4. Základy síťové komunikace, ISO/OSI a TCP/IP model, síťové protokoly, síťové standardy (ethernet, fastethernet, gigabitethernet), bezdrátové technologie (standardy 802.11, WIFI přístupové body, technologie bluetooth)

ISO/OSI a TCP/IP model

- **MODEL ISO/OSI**
  - Teoretický model
  - ISO – vytváří standardy, organizace pro standardy
  - OSI – otevřený systém
  - 7 vrstev – každá vyšší vrstva je složitější
    - 7 Aplikační – data – zabývá se zpracováním dat
      - Umožňuje aplikacím na obou stranách přenosu spolupracovat
      - Síťové aplikace
    - 6 Prezenční – data – zabývá se zpracováním dat
      - Kódování (převod z 1 formy do 2.)
      - Komprese (kódování, ale za účelem rychlejšího a snazšího přenosu)
      - Šifrování (kódování, ale za účelem zabezpečení)
    - 5 Relační – data – zabývá se zpracováním dat
      - Zajišťuje a synchronizuje přeno mezi relačními vrstvami obou stran
      - Vytváří a ukončuje relaci
      - Účastníci si skáčou do „řeči“
    - 4 Transportní – segmenty – spojka mezi vrstvami
      - Funkce:
        - Zajišťuje komunikaci mezi příjemcem a odesílatelem
        - Skládá a rozkládá zprávu do segmentu
        - Obsahuje údaje o cílovém portu, čímž je umožněno více současných přenosů, port = identifikátor procesu
        - Z nespolehlivých služeb vytváří spolehlivé a z nespojovaných služby spojované
        - Segmenty = skupina seřazených paketů
        - Transportní vrstva může komunikovat s každou vrstvou, jiné nikoliv
    - 3 Síťová – pakety – zabývá se fyz. přenosem
      - Funkce – zajišťuje přenos dat mezi uzly bez přímého spojení, tzn. mezi oddělenými sítěmi
      - Provádí směrování (routing) = hledání cesty v sítích
      - Pracuje spolehlivě (= všechny pakety stejnou trasou a ta je předem vytyčena) a nespolehlivě (= každý paket jde jinou cestou)
      - Na úrovni Internetu
      - Router – složitější, důležitější než switch

        - 2 Linková – rámce – zabývá se fyz. přenosem
            - Organizuje bity do rámců (adresa odesílatele/příjemce, flag – oddělení rámců, CRC – bezpečnostní kód)
            - Obsahuje MAC adresu zdroj. a cílového zařízení v síti LAN
            - LLS – vytváření rámců
            - Zajišťuje přenos rámců v oblasti lokální sítě
                - Tvoří intranet, komunikace na úrovni intranetu, vnitřní síť
            - Switch (pracuje s rámci; vytvoří si tabulku, kdo má zapsané MAC adresy), bridge
        - 1 Fyzická – bity – zabývá se fyz. přenosem
            - Funkce:
                - Modulace (A/D D/A převodníky)
                - Navazování a ukončování spojení s komunikačním médiem
                - synchronizace a časování bitů
            - Repeater, hub
- **ARCHITEKTURA TCP/IP**
    - 4 vrstvy
        - 4 Aplikační vrstva
            - Zajišťuje koncové zobrazení dat uživateli spolu s kódováním
        - 3 Transportní vrstva
            - Zajišťuje komunikace vzdálených zařízení napříč sítí a spolehlivý přenos dat
        - 2 Síťová vrstva (Network)
            - Zajišťuje nejlepší cestu dat k cíli
            - Spolehlivost = zpětná vazba
            - Vnější síť a dál
        - 1 Vrstva síť. rozhraní (Network Interface)
            - Zajišťuje přístup dat na síť, kontroluje zařízení a síťová média v síti
            - Využívá existující technologii – např. Ethernet
            - Vše, co se rozum LAN síť (přenos dat, HW)
            - Pasiv. / Aktiv.

SÍŤOVÉ PROTOKOLY

- TCP/IP protokoly
- **L2:**
    - RIP (Routing Information Protocol) – pomocí něho se směruje
        - Tolik se nepoužívá
        - Max. 20 hopů
        - Microsoft
    - OSPF
        - Omezen hopama
        - Náročný na konfiguraci
    - IP (Internet Protocol)
        - Identifikátor PC sítě
        - IPv4 x IPv6
        - Důležitý protokol
        - Adresování a identifikování serverů
    - ARP (Adress Resolution Protocol)
        - Propojuje identifikátory sítí – IP adresy s MAC adresy
    - ICMP
        - Příkaz PING – zjištění konektivity
    - IGMP (Internet Group Management)
- **L3:**
    - TCP vs. UDP
        - Spolehlivý vs. Nespolehlivý (u UDP nedostaneme zprávu o tom, že došla data)
        - Spojovaný vs. Nespojovaný
        - Pomalý vs. Rychlý
        - Zabezpečení vs. Hodí se tam, kde není potřeba spolehlivost
- **L4:**
    - NTP (Network Time Protocol) – PORT 123
        - Synchronizace vnitřních hodin PC po paketové síti s proměnným zpožděním
        - Zajištění stejného a přesného času pro všechny PC v síti
    - DNS (Domain Name Systém) – PORT 53
        - Vzájemná překlad domén a IP adres
        - XXX.XXX.XXX.XXX -> www.---.com
    - DHCP (Dynamic Host Configuration Protocol) – PORT 67
        - Automatické přidělování IP adres
        - Řády domén, FQDN (Full Qualified Domain Name) -> řetězec.přípona
            - 1. řád = TLD (Top Level Domain): .cz
            - 2. řád: něco.cz
            - 3. řád: www.něco.cz

- SSH (Secure Shell) – PORT 22
  - Zabezpečený komunikační protokol v PC síti
  - Vzdálený přístup skrze terminál
- NFS (Network File System) – PORT 2049
  - Vzdálený přístup k souborům přes PC síť
- HTTP (Hypertext Transfer Protocol) – PORT 80
  - Komunikace s www serverů
  - Přenos hypertext. Dokumentů ve formátu HTML, XML, …
- HTTPS (HTTP Secure) – PORT 443
  - Komunikace web. prohlížeče s web. serverem
  - Zajištění autentizace, důvěrnosti přenášených dat a jejich integritu
  - Víc safe než http
- FTP (File Transfer Protocol) – PORT 21 & 20; FTPS – šifrovaný
  - přenos souborů mezi PC pomocí PC sítě
  - může být používán nezávisle na použitém OS
  - FTP nešifrovaný, nedoporučuje se
  - Data podle módu
    - Passive
      - Dotazy a odpovědi – port 21
      - Data – dohodnutý vysoký port, např. 2024
        - Server má nakonfigurovaný rozsah portů pro data a sdělí klientovi port pro data
      - Může mít problém s překladem adres na routeru
    - Active – port 20 nebo 989
      - Dotazy a odpovědi – port 21
      - Data – port 20

- **Mailové:**
  - SMTP(s) (Simple Mail Transfer Protocol; (s) = šif□) – PORT 25; šif□465, 587
    - Přenos zpráv el. pošty mezi přepravci el. pošty
    - Odesílání z klienta, posílá mezi servery
  - POP3(s) (Post Office Protocol; (s) = šif□) – PORT 110; šif□995
    - Stahování e-mail. zpráv ze vzdál. serveru klienta
    - Příjem do office klienta
  - IMAP(s) (Internet Message Access Protocol; (s) = šif□) – PORT 143; šif□993
    - Umožnění přístupu k emailu odkudkoli z libovolného zařízení
    - Vzdálený přístup k emailové schránce prostřednictvím email. Klienta
    - Transparentní pohled na schránku na serveru

SÍŤOVÉ STANDARDY

- **Ethernet**
  - Souhrn technologií pro sítě LAN, WAN
  - Standard IEEE 802.3, propojuje různá zařízení
  - Stal se dominantní technologií pro drát. sítě
    - Kroucená dvojlinka, koax, optika
  - Výhody:
    - Snadné zavedení, údržba, snaha přizpůsobovat se novým technologiím
    - Spolehlivost, nízká cena
    - Je schopný přenášet odlišnými rychlostmi od Mbit/s po Gbit/s
- **Ethernet a CSMA/CD**
  - Funguje na síťovém rozhraní architektury TCP/IP
  - Pro přístup na sdílené médium používá CSMA/CD, detekuje vysílání včetně kolizí
    - Carrier Sense Multiple Access with Collision Detection
  - Princip CSMA/CD
    - Naslouchá, zda je médium volné
    - Zahájí vysílání a současně naslouchá pomocí signálu JAM
    - V případě, že zachytí signál kolizi, celý proces se opakuje
- **Standardy**
  - 10Mbit Ethernet
    - 10BASE5 (10Mbit/s; základ. pásmo; impedance 50ohm) – tlustý koax/ethernet
    - 10BASE2 – tenký koax/ethernet
    - 10BASE-T – kroucená dvojlinka cat3 (pouze 2 páry vodičů)
  - 100Mbit Ethernet
    - 100BASE-TX – 100Mbit/s ethernet označován jako Fast Ethernet (2 páry UTP, STP cat5)
    - 100BASE-T2/T4 – UTP cat 3, 4, 5 (T2 – 2páry, T4 – 4 páry)
    - 100BASE-FX – Fast ethernet pomocí opt. vláken
  - **1000Mbit Ethernet**
    - 1000BASE-T – Gbitový ethernet, 4 páry vodičů UTP cat5e
  - **10Gbit Ethernet**
    - 10GBASE-T – Gbitový ethernet, UTP cat6e, cat7

BEZDRÁTOVÉ TECHNOLOGIE

- **Bezdrátová komunikace**
  - Nositelem informace je atmosféra a nosičem je signál
  - Nosné médium
    - Opt. komunikace (infrared spoje, světel. paprsek, IrDA, Ronja) – rámce
    - Rádiová komunikace/mikrovln. spoje (vysílačky, TV přenos, periferie PC, WiFi, WiMax)
    - Sonická komunikace (ultrazvuk ponorky)
- **Standard IEEE 802.11**
  - Standardem pro WiFi, Wireless LAN
  - Komunikace je zajišťována na linkové vrstvě
    - Přenáší zapouzdřené ethernetové rámce, využívá CSMA/CA
      - CSMA/CA zabraňuje kolizím
  - Standard zahrnuje:
    - Jsou značena písmenem
    - Druh modulace (překódování)
    - Přenos. pásmo
    - Max. přenos. rychlost
    - Rok vydání
- **Licencované přenosové pásmo**
  - Rádiové vysílání může být ovlivněno vodou, objekty či jiným zařízením
  - Vysílání probíhá na určité frekvenci a jejich počet (frekvencí) je omezen
  - Stát pronajímá přenosová pásma
  - U nás zastřešuje český telekomunikační úřad
  - Komerčně nevyužitá pásma – 2,4 a 5 GHz
- **Bezlicenční pásma**
  - 2,4 GHz
    - Nižší přenosová rychlost
    - Lepší propustnost
    - Má větší tendenci se zarušovat
    - Děleno na kanály
  - 5 GHz
    - Vyšší přenosová rychlost
    - Horší propustnost
- **WiFi kanály**
  - IEEE dělá pásma do kanálu podobně jako u TV vysílání
  - V ČR je jich 13
  - Ideální rozdělení je 1, 7, 13

- **Metody přístupu**
  - Ovlivňuje přenosovou rychlost daného standardu
  - CSMA/CA (… with Collision Avoidance)
    - oproti CSMA/CD nezjišťuje vznik kolizí, ale zabraňuje jim
  - Průběh
    - Naslouchá
    - Využívá RTS (Request To Send – dotaz na vysílání) a CTS (Clear To Send – volno k vysílání)
- **Registrace do WiFi**
  - Identifikátor SSID (Serive Set Identifier) fungující jako broadcst
  - Ad-hoc sítě – spojení 2 si rovných klientů (peer-to-peer)
  - Infrastrukturní sítě
    - Obsahuje 1 nebo více přístupových bodů (AP – Access Point), které vysílají SSID
- **Zabezpečení WiFi**
  - Zablokování SSID
  - Kontrola MAC adres klientů (blacklist & whitelist)
  - Šifrování (WEP, WPA, WPA2, WPA3)
    - Autorizace probíhá v šifrované formě pomocí klíčů
    - Dnes používáno WPA2, WPA3
  - Pojmy
    - Šifrování = zabezpečení přenášených dat před odposlechem
    - Autorizace = řízení přístupu oprávněných uživatelů
- **Bluetooth – IEEE 802.15**
  - Bezdrátová rádiová technologie určená pro nasazení na krátkou vzdálenost (PAN)
  - Bezlicenční pásmo 2,4 GHz
  - Rozděleno na 79 frekvenčních kanálů o šířce 1MHz
  - FHSS (Frequency Hopping Spread Spectrum) => (1600 přeskoků/sekunudu)
  - Point to point, point to multiple
- **Architektura Bluetooth**
  - Piconet
    - Nejmenší síť – soustava uzlů, které se sjednotily na stejné posloupnosti přeskakování frekvencí
    - Uzel v roli Master určuje posloupnost přeskoků
    - Max 7 uzlů a jeden Slave
  - Scatternet
    - Propojení více piconetů
- **Bluetooth – komunikace**
  - Fáze:
    - 1. párování (výměna klíčů, šifrování, autentizace)
    - 2. navázání spojení (rozhodnutí kdo je Master, kdo je Slave)
    - Výměna dat (skutečná výměna dat včetně profilu)

- **Bluetooth**
    - Class: udává výkon a dosah
    - Verze: BT 4.0, 5.0, 5.2
        - Snaha zvýšit přenosovou rychlost a snížit energetickou náročnost
    - Profily:
        - Každý profil definuje 1 činnost
        - Celkem 36, SYNCH, VDP, …
- **WPA (Wifi Protected Access)**
    - Vznikl jako rychlá náhrada za WEP, 256bit klíč
    - Využívá TKIP (Temporal Key Integrity Protocol)
        - Klíče jsou dynamicky měněný
        - Každý paket používá jiný klíč
    - WPA bylo překonáno a nahrazeno WPA2, WPA3
        - WPA2 – nahradilo TKIP protokolem CCMD a šifr. algoritmem AES