Aplikační vrstva TCP/IP

* V ISO modelu se jedná o tři vrstvy: Aplikační, Prezentační, Relační
* Aplikační vrstva
  + Je nejblíže k uživateli
  + Fungují na ní aplikace a mechanismy, které má smysl standardizovat (mechanismy elektronické pošty)
  + Poskytuje ucelené služby
* Prezentační
  + Transformuje data do tvaru, který používají aplikace (šifrování, konvertování, komprimace)
  + Zabývá se strukturou dat, ne jejich významem
* Relační
  + Udržuje relaci (session)
  + Uchovává informace mezi jednotlivými spojeními na úrovni transportní vrstvy

# Peer to Peer

* Síť, kde spolu komunikují přímo jednotlivý klienti
* Sdílení prostředků bez serveru
* Všechna zařízení mohou sloužit jako server i jako klient
* Gnutella, BitTorrent

# Klient-server

* Žadatel a poskytovatel
* Na serveru běží jedna či více služeb
* Klient inicializuje komunikační relaci se serverem, který čeká na příchozí požadavky (3-way handshake)
* Email (SMTP), web (HTTPS)

# Aplikace

* Každá služba nebo aplikace využívá nějaký port
* Well-known (vyhrazené pro nejběžnější služby) – 0 až 1023
* Registered (určitý protokol nebo aplikace) – 1024 až 49151
* Dynamic (Porty pro dočasnou krátkou komunikaci) – 49152 až 65535

# WEB

* port 80 – HTTP (Hypertext Transfer Protocol)
* Request-response protokol
* Přenos souborů (HTML, CSS, Javascript)
* URL převedena pomocí DNS na IP serveru s požadovaným souborem
* Vrátí data nebo response status code
* 443 – HTTPS – zašifrované HTTP (využití TSL k zašifrování)

# Email

* Klienti komunikují se serverem kvůli odesílání a přijímání e-mailů
* Servery komunikují mezi sebou kvůli odesílání mezi různými e-mailovými doménami
* 25 – SMTP – Simple Mail Transfer Protocol
  + Pomocí mailového klienta je odeslán email na server
  + Server přijme zprávu
  + Pokud je určena systému, na kterém běží, odešle ji lokálně
  + Jinak ji odešle na jiný příslušný emailový server (DNS)
* 110 – POP3 – Post Office Protocol
  + Načítání pošty z webového serveru
  + Server na vyžádání odešle zprávu klientovi, a pak ji ze serveru smaže
  + Žádné centralizované místo, kde jsou e-maily uchovány
* 143 – IMAP – Internet Message Access Protocol
  + Narozdíl od POP3 si klient stahuje kopie zpráv a originál zůstane na serveru
  + Když klient zprávu smaže, server se sesynchronizuje a také ji smaže

# DHCP

* Klient komunikuje na portu 68, server poslouchá na portu 67
* Protokol, který koncovým zařízením v síti automaticky přiřazuje IP adresu, masku, default gateway a adresu DNS serveru
* Discover→ Offer → Request →ACK
* DHCP Relay – server se nachází mimo lokální síť (přeposílání DHCP zpráv mimo do jiné síťě)
* V případě neúspěšného přiřazení dostane zařízení dočasnou adresu 164.254.x.x

# NAT – Network Address Translation

* Překládá adresy (většinou) z privátního do veřejného bloku
* Privátní adresy:
  + 10.0.0.0/8
  + 172.16.0.0/12
  + 192.168.0.0/16
* Šetří počet veřejných adres
* Možnost znovuužití privátních adres
* Bezpečnost
* Na druhou stranu zpoždění při převodu adres, porušení síťové vrstvy (router sahá na porty, které jsou v transportní vrstvě)
* Static NAT – jedna privátní adresa má jednu veřejnou (web hosting)
* Dynamic NAT – privátní adresa je převedena na jednu veřejnou adresu z poolu
* PAT (NAT overload) – více privátních adres má jednu veřejnou adresu (rozlišení pomocí portů), nejčastější řešení
* Port-forwarding – uveřejní porty, na kterých běží webové služby

# DNS (Domain Name System)

* Port 53
* FQDN - Fully Qualified Domain Name (úplné doménové jméno, kterým lze na internetu jednoznačně identifikovat server) - classroom.google.com
* DNS – překládá URL na adresu příslušného serveru
* Top level domain – cz, com, eu
* Second level domain – doména druhého řádu – [www.shop.**example**.com](http://www.shop.example.com)
* Autoritativní odpověď – odpověď DNS serveru, která byla získána přímo, bez prostředníka

# FTP (File Transfer Protocol)

* 20 přenos dat
* 21 – přenos souborů
* TCP
* poskytuje autentifikaci

# SMB (Server Message Block)

* 445
* protokol, který slouží ke sdíleném přístup k souborům, tiskárnám,…
* Hlavně Windows, Linux má Sambu

# NFS (Network File System)

* Vzdálený přístup k souborům

# TFTP (Trivial File Transfer Protocol)

* 69
* UDP
* bez autentifikace či konfigurace

# NTP (Network Time Protocol)

* 123
* Synchronizace vnitřních hodin PC

# Telnet – Teletype Network

* 23
* Připojení ke vzdálenému PC pomocí textového UI – virtuální terminál
* Nešifrovaná komunikace – přechod na SSH

# SSH – Secure Shell

* 22
* Šifrovaná náhrada za Telnet