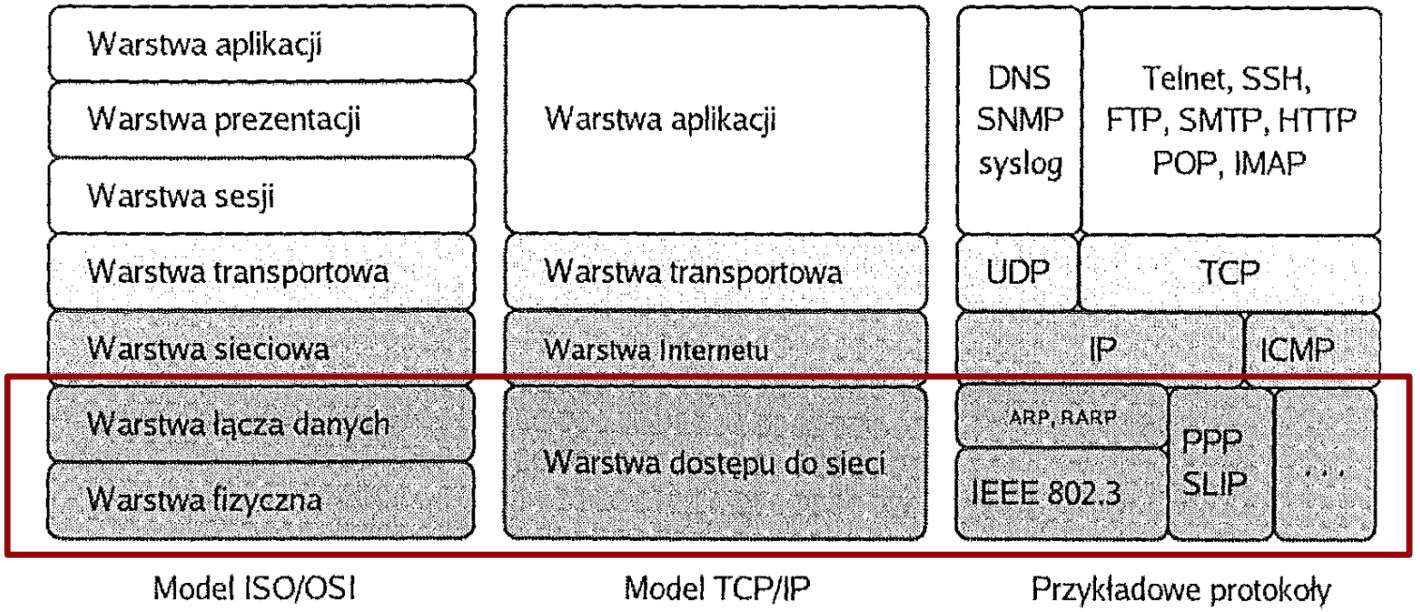
Sieci komputerowe

Wykład 3
10.03.2021

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

Semestr letni 2020/2021

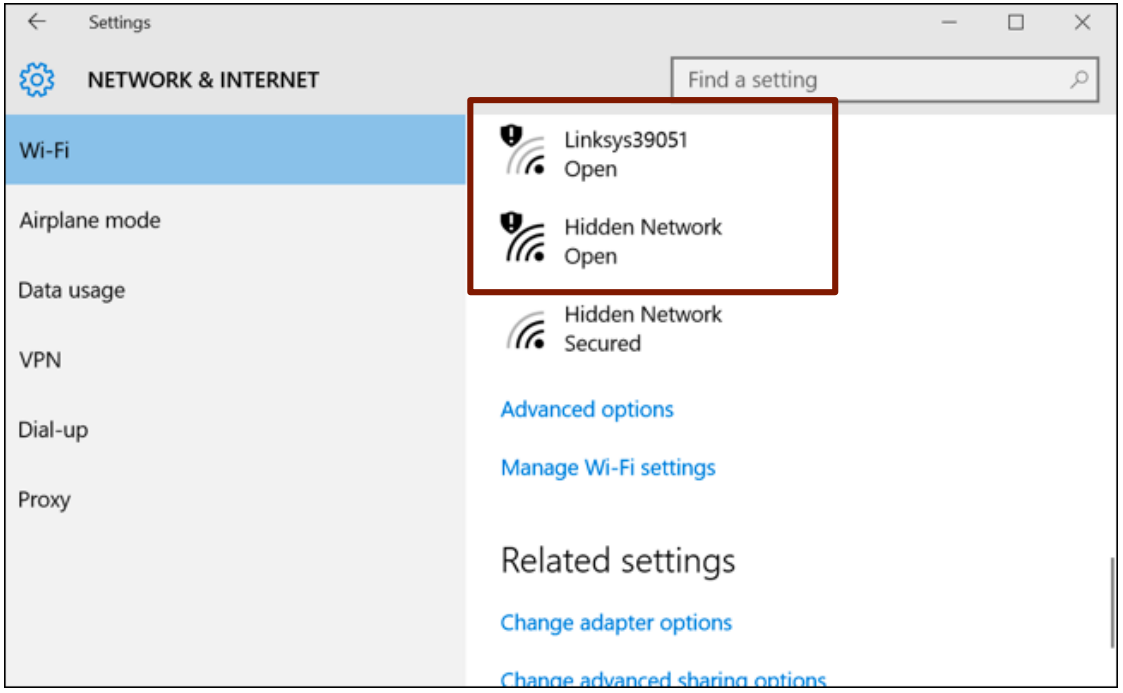
Warstwa dostępu do sieci przypomnienie

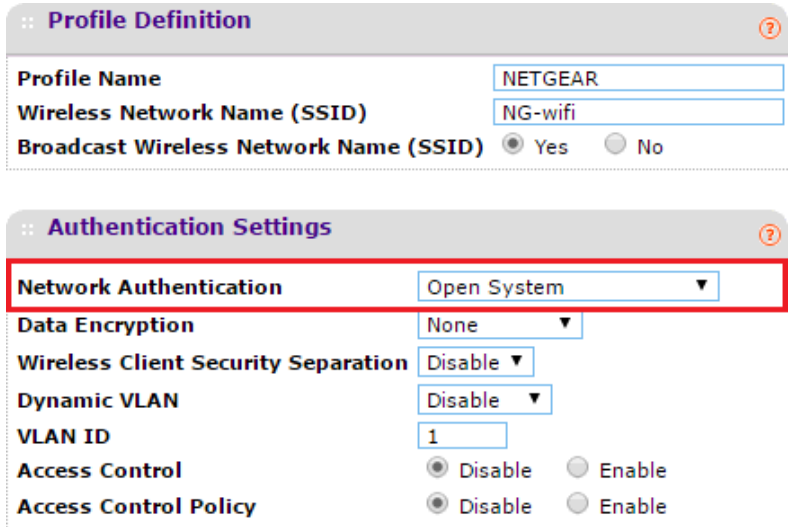


źródło: Helion

WiFi – połączenie i uwierzytelnianie

- Połączenie jest dokonywane poprzez wysłanie parametrów stacji do AP
- W standardzie 802.11 zakładamy wiarygodność AP (wada → można stworzyć fałszywy AP) i uwierzytelnianie samego AP spada na stację
- Uwierzytelnianie może być typu **open-system** (**OSA – Open System Access**) lub **shared-key**

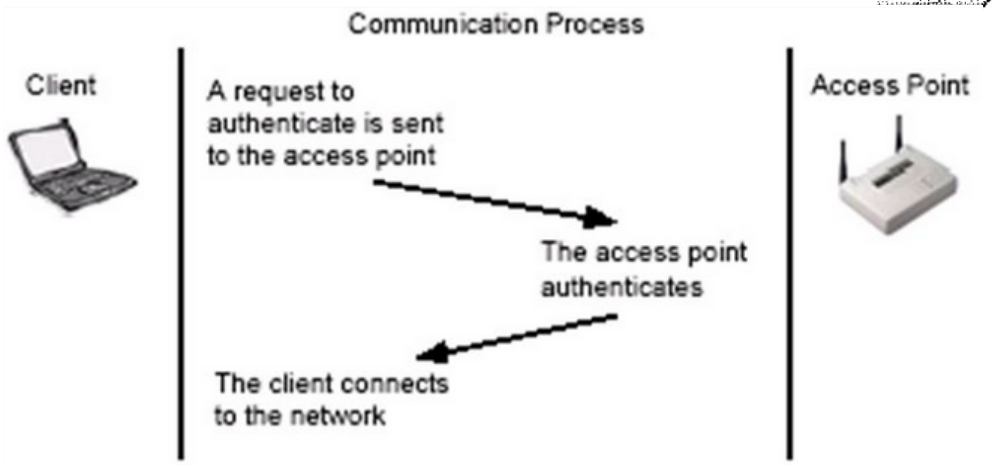


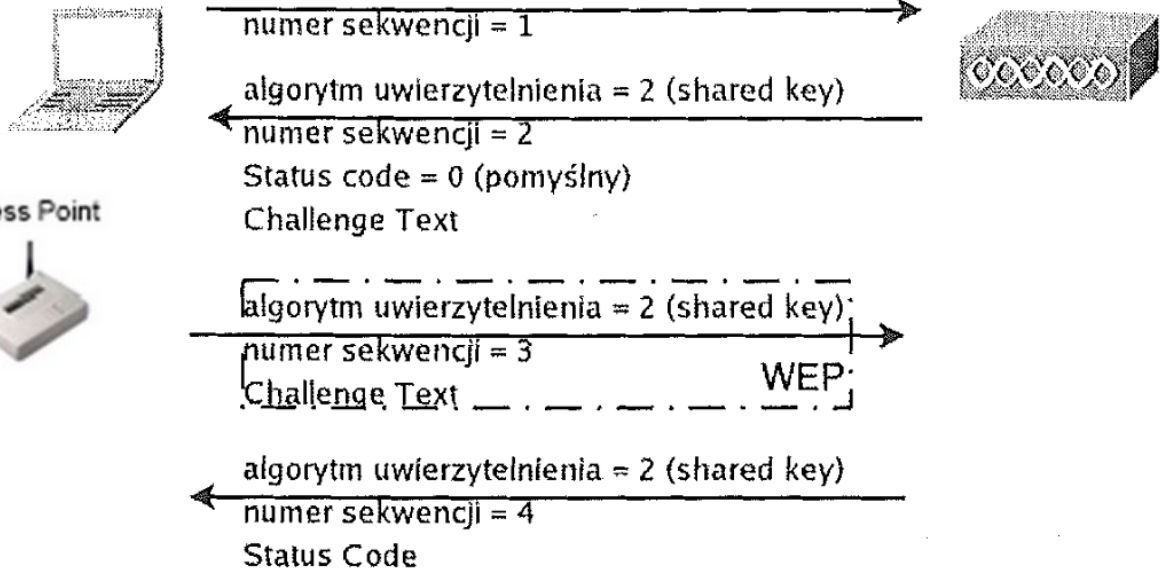


WiFi – połączenie i uwierzytelnianie

- W ***shared-key*** przy odpowiedzi AP zostaje dołączone do ramki pole **Challange Text**, np. ma 128 losowych bajtów. W trzecim kroku stacja odsyła zaszyfrowane pole *Challange Text* (np. WEP) i jeżeli AP odszyfruje tekst i zgadza się on z wysłanym wcześniej, to akceptuje stację
- Po uwierzytelnieniu stacja wysyła **AR** (*Assosiation Request*) i dostaje od AP **AID** (*Association ID*) → kojarzenie (powiązanie)

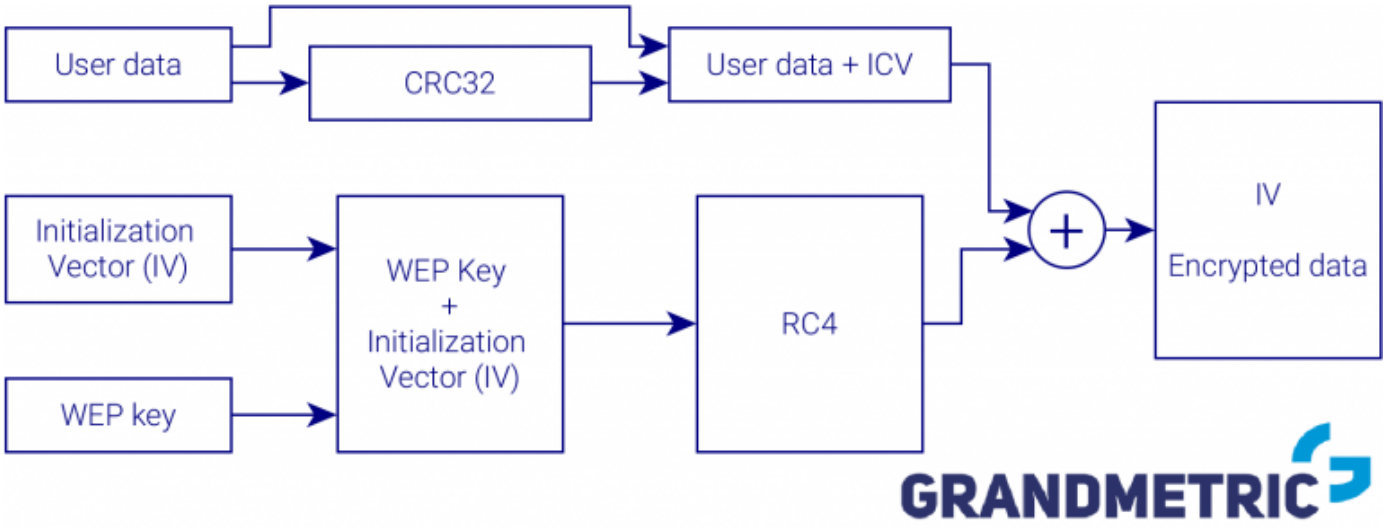
Rysunek 4.10.
Uwierzytelnianie typu shared-key





WiFi – szyfrowanie

- Historycznie używany był protokół **WEP** (*Wired Equivalency Privacy*)
- Do ramki 802.11 jest dodawane odpowiednie pole z kluczem szyfrującym
- Jest zupełnie nieodporny na ataki – łatwo złamać poprzez podsłuchanie 1-2 milionów ramek (darmowe narzędzia)
- Użycie protokołu pooduje zwiększenie długości ramki (mniejsza wydajność)

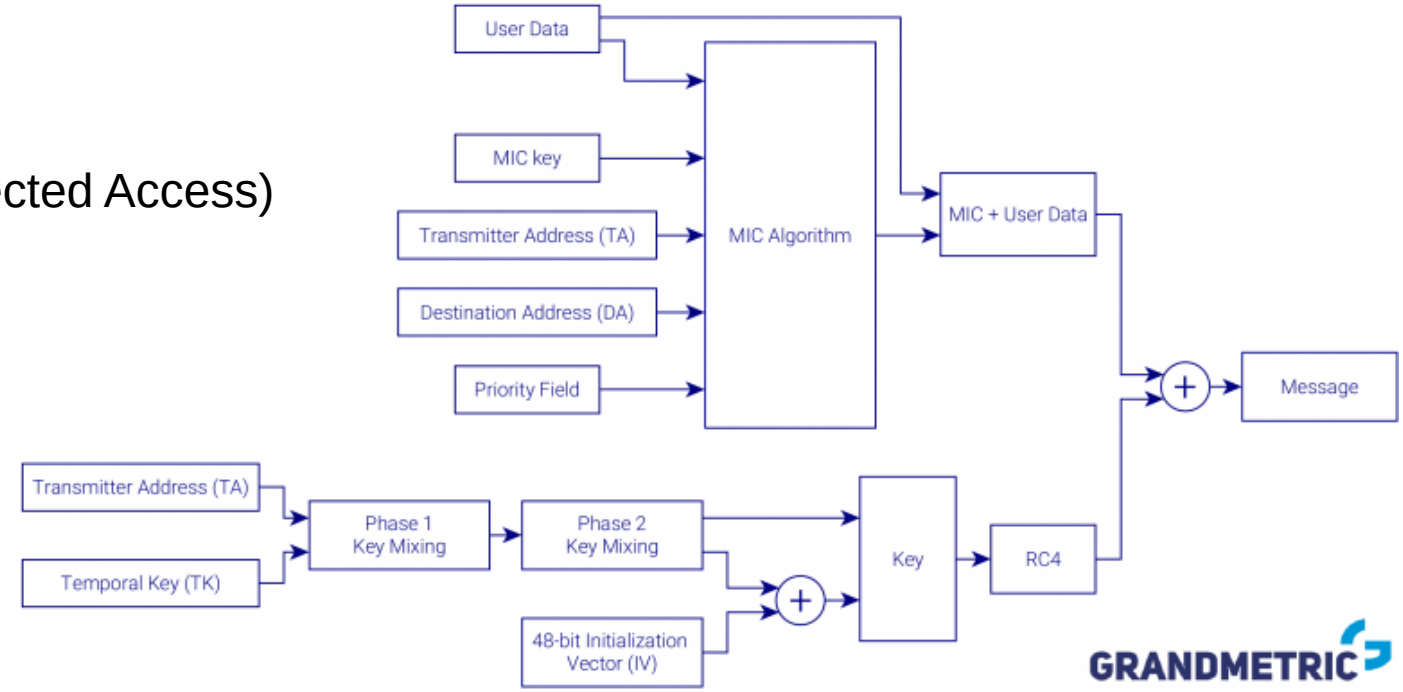


Problemy z WEP

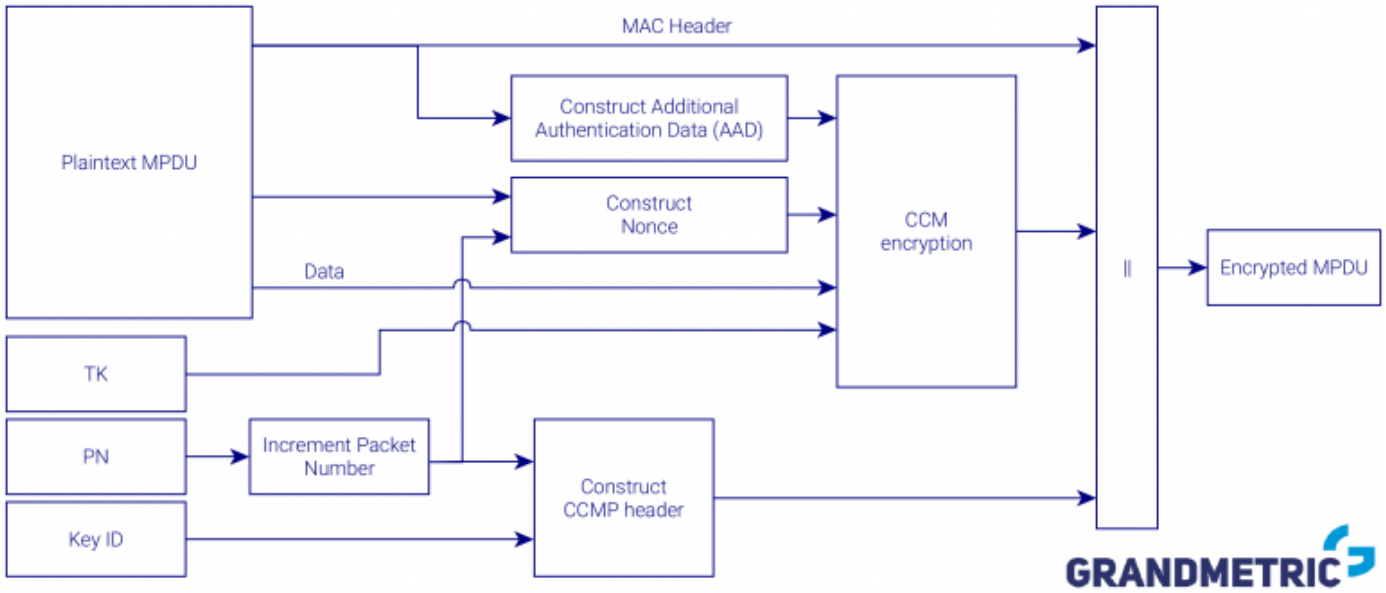
1. Klucze szyfrujące muszą być ręcznie skonfigurowane na każdym z komunikujących się urządzeń. Nastręcza to wiele problemów. Głównym jest zapewnienie poufnego transportu klucza. Często się zdarza, że pracownik korzystający z sieci WLAN dostaje od administratora klucz i sam go sobie wpisuje w konfiguracji karty sieciowej. A co z przypadkiem, gdy ten pracownik odejdzie z firmy? Należałoby zmienić klucz na wszystkich stacjach korzystających z sieci WLAN. Dodatkowo powinna zostać wdrożona (tak jak z innymi hasłami) procedura okresowej zmiany klucza. Jednak najczęstszą praktyką — ze względu na dużą uciążliwość zmiany — jest pozostawianie kluczy bez modyfikacji przez długie miesiące.
2. Wielu administratorów korzysta ze słabszych kluczy 40-bitowych — głównie dlatego, że są łatwiejsze do zapamiętania, gdy trzeba skonfigurować wiele urządzeń.
3. W 2001 roku pojawiły się opracowania naukowe opisujące metody „łamania" kluczy wykorzystujące słabości w algorytmie WEP. Okazało się, że po podsłuchaniu dużej ilości danych (wystarczy ok. 1 – 2 miliony ramek) można za pomocą algorytmów o mniejszej sile obliczeniowej niż użyty do kodowania odkryć klucz WEP. Niebawem pojawiło się darmowe, ogólnodostępne oprogramowanie do wykonywania takich działań.
4. Autoryzacja stacji użytkowników odbywa się poprzez weryfikację adresu MAC. Zmiana adresu MAC stacji radiowej jest dziecinnie prosta, nawet w systemach Windows.
5. Każdy z użytkowników sieci WLAN może podsłuchiwać innych (z różnym skutkiem, w zależności od odległości) transmitujących z tym samym kluczem WEP. WEP nie zabezpiecza przed podsłuchaniem transmisji sąsiada, traktując wszystkich użytkowników sieci bezprzewodowej jak rodzinę.

WiFi – szyfrowanie

WPA
(Wi-Fi Protected Access)

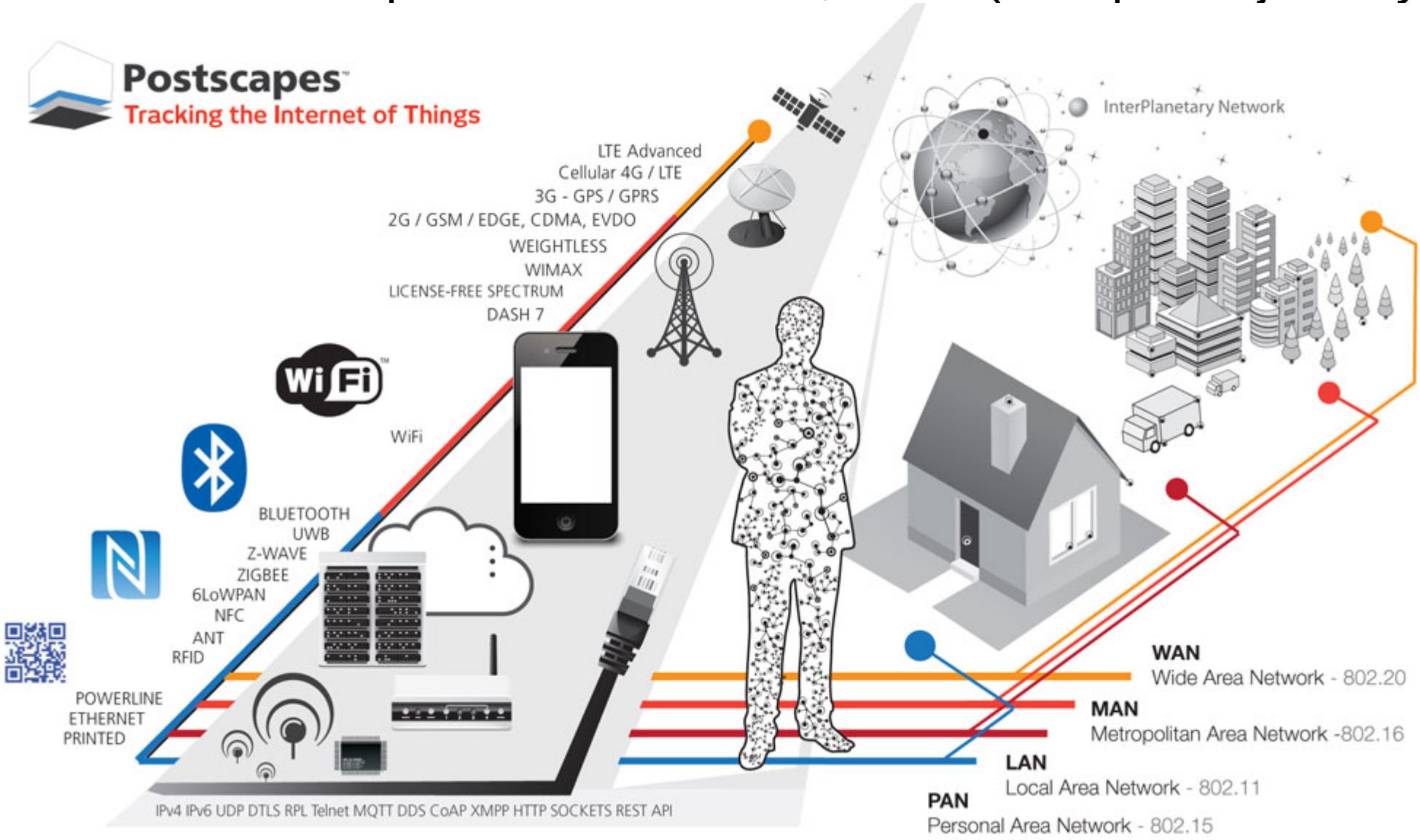


WPA2



Warstwa dostępu do sieci - przypomnienie

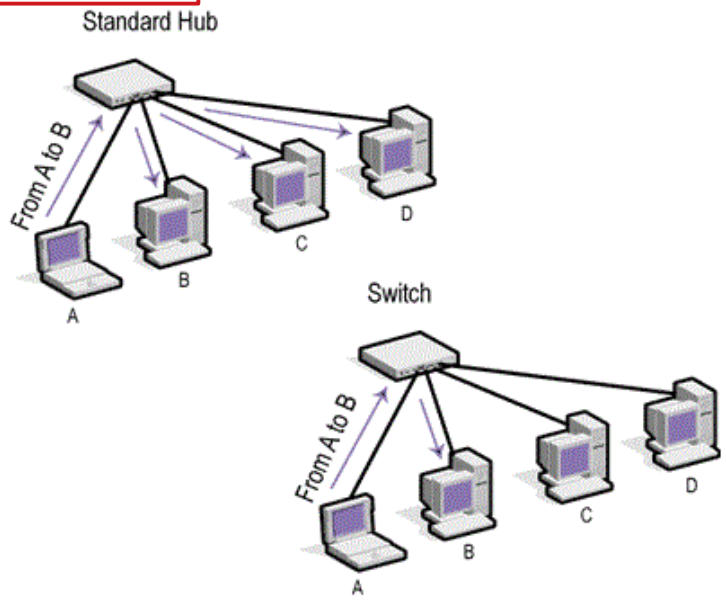
- Różne standardy (Ethernet, WiFi, WiMax, LTE, itp.) - zdefiniowane np. w normach IEEE, ramki (enkapsulacja danych)



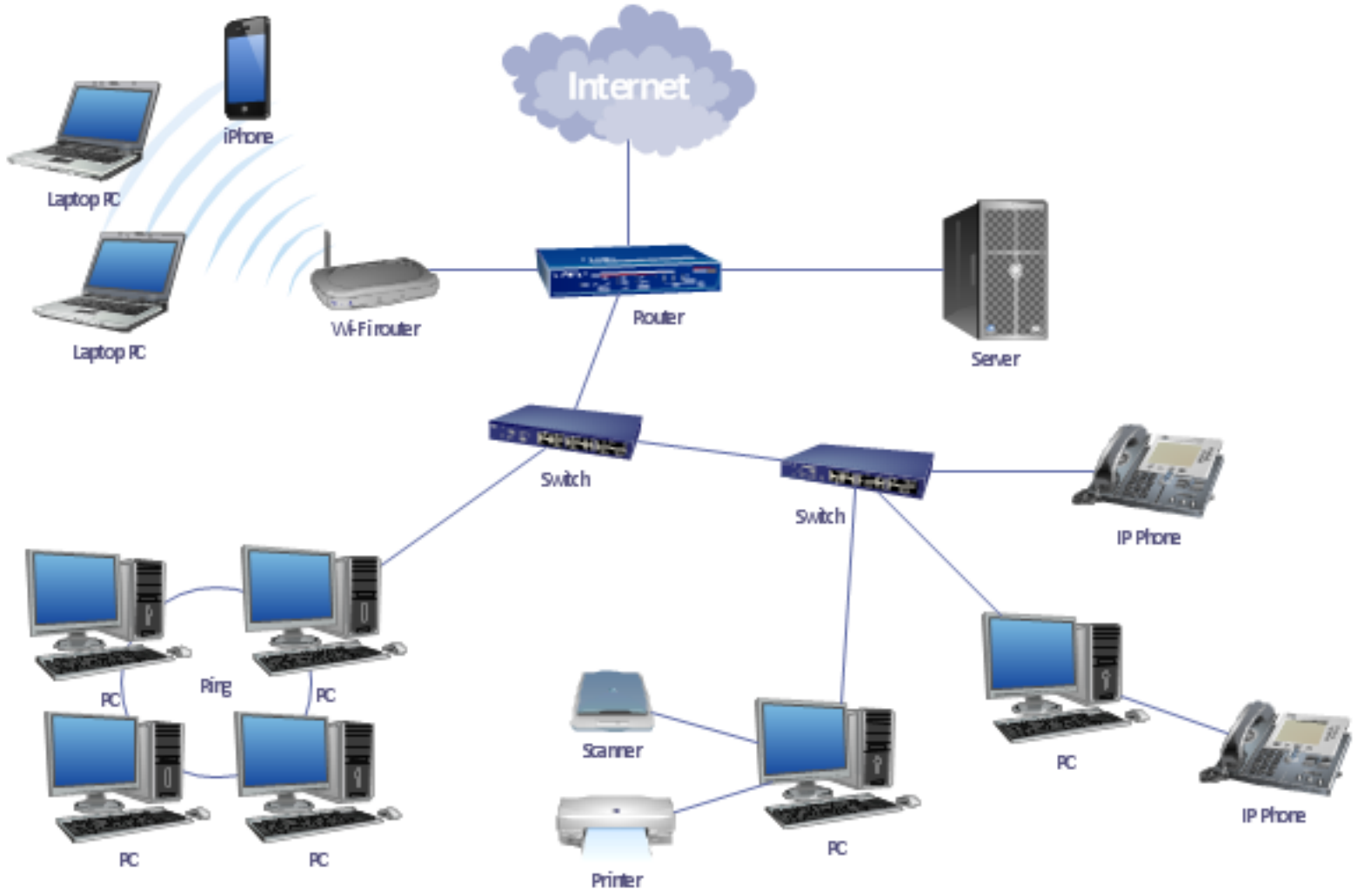
Hub vs switch vs router

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.			

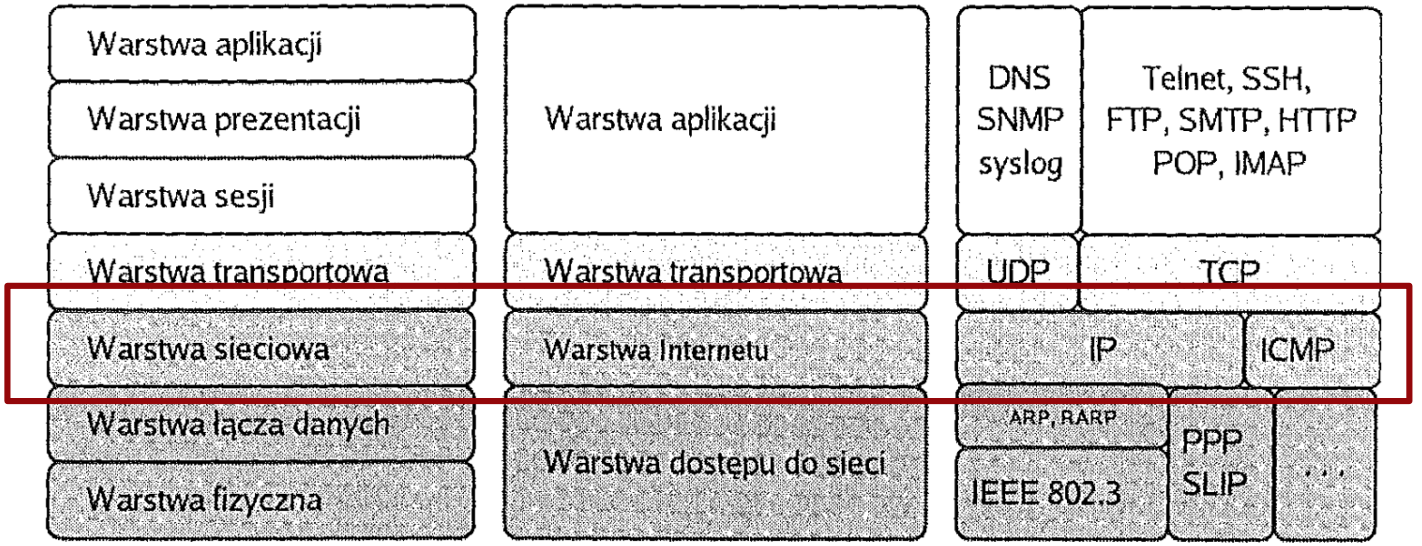
- Hub przekazuje sygnał z jednego portu do wszystkich pozostałych (broadcast) – **działa w warstwie fizycznej**
- Switch przekazuje sygnał do wybranego adresata na podstawie MAC adresu – **działa w warstwie łącza danych**



Hub vs switch vs router



Warstwa Internetu



źródło: Helion

Krótka (polska) historia Internetu

- Swoją cegiełkę do historii rozwoju Internetu dołożył Polak z pochodzenia – Paweł (Paul) Baran
- Urodzony 26.04.1926 r. w Grodnie (teraz Białoruś)
- Wyemigrował do Bostonu w 1928 roku.
- Ukończył Drexel University a następnie UCLA (University of California, Los Angeles)
- Pracował w RAND Corporation – naukowej organizacji non-profit prowadzacej badania w matematyce i informatyce (pierwotnie na potrzeby wojska)
- W czasie gdy pracował w niej Baran, RAND Corproration skupiała się na sprawach związanych z Zimną Wojną

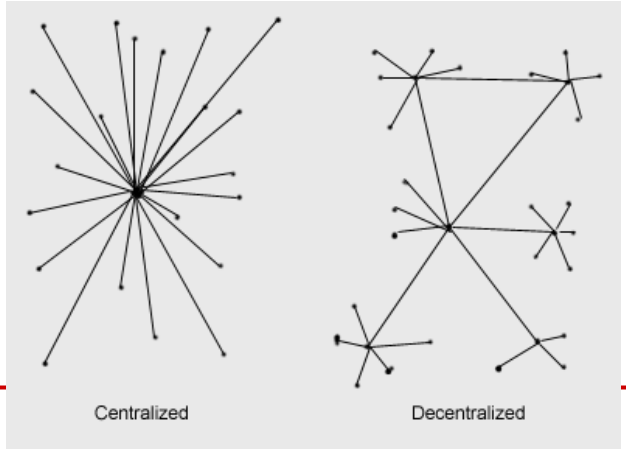
http://ibiblio.org/pioneers/baran

Krótka (polska) historia Internetu

- Baran w RAND Corp. prowadził badania nad siecią, komputerową, która przetrwałaby atak nuklearny
- Sieć taka łączyłaby skupiska ludzkie w epoce post-apokaliptycznej

"Both the US and USSR were building hair-trigger nuclear ballistic missile systems. If the strategic weapons command and control systems could be more survivable, then the country's retaliatory capability could better allow it to withstand an attack and still function; a more stable position. But this was not a wholly feasible concept, because long-distance communication networks at that time were extremely vulnerable and not able to survive attack. That was the issue. Here a most dangerous situation was created by the lack of a survivable communication system." (Baran in Abbate, 10).

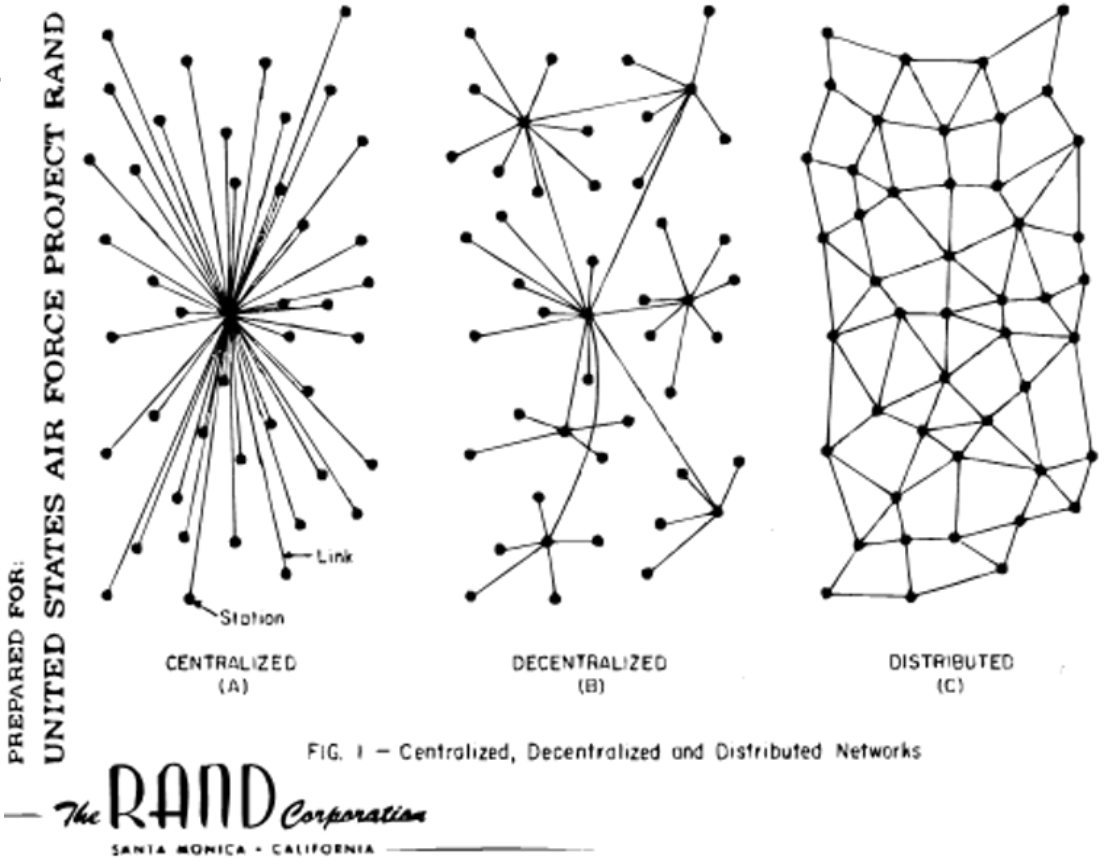
- Idea polegała na stworzeniu bardziej odpornej sieci komunikacyjnej w oparciu o ideę **redundacji** (*redundancy*)
- W owym czasie – sieci komunikacyjne scentralizowane i zdecentralizowane



http://ibiblio.org/pioneers/baran

Krótka (polska) historia Internetu

- Baran zaproponował trzeci model – sieci rozproszonej (**distributed network**)
- W sieci rozporoszonej nie ma jednego centralnego węzła i każdy węzeł jest podpięty do kilku innych
- Taka konfiguracja pozwala na wiele możliwych dróg komunikacji
- Znieszczenie jednego węzła nie blokuje całej sieci



http://ibiblio.org/pioneers/baran

Krótka (polska) historia Internetu

- Drugą ideą zaproponowaną przez Barana było dzielenie wiadomości na bloki przed wysłaniem ich w sieć
- Bloki byłyby wysyłane osobno i następnie łączone w całość w węźle docelowym – **komutacja pakietów**
  - jeżeli mamy linię telefoniczną i akurat przerwę w rozmowie, nikt inny z tej linii korzystać nie może – tracimy zasoby
- Baran wymyślił sieć węzłów, które by działały na zasadzie przesyłania sobie nawzajem pakietów (**routing**) na trasie do celu (ostateczny węzeł). Węzły mogłyby zbierać dane o ruchu w sieci i wysyłać pakiety najlepszą (najmniej obciążoną drogą) – taka metoda nazywana jest **dynamic routing**
- System został nazwany przez Barana **hot-potato routing**

http://ibiblio.org/pioneers/baran

Krótka (polska) historia Internetu

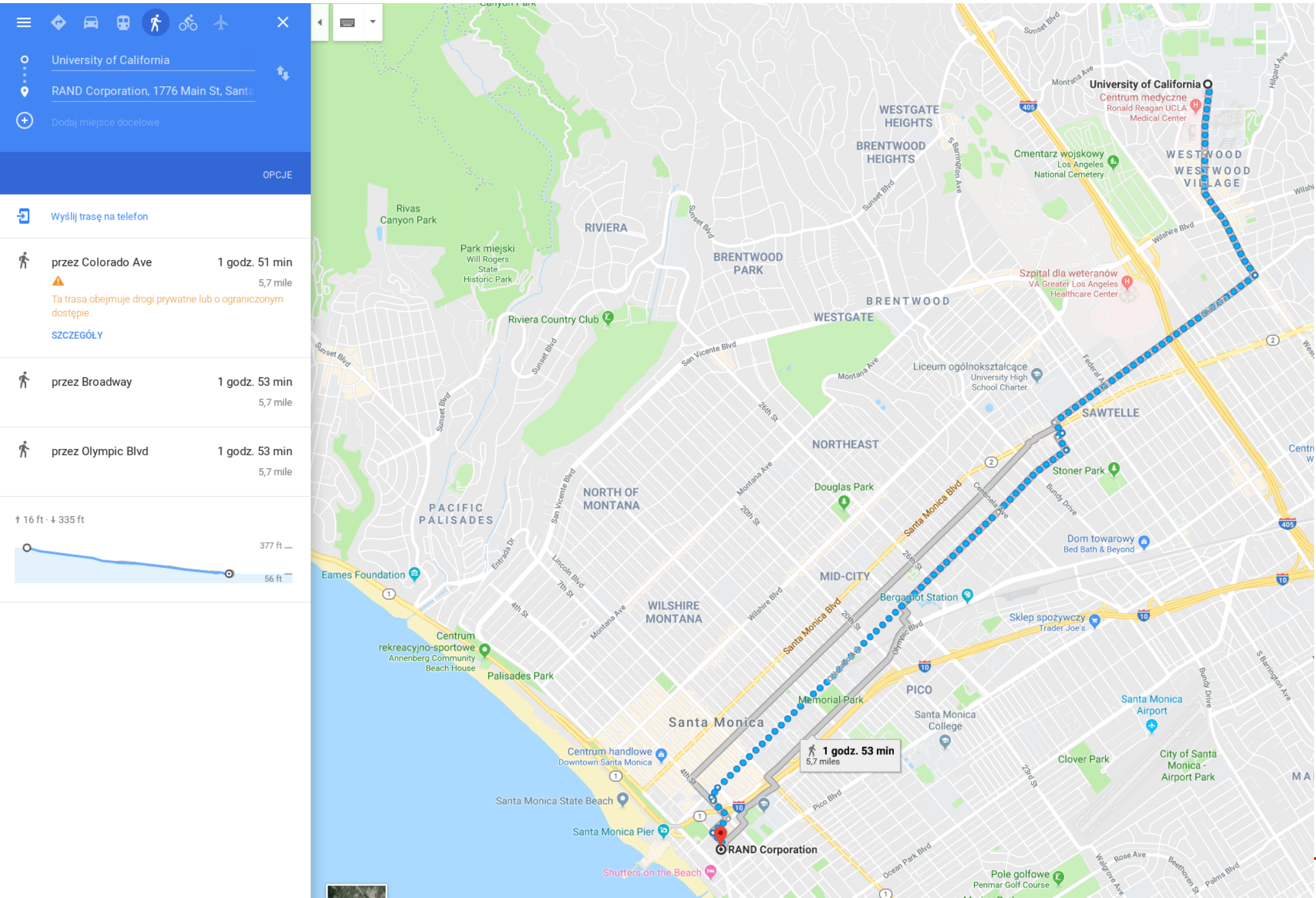
- Paweł Baran opisał wszystkie swoje badania w **12(!) tomowej** monografii

  “On distributed communication networks.”
  Rand Corporation Document Series, 1964

- Początkowo US Army nie było mocno zainteresowane wynikami Barana
- Dopiero w 1969 roku koncepcja została przetestowana na 7 węzłach między UCLA i RAND w Santa Monica
- Na początku lat 70 Larry Roberts, rozpoczynając prace nad ARPANET, usłyszał o ideach Barana
- Idea sieci rozproszonej oraz oraz routingu dynamicznego stały się kluczową częścią ARPANET

http://ibiblio.org/pioneers/baran

Krótka (polska) historia Internetu



Protokół IP

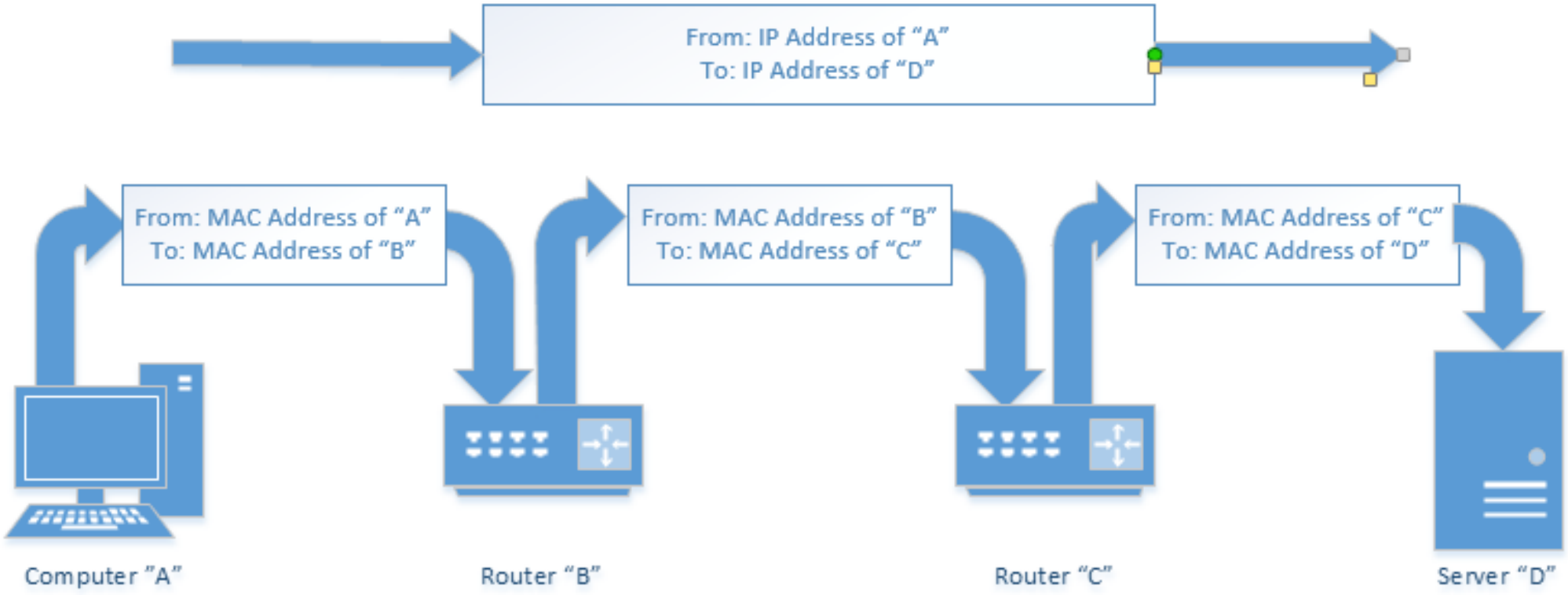
- Główną częścią warstwy Internetu jest protokół **IP** – *Internet Protocol* (protokół transportowy w Internecie)
- IP zapewnia przenoszenie danych pomiędzy odległymi węzłami
- Jednostką przesyłanej informacji jest **pakiet**, ale formalnie poprawnie (zgodnie ze standardem) powinniśmy mówić o **datagramach** 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.

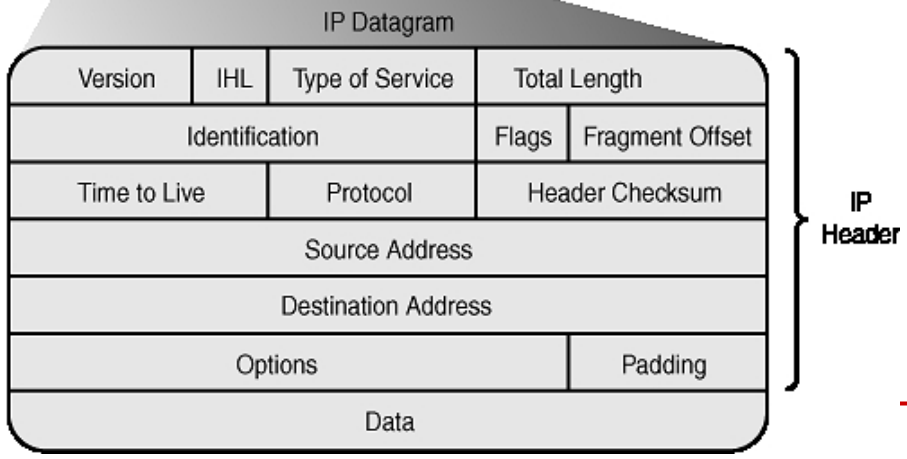
https://askleo.com/whats_the_difference_between_a_mac_address_and_an_ip_address/



Protokół IP

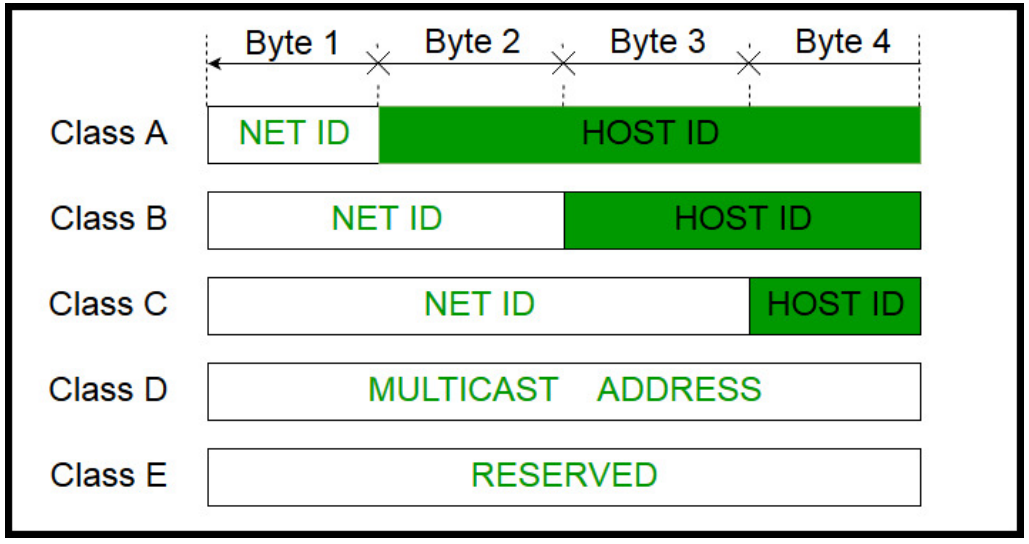
- Czego IP nie robi:
  - jest **protokołem bezpołączeniowym** – nie nawiązuje połączenia (tj. nie sprawdza gotowości do odbioru)
  - jest **protokołem niepewnym** – nie zapewnia korekcji i wykrywania błędów transmisji
- IP "jedynie" definiuje jednostkę przesyłanej informacji (datagram), sposób adresacji 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

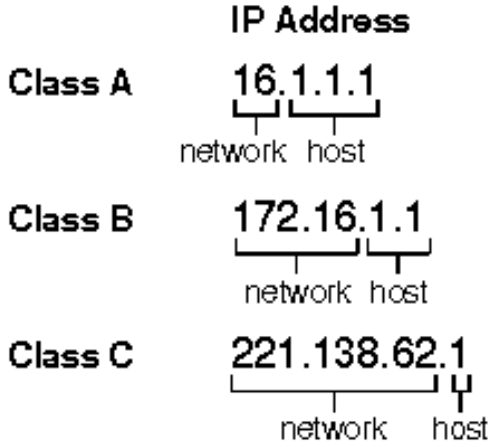


	Range for first byte
Class A	0 - 127
Class B	128 - 191
Class C	192 - 223
Class D	224 - 239
Class E	240 - 255

Adresowanie IP

- W każdym numerze IP część cyfr odpowiada za numer sieci, a część za numer hosta

	1st octet	2nd octet	3rd octet	4th octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host
Class A or /8	11111111	00000000	00000000	00000000
Class B or /16	11111111	11111111	00000000	00000000
Class C or /24	11111111	11111111	11111111	00000000



- Im więcej bitów przeznaczonych na hosty, tym więcej urządzeń możemy podłączyć

Zanalizujmy przykładowy adres klasy C:

110x xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx

21 bitów = 2^{21} > 2M sieci

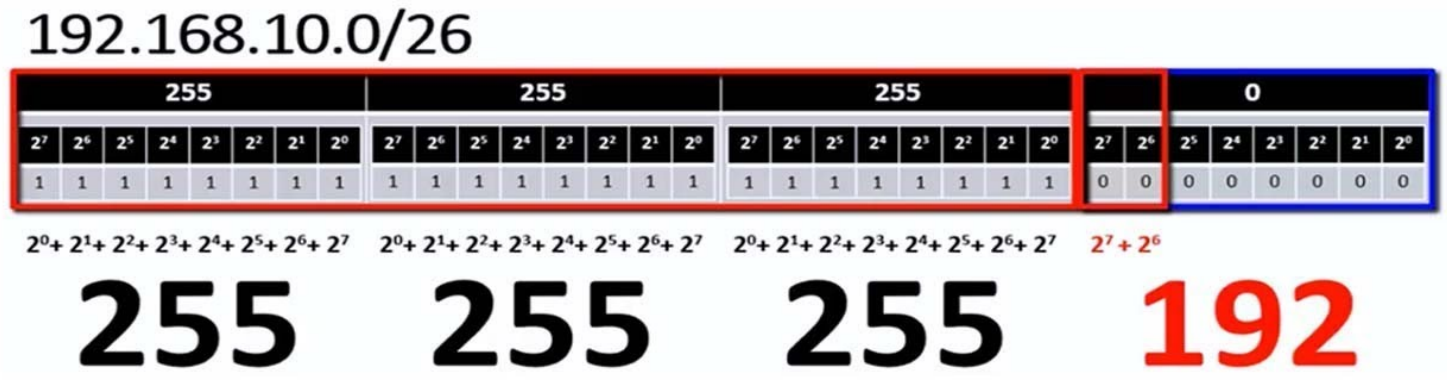
8 bitów = 2^8 = 256 hostów

Maska podsieci

- Załóżmy, że potrzebujemy w naszej firmie sieć z 500 komputerami – musielibyśmy wykorzystać sieć typu B (C jest zbyt mała – max 254 hosty)
  - sieć typu B może adresować 65 034 komputery – jeśli tego nie wykorzystamy, to reszta jest nieużywana → bez sensu
- Rozwiązanie – bezklasowe routowanie międzydomenowe (**VLSM** – *Variable Length Subnet Mask* oraz **CIDR** – *Classless Inter-Domain routing*)
  - VLSM – tworzymy podsieci w ramach sieci danej klasy (lokalnie)
  - CIDR – bezklasowy podział całego protokołu IPv4
- CIDR oraz VLSM wprowadzają pojęcie **maski sieci**, które pozwala efektywniej gospodarować adresami
- Maska podsieci to 32-bitowe liczby – podobnie jak adres IP, związane binarną operacją AND z adresem IP (wyznaczają prefiks sieci z adresu IP)

Maska podsieci – przykład

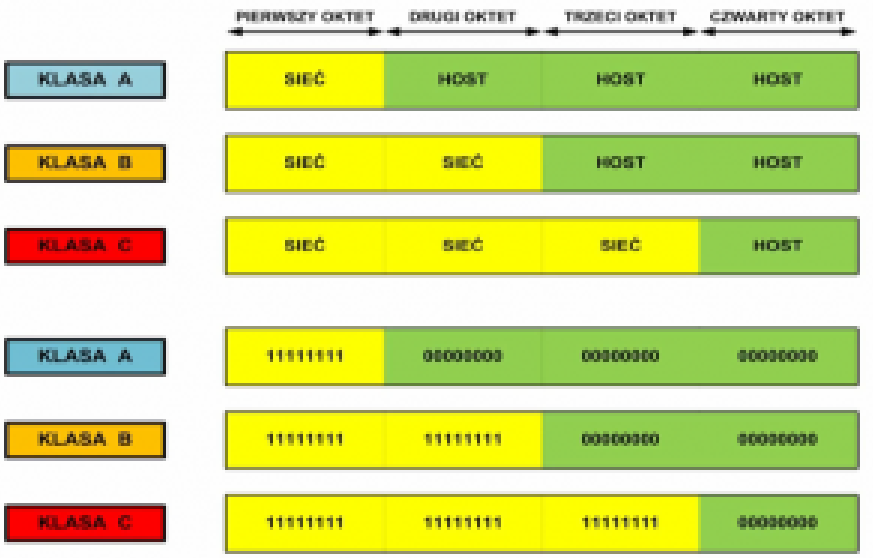
- Zakładamy, że mamy jedną sieć z klasy C
- Ze standardową maską podsieci 255.255.255.0 możemy zaadresować 254 hosty
- Gdybyśmy chcieli efektywniej zarządzać przestrzenią adresową, np. firmie znajduje się kilka działów i w każdym z tych działów chcielibyśmy mieć osobne podsieci → podział na podsieci



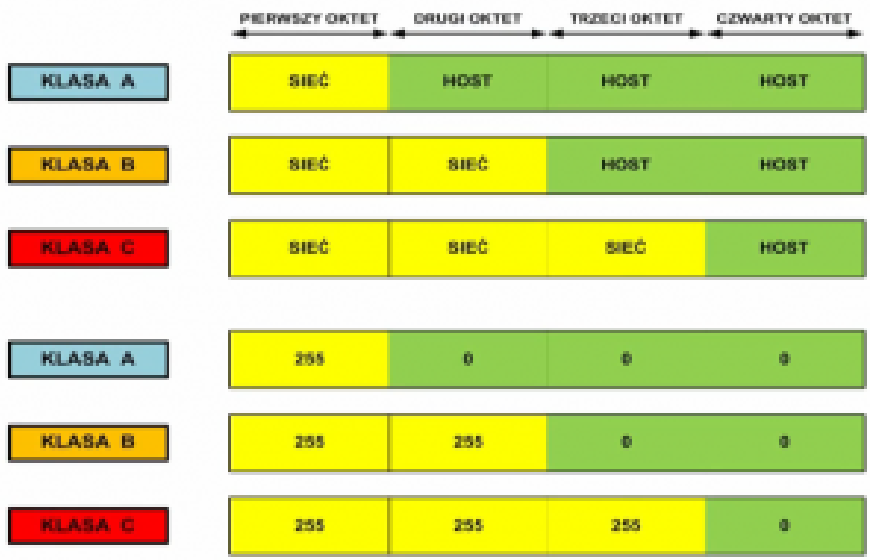
- Należy pamiętać, że bity z których będziemy wyróżniać sobie podsieci możemy "pożyczać" tylko i wyłącznie z części hostowej
- Część sieciowa (określająca klasę sieci) administrowana jest odgórnie i niestety zmienić jej nie możemy, natomiast w części hostowej możemy tą przestrzenią dowolnie gospodarować
- Taka procedura nazywa się **VLSM – Variable Length Subnet Mask**

Maska podsieci – przykład, sieć typu C

Standardowe maski podsieci w postaci binarnej



Standardowe maski podsieci w notacji dziesiętnej



Podział na podsieci z maską 25-bitową

	SIEĆ	SIEĆ	SIEĆ	HOST (PODSIEĆ)
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	10000000
	255	255	255	128

- Adres sieciowy z klasy C
- Zapożyczony 1 bit
- Maska podsieci o adresie 255.255.255.128
- 2 podsieci po 126 hostów

Podział na podsieci z maską 26-bitową

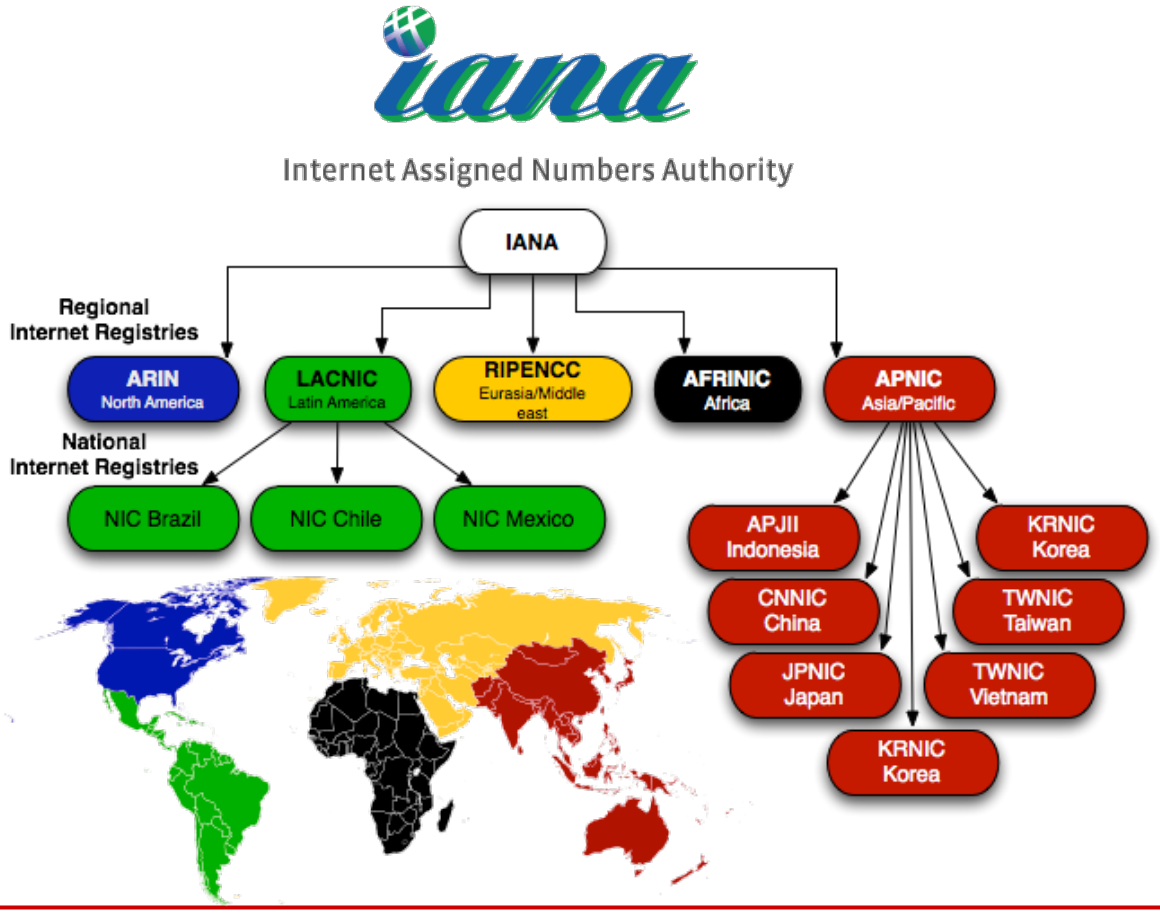
	SIEĆ	SIEĆ	SIEĆ	HOST (PODSIEĆ)
ADRES	203	117	78	0
	11001011	01110101	01001110	00000000
MASKA	11111111	11111111	11111111	11000000
	255	255	255	192

- 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*)

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

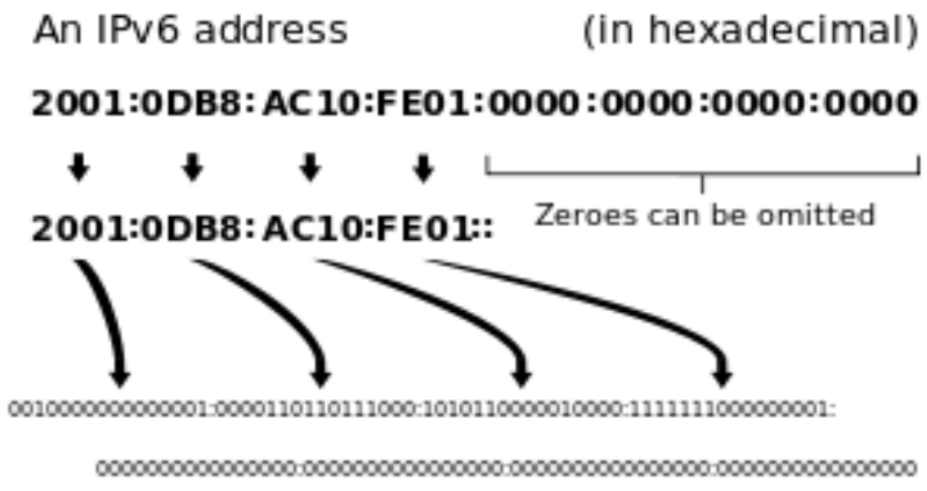


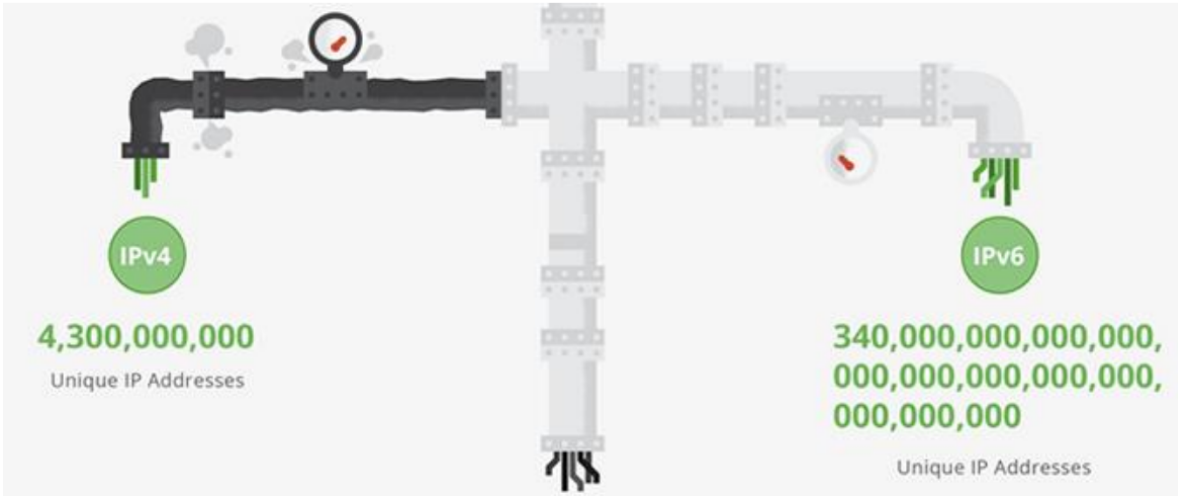
Czy adresy nam się nie skończą?

- Cóż…
- Ostatnia pula adresów IPv4 została rozdzielona przez IANA w dniu 3.02.2011
- Więc co teraz?

Ograniczenia IPv4

- Zapotrzebowanie na adesy IP wzrasta (urządzenia mobilne, itp.)
- Całkowita liczba adresów: 2^{32} = 4,29 mld
- **Rozwiązanie – IPv6**
  - adres zapisywany na 128 bitach (16 bajtów)
  - 2^{128} = 340 trylionów adresów
  - 6,7 miliardów adresów na metr kwadratowy Ziemi
- IPv6 upraszcza strukturę datagramu, nie ma defragmentacji, itp.
- Ale: protokół IPv6 nie jest kompatybilny z IPv4

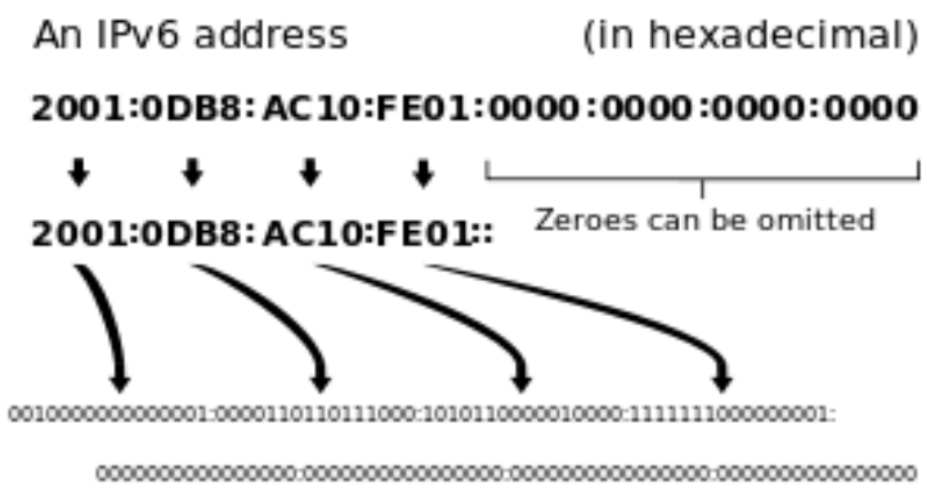


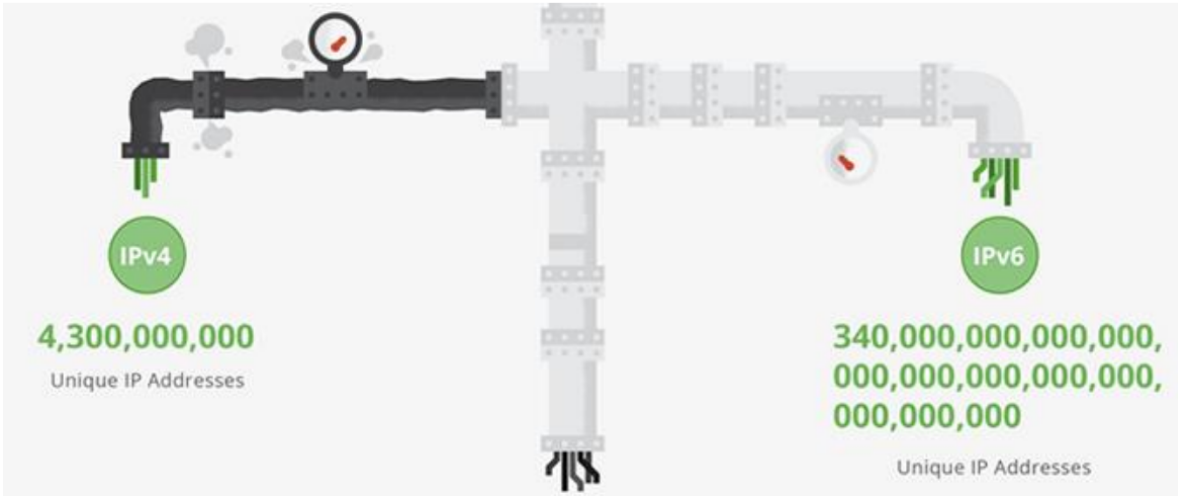


Ograniczenia IPv4

- Zapotrzebowanie na adesy IP wzrasta (urządzenia mobilne, itp.)
- Całkowita liczba adresów: 2^{32} = 4,29 mld
- **Rozwiązanie – IPv6**
  - adres zapisywany na 128 bitach (16 bajtów)
  - 2^{128} = 340 trylionów adresów
  - 6,7 miliardów adresów na metr kwadratowy Ziemi
- IPv6 upraszcza strukturę datagramu, nie ma defragmentacji, itp.
- Ale: protokół IPv6 nie jest kompatybilny z IPv4

Jeśli ktoś chce spróbować używać IPv6 to Polsce Orange umożliwia taki dostęp.





Czy adresy nam się nie skończą?

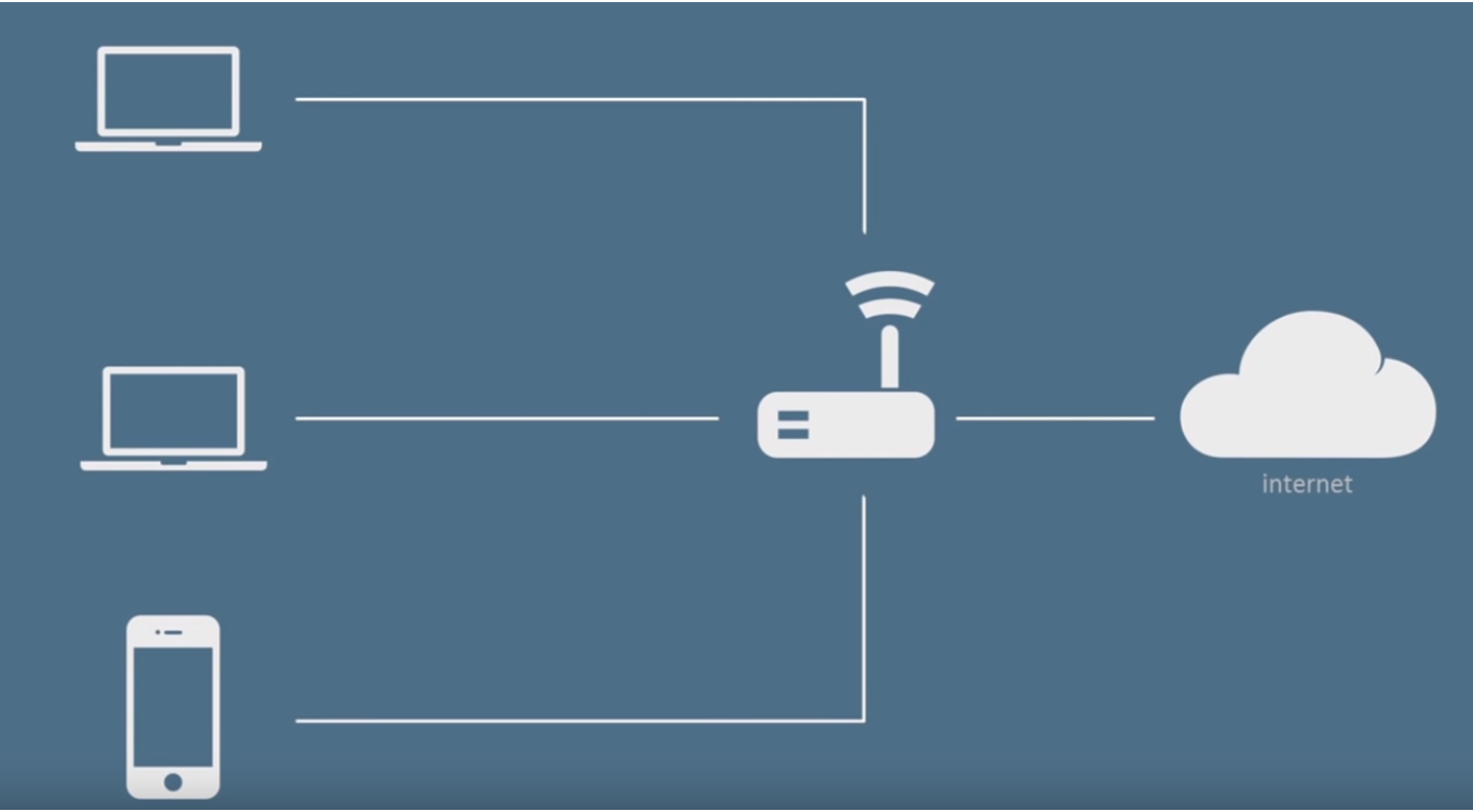
- Inne rozwiązanie (obecne) – wprowadzić **powtarzajace się podsieci**
- Istnieją specjalne adresy sieci prywatnych – mogą się powtarzać w wielu sieciach (adresy “nieroutowane”, nie są dostępne w globalnym Internecie):
  - 10.0.0.0 – 10.255.255.255 – jedna sieć klasy A
  - 172.16.0.0 – 172.31.255.255 – 16 sieci klasy B
  - 192.168.0.0 – 192.168.255.255 – 256 sieci klasy C

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
- Istnieje kilka rodzajów NAT różniących się implementacją (które adresy zmieniamy,

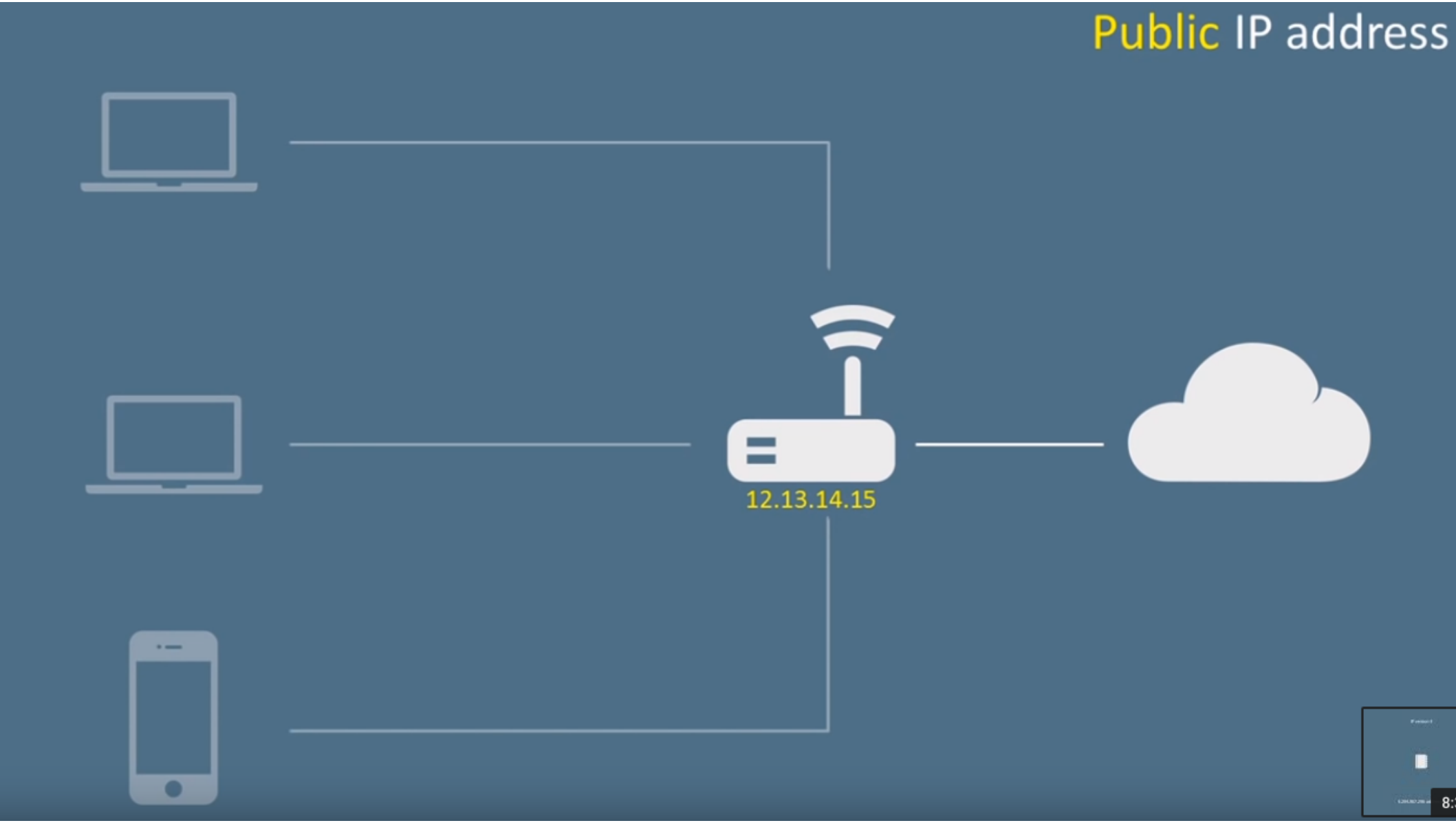
Polecam: https://www.youtube.com/watch?v=QBqPzHEDzvo !

NAT



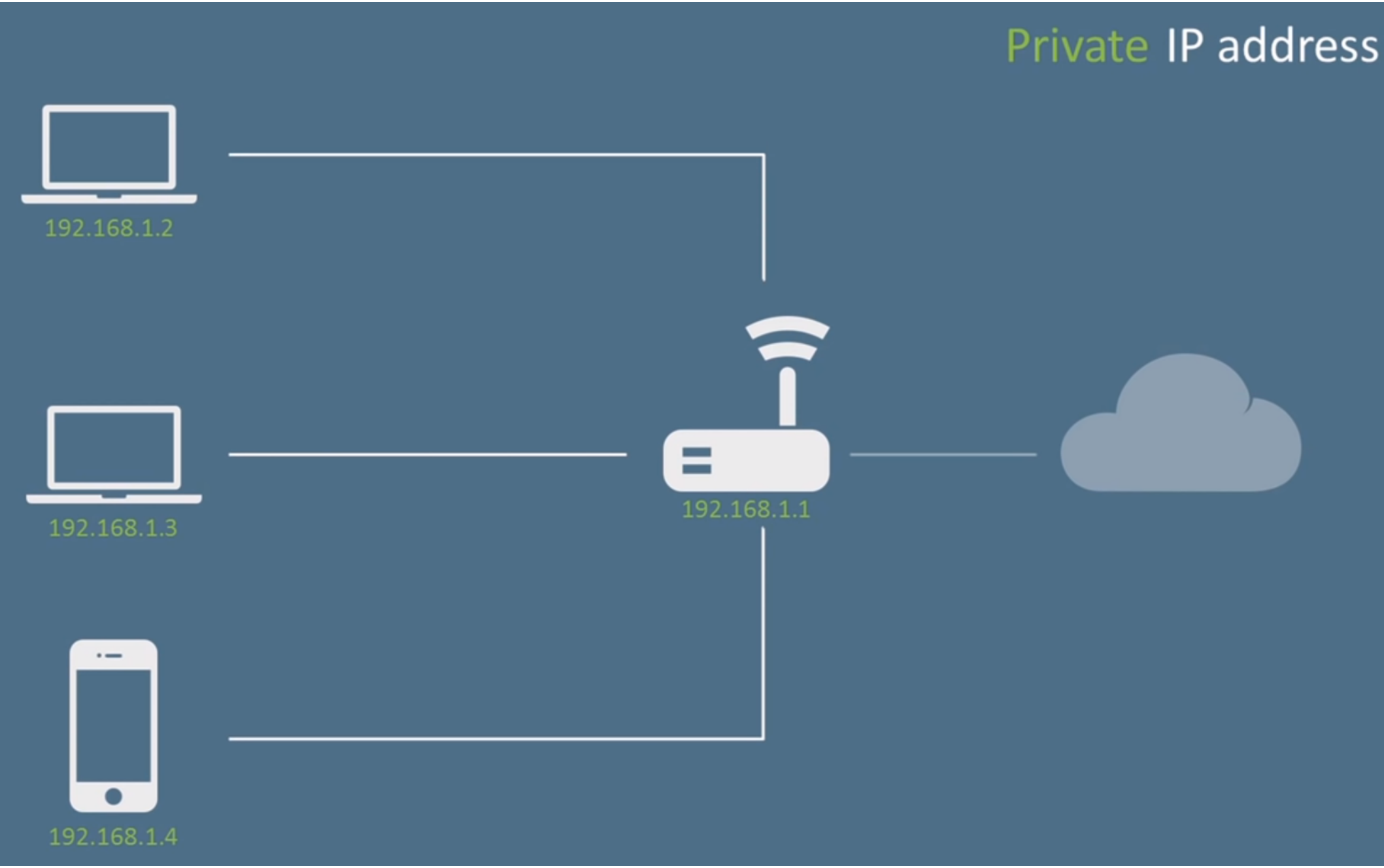
https://www.youtube.com/watch?v=QBqPzHEDzvo

NAT

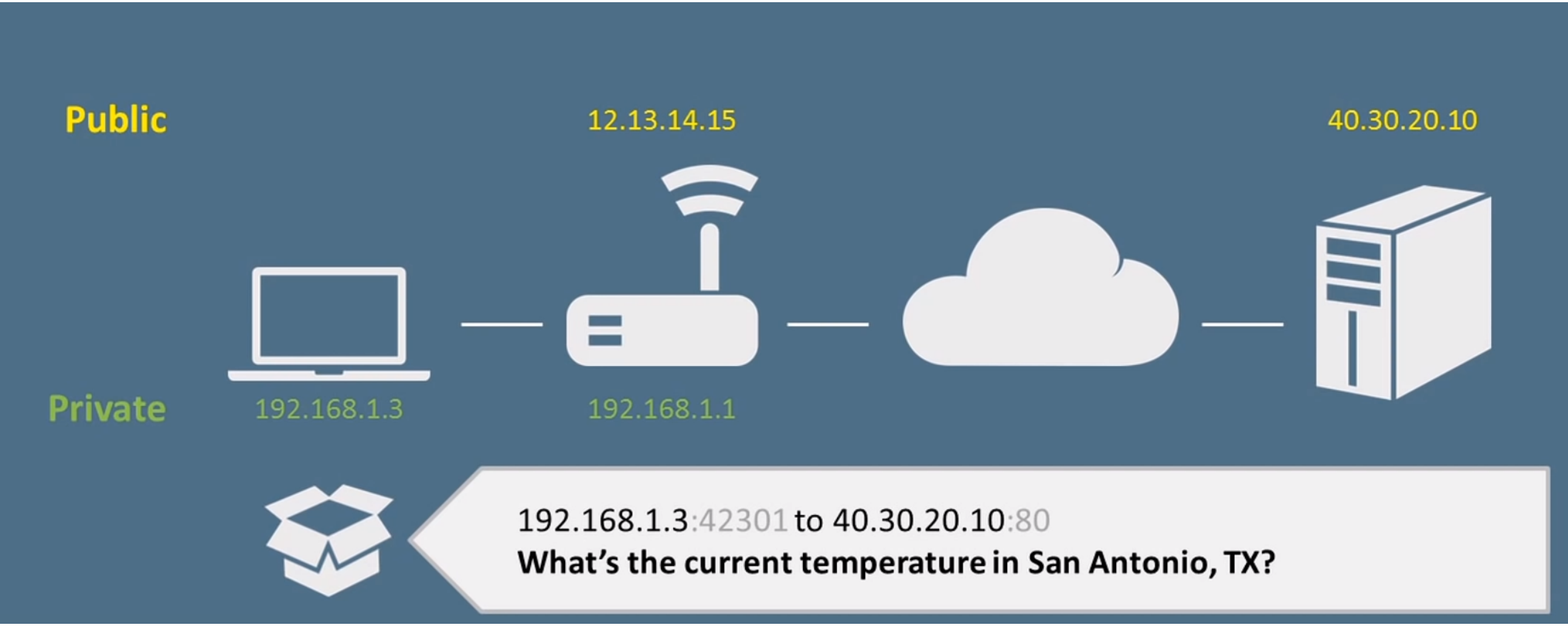


https://www.youtube.com/watch?v=QBqPzHEDzvo

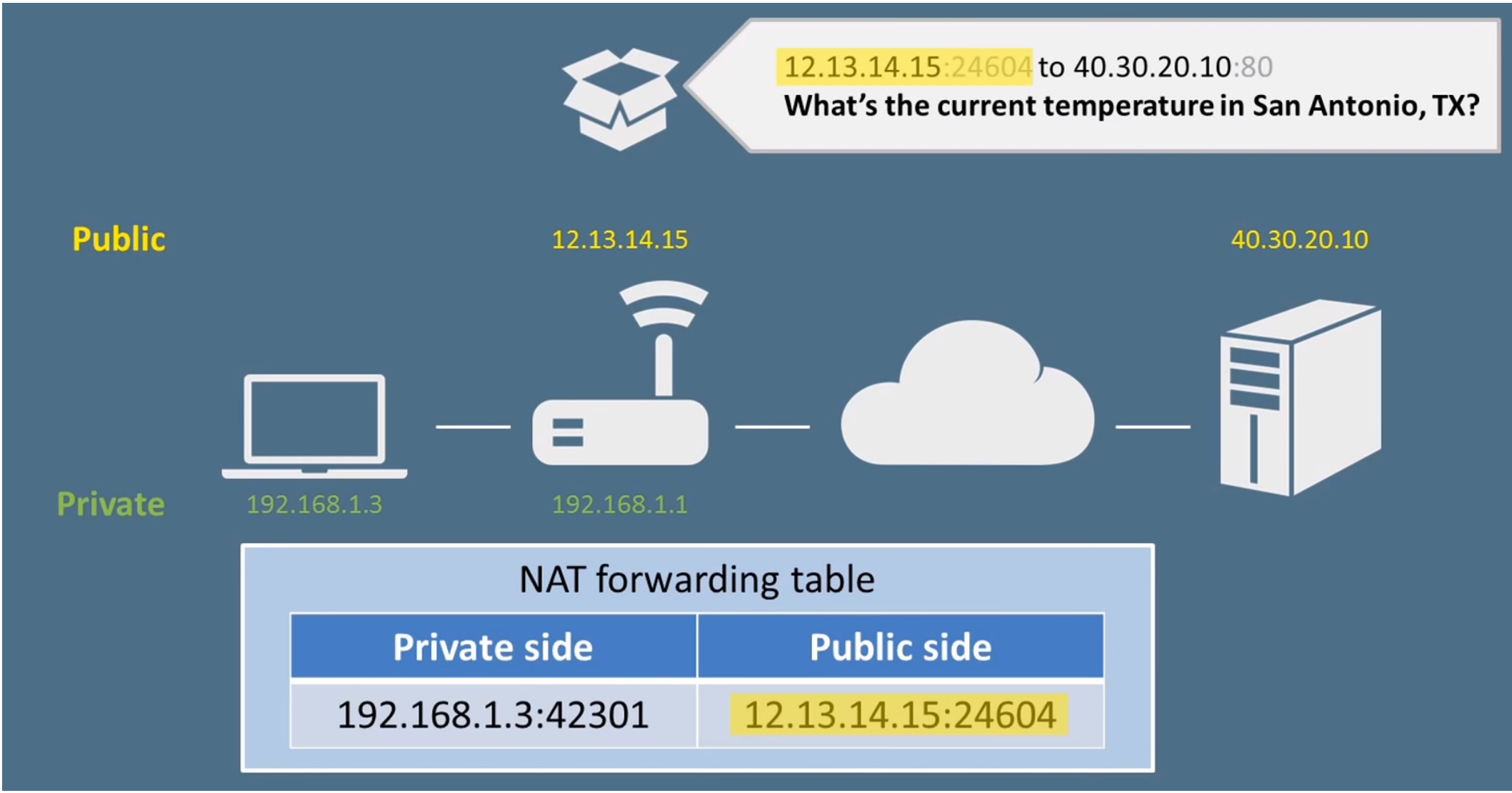
NAT



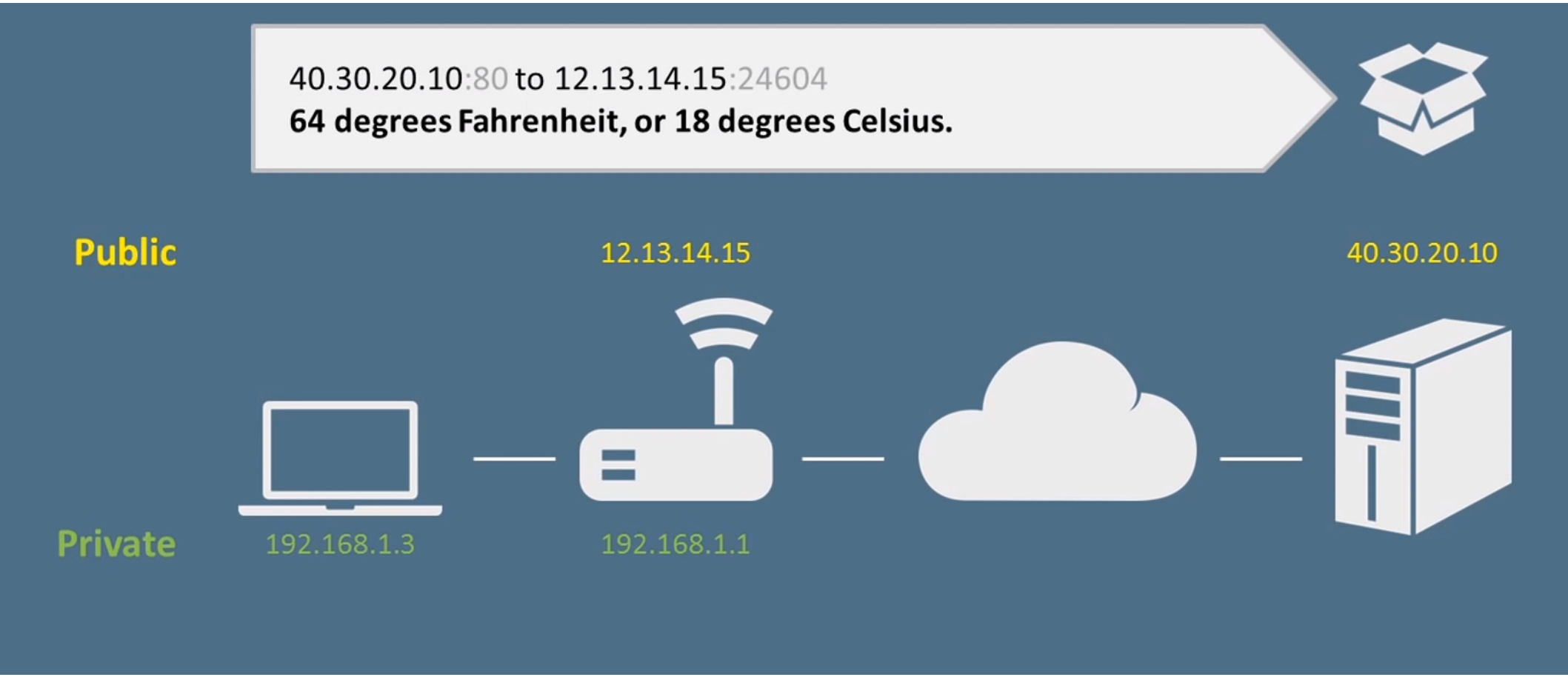
NAT


Public
12.13.14.15
40.30.20.10
Private
192.168.1.3
192.168.1.1
192.168.1.3:42301 to 40.30.20.10:80
What's the current temperature in San Antonio, TX?

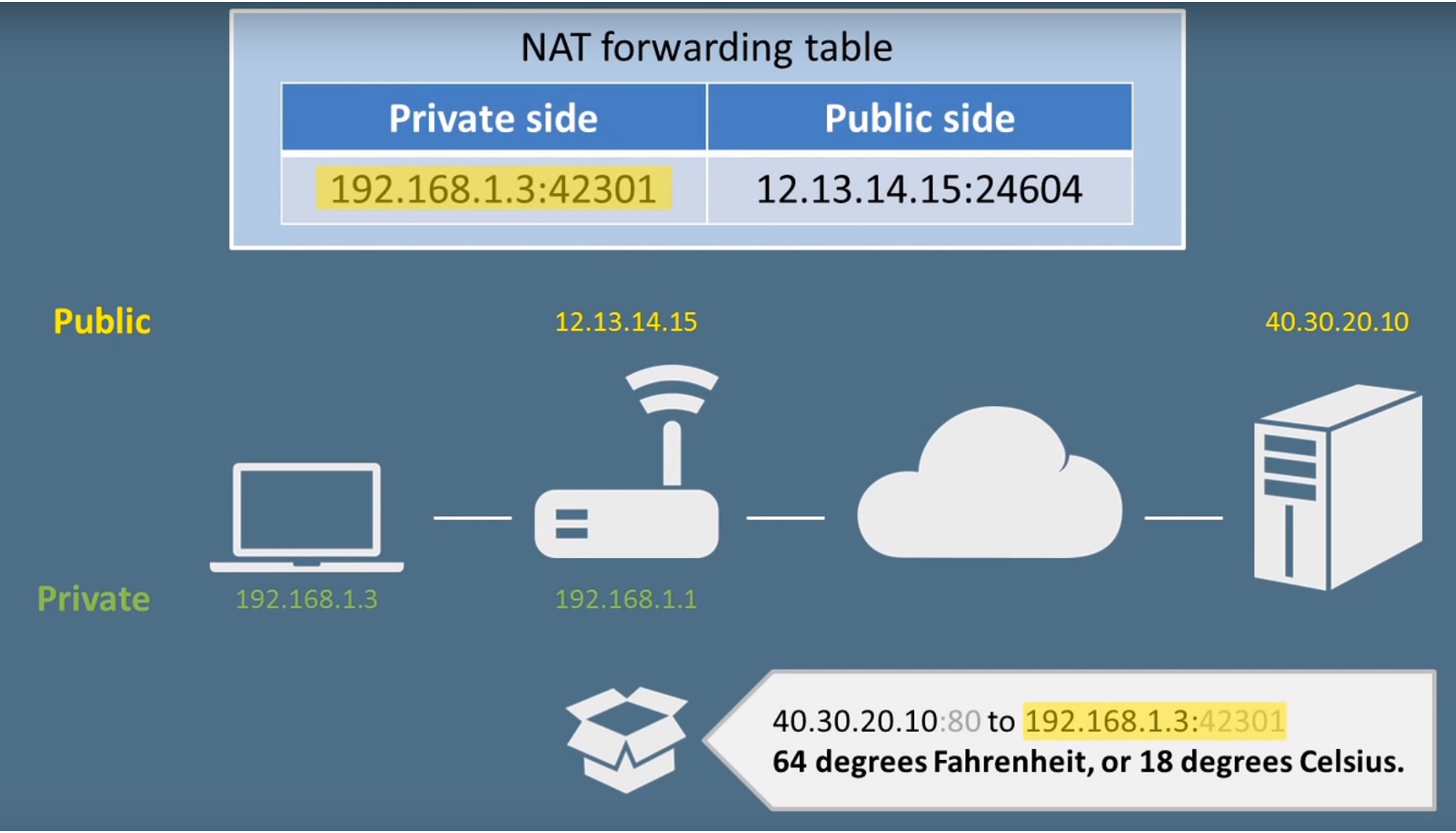
NAT


12.13.14.15:24604 to 40.30.20.10:80
What's the current temperature in San Antonio, TX?
Public
12.13.14.15
40.30.20.10
Private
192.168.1.3
192.168.1.1
NAT forwarding table
Private side
Public side
192.168.1.3:42301
12.13.14.15:24604

NAT


40.30.20.10:80 to 12.13.14.15:24604
64 degrees Fahrenheit, or 18 degrees Celsius.
Public
12.13.14.15
40.30.20.10
Private
192.168.1.3
192.168.1.1

NAT


NAT forwarding table
Private side
Public side
192.168.1.3:42301
12.13.14.15:24604
Public
12.13.14.15
40.30.20.10
Private
192.168.1.3
192.168.1.1
40.30.20.10:80 to 192.168.1.3:42301
64 degrees Fahrenheit, or 18 degrees Celsius.

Adresowanie w IP

- Adres IP nie może kończyć się na 0 lub 255 (adres kończący się na 255 to **broadcast**)
- Adres 127.0.0.1 to “pseudoadres”, tzw. “loopback”, czyli adres własnego komputera – urządzenie widzi na nim samo siebie
- W systemach Linux informację o IP i MAC adresach uzyskamy wpisując polecenie **ifconfig** (w systemach Windows **ipconfig**)
  - każdy komputer może mieć wiele intefejsów (kart) sieciowych, każdy ma swój unikalny adres IP
  - każdy interfejs może mieć jeden **lub więcej** adresów IP

Adresowanie w IP

```
tecmint@tecmint ~ $ ifconfig
eth0      Link encap:Ethernet  HWaddr 28:d2:44:eb:bd:98
          inet addr:192.168.0.104  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::2ad2:44ff:feeb:bd98/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:342087 errors:0 dropped:0 overruns:0 frame:0
          TX packets:233764 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:406375041 (406.3 MB)  TX bytes:25096967 (25.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:5146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:5146 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:469809 (469.8 KB)  TX bytes:469809 (469.8 KB)

wlan0     Link encap:Ethernet  HWaddr 38:b1:db:7c:78:c7
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tecmint@tecmint ~ $
```

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**

Protokół ICMP

- **ping**

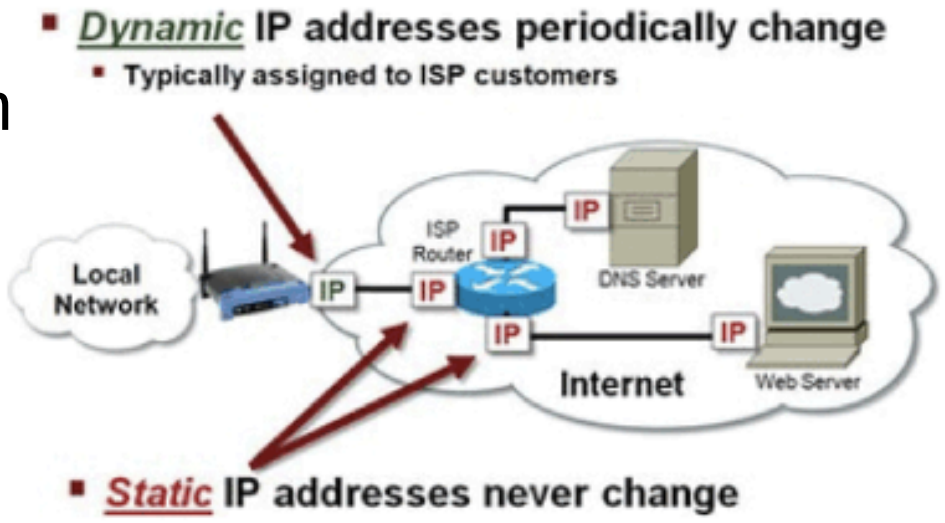
```
wfpw@meyrin:~$ ping google.pl
PING google.pl (216.58.209.35) 56(84) bytes of data.
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=1 ttl=56 time=7.33 ms
64 bytes from waw02s05-in-f35.1e100.net (216.58.209.35): icmp_seq=2 ttl=56 time=9.07 ms
64 bytes from waw02s05-in-f35.1e100.net (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
```

- **traceroute**

```
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
```

Uzyskiwanie adresu IP

- Do tej pory zajmowaliśmy się adresami IP oraz przepływem informacji między węzłami w Internecie
- Jak natomiast wygląda samo uzyskiwanie adresu IP po przyłączeniu komputera do sieci?
- Adres IP możemy uzyskać na dwa sposoby:
  - **statycznie** – zachowane w konfiguracji sieci
  - **dynamicznie** – przyporządkowywane za każdym razem gdy się łączymy z siecią
- Może wystąpić **konflikt** gdy dwa urządzenia mają ten sam adres IP (system operacyjny notyfikuje administratora)



Inne protokoły

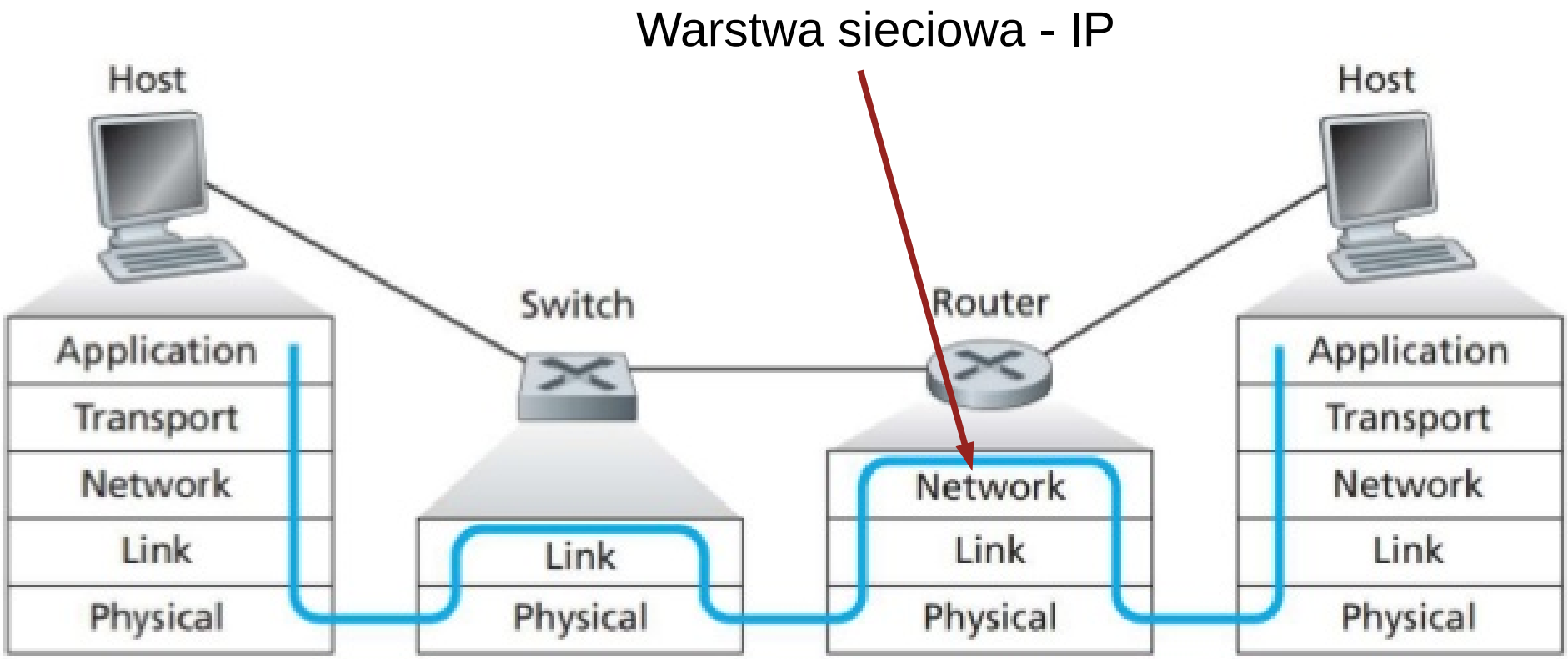
- Dynamiczne uzyskiwanie adresu IP
  - **DHCP (*Dynamic Host Configuration Protocol*)**
  - ARP (*Address Resolution Protocol*) / RARP (*Reverse Address Resolution Protocol*)
  - BOOTP (*Bootstrap Protocol*) – nie będziemy omawiać

Protokół DHCP

- Najpopularniejszym protokołem automatycznego przydzielania IP jest DHCP (*Dynamic Host Configuration Protocol*)
- Protokół działa w architekturze klient-serwer
- Serwer DHCP odpowiada za przydzielanie adresów, tworzy maskę podsieci, oraz wyznacza czas jaki dany adres może być przypisany do jednego klienta
- Po podłączeniu do sieci to klient prosi serwer DHCP o przydzielenie jednego z wolnych adresów
- Bardzo czesto rolę serwera DHCP pełni **router** (router operuje na warstwie sieciowej, w przeciwieństwie do switcha)

Router vs switch

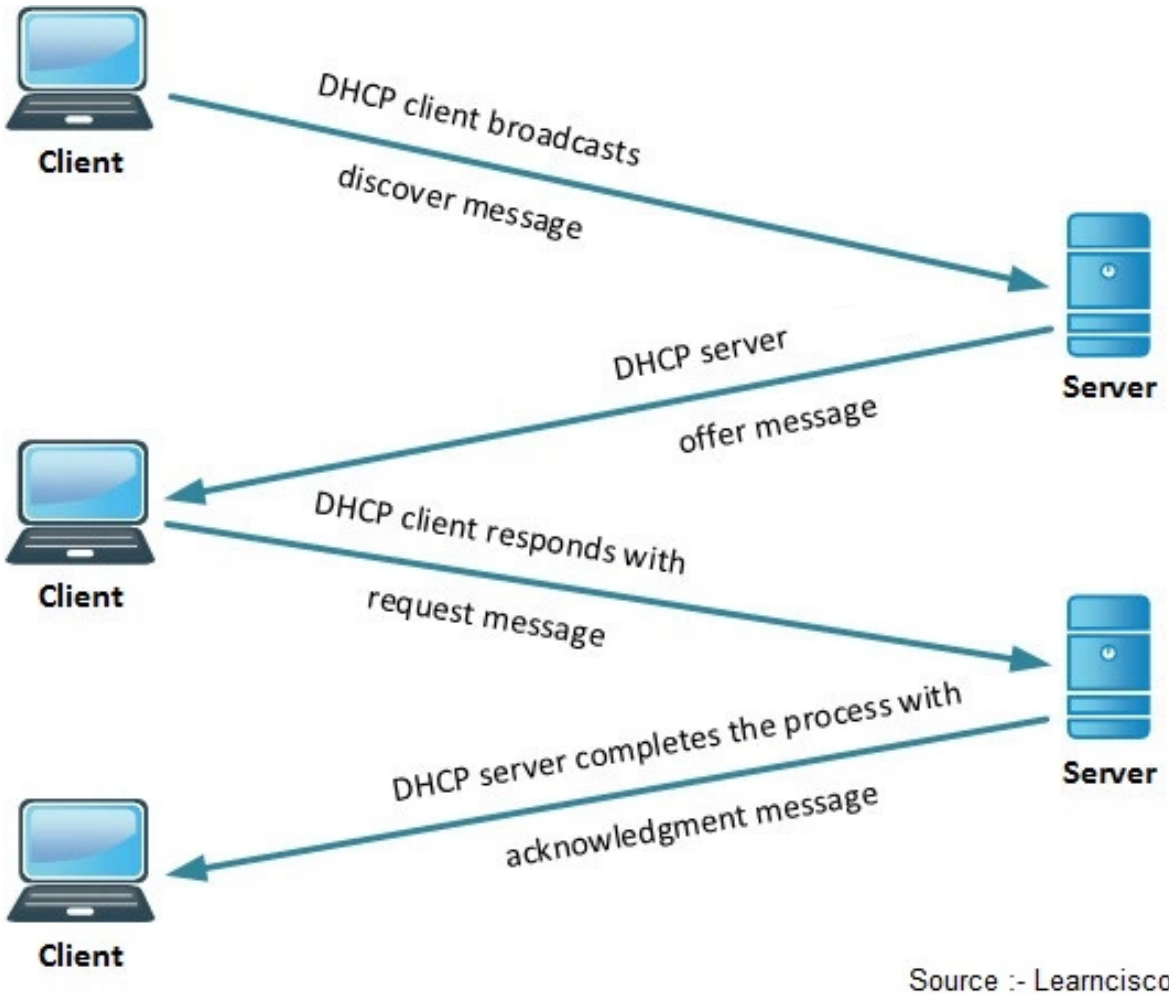
A router in that it forwards packets using MAC addresses (layer-2) whereas a router is a layer-3 packet switch.



Protokół 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

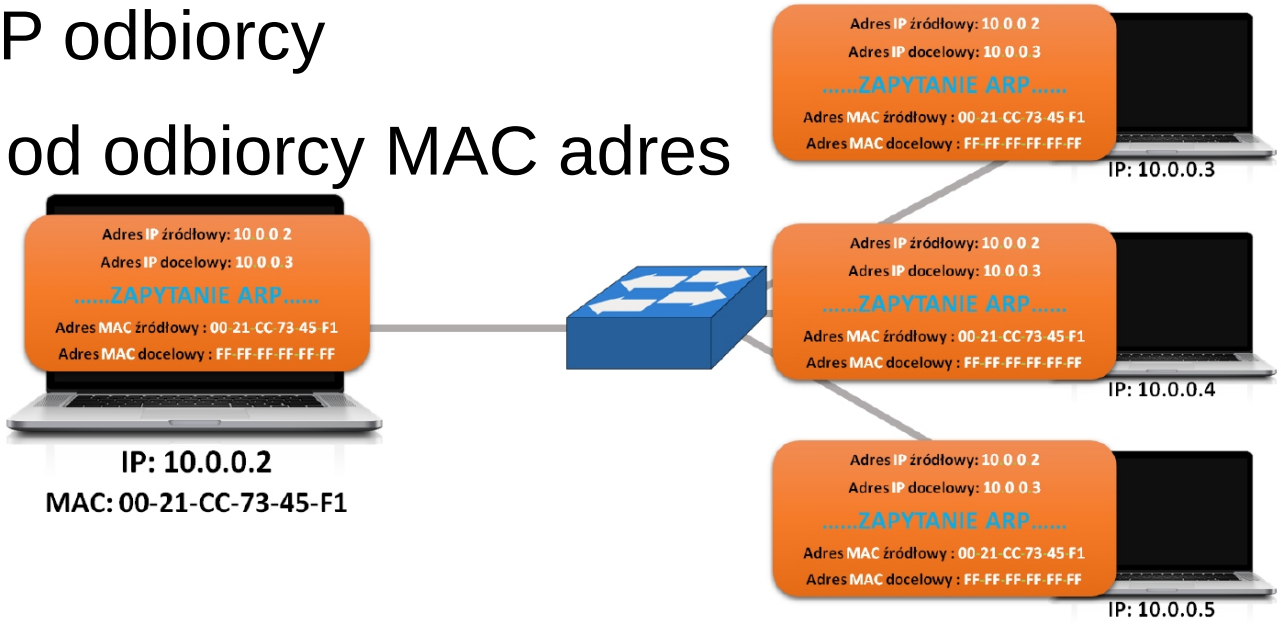


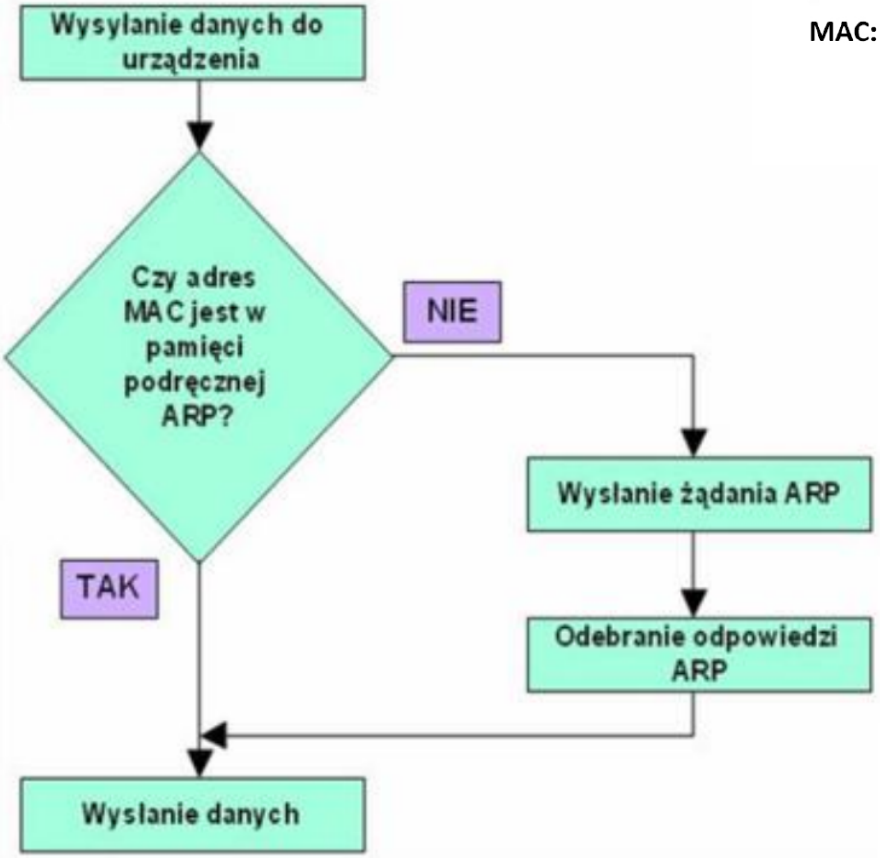
Inne protokoły

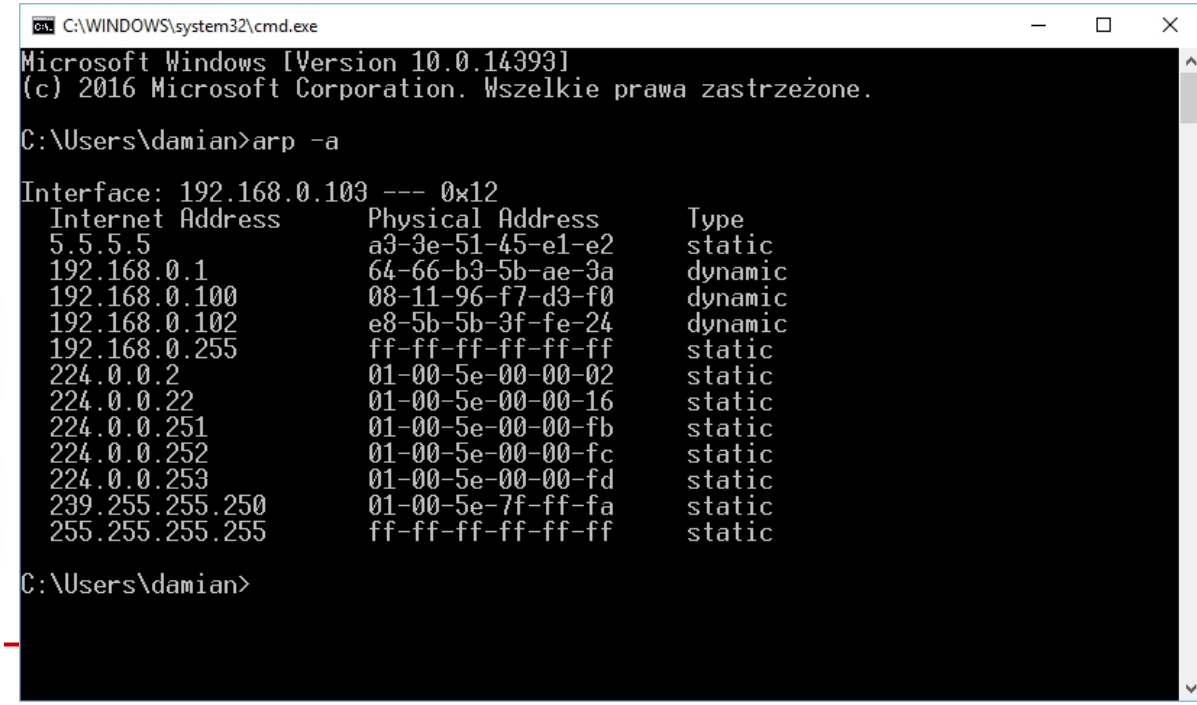
- Jak to adresowanie po IP ma się do ramek ethernetu?
  - **Protokół ARP** odzworowuje znany adres IP na adres sprzętowy MAC

Protokół ARP

- Komputer nadawca najpierw wysyła zapytanie ARP na broadcast z adresem IP odbiorcy
- W odpowiedzi dostaje od odbiorcy MAC adres
- MAC jest dodawany do tablicy ARP na komputerze nadawcy





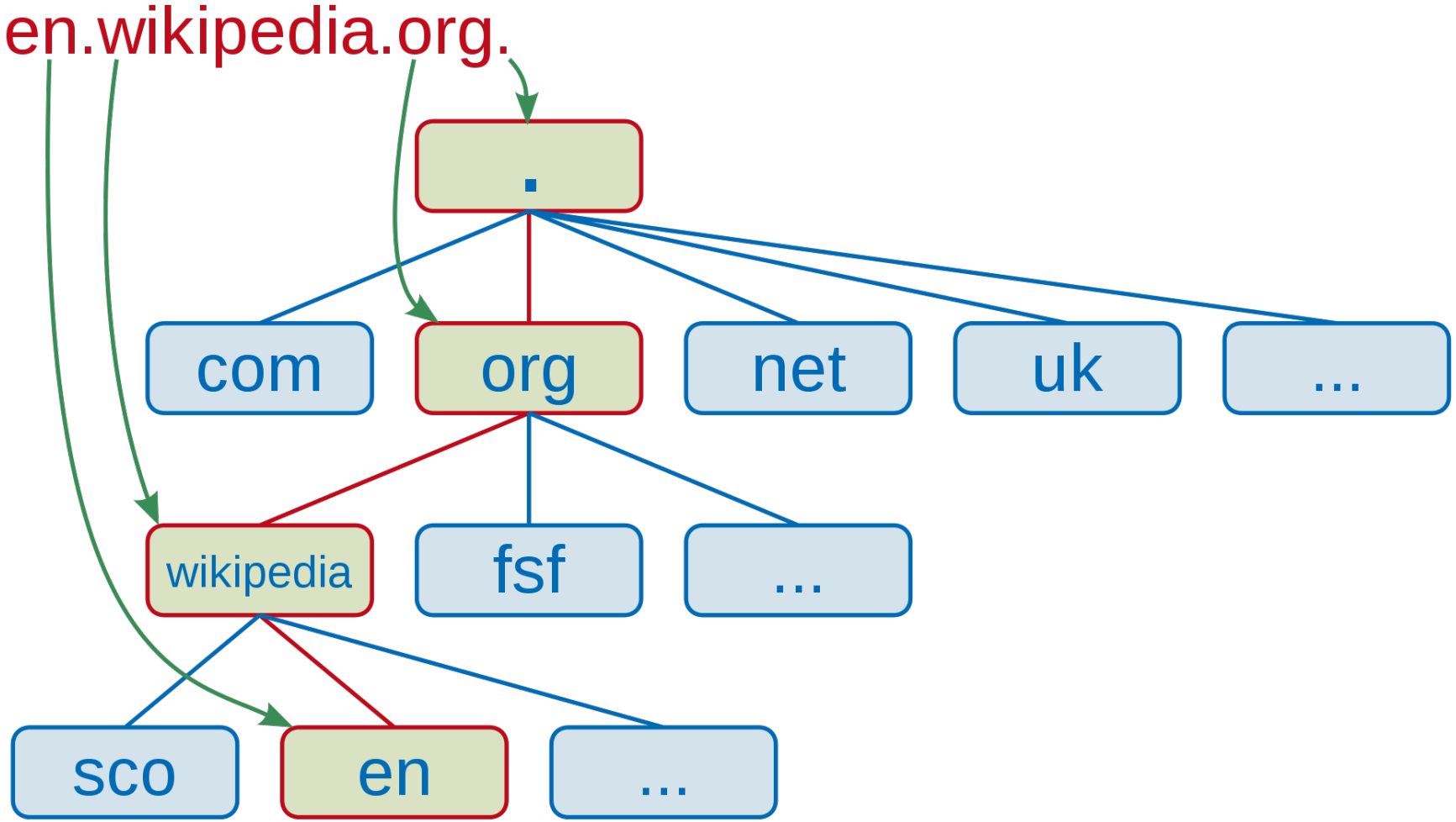


Serwer DNS

- 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
- Zadaniem DNS jest translacja tekstu zrozumiałego dla człowieka (nazwy) na adres liczbowy
- Nazwa DNS może tez oznaczać cały system (Domain Name System) nazewnictwa urządzeń i usług w sieci (nie tylko adresy IP)

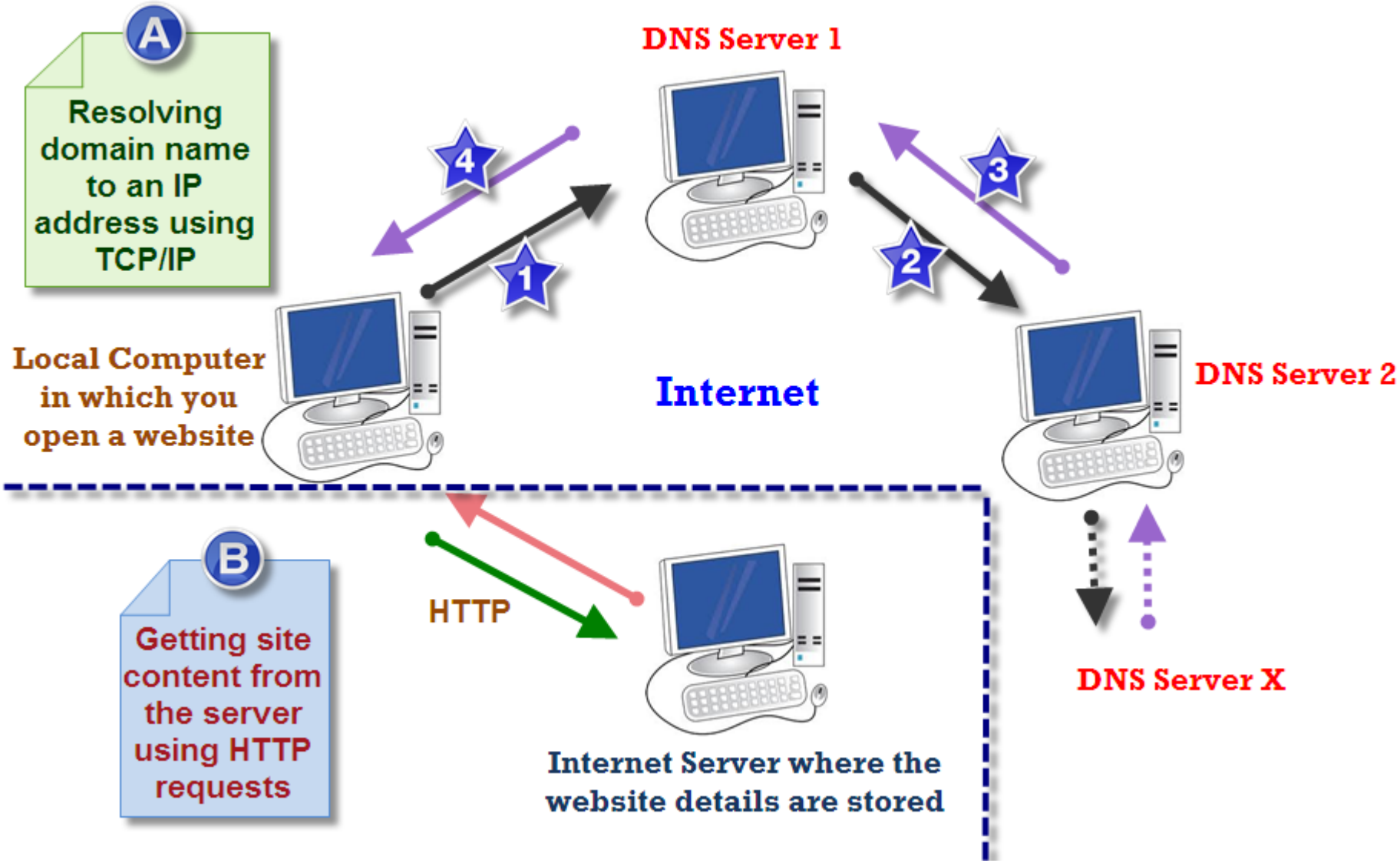
Serwer DNS

- Domeny dzielą się na strefy ustawione hierarchicznie
- Każda domena zaczyna się od strefy root (top-level domain)



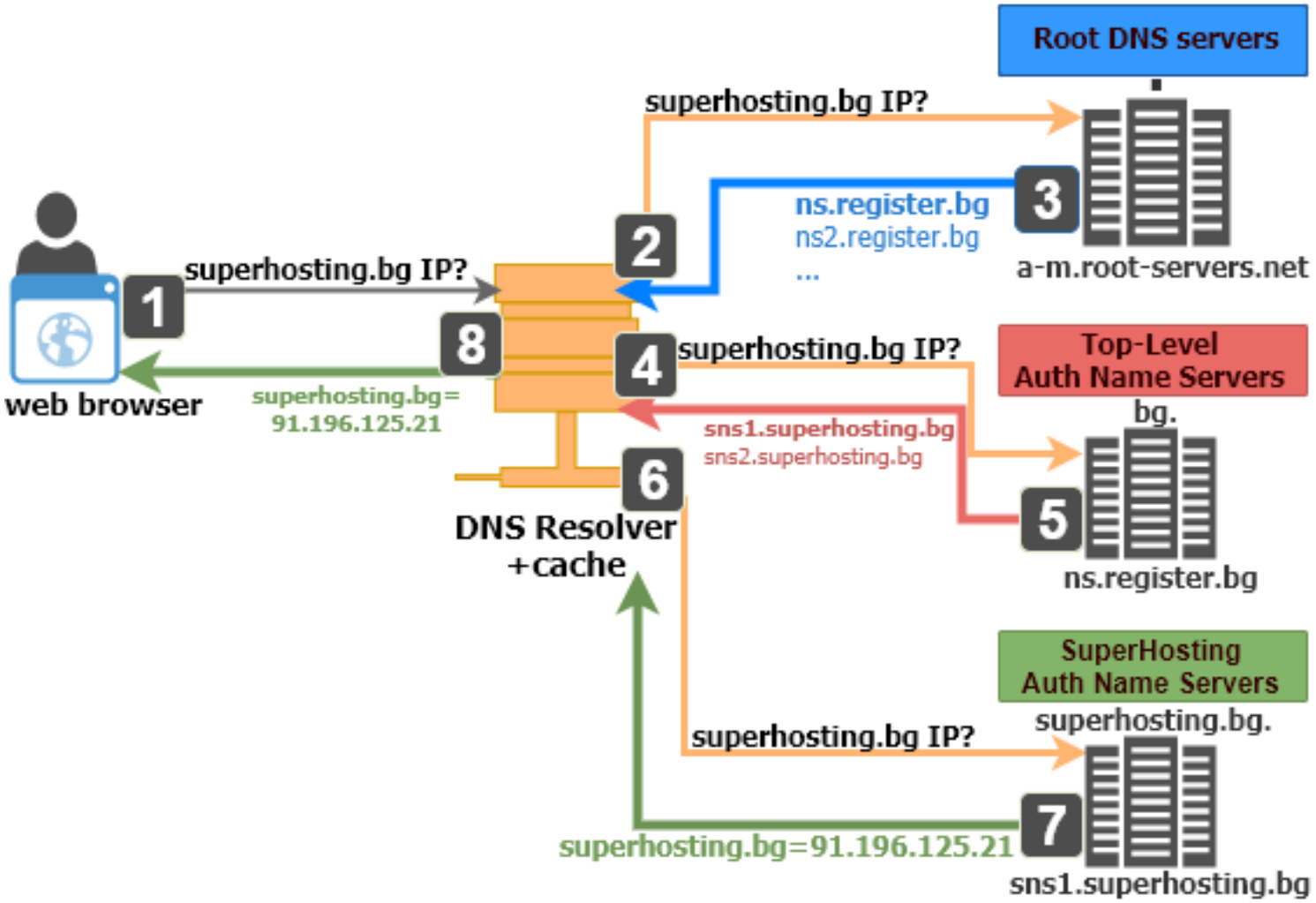
Serwer DNS

- Przykład – otwarcie strony WWW



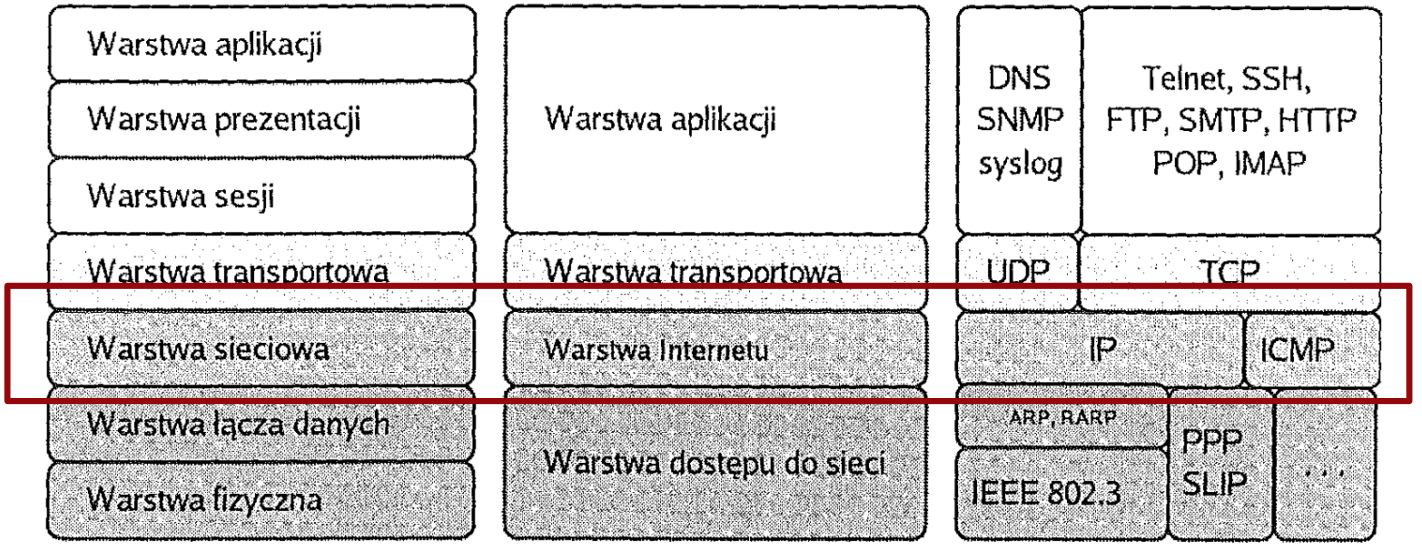
Serwer DNS

- Przykład – otwarcie strony WWW
- Odpytujemy po kolei kolejne serwery DNS, zaczynając od poziomu (strefy) root



KONIEC

Warstwa Internetu



źródło: Helion