

# Počítačové sítě

ÚVOD DO ICT, 2. PROSINCE 2024



# Čtyři vrstvy modelu TCP/IP

## 1. Vrstva síťového rozhraní

- Umožňuje přístup k fyzickému přenosovému médiu.
- Ethernet
- Síťová vrstva
  - „Posílčec“. Zajišťuje adresaci, směrování a předávání *datagramů*.
  - Protokol IP
- Transportní vrstva
  - Koncové body transportu – odeslání a doručení
  - Protokoly TCP (spolehlivý) a UDP (nespolehlivý)
- Aplikační vrstva
  - Např. HTTP(S) pro přenos webových stránek

# Ethernet

- Jednoznačně nejrozšířenější technologie síťového přenosu
  - S jinými se lze potkat jedině snad v IT muzeu (viz např. [ALOHAnet](#))
- Historicky koncipováno jako „vysílání do éteru“
  - Zprávy se v rámci sdíleného média vysílaly všesměrově, pro všechna PC
  - Příjemce kontroloval, zda je zpráva pro něj, pokud ano, přijal ji
- Sdílené médium
  - Dříve koaxiální kabel, rychlost do 10 Mb/s
  - Dnes kroucený kabel s koncovkou RJ45, rychlost až 40 Gb/s
  - A zároveň také bezdrátová [WiFi](#), ve verzi 6 (802.11ax) až 9,6 Gb/s
- MAC adresa
  - Jedinečný identifikátor síťové karty (drátové i bezdrátové)

# Wi-Fi

- Bezdrátové „rozšíření“ Ethernetu
  - Koncipováno pro připojení digitálních zařízení v rámci „domu“
  - Používá(-alo) se však i pro připojení domů k internetu (ve vesnicích)
- Využívá celosvětově harmonizovaná bezlicenční pásma
  - 2,4 GHz – 11 až 14 kanálů (3 nepřekrývající), větší vzdálenost, menší rychlost
  - 5 GHz – 23 nepřekrývajících se kanálů, menší vzdálenost, větší rychlost
    - Neplést s [5G](#) pro mobilní sítě!
- Důležité zkratky
  - SSID – identifikátor bezdrátové sítě, síť by jej měla pravidelně vysílat
  - WEP, WPA, WPA2 – metody šifrování přenášených dat v síti

# Protokol IP

- Jednoduchá přenosová služba pro přenos datagramů
  - Tj. dat v obálce, s adresou odesílatele a příjemce
- Nespolehlivá
  - Pokud ztratí data, nemusí to řešit
- IP-adresa (IPv4)
  - Čtyři čísla v rozsahu 0–255 oddělená tečkou, např. 192.168.14.207
  - První část IP-adresy představuje „adresu sítě“
  - Druhá (zbývající) část IP-adresy představuje „adresu koncového zařízení“
  - Dělitelem těchto adres je tzv. maska sítě, např. 255.255.255.0
- IPv6
  - Novější verze protokolu s větším počtem adres a lepšími možnostmi

# Protokoly TCP a UDP

- Zajišťují spojení mezi koncovými body (aplikacemi)
- Aplikace rozlišují pomocí portů
- TCP (Transmission Control Protocol)
  - Ručí za spolehlivý přenos dat
  - Doručí všechna data ve správném pořadí
  - Je zapotřebí spojení navázat a následně ukončit
- UDP (User Datagram Protocol)
  - Bez záruky doručení, prostě se jen vysílá (např. jak TV vysílání)
  - Nenavazuje ani neukončuje spojení
  - Nemá tak velkou režii, je proto rychlejší

# Aplikační protokoly

- Správa sítě
  - DNS (překlad domén na IP-adresy), DHCP (přidělování IP-adres)
- E-mail
  - SMTP (odesílání), IMAP (čtení na serveru), POP3 (stahování zpráv)
- Web
  - HTTP, HTTPS (webové stránky), WebDAV (rozšíření HTTP o práci se soubory)
- Soubory
  - NFS (síťový systém), SMB (sdílení ve Windows), FTP (přenos souborů)
- Jiné
  - SSH (zabezpečený vzdálený terminál i přenos souborů), NTP (synchronizace času), SSL/TSL (šifrování spojení)

# Útoky na síti

- Odposlechy
  - V rámci lokální sítě je možné monitorovat, co se kde „šustne“
- Vetření se do spojení (man-in-the-middle)
  - Vetřelec předstírá před klientem, že je server a před serverem, že je klient
  - Probíhající komunikaci přeposílá na obě strany a může do ní vstupovat
- Denial of Service (DoS)
  - Snaha o zahlcení systému zasíláním příliš mnoha požadavků
  - Varianta DDoS zahlcuje požadavky z vícero stran najednou
- Lámání hesel
  - S pomocí speciálních programů



# Firewall

- Pravidla, co smí dovnitř a co ven
- Filtrování paketů (= balíčku dat)
  - Stanoví se, ze které adresy a portu smí přicházet požadavky (a případně kam)
- Aplikační brány
  - Působí jako prostředník v komunikaci, kterou může ovlivňovat
  - Stejný princip jako man-in-the-middle, tentokrát ale pod kontrolou správce
- Stavové filtry
  - Dočasně si ukládají informace o probíhajících spojeních, které pomáhají při rozhodování o korektnosti
  - Pokročilé verze zkoumají i hlavičky aplikačních protokolů, zda jsou korektní

# Další síťové technologie

- NAT – Network Address Translation
  - Překlad adres z jedné sítě do druhé
  - Používají prakticky veškeré domácnosti – síť 192.168.x.x
- VPN – Virtual Private Network
  - Vzdálený počítač připojí do „lokální sítě“ zašifrovaným „tunelem“
  - Vzdálený počítač získá virtuální síťovou kartu a IP-adresu z rozsahu sítě, do které se připojí
- Proxy-server
  - Prostředník v komunikaci
  - Může filtrovat provoz, „kešovat“ obsah, obcházet regionální filtry apod.

# Praktická ukázka

- Možnosti nastavení domácí sítě
  - Router
    - IP-adresa zařízení
    - Brána
    - DNS server
  - WiFi
    - SSID
    - Kanál
    - Forma zabezpečení
  - Jiné
- <https://demoui.asus.com/>
- [https://emulator.tp-link.com/TL-WR841ND\\_V8/Index.htm](https://emulator.tp-link.com/TL-WR841ND_V8/Index.htm)