

Architektura

- Počítačová síť, jako je např. založená na IP, představuje složitý systém
- Lze ji rozložit do několika vrstev
 - Zjednodušení implementace
 - Jednodušší k pochopení

- i-tá vrstva
 - využívá služeb i-1 vrstvy
 - poskytuje služby i+1 vrstvě
 - skrývá se složitost nižších úrovní
 - služby poskytované nižší úrovní jsou nezávislé na jejich implementaci

- Rozhraní definuje, jak lze využívat poskytované služby

- Mezi vrstvené modely patří
 - Zásobník protokolů TCP/IP
 - Model ISO/OSI

Zásobník protokolů TCP/IP

- 70-tých letech vyvinut DARPO
 - Referenční model ARPANetu
- Jde o množinu pravidel, která umožňují uzlům sítě spolu komunikovat

- Princip robustnosti
 - Konzervativní přístup k odesílání
 - Všechny odesílaná data striktně vyhovují normě
 - Liberální přístup k příjmu
 - Přijmou se jakákoliv data, která je možné interpretovat

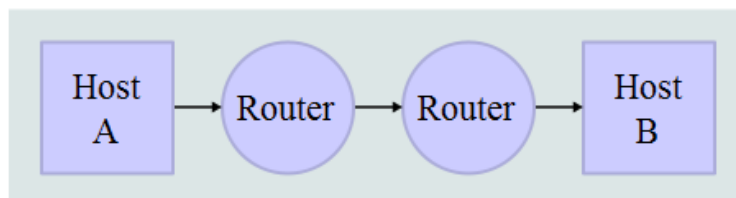
- Má čtyři vrstvy (řazeno od nejvyšší po nejnižší):
 - Aplikační
 - Transportní
 - Internetová
 - Linková

 - Čím vyšší vrstva, tím více je orientována na uživatelské aplikace (ne na uživatele)
 - Čím nižší vrstva, tím více je orientována na fyzický přenos dat

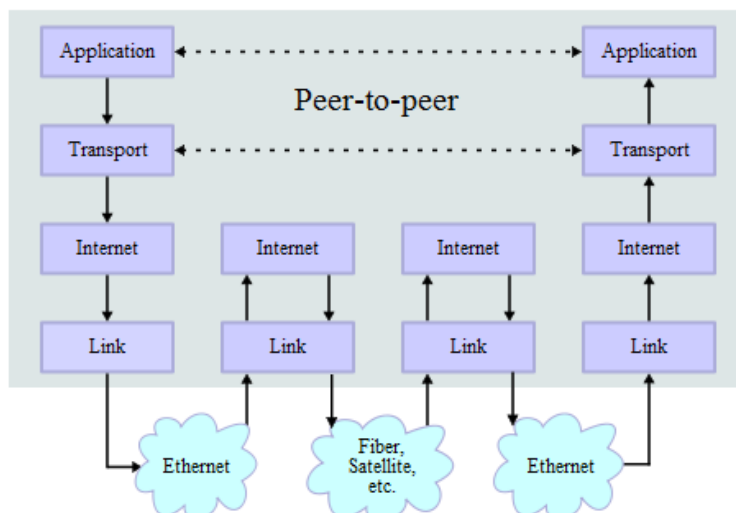
- Linková vrstva
 - Definuje přenos paketu mezi dvěma uzly po komunikačním médiu
 - Ethernet, Wi-Fi, ...
 - Ale i třeba přes VPN
 - Virtuální privátní síť

- Internetová vrstva
 - Definiuje přenos paketu přes několik uzlů
 - IP, ICMP, OSPF
 - U IP se zde provádí směrování
- Transportní vrstva
 - Definiuje přenos datových zpráv programů mezi dvěma uzly
 - Nespojovaný protokol UDP
 - Spojovaný protokol TCP
- Aplikační vrstva
 - Přenos datových zpráv, jejichž obsah je definován konkrétním programem (aplikací)
 - TCP, FTP, HTTP, NTP
 - Např. v případě využití TCP se řekne „doruč tento objem dat na tuto adresu“

Network Connections



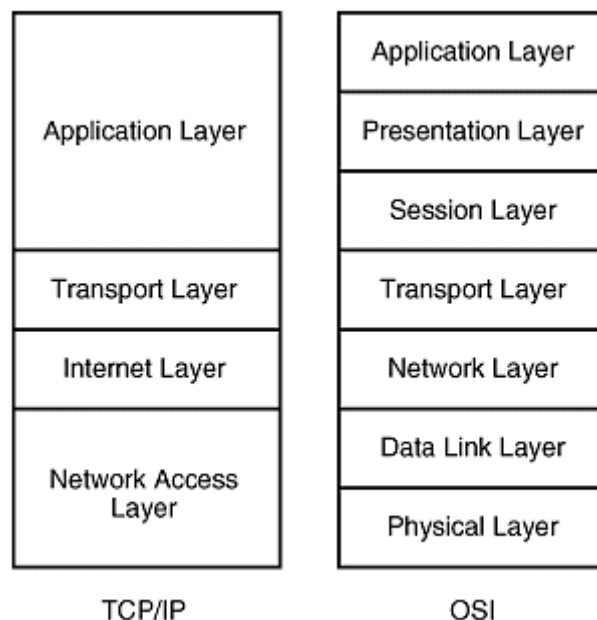
Stack Connections



http://en.wikipedia.org/wiki/TCP/IP_model

TCP/IP vs. ISO/OSI

- TCP/IP model má méně vrstev
- Vrstvy TCP/IP modelu lze namapovat na model ISO/OSI
 - Ačkoliv ne vždy zcela „čistě“
 - Např. tunelování (VPN)
 - Některé protokoly byly specifikovány s ohledem na zásobník TCP/IP
- Model TCP/IP upřednostňuje jednoduchost a snadnost implementace
- ISO/OSI není zamýšlen pouze pro IP protokoly
 - Ale i jeho alternativy, např. IPX fy Novell
- ISO/OSI je standard de-jure
- TCP/IP je standard de-facto



<http://www.adbh.co.uk/t171/tma4.php>

Model ISO/OSI

- V roce 1977 začal vývoj vrstveného modelu síťové architektury
 - International Organization for Standardization začala vyvíjet Open Systems Interconnection model
- OSI model se dělí na 2 části
 - Základní referenční model
 - Abstraktní popis vrstvené komunikace a síťových protokolů
 - 7-vrstvý model
- 7 vrstev – seřazeno od nejvyšší po nejnižší
 - Aplikační (Application)
 - Prezentační (Presentation)
 - Relační (Session)
 - Transportní (Transport)
 - Síťová (Network)
 - Linková (Data Link)
 - Fyzická (Physical)

1. Fyzická vrstva

- Přenos jednotlivých bitů po komunikačním médiu
- 100BASE-TX

2. Linková vrstva

- Komunikace mezi dvěma uzly připojenými ke stejnému komunikačnímu médiu
- Zajištění bezchybného přenosu dat
 - Detekce a případně oprava chyb z fyzické vrstvy
- Ethernet, Wi-Fi

3. Síťová vrstva

- Přenos paketů mezi uzly, které nemusí sdílet stejné komunikační médium
 - Tj. přenos paketu přes několik uzlů
- Adresování a směrování
- Mechanismy předcházení zahlcení sítě

- NetBIOS
 - Pro zajímavost, mimo rozsah KIV/ZPS
 - Zastaralý, nesměřovatelný protokol, který používal Microsoft (ale i např. Novell a IBM) až do Windows 2000 včetně
 - Do WXP lze doinstalovat oficiálně
 - Do WVista neoficiálně z WXP
 - Propojení počítačů ke sdílení souborů a tiskáren

4. Transportní vrstva

- Přenos datových zpráv programů mezi dvěma uzly
- Srovnání rychlosti vysílače a přijímače
- TCP, UDP

5. Relační vrstva

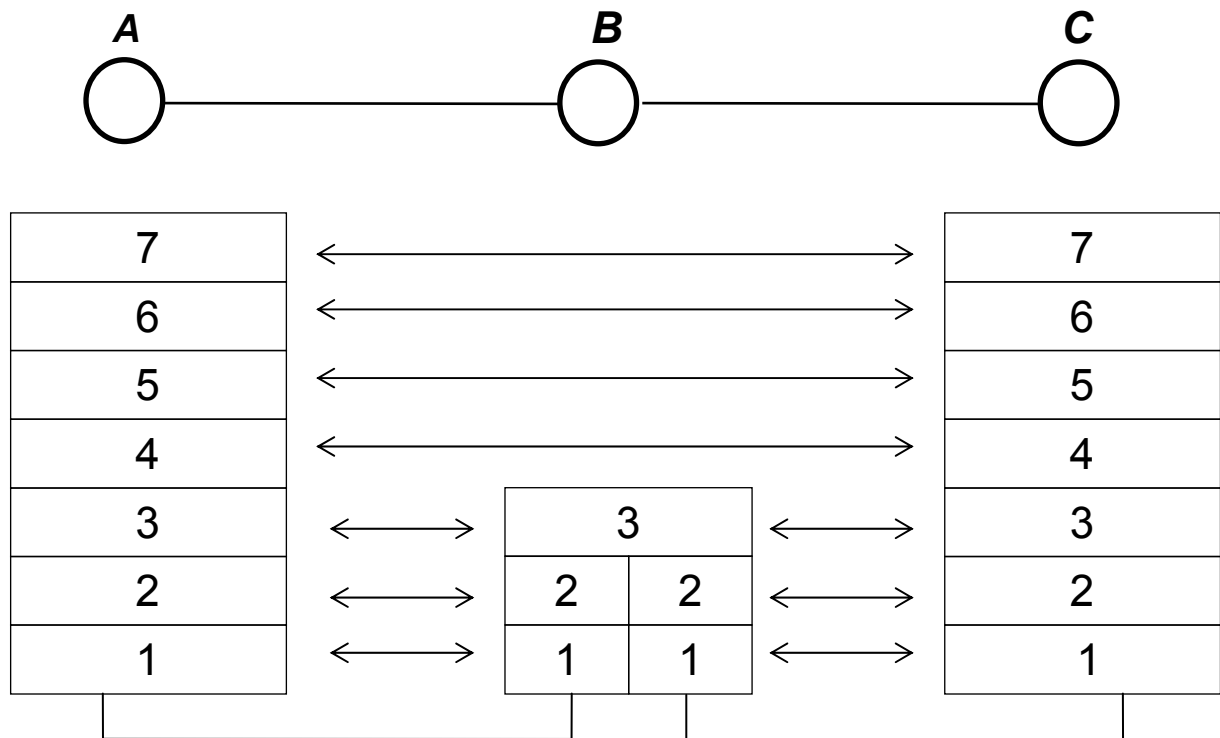
- Spojení komunikujících programů relací
 - Vytvoření, udržení, obnovení po chybě a ukončení relace
- RPC

6. Prezentační vrstva

- Společný formát dat, kterému rozumí komunikující programy
 - Kompresi a ochrana (šifrování) dat
- ASCII, SSL, TSL

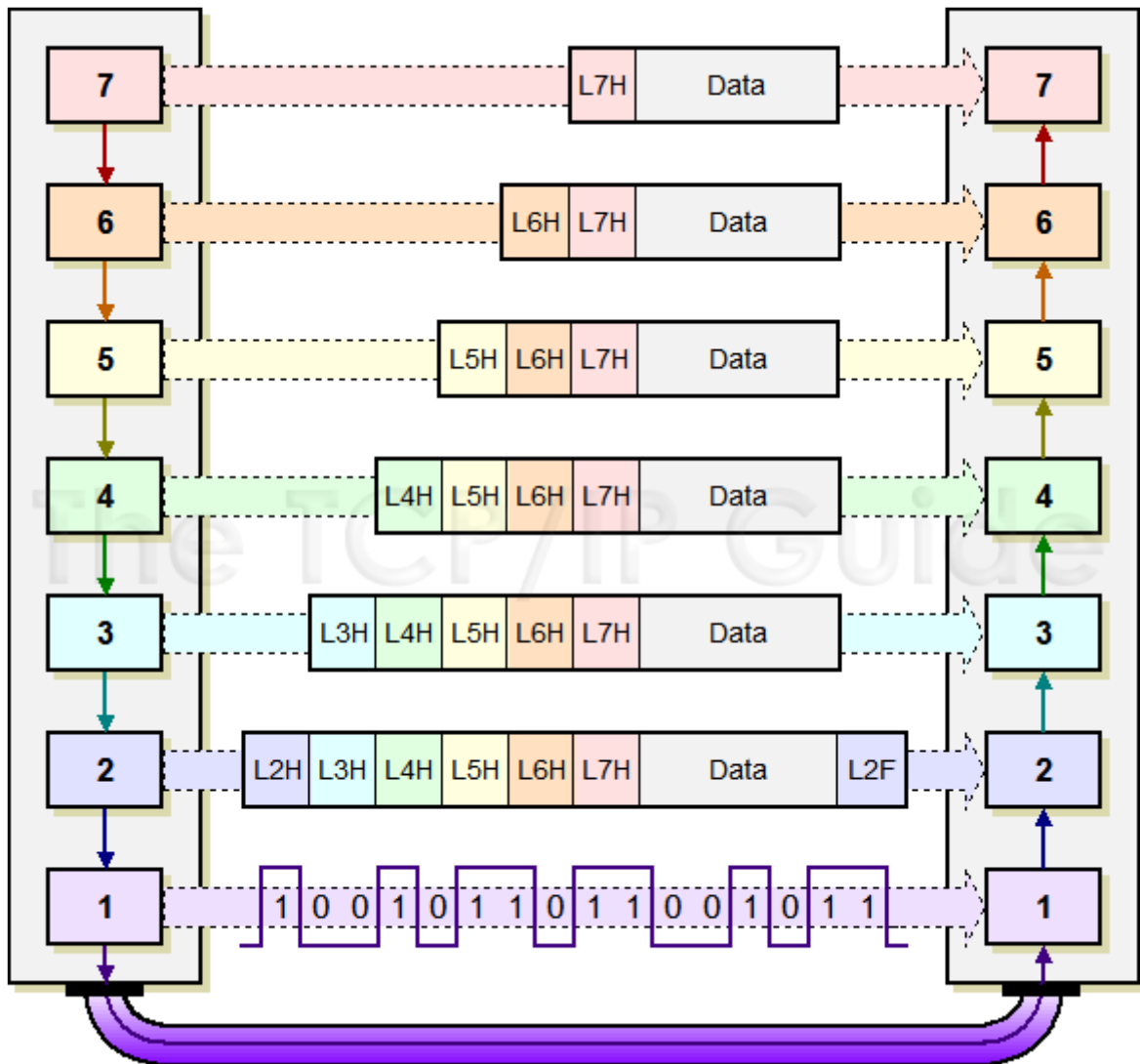
7. Aplikační vrstva

- Formátu přenášených dat už musejí rozumět jenom komunikující programy
- FTP, HTTP, HTTPS, NTP, DNS, SNMP, Telnet

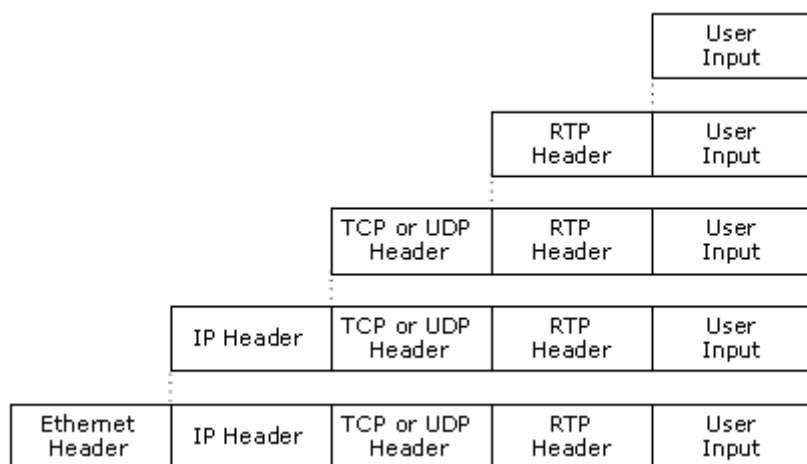


Zapouzdření protokolů

- Princip ruské bábušky
 - Nejmenší je datová zpráva programu
 - Každá další bábuška je větší hlavičku každé vrstvy, kterou projde
 - Poslední vrstva si přidá ještě patičku
 - Největší bábuška je např. Ethernet



http://www.tcpipguide.com/free/t_DataEncapsulationProtocolDataUnitsPDUsandServiceDa.htm

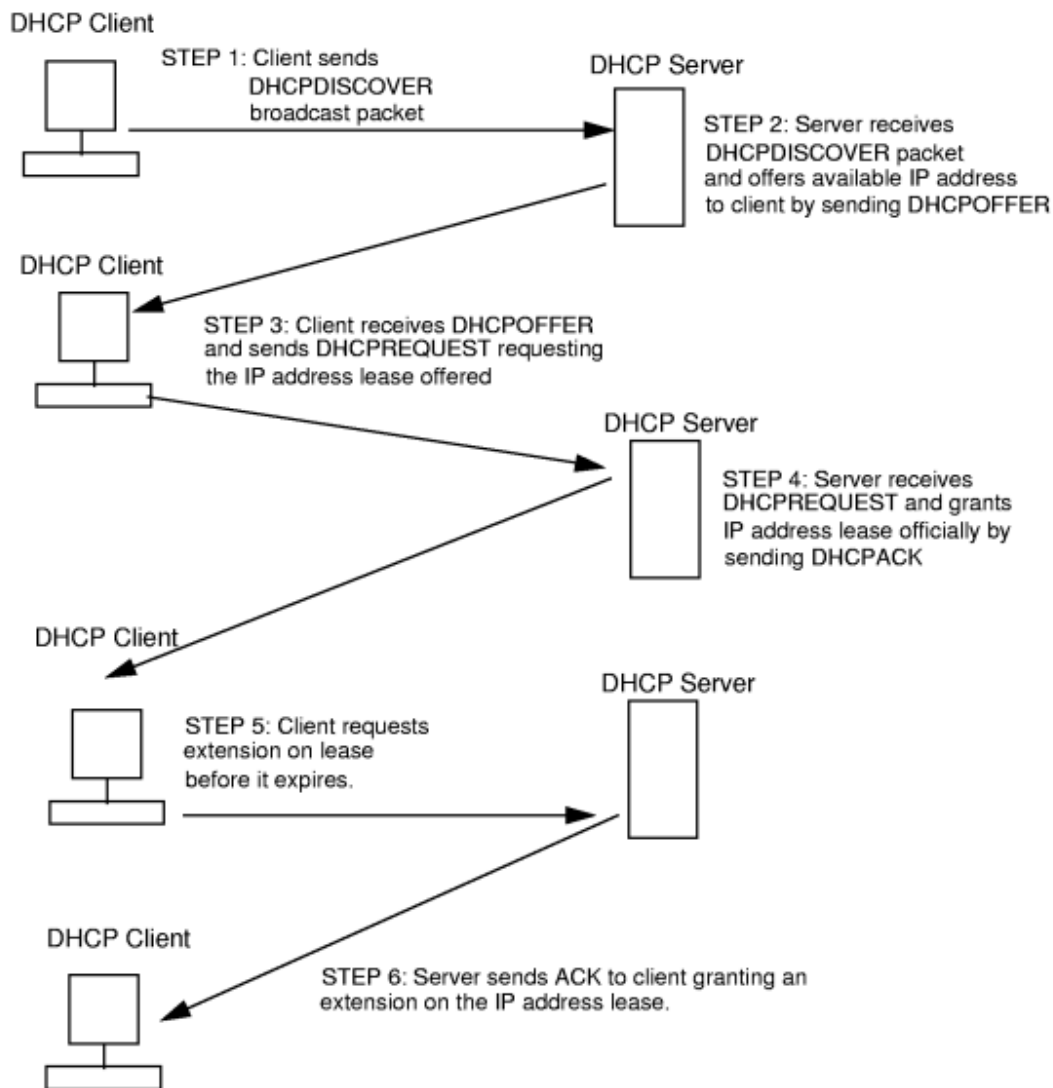


<http://technet.microsoft.com/en-us/library/bb457036.aspx>

Některé často používané protokoly

- R/ARP
 - Linková úroveň
 - Address Resolution Protocol
 - Převádí adresu síťové úrovně na adresu linkové úrovně
 - Nejčastěji převádí IPv4 adresu na MAC adresu
 - Pro IPv6 se používá Neighbor Discovery Protocol
 - Reverse Address Resolution Protocol
 - Převádí adresu linkové úrovně na adresu síťové úrovně
 - Např. MAC na IP
 - Byl nahrazen protokolem BOOTP a ten byl ještě později nahrazen protokolem DHCP
- DHCP
 - Používán pro nastavení síťových parametrů hostitele tak, aby mohl používat IP protokol
 - Typicky jeden server, ke kterému se svém startu připojují počítače a získají z něho
 - IP adresu
 - Adresy DNS serverů
 - Směrovací informace
 - Atd.
 - Nahrazuje BOOTP protokol, který umožňoval zavést operační systém ze sítě
 - Ač poskytuje služby linkové úrovně, používá i UDP

- Přidělování IP adres
 - Staticky
 - DHCP server má tabulku dvojic MAC-IP adres
 - Klient posílá svou MAC adresu
 - Server se podívá do tabulky a pošle odpovídající IP adresu
 - Dynamicky
 - DHCP server má k dispozici rozsah IP adres, ze kterého přidělí volnou adresu
 - Adresa má časově omezenou platnost
 - Tj. server adresu pronajme (lease)
 - Klient si musí včas požádat o prodloužení přidělené adresy, jinak ji server může přidělit někomu jinému
 - Některé implementace žádají po uplynutí polovin lhůty
 - Automaticky
 - Stejně jako dynamicky, ale server si vytváří tabulku dvojic MAC-IP adres
 - Je přidělena ta samá IP adresa i poté, co vypršel čas pronájmu
 - Pochopitelně, když není více počítačů než adres k dispozici
 - Např. když na noc vypnete počítač
 - Manuálně
 - Klient si sám nastaví svou IP adresu



<http://docs.hp.com/en/B2355-90685/ch06s02.html>

- Po zapnutí klient pošle broadcast (tj. všem uzlům) se zprávou pro DHCP server
- DHCP server odpoví a nabídne IP adresu
- Klient si vyžádá nabídnutou IP adresu
- Server ji přidělí
- Klient IP si zažádá o prodloužení platnosti IP adresy, než vyprší doba jejího pronájmu
- Server prodlouží pronájem
- Jako když sháníte pronájem ;-) (možná až na broadcast?)

- UDP
 - User Datagram Protocol
 - Transportní úroveň
 - Nespojově orientovaný protokol
 - Posílají se datagramy
 - Datagram má omezenou maximální velikost
 - Datagramy se mohou ztratit, dorazit v jiném pořadí, než ve kterém byly doručeny, jeden datagram může být doručen dvakrát
 - Na rozdíl od např. TCP tak má nižší režii
 - Díky nízké režii ho používá např. protokol NTP – zjišťování přesného času, nebo VoIP (Voice over IP)
 - Ale i on-line hry
 - Quake
 - World of Warcraft (používá TCP i UDP)

- TCP
 - Transmission Control Protocol
 - Transportní vrstva
 - Spojově orientovaný protokol
 - Neposílají se datagramy
 - Protokol představuje souvislý proud dat
 - Posílají se datové zprávy po navázaném spojení
 - Analogie s poštovním potrubím
 - Vkládám do něj zprávy pořád dál a na jeho konci vypadávají příjemci

 - Garantuje doručení všech zpráv v pořadí a počtu, v jakém byly odeslány
 - Vyžaduje kontrolní mechanismy, které způsobují větší režii protokolu, než má např. UDP
 - Používají ho DNS, HTTP, FTP, WoW, ...

- RPC
 - Pro zajímavost, mimo rozsah KIV/ZPS
 - Remote Procedure Call
 - Požadavek na spuštění programu na vzdáleném uzlu a předání výsledku zpět volajícímu
 - Způsob, jak se realizuje sdílení souborů a tiskáren
 - Např. vypiš obsah adresáře
 - Např. SMB (Server Message Block) ve Windows

- SNMP
 - Pro zajímavost, mimo rozsah KIV/ZPS
 - Simple Network Management Protocol
 - Umožňuje získat různé údaje o uzlech v síti, které se je rozhodly zveřejnit
 - IP adresy
 - Zatížení procesorů
 - Údaje o hardwaru
 - Různé statistiky jako je např. počet odeslaných bytů
 - Atd.

- Telnet
 - TELEcommunication NETwork
 - Dnes používá TCP
 - Původně používal NCP (Network Control Protocol)
 - Pro zajímavost
 - Většina aktivních síťových prvků a operačních systémů umožňuje svou administraci pomocí telnetu
 - Resp. OS dnes pomocí SSH, protože spojení telnetem není šifrováno

- Uživatel se připojí k uzlu, na kterém spouští programy
 - Tj. poskytuje vstup (klávesnice) vzdálenému počítači a zobrazuje se mu výstup vzdáleného počítače
- Lze ho také využít k tzv. Raw-TCP spojení
 - Některé protokoly jako SMTP, POP, nebo HTTP, mají lidsky čitelnou syntaxi
 - Lze je použít např. pro diagnostiku, aniž bych musel mít k dispozici speciální software zvládající daný protokol
- Konfigurace CISCO routeru
 - Zcela určitě mimo rozsah KIV/ZPS :-)

```
smerovac#config
smerovac(config)#interface ethernet 1/1
smerovac(config-if)#ip address
                        192.168.100.1 255.255.255.0
smerovac(config-if)#no shutdown
```

- Přístup k eryx.zcu.cz
 - Zcela určitě v rozsahu KIV/ZPS
 - Viz cvičení

```
eryx1> cd snmp
eryx1> ls -al
total 15
drwxr-xr-x  3 txkoutny users 2048 May 12 12:17 .
drwx----- 37   457717 users 4096 May 12 12:12 ..
drwxr-xr-x  7 txkoutny users 2048 May 12 12:27 lib
-rw-r--r--  1 txkoutny users  452 Mar 24  2007 makefile
-rw-r--r--  1 txkoutny users 5435 May 12 12:17 snmp.c
eryx1>
```

- IP, Ethernet
 - Viz dříve

- FTP, SCP, SFTP
 - Přenos souborů
 - Viz později

- SMTP, POP, IMAP
 - Poštovní protokoly
 - Viz poději

- NTP
 - Přenos a nastavování času
 - Viz později

- HTTP
 - Webové stránky
 - Viz později

- SSL, TSL, SSH
 - Bezpečnost, šifrování
 - Viz později

- RIP, OSPF, BGP
 - Směrovací protokoly
 - Viz později

- ICMP
 - Diagnostika sítě
 - Viz později