evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

PSK2-12

Název školy:	Vyšší odborná škola a Střední průmyslová škola, Božetěchova 3
Autor:	Ing. Marek Nožka
Anotace:	Protokoly transportní vrstvy
Vzdělávací oblast:	Informační a komunikační technologie
Předmět:	Počítačové sítě a komunikační technika (PSK)
Tematická oblast:	Vrstvy protokolu TCP/IP
Výsledky vzdělávání:	Žák popíše protokoly TCP a UDP a jejich vlastnosti
Klíčová slova:	TCP/IP, transportní vrstva, síťový port, TCP, UDP
Druh učebního materiálu:	Online vzdělávací materiál
Typ vzdělávání:	Střední vzdělávání, 3. ročník, technické lyceum
Ověřeno:	VOŠ a SPŠE Olomouc; Třída: 3L
Zdroj:	Vlastní poznámky, Wikipedia, Wikimedia Commons

Protokoly TCP a UDP

TCP a UDP jsou hlavní komunikační protokoly na Transportní vrsvě rodiny protokolů TCP/IP

Transportní vrstva umožňuje umožňuje adresovat přímo aplikace. K adresování aplikací se používá tzv. síťový port.

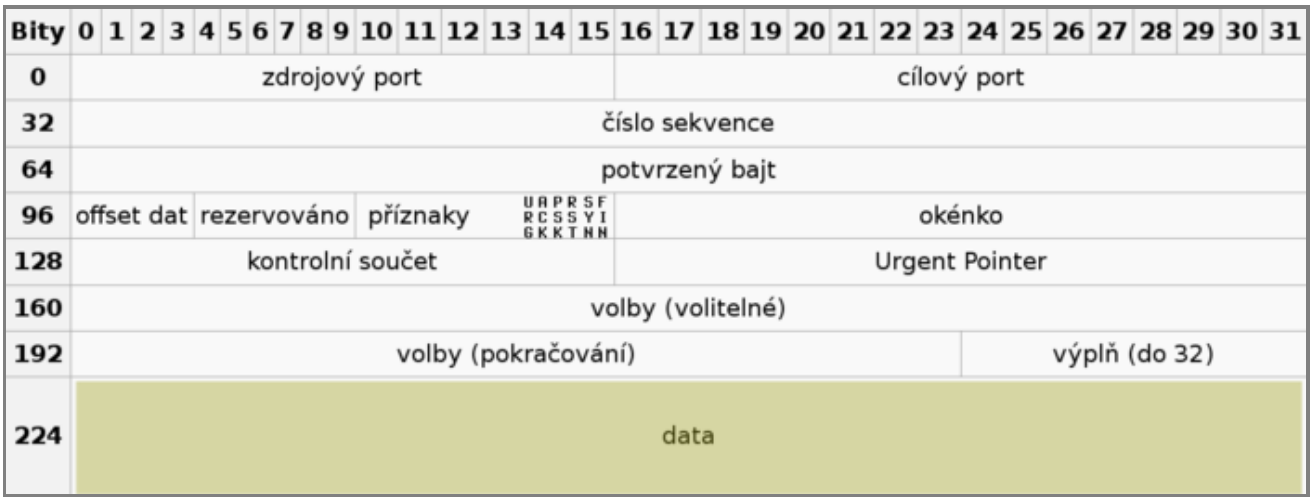
Transmission Control Protocol -- TCP

Použitím TCP mohou aplikace na počítačích propojených do sítě vytvořit mezi sebou spojení, přes které mohou přenášet data. Protokol garantuje spolehlivé doručování a doručování ve správném pořadí. TCP také rozlišuje data pro vícenásobné, současně běžící aplikace (například webový server a emailový server) běžící na stejném počítači.

TCP je tedy *spojově orientovaný* protokol pro přenos toku bajtů na transportní vrstvě se *spolehlivým doručováním*. Slovu *spolehlivý* musíme rozumět ve významu, že protokol jako takový garantuje doručení

všech dat (a to ve správném pořadí). To znamená, že protokol má své vlastí vnitřní mechanizmy, pomocí kterých zjistí jestli byla data správně doručena a případně zjedná nápravu.

Na obrázku vidíme TCP hlavičku.



Aplikace posílá proud (stream) 8-bitových bajtů TCP protokolu k doručení sítí. TCP rozděluje proud bajtů do přiměřeně velkých segmentů. TCP pak předá takto vzniklé pakety IP protokolu k přepravě internetem do TCP modulu na druhé straně TCP spojení. TCP ověří, že se pakety neztratily tím, že každému paketu přidělil pořadové číslo, které se také použije k ověření, že data byla přijata ve správném pořadí.

TCP modul na straně příjemce posílá zpět potvrzení pro pakety, které byly úspěšně přijaty. Pokud by se odesilateli potvrzení nevrátilo do rozumné doby, vypršel by odesilatelův časovač a data by vyslal znovu.

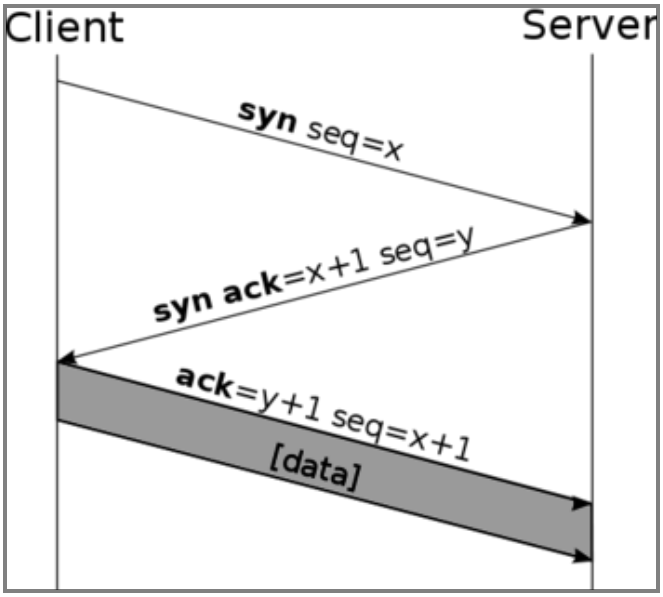
TCP protokol ověřuje, zda přenesená data nebyla poškozena šumem tím, že před odesláním spočítá kontrolní součet, uloží jej do odesílaného paketu a příjemce kontrolní součet vypočítá znovu a ověří, že se shodují.

Navázání TCP spojení

K navázání spojení slouží tzv. three-way handshake (trojí potřesení rukou). V průběhu navazování spojení se obě strany dohodnou na **číslu sekvence** a **potvrzovacím čísle**. Pro navázání spojení se odesílají datagramy s nastavenými příznaky SYN a ACK.

Jak z názvu vyplývá, navázání spojení probíhá ve třech krocích:

1. Klient odešle na server datagram s nastaveným příznakem SYN a *náhodně vygenerovaným* číslem sekvence (x), potvrzovací číslo=0.
2. Server odešle klientovi datagram s nastavenými příznaky SYN a ACK, potvrzovací číslo=x+1, číslo sekvence je *náhodně vygenerované* (y)
3. Klient odešle datagram s nastaveným příznakem ACK, číslo sekvence=x+1, číslo odpovědi=y+1.



Čísla se náhodně generují proto, aby se data do komunikace nemohl připlést žádný další zbloudilý (opožděný) paket z předchozího nebo jiného spojení.

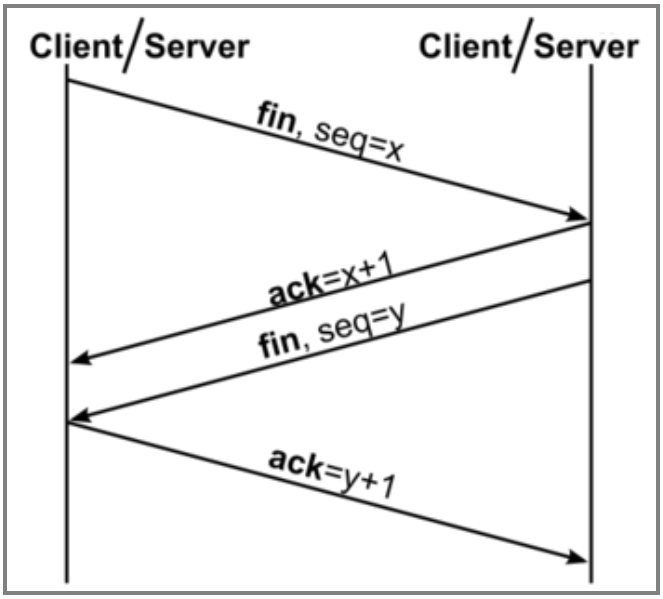
Obě strany si pamatují číslo sekvence své i protistrany. Používají se totiž i pro další komunikaci a určují pořadí paketů. Když úspěšně proběhne trojcestný handshaking, je spojení navázáno a zůstane tak až do ukončení spojení. To se může zneužít na SYN flood útok.

Ukončení spojení

Ukončení spojení probíhá podobně jako jeho navázání. Používá se k tomu příznaků FIN a ACK:

1. Klient odešle datagram s nastaveným příznakem FIN
2. Server odpoví datagramem s nastaveným příznakem ACK
3. Server odešle datagram s nastaveným příznakem FIN
4. Klient odpoví s nastaveným příznakem ACK

Teprve po těchto čtyřech krocích je spojení ukončeno.



User Datagram Protocol -- UDP

O protokolu UDP říkáme, že nedává záruky na datagramy, které přenáší mezi počítači v síti. Někdy je označován jako *nespolehlivý*, ale to je velmi zavádějící označení. Na rozdíl od protokolu TCP totiž nezaručuje, zda se přenášený datagram neztratí, zda se nezmění pořadí doručených datagramů nebo zda se některý datagram nedoručí vícekrát.

V sadě protokolů Internetu poskytuje UDP velmi jednoduché rozhraní mezi síťovou vrstvou pod a aplikační vrstvou nad. UDP neposkytuje žádné záruky doručení a odesilatelova UDP vrstva si u jednou už odeslaných zpráv neudržuje žádný stav. **UDP pouze přidává kontrolní součty a schopnost roztřiďovat UDP pakety mezi více aplikací běžících na stejném počítači.**

UDP hlavička:

+	bity 0 - 15	16 - 31
0	zdrojový port	cílový port
32	délka	kontrolní součet
64	data	

Protokol UDP je vhodný pro nasazení, které vyžaduje jednoduchost nebo pro aplikace pracující systémem otázka-odpověď (např. DNS, sdílení souborů v LAN). Jeho *bezstavovost* je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami datagramů a není vhodné, aby se ztrácel čas novým odesíláním (starých) nedoručených zpráv

Další související odkazy

- Seznam čísel portů TCP a UDP
- tcp spojení
- Jak unést TCP spojení
- Resetovací útoky na TCP spojení