Specyfikacja zagadnień

Sieci

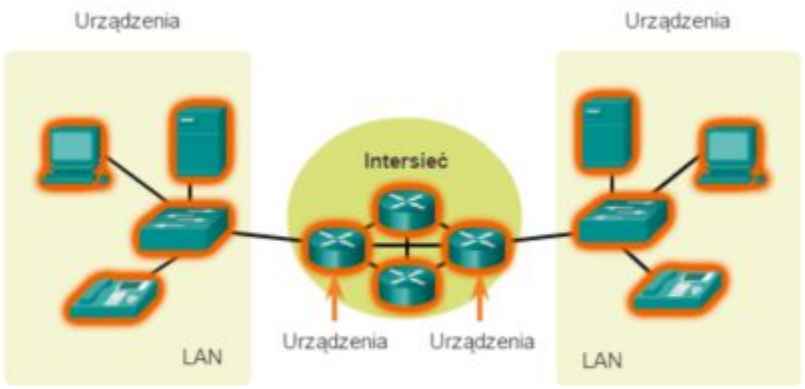
- Co to jest sieć?
- Rozmiary sieci (dom, małe biuro, średnia firma, globalny)
- Wspomaganie (komunikacja, praca, nauka, zabawa)
- Serwery i klienci

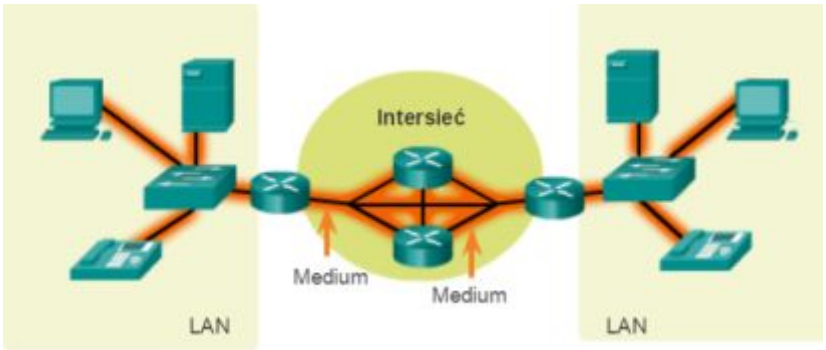
LAN, WAN i Internet

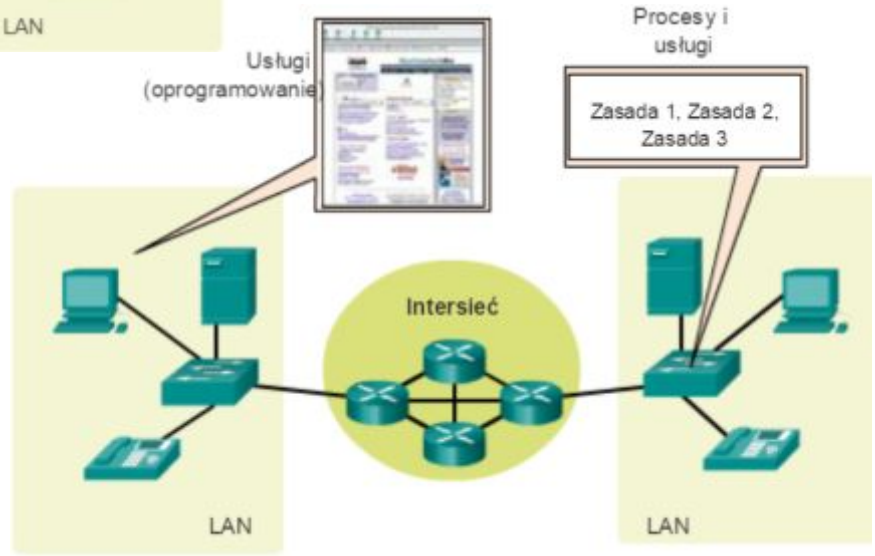
Komponenty sieci

Sieci składają się z trzech elementów, do których zaliczamy:

- urządzen
- media
- usługi







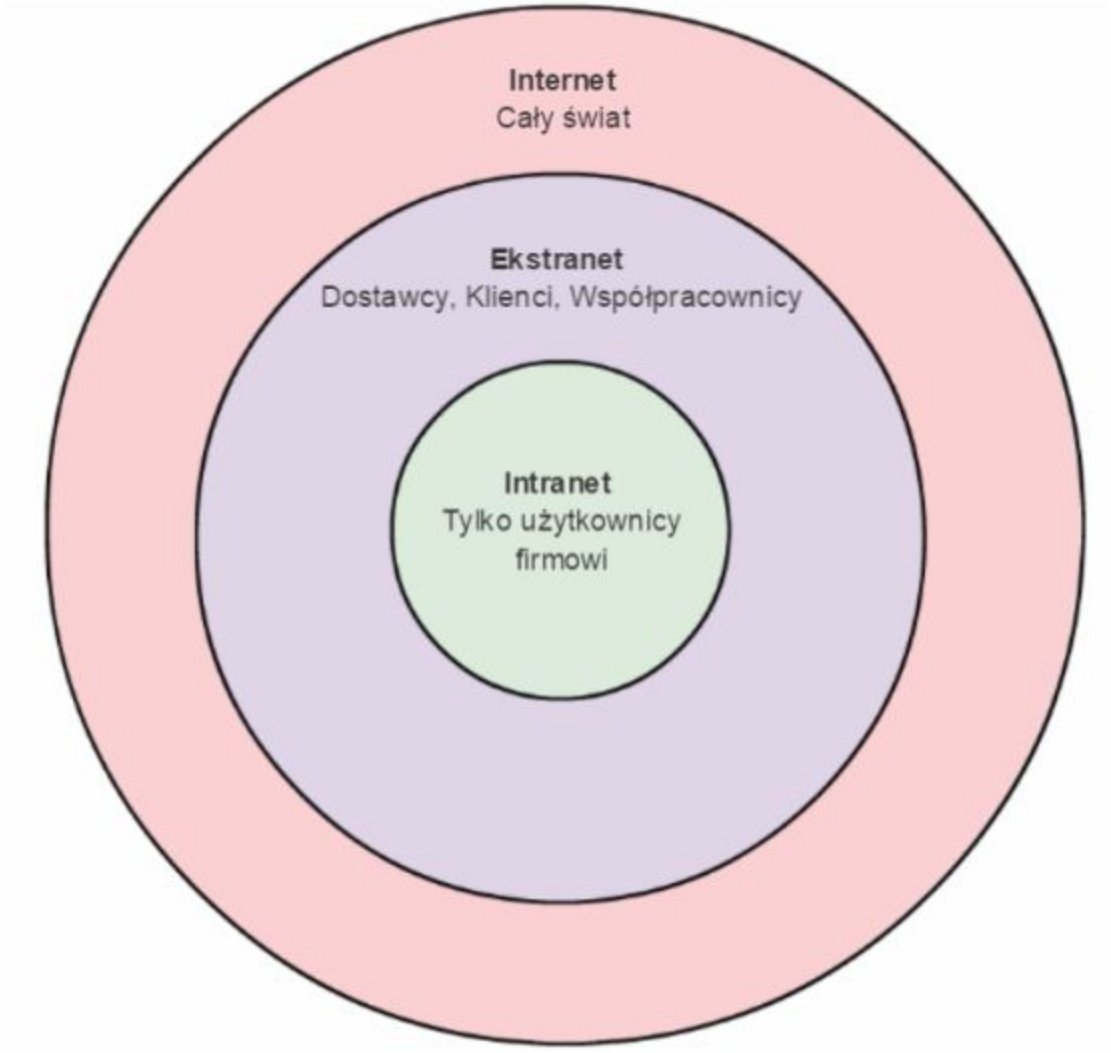
Komponenty sieci

- Urządzenia końcowe (komputery, drukarki, ….)
- Media (bezprzewodowe i przewodowe – miedziane i światłowody)
- Urządzenia sieciowe (dostępowe – switch, koncentrator ….., łączące sieci - router, bezpieczeństwo – firewall)
- Topologie – fizyczne (peer-to-peer, gwiazda,….) i logiczne (Ethernet, Token-ring)

- Typy sieci (WAN, LAN, MAN, SAN, Pan, WLAN)
- Opcje połączeń (dzierżawione, DSL, modem …)
- Wspieranie architektury (skalowalność, tolerancja błędów, QoS, bezpieczeństwo….)
- Trendy w sieciach (praca grupowa, chmura obliczeniowa, komunikacja video, centra danych, PoE….)

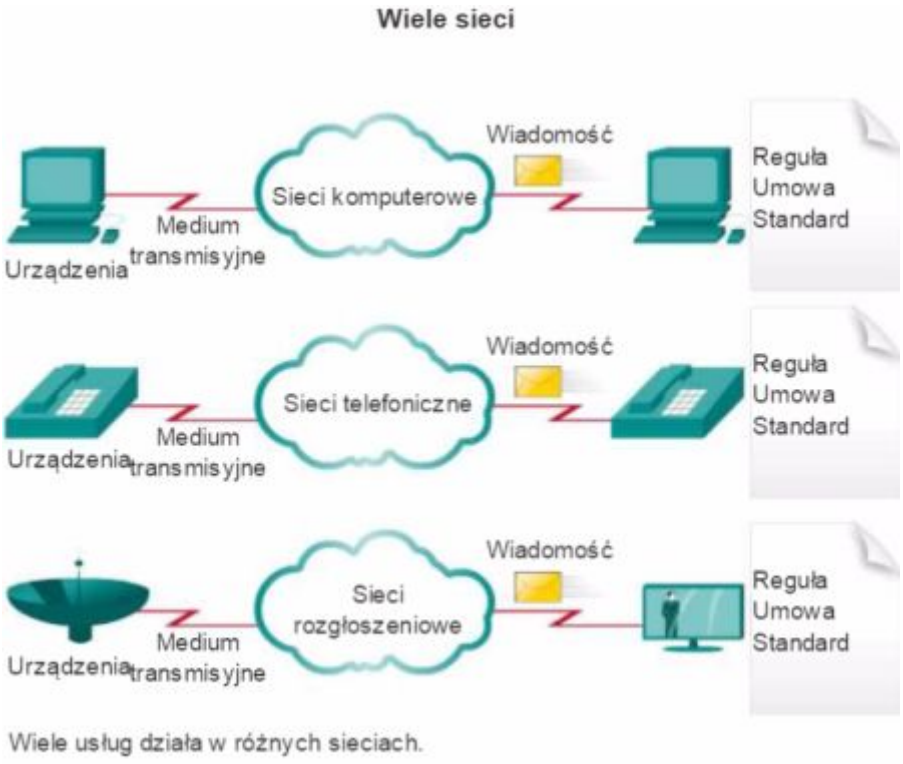
Sieci LAN i WAN i Internet

Intranet i Extranet

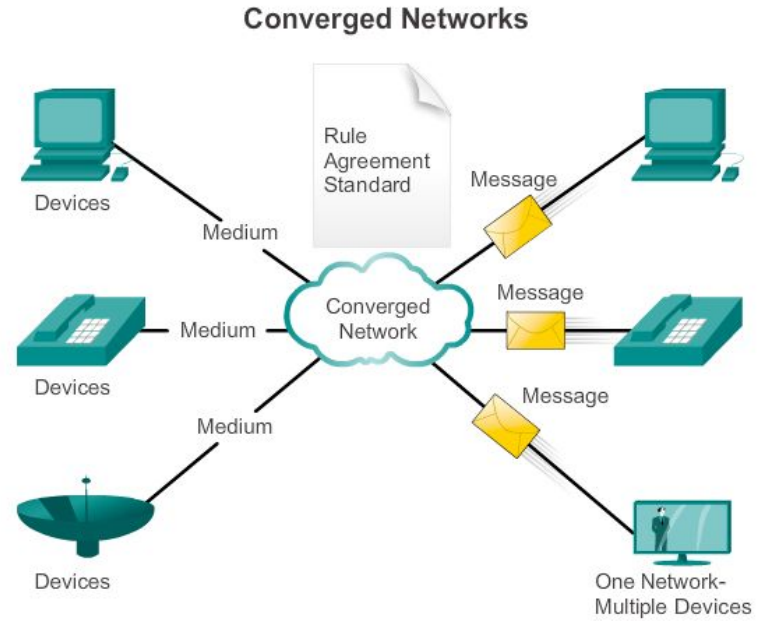


Sieci konwergentne

Konwergencja sieci



Wiele usług działa w różnych sieciach.



Converged data networks carry multiple services on one network.

Zapewnianie bezpieczeństwa sieci

Bezpieczeństwo sieci jest ważnym czynnikiem podczas korzystania z sieci

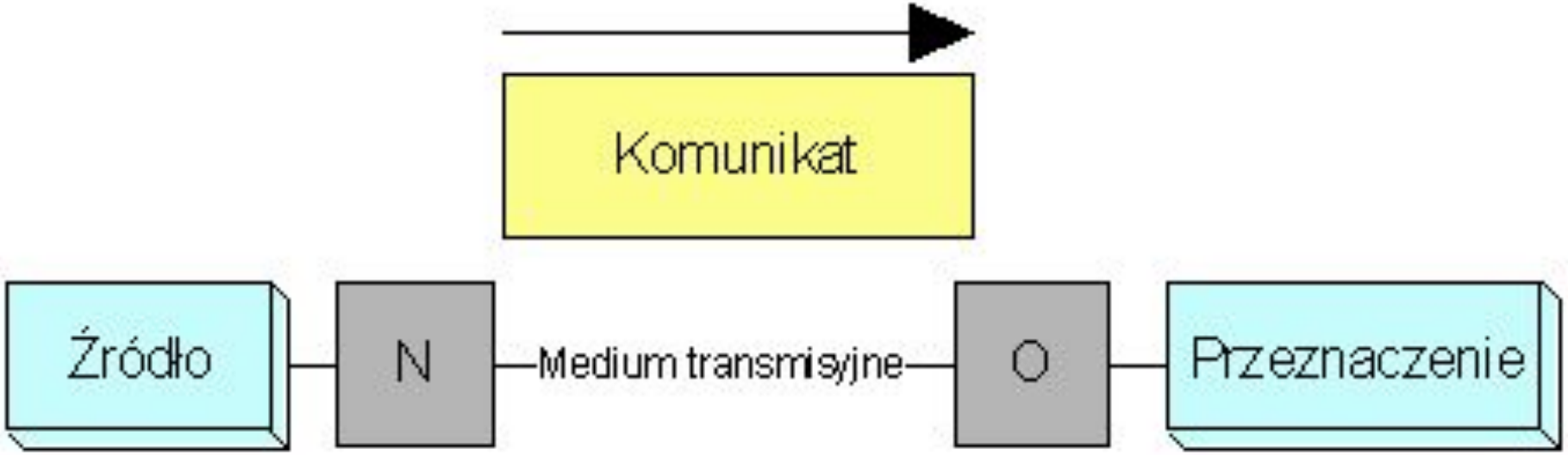
Transmisja poufnych, z punktu widzenia użytkownika, danych i informacji jest zabezpieczona przed dostępem niepowołanych osób.

Protokoły sieciowe i komunikacja

Sieć jest systemem komunikacji komputerów między sobą poprzez medium transmisyjne z użyciem określonych protokołów komunikacyjnych.

Protokołem komunikacyjnym określa się zespół zasad i reguł przekazywania komunikatów między komputerami – stacjami sieciowymi.

Medium transmisyjne jest to nośnik umożliwiający rozchodzenie się informacji w postaci prądu elektrycznego, fali elektromagnetycznej, świetlnej, akustycznej, itp.



Reguły

- identyfikacja nadawcy i odbiorcy,
- uzgodnienie metody komunikacji (bezpośrednia, przez telefon, list, fotografia),
- wspólny język i gramatyka,
- szybkość i czas dostarczenia,
- wymagania dotyczące potwierdzenia otrzymania wiadomości

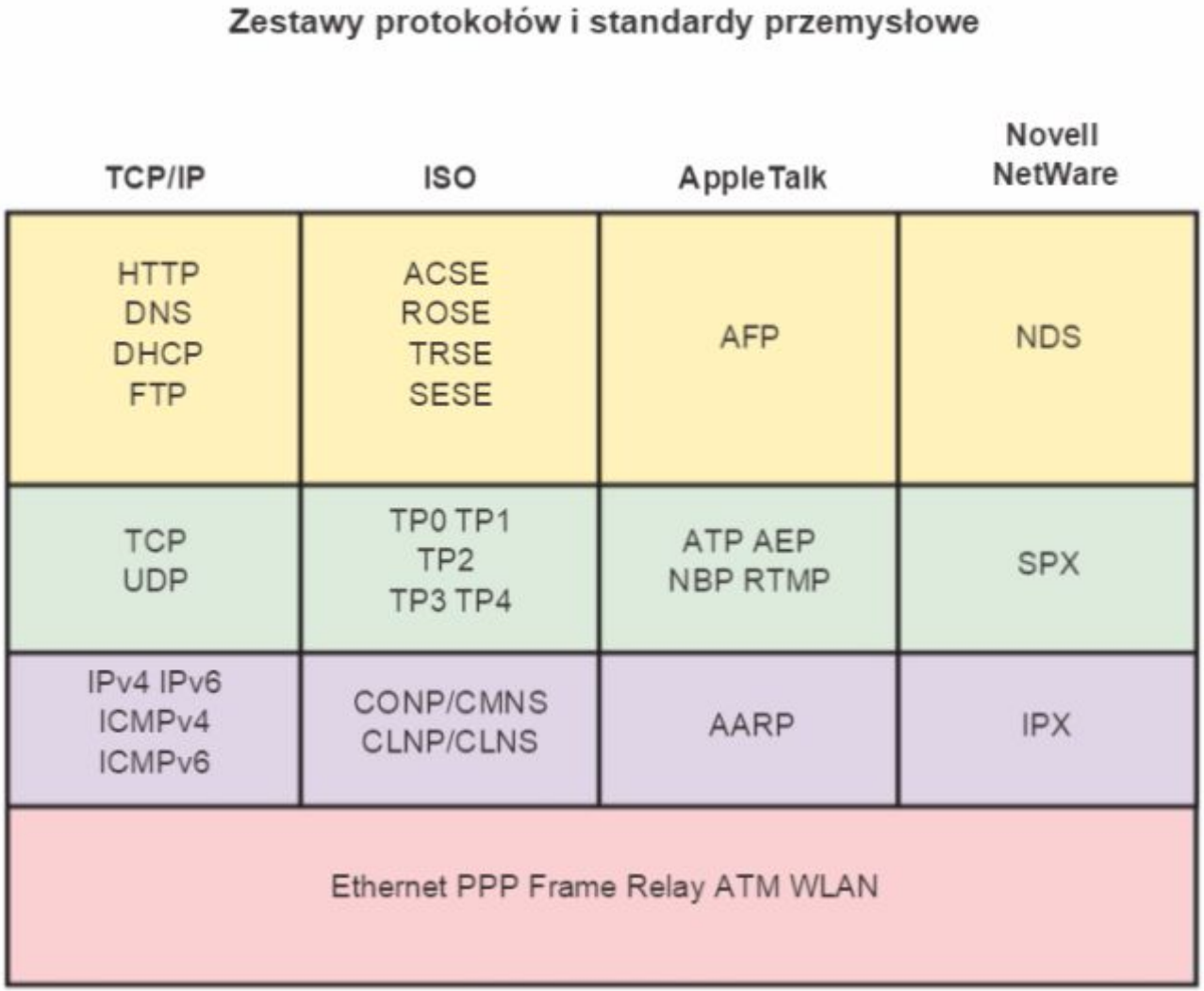
Opcje dostarczenia wiadomości

- Unicast
- Multicast
- Broadcast

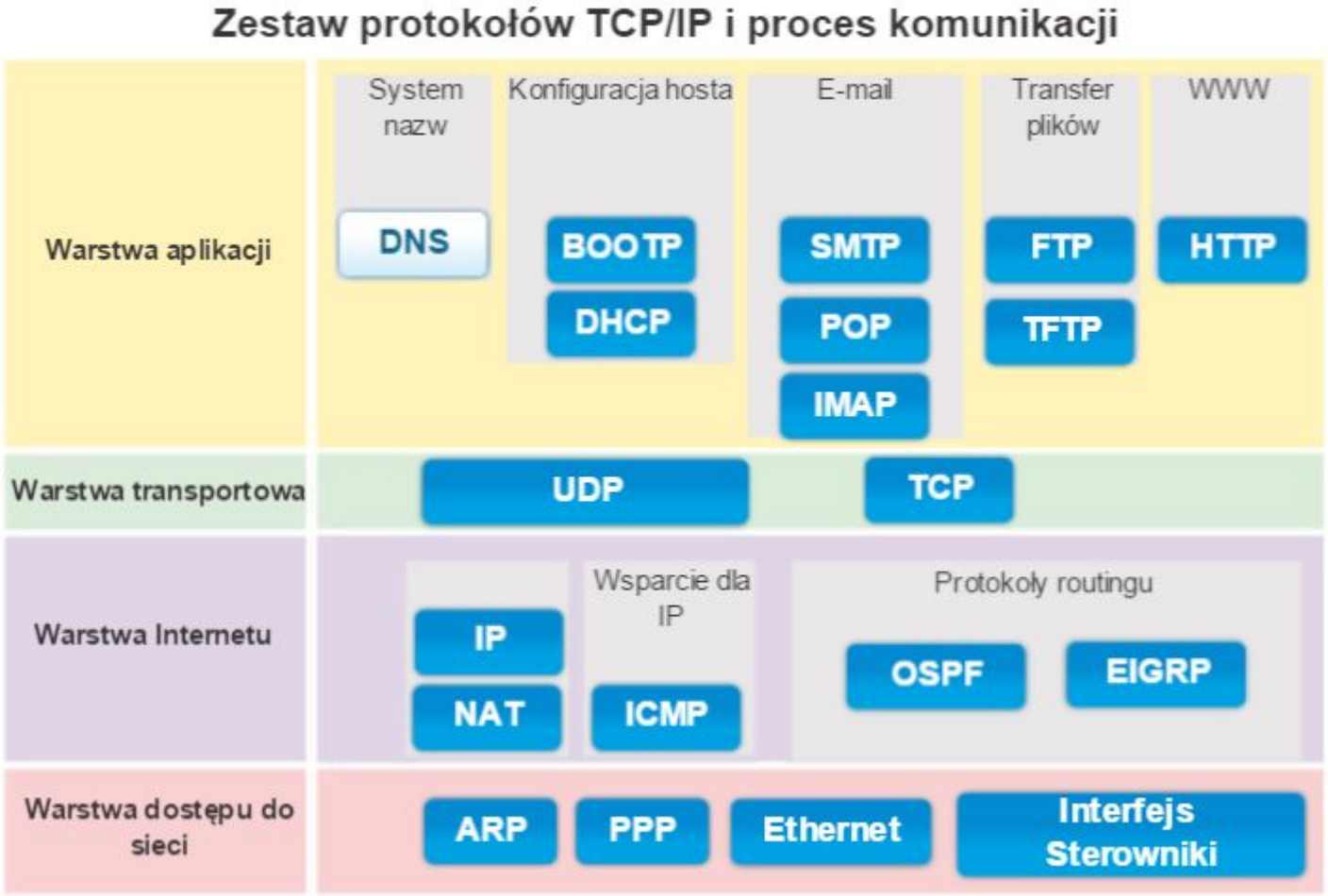
Protokoły sieciowe

- Idea
- współdziałanie

Zestawy protokołów i standardy przemysłowe



Stos protokołów TCP/IP i komunikacja



Model warstwowy sieci

1978 r. - wzorcowy model warstwowy sieci (ISO/OSI):

– nadanie nazw;

– określenie zadań.

Warstwy umożliwiają:

– przesyłanie informacji między sieciami o różnych technologiach;

– współdziałanie różnorodnego sprzętu, urządzeń i programów;

– zrozumienie działania sieci;

– dzielenie komunikacji i ułatwienie pracy;

– dokonywanie zmian w warstwie nie zmienia struktury pozostałych.

Warstwy sieci komputerowych

aplikacji	VII	aplikacji
	VI	prezentacji
	V	sesji
przepływu	IV	transportu
	III	sieciowa
	II	łączna danych
	I	fizyczna

<u>Usługi komunikacyjne</u>:

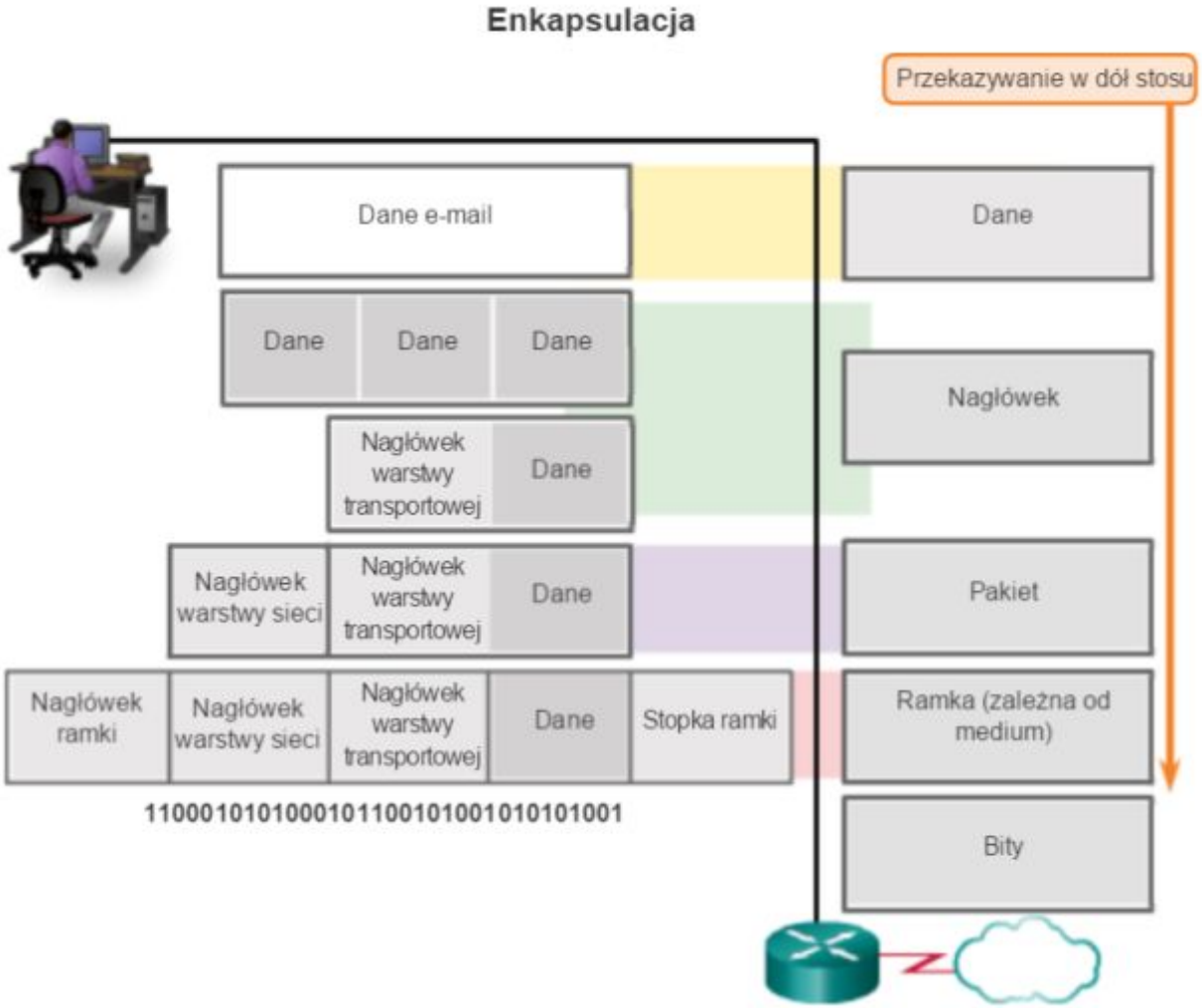
- dostęp do zasobów innych użytkowników;
- drukowanie w sieci;
- obsługa poczty elektronicznej;
- przesyłanie i przeglądanie plików;
- przyłączanie terminali.

OPROGRAMOWANIE W STOSIE PROTOKOŁÓW **OSI**, KTÓRE UDOSTĘPNIA PUNKT STARTOWY DLA SESJI KOMUNIKACJI.

Enkapsulacja danych

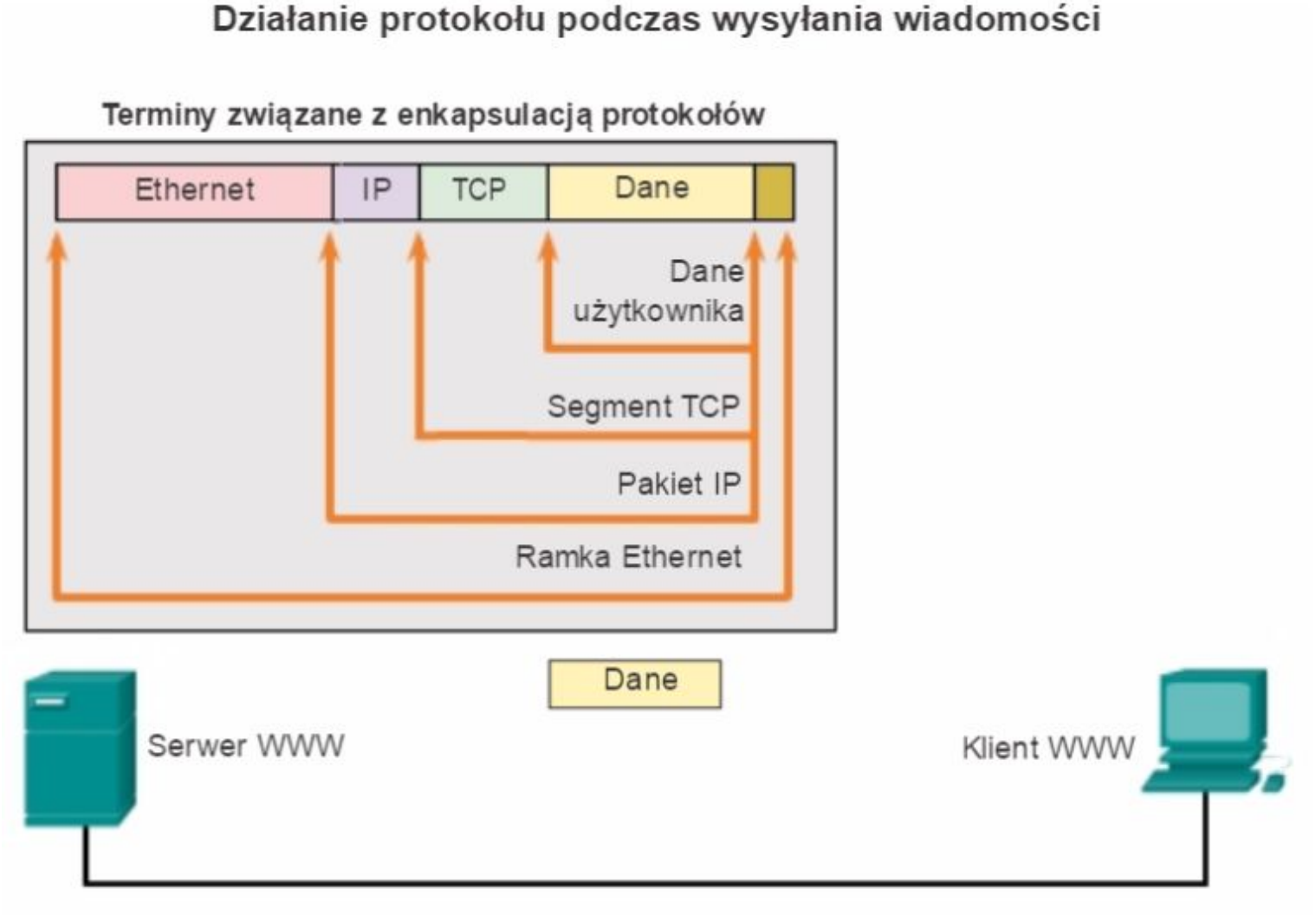
Jednostka danych protokołu PDU (ang. Protocol Data Unit)

- Dane
- Segment
- Pakiet
- Ramka
- Bity



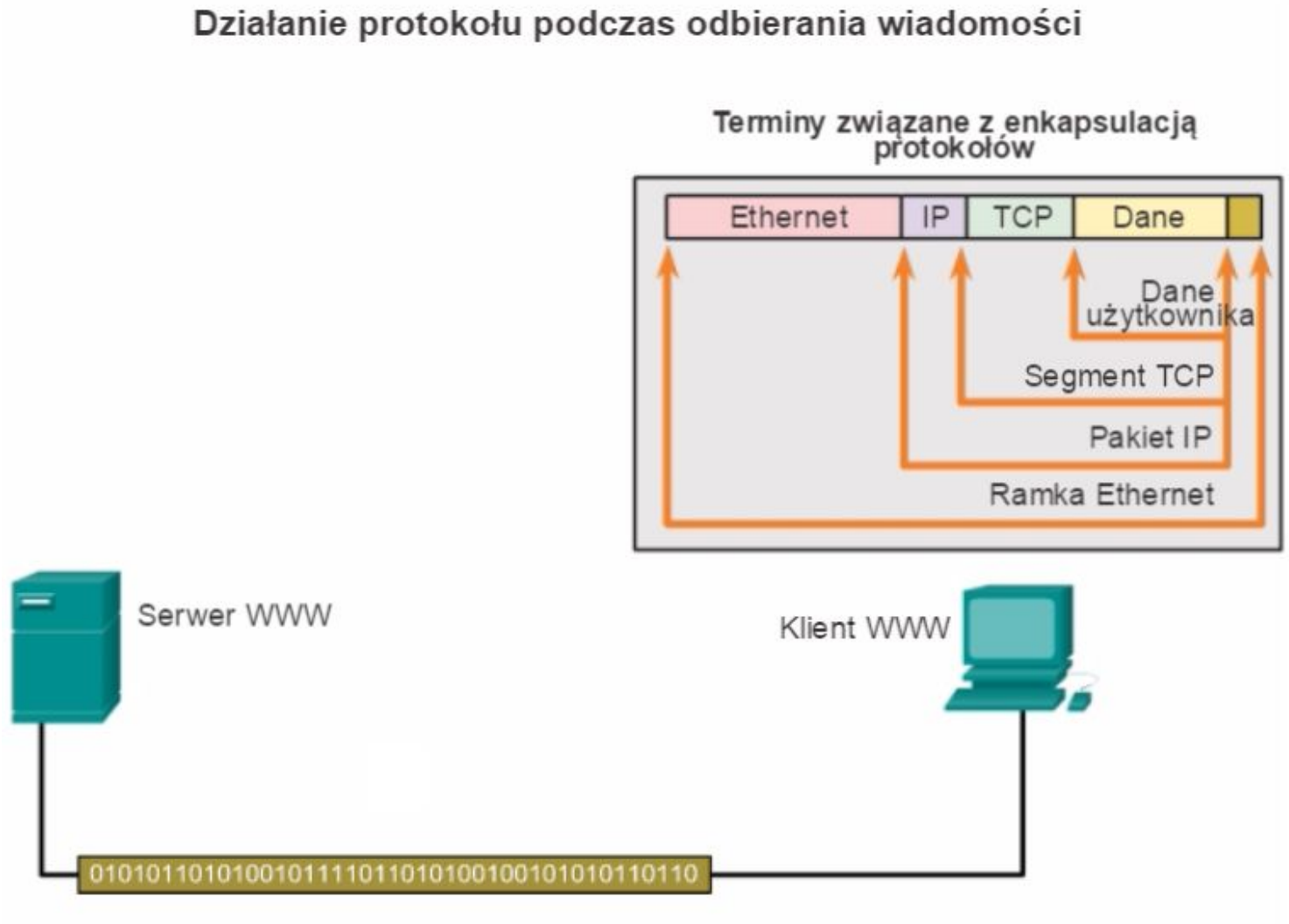
Enkapsulacja danych

Enkapsulacja



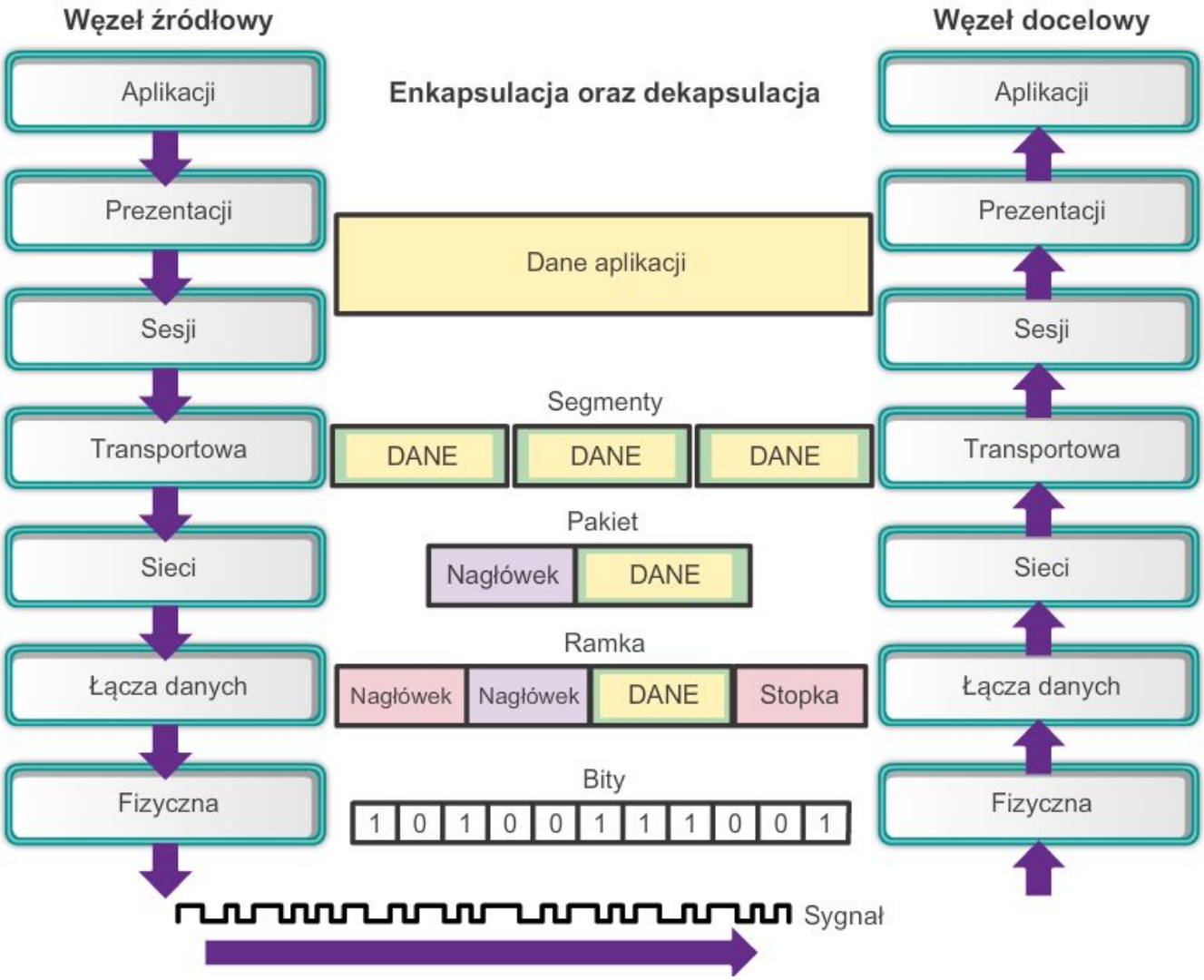
Enkapsulacja danych

Dekapsulacja



Warstwa fizyczna - cele

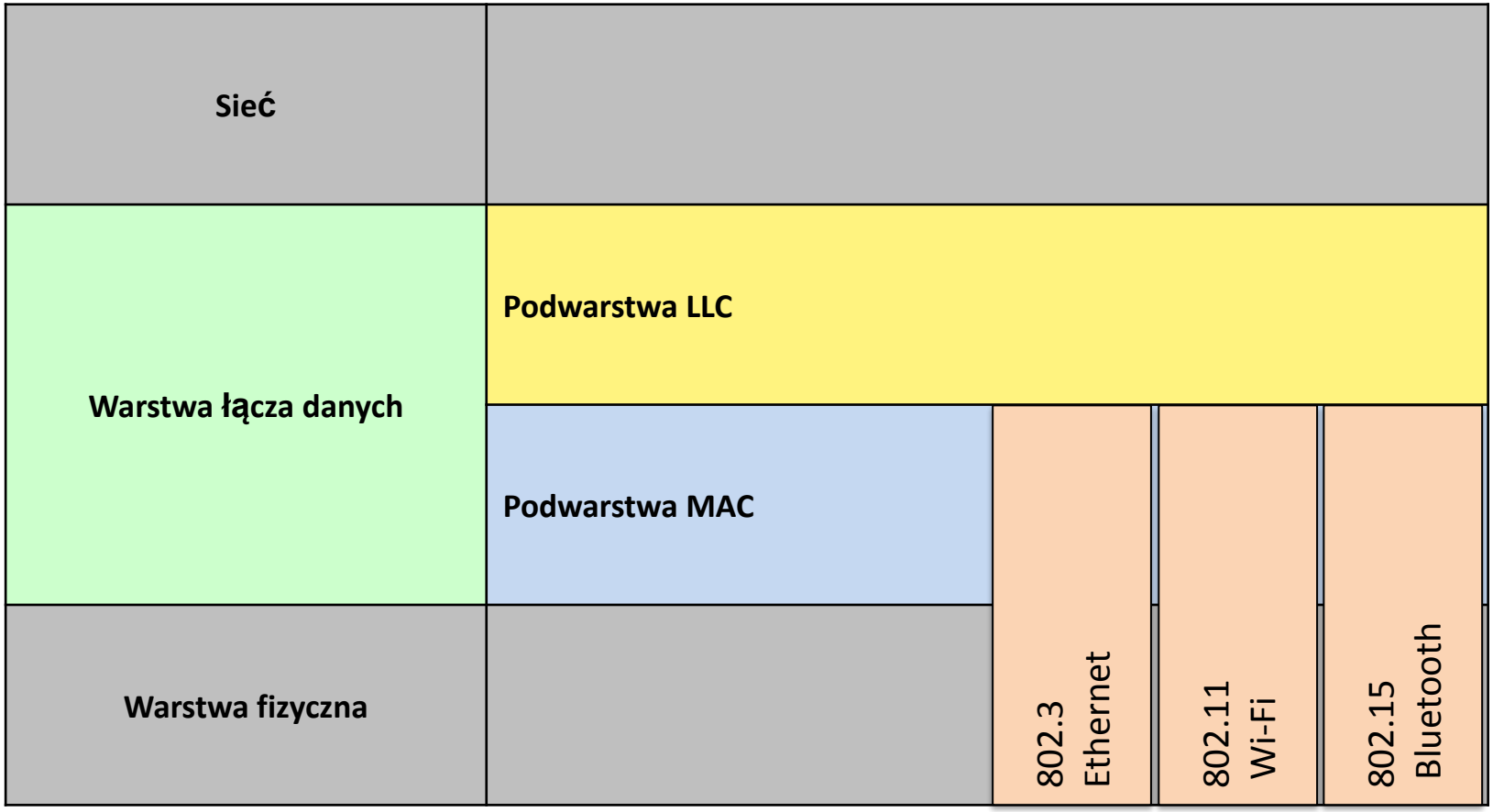
Warstwa fizyczna



Media sieciowe – budowa, zastosowania

- Światłowody (jedno i wielomodowe)
- Miedziane (UTP, STP, koncentryczny)
- Bezprzewodowe
- Złącza
- Właściwości

Podwarstwy warstwy łącza danych



Współdzielenie medium

- Rywalizacja, dostęp kontrolowany
- Kolizje, domeny kolizyjne

Ramka łącza danych

Ramka Ethernet

Protokół Ethernet

Powszechny protokół warstwy łącza danych w sieciach LAN

	Ramka					
Nazwa pola	Preambuła	Cel	Źródło	Typ	Dane	Suma kontrolna ramki
Rozmiar	8 bajtów	6 bajtów	6 bajtów	2 bajty	46-1500 bajtów	4 bajty

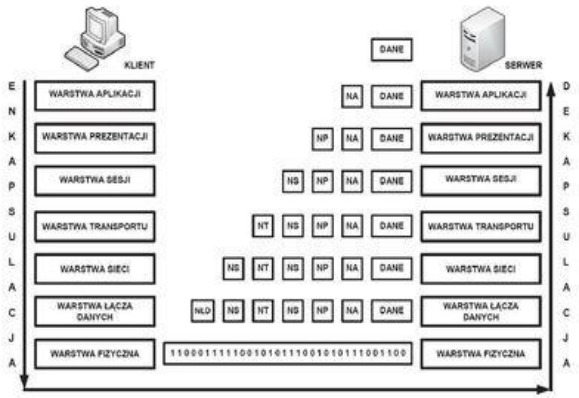
Preambuła - Wykorzystana w celu synchronizacji; zawiera również znacznik pozwalający na określenie zakończenia informacji taktowania.
Adres docelowy - 48 bitowy adres węzła docelowego.
Adres Źródłowy - 48-bitowy adres węzła źródłowego.
Typ - Wartość wskazująca jaki protokół warstwy wyższej otrzyma dane po zakończeniu procesu przetwarzania przez protokół Ethernet.
Dane - jest to datagram PDU, zazwyczaj jest to pakiet IPv4, który jest przesyłany przez medium.
Suma kontrolna ramki (FCS) - Wartość wykorzystywana w celu wykrycia uszkodzonych. ramek

Ethernet

Enkapsulacja

Warstwy w modelu odniesienia ISO/OSI współpracują ze sobą zarówno w pionie jak i w poziomie. Na przykład warstwa transportu klienta współpracuje z warstwami sesji i sieci klienta a także warstwą transportu serwera.

Enkapsulacja (dekapsulacja) danych

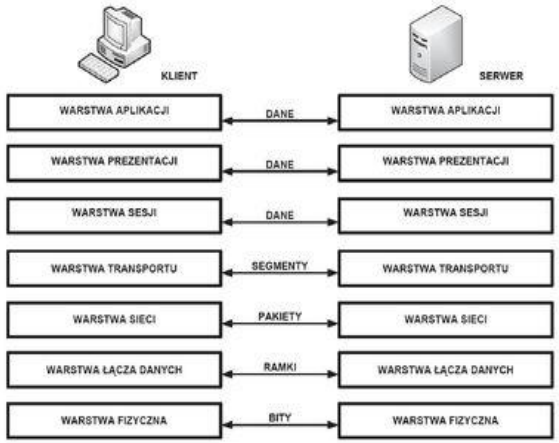


Rysunek 10.
Proces enkapsulacji i dekapsulacji danych

Enkapsulacja (dekapsulacja) danych jest procesem zachodzącym w kolejnych warstwach modelu ISO/OSI. Proces enkapsulacji oznacza dokładanie dodatkowej informacji (**nagłówka**) związanej z działającym protokołem danej warstwy i przekazywaniu tej informacji warstwie niższej do kolejnego procesu enkapsulacji. Proces **dekapsulacji** polega na zdejmowaniu dodatkowej informacji w kolejnych warstwach modelu ISO/OSI.

Dane, segmenty, pakiety, ramki, bity

W poszczególnych warstwach w modelu odniesienia ISO/OSI przechodzące dane noszą nazwę jednostek danych protokołu PDU (ang. *Protocol Data Unit*).



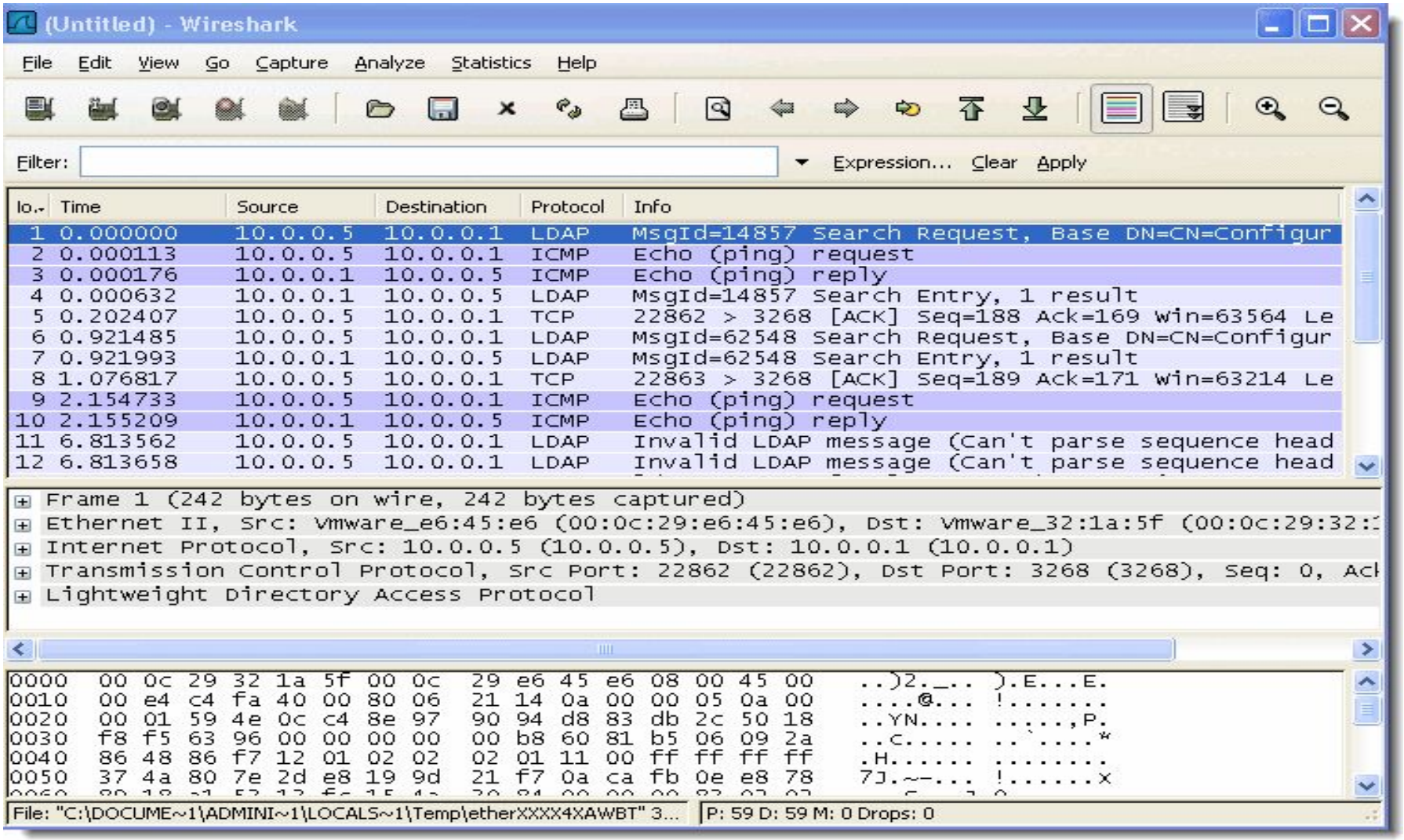
Rysunek 11.
Jednostki informacji w poszczególnych warstwach w modelu odniesienia ISO/OSI

Jednostki te mają różne nazwy w zależności od protokołu. I tak w trzech górnych warstwach mamy do czynienia ze **strumieniem danych**, w warstwie transportu są **segmenty**, w warstwie sieci są **pakiety**, w warstwie łącza danych – **ramki**, a w warstwie fizycznej – **bity** (zera i jedynki). Jednostki te w poszczególnych warstwach różnią się częścią nagłówkową.

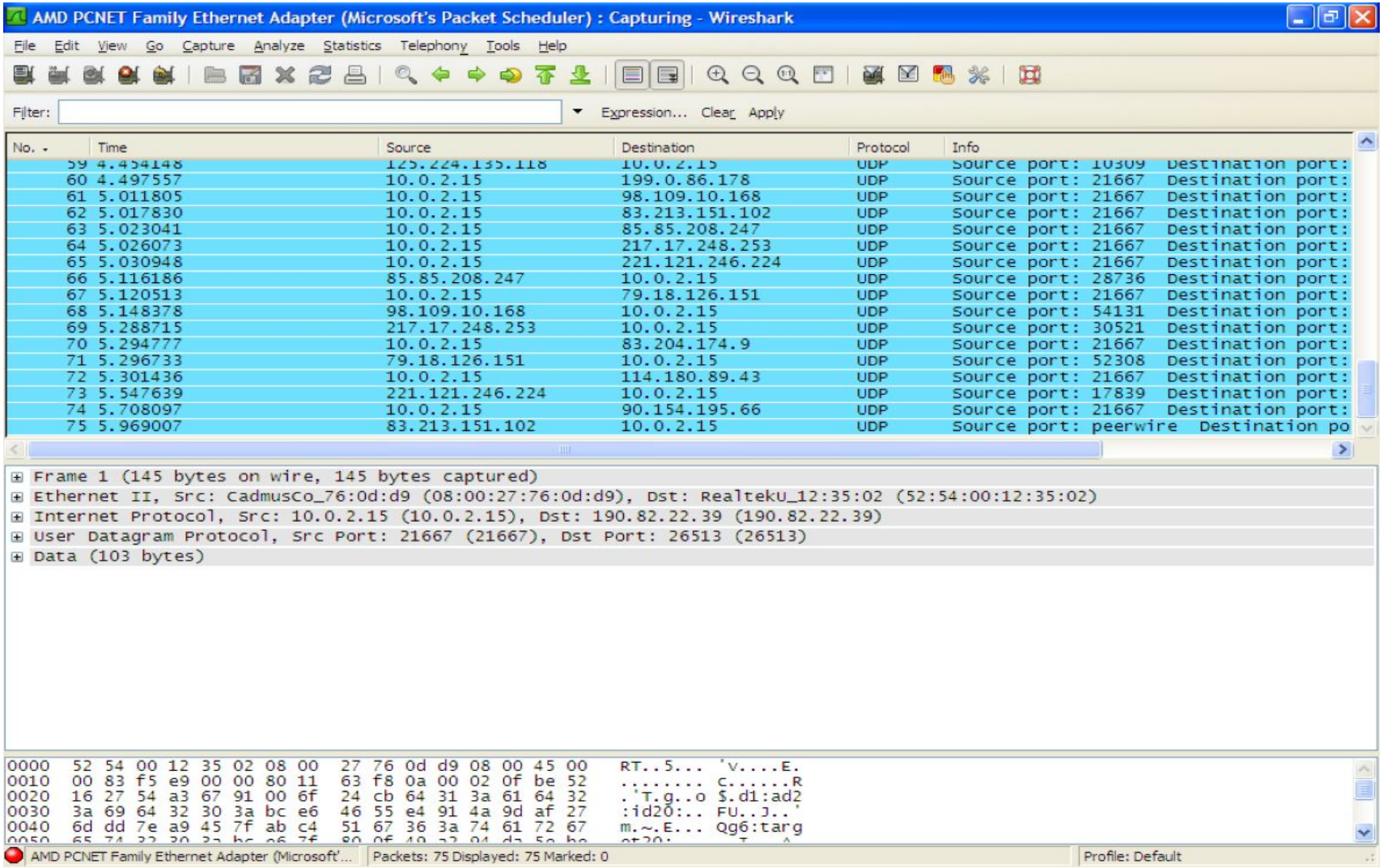
Model TCP/IP

Historycznie starszym modelem sieciowym jest **model TCP/IP** (ang. *Transmission Control Protocol/Internet Protocol*). Działanie sieci Internet opiera się właśnie na tym modelu sieciowym (patrz rys. 12). Opracowano go w połowie lat siedemdziesiątych XX wieku w amerykańskiej agencji DARPA (ang. *Defence Advanced Research Projects Agency*). Model TCP/IP składa się z czterech warstw.

Enkapsulacja w Wireshark



Enkapsulacja w Wireshark



Kontrola dostępu do medium

- Kontrola
- Adresy MAC
- Protokół ARP, tablica ARP
- Problemy ARP, eliminowanie problemów

Przełączniki

- Full Duplex, Half Duplex, Auto MDIX
- Metody przesyłania ramek (Fast Forward, Cut-through…..)
- Przełączniki wielowarstwowe

Warstwa sieci

Protokoły warstwy sieci

Podstawowe protokoły warstwy sieci to:

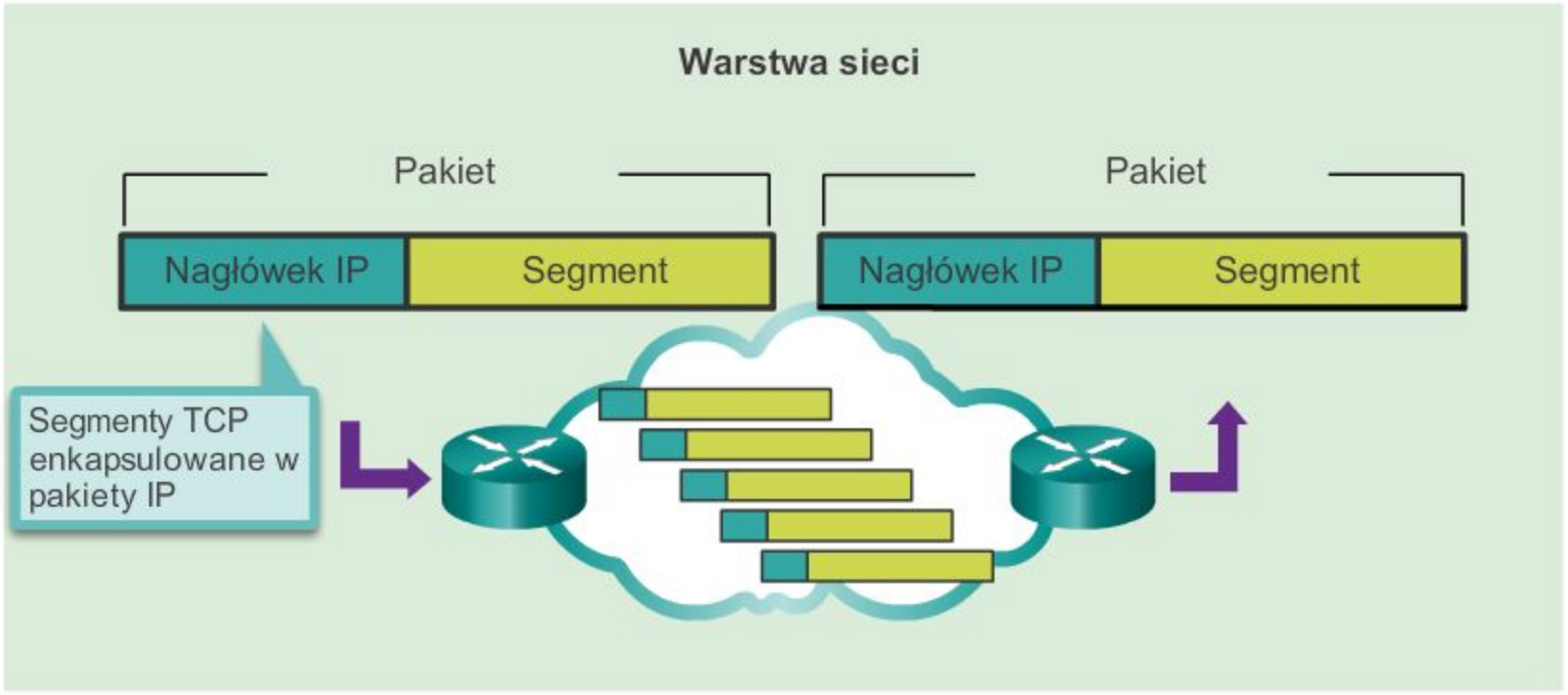
- IP w wersji 4 (IPv4)
- IP w wersji 6 (IPv6)

Tradycyjne protokoły warstwy sieci to:

- Protokół Novell IPX (Internetwork Packet Exchange)
- AppleTalk
- Bezpołączeniowa usługa sieciowa (CLNS/DECNet)

Charakterystyka IP

Komponenty IP



Pakiety IP przepływają przez sieć komputerową.

Charakterystyka protokołu IP

IP - Bezpołączeniowe

Komunikacja bezpołączeniowa

Nadawca nie wie:

- Czy odbiorca jest dostępny
- Czy przesyłka dotarła
- Czy odbiorca może przeczytać wiadomość

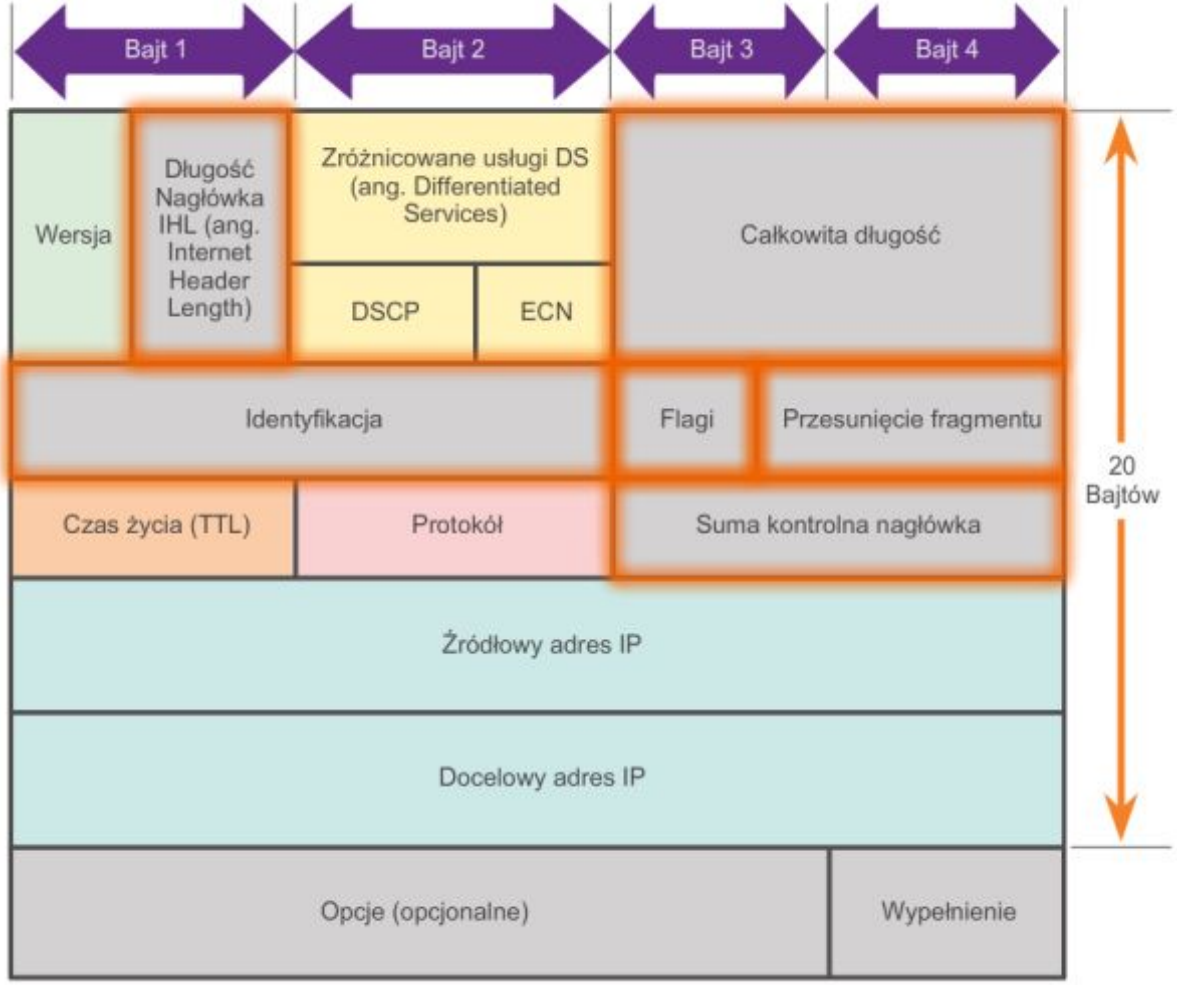
Odbiorca nie wie:

- Kiedy pakiet nadejdzie

IPv4 vs IPv6

IPv4 Nagłówek pakietu IPv4

Zawartość nagłówka pakietu IPv4



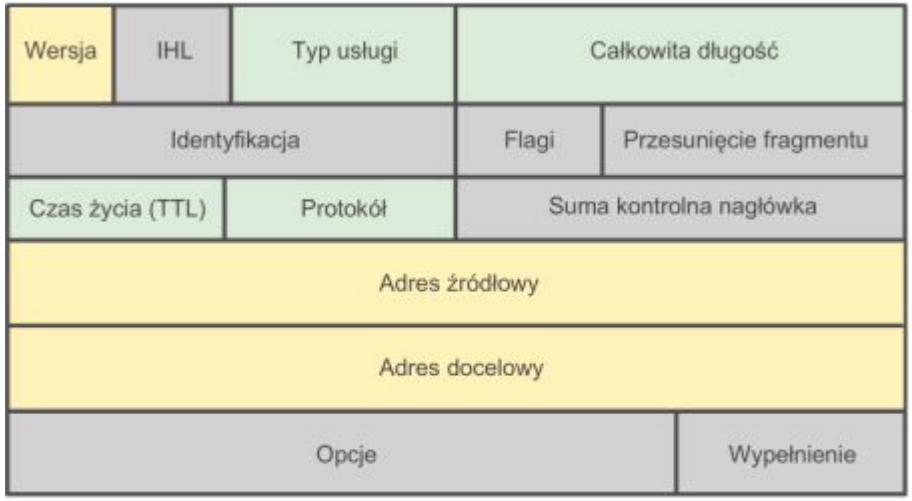
Wprowadzenie do IPv6

- zwiększona przestrzeń adresowa,
- udoskonalenie obsługi pakietów,
- eliminuje potrzebę wykorzystywania NAT,
- zintegrowane bezpieczeństwo,
- 4 miliardy adresów IPv4
  4 000 000 000
- 340 sekstylionów adresów IPv6
  340 000 000 000 000 000 000 000 000 000 000 000 000

Pakiet IPv6

Enkapsulacja IPv6

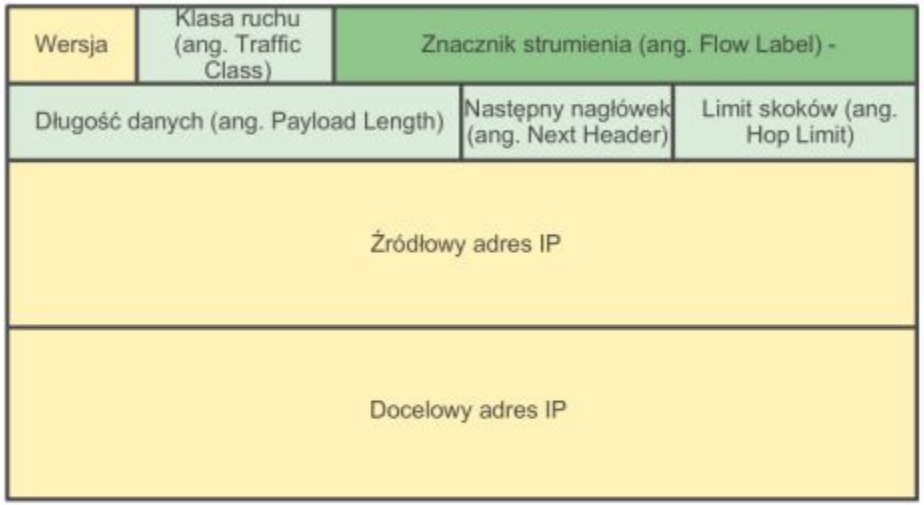
Nagłówek IPv4



Opis

- Nazwy pól protokołu IPv4 zachowane w protokole IPv6
- Nazwy pól oraz miejsca w datagramie zmienione w IPv6
- Pola niewystępujące już w protokole IPv6

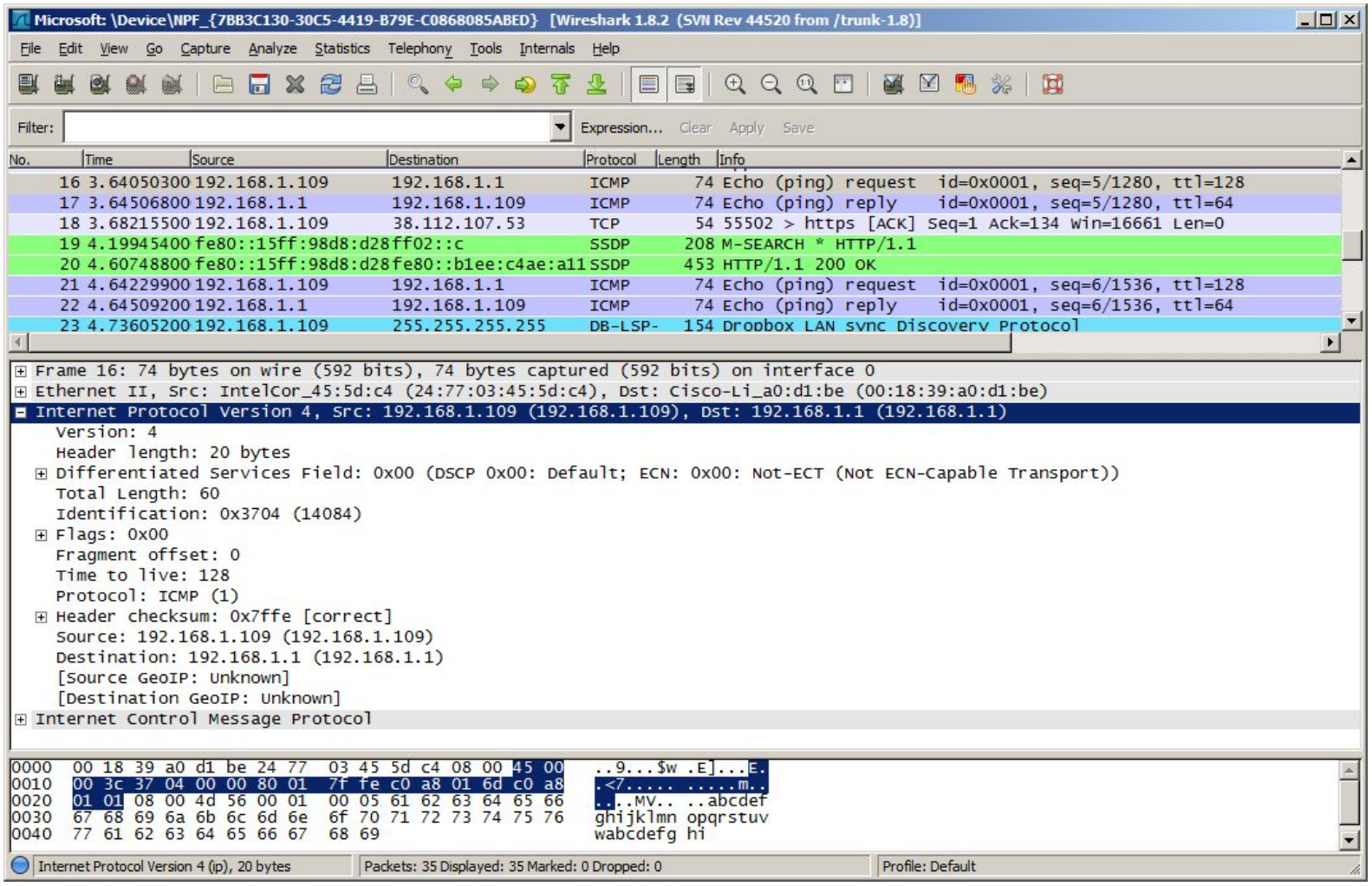
Nagłówek IPv6



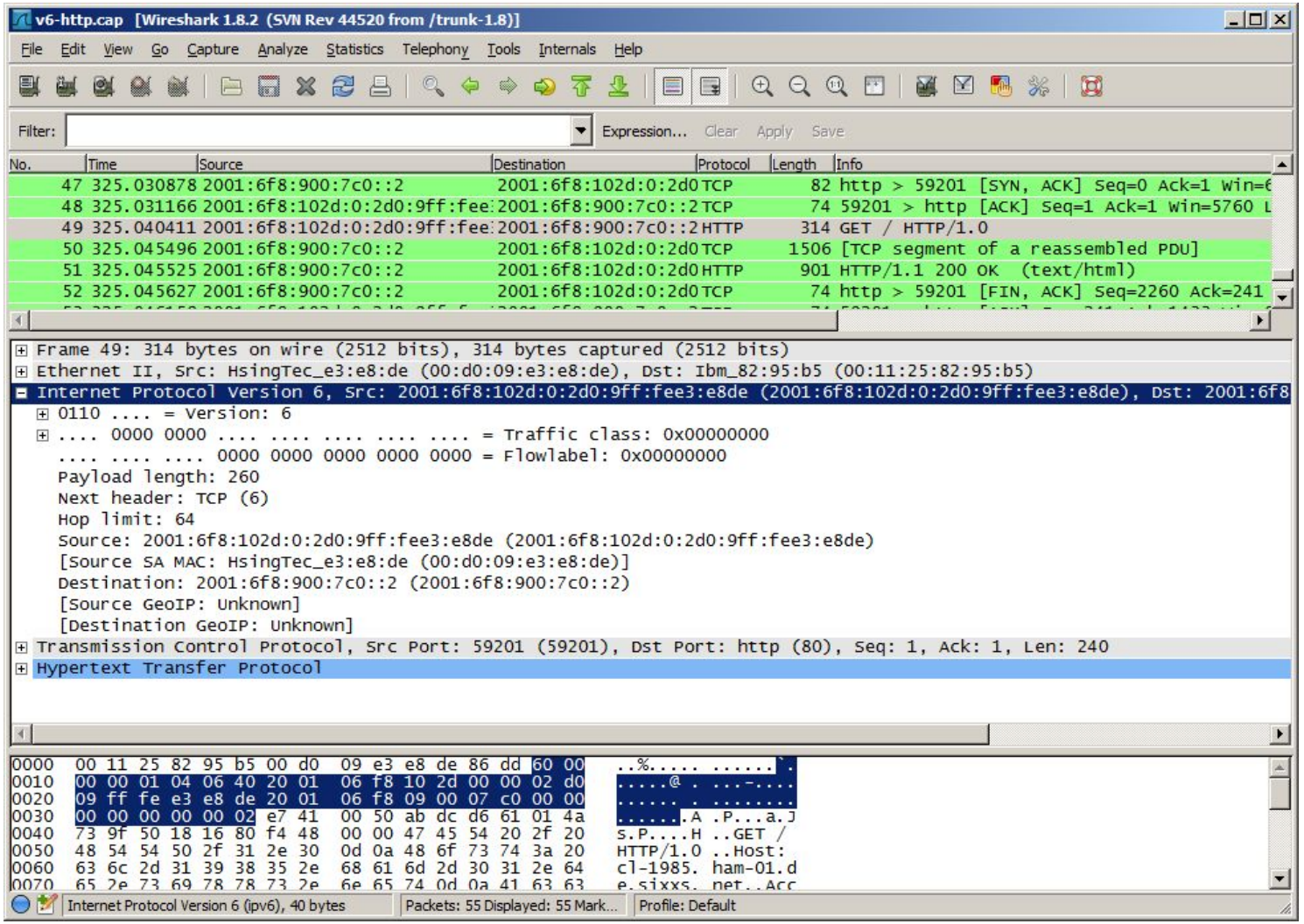
Opis

- Nazwy pól protokołu IPv4 zachowane w protokole IPv6
- Nazwy pól oraz miejsca w datagramie zmienione w IPv6
- Nowe pole w IPv6

Przykładowy nagłówek IPv4



Przykładowy nagłówek IPv6



Routing

- Brama domyślna, tablice routingu

Anatomia routera

Wnętrze routera

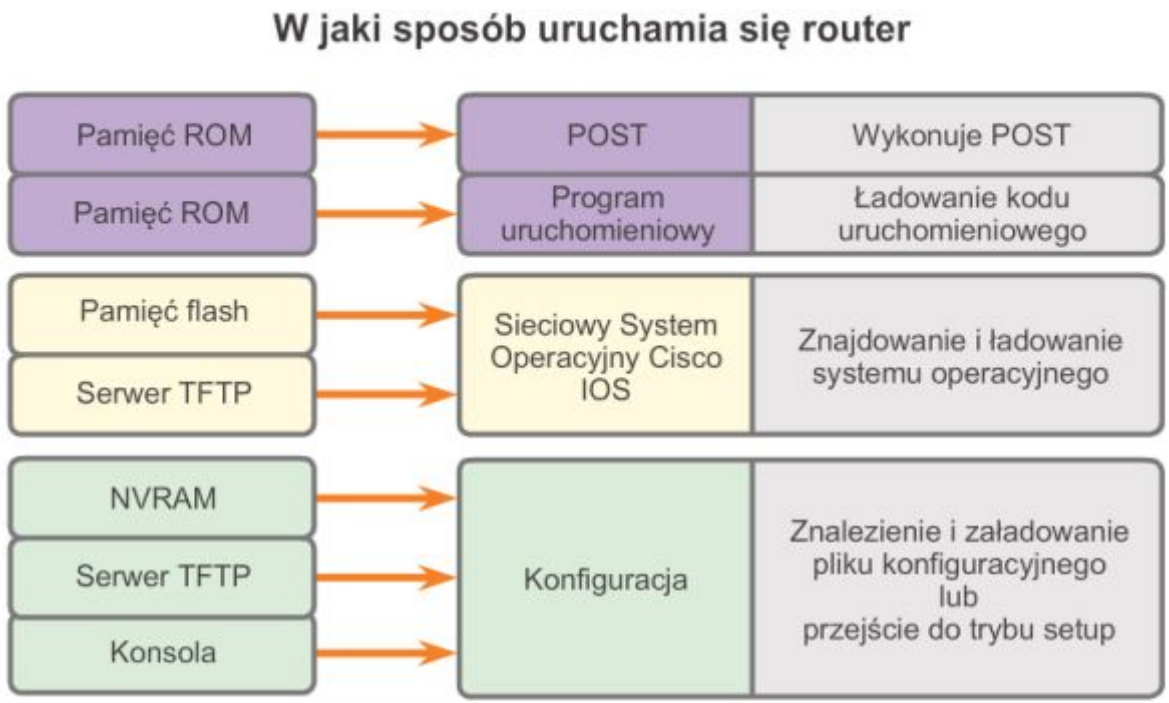
1. Moduł zasilacza
2. Gniazdo dla modułu WIC
3. Wentylator
4. SDRAM
5. NVRAM
6. Procesor
7. Advanced Integration Module (AIM)

Anatomia routera

Pamięć routera

Pamięć	Ulotna / Nieulotna	Przechowuje
RAM	Ulotna	• Uruchomiony IOS • Plik konfiguracji bieżącej (running-config) • Tablice routingu i tablice ARP • Bufor pakietów
ROM	Nieulotna	• Rozkazy procesu rozruchowego • Podstawowe oprogramowanie diagnostyczne • Ograniczony funkcjonalnie IOS
NVRAM	Nieulotna	• Plik konfiguracji startowej
Pamięć flash	Nieulotna	• IOS • Pozostałe pliki systemowe

Proces rozruchu routera



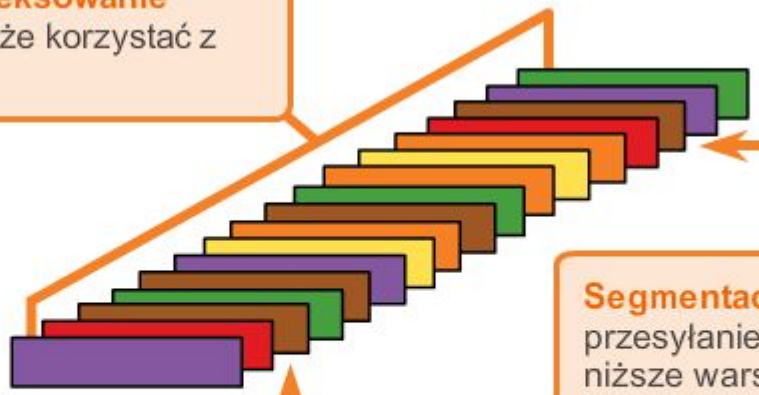

```
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport

<saída omitida>
```

Warstwa transportowa

TCP i UDP

Multipleksowanie konwersacji (cd.)

Segmentacja umożliwia **multipleksowanie** konwersacji - wiele aplikacji może korzystać z sieci w tym samym czasie.



Segmentacja umożliwia przesyłanie danych przez niższe warstwy sieciowe.

Kontrola błędów może zostać przeprowadzona na danych w segmencie w celu sprawdzenia, czy zawartość segmentu zmieniła się podczas jego transmisji.

Niezawodność warstwy transportowej

Różne aplikacje mogą wymagać różnych mechanizmów niezawodności.
TCP/IP zapewnia dwa protokoły warstwy transportowej, **TCP i UDP.**

TCP

- Zapewnia niezawodność dostarczenia upewniając się że wszystkie dane dotarły do celu.
- Wykorzystuje potwierdzenie dostarczenia i inne procesy w celu zapewnienia dostarczenia.
- Ma większe wymagania sieciowe- większe narzuty.

UDP

- Zapewnia tylko podstawowe funkcje dostawy - bez zapewnienia niezawodności.
- Mniejszy narzut

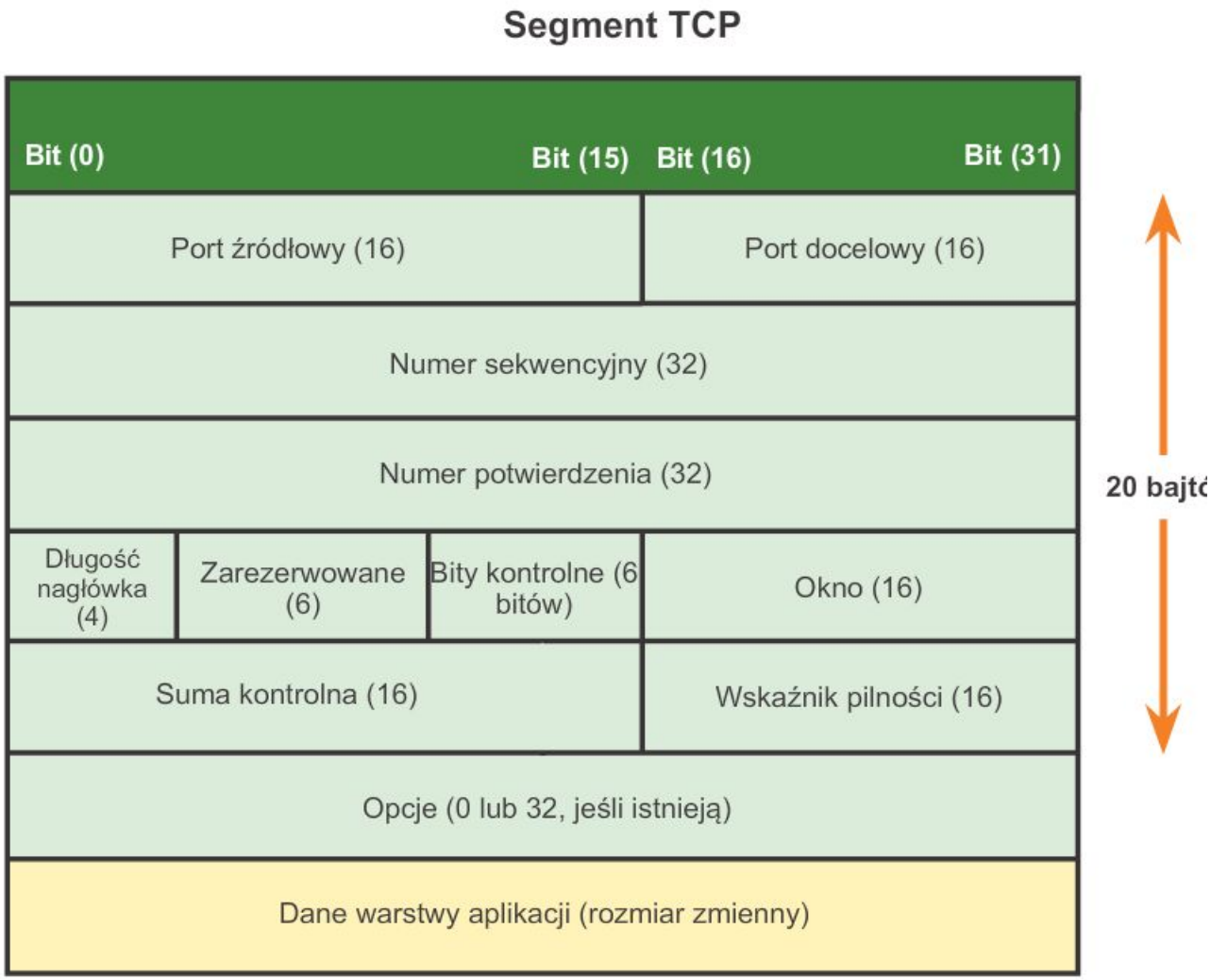
TCP czy UDP

- Jest to kompromis pomiędzy wartością niezawodności i obciążeniem wprowadzanym przez nią do sieci.
- Twórcy aplikacji wybierają protokół transportowy w oparciu o wymagania ich aplikacji.

Wprowadzenie do TCP

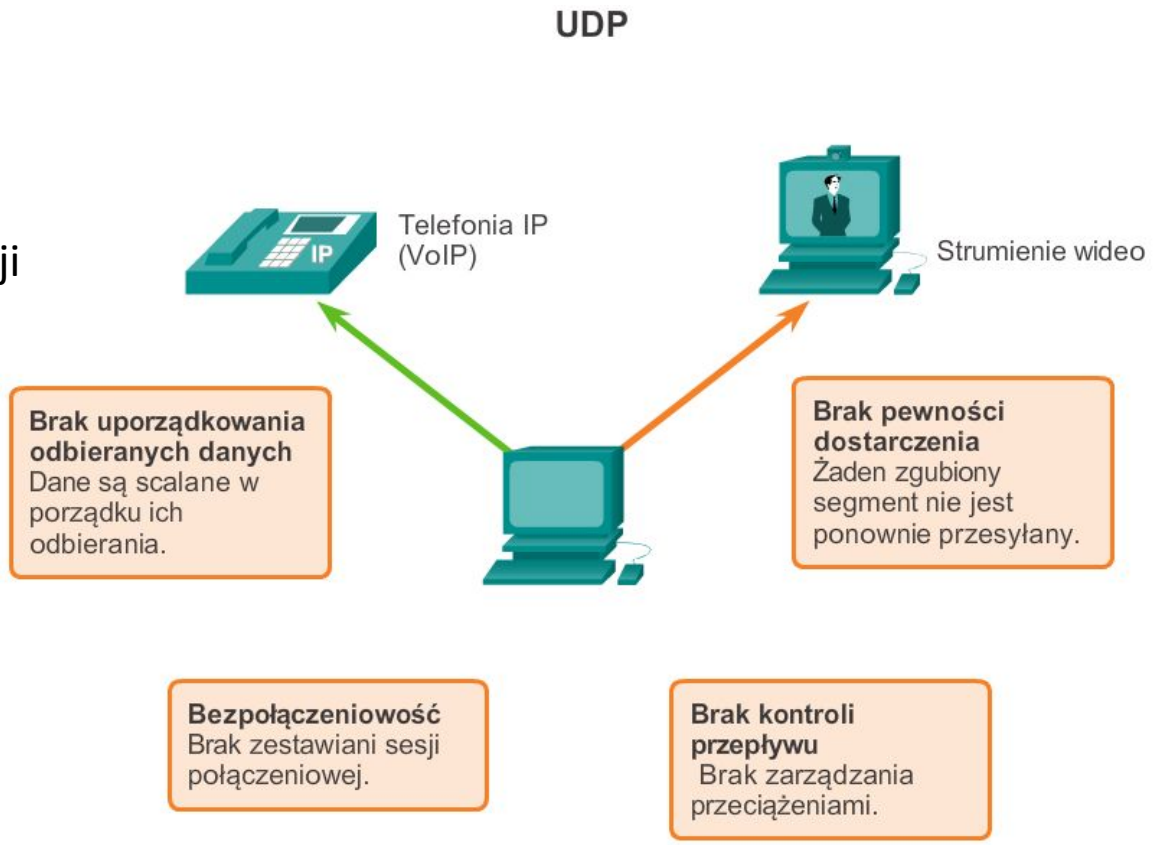
- Zdefiniowany w RFC 793
- Połączeniowy - tworzy sesję pomiędzy źródłem a odbiorcą.
- Niezawodna dostawa - retransmituje utracone lub uszkodzone dane.
- Uporządkowana rekonstrukcja danych - rekonstruuje numerację i sekwencjonowanie segmentów.
- Kontrola przepływu - reguluje ilość przesłanych danych.
- Protokół stanowy - śledzenie sesji.

Wprowadzenie do TCP



Wprowadzenie do UDP

- RFC 768.
- Bezpołączeniowy.
- Brak gwarancji dostarczania danych.
- Brak możliwości rekonstrukcji danych we właściwej kolejności.
- Brak kontroli przepływu.
- Protokół bezstanowy.



Aplikacje wykorzystujące UDP:

- Protokół DNS (ang. Domain Name System), system nazw domenowych)
- aplikacje przesyłające strumienie Video,
- VoIP

TCP, UDP, adresacja portów

- Porty dobrze znane,
- Zarejestrowane
- prywatne i/lub dynamiczne

- Niezawodność TCP
- Szybkość UDP

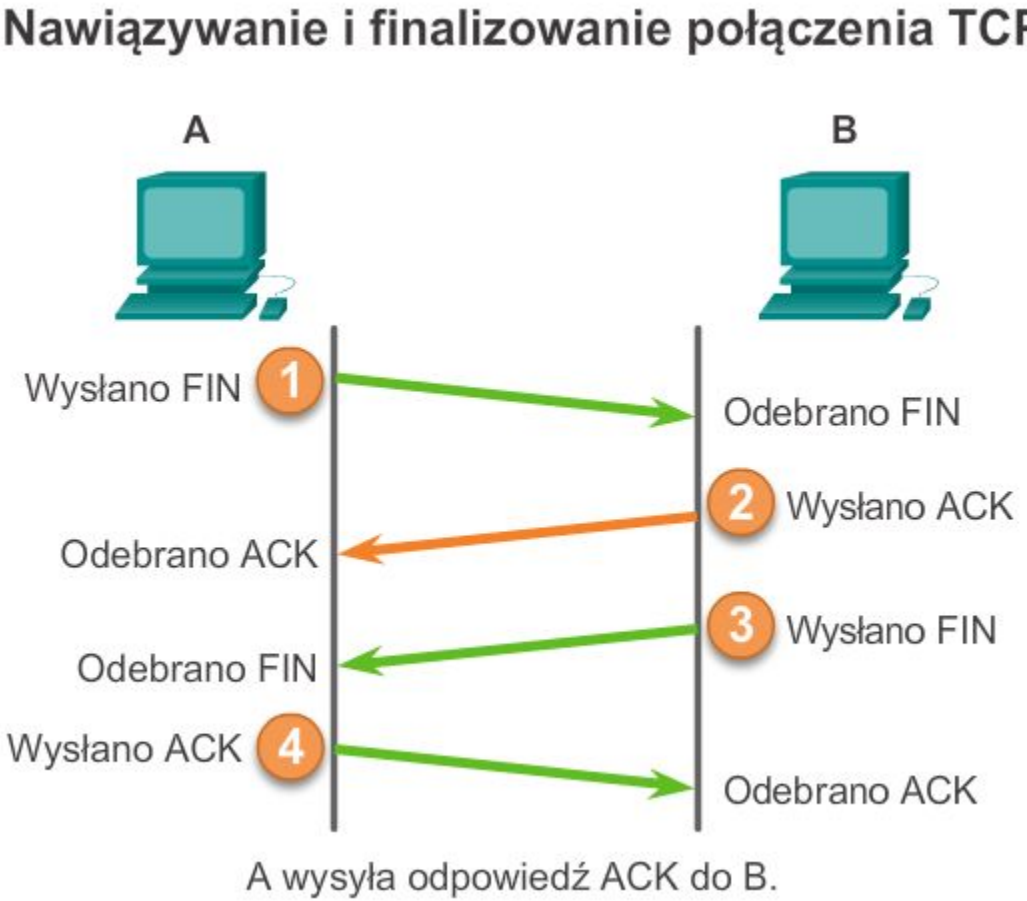
Porty programów w TCP

Numer portu TCP	Opis
20	Serwer FTP (kanał danych)
21	Serwer FTP (kanał kontrolny)
23	Serwer Telnet
53	Transfery stref DNS
80	Serwer sieci Web (HTTP)
139	Usługa sesji NetBIOS

Porty UDP

Numer portu UDP	Opis
53	Kwerendy nazw DNS
69	Protokół TFTP (Trivial File Transfer Protocol)
137	Usługa nazw NetBIOS
138	Usługa datagramów NetBIOS
161	Protokół SNMP (Simple Network Management Protocol)
520	Protokół RIP (Routing Information Protocol)

Kończenie sesji TCP (i nawiązywanie sesji)



Porównanie UDP i TCP

UDP

Usługa bez ustanowionego połączenia; między hostami nie jest ustanawiana sesja.

Protokół UDP nie gwarantuje dostarczenia przesyłki, a także potwierdzania i szeregowania danych.

Programy wykorzystujące protokół UDP odpowiadają za prawidłowe transportowanie danych.

Protokół UDP jest szybki, ma niskie wymagania organizacyjne i obsługuje połączenia bezpośrednie i połączenia jednego punktu z wieloma punktami.

TCP

Usługa zorientowana na połączenie; między hostami jest ustanawiana sesja.

Protokół TCP gwarantuje dostarczenie przesyłki dzięki użyciu potwierdzania i szeregowania dostarczania danych.

Programy wykorzystujące protokół TCP mają zapewniony niezawodny transport danych.

Protokół TCP jest wolniejszy, ma wyższe wymagania organizacyjne i obsługuje tylko połączenia bezpośrednie.

Adresacja IP i podsieci

ADRESY INTERNETOWE

ADRES **IP** → identyfikacja docelowej maszyny

ADRES **IP** → identyfikuje interfejs sieciowy komputera

jeżeli komputer posiada wiele interfejsów sieciowych (np. do różnych sieci) - będzie też posiadał wiele adresów IP

! Tak jak w przypadku telefonów, wszystkie sieci pewnego dnia będą połączone ze sobą.

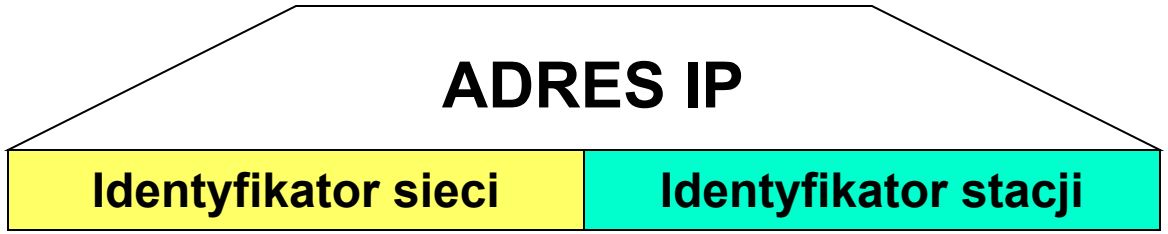
IP musi być unikalny w sensie globalnym

przyznawanie IP musi być koordynowane globalnie

Obecnie (**IP v.4**) → używane są adresy **32 bitowe**

co pozwala nadać adresy $\mathbf{2^{32}}$ stacjom

czyli 4 294 967 296 stacjom

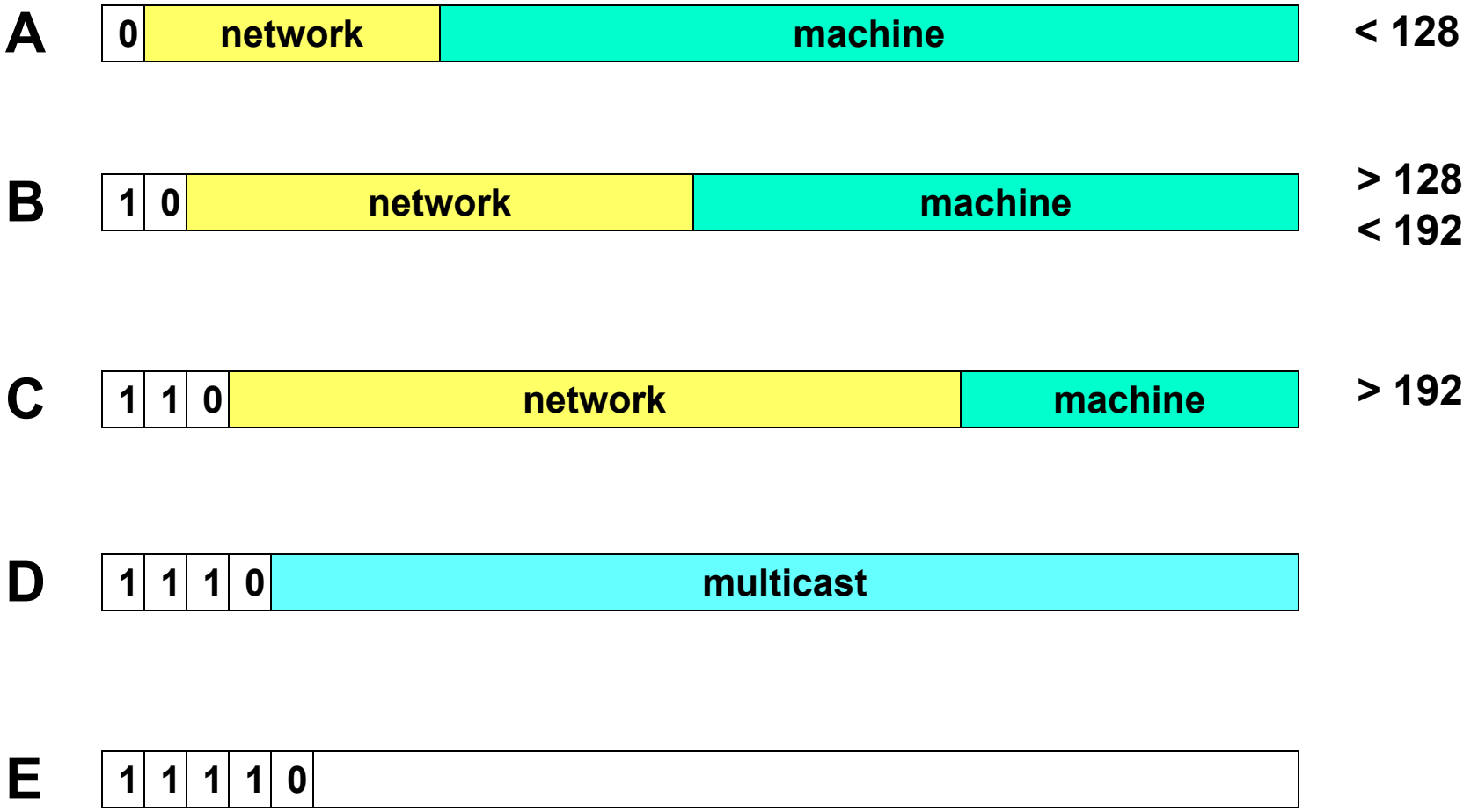


- **Routowanie w sensie globalnym** „nie przejmuje się” identyfikowaniem stacji - uwzględniany jest jedynie identyfikator sieci
- **Routowanie lokalne** (tzn. takie w którym id_sieci = IP_sieci w adresie) używa jedynie identyfikatora stacji.
- Jeżeli komputer zostanie przeniesiony do innej sieci jego adres musi ulec zmianie.

KLAS A

5 KLAS ADRESÓW IP

NUMER SIECI



NOTACJA ADRESÓW IP - „kropkowana” dziesiętna

przykład **130.104.29.10**

128<130<192
klasa B

Stacja nr 29.10

ADRESY SPECJALNE

0 oznacza „this” - określenie aktualnej sieci

wszystkie bity = 1 wszystkie maszyny w danej sieci (*Broadcast address)*

127.0.0.1 lokalna pętla umożliwiająca TCP/IP komunikację pomiędzy procesami na lokalnej maszynie

PROBLEMY Z ADRESAMI IP

- Adresy dla sieci klasy B są już prawie wyczerpane
- Nie stworzono klas dla średnich wielkości sieci (pomiędzy 256 a 5000 stacji)
- Rozmiary tablic routingu wymykają się spod kontroli
  - nie ma związku z numerem sieci i jej lokalizacją
  - w backbone routerach w tablicach routingu znajduje się po jednej linii dla każdego adresu IP na świecie !

ROZWIĄZANIE: CIDR (Classless Inter-Domain Routing)

- generalizacja idei maskowania
- fuzja klas A,B i C
- sieć identyfikowana przez parę <prefix maska>

Maski

- Daną klasę adresów można podzielić na logiczne podsieci za pomocą Maski
- Jeśli bit w masce ma wartość 1, to odpowiadający mu bit w adresie IP jest bitem części sieciowej
- Jeśli bit w masce jest równy 0, to bit adresu należy do części określającej komputer

Przykład maski

adres dziesietnie	62	121	77	1
adres bitowo	00111110	01111001	01001101	00000001
maska dziesietnie	255	255	252	0
maska bitowo	11111111	11111111	11111100	00000000

Operacja AND na odpowiadających sobie bitach adresu IP i Maski pozwala ustalić adres sieci

Maski podsieci dla klas adresów

Klasa adresu	Bity maski podsieci	Maska podsieci
Klasa A	11111111 00000000 00000000 00000000	255.0.0.0
Klasa B	11111111 11111111 00000000 00000000	255.255.0.0
Klasa C	11111111 11111111 11111111 00000000	255.255.255.0

Poziomy hierarchii w adresacji IP

- Tradycyjna adresacja (dwupoziomowa): sieć i host (router przekazuje pakiet do właściwej sieci, korzystając z części sieciowej adresu a po osiągnięciu sieci identyfikuje urządzenie końcowe korzystając z części hostowej adresu IP
- Współcześnie (trzypoziomowa): sieć, podsieć, host. Efektem jest przyśpieszenie dostarczenia pakietu i minimalizacja ruchu lokalnego.

Po co podział na podsieci?

Łatwiej zapanować nad kilkoma mniejszymi częściami niż nad dużą całością

Minimalizowanie ruchu wewnętrznego (np. transmisje rozgłoszeniowe)

Kryteria podziału na podsieci

- Lokalizacja geograficzna (np. piętra w budynku)
- Jednostki organizacyjne (sprzedaż, księgowość, projektanci)
- Typy urządzeń (serwery, drukarki)
- Inne – logiczny i ważny

Adresy prywatne - zakresy

- 10.0.0.0 z maską podsieci 255.0.0.0
- 172.16.0.0 z maską podsieci 255.240.0.0
- 192.168.0.0 z maską podsieci 255.255.0.0

Zadanie: dla każdej z sieci ustal: minimalny i maksymalny adres hosta oraz liczbę hostów, które w niej zaadresujemy.

Stwórz standardy nadawania adresacji IP w zakresie poszczególnych sieci

- Drukarki oraz serwery będą miały przypisane statyczne adresy IP
- Użytkownicy otrzymają adresy IP z serwera DHCP wykorzystując podsieci z maską /24
- Routerom przypisano pierwszy dostępny adres hosta z puli adresów

A gdy już będziesz umiał(a)….

- www.ipcalc.org – może nie działać
- www.subnetmask.info
- www.42.pl

Projektowanie sieci

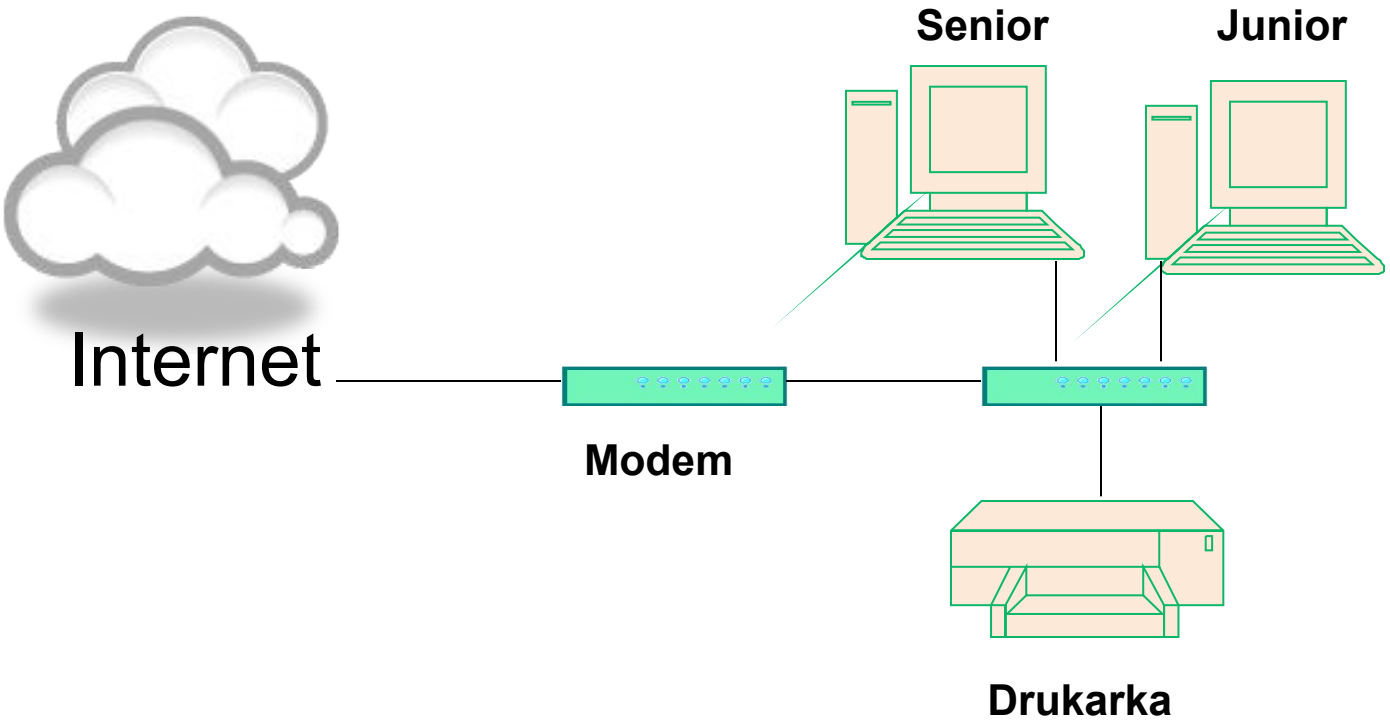
Co to jest niezbędne do budowy sieci?

Aby zbudować sieć komputerową, musimy:

- Zaopatrzyć komputery w karty sieciowe,
- Wybrać odpowiednią topologię sieci,
- Ułożyć okablowanie,
- Zainstalować oprogramowanie klienta sieci,
- Wybrać usługi, z których chcemy korzystać,
- Przydzielić i skonfigurować odpowiednie protokoły komunikacyjne.

Ze względu na rodzaj okablowania aktualnie najpopularniejsze

Są sieci wykonane przy użyciu skrętki ekranowanej lub nieekranowanej



Nawet najmniejsza sieć komputerowa umożliwia korzystanie ze wspólnych zasobów, urządzeń, Internetu oraz realizację projektów zespołowych. Umożliwia również komunikację (dźwięk, obraz, tekst).

Konfiguracja komputerów sieciowych

Kiedy już przygotujemy połączenie sieciowe, można przystąpić do uruchomienia i konfiguracji sieci.

Każdy komputer sieciowy musi posiadać:

- kartę sieciową zgodną ze standardem sieci – najczęściej Fast Ethernet,
- oprogramowanie nazywane klientem sieci i zgodnie z SO,
- protokół sieciowy – sugerujemy wybór protokołu TCP/IP jako najbardziej uniwersalnego i niezbędnego przy połączeniu z Internetem.

Brama

Brama (ang. Gateway) – urządzenie posiadające własny adres IP. Umożliwia ono dostęp do Internetu. Bramą może być router, jak też komputer z dołączonym terminalem SDI. Brama znajduje się w obrębie sieci lokalnej.

Serwer DHCP

Serwer DHCP – program przydzielający automatycznie adresy IP kolejno przyłączanym do sieci komputerom. W sieci lokalnej serwer DHCP może być związany z urządzeniem pełniącym funkcję bramy, a więc np. z routerem. Lokalny serwer DHCP może przydzielać adresy z puli przeznaczonej dla sieci lokalnej. Dynamiczne przydzielone adresy tracą ważność z chwilą odłączenia komputera od sieci. Przy następnym przyłączeniu otrzymany adres może być inny. Na serwerze dostawcy Internetu również działa serwer DHCP. Przydziela on chwilowe adresy IP zgłaszającym się do niego sieciom lokalnym. Numer ten przekazany jest urządzeniu dostępowemu (modem, terminal ISDN, karta sieciowa).

Serwer DNS

Serwer DNS (z ang. Domain Name Server) – serwer nazw domenowych tłumaczący literowe nazwy serwerów przyjazne dla ludzi na ich odpowiedniki liczbowe zrozumiałe dla maszyn. Dzięki wykorzystaniu DNS nazwa mnemoniczna, może zostać zamieniona na odpowiadający jej adres IP, czyli *145.97.39.155*.

Adresy DNS składają się z domen internetowych rozdzielonych kropkami. W ten sposób możliwe jest budowanie hierarchii nazw, które porządkują Internet. DNS to złożony system komputerowy oraz prawny. Zapewnia z jednej strony rejestrację nazw domen internetowych i ich powiązanie z numerami IP. Z drugiej strony realizuje bieżącą obsługę komputerów odnajdujących adresy IP odpowiadające poszczególnym nazwom.