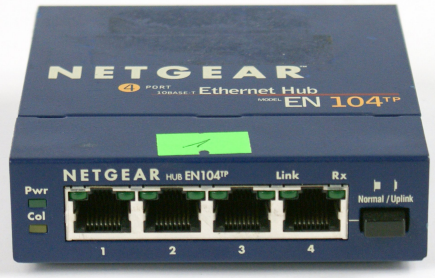
źródło: Helion

Urządzenia warstwy fizycznej

- **Wzmacniak** (repeater) – wzmacnia sygnał, służy do zwiększania sygnału
- **Koncentrator** (hub) – urządzenie pozwalające na przyłączenie wielu urządzeń sieciowych w sieci o topologii gwiazdy, przesyła sygnały z jednego portu na wszystkie inne
- **Karta sieciowa** (network inteface controller – NIC) – zapewnia komunikację komputera z siecią poprzez odbiór sygnałów elektrycznych, świetlnych, radiowych (fal elektromagnetycznych) za pomocą pulsacji (sygnał cyfrowy), urządzenie warstwy 1 i 2 (łącza danych), zapewnia adresowanie MAC (adres łącza w standardzie Ethernet)
- **Modem** (modulator-demodulator) – zapewnia komunikację poprzez kanały częstotliwości radiowych (sygnał analogowy) pomiędzy odbiorcą a siecią (moduluje sygnał do transmisji w sieci i demoduluje sygnał odbierany), urządzenie wartstwy 1 i 2 (łącza danych), jeśli zapewnia adresację IP, także wyższych warstw

źródło: t4ttutorials.com

źródło: allegro.pl



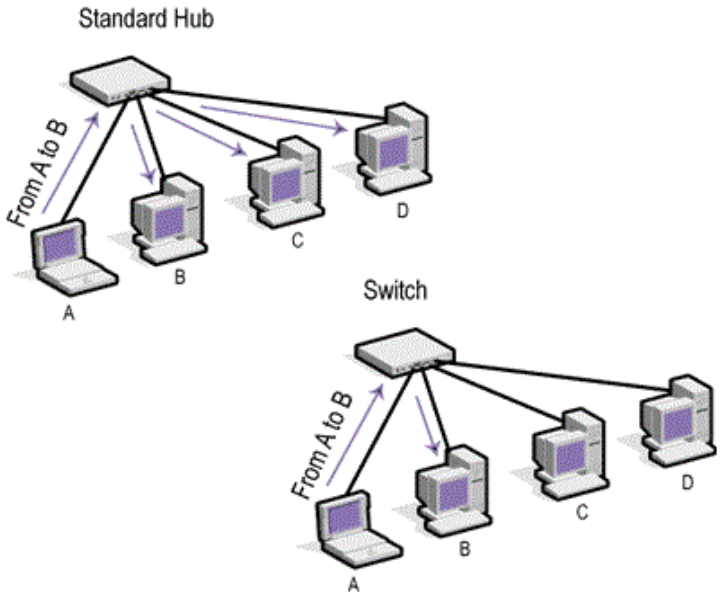
źródło: reichelt.com

źródło: buyapprovedmodems.com

Hub vs switch vs router

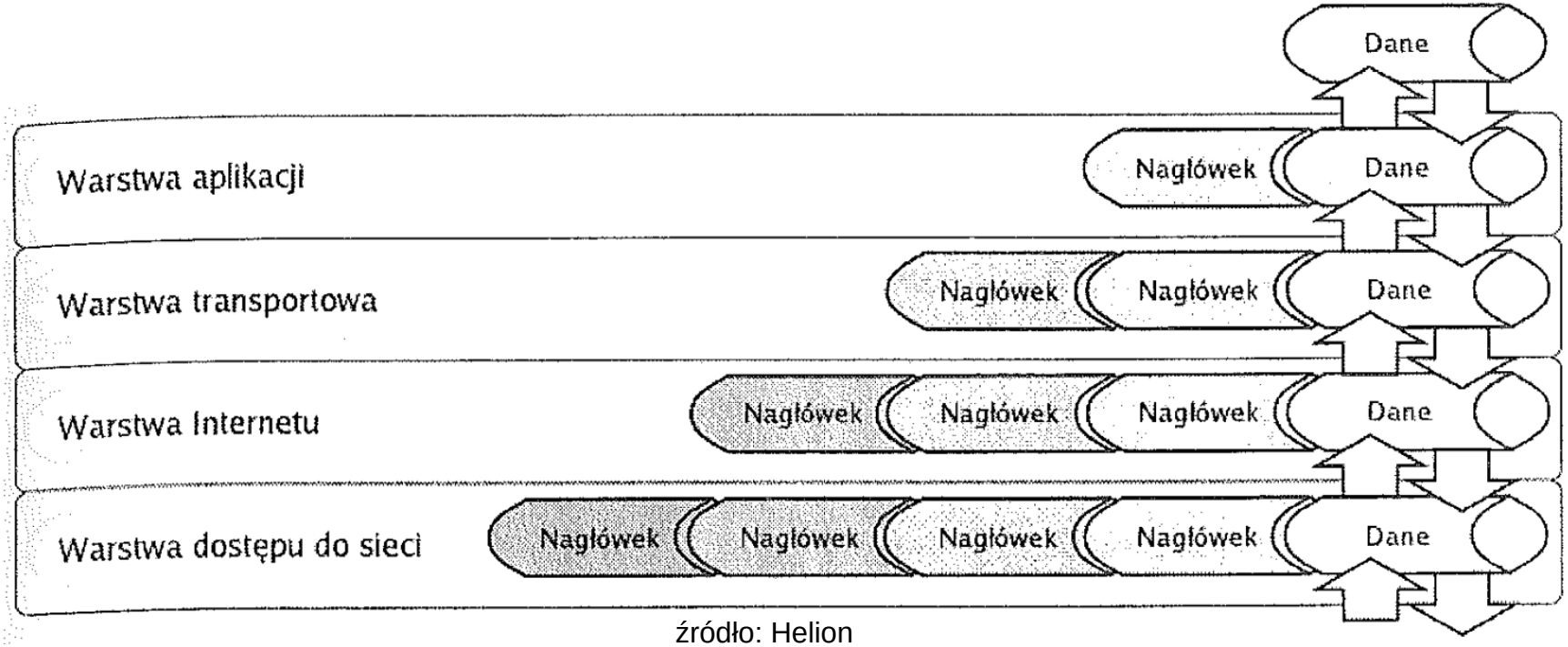
S.No	HUB	SWITCH	ROUTER
1.	Works in Half Duplex mode	Full Duplex	Full Duplex
2.	Sends data in form of bits	Sends data in form of frames	Sends data in form of packets
3.	Broadcast Device	Multicast device	Routing Device
4.	Works in physical layer of OSI model	Works in Data link / Network layer of OSI model	Works in Network layer of OSI model
5.	Used to connect devices to the same network.	Used to connect devices to the network.	Used to connect two networks.
6.	Does not store any MAC address of a node in the network.	Stores MAC address and IP address of nodes in the network.	Stores MAC address and IP address of nodes in the network.
7.	Types are :- Active hub, Passive hub and Intelligent hub.	Types are Layer 2 and layer 3 switch.	Types are Broadband router, Wireless router, Edge router, core router.
8.			

- Hub przekazuje sygnał z jednego portu do wszystkich pozostałych (broadcast) – działa w warstwie fizycznej
- Switch przekazuje sygnał do wybranego adresata na podstawie MAC adresu – działa w warstwie łącza danych
- Router działa w warstwie sieciowej (adresy IP)



Enkapsulacja danych

- **Enkapsulacja** danych polega na dołączaniu przez kolejne warstwy swoich nagłówków (np. numer portu czy adres IP)
- W odbiorze, każda warstwa rozpoznaje swój **nagłówek**, usuwa go przekazując dane wyżej, aż do konkretnej aplikacji, która prezentuje dane użytkownikowi

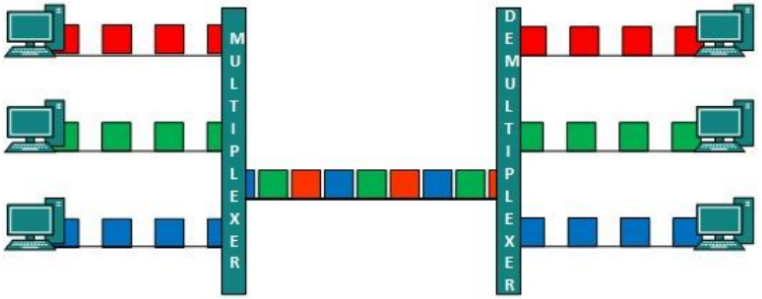


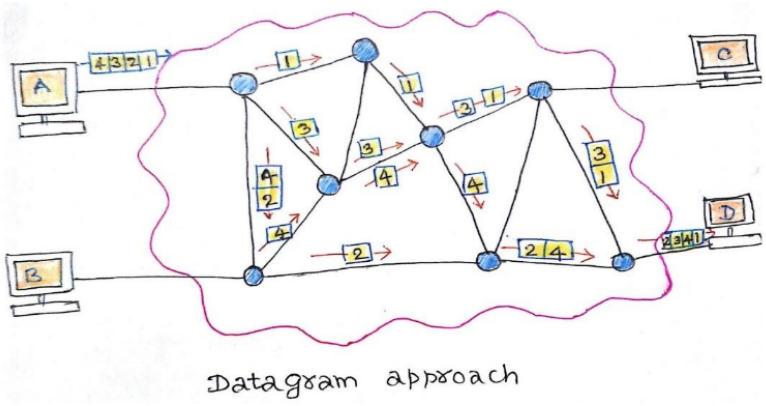
źródło: Helion

Ethernet (IEEE 802.3)

- **Ethernet** – zbiór technologii sieciowych wartwy pierwszej (fizycznej) oraz drugiej (łącza danych) używanych w sieciach komputerowych
- Zaproponowany w 1978 roku w Palo Alto Research Center (Xerox) – pierwsza sieć LAN stosująca kabel koncentryczny
- Obejmuje:
  - typy ***mediów transmisyjnych*** (standardy kabli sieciowych czy światłowodów)
  - standardy ***urządzeń sieciowych*** takich jak karty sieciowe czy hub'y
  - w warstwie drugiej wprawdza ***ramki*** (frames) jako podstawowe kontenery danych
  - wprowadza również ***adresację MAC*** (media access control) jako unikalny adres danej karty sieciowej
  - przesył danych poprzez ***komutację pakietów***
- Standardy bezprzewodowe (np. WiFi) **nie są** częścią ethernetu (aczkolwiek w sporej części bazują na ethernecie)

Preamble	SFD	Destination MAC Address	Source MAC Address	EtherType	Payload	FCS

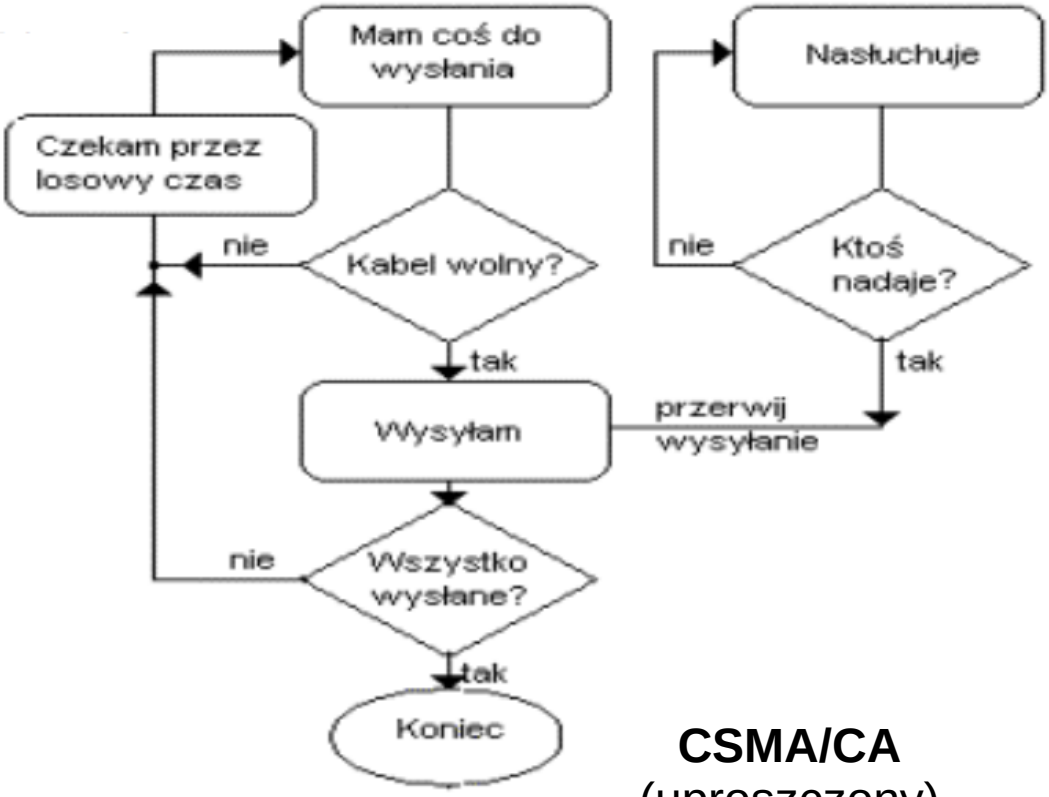




Działanie Ethernetu

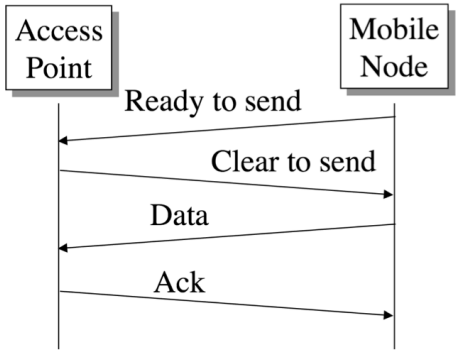
- Unikanie kolizji w ethernecie:
  - ALOHA – nadajemy w dowolnym momencie i czekamy na potwierdzenie odbioru, jeśli nie nadchodzi to ponawiamy → problem **kolizji** (sieć się zapycha, dane się zniekształcają)
  - CSMA (Carrier Sense, Multiple Access) – ciągły nasłuch łącza, gdy łącze wolne rozpoczynamy nadawanie, kolizja możliwa jedynie wtedy, gdy dwie stacje rozpoczną nadawanie w tym samym czasie, oczywiście dowiedzą się o tym i powtórzą transmisję...
  - CSMA/CD (with Collision Detection) – po wykryciu kolizji powtarza sygnał, ale nie przerywa od razu, zniekształcony sygnał jest nadal wysyłany, aby zwiększyć prawdopodobieństwo wykrycia kolizji przez innych (dopiero po chwili jest wysyłany ponownie)
  - CSMA/CA (with Collision Avoidance) – stosowany w sieciach WiFi

CSMA/CD



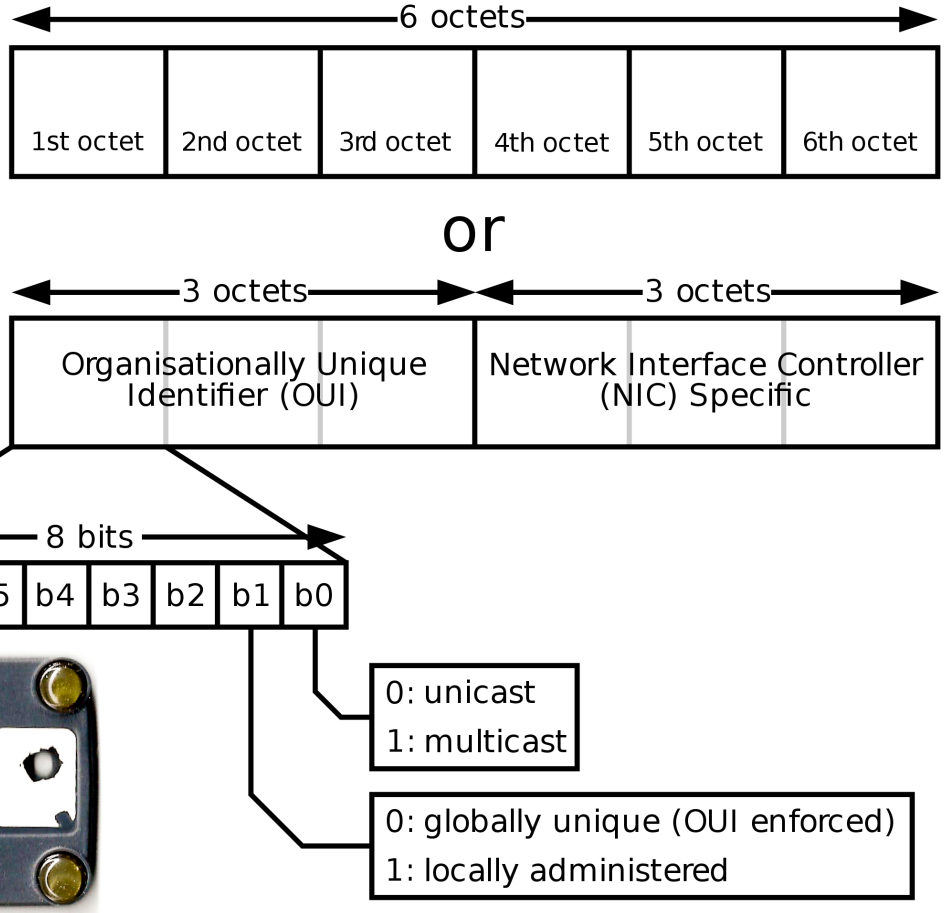
CSMA/CA
(uproszczony)

4-Way Handshake

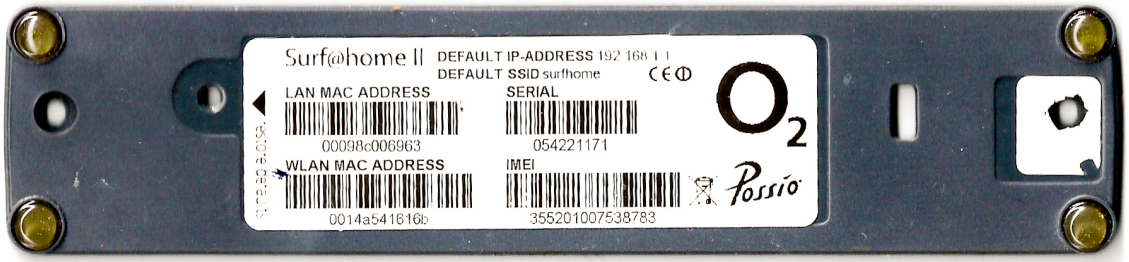


Adres MAC

- Adresacja w warstwie łącza danych, funkcjonująca zarówno w Ethernecie jak i np. WiFi
  - **adres MAC** jest unikalny w skali światowej (przyznawane przez IEEE i ostatecznie ustalane przez producenta urządzenia)
  - adres zawsze ma 48 bitów (6 bajtów), zapisywane w systemie heksadecymalnym
  - przykładowy adres MAC: **B5:AD:C3:2A:D4:F1**
  - ***adres IP jest ustalany na wyższych warstwach***
    → fizycznie wysyłamy na MAC

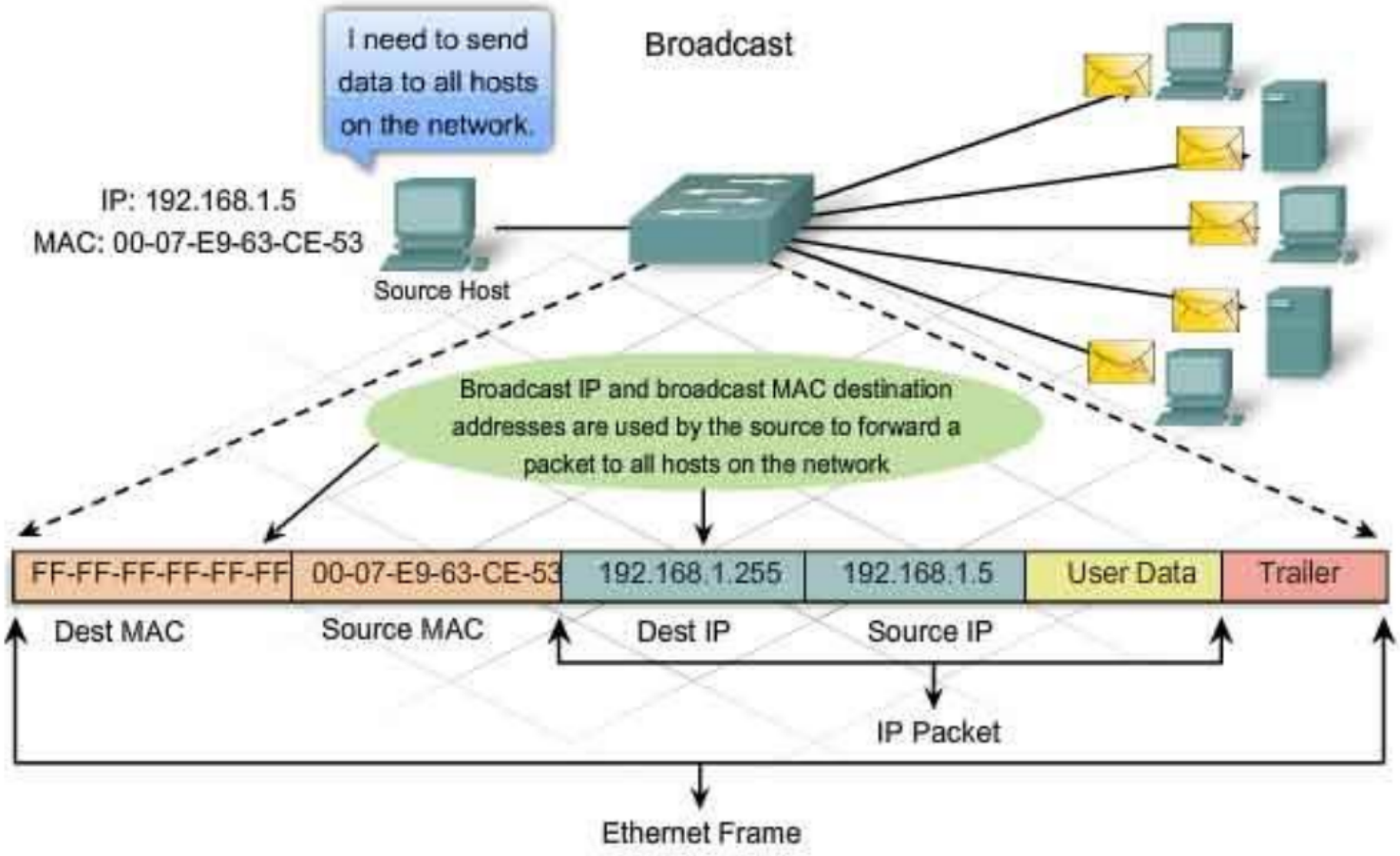


źródło: Wikipedia.org



Adres MAC

- Wyróżniamy również adresy specjalne (zarówno MAC jak i IP):
  - **multicast** – odbieranie ramki przez grupę stacji (01:00:5E:XX:XX:XX)
  - **broadcast** – odbieranie ramki przez wszystkie stacje (FF:FF:FF:FF:FF:FF)

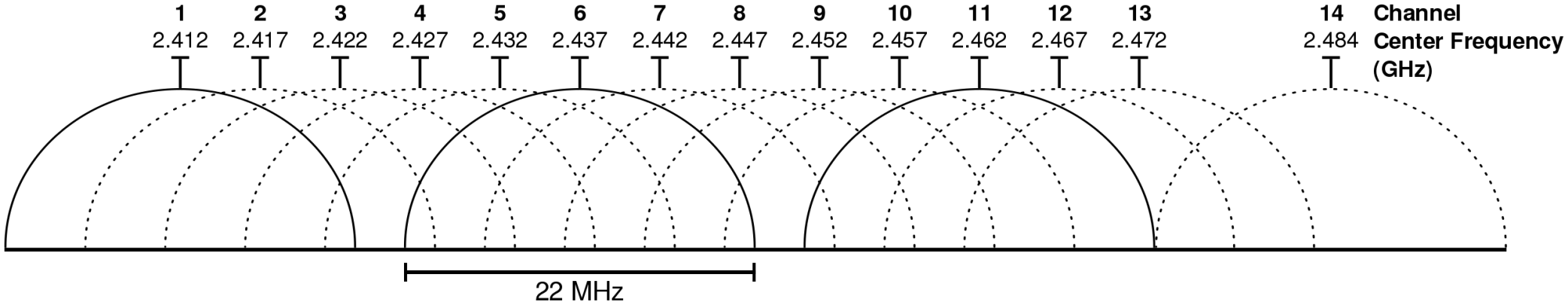


WiFi – standard IEEE 802.11

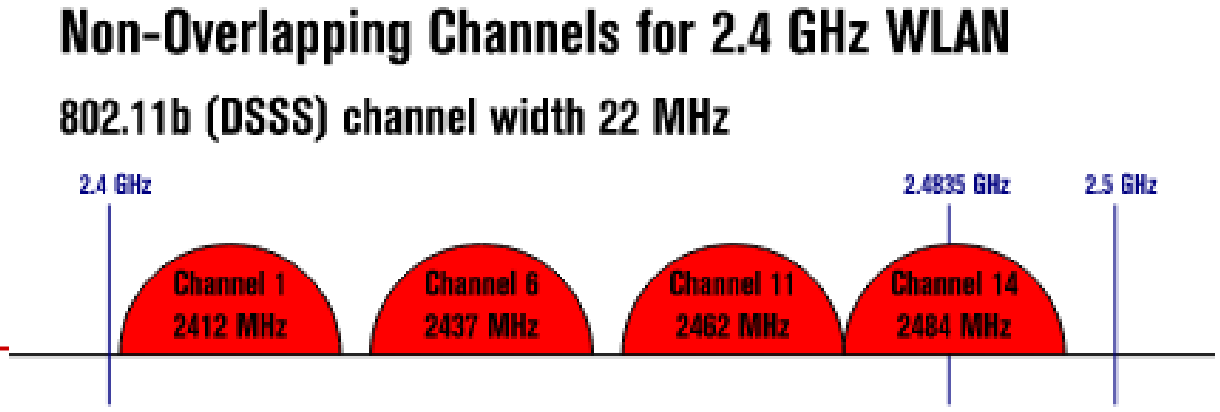
- Przykład standardu **bezprzewodowego**
- Dostępne pasmo dzieli się na **kanały**
- W standardach typu 802.11g **14 kanałów**:
  - pasma oddalone od siebie o 5 MHz
  - pasma się na siebie **nakładają**

Tabela 4.1. *Porównanie standardów transmisji bezprzewodowej*

	Standard					
	IrDA	**Bluetooth**	**IEEE 802.11**	**IEEE 802.11b**	**IEEE 802.11a**	**IEEE 802.11g**
Zasięg	1 m	10 m	60 m	100 m	75 m	100 m
Maksymalna szybkość transmisji	4 Mb/s	1 Mb/s	2 Mb/s	11 Mb/s	54 Mb/s	54 Mb/s
Medium	podczerwień	fale radiowe				
Wrażliwość na zakłócenia	duża	średnia	średnia	mała	średnia	duża
Długość fali/ częstotliwość	850 – 900 nm	2,4 GHz	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz
Data zatwierdzenia	1993 r.	1998 r.	06.1997 r.	08.1999 r.	08.1999 r.	06.2003 r.



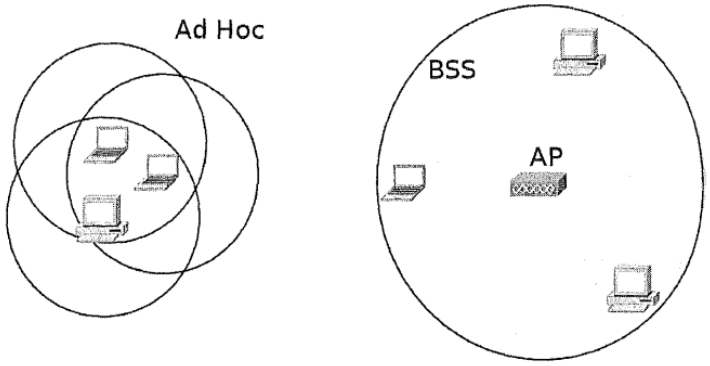
  - bez zakłóceń wybieramy kanały **1, 6 i 11**



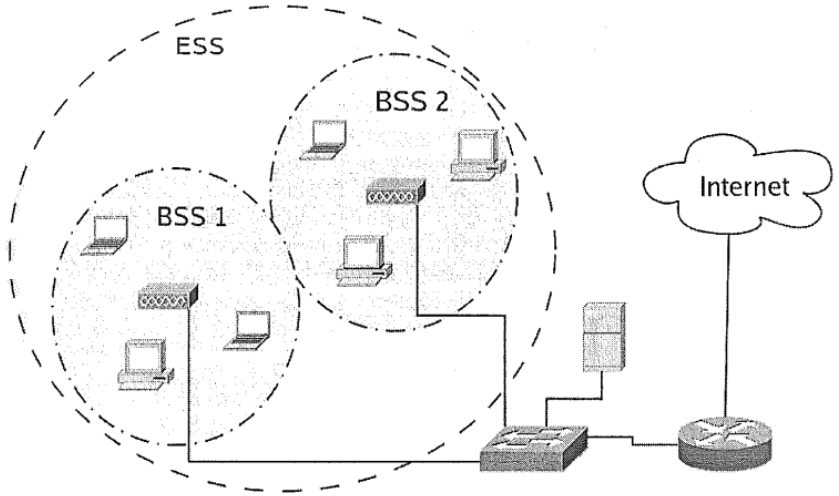
WiFi – struktura sieci WLAN

- Proste sieci WLAN możemy tworzyć jako:
  - **ad hoc** (*IBSS*) – komputery łączą się za pomocą swoich kart sieciowych
  - **BSS** (*Basic Service Set*) – używając punktu dostępowego (***access point*** – ***AP*** – odpowienik koncentratora w ethernecie)

Rysunek 4.2.
Sieć Ad Hoc i BSS



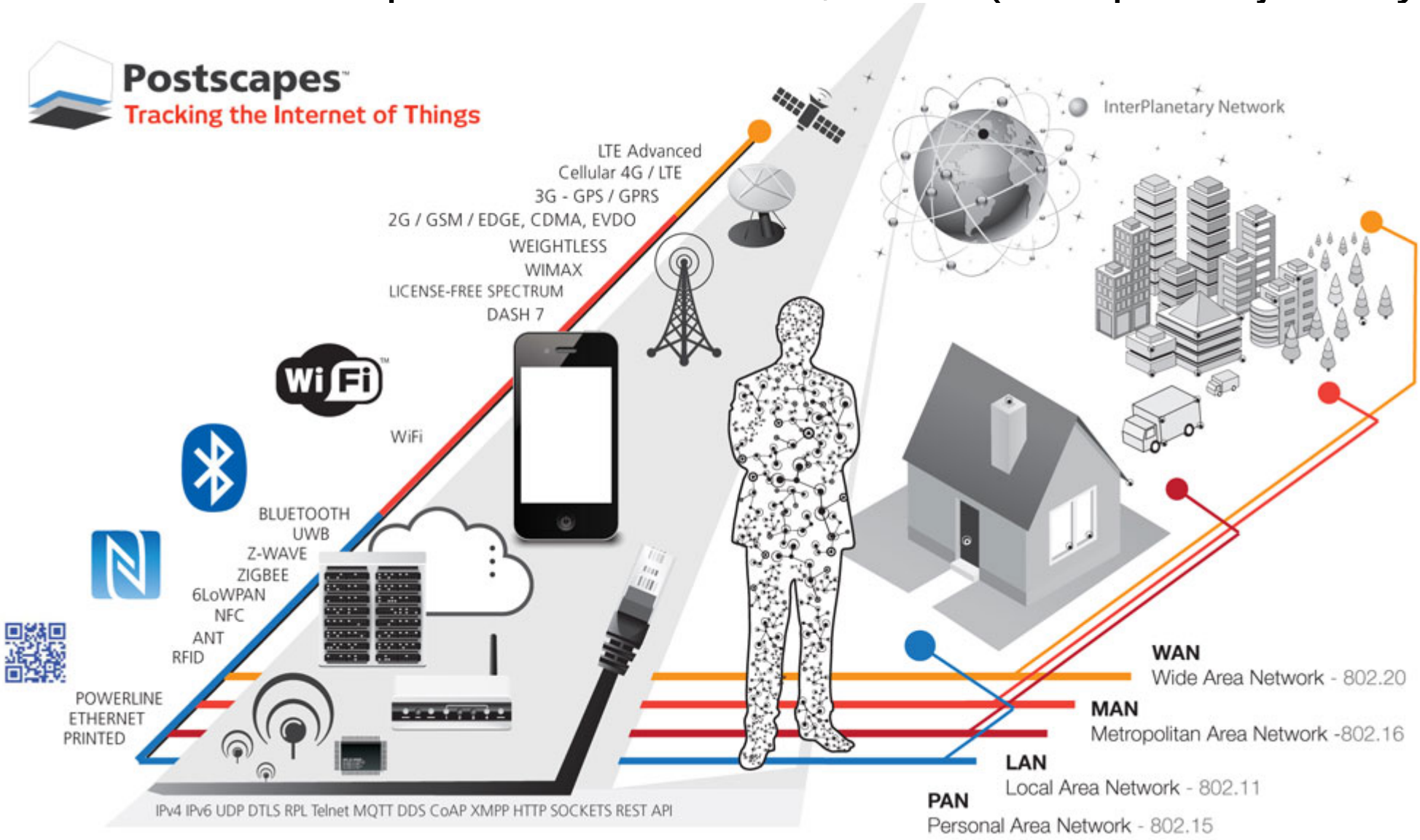
  - **ESS** (Extended Service Set) – kilka AP tworzących swoje BSS
  - **roaming** – przełączanie między BSS w ramach tej samej ESS



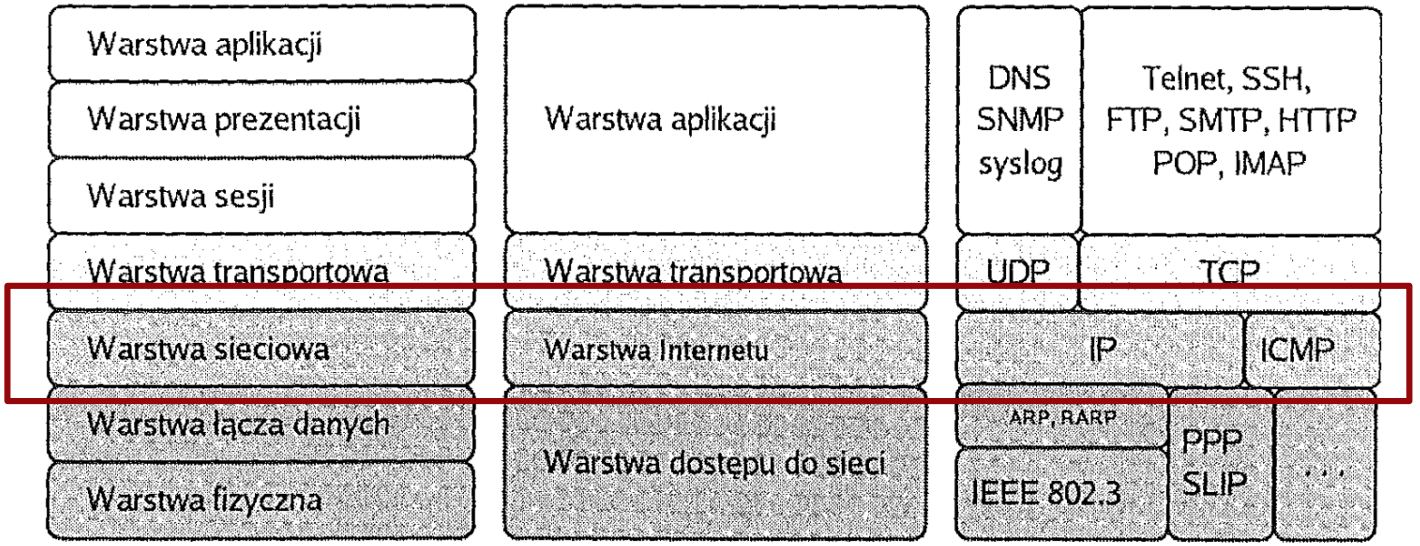
Rysunek 4.3. *Struktura sieci WLAN*

Warstwa dostępu do sieci

- Różne standardy (Ethernet, WiFi, WiMax, LTE, itp.) - zdefiniowane np. w normach IEEE, ramki (enkapsulacja danych)



Warstwa Internetu



źródło: Helion

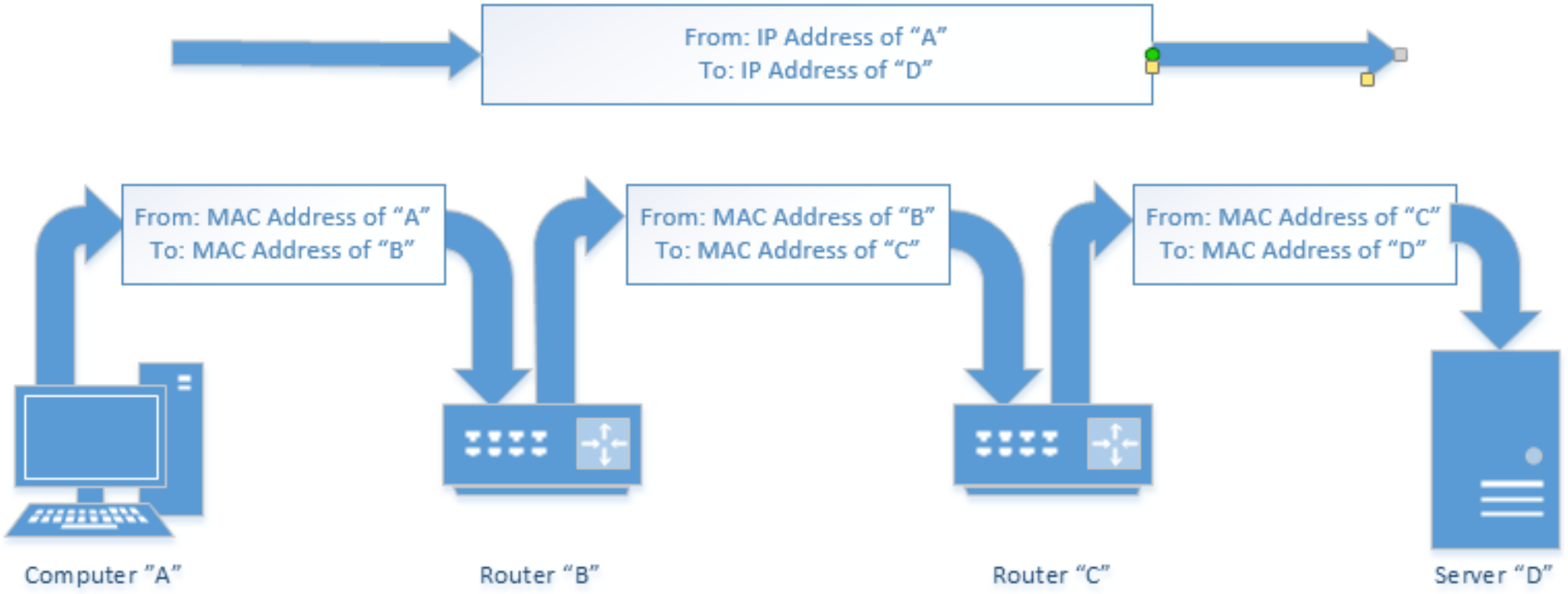
Protokół IP

- Główną częścią warstwy Internetu jest protokół **IP** – *Internet Protocol* (protokół transportowy w Internecie)
- IP zapewnia przenoszenie danych pomiędzy odległymi węzłami
- Jednostką przesyłanej informacji jest **pakiet**, ale formalnie poprawnie (zgodnie ze standardem) powinniśmy mówić o **datagramach** protokołu IP
- Protokół IP:
  - definiuje format i znaczenia pól w datagramach
  - określa schemat adresowania w całym Internecie
  - zapewnia wybór trasy (**trasowanie – routing**)
  - zapewnia **fragmentację** (podział danych) i **defragmentację** danych (łączenie danych)

Adres IP a adres MAC

An **IP address** is kind of like your postal address. Anyone who knows your postal address can send you a letter. That letter may travel a simple or complex route to get to you, but you don't care, as long as it makes it.

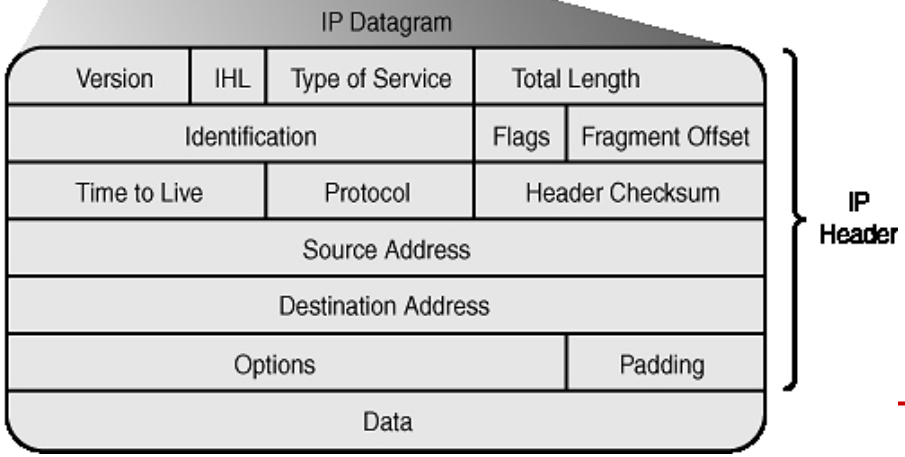
A **MAC Address** is kind of like the color, size, and shape of your physical mailbox. It's enough that the mail clerk (your network router) can identify it, but it's unique to you. There's no reason that anyone other than your postal carrier might care what it is, and you can change it by getting a new mailbox (network card) at any time and slapping your name (IP address) on it, without affecting your delivery.



Protokół IP

- Czego IP nie robi:
  - jest **protokołem bezpołączeniowym** – nie nawiązuje połączenia (tj. nie sprawdza gotowości do odbioru)
  - jest **protokołem niepewnym** – nie zapewnia korekcji i wykrywania błędów transmisji
- IP "jedynie" definiuje jednostkę przesyłanej informacji (datagram), sposób adresacji oraz wybór drogi
- Datagram jest oczywiście zawarty jako "payload" ramki (np. ethernet)

Preamble	SFD	Destination MAC Address	Source MAC Address	EtherType	Payload	FCS



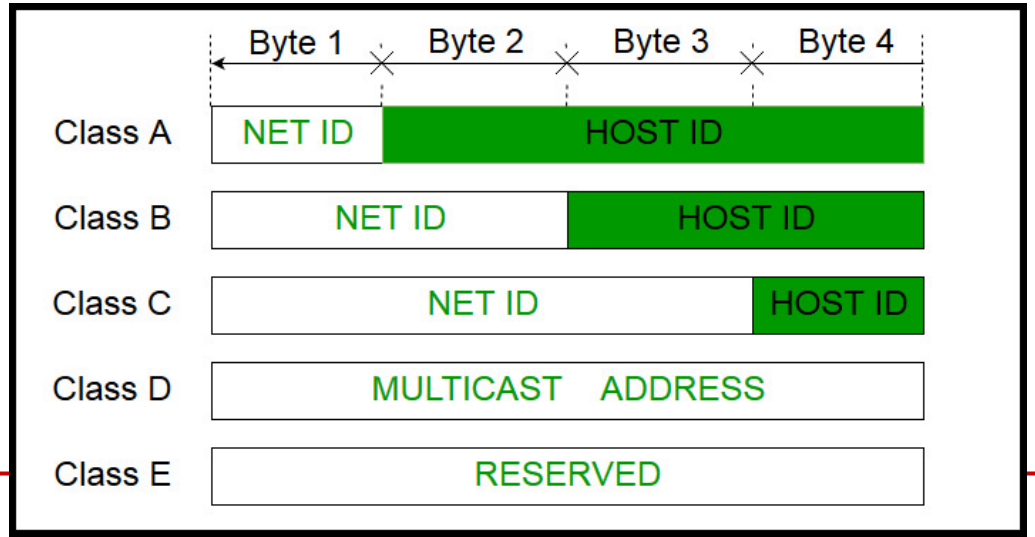
Adresowanie w IP

- Stosowane w Internecie adresy IP wynikają z rozmiaru nagłówka datagramu IP – **4 bajty** (w IPv4)
- Najłatwiej zapamiętać liczby, wobec czego adres najczęściej zapisuje się jako 4 liczby od 0 do 255, odzielone znakiem “.”, np:
  - 194.29.170.123
- Adres można podzielić na dwie części:
  - część identyfikująca daną sieć (np. LAN) w Internecie
  - część definiująca dany komputer wewnątrz sieci LAN
  - adresowanie klasowe oraz (obecnie) maska podsieci

Podział na podsieci z maską 26-bitową

	SIEĆ	SIEĆ	SIEĆ	HOST / PODSIEĆ
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11000000
	255	255	255	192

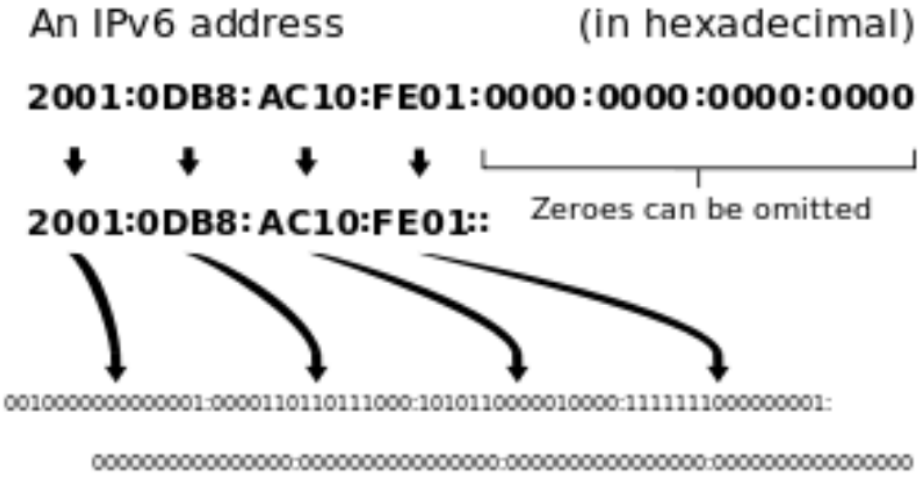
- Adres sieciowy z klasy C
- Zapożyczone 2 bity
- Maska podsieci o adresie 255.255.255.192
- 4 podsieci po 62 hosty

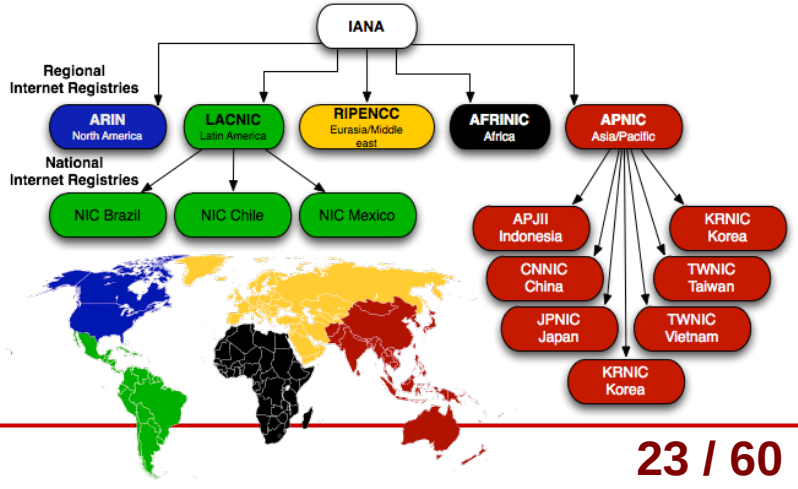


Adresowanie w IP

- Dana firma, przydzielająca adresy IP użytkownikom, ma do dyspozycji ograniczoną pulę adresów – **przestrzeń adresową**
- Przydzielaniem puli adresów IP firmom zajmuje się IANA i organizacje regionalne, a następnie krajowe (w Europie **RIPE** - *Réseaux IP Européens*)
- Całkowita liczba adresów: 2^{32} = 4,29 mld
- **Rozwiązanie – IPv6**
- adres zapisywany na 128 bitach (16 bajtów)
- 2^{128} = 340 trylionów adresów

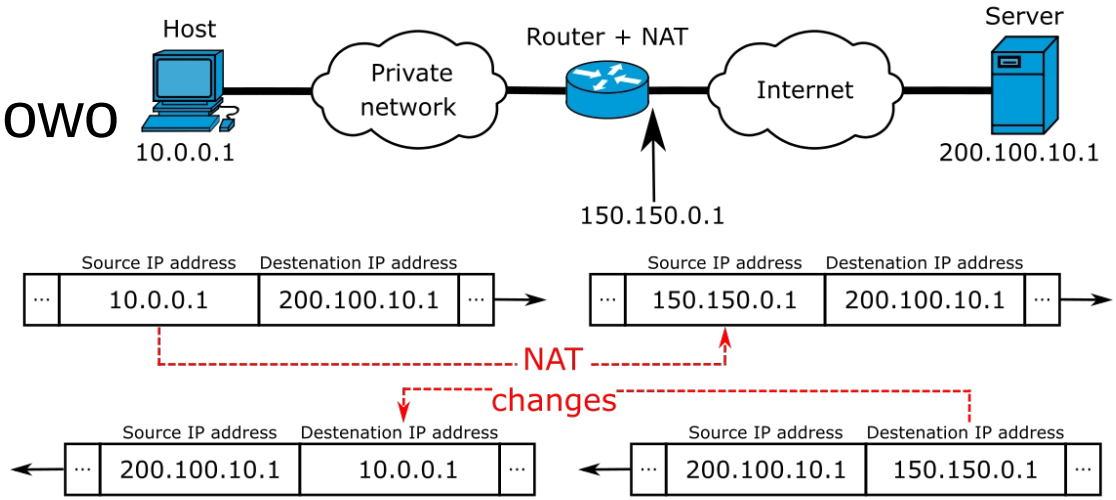
Internet Assigned Numbers Authority





Technologia NAT

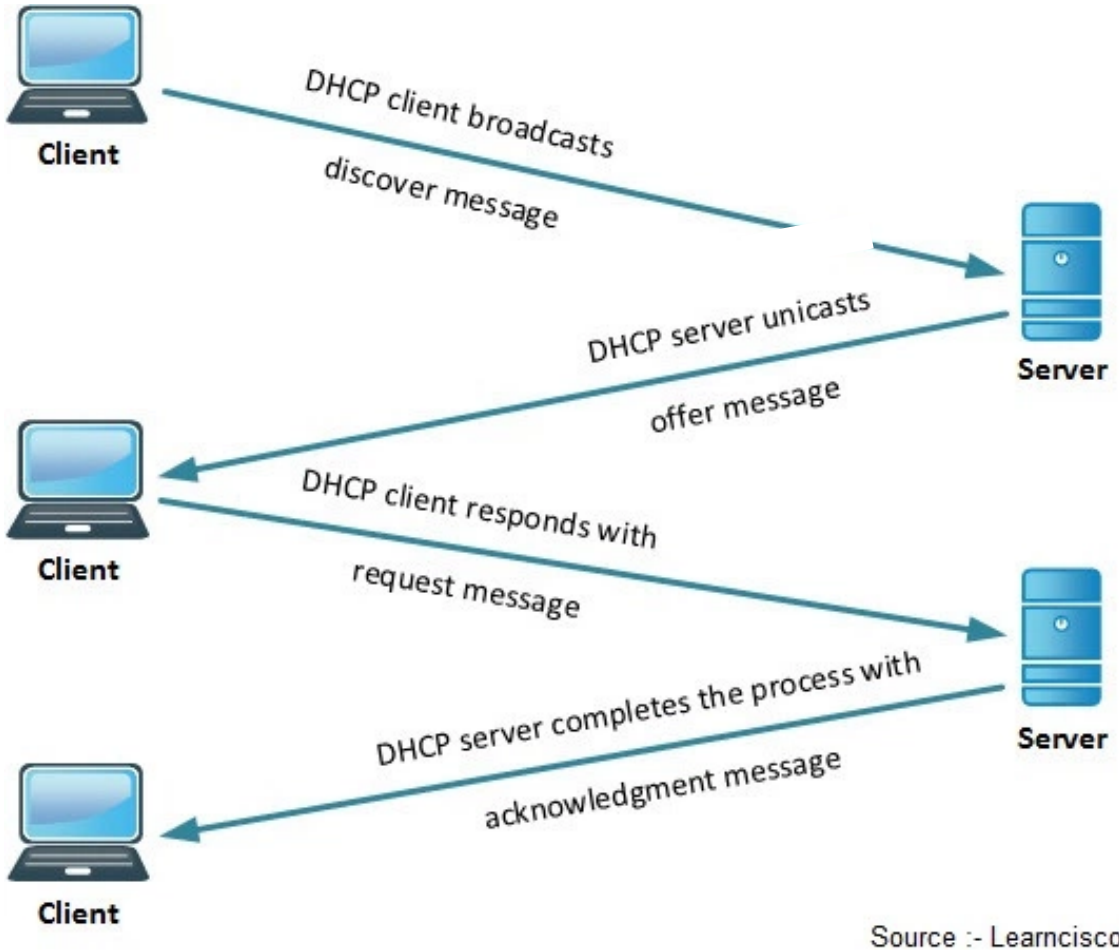
- NAT (*Native Address Transmission*) – zwana również **maskaradą sieci/IP**, to technika przesyłu danych przez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP (równiez portów TCP/UDP)
- Po co to robić?
  - umożliwiamy wielu urzadzeniom dostęp do Internetu po jednym publicznym adresie IP (tzw. **brama sieciowa – gateway**)
  - kosztem jest brak publicznego IP konkretnego hosta oraz możliwa komplikacja komunikacji (np. zmniejszone prędkości przesyłu danych)
  - użycie NAT pomaga częściowo rozwiązać problem skończonej puli adresów IPv4



Protokół DHCP

- IP można otrzymać **statycznie** lub **dynamicznie** (DHCP)
- Otrzymanie adresu IP jest wysłania odpowiedniego zapytania do serwera DHCP i otrzymania potwierdzenia
- Serwer DHCP przydziela adres z dostępnej wolnej puli adresów dla danej podsieci
- Serwer DHCP utrzymuje tablicę wcześniejszych przypisań

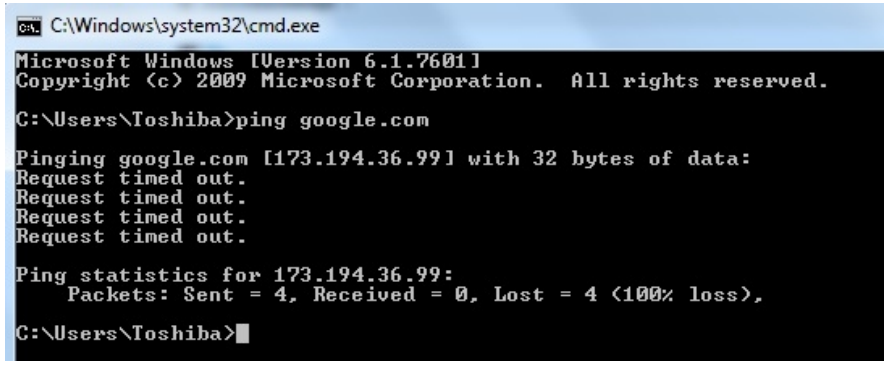
  → urządzenie
  może dostać poprzednio
  otrzymany adres IP



Source :- Learncisco

Protokół ICMP

- Protokół IP nie sprawdza czy dane dotarły do adresata
  - taka możliwość jest dopiero w wyższych warstwach
- Jedyne co mozna zrobić, to sprawdzenie dostępności sieci docelowej → protokół ICMP (*Internet Control Message Protocol*)
- ICMP jest protokołem kontrolnym, do wykrywania sytuacji awaryjnych
- Odbiorca może wysłać do nadawcy kilka różnych komunikatów, np. prosząc o wstrzymanie lub informując, że jest nieosiągalny
- Testowanie osiągalności odbywa się za pomocą polecenia **ping**
- Trasę można testować za pomocą polecenia **traceroute**

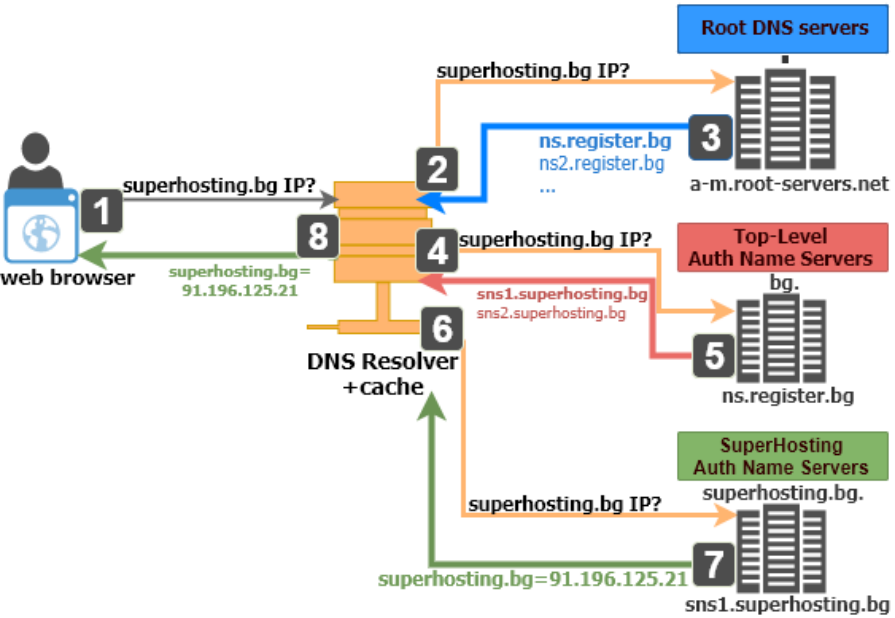


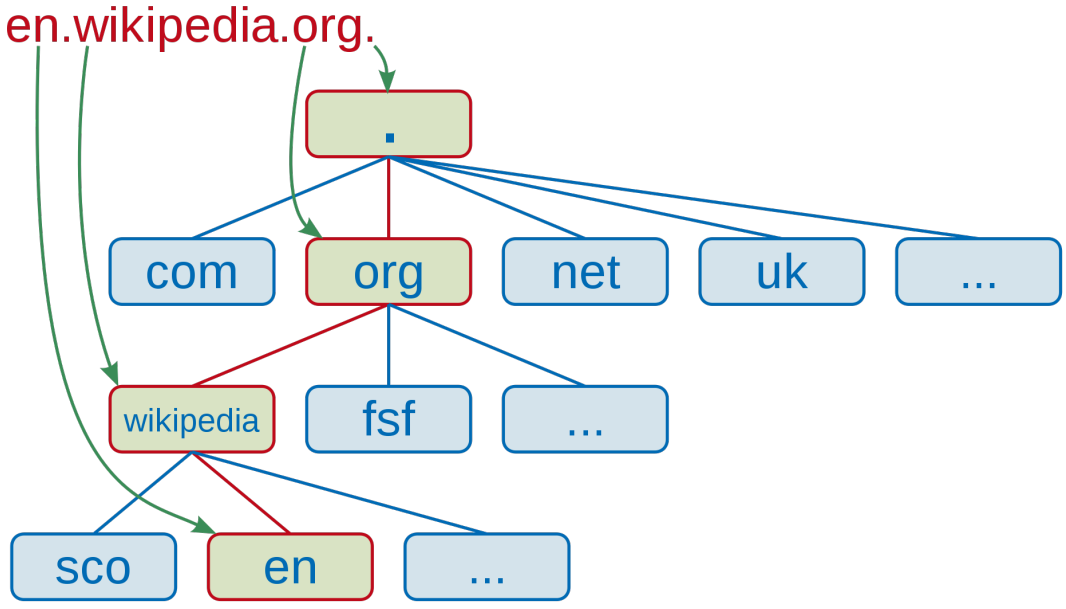

```
wfpw@meyrin:~$ ping google.pl
PING google.pl (216.58.209.35) 56(84) bytes of data.
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=1 ttl=56 time=7.33 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=2 ttl=56 time=9.07 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=3 ttl=56 time=11.4 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=4 ttl=56 time=19.0 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=5 ttl=56 time=31.4 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=6 ttl=56 time=32.1 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=7 ttl=56 time=17.4 ms
^C
--- google.pl ping statistics ---
8 packets transmitted, 7 received, 12% packet loss, time 7010ms
rtt min/avg/max/mdev = 7.332/18.285/32.163/9.404 ms
```

```
wfpw@meyrin:~$ traceroute google.pl
traceroute to google.pl (216.58.209.35), 30 hops max, 60 byte packets
 1  out.if.pw.edu.pl (194.29.174.62)  0.385 ms  0.325 ms  0.357 ms
 2  194.29.132.164 (194.29.132.164)  0.268 ms  0.288 ms  0.301 ms
 3  pw-r1-ge2-0-8-501.warman.nask.pl (148.81.253.69)  0.409 ms  0.402 ms  0.399 ms
 4  z-nask.poznan-gw3.10Gb.rtr.pionier.gov.pl (212.191.224.73)  4.955 ms  4.979 ms  4.969 ms
 5  72.14.203.178 (72.14.203.178)  8.247 ms  8.280 ms  8.270 ms
 6  108.170.250.209 (108.170.250.209)  9.028 ms 108.170.250.193 (108.170.250.193)  8.261 ms  8.248 ms
 7  216.239.40.153 (216.239.40.153)  8.230 ms 216.239.40.155 (216.239.40.155)  8.499 ms 216.239.40.153 (216.239.40.153)  8.479 ms
 8  waw02s05-in-f35.1e100.net (216.58.209.35)  8.164 ms  8.186 ms  8.169 ms
```

Serwer DNS

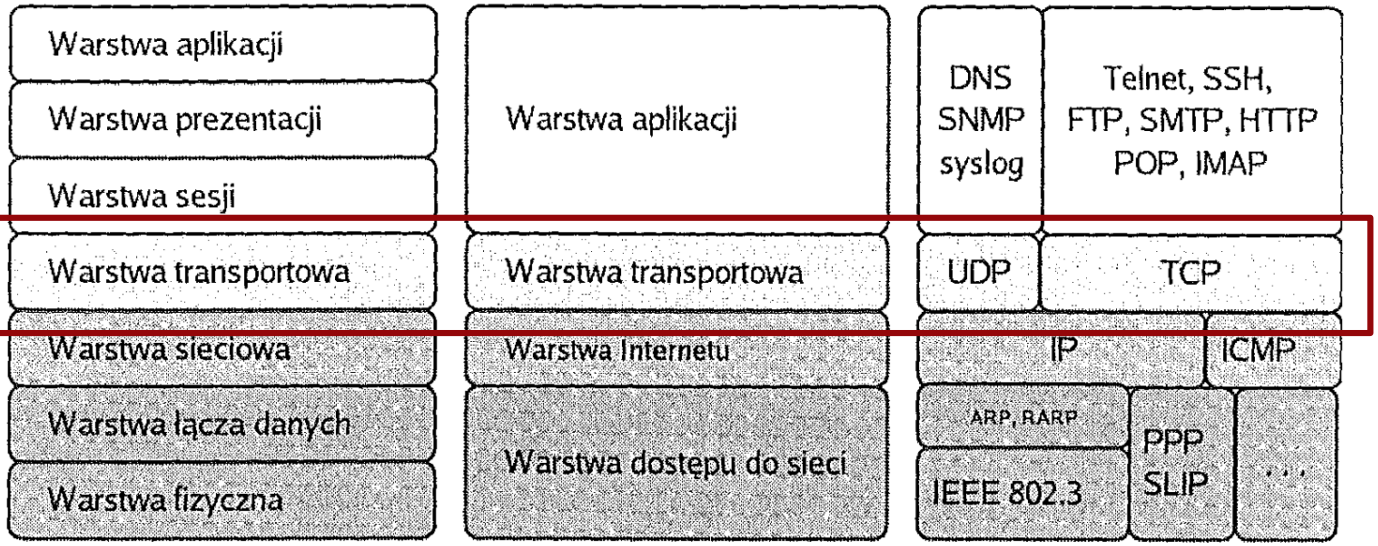
- **DNS** (*Domain Name Server*) – to serwer, na którym przechowywana jest tablica publicznych adresów IP, którym przypisane są nazwy hostów (hostnames) i domen
  - ***hostname*** to nazwa konkretnego urządzenia zapisana zrozumiałym dla człowieka tekstem
  - ***domena*** to grupa hostów w obrębie jednej administracji, wspólnie zarządzana
- Odpytujemy po kolei kolejne serwery DNS, zaczynając od poziomu (strefy) root





Warstwa transportowa

Protokoły TCP i UDP



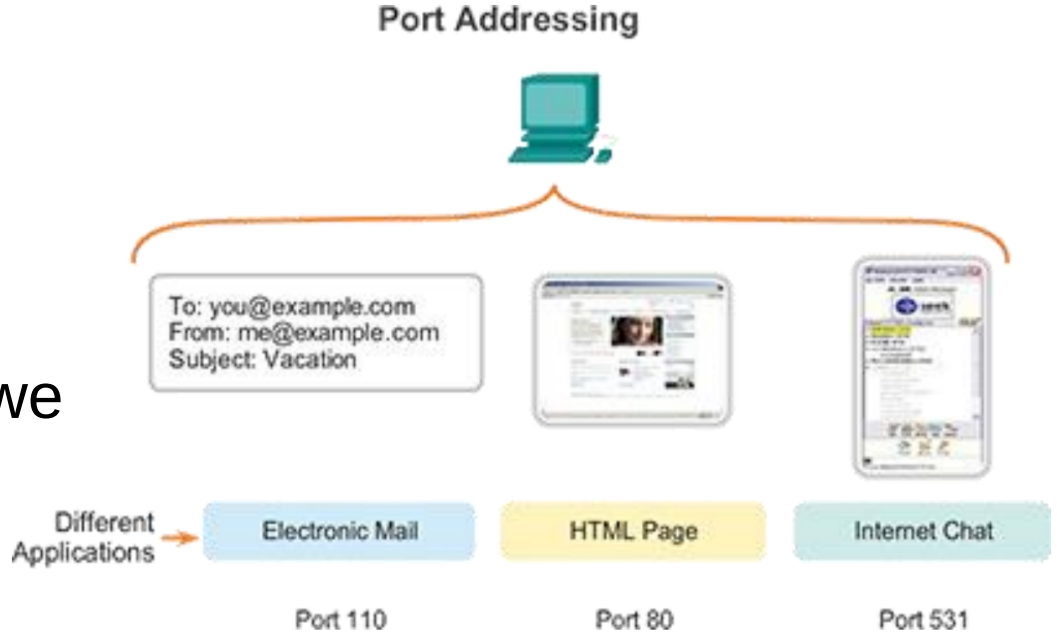
źródło: Helion

Warstwa transportowa

- Zadaniem wartstwy transportowej jest **niezawodne** przesyłanie danych między urządzeniami
- Protokoły warstwy transportowej otrzymują dane z warstwy Internetu i rozdzielają je na poszczególne procesy w warstwie aplikacji (“ten fragment danych idzie do komunikatora, ten do e-mail’a a ten do przeglądarki”)
- Zawiera mechanizmy:
  - inicjalizowania, utrzymania, zamykania połączenia
  - sterowania przepływem danych
  - wykrywania błędów transmisji
- Istnieje wiele protokołów warstwy transportowej, ale najważniejsze są dwa:
  - TCP
  - UDP

Gniazdo sieciowe

- Identyfikacja procesu, który ma odebrać daną porcję danych, odbywa się na podstawie numeru portu
  - **numer portu** jest 16-bitową liczbą związaną z danym typem komunikacji w sieci – przykładowo, serwer WWW odbierając zapytanie i następnie przesyłając stronę odbiorcy działa na porcie 80
- **Gniazdo sieciowe** (*network socket*) to para liczb (numer IP oraz numer portu), które identyfikują zarówno odbiorcę jak i dany proces (aplikację)
  - zapis: 62.211.243.226:80 (IP:port)
  - zakres portów: 0 - 65 535
  - (opcjonalnie) gniazdo sieciowe może zawierać informację o protokole (np. TCP)



“Well-known ports”

- Istnieje lista zarezerwowanych portów (*well-known ports*), które są przypisane do różnych aplikacji (usług)
- Organizacja IANA prowadzi rejestr zarezerwowanych portów:

  https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

- Obecnie otwarte porty możemy sprawdzić poleceniem **netstat** (zarówno Windows i Linux)

```
C:\Users\opal>netstat -o

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    127.0.0.1:1028         raft:5905              ESTABLISHED     1424
  TCP    127.0.0.1:1029         raft:5905              ESTABLISHED     1424
  TCP    127.0.0.1:5905         raft:1032              ESTABLISHED     1424
  TCP    127.0.0.1:5905         raft:1033              ESTABLISHED     1424
  TCP    192.168.1.101:1344     poczta:imaps           ESTABLISHED     5876
  TCP    192.168.1.101:1421     poczta:imaps           ESTABLISHED     5876
  TCP    192.168.1.101:1422     poczta:imaps           ESTABLISHED     5876
  TCP    192.168.1.101:1423     poczta:imaps           ESTABLISHED     5876
  TCP    192.168.1.101:3027     rmfstream3:8009        ESTABLISHED     5372
  TCP    192.168.1.101:3116     wg-in-f189:https       ESTABLISHED     5372
  TCP    192.168.1.101:3286     www:http               ESTABLISHED     5372
  TCP    192.168.1.101:3306     poczta:imaps           ESTABLISHED     5876
  TCP    192.168.1.101:3327     74.125.133.106:https   ESTABLISHED     5372
  TCP    192.168.1.101:3332     host-213:https         ESTABLISHED     5372
  TCP    192.168.1.101:3349     74.125.133.95:http     ESTABLISHED     5372
  TCP    192.168.1.101:3351     74.125.206.95:http     ESTABLISHED     5372
  TCP    192.168.1.101:3352     74.125.206.95:http     ESTABLISHED     5372
  TCP    192.168.1.101:3359     wg-in-f94:http         ESTABLISHED     5372
  TCP    192.168.1.101:3360     wg-in-f94:http         ESTABLISHED     5372
  TCP    192.168.1.101:3361     wg-in-f101:https       ESTABLISHED     5372
  TCP    192.168.1.101:3362     wg-in-f94:http         ESTABLISHED     5372
  TCP    192.168.1.101:3363     wg-in-f94:http         ESTABLISHED     5372
  TCP    192.168.1.101:3376     wj-in-f84:https        ESTABLISHED     5372
```

Protocol	Port	Protocol	Purpose
echo	7	TCP/UDP	Echo is a test protocol used to verify that two machines are able to connect by having one echo back the other's input.
discard	9	TCP/UDP	Discard is a less useful test protocol in which all data received by the server is ignored.
daytime	13	TCP/UDP	Provides an ASCII representation of the current time on the server.
FTP data	20	TCP	FTP uses two well-known ports. This port is used to transfer files.
FTP	21	TCP	This port is used to send FTP commands like put and get.
SSH	22	TCP	Used for encrypted, remote logins.
telnet	23	TCP	Used for interactive, remote command-line sessions.
smtp	25	TCP	The Simple Mail Transfer Protocol is used to send email between machines.
time	37	TCP/UDP	A time server returns the number of seconds that have elapsed on the server since midnight, January 1, 1900, as a four-byte, signed, big-endian integer.
whois	43	TCP	A simple directory service for Internet network administrators.
finger	79	TCP	A service that returns information about a user or users on the local system.
HTTP	80	TCP	The underlying protocol of the World Wide Web.
POP3	110	TCP	Post Office Protocol Version 3 is a protocol for the transfer of accumulated email from the host to sporadically connected clients.

Porównanie UDP i TCP

Cecha	UDP	TCP
Opis	Prosty protokół dużych przepustowości (przeniesienie funkcjonalności na warstwy wyższe)	W pełni funkcjonalny, niezawodny protokół komunikacyjny z mechanizmami obsługi błędów warstwy sieciowej
Ustanawianie połączenia	bezpołączeniowy	Połączeniowy, faza nawiązania połączenia
Interfejs danych dla aplikacji	Zorientowany na wiadomości	Zorientowany strumieniowo
Wiarygodność i potwierdzenia	Zawodny, bez potwierdzeń	Niezawodny, wymaga potwierdzeń dostarczenia datagramów
Retransmisje	Nie obsługiwane (przeniesione do warstw wyższych)	Obsługiwane automatycznie
Kontrola przepływu	Brak	Okno przesuwne zmiennych rozmiarów, mechanizmy zapobiegania przeciążeniom
Narzut	Bardzo mały	Mały
Prędkość transmisji	Bardzo duża	Duża
Typ danych (wielkość, rozmiar)	od małych do średnich	Od małych do bardzo dużych

Jak zbudowany jest Internet?

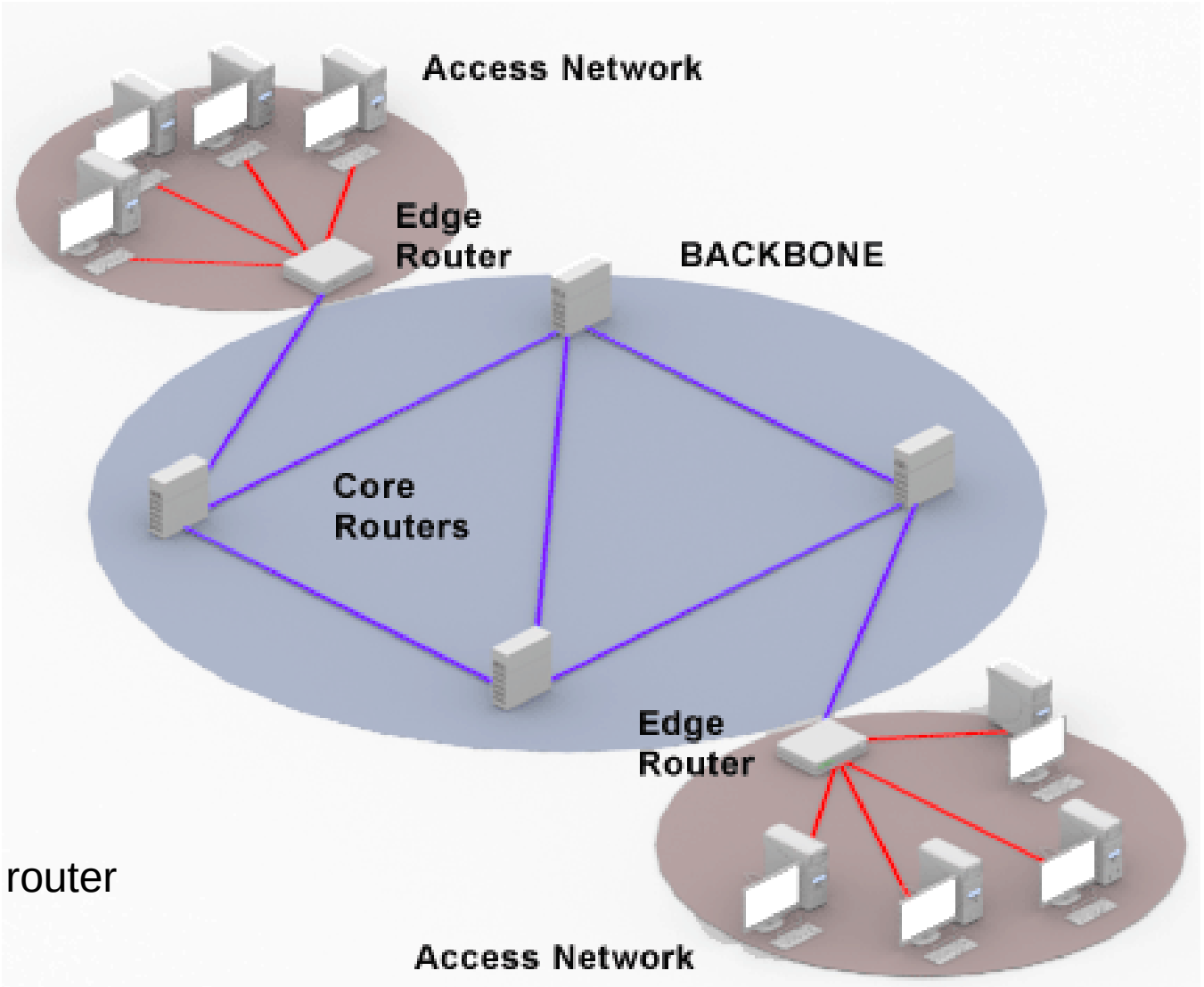
- Internet jest siecią rozproszoną wykorzystującą protokół IP (oraz TPC i UDP – o nich za chwilę) oraz DNS do przydzielania nazw
- Jest niezależna od fizycznego sposobu realizacji łącza (użytych kabli, sieci radiowych, etc.)
- Najważniejszym urządzeniem w Internecie (obok komputerów-klientów :)) jest router
  - jak już wiemy – router to urządzenie w warstwie Internetu, działające na protokole IP, przekazujące ruch pomiędzy dwoma sieciami
  - routery dzielimy na
    - routery na brzegach (**edge routers**) – bezpośrednio połączone z sieciami (klientami) docelowymi oraz jednym routerem rdzenia
    - routery rdzenia (**core routers**) – połączone ze sobą oraz z core routers, tworzą szkielet sieci (**backbone**)

Jak zbudowany jest Internet?

- Coure routers to urządzenia bardzo drogie, działające z maksymalną możliwą prędkością przesyłania pakietów
- Kilku producentów
  np. CISCO, HUAWEI

core router

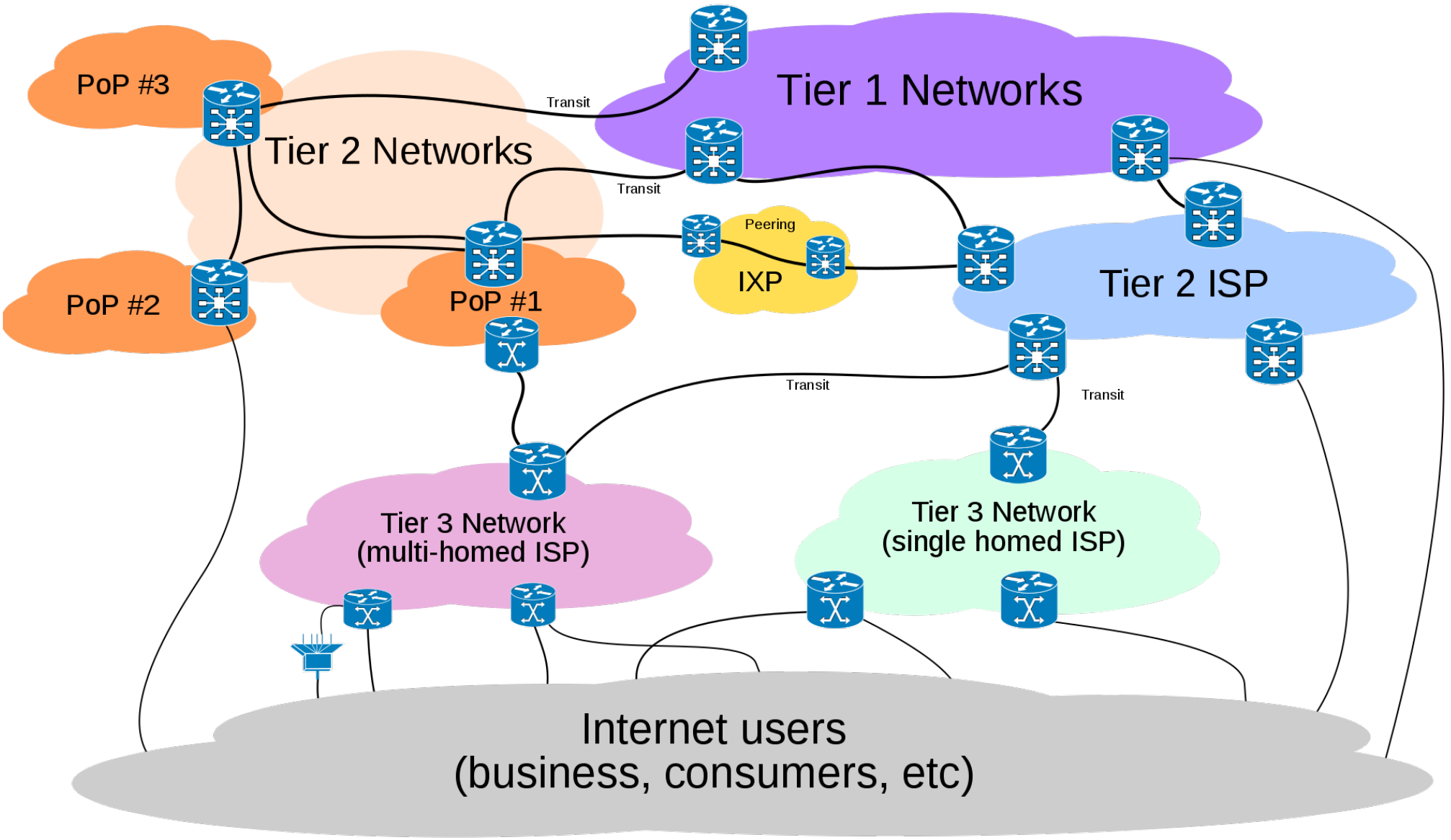
edge router



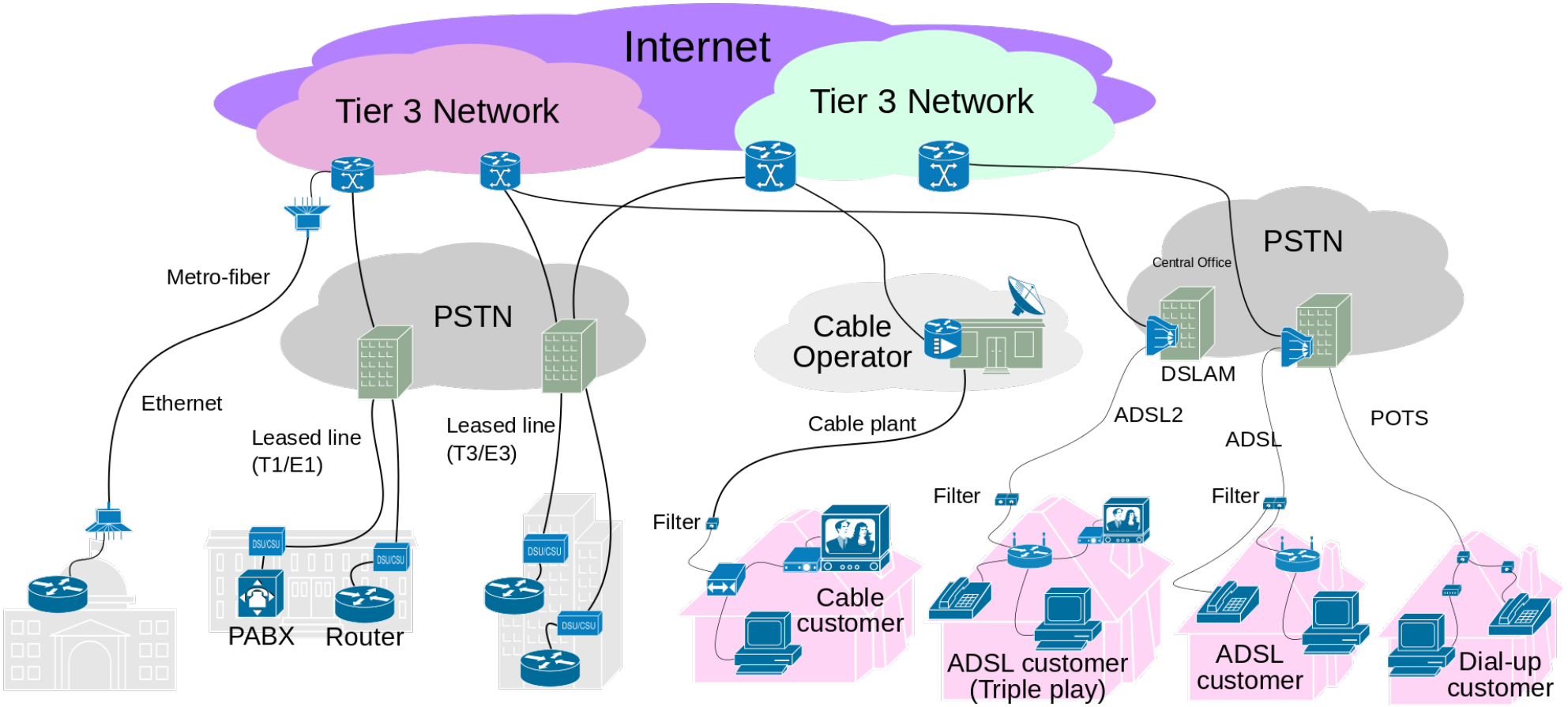
Jak zbudowany jest Internet?

- Internet tworzą tzw. **Systemy Autonomiczne** (AS)
  - zwykle zarządzane przez jedną organizację
  - mającą własną sieć szkieletową (wiele routerów) i systemy klienckie
- Dostawca Internetu (**ISP** – ***Internet Service Provider***) to taki AS, który jest podłączony do innych sieci i może pełnić rónież rolę tranzytową (połączony jest z wieloma sieciami klientów oraz z innymi ISP, umożliwia pełną komunikację w Internecie)
- ISP grupuje się w kategorie (**tiers**):
  - np. Tier 1 – połączone każda ze sobą (za pomocą odpowiednich umów), główny szkielet Internetu
  - Tier 2 – musi wykupywać dostęp do części (np. aby dostać się do innego Tier 2 przez kilka Tier 1)
  - Tier 3 – z reguły to z czym komunikujemy się z domu (nasz dostawca Internetu)
  - najlepiej to zobrazować na obrazkach (następne dwa slajdy)

Jak zbudowany jest Internet?



Jak zbudowany jest Internet?

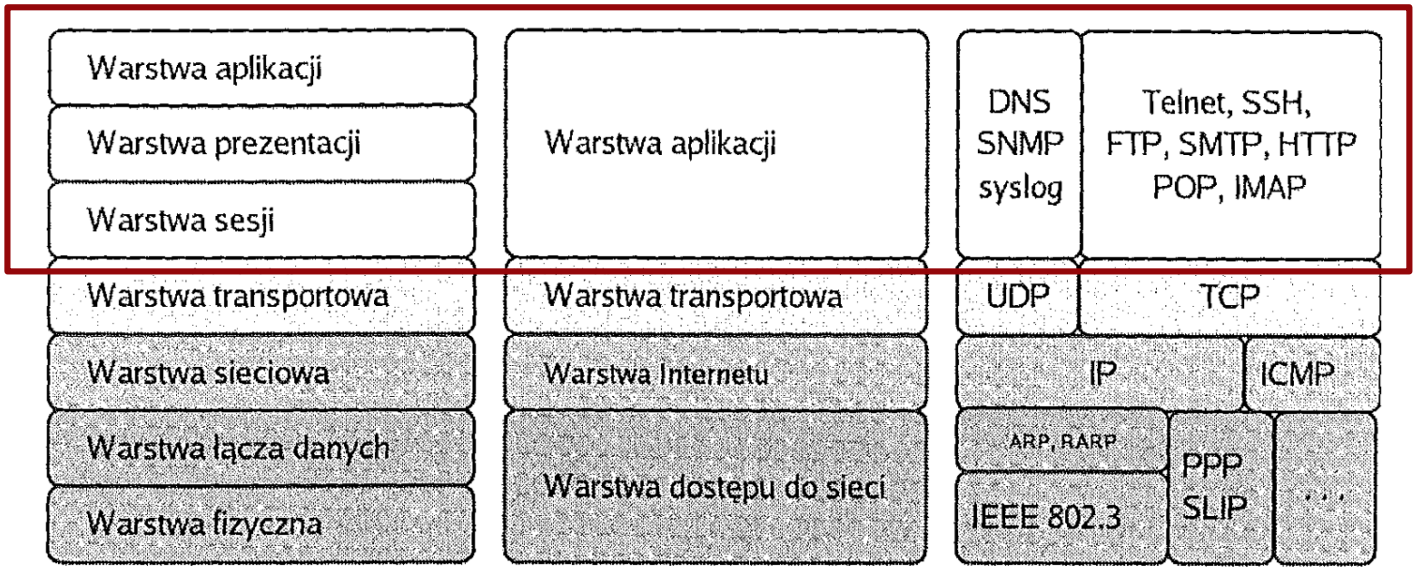


CERN Internet Exchange Point

- Poziom 0 (parter) CERN Data Center
- Szafy z czerwonymi kablami - CIXP

Warstwa aplikacji

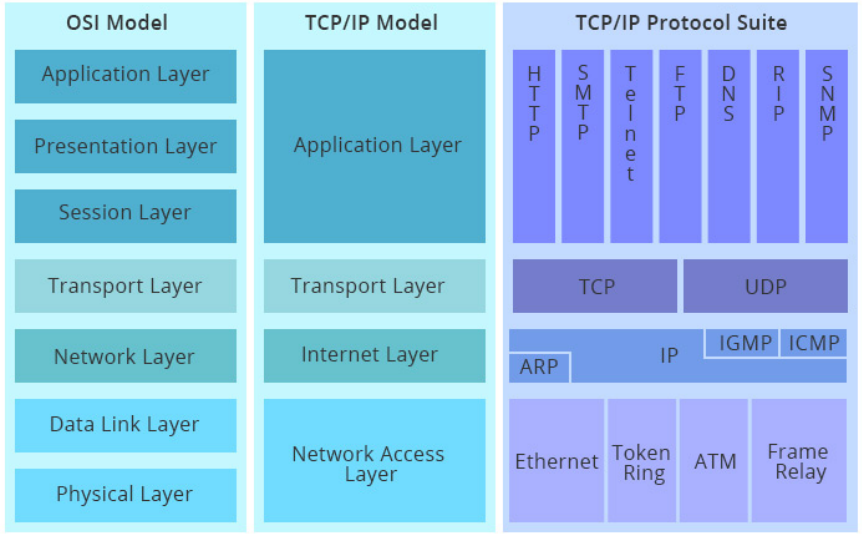
Usługi sieciowe

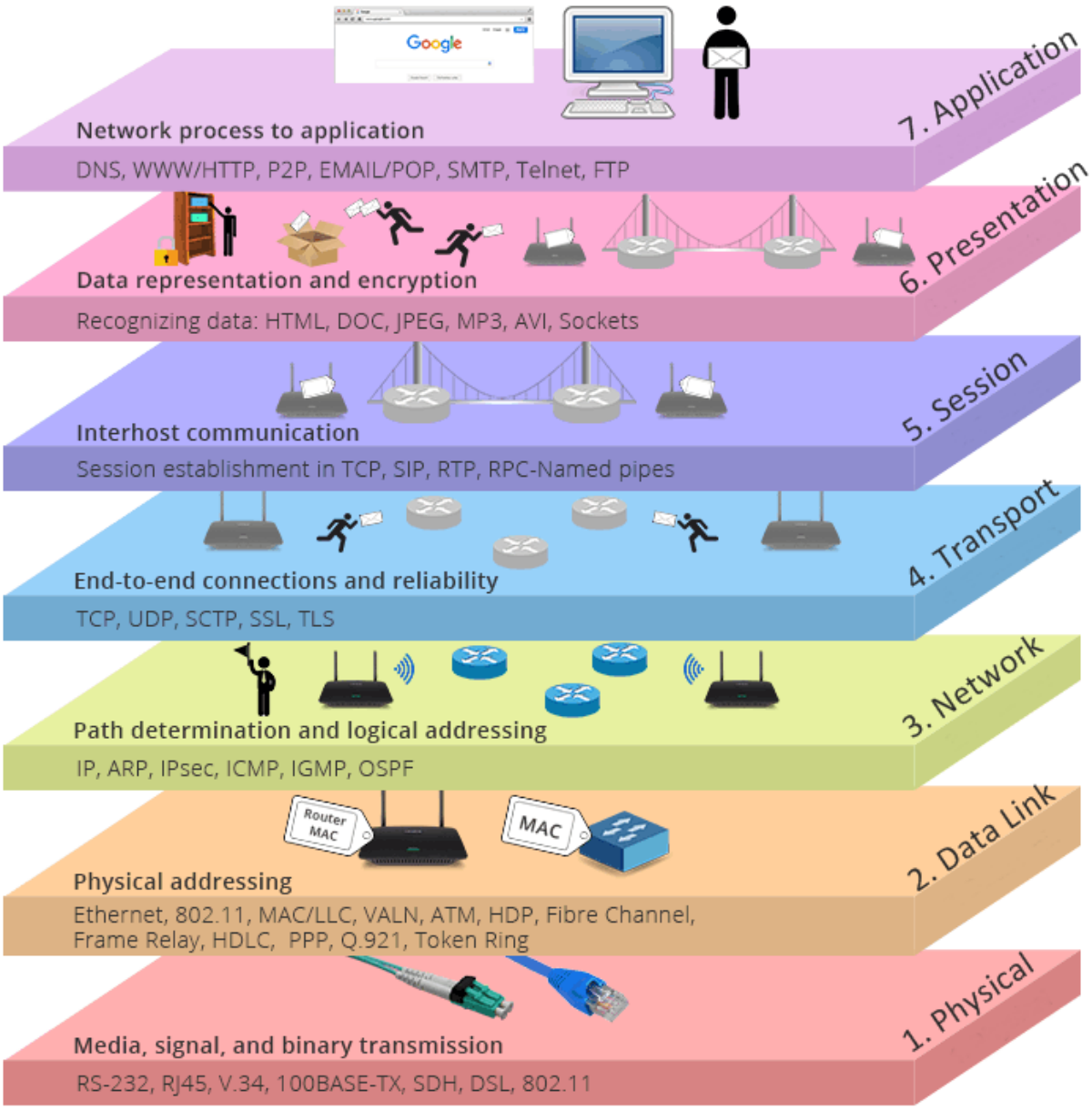


źródło: Helion

Warstwa aplikacji

- W modelu ISO/OSI wyróżniamy w zasadzie trzy górne warstwy:
  - warstwa sesji
  - warstwa prezentacji
  - warstwa aplikacji
- W praktyce to aplikacje TCP(UDP)/IP realizują zadania ostatnich 3 warstw



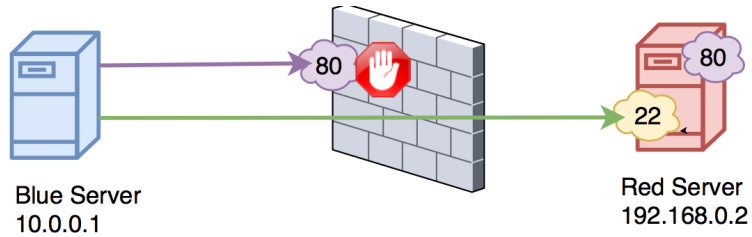


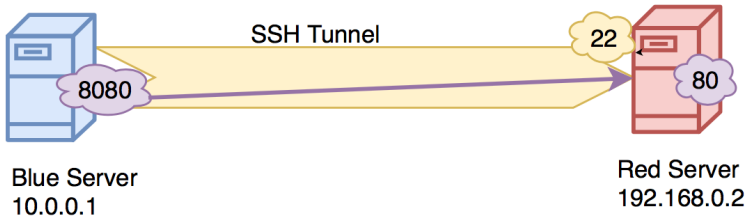
Warstwa aplikacji

- W ostatniej warstwie działają **protokoły komunikacji**, które używane są przez finalne aplikacje komunikujące się z użytkownikiem
- Część z nich już poznaliśmu (np. DNS czy DHCP)
- Protokoły zapewniają możliwość korzystania z różnych **usług** dostępnych w sieci, np.:
  - WWW/HTTP – przeglądanie stron internetowych
  - FTP – serwery plików
  - SMTP – wysyłanie/odbieranie e-mail'i
  - POP oraz IMAP – odczytywanie e-maili z serwera przez aplikacje klienckie
  - SSH – bezpieczne logowanie
  - LDAP – usługi katalogowe (np. wspólne usługi drukarek, logowanie, itp.)
  - … itp./itd.

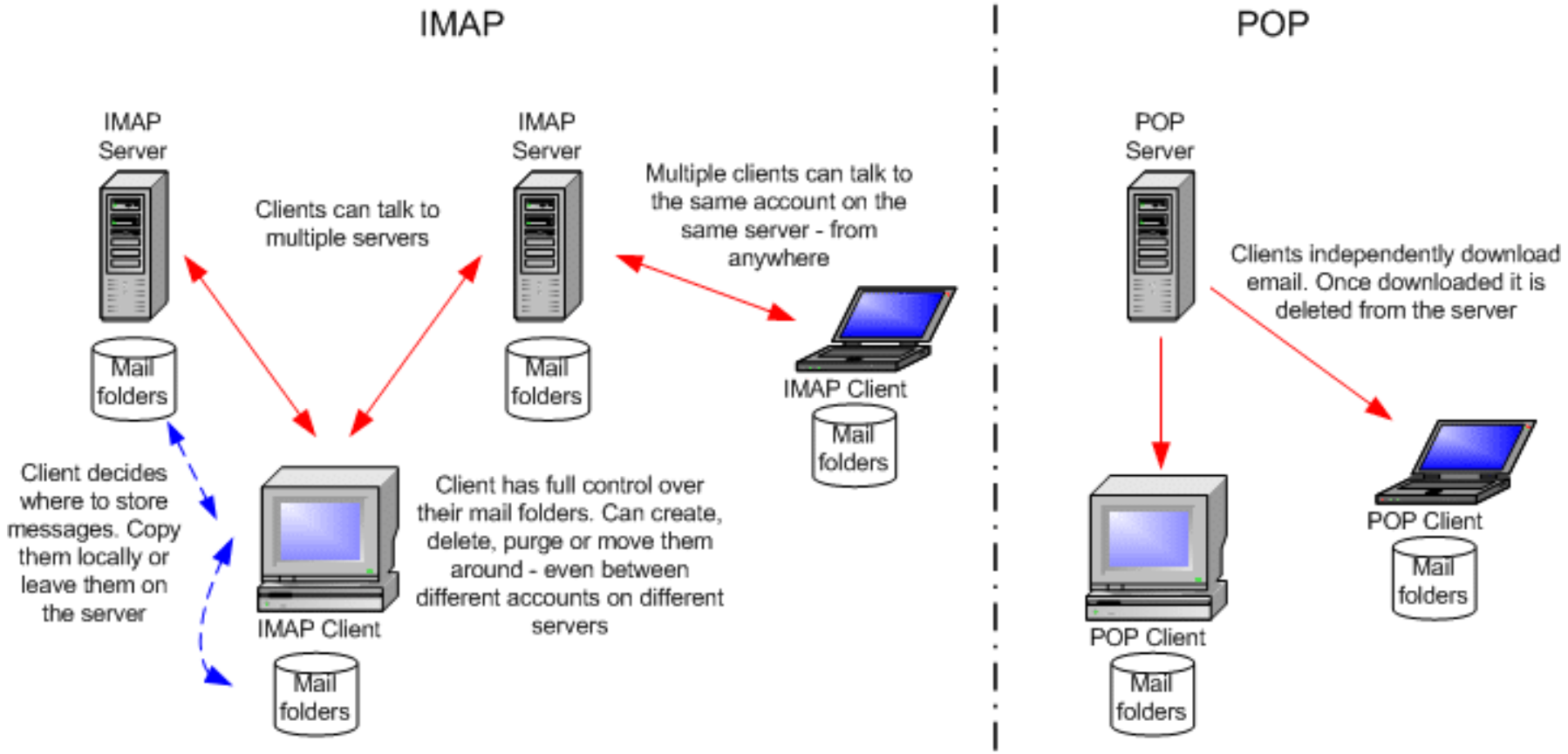
SSH

- **SSH** (*Secure Shell Login*) jest protokołem zadalnego dostępu do komputera, jak telnet, ale z wykorzystaniem szyfrowania, RFC 4253
- Działa za pomocą protokołu TCP, *well known port* to 22
- Szyfrowanie asymetryczne (hasła, klucze)
  - szyfrowane zarówno hasło jak i klucze
- Dużo więcej możliwości:
  - terminal (ssh)
  - przesyłanie plików (scp, sftp)
  - zdalna kopia (rsync)
  - tunelowanie (np. aplikacje GUI, X11)



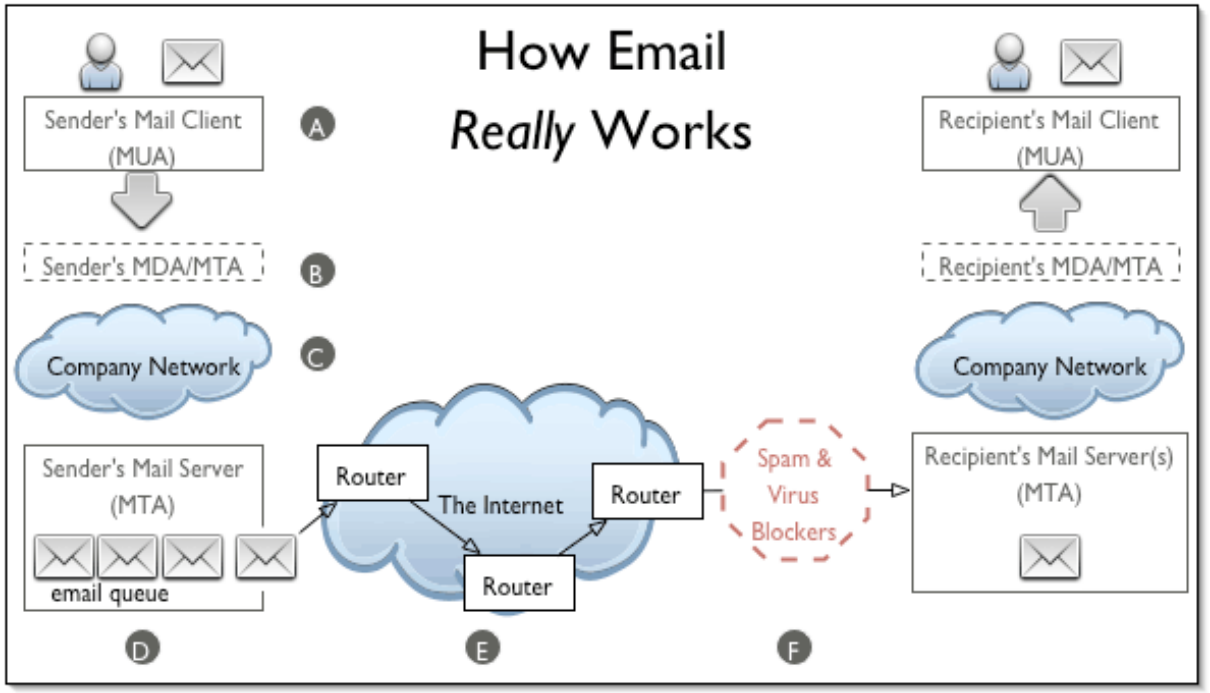


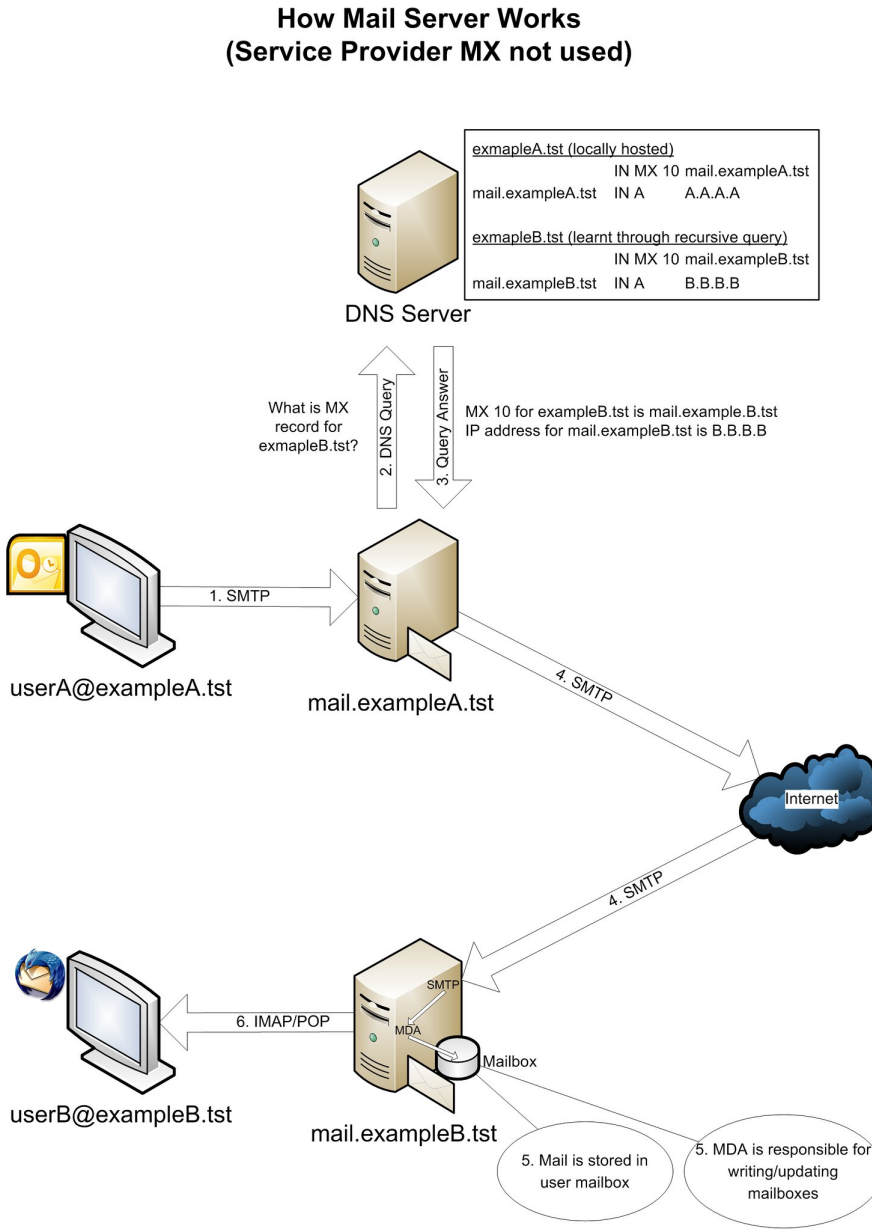
IMAP


IMAP
IMAP Server
IMAP Server
Clients can talk to multiple servers
Multiple clients can talk to the same account on the same server - from anywhere
Mail folders
Mail folders
IMAP Client
Mail folders
Client decides where to store messages. Copy them locally or leave them on the server
IMAP Client
Mail folders
Client has full control over their mail folders. Can create, delete, purge or move them around - even between different accounts on different servers
POP
POP Server
Clients independently download email. Once downloaded it is deleted from the server
POP Client
Mail folders
POP Client
Mail folders

SMTP

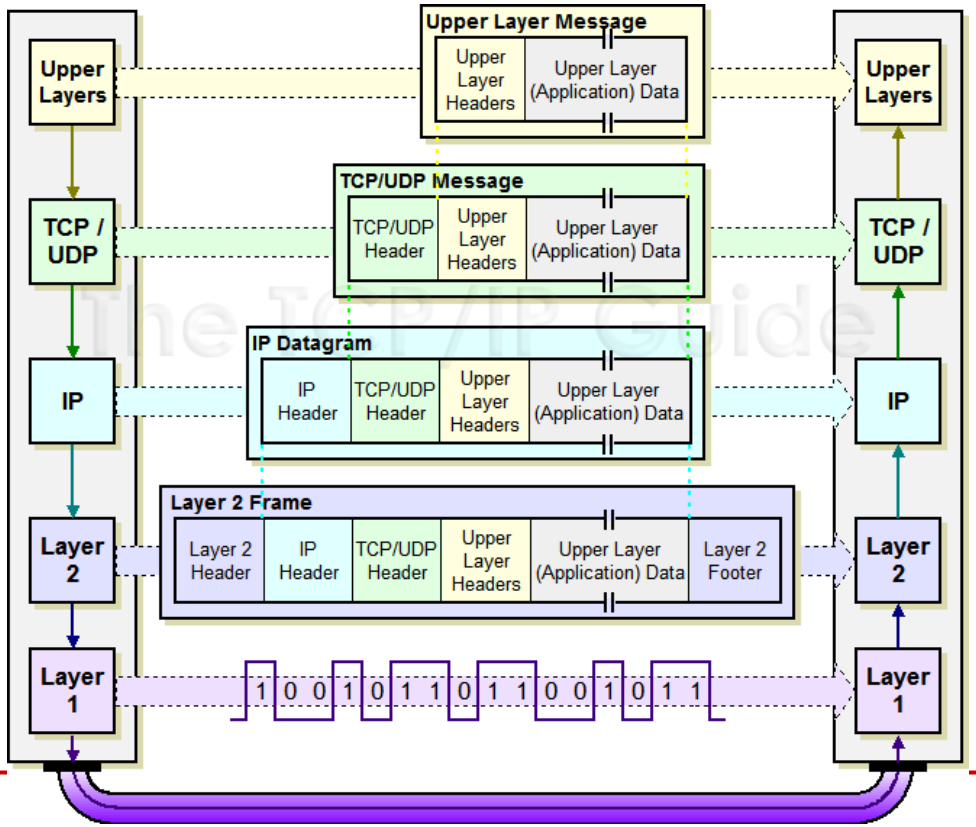
- A w praktyce wygląda to tak:





Inne protokoły

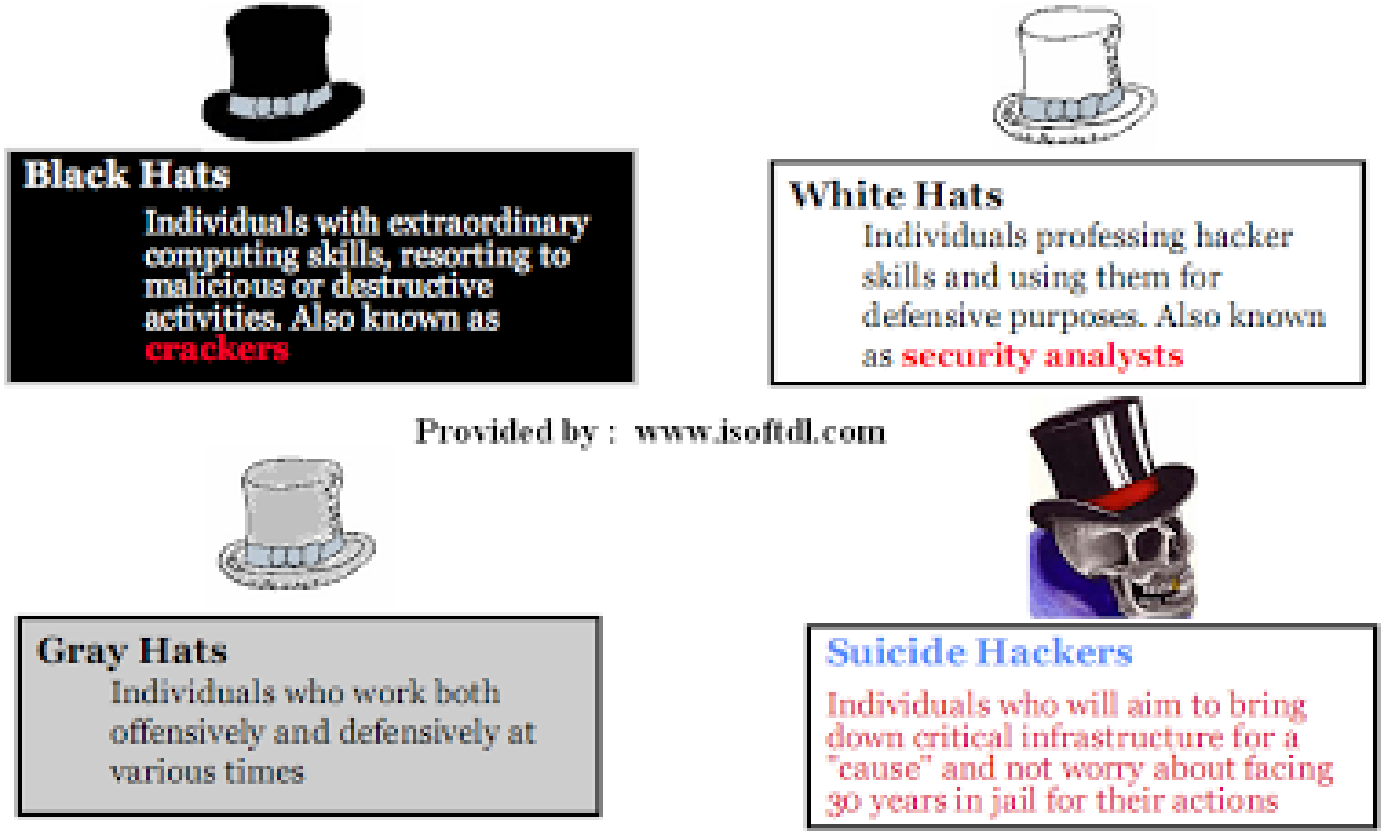
- Protokołów jest oczywiście bardzo dużo
- Pisząc program komputerowy albo korzystamy z już istniejącego (np. nasz klient SSH), albo tworzymy swój własny (np. jakaś gra komputerowa)
- Dane są oczywiście ubierane w nagłówki protokołu (np. HTTP) kapsułkowane do niższych warstw modelu ISO/OSI



Bezpieczeństwo

“Hacker” a “cracker”

- ***Hacker*** to osoba czasami znana z imienia i nazwiska, pasjonat, entuzjasta, zajmuje się badaniem działania oprogramowania i szukaniem błędów, nie tworzy szkód i informuje administratorów
- ***Cracker*** to z kolei osoba, której celem jest działanie destrukcyjne, w celu osiągnięcia korzyści

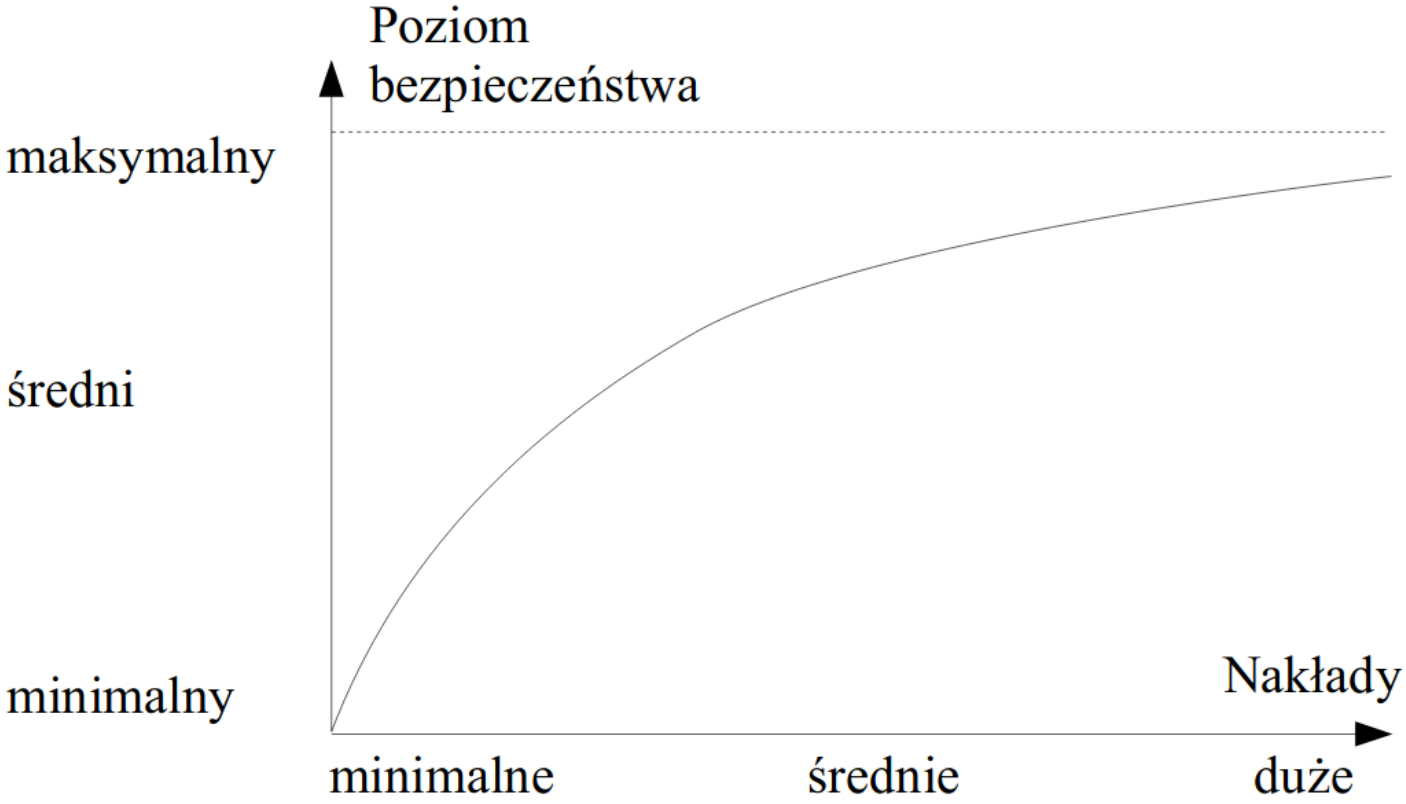


Polityka bezpieczeństwa

- W każdej szanującej się firmie powinien istnieć dokument "***Polityka bezpieczeństwa***"
  - określa, co w firmie powinno być chronione i jakimi metodami
  - powinien definiować procedury postępowania w razie awarii czy włamania
  - powinien być zgodny z normami prawnymi, np. PN-EN ISO/IEC 27001:2017-06
- Równie ważne jest również przestrzeganie ww. dokumentu
  - trzeba wyznaczyć osobę lub osoby odpowiedzialne za wdrażanie dokumentu
  - jasne konsekwencje jego nieprzestrzegania
- Przykładowo – co się stanie w przypadku awarii klimatyzatora w serwerowni?

Poziom bezpieczeństwa

- Poziom bezpieczeństwa jest nieproporcjonalny do poniesionych nakładów
- Minimalne nakłady początkowo powodują znaczące zwiększenie poziomu bezpieczeństwa
- **Nigdy nie da się osiągnąc 100% poziomu bezpieczeństwa**



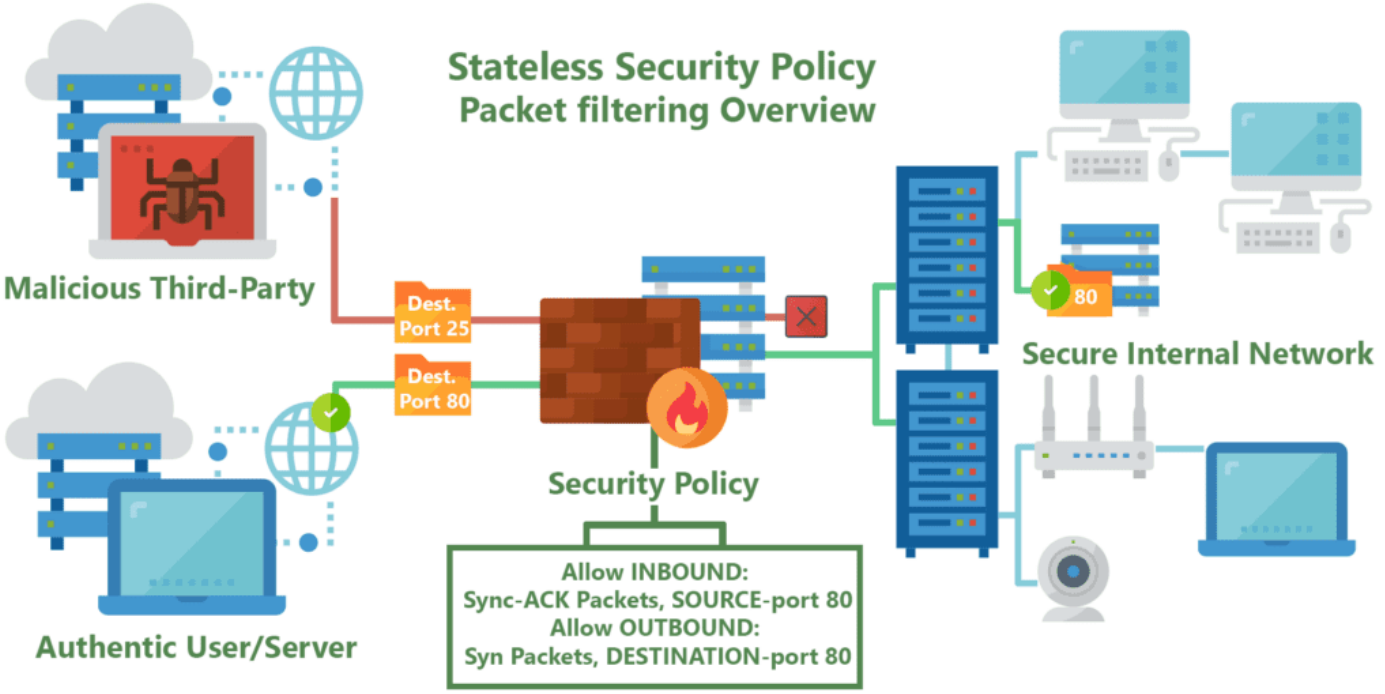
Warstwy TCP/IP a bezpieczeństwo

- W analizie bezpieczeństwa można się oprzeć na warstwach TCP/IP
- Możemy dodać dwie warstwy: zasoby fizyczne oraz człowiek
  - nawet komputer odłączony od sieci może paść ofiarą ataku lub awarii! (np. sprzątaczka z wodą i zalanie)
- Szczegóły różnych ataków – Wykład 6

Warstwa	**Przykłady zagrożeń/ataków**
Zasoby fizyczne	Awaria zasilania, zalanie, pożar, przegrzanie, włamanie lub kradzież, uszkodzenia łączy, nieuprawniony dostęp fizyczny do sprzętu lub infrastruktury
Warstwa dostępu do sieci	Sniffing, arp-spoofing, mac-flooding
Warstwa Internetu	Spoofing, icmp-redirect, icmp-flood
Warstwa transportowa	Skanowanie, DoS, DDoS, DNS-spoofing
Warstwa aplikacji	Buffer overflow, string formatting, SQL injection, wirusy, konie trojańskie, robaki, błędy w skryptach, backdoor
Człowiek	Social engineering, „hasło pod klawiaturą”, nieuwaga

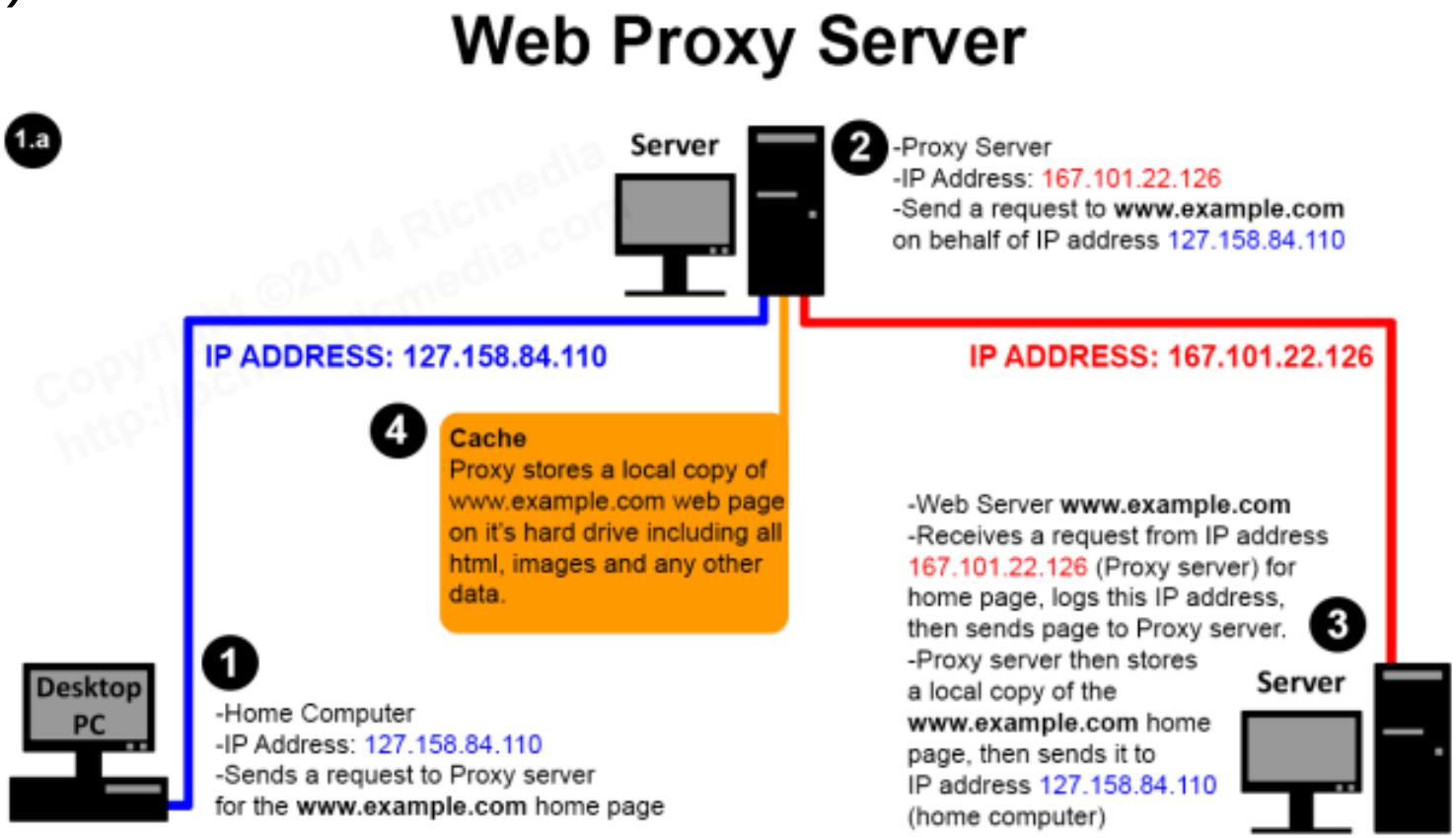
Firewall

- **Firewall** (*zapora ogniowa*) – zabezpieczenie przed próbą podłączenia się do zasobów, które nie powinny być udostępnione:
  - **filtrujący** – dziala w warstwie Internetu na poziomie IP; na podstawie numeru IP oraz numeru portu przepuszcza lub nie dany datagram; bardziej zaawansowane ***firewalle z inspekcją stanu*** (*statefull inspection*) mogą kontrolować całą sesję i korzystają również z wyższych warstw



Firewall

- **połączeniowy** – zestawiają połączenia pomiędzy siecią lokalną a Internetem wg określonych reguł, np. poprzez *serwery proxy*
  - **serwer połączeniowy** (*proxy*) – wykonują połączenia sieciowe zamiast komputera sieci lokalnej; najczęściej udostępnianie WWW, ale możliwe też inne usługu (uwaga na strony dynamiczne, np. PHP)



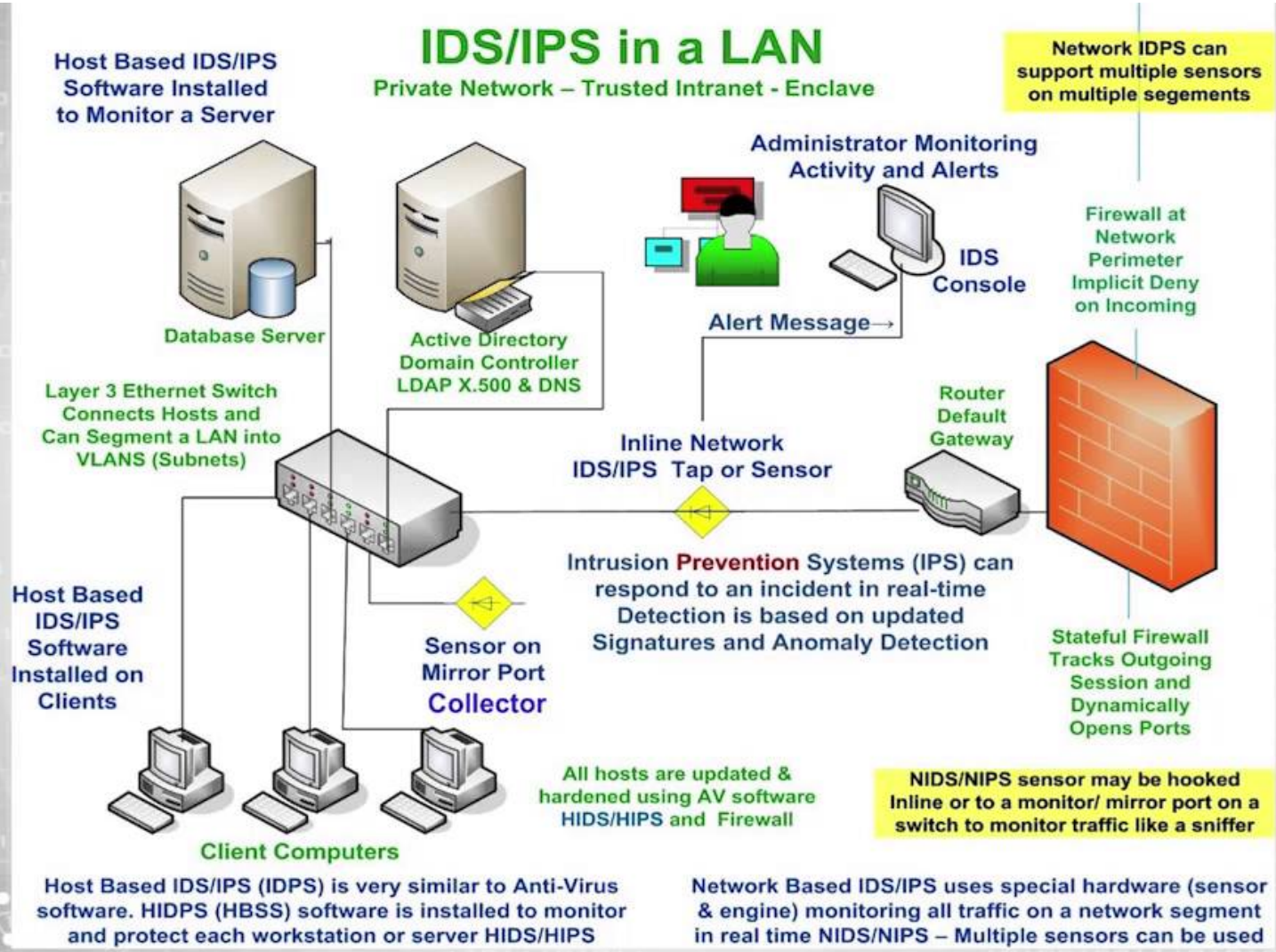
Inne technologie bezpieczeństwa

- **NAT** – to już znamy, translacja adresów IP sieci wewnętrtznej i adresy nieroutowalne – sieć lokalna widoczna pod zupełnie innymi adresami
  - ataki na sieć lokalną zostaną “przejęte” przez serwer NAT, który powinien być lepiej zasbezpieczony niż komputery klienckie
- **Kryptografia** – szyfrowanie połączeń oraz wiadomości (w tym klucze publiczne i prywatne, certyfikaty)
- **VPN** (*Virtual Private Network*) – wirtualne sieci prywatne, sieć transmitująca prywatne dane przez infrastrukturę telekomunikacyjną – z reguły taka usługa u operatora kosztuje; dostawca usług wydziela w swojej sieci połączenie (między naszymi routerami granicznymi), które będzie należało do nas i to od nas zależy co i jak prześlemy – połączenie z VPN szyfrowane

IDS i IPS

- **IDS** (*Intrusion Detection System*) – urządzenie lub program służący do wykrywania prób włamań do zasobów chronionych; np. złodzieje mogą wykorzystać luki w oprogramowaniu (np. w naszym firewall). Dzielimy je na kilka rodzajów:
  - **Host IDS** (*systemowy IDS*) – analizuje pracę systemu operacyjnego
  - **Network IDS** (*sieciowy IDS*) – analizuje ruch sieciowy i wykrywa odstępstwa
  - **Network Node IDS** (*IDS stacji sieciowej*) – system instalowany na poszczególnych stacjach sieciowych i analizuje jedynie ruch na tej stacji, najczęściej stosowany w VPN
- **IPS** (*Intrusion Prevention System*) – system aktywnej reakcji na ataki i następnie raportują co się stało (człowiek nie jest w stanie odpowiednio szybko zareagować)

IDS i IPS



SKILLSET

Ataki – rozpoznanie sieci

Załóżmy, że chcemy włamać się do sieci wewnętrznej firmy XYZ

1) ***Analiza zasobów Internetowych*** (strony oficjalne, for a internetowe – może np. na forum ktoś szukał pomocy o systemie operacyjnym → wiemy czego używają) → obrona: **zdrowy rozsądek**

2) ***Inżynieria społeczna*** – podszywanie się pod osoby upoważnione i uzyskiwanie dostępu do sieci (np. telefon do jakiegoś działu i prośba o hasło) → obrona: **zdrowy rozsądek i szkolenie pracowników**

3) ***Analiza DNS i użycie*** *whois* – można dzięki temu znaleźć zakres IP przydzielonych firmie, dane administratora czy dostawcę Internetu

4) ***Mapowanie sieci*** – uzyskiwanie listy aktywnych numerów IP i topologii połączeń poprzez ICMP (ping) oraz tracerout → obrona: blokowanie ICMP, IDS

Ataki – bezpieczeństwo

- Polecam również bieżącą lekturę strony niebezpiecznik.pl

- Najwięcej włamań wynika z błędu ludzkiego (np. Kliknięcia na zły link w e-mailu, czy błędach administratorów)

9:20 18/4/2019 Facebook wyłudził 1,5 mln haseł do e-maili po czym "niechcący" wykradł użytkownikom książki kontaktowe

10:52 4.4.2019 Pociekły dane 540 mln użytkowników Facebooka, ale ich administrator nie spieszył się z reakcją

14:19 3.4.2019 To nie był "wyciek" tylko "błąd ludzki"? Dlaczego warto separować kod od danych

14:58 28.3.2019 Domyślny PIN umożliwił kradzież 120 tys. litrów paliwa
Autor: Marcin Maj | Tagi: dystrybutory paliwa, Francja, klucze, paliwo, PIN, stacje benzynowe, USA

11:33 25.3.2019 Chcesz oddać lub sprzedać dysk? Nie myśl, że sprzedawca go bezpiecznie wyczyści

21:01 21.3.2019 Hasła 600 milionów użytkowników Facebooka były dostępne bez szyfrowania. Przez przypadek…

20:40 4.3.2019 [AKTUALIZACJA #2] Rządowy serwis loterii paragonowej serwuje porno w domenie gov.pl i ujawnia masowy, globalny atak na "porzucone" domeny
Autor: redakcja | Tagi: Hacked!, loteria paragonowa, pornografia

19:35 16.11.2019 Zgubiono laptopa z danymi setek tysięcy studentów SGGW
Autor: redakcja | Tagi: dane osobowe, kradzież, kradzież

12:08 29.10.2019 [AKTUALIZACJA] Serwerownia pod wanną emeryta zalana. Starty: 400 000 PLN
Autor: redakcja | Tagi: śmieszne, UPC, woda, wycieki

Ataki – bezpieczeństwo

20:05
10/2/2019

Jak ukraść miliony z polskich firm jednym e-mailem lub listem?

Tuż przed weekendem RMF poinformowało o tym, że należąca do **Polskiej Grupy Zbrojeniowej** spółka **Cenzin** straciła **4 miliony złotych** bo — na podstawie "fałszywego" maila od kontrahenta — pieniądze przelała na złe konto. Ta metoda kradzieży w internecie jest stara jak świat. Na niebezpiecznikowych szkoleniach dla firm przestrzegamy przed nią od ponad 9 lat! Ale niestety, tego typu ataki regularnie powracają, a straty prawie zawsze idą w co najmniej **setki tysięcy złotych**. W tym artykule, chciałbym więc zwrócić Wam uwagę na to **jak wykryć tego typu przekręty** oraz co zrobić, żeby Twoja firma nie była kolejną, która pośle miliony złodziejom…

- 560 000 zapłaciło warszawskie metro za usługi sprzątania komuś, kto podszył się pod firmę Impel i "podmienił" numer rachunku sfałszowanym pismem.
- 3,7 miliona złotych przelał złodziejom Podlaski Zarząd Dróg Wojewódzkich, bo podszyli się pod wykonawcę Unibep i na piśmie z prośbą o zmianę numeru rachunku umieścili pieczątkę, a urzędnicy w pieczątki wierzą…

Nie tylko Polacy mają problemy z takimi oszustwami. Za granicy nazywa się je mianem Business Email Compromise, a rekordzistą jest firma z branży …bezpieczeństwa: **Ubiquiti**. Ten znany producent urządzeń sieciowych złodziejom przelał aż 46,7 milionów dolarów. Ciekawy był też przypadek firmy Ryanair, która za paliwo zapłaciła 5 milionów euro nie temu, komu powinna.

Zaliczenie

- Zaliczenie tylko na podstawie projektów (2x15 pkt) oraz testu z wykładu (20 pkt)
- Suma punktów **50**
- Test wykładowy:
  - platforma Moodle
  - 20 pytań **zamkniętych**
  - pytania losowane z bazy pytań (każdy student będzie miał różne pytania)

Protokół IMAP:

a. służy do wysyłania wiadomości e-mail

b. służy do odbierania wiadomości e-mail

c. jest bardziej zaawansowany od POP3

d. wszystkie powyższe

*Protokół TCP względem UDP **nie** jest:*

a. wolniejszy

b. mniej wiarygodny

c. bezpołączeniowy

d. wszystkie powyższe


WYDZIAŁ FIZYKI
POLITECHNIKA WARSZAWSKA
POLITECHNIKA WARSZAWSKA
WARSAW UNIVERSITY OF TECHNOLOGY

KONIEC