# 10. TCP, UDP, datagramy a porty obecně

## Teoretická část:

**Vysvětlete a popište protokoly transportní vrstvy TCP/IP: TCP, UDP vč.** **datagramů, paketů a portů. Specifikujte jednotlivé skupiny.**

## Praktická část:

1. **Nakreslete, nebo popište strukturu UDP datagramu. Popište jeho použití.**
2. **Porovnejte strukturu TCP paketu s UDP. Vysvětlete výhody a nevýhody obou.**
3. **Popište aplikaci blokování určitého portu na firewallu routeru.**

## Doplňující otázky:

1. **Připojte k portům příslušný protokol či službu: http, 443, 8080, 53, (20, 21, SSH,23), IMAP, POP.**
2. **Jakým příkazem v cmd vypíšete routovací tabulku?**

# Transportní vrstva

Transportní vrstva je první vrstvou, se kterou se setkáme pouze v koncových uzlech sítě, ale nikoli v jejích vnitřních uzlech (ve směrovačích). Však také hlavním úkolem transportní vrstvy je zajišťovat vzájemnou komunikaci koncových uzlů (tzv. end-to-end komunikaci). Je také první vrstvou, která v rámci uzlu rozlišuje jednotlivé entity (procesy), prostřednictvím tzv. portů. Nižší vrstvy se na jednotlivé uzly dívají vždy jako na dále nedělitelný celek.

## TCP (Transmission Control Protocol)

Transmission Control Protocol vytváří virtuální okruh mezi koncovými aplikacemi, tedy spolehlivý přenos dat. TCP je spojově orientovaný protokol. Zajišťuje:

* **proudový přenos dat** – není potvrzován každý paket, ale skupina (window); každý segment je identifikován sekvenčním číslem; pokud TCP dostane od vyšších vrstev balík dat, rozdělí je do segmentů, označí sekvenčním číslem a pošle 3. vrstvě (IP) k přenosu;
* **spolehlivost** – zajištěna potvrzováním příjmu skupiny paketů; Spolehlivá transportní služba, doručí adresátovi všechna data bez ztráty a ve správném pořadí. Služba se spojením, má fáze navázání spojení, přenos dat a ukončení spojení.
* ztracené nebo opožděné pakety příjemce nepotvrdí a odesílatel je pošle znovu; efektivní řízení toku – příjemce nepotvrzuje každý paket, ale skupinu (příjemce informuje odesílatele jaké množství paketů je schopen přijmout čímž je zamezeno přetečení jeho interních bufferů);
* **plně duplexní operaci** – TCP umožňuje přijímat i odesílat data současně;
* **multiplexing** – možnost datových toků různých aplikací vyšších vrstev najednou prostřednictvím jednoho spojení. Rozlišování aplikací pomocí portů.

Aplikace používající TCP jako přenosový protokol – např. FTP, SMTP, http, SAP, SMB.

## UDP (User Datagram Protocol)

User Datagram Protocol poskytuje nespolehlivou transportní službu pro takové aplikace, které nepotřebují spolehlivost, jakou má protokol TCP. Nemá fázi navazování a ukončení spojení a už první segment UDP obsahuje aplikační data. UDP je používán aplikacemi jako je DHCP, TFTP, SNMP, DNS a BOOTP.   
Protokol používá podobně jako TCP čísla portů pro identifikaci aplikačních protokolů.

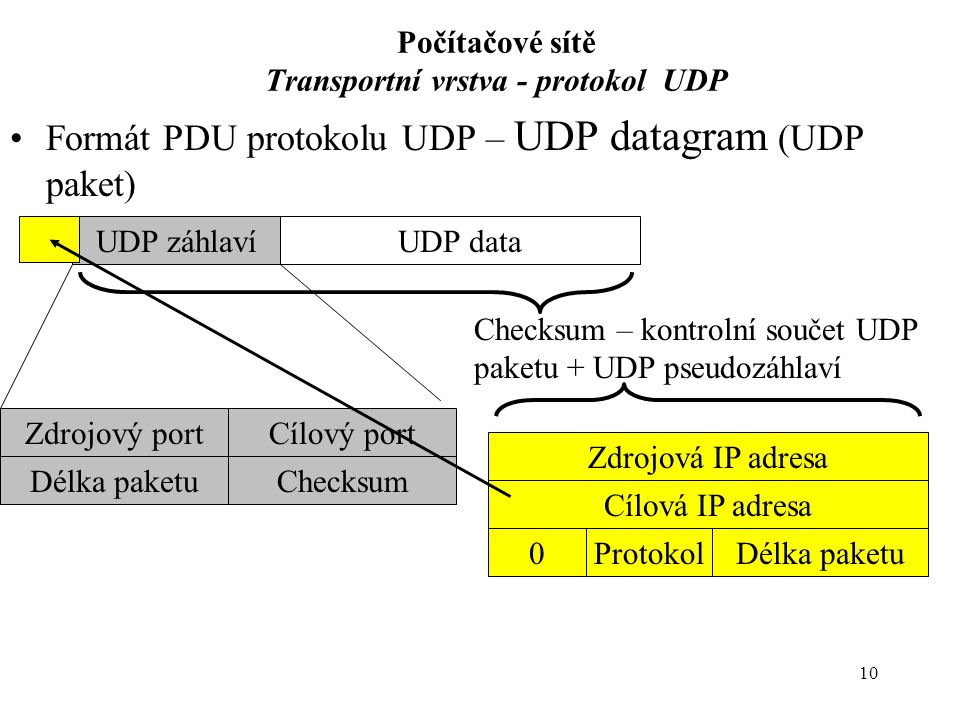
* UDP je nespojový (connectionless) protokol;
* nepřináší vlastnosti spolehlivosti přenosu, řízení toku nebo funkcí opravy chyb;
* jde o jednoduchý interfejs mezi protokoly vyšší vrstvy a IP protokolem,
* hlavička protokolu UDP obsahu menší množství informací než hlavička TCP a tím má tento protokol menší režii;
* protože UDP nemá žádné mechanismy pro dorozumívání se obou komunikujících stran je přenos rychlejší než v případě TCP.

Aplikace používající UDP jako přenosový protokol – např. SNMP, NFS, TFTP, protokoly pro VoIP (např. RTP), … Logika existence dvou transportních protokolů, které jsou vzájemně alternativní, je v tom že aplikace si mohou samy svobodně vybrat, který z nich chtějí používat. Například "klasické" počítačové aplikace, jako například přenos souborů, el. pošta atd., preferují zajištění spolehlivosti, a dávají přednost protokolu TCP. Naproti tomu novější multimediální aplikace dávají přednost spíše protokolu UDP, protože ten se nezdržuje zajišťováním spolehlivosti, a dokáže tak přenášet data rovnoměrněji a s menší prodlevou (latencí), než protokol TCP.

## Datagram

Je v [informatice](https://cs.wikipedia.org/wiki/Informatika) označení pro základní jednotku, která je přepravována v [počítačové síti](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) s [přepojováním paketů](https://cs.wikipedia.org/wiki/P%C5%99epojov%C3%A1n%C3%AD_paket%C5%AF), kde není zajištěno jejich doručení, zachování pořadí ani eliminace duplicity. Datagram obsahuje hlavičku, která nese služební informace (cíl, odesílatel a případně další řídící informace) a tělo, které obsahuje vlastní přenášená [data](https://cs.wikipedia.org/wiki/Data). Díky tomu není přeprava datagramů v takové síti závislá na předchozím stavu sítě nebo vlastním pohybu datagramu, což vede k zjednodušení řízení sítě i vlastního doručování dat.

Termín datagram je někdy chápán jako [synonymum](https://cs.wikipedia.org/wiki/Synonymum) s termínem [paket](https://cs.wikipedia.org/wiki/Paket), avšak jsou mezi nimi jemné rozdíly. Zatímco paket označuje obecná data přepravovaná v síti s přepojováním paketů, datagram obvykle označuje pakety související se službami, které neposkytují záruky ([IP datagram](https://cs.wikipedia.org/wiki/IP_datagram), [UDP](https://cs.wikipedia.org/wiki/UDP) datagram). V případě, kdy je IP datagram [fragmentován](https://cs.wikipedia.org/wiki/Fragmentace_(informatika)), označují se vzniklé [IP fragmenty](https://cs.wikipedia.org/wiki/IP_fragmentace) jako pakety.

Do výše uvedeného pravidla však nezapadá označení [TCP segment](https://cs.wikipedia.org/w/index.php?title=TCP_segment&action=edit&redlink=1), který označuje IP datagram nesoucí část souvislého toku dat přepravovaného pomocí [TCP](https://cs.wikipedia.org/wiki/TCP) protokolu, který poskytuje na přepravu záruky (záruka pro doručení, resp. vyřešení ztrát, zachování pořadí a odstranění duplicit).

Paket  
Označuje v [informatice](https://cs.wikipedia.org/wiki/Informatika) blok [dat](https://cs.wikipedia.org/wiki/Data) přenášený v [počítačových sítích](https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_s%C3%AD%C5%A5) založených na [přepojování paketů](https://cs.wikipedia.org/wiki/P%C5%99epojov%C3%A1n%C3%AD_paket%C5%AF), kde je možné přenášet data i při výpadcích některých spojů. Některé typy síťových spojů přenos paketů nepodporují (například tradiční telekomunikační linky typu bod-bod, [anglicky](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina) point-to-point) a data se v nich přenášejí jako proud [bajtů](https://cs.wikipedia.org/wiki/Byte), znaků nebo [bitů](https://cs.wikipedia.org/wiki/Bit).

Porty

Protokoly rodiny IP používají pro rozlišení jednotlivých počítačů IP adresy. Protokoly TCP a UDP navíc používají pro rozlišení jednotlivých služeb v rámci jednoho počítače (resp. jedné IP adresy) tzv. síťové porty. I když je zpravidla technicky možné nastavit pro službu libovolný port, byl z důvodu zjednodušení práce pro uživatele i správce služeb zřízen oficiální Seznam čísel portů TCP a UDP, který přiřazuje jednotlivým službám různých programů předem stanovená standardní čísla portů. Čísla portů přiděluje organizace ICANN.

Porty jsou rozděleny do tří skupin:

* **(dobře) známé porty (**[**anglicky**](https://cs.wikipedia.org/wiki/Angli%C4%8Dtina)**well known ports)** – porty v rozsahu 0 až 1023; vyhrazené pro nejběžnější služby
* **registrované porty** – v rozsahu 1024 až 49151, použití portu by se mělo registrovat u ICANN
* **dynamické a soukromé porty** – v rozsahu 49152 až 65535, vyhrazené pro dynamické přidělování a soukromé využití, nejsou pevně přiděleny žádné aplikaci

### Well-known porty

* **některé porty, mají definován význam**
  + udávají, jaká aplikace (služba) na daném portu pracuje
  + umožňují komunikaci s aplikací na vzdáleném serveru (pokud by byly porty náhodné, nevíme, kam se připojit)
* **well-known (dobře známé) porty: mají čísla 0-1023**
  + přiděluje ICANN
  + 20, 21 – FTP, 22 – SSH (secure shell), 23 – telnet,, 53 – DNS
  + 80 – HTTP (WWW), 110 – POP3 (vybírání pošty), 143 – IMAP
  + 443 – HTTPS (šifrovaný web), ...
* **registrované porty: mají čísla 1024 – 49151**
  + IANA nepřiděluje, pouze registruje použití (3306 – MySQL, 8080 - Apache Tomcat)
* **ostatní porty: 49152 – 65535**
  + volně k použití (např. pro klienty)

### Porovnejte strukturu TCP paketu s UDP. Vysvětlete výhody a nevýhody obou.

TCP paket má v sobě ještě Sekvenční číslo paketu,

### Popište aplikaci blokování určitého portu na firewallu routeru.

Na Firewallu si můžeme nastavit blokování/povolování jednotlivých portů. Služby, které tyto porty využívají, se nedostanou přes ke své aktivitě.

### Výpis Routovací tabulky

CMD -> route print