KOMUNIKAČNÉ A INFORMAČNÉ SIETE

TRANSPORTNÁ VRSTVA
RELAČNÁ VRSTVA
PREZENTAČNÁ VRSTVA

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas

OBSAH

- Transportná vrstva
  - UDP - User datagram protocol
  - TCP – Transmission control protocol
- Relačná vrstva
  - RTP – Real-time transport protocol
  - RTCP, TLS
- Prezentačná vrstva
  - ASCII, ASN.1

Transportná vrstva

- 4. vrstva OSI modelu – Transport layer,
- komunikácia medzi aplikáciami koncových bodov,
- detekcia a/alebo oprava chýb,
- prenáša segmenty TCP alebo datagramy UDP,
- vytvára end-to-end spojenie,
- najčastejšie využíva 2 protokoly:
  - User Datagram Protocol – UDP
    - nespoľahlivá, nespojovo-orientovaná transportná služba
  - Transmission Control Protocol – TCP
    - spoľahlivá, spojovo-orientovaná transportná služba
- okrem toho protokoly RSVP, DCCP, SCTP

Transportná vrstva

- Port:
  - číselné označenie SAP medzi transportnou a vyššími vrstvami,
  - identifikácia aplikačného protokolu,
  - rozdielne pre TCP a UDP,
  - slúži na adresáciu a rozlíšenie konkrétneho komunikačného aplikačného procesu.

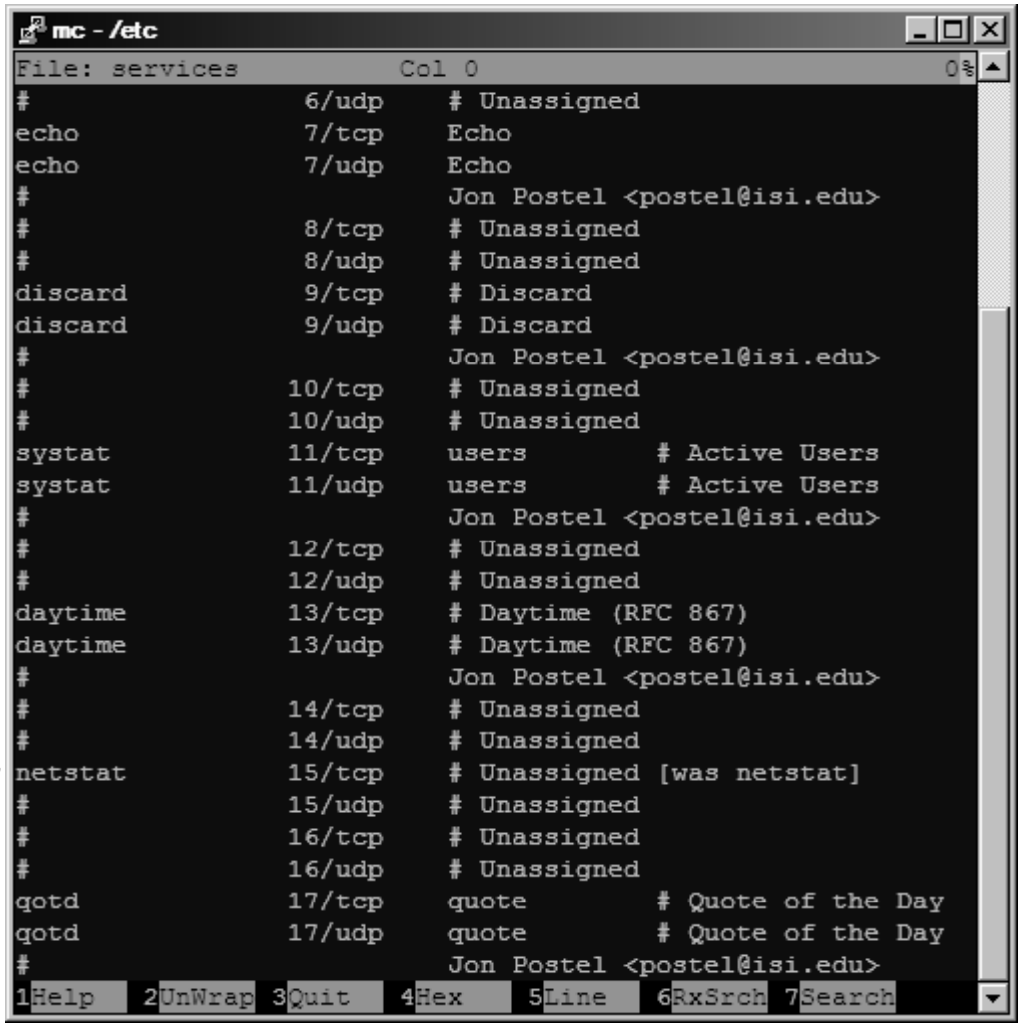
Transportná vrstva

- Port:
  - známe porty (0 – 1023)
    - pevne definované porty pre aplikačné protokoly RFC1700, prideľuje IANA (Internet Assigned Number Authority),
  - registrované porty (1024 – 49151)
    - využívané pre bežné užívateľské aplikácie, registruje IANA,
  - dynamické/súkromné porty (49152 – 65535)
    - ľubovoľne užívateľsky konfigurované porty, súkromné nikde neregistrované, často si ich náhodne volia klientské procesy.

Transportná vrstva

Čísla portov :

- 7 – **ICMP** echo,
- 20-21 – **FTP** (File transfer protocol),
- 22 – **SSH** (Secure Shell),
- 23 – **Telnet,**
- 25 – **SMTP** (Simple mail transfer protocol),
- 53 – **DNS** (Domain name system),
- 67-68 – **DHCP** (Dynamic Host Configuration Protocol),
- 80 – **HTTP** (Hypertext transfer protocol),
- 110 – **POP3** (Post office protocol),
- 179 – **BGP** (Border gateway protocol),
- 443 – **HTTPS** (HTTP over TLS/SSL),
- 465 – **SMTPS** (SMTP over SSL),
- 995 – **POP3S** (POP3 over TLS/SSL).



Transportná vrstva

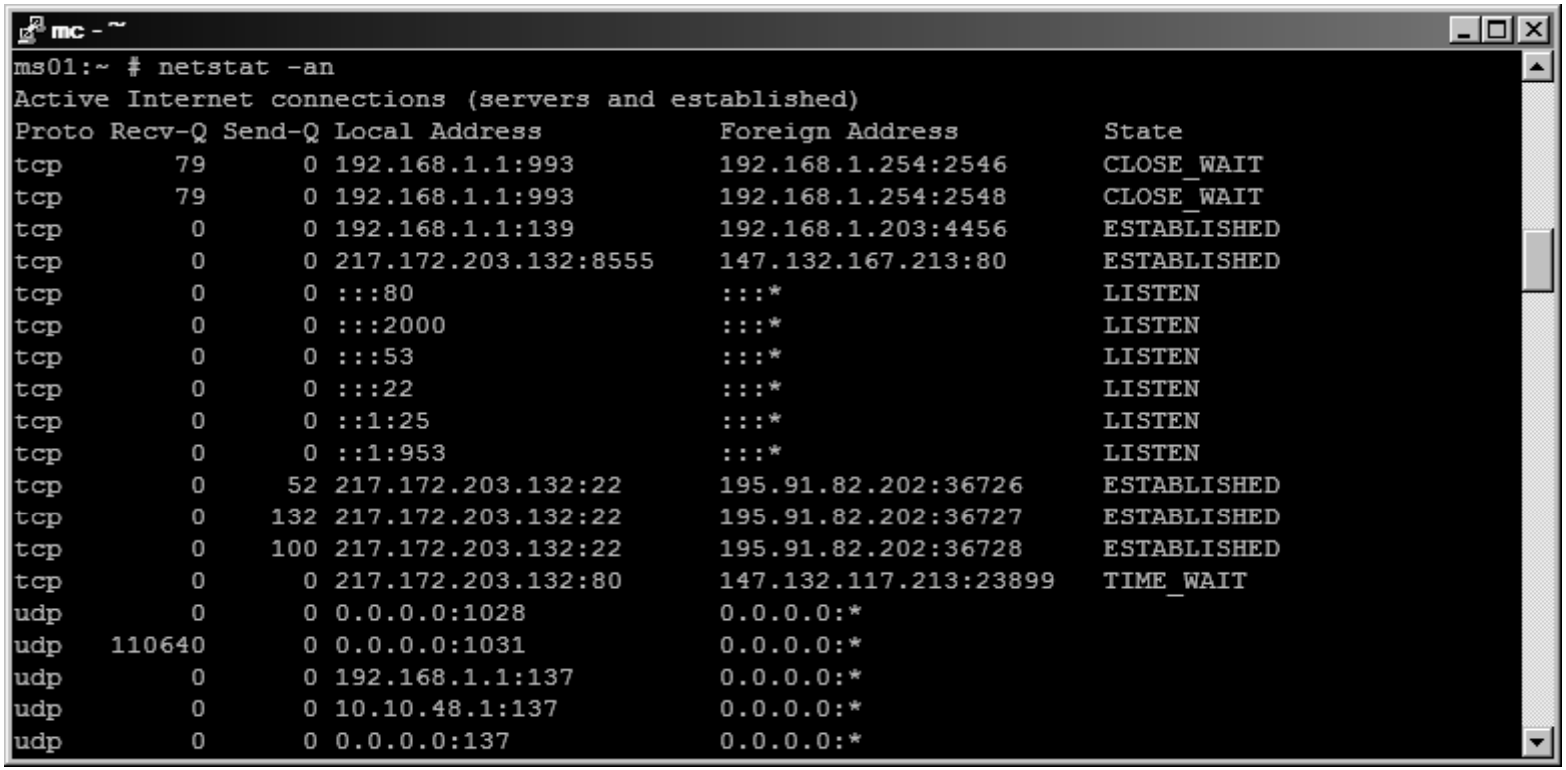
- Socket:
  - jednoznačné určenie komunikačného procesu/služby,
  - usporiadaná pätica:
    - transportný protokol,
    - zdrojová IP adresa,
    - zdrojový port,
    - cieľová IP adresa,
    - cieľový port.

Transportná vrstva

- Primitívy socketov:
  - **SOCKET** – vytvor nový komunikačný bod,
  - **BIND** – pripoj lokálnu adresu do socketu,
  - **LISTEN** – informuj o ochote akceptovať pripojenia,
  - **ACCEPT** – akceptuj prichádzajúce spojenie,
  - **CONNECT** – pokús sa o nadviazanie spojenia,
  - **SEND** – odošli dáta,
  - **RECEIVE** – prijmi dáta,
  - **CLOSE** – ukonči spojenie.

Transportná vrstva

- Socket
  - príkaz ***netstat***



Transportná vrstva

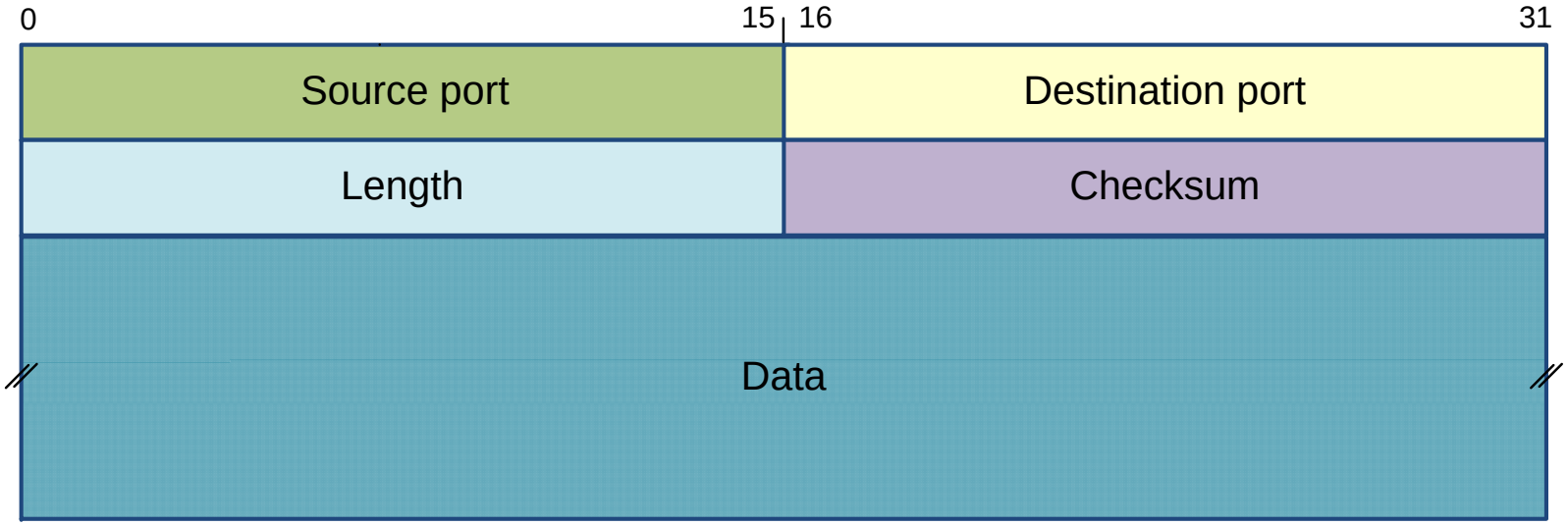
- Možné spôsoby realizácie v OS:
  - Spustenie komunikačnej služby pri štarte systému a jej priradenie definovanému portu.
  - Spustenie centrálneho komunikačného démona v čase štartovania, ktorý následne spúšťa jednotlivé komunikačné služby podľa potreby, v prípade príchodu požiadavky na daný port.
    - v UNIXe inetd a xinetd
  - Pre určité porty spustenie samotnej danej služby napr. webserver port 80, pre ostatné xinetd.

UDP – User Datagram Protocol

- User Datagram Protocol RFC 768:
  - nespojovo orientovaný protokol,
  - poskytuje nespoľahlivú službu,
  - umožňuje odosielať dáta bez potreby vytvorenia spojenia,
  - neposkytuje mechanizmy riadenia toku a riadenia chybovosti, môže poskytovať len detekciu chybovosti,
  - poskytuje vysielanie na všeobecné adresy, broadcast,
  - UDP datagram sa nefragmentuje sieťovou vrstvou (IP), IP paket však môže byť fragmentovaný na linkovej vrstve.

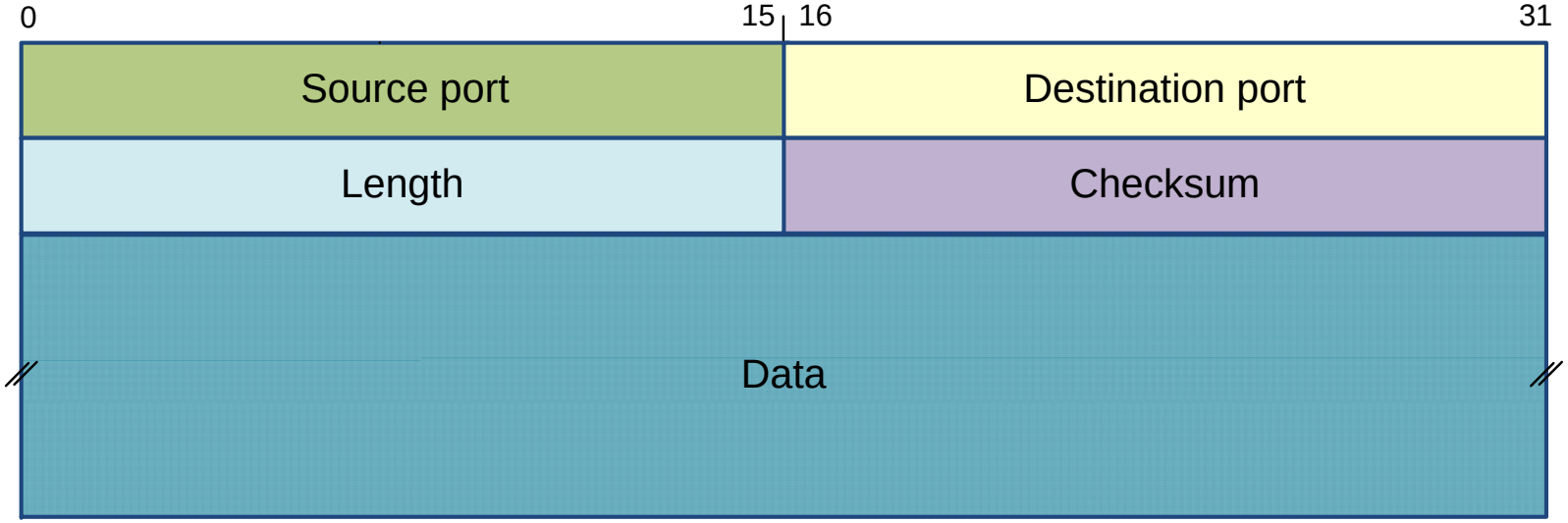
UDP – User Datagram Protocol

- Source/Destination port (16b) – zdrojový/cieľový port:
  - identifikácia aplikačných procesov,
  - informačné pole prichádzajúceho UDP segmentu sa odovzdá procesu pridelenému k danému cieľovému portu (napr. použitím primitívy BIND),
  - zdrojový port je nepovinný.



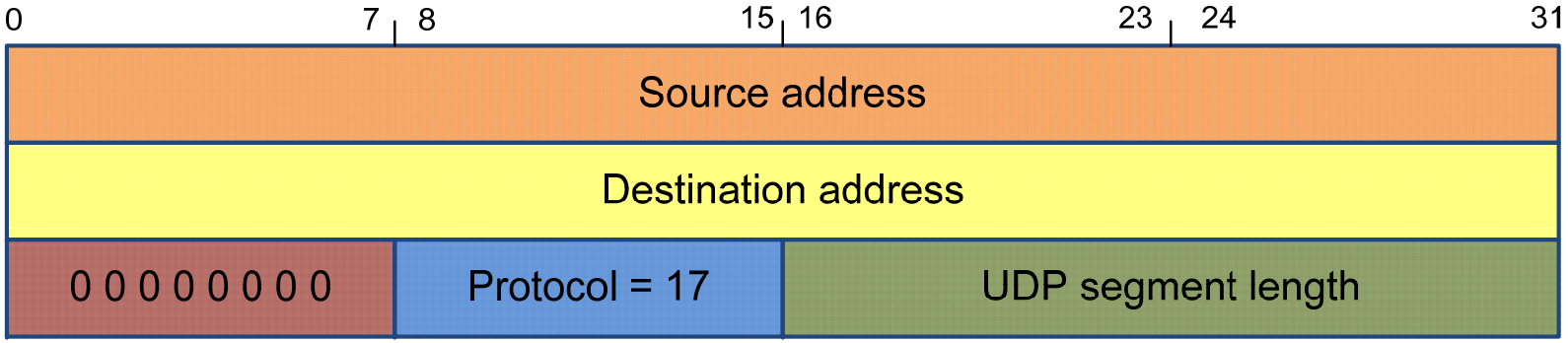
UDP – User Datagram Protocol

- Length (16b) – dĺžka celého UDP segmentu
  - v násobkoch 32b.
- Checksum (16b) – kontrolný súčet
  - celý UDP segment + pseudohlavička,
  - je nepovinný.



UDP – User Datagram Protocol

- Pseudohlavička:
  - slúži len na výpočet kontrolného súčtu, nepridáva sa do IP paketu,
  - fiktívne sa predradí pred pôvodný segment,
  - narušuje protokolovú hierarchiu, hlavička IP protokolu sa spracováva v transportnej vrstve,
    - IP adresa zdroja/cieľa (32b),
    - číslo protokolu UDP = 17, TCP = 6,
    - dĺžka segmentu – dĺžka pôvodného UDP datagramu bez pseudohlavičky.



UDP – User Datagram Protocol

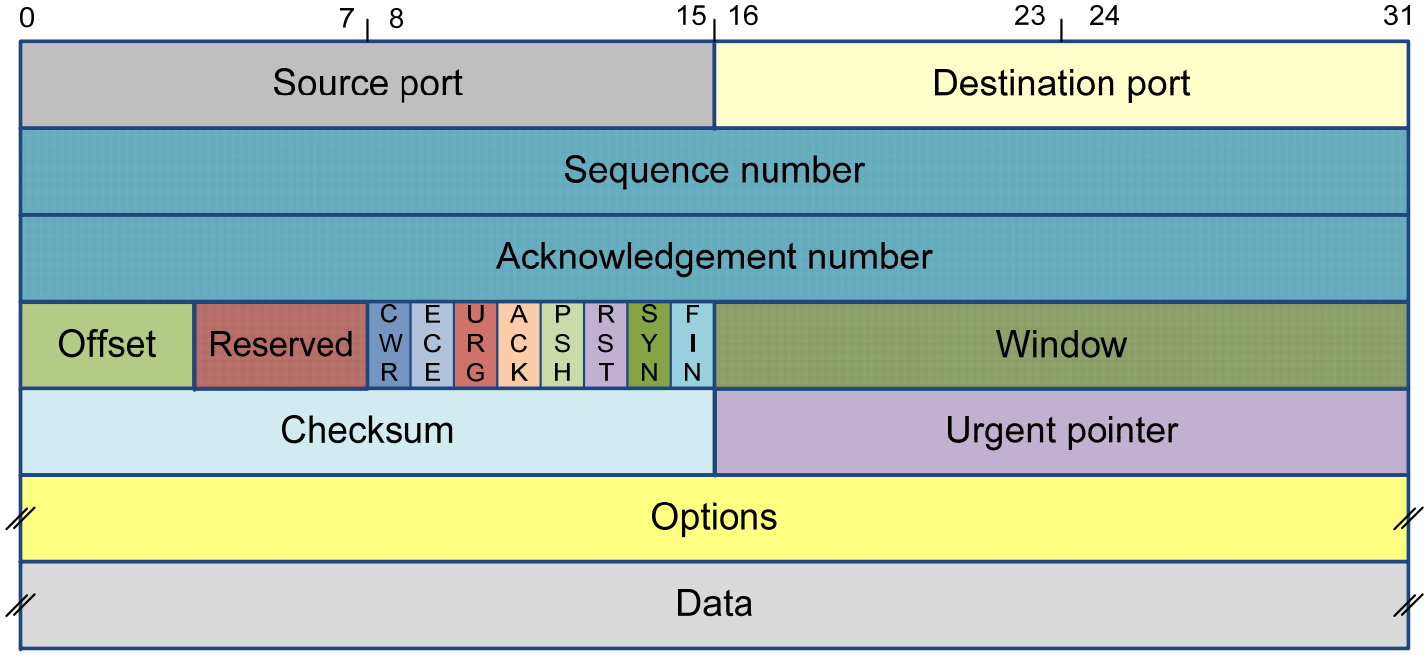
- Využíva sa hlavne pre služby, ktoré nevyžadujú spoľahlivý prenos a proces vytvárania spojenia pre samotný prenos je zbytočne zdĺhavý a neefektívny.
- Pre služby požadujúce broadcast vysielanie:
  - RTP - Real-time Transport Protocol (port 5004-5005),
  - SNMP – Simple Network Management Protocol (port 161-162),
  - DNS – Domain Name System (port 53),
  - BOOTP – BootStrap Protocol (port 67-68),
  - DHCP – Dynamic Host Configuration Protocol (port 67-68),
  - RIP – Routing Information Protocol (port 520),
  - TFTP – Trivial File Transfer Protocol (port 69),
  - ICPM echo – (port 7).

TCP – Transmission Control Protocol

- Transmission Control Protocol:
  - RFC 793, RFC 1122, RFC 1323,
  - spojovo orientovaný protokol,
  - poskytuje spoľahlivý, plne duplexný prenos dát,
  - vykonáva riadenie chybovosti a riadenie toku dát,
  - prenáša súvislý tok dát, tzv. stream, po predtým vytvorenom virtuálnom kanále,
  - dáta delí na segmenty, dĺžky zodpovedajúcej veľkosti IP datagramu,
  - kanál je identifikovaný príslušným socketom.

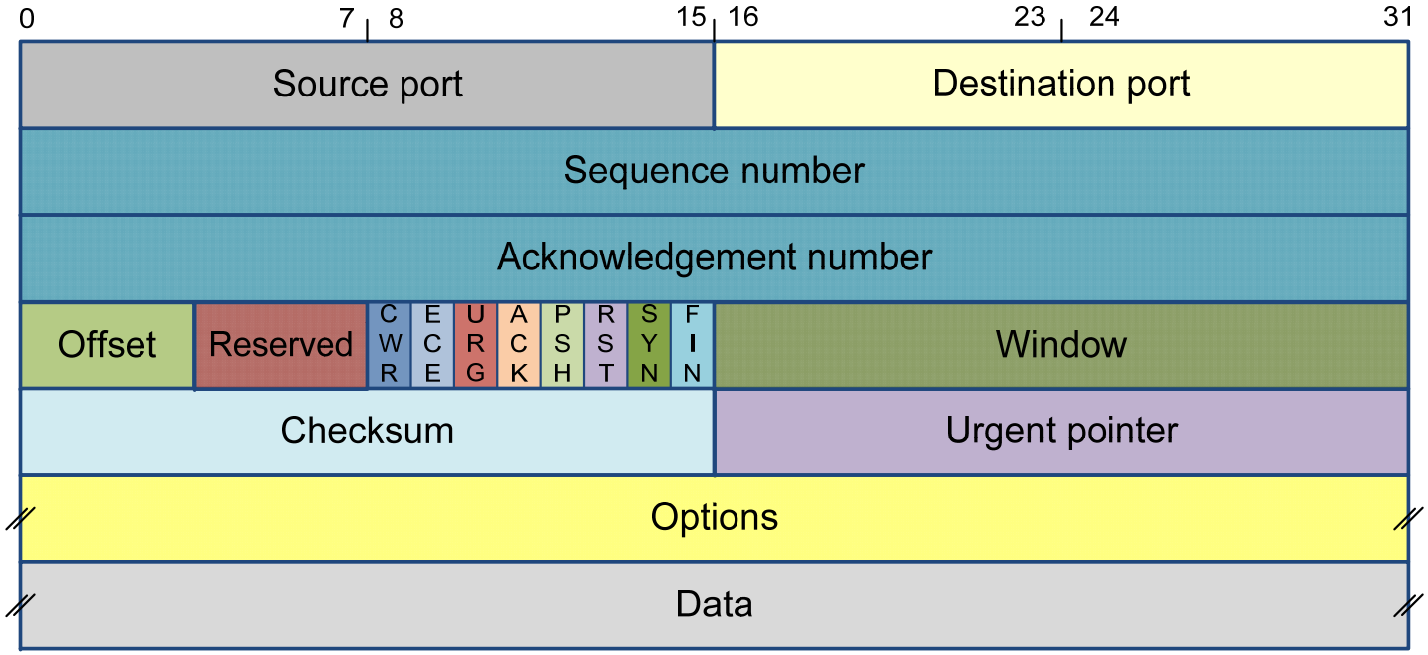
TCP – Transmission control protocol

- Source/destination port (16b) – zdrojový/cieľový port.
- Sequence number (32b) – poradové číslo prvého oktetu dát v segmente, počiatočná hodnota sa volí náhodne.
- Acknowledgement number (32b) – potvrdenie, špecifikuje poradové číslo oktetu, ktorý sa očakáva ako nasledujúci.



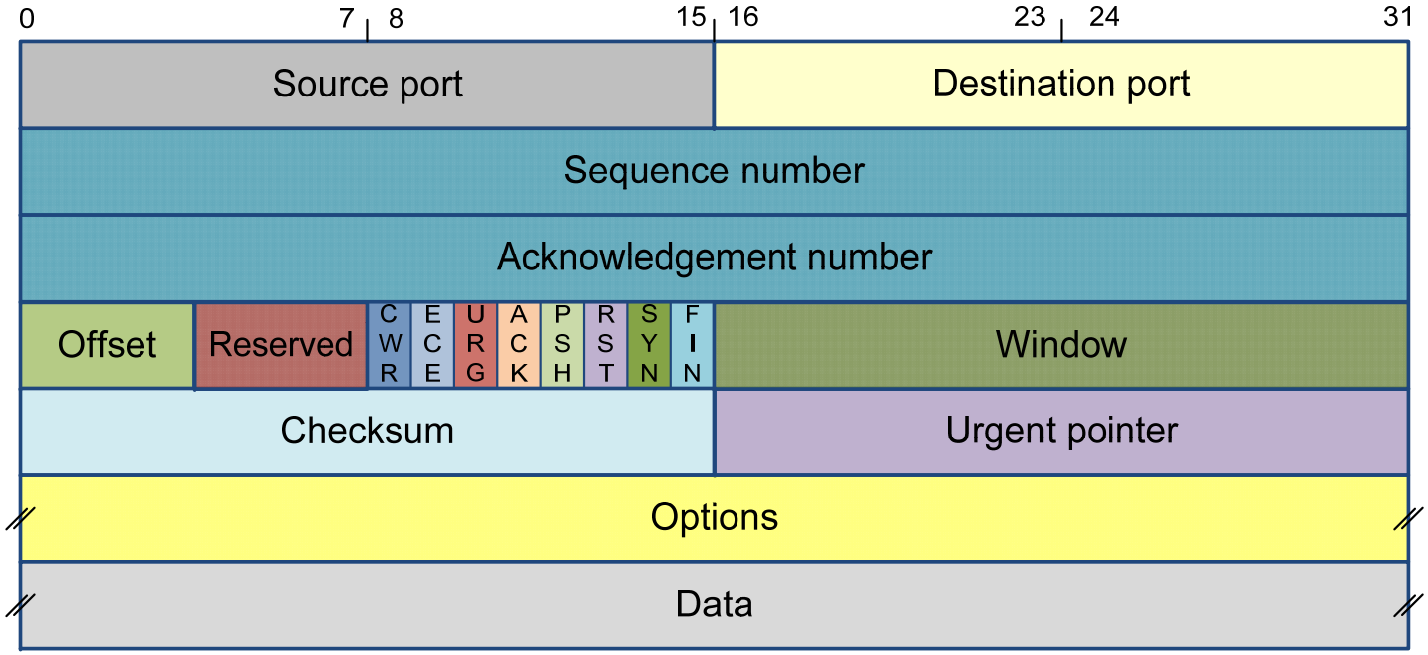
TCP – Transmission control protocol

- Offset (4b) – dĺžka hlavičky
  - v násobkoch 32b, vrátane voliteľných polí hlavičky, začiatok dát v pakete.
- TCP flags:
  - CWR (1b) – Congestion Window Reduced – informácia, že vysielač reagoval na oznámenie, o možnom zahltení prenosovej cesty.
  - ECE (1b) – ECN echo – informácia pri nadviazaní spojenia, že koncové zariadenia má ECN podporu (Explicit Congestion Notification).



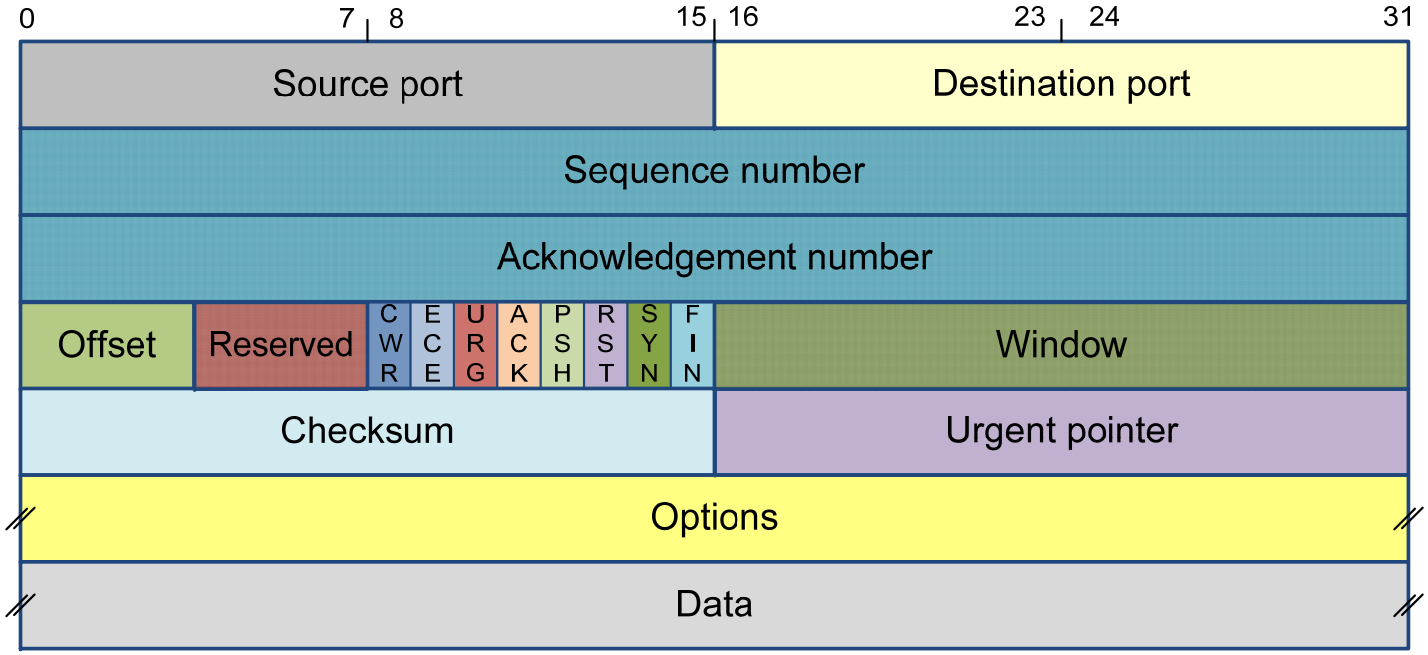
TCP – Transmission control protocol

- TCP flags:
  - URG (1b) – Urgent – dôležité dáta, prednostné doručenie,
  - ACK (1b) – označenie platnosti pola s číslom potvrdenia,
  - PSH (1b) – Push – požiadavka na okamžité doručenie segmentu protokolu vyššej vrstvy.



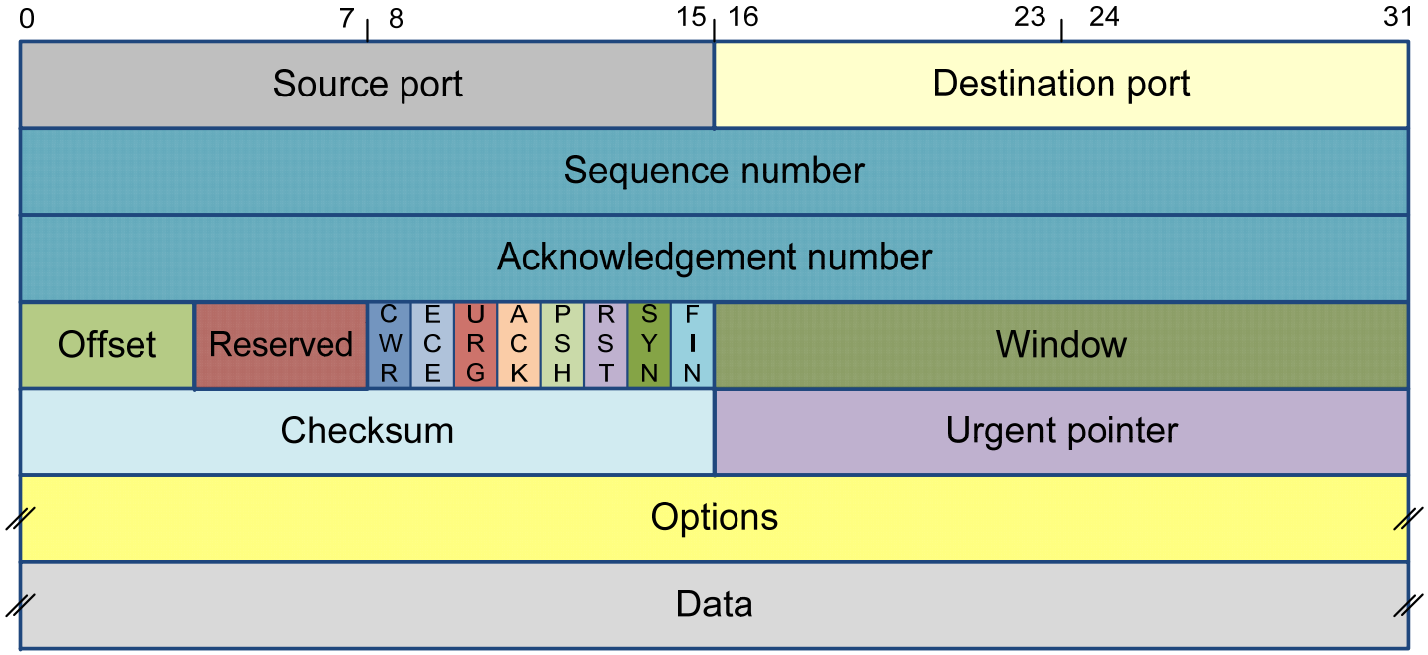
TCP – Transmission control protocol

- TCP flags:
  - RST (1b) – Reset – požiadavka na opätovné nadviazanie spojenia,
  - SYN (1b) – Synchronization – žiadosť o nadviazanie spojenia,
  - FIN (1b) – Finish – žiadosť o ukončenie spojenia.



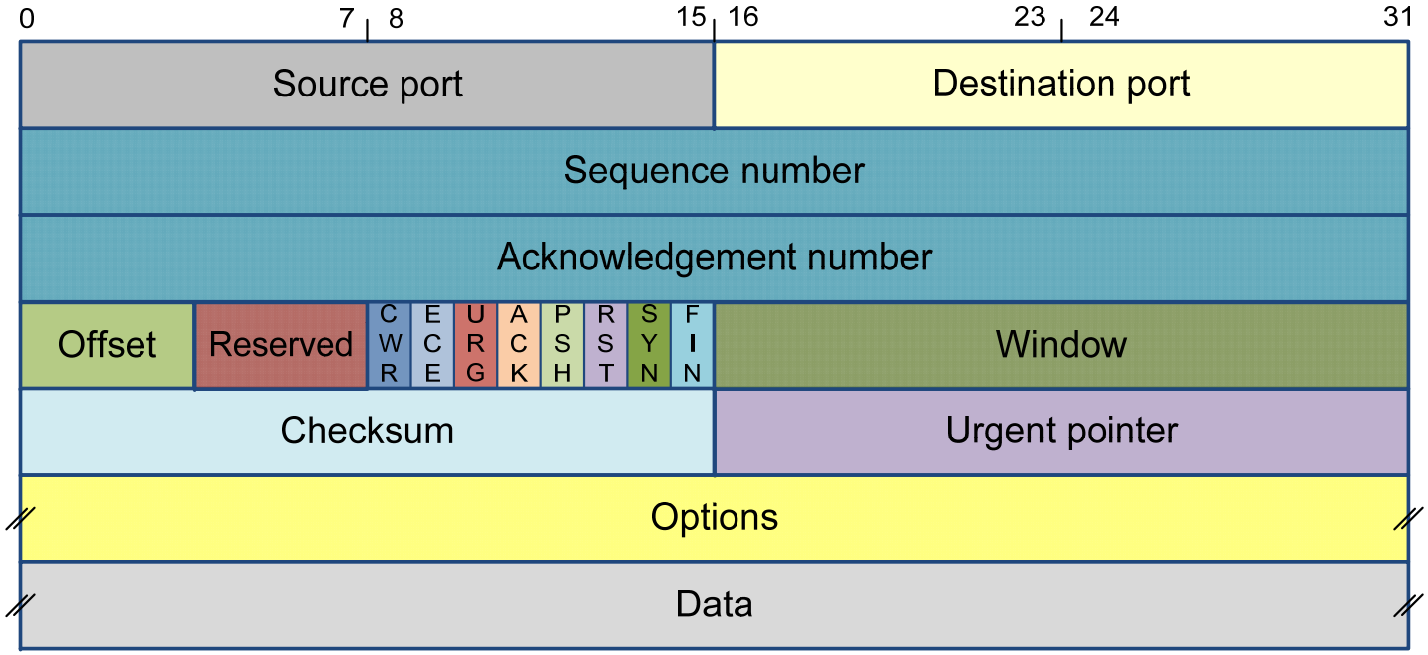
TCP – Transmission control protocol

- Window (16b) – veľkosť okna (počet oktetov, ktoré je možné vyslať bez priebežného potvrdenia).
- Checksum (16b) – kontrolný súčet celého segmentu vrátane pseudohlavičky.
- Urgent pointer (16b) – určuje posledný oktet urgentných dát v prípade, že URG = 1.



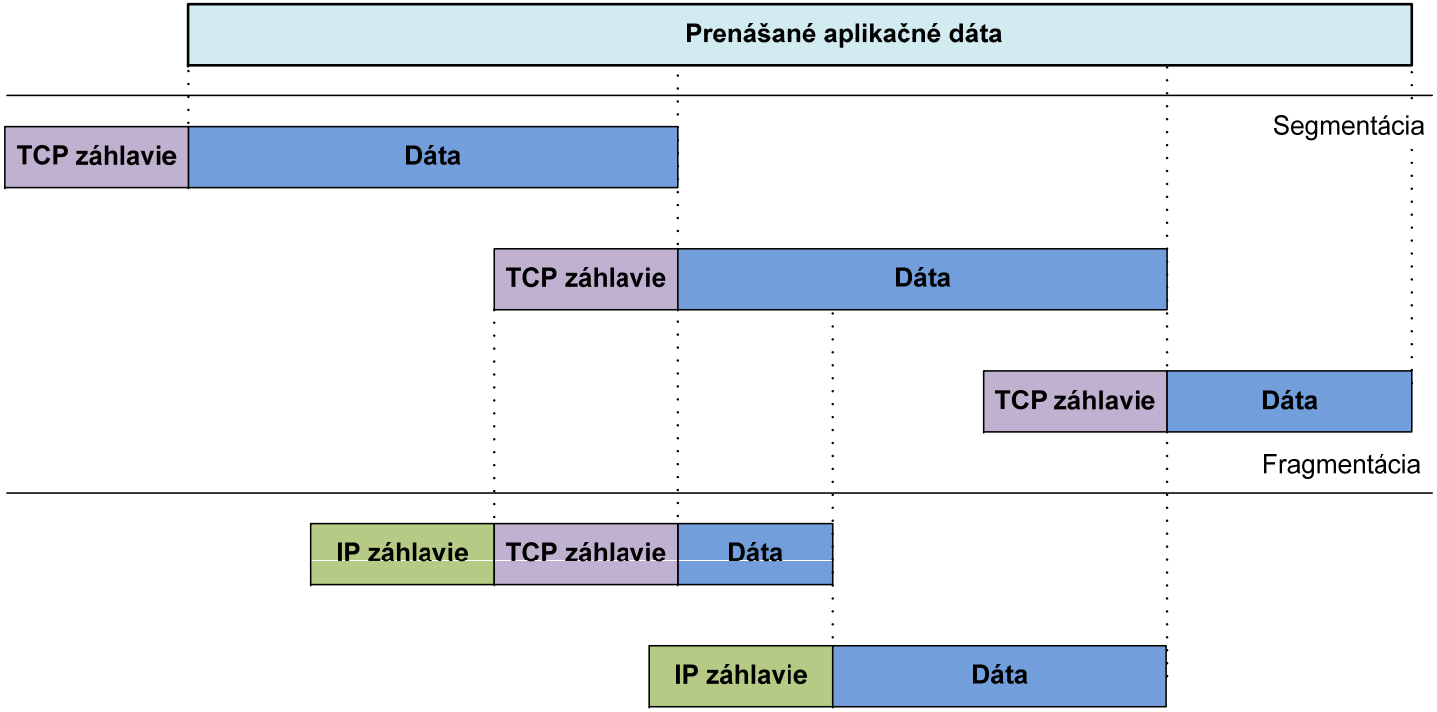
TCP – Transmission control protocol

- Options (max 320b) – doplnkové informácie, napr. maximálna veľkosť segmentu, nepovinné
  - veľkosť musí byť v násobkoch 32b.
- Data
  - veľkosť musí byť v násobkoch 32b.



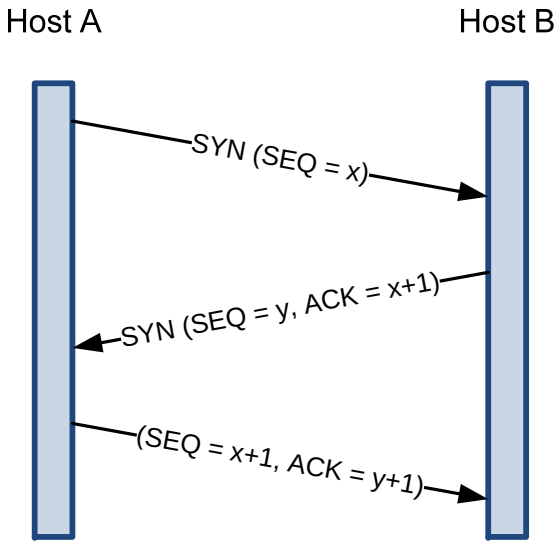
TCP – Transmission control protocol

- Dĺžka TCP segmentu
  - TCP segment (hlavička 20B + voliteľná časť 40B + dáta) < 65515B (IP payload).
  - TCP segment + IP hlavička < MTU (väčšinou 1500B), inak je potrebná fragmentácia.



TCP – Transmission control protocol

- Nadviazanie spojenia:
  - pred samotným začatím prenosu je potrebné nadviazať spojenie, tzv. three way handshake,
  - klient iniciuje spojenie, server naň odpovedá,
  - klient si svoj port zvyčajne volí dynamicky,
  - server vo väčšine prípadov používa všeobecne známy port (definovaný IANA),
  - pri nadviazaní spojenia si komunikačné strany dohodnú maximálnu veľkosť TCP segmentu, tak aby sa zamedzilo fragmentácii.



TCP – Transmission control protocol

- Prenos dát:
  - korektné prijatie segmentu je potvrdzované prijímačom,
  - využíva sa mechanizmus „sliding-window“,
    - pôvodne sa používalo ACK potvrdzovanie,
    - neskôr RFC 1106 pridalo NAK potvrdenie,
  - zlepšuje sa tým využitie prenosovej kapacity spojenia,
    - pôvodne sa používala ARQ metóda Go-Back-N,
    - RFC 2018 umožnilo využívať aj efektívnejšiu ARQ Selective repeat
  - veľkosť okna sa dynamicky mení v priebehu prenosu, nemusí byť rovnaké pre oba smery,
  - vďaka dynamickej zmene je možné efektívne riadiť tok dát tak, aby nedochádzalo k preťaženiu siete.

TCP – Transmission control protocol

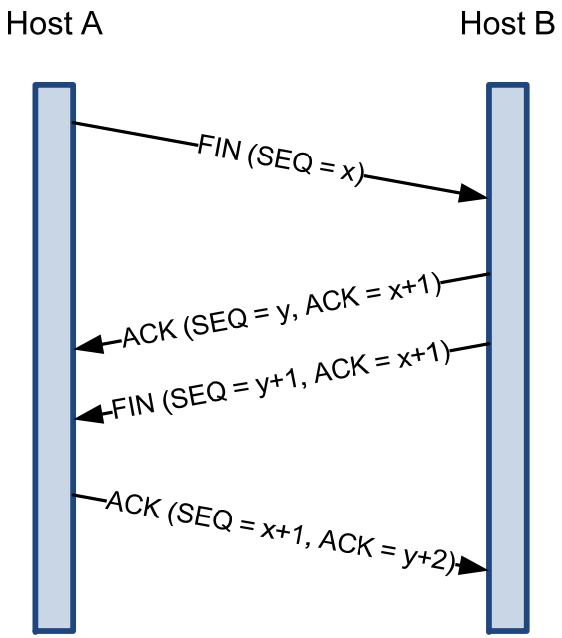
- Prenos dát:
  - prenášané segmenty sú číslované,
  - počiatočná hodnota čísla prvého segmentu sa volí náhodne,
  - oba smery komunikácie majú nezávislé číslovanie,
  - ak sa použije príznak SYN začne sa číslovať odznova,
  - číslovanie sa cyklicky počíta od 0 po 2^{32}-1,
    - problém pri vysokorýchlostných sieťach, veľkosť okna nepostačuje, je ho potrebné rozšíriť pomocou voliteľných položiek v hlavičke RFC 1323 (+14b).

TCP – Transmission control protocol

- Prenos dát:
  - ak segment nepríde alebo príde poškodený, vyžaduje sa jeho retransmisia,
  - stratené alebo poškodené segmenty sú znova vyžiadané,
  - retransmisia má nepriaznivý vplyv na oneskorenie,
  - prenosy, pri ktorých požadujeme minimalizáciu oneskorenia a bezchybný prenos, nie je veľmi dôležitý, nie je vhodné prenášať TCP protokol, vhodnejší je jednoduchší UDP protokol.

TCP – Transmission control protocol

- Ukončenie spojenia:
  - môže iniciovať ktorákoľvek komunikujúca strana,
  - prvá strana pomocou príznaku FIN vykoná tzv. aktívne ukončenie, druhá strana následne pasívne ukončenie,
  - ak strana vykoná aktívne ukončenie, nemôže už ďalej odosielať dáta, druhá strana však môže odosielať dáta, kým nevykoná pasívne ukončenie.



TCP – Transmission control protocol

- Využíva sa hlavne pre služby, ktoré vyžadujú spoľahlivý prenos dát a nie sú citlivé na oneskorenie prenosu:
  - TELNET ,
  - FTP – File transfer protocol,
  - HTTP – Hypertext transfer protocol,
  - SMTP – Simple mail transfer protocol,
  - IMAP4 – Internet message access protocol,
  - POP3 – Post office protocol,
  - BGMP – Border gateway protocol.

Relačná vrstva

- 5. vrstva OSI modelu – Session layer.
- nezávislá od technológií jednotlivých podsietí.
- nezávislá od topológie siete.
- hlavnou funkciou je riadenie relácie,
  - zabezpečuje, aby komunikácia medzi koncovými stanicami bola koordinovaná,
  - nadviazanie spojenia,
  - dohodnutie spôsobu komunikácie,
  - ukončenie prenosu,
  - obnovenie prerušeného dialógu.

Relačná vrstva

- Synchronizácia:
  - nie ako synchronizácia na fyzickej vrstve,
  - vkladajú sa synchronizačné body tzv. checkpoints, ktoré v prípade výpadku spojenia umožnia jeho obnovenie v danej pozícii prenosu, netreba prenášať všetko znova,
- zabezpečenie - šifrovanie,
- podpora transakcií.

Relačná vrstva

- model TCP/IP nepozná relačnú vrstvu, jej funkcionalitu zastrešuje v „Application layer“, mnoho protokolov, preto na prenos nevyužíva služby relačnej vrstvy, ale priamo prenáša dáta cez transportnú vrstvu,
- najpoužívanejšie protokoly:
  - **RTP** – Real-time transport protocol,
  - **RTCP** – Real-time transport control protocol,
  - SRTP – Secure RTP,
  - SSL – Secure socket layer,
  - **TLS** – Transport layer security,
  - L2TP – Layer 2 Tunneling Protocol,
  - LDAP – Light weight access protocol.

RTP – Real-time transport protocol

- Prenos dát v reálnom čase,
  - RFC 1889, RFC 1890, RFC 3550, RFC 3551.
- Základné služby:
  - rekonštrukcia dát v čase,
  - detekcia straty dát,
  - identifikácia prenášaných dát a ich bezpečnosť.
- najčastejšie sa využíva pre prenos audio a video dát,
- zabezpečuje doručenie segmentov v správnom poradí,
- pomocou časových značiek, ktoré vkladá do prenosu, je prijímač schopný rekonštruovať signál v čase.

RTP – Real-time transport protocol

- Definuje špeciálne profily:
  - RFC 3551 – RTP Profile for Audio and Video Conferences with Minimal Control,
    - prenos audio a video konferencií s minimálnym riadením,
  - RFC 3711 - Secure Real-time Transport Protocol (SRTP) profil,
    - rozšírenie RTP profilu pre audio a video konferencie,
    - zvýšenie zabezpečenia prenosu,
      - utajenie,
      - overenie správ,
      - ochrana pre opätovným prehraním dát.

RTP – Real-time transport protocol

- umožňuje unicast aj multicast vysielanie,
- ako transportný protokol využíva UDP protokol,
- prenos dát v reálnom čase vyžaduje minimalizáciu oneskorenia,
  - TCP protokol má príliš veľkú réžiu a retransmisia chybných dát zvyšuje oneskorenie, preto nie je vhodné využívať tento protokol,
- RTP protokol nezabezpečuje minimalizáciu oneskorenia, to je potrebné vykonať na nižších vrstvách, v rámci implementácie metód zabezpečenia QoS (Quality of service).

RTP – Real-time transport protocol

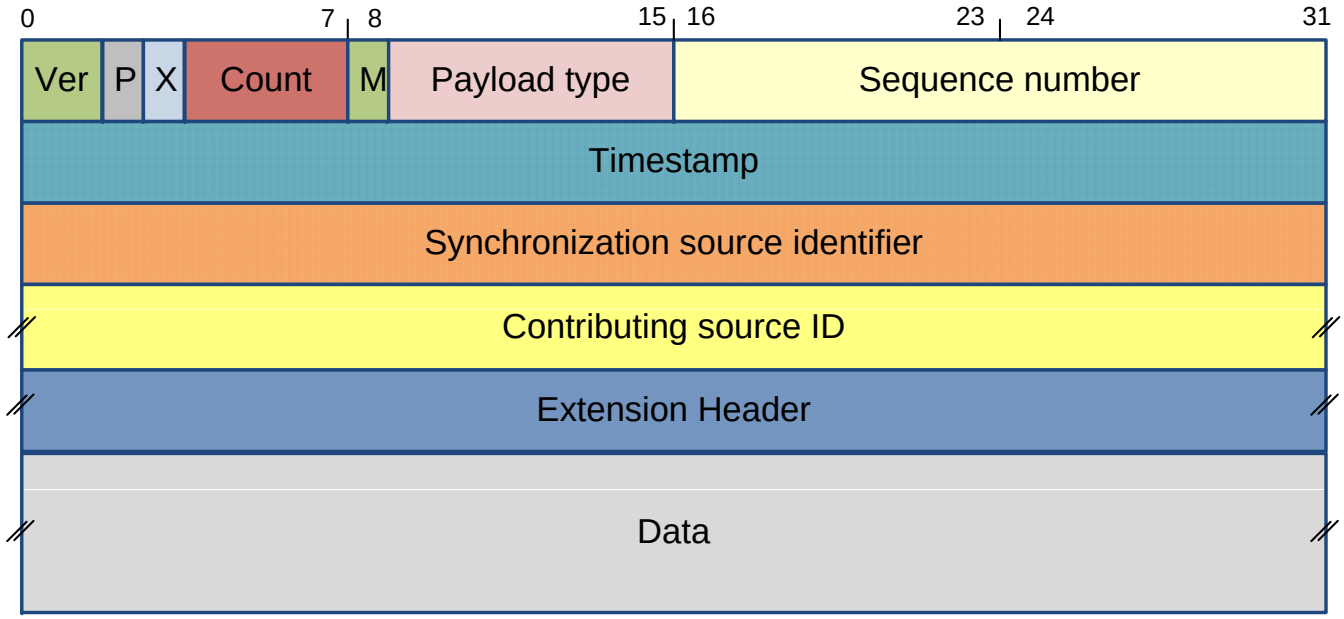
- multiplexovanie viacerých signálov v reálnom čase do spoločného toku UDP paketov,
- chýbajúce dáta je potrebné v prijímači interpolovať, ich znovu vyslanie by trvalo dlhý čas,
- RTP neposkytuje:
  - riadenie chybovosti,
  - riadenie toku dát,
  - mechanizmus potvrdenia prijatia správ,
  - vyžiadanie znovu vyslania chybných dát.

RTP – Real-time transport protocol

- využíva sa pri prenose aplikácií vyžadujúcich rekonštrukciu signálu v čase,
- mnoho z nich vyžaduje aj minimalizáciu oneskorenia
  - prenos telefónnych volaní pri VoIP technológii (Voice over IP),
  - prenos videa v IPTV,
  - videokonferencie,
  - internetové rádia,
  - streaming videa,
  - hudba a video na požiadanie.

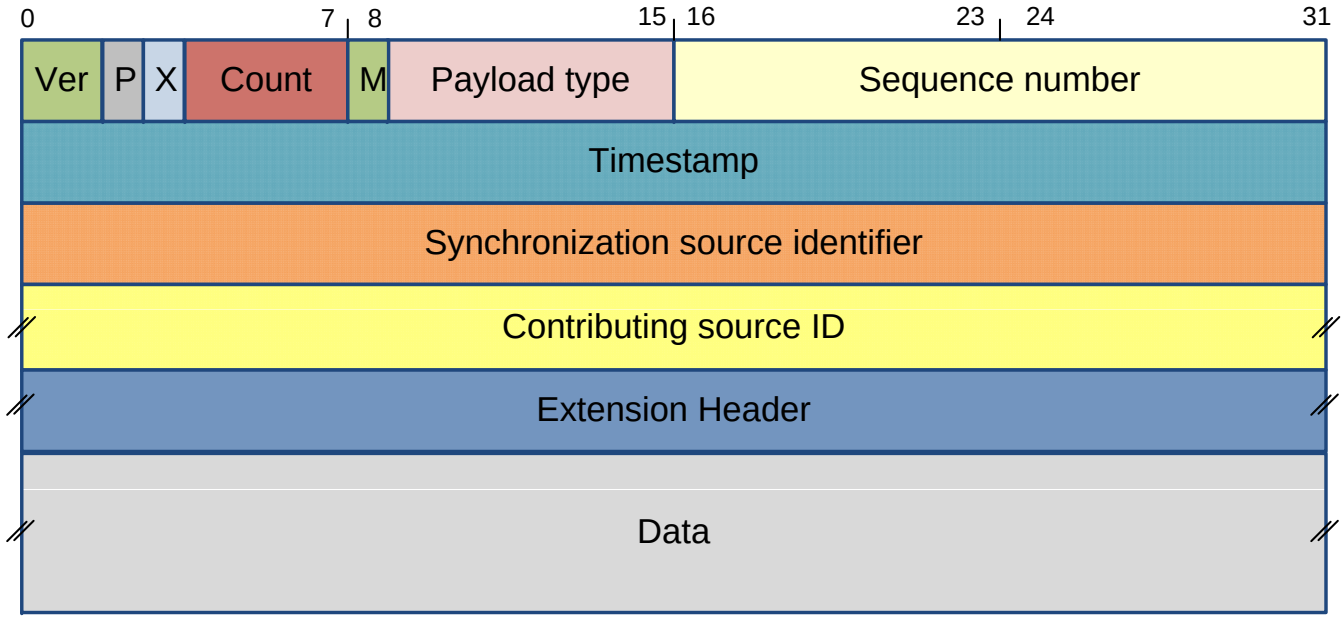
RTP – Real-time transport protocol

- **Ver**sion (2b) – verzia RTP protokolu aktuálna je v2.
- **P**adding (1b) – výplň:
  - ak je bit nastavený, znamená to, že paket obsahuje na konci dát viacero bajtov výplne, ktoré sú určené na zarovnanie paketu na určitú dĺžku. Posledný bajt výplne obsahuje počet bajtov, ktoré tvoria výplň (výplň je pri spracovaní ignorovaná).



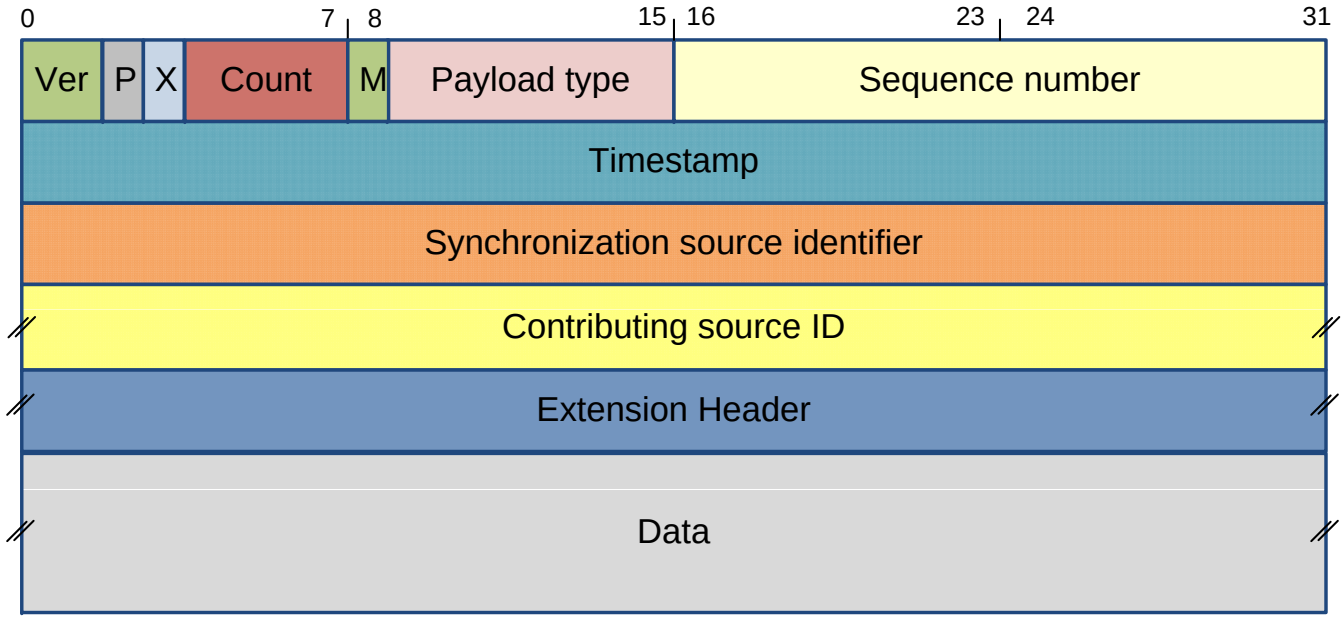
RTP – Real-time transport protocol

- E**x**tension (1b) – rozšírenie:
  - ak je bit nastavený ,tak za fixnou hlavičkou nasleduje ešte rozšírená hlavička.
- **M**arker (1b)– označenie:
  - najčastejšie za využíva na označenie začiatku prenášaných dát, jeho význam sa mení na základe špecifikácie typu prenášaných dát.



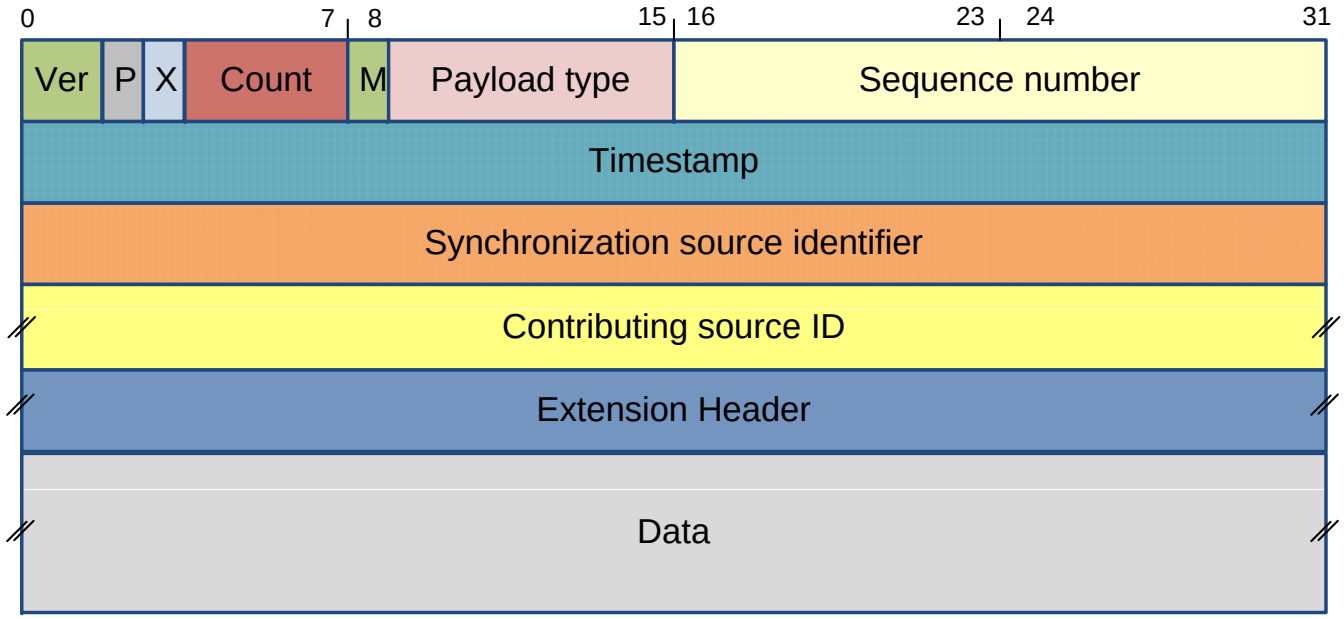
RTP – Real-time transport protocol

- CSRC Count (4b) – počet identifikátorov všetkých zdrojov
  - V prípade, že relácia má viac ako dvoch účastníkov, je možné využiť tzv. RTP mixer, ktorý spája viacero samostatných zdrojov RTP dát do jedného toku. Výhodné je to napríklad pri konferencii viacerých účastníkov, kedy sa vygeneruje jeden RTP stream obsahujúci toky všetkých zdrojov. Indetifikátory všetkých zdrojov sú prenášané za fixnou hlavičkou. CSRC Count pole obsahuje ich počet.



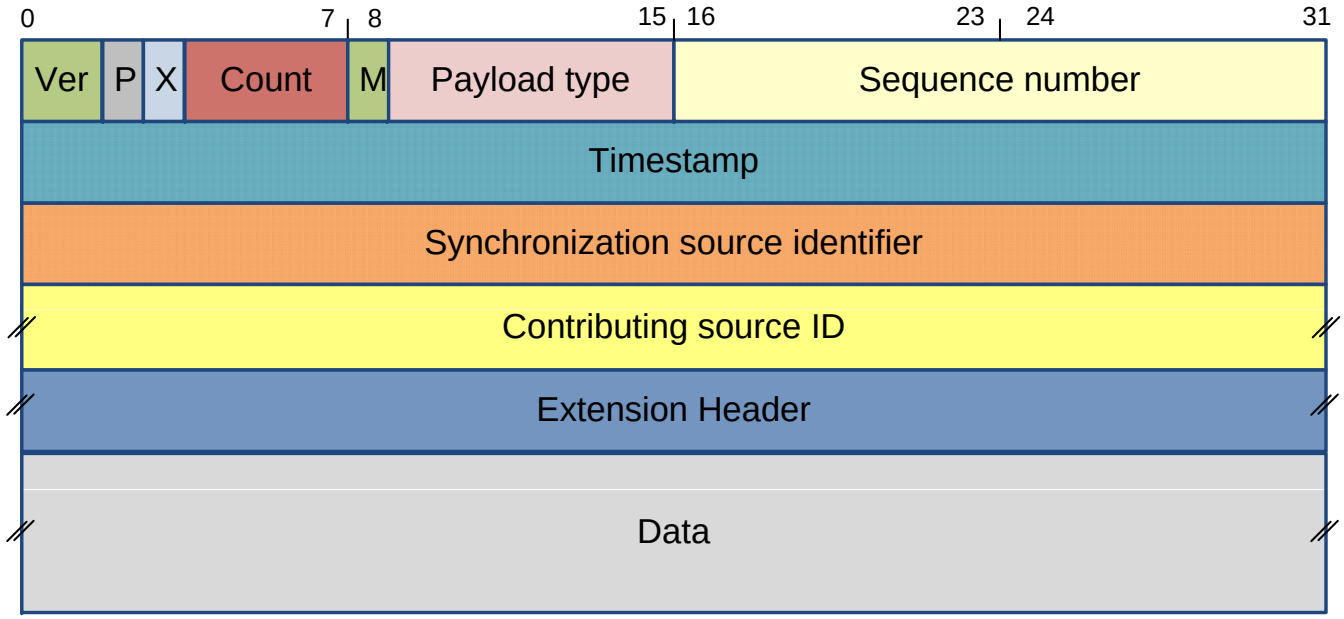
RTP – Real-time transport protocol

- Payload Type (7b) – typ prenášaných dát
  - udáva typ prenášaných dát a ich interpretáciu aplikáciami, je definovaný použitým profilom.
- Sequence number (16b) – sekvenčné číslo
  - číselné označenie paketu, vždy sa zvyšuje o 1 pre ďalší paket. Slúži na detekciu straty dát a na obnovenie správneho poradia paketov. Počiatočná hodnota sa volí náhodne, hlavne z dôvodu zvýšenia bezpečnosti.



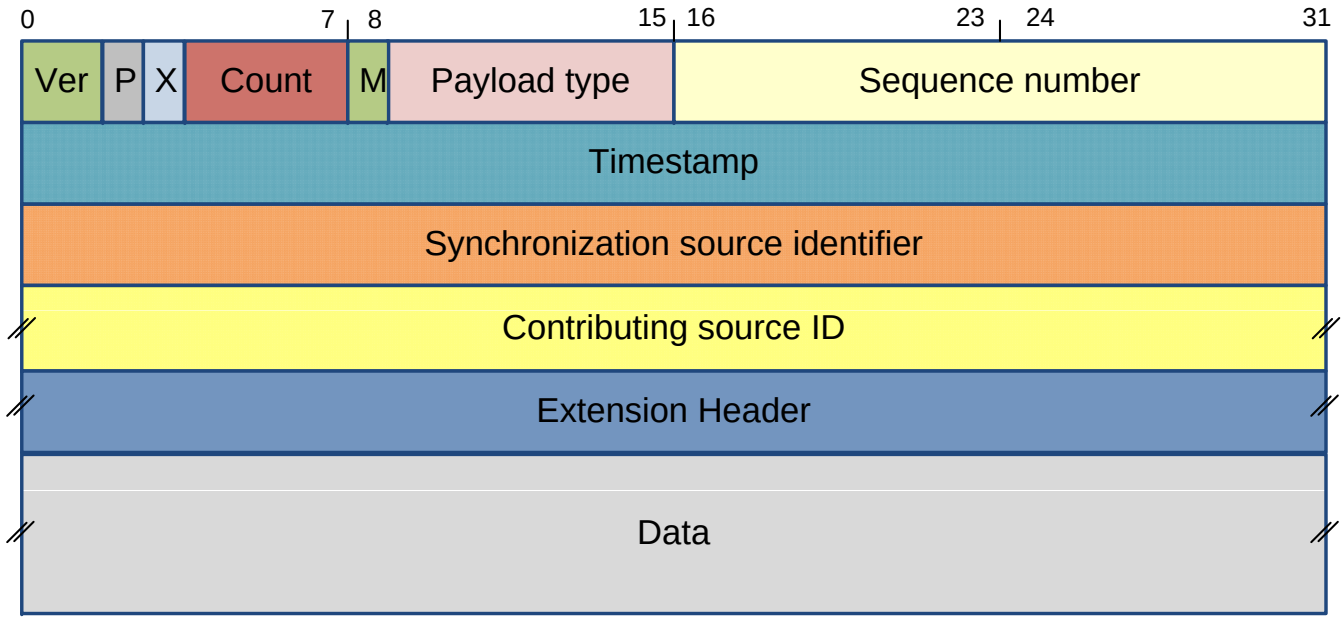
RTP – Real-time transport protocol

- Timestamp (32b) – časová značka
  - reprezentuje čas navzorkovania prvého bajtu dát v pakete. Umožňuje prijímaču rekonštruovať signál v čase. Aký časový údaj vyjadruje pole timestamp je definované v profiloch.
- Synchronization source identifier (32b) – identifikátor zdroja
  - jednoznačný identifikátor zdroja daného toku.



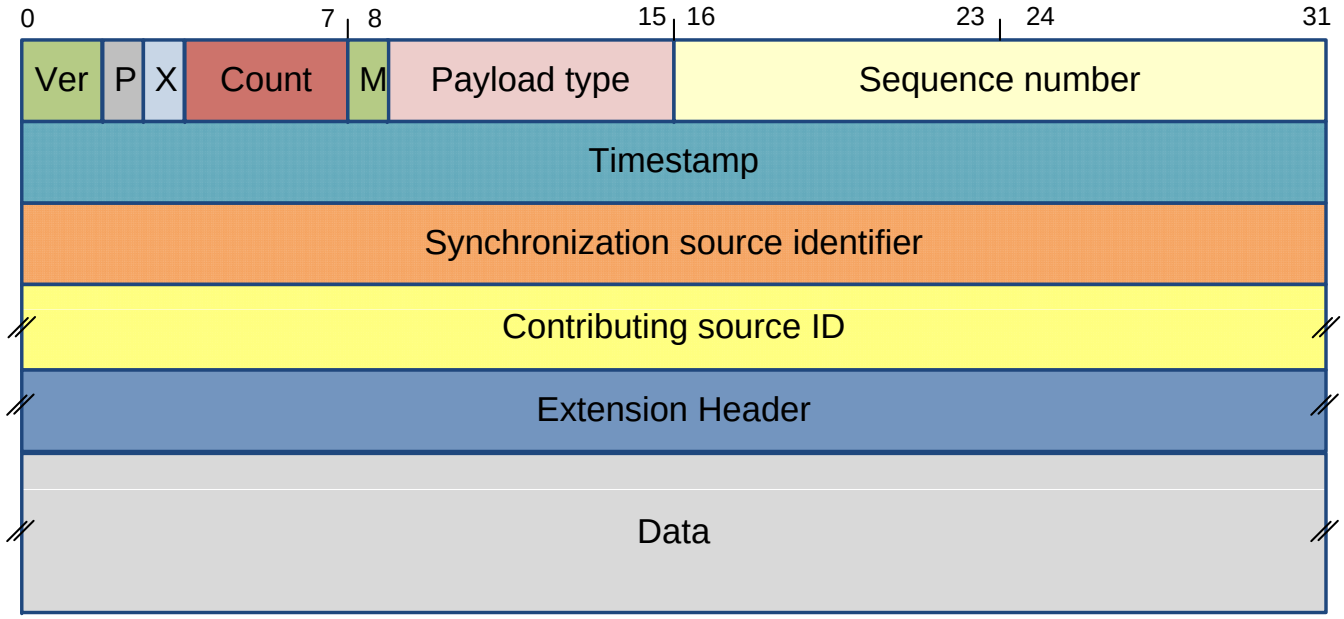
RTP – Real-time transport protocol

- Contributing source IDs (násobky 32b) – identifikátory zdrojov
  - identifikátory jednotlivých zdrojov, ktoré prispeli k vytvoreniu prenášaného toku dát,
  - nepovinná položka, využíva sa ak sa pomocou RTP mixera spája viacero tokov do jedného.



RTP – Real-time transport protocol

- Extension header – rozšírená hlavička :
  - voliteľná položka,
  - Profile identifier (16b) – identifikátor profilu,
  - Extension header length (16b) – dĺžka rozšírenia,
    - dĺžka rozšírenia v násobkoch 32b, vrátane hlavičky rozšírenia.



RTCP – Real-time transport control protocol

- RFC 1889 a RFC 3550,
- podporný protokol pre RTP, neprenáša žiadne multimediálne dáta,
- riadenie distribúcie dát a poskytovanie spätnej väzby o kvalite prenosu,
  - oneskorenie, jitter, šírka pásma, preťaženie,
- pracuje na princípe periodického vysielania riadiacich paketov, všetkým účastníkom prenosu.

RTCP – Real-time transport control protocol

- Základné funkcie:
  - poskytovanie spätnej väzby od príjemcov o kvalite distribúcie dát,
    - dáta sa posielajú všetkým účastníkom spojenia, taktiež je možné dáta posielať aj entitám, ktoré sa samotného RTP prenosu nezúčastňujú,
  - prenáša identifikáciu RTP zdroja, tzv. CNAME,
    - slúži na identifikáciu viacerých RTP tokov, že patria spolu (audio+video), na rozdiel od SSRC sa nemení (SSRC sa môže zmeniť v prípade kolízie s SSRC iného zdroja),
  - zisťovanie počtu účastníkov prenosu a rýchlosť odosielania RTCP paketov účastníkmi,
  - prenos doplnkových informácií o účastníkoch prenosu, napríklad mená účastníkov.

RTCP – Real-time transport control protocol

- Typy RTCP paketov:
  - **SR** – Sender Report
    - prenos kvalitatívnych parametrov o vysielaní a príjme od všetkých aktívnych účastníkov prenosu,
  - **RR** – Receiver Report
    - prenos kvalitatívnych parametrov o príjme od neaktívnych účastníkov prenosu,
  - **SDES** – Source Description Items
    - popis zdrojov dát, napr. CNAME,
  - **BYE** – Oznámenie o ukončení komunikácie,
  - **APP** - Application Specific Functions
    - prenos špecifických informácií danej aplikácie využívajúcej RTP.

Komprimovaný RTP

- RTP kompresia:
  - v dátovej časti
    - RFC 2435 – RTP Payload Format for JPEG-compressed Video,
  - v hlavičke
    - RFC 2508 – Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.
- CRTP – Compressed RTP:
  - kompresia hlavičky IP, UDP a RTP protokolu,
  - pre spoľahlivé a rýchle dvojbodové spoje,
  - RFC 2509 – IP Header Compression over PPP.
- ECRTP – Enhanced CRTP:
  - pre VoIP a málo spoľahlivé siete s dlhými odozvami,
  - RFC3545 – Enhanced Compressed RTP (CRTP) for links with high delay, packet loss and reordering.

TLS – Transport layer security

- slúži na šifrovanie dát protokolov vyšších vrstiev,
- predchodca je protokol SSL – Secure socket layer,
- využíva transportný protokol TCP,
- komunikácia sieťou je šifrovaná, aby bolo znemožnené
  - odpočúvanie komunikácie,
  - manipulácia a falšovanie správ,
- poskytuje mechanizmy na overenie dôveryhodnosti komunikujúcich strán,
  - autentifikácia.

TLS – Transport layer security

- Autentifikácia:
  - jednostranná
    - najčastejšie je autentifikovaný server
    - klient si môže byť istý s kým komunikuje,
    - klient zostáva neautentifikovaný,
  - obojstranná
    - autentifikovaný je aj server aj klient,
    - využíva sa „infraštruktúra verejného kľúča“ Public key infrastructure PKI.

TLS – Transport layer security

- Proces šifrovania zahŕňa 3 fázy:
  - užívatelia sa dohodnú na podporovaných algoritmoch šifrovania,
  - pomocou dohodnutých šifrovacích algoritmov si vymenia šifrovacie kľúče,
    - využívajú asymetrické šifrovanie s použitím verejných kľúčov,
    - identitu overujú pomocou certifikátov,
  - pomocou dohodnutých algoritmov symetrickou šifrou šifrujú prenášané dáta,
    - šifrovací kľúč získajú výmenou cez asymetricky šifrované spojenie,
    - symetrické šifrovanie je výkonnejšie ako asymetrické.

TLS – Transport layer security

- Podporované možnosti:
  - asymetrické šifrovanie s verejným kľúčom
    - RSA, Diffie-Hellman, DSA,
  - symetrické šifrovanie
    - RC2, RC4, IDEA, DES, Triple DES, AES, Camellia,
  - jednosmerná transformačná funkcia tzv. hash
    - Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2).

- SSL a TLS prenos využívajú napríklad protokoly:
  - HTTP (HTTPs), IMAP (IMAPs), POP3 (POP3s), FTP (SFTP).

Prezentačná vrstva

- 6. vrstva OSI modelu – Presentation layer.
- rovnaké interpretovanie rovnakých dát,
- konverzia (kódovanie znakov, formát číslic)
  - existuje množstvo systémov, ktoré majú rôzne kódované znaky, je potrebné vykonať ich prevod.
- šifrovanie, kompresia,
  - veľmi často je jej funkcionalita implementovaná v aplikáciách na aplikačnej úrovni,
  - protokoly,
    - ASCII, ASN.1, X.25, RDP, AES, DES.

ASCII

- American Standard Code for Information Interchange,
- kódovací štandard bitovej reprezentácie jednotlivých znakov (abeceda, číslovky, špeciálne znaky),
- každý znak je reprezentovaný 8 bitmi (pôvodne 7b),
- pre potreby reprezentácie špecifických znakov jednotlivých jazykov boli vytvorené kódovacie tabuľky,
- napr. pre slovenčinu
  - ISO 8859-2, Windows -1250, CP852 (Latin2), Kód Kamenických,
- v súčasnosti sa nahrádza kódovaním Unicode (UTF-8, UTF-16).

ASN.1

- Abstract Syntax Notation One,
- odporúčanie ITU X.208, X.680, X.683,
- poskytuje mechanizmus na reprezentáciu dátových objektov tak, aby bol ich význam a hodnota jednoznačne definovaná,
- jazyk umožňuje:
  - definovať jednotlivé údajové položky,
  - definovať ich typ,
  - prideliť im názov.

KOMUNIKAČNÉ A INFORMAČNÉ SIETE

TRANSPORTNÁ VRSTVA
RELAČNÁ VRSTVA
PREZENTAČNÁ VRSTVA

Ing. Michal Halás, PhD.
halas@ktl.elf.stuba.sk, B-514 , http://www.ktl.elf.stuba.sk/~halas