AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Sieci komputerowe

Protokoły warstwy transportowej

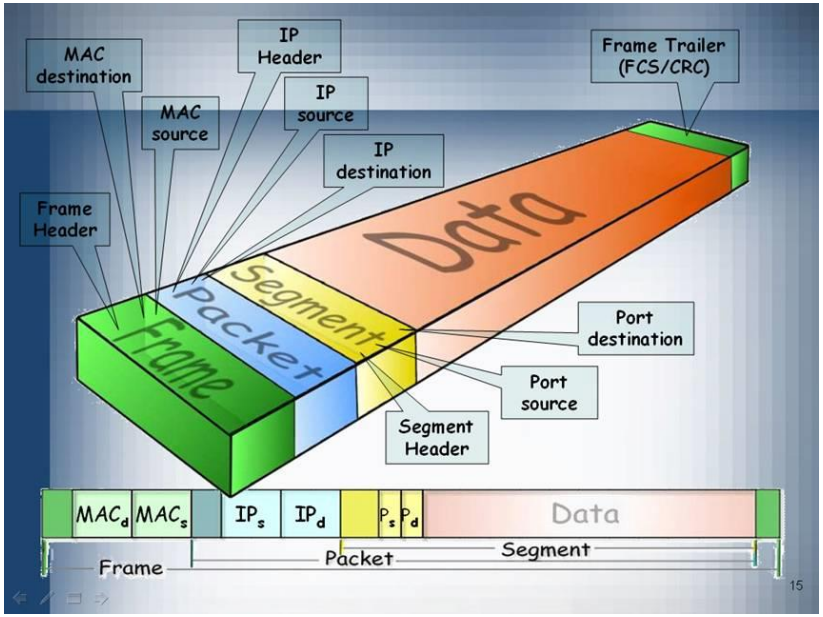
dr inż. Andrzej Opaliński
andrzej.opalinski@agh.edu.pl

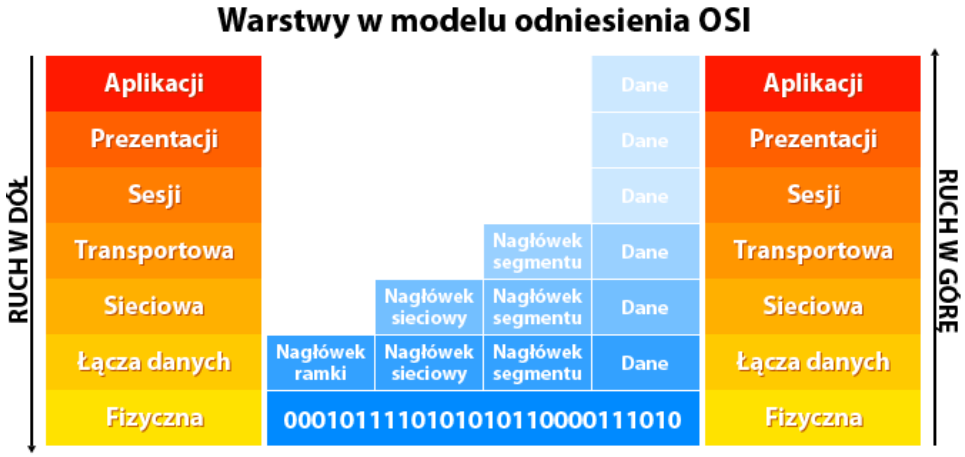
Plan wykładu

- **Wprowadzenie – opis warstwy transportowej**
- **Protokoły spoza stosu TCP/IP**
- **Protokół UDP**
- **Protokół TCP**
- **Porównanie**

Transmisja danych - przypomnienie

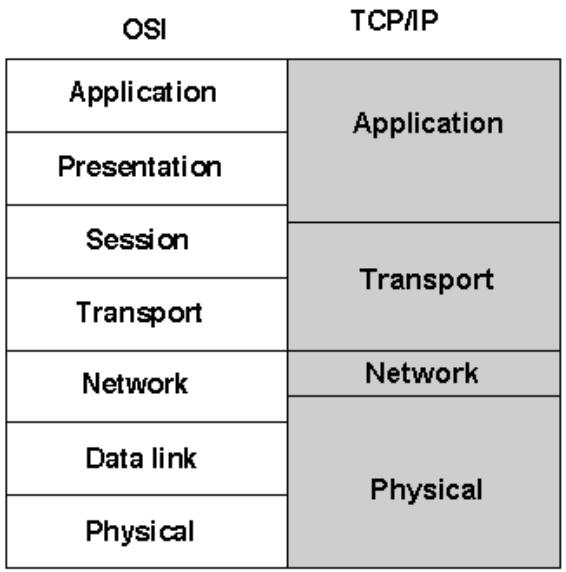
- **Enkapsulacja**
- **Analiza poszczególnych warstw**





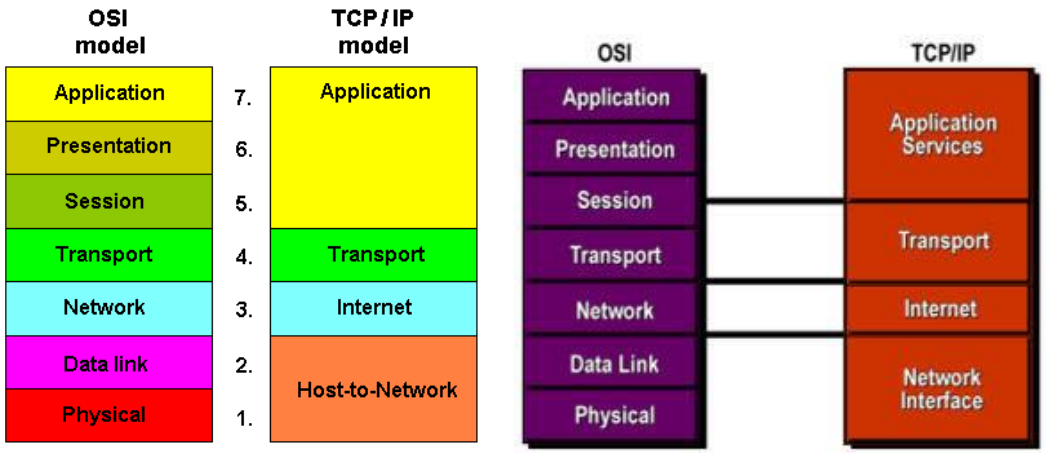
Wprowadzenie

- **Warstwa transportowa (OSI-ISO / TCP/IP)**
  - Zadanie: niezawodne przesyłanie danych między urządzeniami
  - Zawiera mechanizmy:
    - Inicjacji, utrzymania, zamykania połączenia między urządzeniami
    - Sterowania przepływem danych
    - Wykrywania błędów transmisji
- **Protokoły działające w obrębie warstwy transportowej**
  - DCCP
  - SCTP
  - RSVP
  - TCP
  - UDP



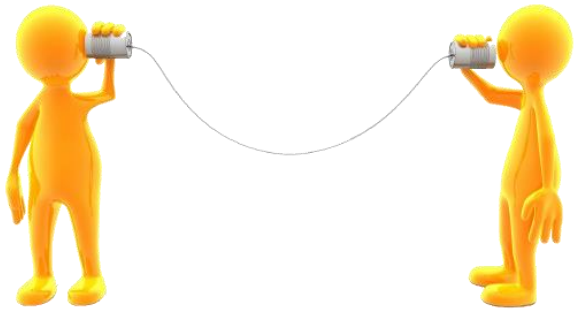
Funkcjonalności warstwy transportowej

- **Komunikacja (bez)połączeniowa** – zestawienie połączenia, interpretowanie połączenia jako ciągłego strumienia danych
- **Zachowanie kolejności dostarczenia pakietów**
- **Niezawodność dostarczenia pakietów** (kody kontrolne, ACK/NACK)
- **Kontrola przepływu** (dostosowanie przepustowości transmisji do możliwości odbiorcy/sieci)
- **Unikanie (kontrola) przeciążeń** (avoid oversubscription, link capabilities, slow-start)
- **Multipleksacja**
  - gniazdo/porty,
  - w modelu TCP,
  - w modelu OSI w warstwie sesji



Klasyfikacje komunikacji w warstwie transportowej

- **Połączeniowa (connection-oriented)**
  - Etap połączenia przed właściwym przesłaniem danych
- **Bezpołączeniowa (connectionless)**
  - Przesyłanie danych bez sprawdzania czy dotarły do adresata

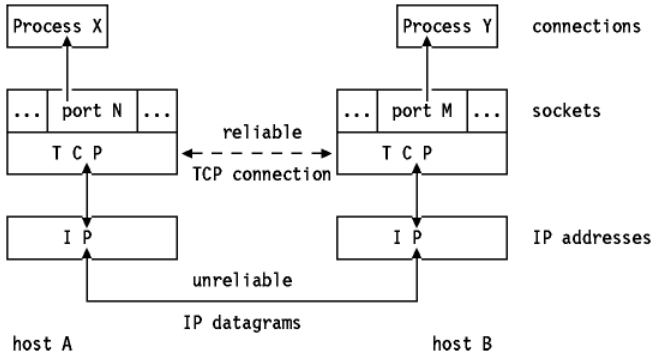


- **Niezawodna (reliable)**
  - Zapewnienie kontroli procesu przesyłania,
  - ponawianie transmisji w wypadku niedostarczenia segmentu
- **Zawodna (unreliable)**
  - Brak kontroli dostarczenia pakietów
  - Brak retransmisji pakietów (ew. warstwy wyższe)

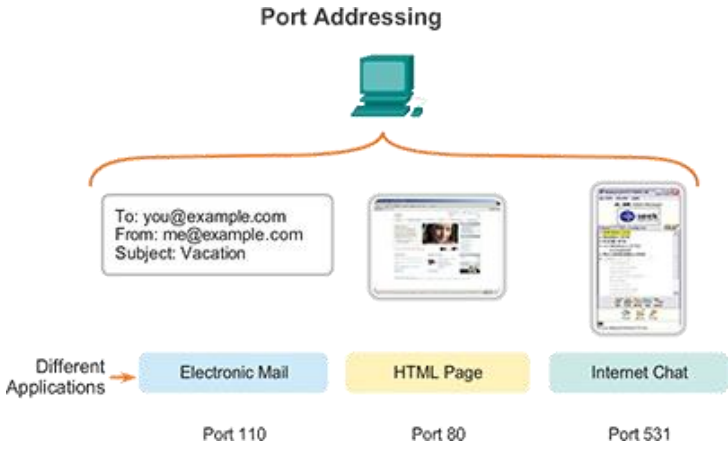
- **Stanowa (stateful)**
  - Sesja pomiędzy serwerem i klientem (monitorowana przez serwer)
- **Bezstanowa (stateless)**
  - Brak monitorowania stanu klienta przez serwer
  - Mniejsze obciążenie, brak informacji o poprzednich odpowiedziach

Gniazdo i port

- **Port**
  - Wartość 16 bitowa (2 bajty) – od 0 do 65 535
  - Identyfikuje procesy na hostach
  - Dwie wartości (źródłowy i docelowy)
  - Wartości liczbowe
    - 0 - 1023 – porty systemowe (dostępne tylko dla procesów uprzywilejowanych)
    - 1024 – 49 151 – porty użytkownika (registered)
    - 49 152 – 65 535 – porty prywatne i dynamicznie przydzielane



- **Gniazdo (ang. Socket)**
  - Abstrakcyjna reprezentacja dwukierunkowego zakończenia połączenia
  - Charakteryzowane przez
    - Typ/protokół (najczęściej TCP lub UDP)
    - Adres lokalny (najczęściej IP)
    - Numer portu identyfikujący proces
  - Przykład: TCP 149.156.96.52:80 (strona główna AGH)



Well-known ports

- **Porty zarezerwowane dla konkretnych usług**
- **Szczegóły (lista)**
  - %WINDIR%\system32\drivers\etc
  - /etc/services
  - /etc/protocols
- Lista otwartych portów
  - Netstat

```
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
```

- **Przydzielane przez IANA**

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

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.

Protokoły spoza stosu TCP/IP

- **DCCP (Datagram Congestion Control Protocol) RFC 4340**
  - Bezpośredni dostęp do mechanizmów kontroli przeciążeń
  - Dedykowany do zastosowań z czasowymi ograniczeniami transmisji danych (strumieniowanie, gry wieloosobowe, VoIP)
  - Transmisja zawodna, bez kontroli kolejności
- **SCTP (Stream Control Transmission Protocol) RFC 2960**
  - Transmisja niezawodna, z zagwarantowaną kolejnością i brakiem przeciążeń (jak w TCP)
  - Message-oriented (jak w UDP)
  - Dedykowany dla VoIP
  - Multihoming
    - Możliwość transmisji przy użyciu wielu łączy
    - zakończenia połączeń mogą zawierać wiele adresów IP

- **RSVP (Resource Reservation Protocol) RFC2205**
  - Konfiguracja zasobów w systemach IntegratedServices (QoS)
  - Działa w oparciu o IPv4 lub IPv6
  - Nie jest protokołem transmisji danych ani routingu

Protokół DCCP

DCCP (Datagram Congestion Control Protocol)

- protokół kontroli przeciążeń datagramów (RFC 4340,4336–2006 rok)
- Uniwersalny protokół transportowy przeznaczony do transmisji danych w trybie rzeczywistym
- Transmisja niezawodna
- Brak gwarancji kolejności dostarczenia datagramów

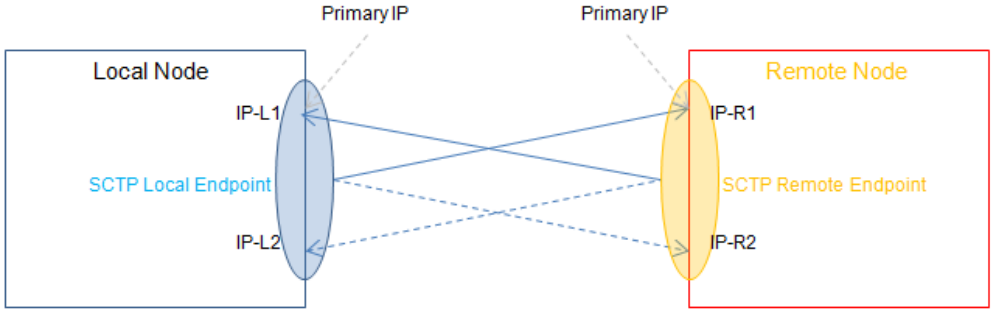
- Implementuje mechanizmy ECN (Explicit Congestion Notification)
  - Powiadamianie o zatorach bez gubienia pakietów
  - Realizowany przez urządzania wspierające (końcowe i pośredniczące)
  - Sygnalizowanie nadchodzącego przeciążenia przez routery
    - Dodanie znacznika do nagłówka IP
    - Przekazanie do odbiorcy, odesłane do nadawcy, który ogranicza transmisje
    - W odróżnieniu do TCP, który sygnalizuje przeciążenie przez odrzucanie pakietów
  - Liczba serwerów nieobsługujących mechanizmu ECN < 1% (2015r.)
  - Wsparcie pasywne – 70 % najpopularniejszych domen w 2017 r.

- stosowany przy z **czasowych ograniczeniach transmisji** (strumieniowanie, gry wieloosobowe, VoIP) – preferowane otrzymywane nowych danych nad dosyłanie starych

Protokó SCTP

SCTP (Stream Control Transmission Protocol)

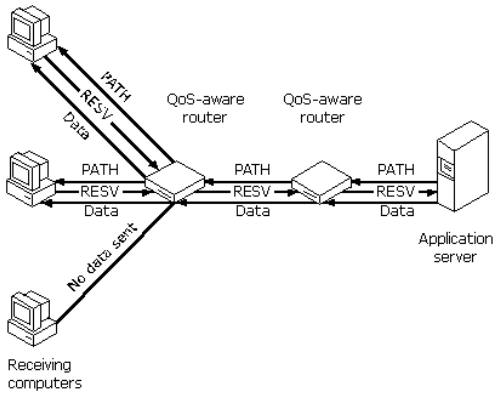
- zaprojektowany jako protokół transportowy w sieciach PSTN (Signaling System 7)
- alternatywa dla TCP i UDP, zdefiniowany w 2000 r. RFC 2960,
- podobieństwa do TCP
  - Transmisja niezawodna,
  - z zagwarantowaną kolejnością
  - brakiem przeciążeń (jak w TCP)
- Podobieństwa do UDP
  - Message-oriented (jak w UDP)
- Dedykowany dla VoIP
- Multihoming
  - Zakończenia połączeń mogą zawierać wiele adresów IP
  - Możliwość transmisji przy użyciu wielu łączy
- Przy braku natywnego wsparcia przez OS możliwość
  - tunelowania w ramach UDP
  - mapowania TCP API na SCTP API



Protokół RSVP

RSVP (Resource Reservation Protocol) RFC2205,2210

- Nie jest protokołem transmisji danych ani routingu
- Konfiguracja zasobów w systemach zintegrowanych usług IntegratedServices
  - Zasoby sieci zarezerwowane dla poszczególnych strumieni danych (w oparciu o protokół RSVP)
  - Implementacja protokołu wymagana na każdym routerze IP
    - Przyjmowanie żądań rezerwacji
    - Kojarzenie rezerwacji ze strumieniem danych
  - Usługi w architekturze IntServ
    - BestEffort – usługa standardowa
    - Guaranteed Service – gwarancja odnośnie parametrów związanych z opóźnieniami
    - Controlled-load Service – bezstratny przekaz danych, jakość lepsza niż Best Effort

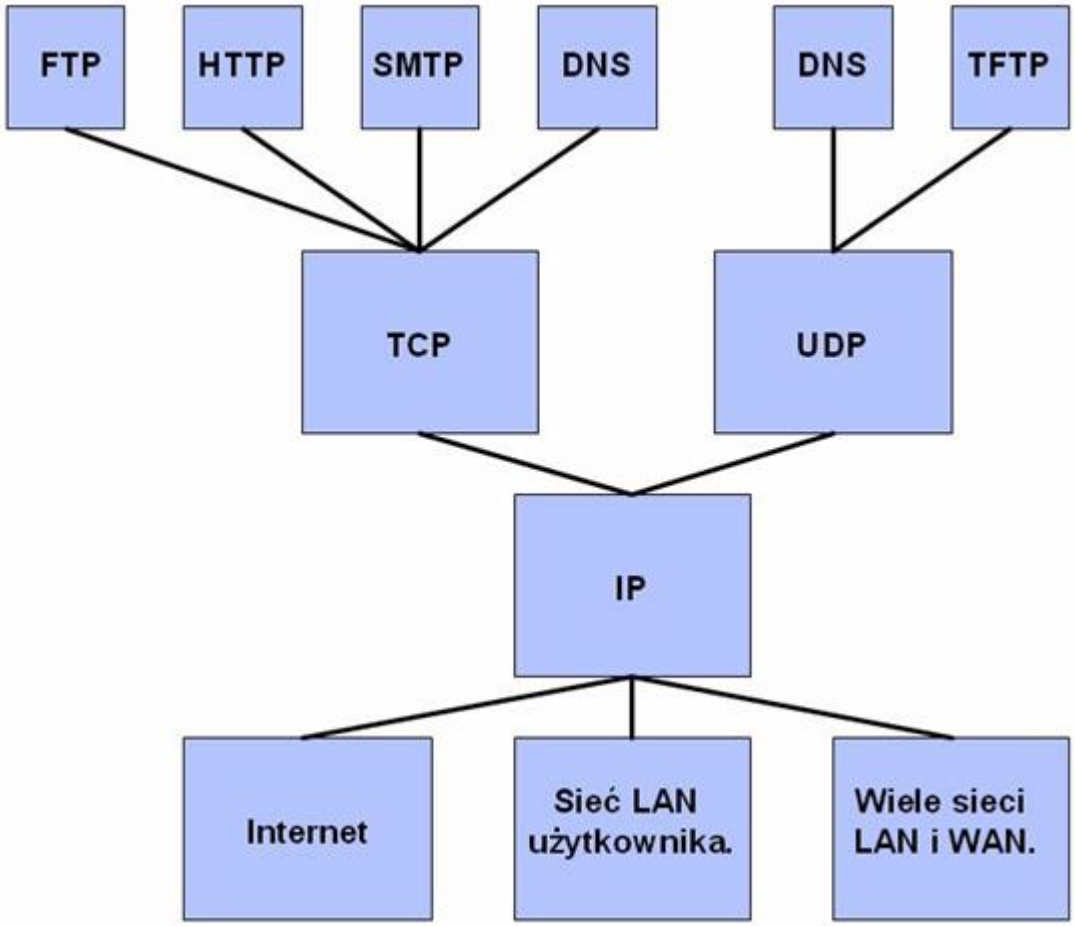


- umożliwia realizację żądania przez daną aplikację rezerwacji zasobów w sieci
  - niezależny od protokołów trasowania;
  - obsługuje transmisje unicast oraz multicast
  - umożliwia aplikacji inicjującej przesyłanie danych
    - zarezerwowanie przepustowości połączenia,
    - zarządzanie zarezerwowanymi na węzłach sieciowych zasobami ,
    - zwolnienie zasobów po zakończeniu transmisji;
  - wymaga okresowego odnawiania dokonanych na każdym węźle rezerwacji, co umożliwia dostosowanie do zmieniającego się ruchu w sieci;
  - oferuje dużą skalowalność.

Protokoły stosu TCP/IP

- **TCP**
- **UDP**

Główne zadanie:
Dzielenie danych z warstw wyższych na segmenty



Protokół UDP

- **User Datagram Protocol – protokół pakietów użytkownika**

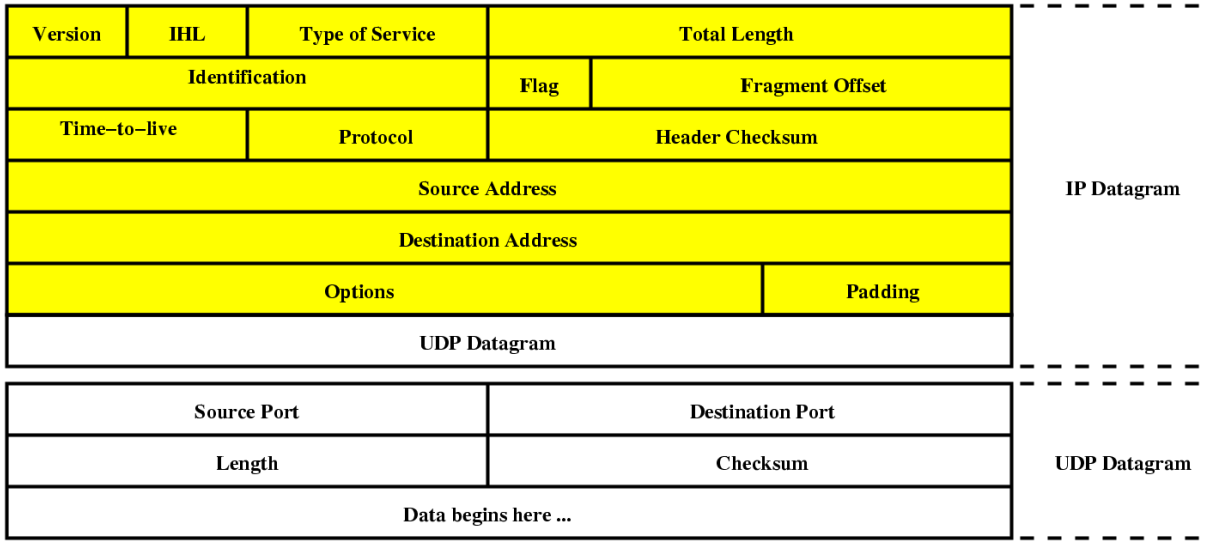
- **Bezpołączeniowy (jak IP)**
- **Brak potwierdzenia dotarcia segmentu do adresata**
- **Brak mechanizmów kontroli przepływu**

(obsłużone przez warstwy wyższe)

- **Korzyści:**
  - Większa szybkość (uproszczenie)
  - Brak dodatkowych zadań dla adresata
  - Obsługa trybu multicast

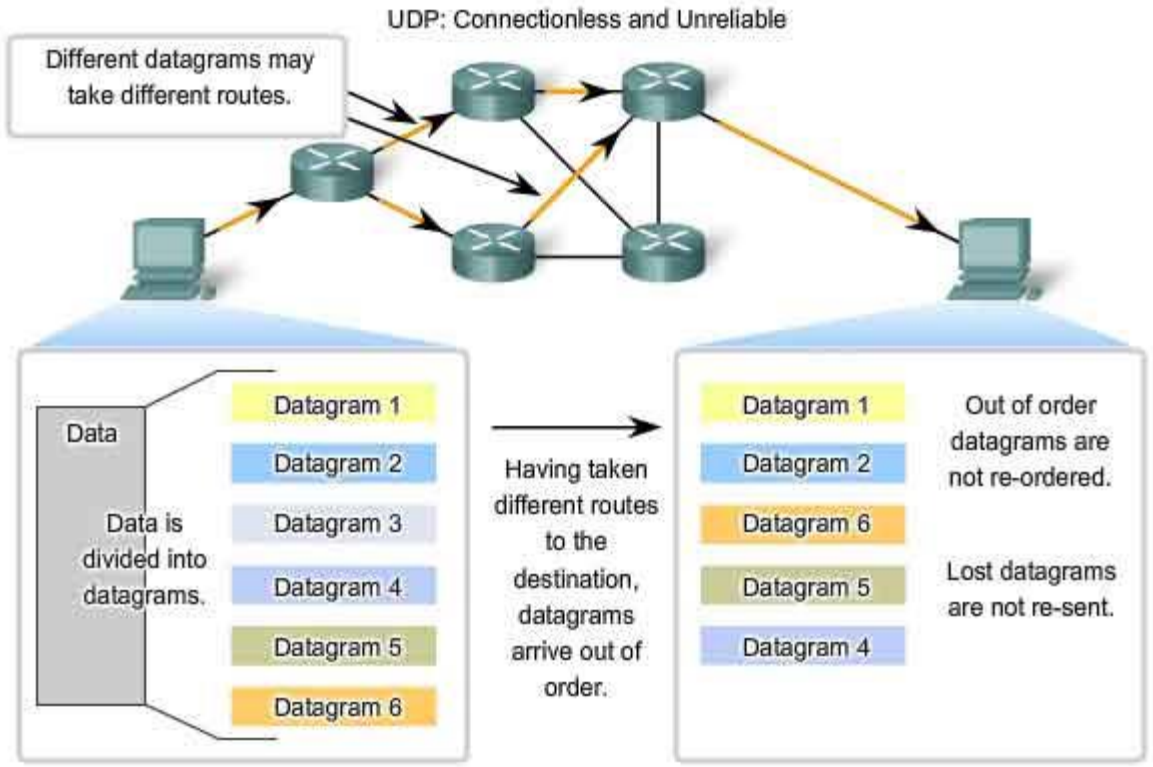
- **zastosowanie**
  - Aplikacje komunikacji multimedialnej
  - Wideokonferencje / komunikatory
  - Strumieniowe przesyłanie dźwięku i obrazu
  - Gry sieciowe
  - DNS – rozwiązywanie nazw symbolicznych
  - TFTP – transfer plików

Datagram UDP



- **Efektywność UDP**
  - Krótki nagłówek
  - Brak kontroli przepływu
- **UDP w IPv4**
- **Pola nagłówka UDP**
  - Port nadawcy
  - Port odbiorcy
  - Długość całego datagramu UDP (nagłówek + dane)
    - Minimum 8 bajtów – sam nagłówek
    - Maksimum – 65537 bajtów
  - Suma kontrolna (nie wykorzystywana w LAN)

UDP – transmisja danych

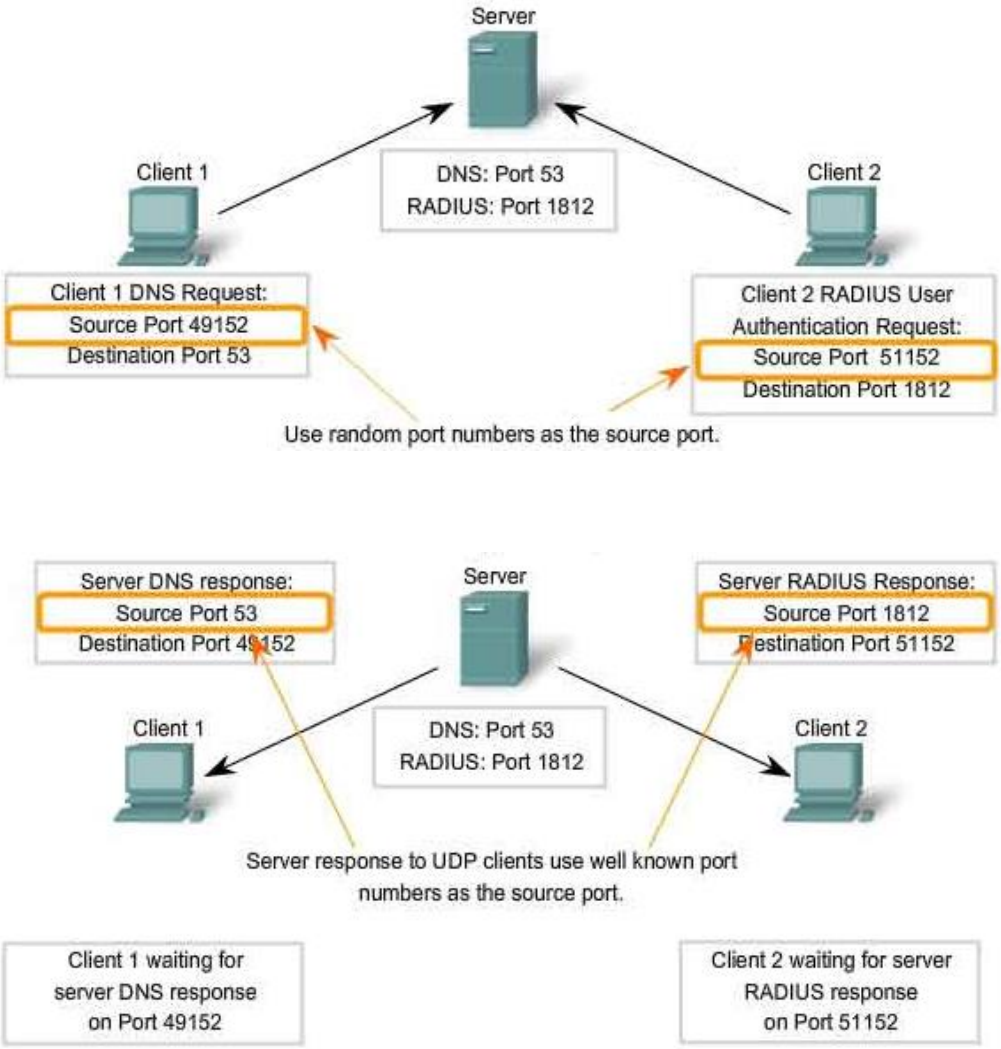


- **Różne trasy transmisji**
- **Różna kolejność dostarczania datagramów**
- **Brak retransmisji pakietów**

- **Jeśli wymagane – obsługiwane w wyższych warstwach**

UDP – komunikacja klient - serwer

- **Identyfikacja punktów końcowych w oparciu o gniazdo (socket)**
- **Zapytanie od klienta do serwera**
  - **W oparciu o „well known ports”**
  - **Klient – porty dynamiczne** (49 152 – 65 535)
- **Odsyłanie odpowiedzi do klienta**
  - **Port źródłowy – WKP**
  - **Port docelowy – port dynamiczny klienta**
- **Losowe wybieranie portów**
  - **Zwiększenie bezpieczeństwa**

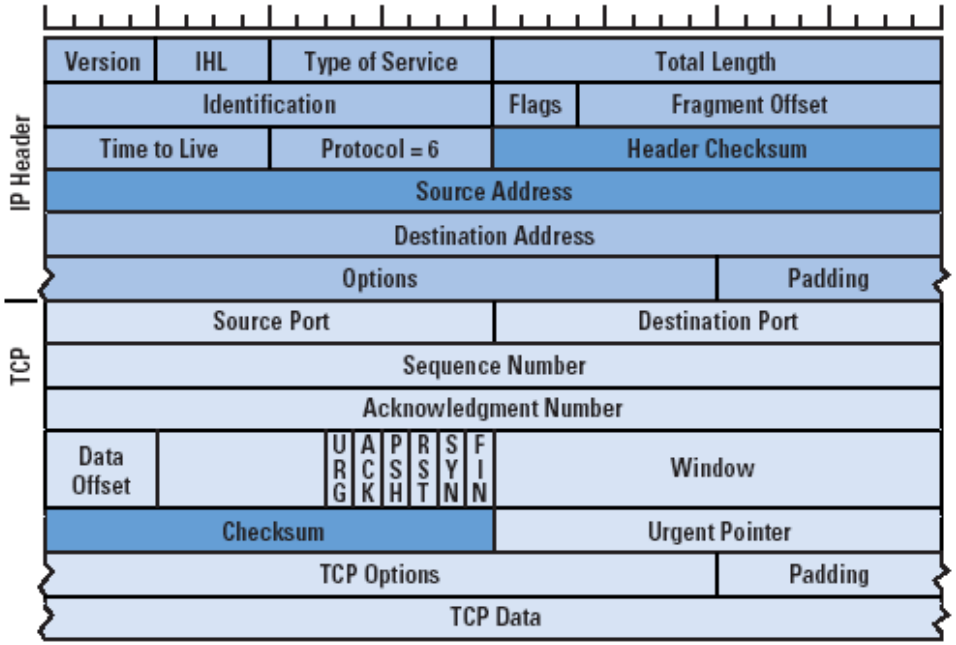


Protokół TCP

- **Transmission Control Protocol – RFC 793**
- **Transmisja:**
  - Wiarygodna – gwarancja dostarczenia wszystkich danych (bez duplikatów)
  - Z zachowaniem kolejności
  - Strumieniowa
  - Z kontrolą przeciążeń
  - Możliwość sterowania przepływem
- **Datagramy TCP enkapsulowane w IP**
  - Docierają w różnej kolejności
  - Mechanizm porządkowania (złożenie danych)
- **Możliwość sterowania przepływem**
  - Przesłanie kilku segmentów w jednym pakiecie
  - Podział jednego datagramu na kilka pakietów
- **Trasmisja w trybie klient serwer**
  - Serwer oczekuje na połączenie na określonym porcie
  - Klient inicjuje połączenie do serwera
- **Większy rozmiar nagłówka (obciążenie sieci)**

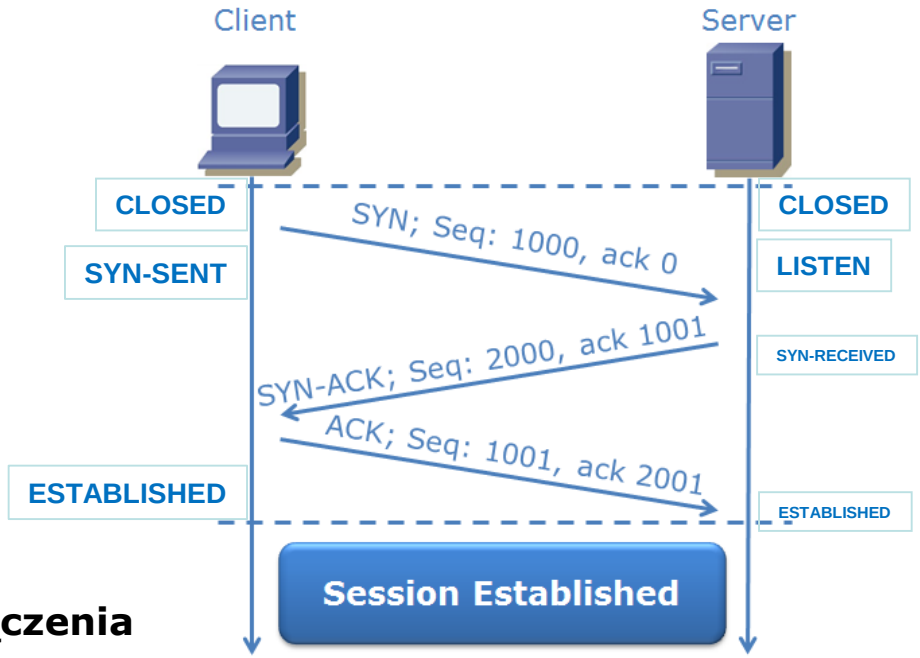
TCP – budowa datagramu

- Port nadawcy (2 bajty)
- Port odbiorcy (2 bajty)
- Numer sekwencyjny – miejsce pakietu przed segmentacją (4 bajty)
- Numer potwierdzenia – synchronizacja odebrania pakietu z odbiorcą (4 bajty)
- Długość nagłówka (1 bajt) (krotność 4bajtów)
- Zarezerwowane na przyszłość (3 bity)
- Flagi: (9 bitów)
  URG – istotność pola priorytet
  ACK – istotność pola numer potwierdzenia
  PSH – wymuszenie przesłania pakietu
  RST – resetowanie połączenia
  SYN – synchronizacja kolejnych sekwencji
  FIN – zakończenie przesyłu danych
  (+ flagi NS,CRW,ECE – odebranie powiadomienia przez nadawcę, potwierdzenie przez odbiorcę, suma kontr.)
- Szerokość okna (2 bajty)
- Suma kontrolna – obliczana z całego pakietu (2 bajty)
- Wskaźnik priorytetu – jeśli włączona flaga URG (2 bajty)
- Opcje – (3 bajty)
  0 – koniec listy opcji
  1 – brak działania
  2 – ustawienie maksymalnej długości segmentu
- Uzupełnienie do wielokrotności 4bajtów (32 bitów)



TCP – nawiązywanie połączenia

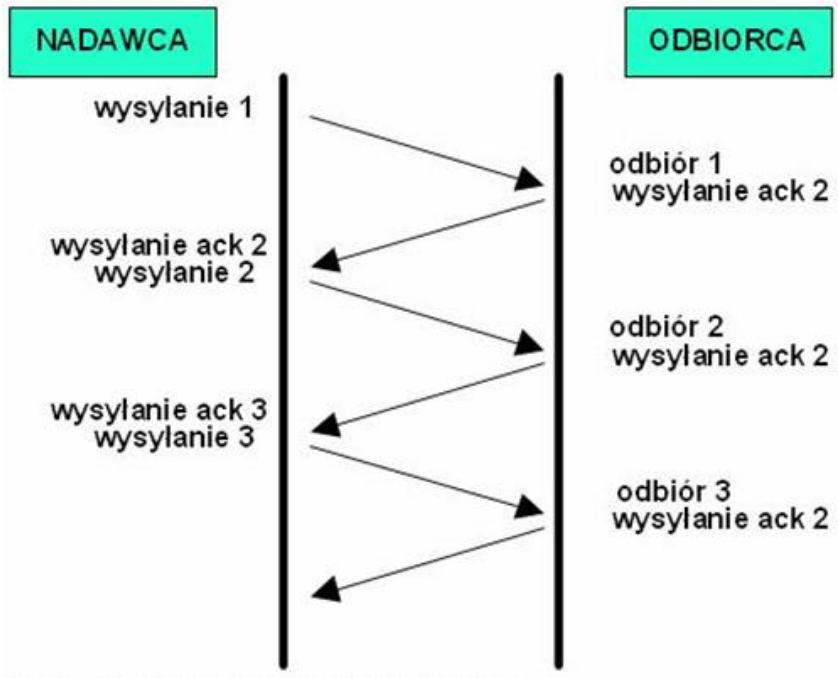
- **Procedura Three-way-handshake**
  - A->B, SYN, dolna wartość numerów sekwencyjnych (A przechodzi w stan SYN-SENT)
  - B przechodzi w stan SYN-RECEIVED
  - B->A, SYN, dolna wartość swoich numerów sekwencyjnych + ACK z polem numeru sekwencji A+1
  - A przechodzi w stan ESTABLISHED odsyła ACK z numerem sekwencji B+1
  - B odbiera ACK i przechodzi w stan ESTABLISHED
  - A może rozpocząć przesyłanie danych



- **Jeśli B nie chce (nie może) odebrać połączenia odsyła odpowiedź z flagą RST (reset)**

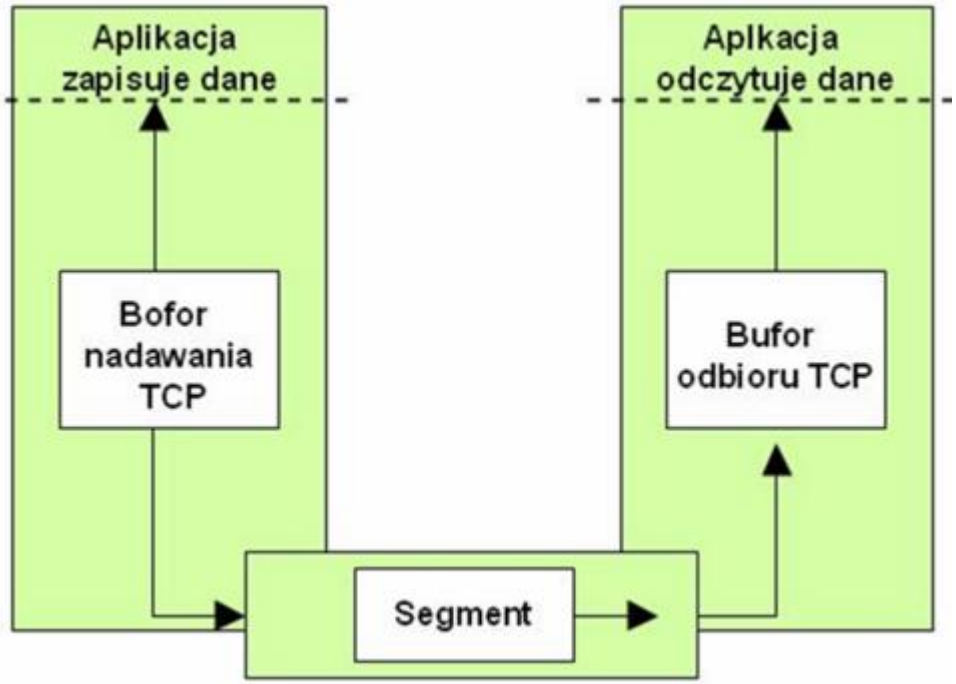
TCP – transmisja danych

- **ACK – numer kolejnej sekwencji**
- **Teoretycznie – połączenie symetryczne (full-duplex)**
- **Praktycznie**
  - W jedną stronę – dane
  - W drugą stronę – potwierdzenia
- **Mała efektywność**
  - Potwierdzenie po 1 segmencie
  - Potwierdzenie po każdym segmencie
- **Zwiększenie wydajności**
  - Buforowanie
  - Mechanizm przesuwnego okna



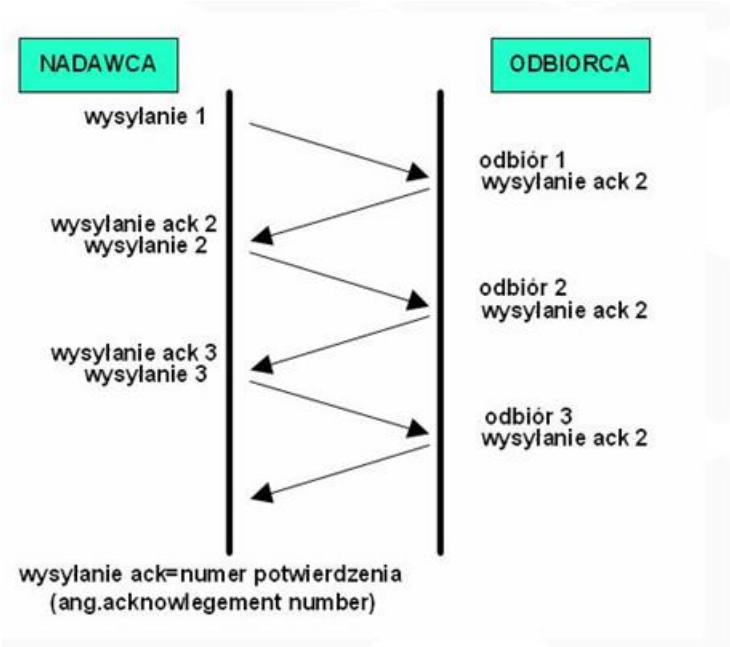
TCP – buforowanie segmentów

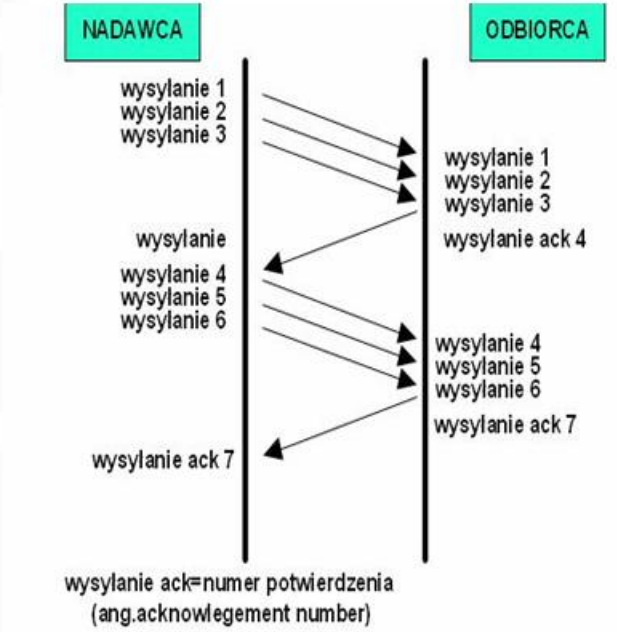
- **Bufory – przechowują segmenty TCP po stronie klienta i serwera**
- **Wielkości buforów ustawiane w trakcie nawiązywania połączenia**



TCP – mechanizm przesuwnego okna

- **Mechanizm przesuwnego okna (ang. sliding window)**
- **Nieefektywne przesyłanie/potwierdzanie pojedynczych segmentów**
- **Wykorzystanie bufora**



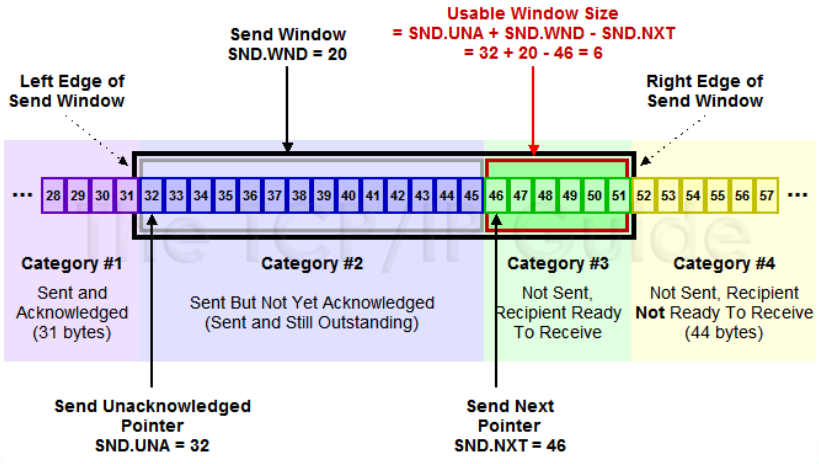


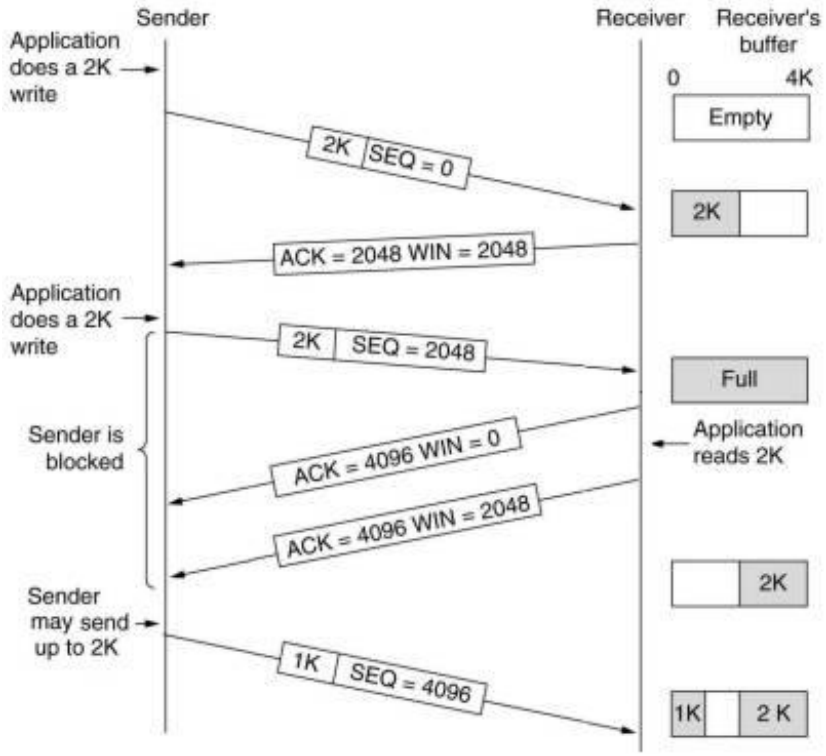
TCP – mechanizm przesuwnego okna

- **Przesuw okna**
  - **Wysyłanie segmentów w liczbie odpowiadającej rozmiarowi okna (bez konieczności potwierdzenia)**
  - **Przesuw okna po otrzymaniu potwierdzenia konkretnego segmentu**
  - **Retransmisja – osobny zegar dla każdego segmentu**
- **Zmiana rozmiaru okna**
  - **Odbiorca nie może obsłużyć nadchodzących danych**
  - **Żądanie zmniejszenia rozmiaru okna**

TCP – mechanizm przesuwnego okna - przykład

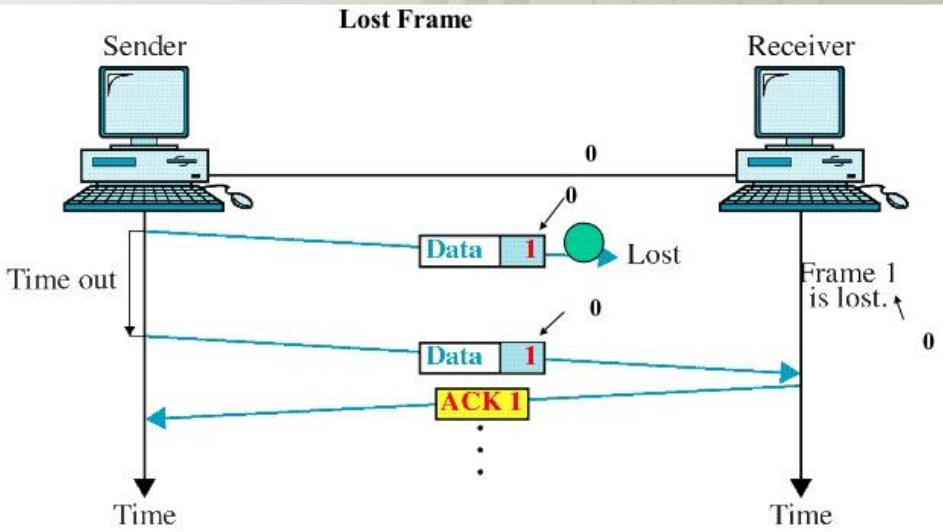
- **Ustalenie rozmiaru okna**
  (na przykładzie po prawej – max 4k)
- **Wysłanie danych:**
  - W blokach
  - Po potwierdzeniu odebrania poprzedniego segmentu
- **Mechanizm kontroli przepływu**
  - Zmienny rozmiaru okna
  - możliwość zablokowana nadawcy

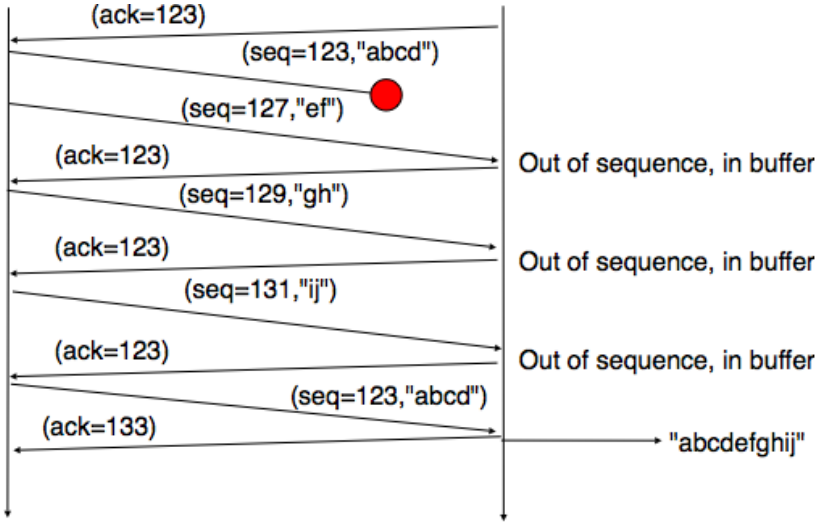


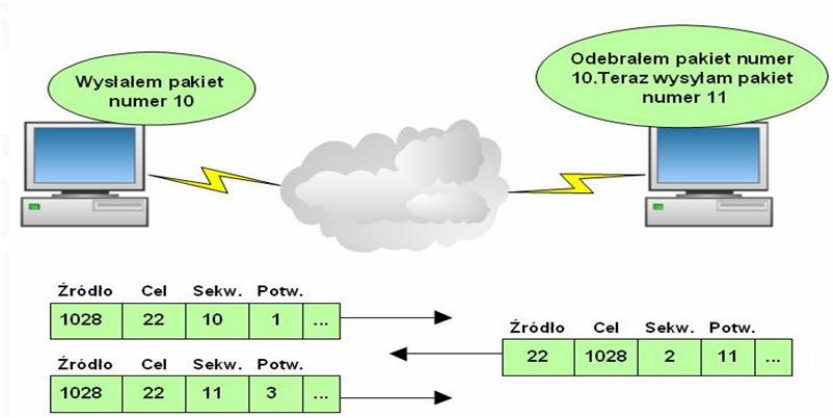


TCP – retransmisja pakietów

- **Utracone datagramy**
  - Timeout
  - Przesyłane powtórnie
- **Buforowanie danych u klienta**
  - Przesłanie całości do w.wyższej
  - Szeregowanie (w oparciu o **numer sekwencji**)





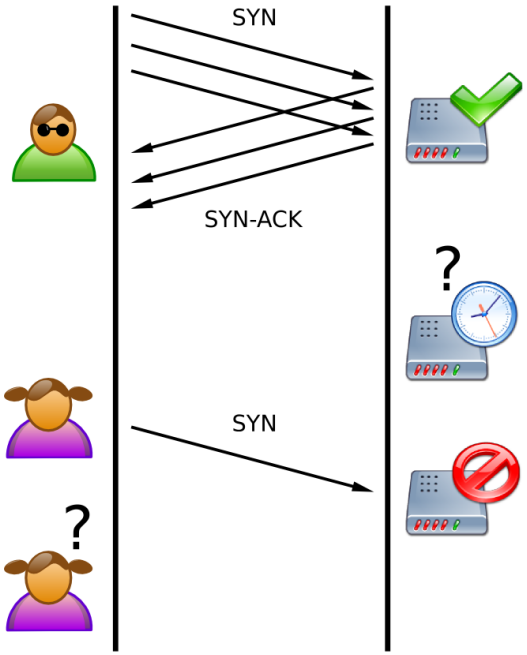


TCP – mechanizmy sterowania przepływem

- **Problemy:**
  - **Duża liczba klientów/połączeń**
    - Brak możliwości obsłużenia transmisji
  - **Przeciążenie sieci**
    - Pakiety nie docierają na czas
    - Duża liczbie retransmisji segmentów
- **Rozwiązania:**
  - Zmniejszanie okna (o połowę)
  - Zwiększenie czasu oczekiwania przed retransmisją
- **Algorytm powolnego startu**
  - Po ustąpieniu przeciążenia
  - Zwiększanie rozmiaru okna o jeden segment

Ataki DoS

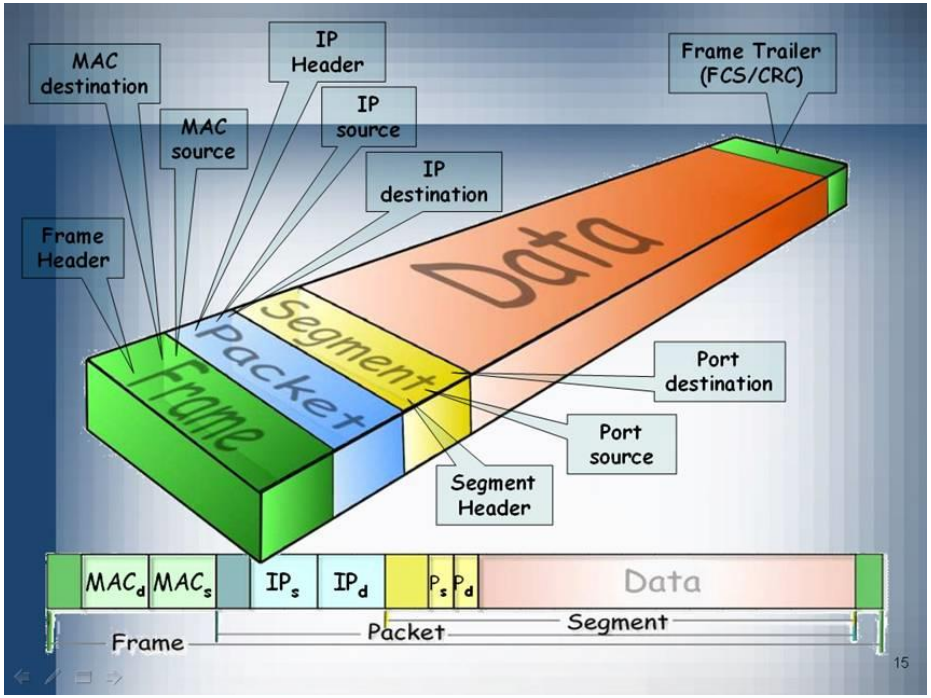
- **DoS (Denial of Service) – odmowa obsługi/dostępu**
- **SYN Flood**
  - popularny typ ataków DoS z wykorzystaniem mechanizmu Three way handshake
  - Wykorzystanie zainfekowanych komputerów zombie – wysyłających zapytania
- **Procedura :**
  - Aktywowanie hostów zombie (wysyłanie wielu zapytań SYN)
  - Ofiara odpowiada SYN-ACK, alokując zasoby
  - Nie dochodzi do połączenia (ofiara wyczekuje na ACK od zombie)
  - Wiele fałszywych połączeń blokuje ofiarę
- **Ofiara nie odpowiada na próby nawiązania połączenia (SYN) prawdziwych użytkowników**



TCP vs UDP

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

Komunikacja TCP/IP – enkapsulacja danych



TCP segment in IPv4 packet in Ethernet frame

Ethernet	Octets				
Preamble	7				
Start of frame delimiter	1				
MAC destination	6				
MAC source	6				
802.1Q tag (opt.)	4				
Ethertype or length	2	IPv4	Bits		
Payload	46 -1500	Version	4		
		Header Length	4		
		Differentiated Services Code Point	6		
		Explicit Congestion Notification	2		
		Total Length	16		
		Identification	16		
		Flags	3		
		Fragment Offset	13		
		Time to Live	8		
		Protocol	8		
		Header Checksum	16		
		Source IP Address	32		
		Destination IP Address	32		
		Options (if Header Length > 5)	?		
		Payload	1440-1480 Bytes	TCP	Bits
				Source Port	16
				Destination Port	16
				Sequence number	32
				Acknowledgment number	32
				Data offset	4
				Reserved	4
				Flag	8
				Window Size	16
				Checksum	16
				Urgent pointer	16
				Options (if Data Offset > 5)	varies
				padding	8
				Payload	Payload
CRC	4				
Interframe gap	12				

Komunikacja TCP/IP

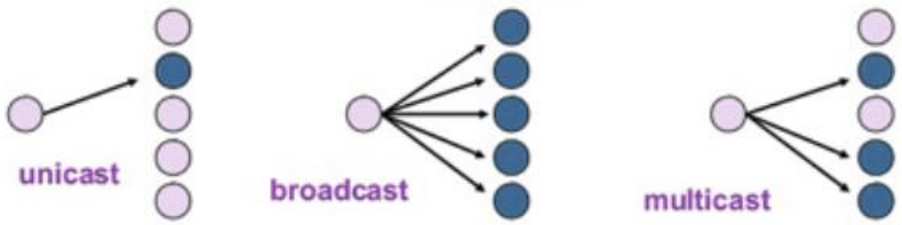
Phase	OSI Layer	CEO Letter	Web Site Connection (Simplified)
Transmission	7	The CEO of a company in Phoenix decides he needs to send a letter to a peer of his in Albany. He dictates the letter to his administrative assistant.	You decide you want to connect to the web server at IP address 10.0.12.34, which is within your organization but not on your local network. You type the address into your browser.
	6	The administrative assistant transcribes the dictation into writing.	(Generally, with a web site connection, nothing happens at this layer, but format translation may be done in some cases.)
	5	The administrative assistant puts the letter in an envelope and gives it to the mail room. The assistant doesn't actually know how the letter will be sent, but he knows it is urgent so he says, "get this to its destination quickly".	The request is sent via a call to an application program interface (API), to issue the command necessary to contact the server at that address.
	4	The mail room must decide how to get the letter where it needs to go. Since it is a rush, the people in the mail room decide they must use a courier. The envelope is given to the courier company to send.	The Transmission Control Protocol (TCP) is used to create a segment to be sent to IP address 10.0.12.34.
Routing	3	The courier company receives the envelope, but it needs to add its own handling information, so it places the smaller envelope in a courier envelope (encapsulation). The courier then consults its airplane route information and determines that to get this envelope to Albany, it must be flown through its hub in Chicago. It hands this envelope to the workers who load packages on airplanes.	Your computer creates an IP datagram encapsulating the TCP datagram created above. It then addresses the packet to 10.0.12.34. but discovers that it is not on its local network. So instead, it realizes it needs to send the message to its designated routing device at IP address 10.0.43.21. It hands the packet to the driver for your Ethernet card (the software that interfaces to the Ethernet hardware).
	2	The workers take the courier envelope and put on it a tag with the code for Chicago. They then put it in a handling box and then load it on the plane to Chicago.	The Ethernet card driver forms a frame containing the IP datagram and prepares it to be sent over the network. It packages the message and puts the address 10.0.43.21 (for the router) in the frame.
	1	The plane flies to Chicago.	The frame is sent over the twisted pair cable that connects your local area network. (I'm ignoring overhead, collisions, etc. here, but then I also ignored the possibility of collisions with the plane. ☺)
	2	In Chicago, the box is unloaded, and the courier envelope is removed from it and given to the people who handle routing in Chicago.	The Ethernet card at the machine with IP address 10.0.43.21 receives the frame, strips off the frame headers and hands it up to the network layer.
	3	The tag marked "Chicago" is removed from the outside of the courier envelope. The envelope is then given back to the airplane workers to be sent to Albany.	The IP datagram is processed by the router, which realizes the destination (10.0.12.34) can be reached directly. It passes the datagram back down to the Ethernet driver.
	2	The envelope is given a new tag with the code for Albany, placed in another box and loaded on the plane to Albany.	The Ethernet driver creates a new frame and prepares to send it to the device that uses IP address 10.0.12.34.
	1	The plane flies to Albany.	The frame is sent over the network.
	2	The box is unloaded and the courier envelope is removed from the box. It is given to the Albany routing office.	The Ethernet card at the device with IP address 10.0.12.34 receives the frame, strips off the headers and passes it up the stack.
Reception	3	The courier company in Albany sees that the destination is in Albany, and delivers the envelope to the destination CEO's company.	The IP headers are removed from the datagram and the TCP segment handed up to TCP.
	4	The mail room removes the inner envelope from the courier envelope and delivers it to the destination CEO's assistant.	TCP removes its headers and hands the data up to the drivers on the destination machine.
	5	The assistant takes the letter out of the envelope.	The request is sent to the Web server software for processing.
	6	The assistant reads the letter and decides whether to give the letter to the CEO, transcribe it to email, call the CEO on her cell phone, or whatever.	(Again, in this example nothing probably happens at the Presentation layer.)
	7	The second CEO receives the message that was sent by the first one.	The Web server receives and processes the request.

http://www.tcpipguide.com/free/t_UnderstandingTheOSIReferenceModelAnAnalogy.htm (EN)
http://www.youtube.com/watch?v=nomyRJehhnM – routing pakietów z hosta źródłowego do docelowego (EN) (12 minut)

video?

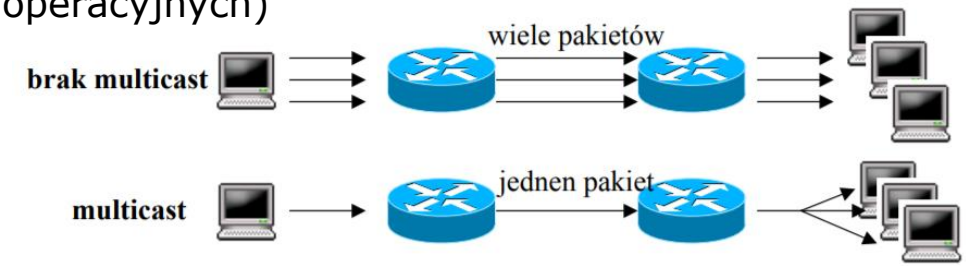
Strumienowanie

- **Transmisja danych od serwera do klienta(ów) w sposób ciągły**
- **Rodzaje dostępu do mediów strumieniowych**
  - Na żywo (live streaming) – np. transmisja koncertu (fale radiowe, telewizyjne, online) – dostępne tylko w konkretnym momencie
  - Na życzenie (on demand) – odtwarzania na żądania klienta (np. internetowa wypożyczalnia filmów) – dostępne przez dłuższy czas
- **Rodzaje transmisji multimedialnych**
  - Unicast – jeden do jednego
  - Multicast – jeden do wielu
  - Broadcast – jeden do wszystkich (kablowe sieci telewizyjne)
- **Transmisja multimediów w sieci**
  - Zapotrzebowanie na wysokie przepustowości
  - Zaawansowane metody kompresji video
    - H.264 (MPEG-4 AVC) – następca MPEG-1,2, Mpeg-4 part2 – DivX,Xvid)
    - HEVC (H.265) – następca H.264
    - VP9 – rozwijany przez Google
  - Kompresja audio (MP3, Vorbis, AAC)



Strumienowanie - multicast

- **Multicast**
  - Transmisja z jednego hosta do grupy odbiorców (od 1 do n hostów)
  - Wszyscy odbiorcy widziani jako jeden odbiorca grupowy (grupa multicastowa) (poszczególni odbiorcy mają różne adresy unicastowe (z różnych klas adresowych))
  - W łączu sieciowym transmisja realizowana raz – dla grupy multicastowej
  - Stosowany do strumieniowania multimediów, videokonferencji, aktualizacji grup komputerów (systemów operacyjnych)



- **Realizacja**
  - Wykorzystanie adresowej klasy D: od 224.0.0.0 do 239.255.255.255 (RFC 3171)
  - Kopiowanie przez routery do wszystkich hostów z grupy multicastowej
  - W routerach zamiast bramy (unicast) jest lista interfejsów (outgoing interfaces)
  - Oparty w większości przypadków na protokole UDP
  - Obsługa przez protokoły
    - W sieciach lokalnych: IGMP (IPv4), MLD (IPv6)
    - W ramach systemu autonomicznego (domeny trasowania): PIM, MOSPF
    - Pomiędzy systemami autonomicznymi: MBGP

Multicast – bloki adresowe

- **Zakresy adresów (224.0.0.0 do 239.255.255.255)**
  - 224.0.0.0 – 224.0.0.255 – multicast lokalny, nie przesyłane przez routery, TTL=1
  - 239.0.0.0 – 239.255.255.255 – prywatne adresy grupowe (RFC 2365)
  - 224.0.1.0 – 238.255.255.255 – używane w skali globalnej
    - 224.0.1.0 – 224.0.1.255 - Internetwork Control Block
      - 224.0.1.1 - NTP - Network Time Protocol
      - 224.0.1.6 - NSS - Name Service Server
      - 224.0.1.9 - MTP Multicast Transport Protocol
      - 224.0.1.75 - SIP
    - 233.0.0.0/8 – adresy GLOP (RFC 2770)
      - dedykowane dla konkretnych systemów autonomicznych
      - Adres AS zaszyty w drugim i trzecim bajcie adresu
      - Przykład: AS nr 62010 => F23A hex => adres 233.242.58.0
- „Well known” (dedykowane) adresy multicast
  - 224.0.0.1 – wszystkie hosty w sieci LAN posiadające funkcjonalność IP multicast
  - 224.0.0.2 – wszystkie rutery ruchu IP multicast w sieci LAN
  - 224.0.0.5 – wszystkie routery protokołu OSPF
  - 224.0.0.9 – wszystkie rutery protokołu RIPv2 w sieci LAN
  - 224.0.0.13 – wszystkie rutery protokołu PIM w sieci LAN
  - 224.0.0.22 – wszystkie rutery protokołu IGMP w sieci LAN

Strumienowanie - RTP

- **UDP** – protokół bazowy dla strumieniowania (w warstwie transportowej)
- **RTP** - Real-time Transport Protocol
  - protokół transmisji w czasie rzeczywistym.
  - zawiera informację o:
    - PT (payload type) - typie przesyłanych danych (H.264, MPEG-4, HEVC, …) – RFC 3551
    - Sequence Number - numerze sekwencyjnym (zagubienie pakietów, ustalenie kolejności)
    - Timestamp - znaczniku czasu strumienia multimedialnego
  - nie gwarantuje jakości usługi (QoS) – wykorzystuje do tego inne protokoły (RTSP, SIP, H.323, RSVP)
    - RTP - obsługuje transmisje strumienie mediów (audio i video)
    - RTCP – monitoruje transmisje, zapewnia synchronizacje i QoS
  - Gwarantuje
    - Jitter compensation – buforowanie pakietów odbieranych ze zmiennym opóźnieniem
    - Wykrycie zagubionych pakietów
    - Synchronizacje kolejności

RTP packet header

Offsets	Octet	0								1								2								3							
Octet	Bit [a]	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version			P	X	CC			M	PT							Sequence number															
4	32	Timestamp																															
8	64	SSRC identifier																															
12	96	CSRC identifiers ...																															
12+4×CC	96+32×CC	Profile-specific extension header ID																Extension header length															
16+4×CC	128+32×CC	Extension header ...																															

Strumienowanie - RTSP

- **RTSP –** Real-Time Streaming Protocol
  - Protokół z warstwy aplikacji (modelu TCP/IP)
  - Zadania:
    - Kontrola serwerów strumieniowania mediów
    - tworzy i steruje strumieniami ciągłych danych (audio i wideo)
    - Zapewnia dostarczanie danych w czasie rzeczywistym
  - Cechy
    - Protokół stanowy
    - Wykorzystuje identyfikator do monitorowania równoległych sesji
    - Wykorzystuje TCP (częściej) lub UDP (rzadziej)
  - Komunikaty:
    - OPTIONS – typy komunikatów zwracanych przez serwer
    - DESCRIBE – opis strumieni dla źródła
    - SETUP – zestawienie strumienia mediów
    - PLAY – odtworzenie strumienia
    - PAUSE – wstrzymanie odtwarzania
    - RECORD – nagrywanie strumienia
    - ANNOUNCE – aktualizacja opisu
    - TEARDOWN – zakończenie sesji
    - REDIRECT – przekierowanie

```
C->S: SETUP rtsp://example.com/media.mp4/streamid=0 RTSP/1.0
      CSeq: 3
      Transport: RTP/AVP;unicast;client_port=8000-8001

S->C: RTSP/1.0 200 OK
      CSeq: 3
      Transport: RTP/AVP;unicast;client_port=8000-8001;server_port=9000-9001;
      Session: 12345678
```

```
C->S: PLAY rtsp://example.com/media.mp4 RTSP/1.0
      CSeq: 4
      Range: npt=5-20
      Session: 12345678

S->C: RTSP/1.0 200 OK
      CSeq: 4
      Session: 12345678
      RTP-Info: url=rtsp://example.com/media.mp4/streamid=0;seq=9810092;rtptime=3450012
```

Strumienowanie - RTCP

- **RTCP** - RTP Control Protocol
  - Protokół sterujący, wspierający RTP (RFC 3550)
  - **Nie transportuje danych**
  - Zadania:
    - Dostarcza zwrotnej informacji odnośnie poprawności odebranych danych (QoS) poprzez przesyłanie statystyk
      - Liczba przesłany pakietów
      - Liczba zgubionych pakietów
      - Zmienność opóźnienia
      - Round-trip delay time – czas transmisji w dwie strony
    - Wykorzystane do ewentualnej zmiany parametrów kodowania przez źródło.
    - Przenosi stały identyfikator transportowy źródła protokołu RTP (SSRC),
  - Standardowo wysyłany przez protokół UDP na numer portu transmisji RTP+1
  - Około 5% nakładu w stosunku do RTP (raporty nie częściej niż co 5 sekund)
  - PR (packet type) – *sender report, receiver report, source description, goodbye*

RTCP packet header

Offsets	Octet	0								1								2								3							
Octet	Bit [a]	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	Version		P	RC					PT								length															
	32	SSRC																															

Literatura, bibliografia

C. Hunt „TCP/IP network administration”; Second Edition, ISBN 1-56592-322-7

W.Graniszewski, E.Grochocki, G.Świątek, „Protokoły warstwy transportowej stosu protokołów TCP/IP” E-Studia Informatyczne, http://ważniak.mimow.edu.pl

B.Komar „Administracja sieci TCP/IP dla każdego” ISBN 83-7197-189-3, 2000

R.Scrimger, P.LaSalle, C.Leitzke, M.Parihar, M.Gupta,”TCP/IP. Biblia”, wyd.Helion 2002

D.Comer, „Sieci komputerowe i intersieci” wyd.Helion 2012

Ch.Kozierok, „The TCP/IP Guide” http://www.tcpipguide.com/free/t_UnderstandingTheOSIReferenceModelAnAnalogy.htm

E.Kohler, M.Handley, S.Floyd „Designing DCCP: Congestion Control Without Reliability”

J.M. de Goyeneche „Multicast over TCP/IP HOWTO”

Real Time Streaming Protocol (RTSP), Request for Comments: 2326, https://tools.ietf.org/html/rfc2326