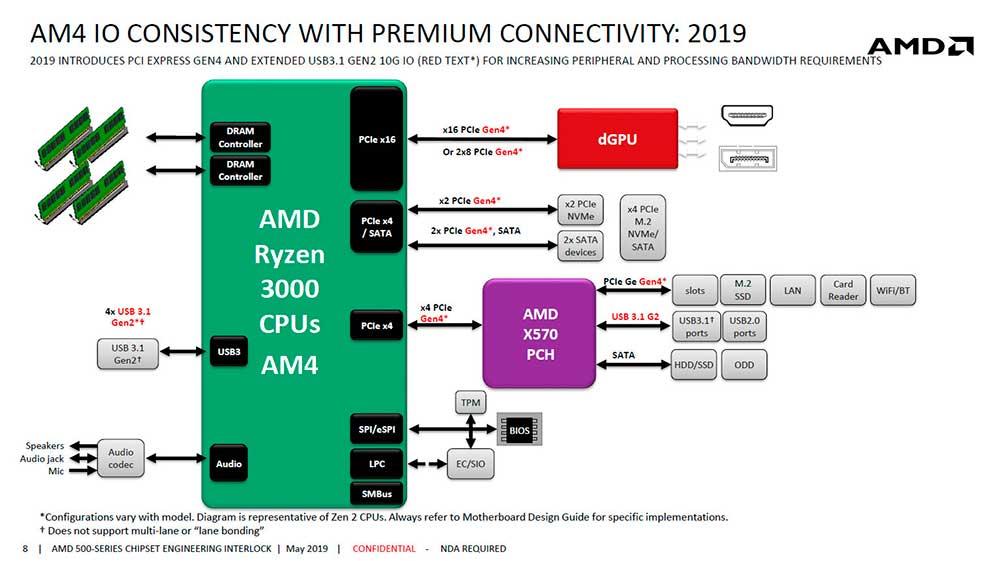
Počítač – základní části počítače, interní, externí, periferie, stavba a konfigurace počítače před instalací OS

Hardware

* **CPU**
  + Ústřední výkonná jednotka počítače, která čte z paměti instrukce a na jejich základě vykonává program.
  + Dříve z elektronek, tranzistorů a kondenzátorů
  + Parametry:
    - **Architektura** (nejčastější značky + uzpůsobení základní desky)
      * AMD (Jenom North Bridge)
      * INTEL (North a South Bridge)
      * Hodně funkcionalit chipsetu se přeouvá přímo na procesor. Rozmach SoC to živí a North Bridge je dnes zpravidla in package.
    - **Patice**
      * Nachází se na základní desce, slouží k připojení procesoru
      * např. Intel – LGA 1151, LGA 2066; AMD – AM4, TR4
    - **Výrobní technologie**
      * Výrobní velikost tranzistorů je nyní okolo 7nm
    - **Počet vláken a jader**
      * běžně 2-4 jádra, 2-4 vláken
      * více vláken znamená, že jádro zvládne zpracovávat více úkolů v reálném čase najednou
    - **Frekvence** (vyšší je lepší)
    - **L1,L2,L3 cache** (vyrovnávací paměť - běžně velikost v jednotkách MB)
    - **Šířka operandu**
      * Počet bitů, který je procesor schopen zpracovat v jednom kroku (takt) - např. 8bit CPU pracuje s čísli v intervalu (0-255)
      * Druhy CPU
        + 8bit (domácí spotřebiče, kancelářské klávesnice,...)
        + 16bit (programovatelné automaty, PDA,...)
        + 32/64bit (počítače, mobilní telefony a další výpočetní technika)
  + CPU komunikuje s čipsetem
  + Schéma CPU
    - **Řadič** (CU) – řídící jednotka, jejíž jádro zajišťuje řízení činnosti procesoru v návaznosti na povely programu
    - **Registry** – rychlá pracovní paměť malé kapacity (cache)
    - **Aritmeticko-logická jednotka** (ALU) – provádí s daty matematické operace
    - **Sběrnice** – přenáší data do a v procesoru, komunikuje s dalšími součástmi počítače
* **GPU**
  + Stará se především o zobrazení obrazu na monitoru, ale používá se i pro grafické (RTX) nebo jiné (mining) výpočty.
  + Připojena je většinou přes PCI-E slot, méně výkonné grafické karty často bývají integrované v procesoru.
  + Základní komponenty:
    - **GPU** – grafický procesor, je výpočetní jádro grafické karty
    - **VRAM** (Video Random Access Memory) – jsou na ní ukládány informace nutné pro grafické výpočty (pokud je karta integrovaná na základní desce, nebo dedikované dojde paměť, používá operační paměť počítače)
    - **RAMDAC** – převodník digitálního signálu na signál analogový
    - **Výstupy** (běžně např. VGA, HDMI, DisplayPort, DVI)
* **RAM**
  + Rychlá paměť
  + Součástka, která umožňuje dočasně ukládat informace a data, která jsou právě počítačem využívána.
  + Maximální kapacita sestavy (dle šírky operandu CPU)
    - 32 bit -> 2^32 = 4GB
    - 64 bit -> 2^64
  + Parametry
    - Kapacita (běžně 8 GB či 16 GB)
    - Frekvence (počet operací, které lze vykonat za vteřinu (běžné hodnoty kolem 3000 MHz, nejlepší paměti až 6400 MHz))
    - Časování
  + Pojmy
    - Single-Channel, Dual-Channel, Quad-Channel (počet kanálů, kterými RAM komunikuje s procesorem (používá se tak, aby každý modul měl svůj kanál))
    - XMP (Extreme Memory Profiles – profily pro automatické přetaktování (Profil 1 nastaví původní hodnoty určené výrobcem, Profil 2 nastaví vyšší hodnoty pro nejlepší výkon))
    - DDRx, kde x je číslo z množiny K = {1,2,3,4,5} (typ SDRAM, číslo označuje generaci, aktuálně 4 a 5)
* **Základní deska**
  + Propojuje jednotlivé součástky počítače do fungujícího celku a poskytuje jim elektrické napájení.
* **Úložiště (HDD/SSD)**
  + Hlavní paměťové zařízení počítače, které slouží pro trvalé uchování dat.
  + Je nástupcem magnetických pásek a disket.
  + **HDD**
    - Pomalejší než SSD
    - Výkon je limitován
      * Otáčky ploten
      * Hustotu zaznamenaných dat
      * Rychlost vystavovacího mechanismu
    - Základní součástí
      * Diskové plotny
      * Diskové hlavy
      * Vystavovací mechanismus
    - Typy
      * SATA
      * PATA
    - Napájení
      * SATA
      * MOLEX
    - Při chybě jsou větší ztráty
  + **SSD**
    - Na rozdíl od pevných disků neobsahuje pohyblivé mechanické části (místo nich využívá flash paměť), tudíž je spolehlivější, také má mnohem nižší příkon, nižší hmotnost a hlavně vyšší přenosovou rychlost.
    - Typy
      * SATA
      * PCIE (NVMe M.2, U.2)
* **Zdroj**
  + Zdroj je elektronická součástka (podobná transformátoru), která dodává počítači elektrický proud v požadovaném napětí.
  + Při nákupu je potřeba přemýšlet dopředu a vypočítat si vyžadovanou spotřebu počítače.
  + Čím menší je procentuální zátěž, tím méně je efektivní (nejefektivnější je většinou okolo 80%).
* **Skříň**
  + Slouží k mechanickému upevnění všech ostatních vnitřních dílů a částí počítače.
  + Obsahuje ovládací prvky (zapínací tlačítko, reset), indikační prvky (LED indikující zapnutí, LED indikující činnost disku) a rozšiřující konektory (USB, audio jack apod.) umístěné většinou na čelním panelu skříně.
  + Řešíme u ní vzhled, airflow atp.
* **I/O**
  + Konektory, pomocí kterých připojujeme periferie
  + Příklad: USB, RJ-45, 3.5mm jack, a pod.

Další pojmy

* **Sběrnice**
  + "Spoje"
  + Slouží pro přenos dat mezi jednotlivými součástkami.
  + Typy
    - **Datová** (data)
    - **Adresová** (adresy, kde data/instkuce jsou)
    - **Řídící** (co s daty/instrkucemi, např. odkud kam)
  + Rychlost určená:
    - Rychlostí sběrnice
    - Taktem
  + Typy
    - **USB**
      * Data
      * Napájení
      * Rychlosti:
        + USB 2.0 - 480Mb/s (oba směry dohromady)
        + USB 3.0 - 5Gb/s
      * Umožňuje stromovou strukturu
    - Sata
      * Sériová
      * Pro připojení disků
    - Pata
      * Paralerní
      * Pro připojení disku
    - Firewire
      * Předchůdce USB 3.0
    - LPT
      * Paralerní
      * Pro komunikaci s tiskárnou
* **Slot**
  + Zdířka na základní desce určená k připojení součástky, napojí součástku na sběrnici a poskytne ji napájení.
* **Chipset**
  + čipy na základní desce, které komunikují s procesorem
  + části chipsetu
    - **North bridge**
      * komunikace mezi CPU a RAM/PCI-e
      * zajišťuje spojení se south bridgem
      * bývá integrovaný v procesoru
    - **South bridge**
      * komunikace na USB, PS/2, SATA, PCI, (PCI Express), ...
      * Chytrý switch
  + Komunikace mezi zařízeními
  + Na základní desce
  + Typy:
    - AMD A
      * Levné
      * Nepodporují taktování
    - AMD B
      * Relativně levné
      * Podporují taktování
      * Ne vždy podporují hardwarový RAID
    - AMD X
      * Drahé
      * Pro výkonné počítače
      * Podporují taktování a většinou hardwarový RAID
    - Intel H
      * Levné
      * Pro běžné počítače
    - Intel B
      * Dražší než H
      * Pro náročné uživatele
    - Intel Z
      * Drahé
      * Pro výkonné počítače
  + Dnes často nahrazováno takzvaným PCH - Platform Controller Hub
    - Technicky se nejedná o chipset, avšak termín je natolik zakořeněný, že označení převzal
    - Zpravidla použit tehdy když je North Bridge plně integrován na procesor (téměř všechny moderní procesory) 
* **RAID**
  + Používá se pro zefektivnění rychlosti zápisu a zvýšení bezpečnosti uložených dat zejména v serverech.
  + Můžeme dělit na hardwareový a softwareový RAID.
  + Umožňuje spojit několik disků v jeden celek, což umožní rychlejší zápis dat a/nebo obnovení ztracených dat v případě selhání jednoho z disků.
    - **RAID 0** – rozdělí data na segmenty mezi disky, díky čemuž dosahuje vyšších rychlostí zápisu a čtení, data ale nejsou nijak chráněna před ztrátou
    - **RAID 1** – zrcadlí data z jednoho disku na druhý, v případě selhání jednoho z disků jsou tedy všechna data zachována
    - **RAID 5** – vyžaduje minimálně tři disky, kapacitu jednoho celého disku zabírají samoopravné kódy (ty jsou ale střídavě rozděleny mezi všechny disky), ustojí selhání jednoho disku
    - **RAID 6** – vyžaduje minimálně čtyři disky, kapacitu dvou celých disků zabírají dva různé bloky samoopravných kódů (opět rozděleny mezi všechny disky), ustojí selhání dvou disků
    - **Kombinace** – tyto typy RAID lze kombinovat v tzv. víceúrovňových polích, například v RAID 50 (5+0) se disky rozdělí na dvě podpole, které obsahují samoopravné kódy, zároveň jsou ale rozložena na segmenty
  + Hardwareový RAID se nastavuje v BIOSu, nebo specifickém programu.
  + Softwareový RAID se na Windows nastavuje buď v ovládacích panelech (Storage Spaces) nebo ve správě disků.

Druhy pamětí

* **Podle způsobu a možnosti zápisu**
  + **RWM** (Read Write Memory) – paměť pro zápis i čtení dat
  + **ROM** (Read Only Memory) – paměť pouze pro čtení (např. DVD s filmem)
  + **PROM** (Programmable Read Only Memory) – na paměť se data naprogramují a v paměti již zůstanou uchována
  + **EPROM** (Erasable Programmable Read Only Memory) – stejná jako PROM, ale data lze přemazat
  + **EEPROM** (Electrically Erasable Programmable Read Only Memory) – stejná jako EPROM, ale data lze přemazat elektronicky
* **Podle technologie uchování dat**
  + **SRAM** (Static Random Access Memory) – malá, rychlá, dražší, menší kapacita; použití například v cache procesoru
  + **DRAM** (Dynamic Random Access Memory) – větší, pomalejší, levnější, vyšší kapacita; používá se jako operační paměť v PC
    - SDRAM (Synchronous Dynamic Random Access Memory) – typ DRAM, který synchronizuje svou činnost s procesorem, a proto dosahuje vyšších rychlostí; nejrozšířenější typ operační paměti
* **Podle velikosti pamětových modulů**
  + **DIMM** – běžný typ paměťových modulů používaný v PC
  + **SO-DIMM** (Small Outline DIMM) – menší verze DIMM, použití v noteboocích

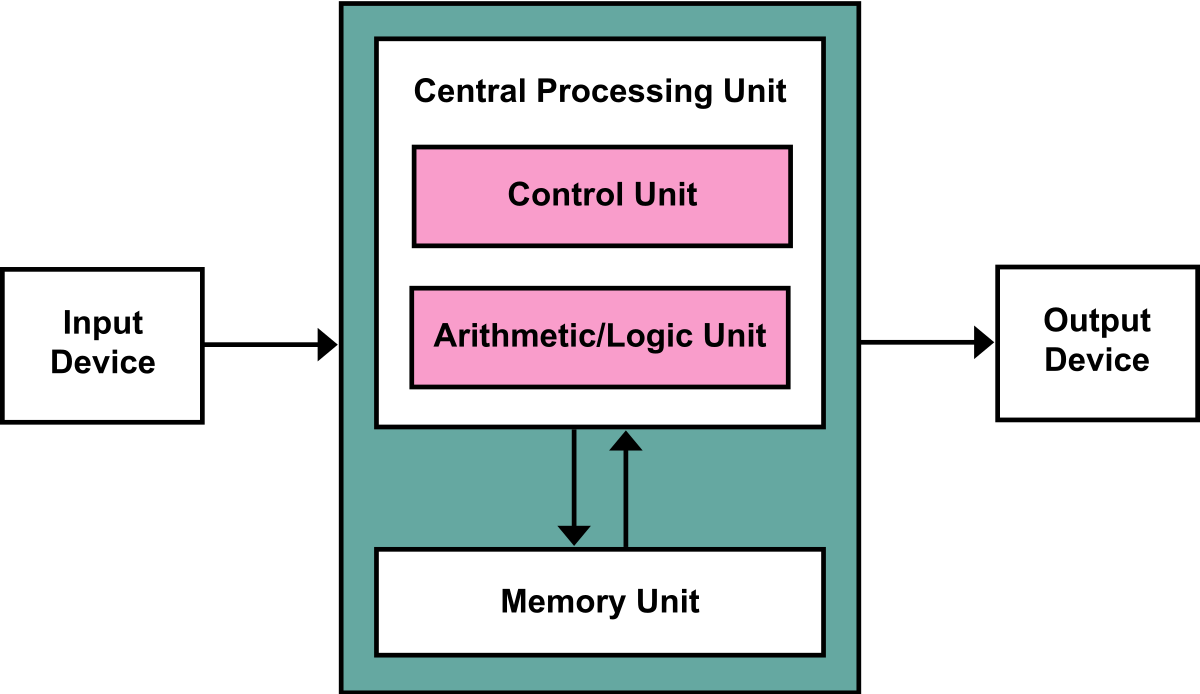
Instrukce

* Co potřebujeme
* S čím
* Kam s ním (Neruda)

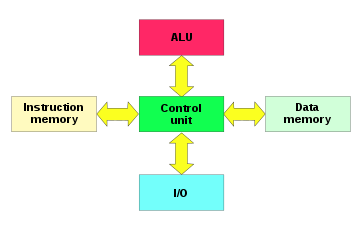
Architektura

* Popisuje programovatelný počítač

Von Neumanova

* Starší architektura než Harvardská
* **Paměť pro instrukce a data je sdílená** 

Harvardská

* **Paměť pro instrukce a data je rozdělená** 

POST (Power on self test)

* Součást BIOSu
* Potřeba klávesnice
* Pípák (beep codes), stavový displej
* **Testuje komponenty počítače, zda nejsou vadové**

BIOS (Basic Input/Output System)

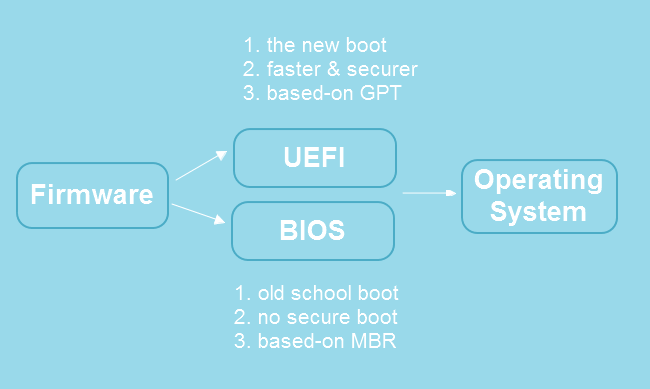
* **Základní program po spuštění počítače** (pro spuštění operačního systému)
* Ovládání počítače
* uložen na základní desce v pamětech typu ROM a EEPROM (flash)
* Při startu kontroluje a konfiguruje připojená hardwarová zařízení (POST)
* Využívá MBR, je legacy
* Bezpečnost
  + Heslo
* Boot po síti
* Vybitá baterie -> Desynchronizace času

UEFI

* Vychází s BIOSu
* **V podstatě grafické rozhraní pro BIOS**, ale disponuje i dalšími novějšími funkcemi
* Podporuje MBR, ale i GPT
* Bezpečnost
  + Secure boot

BIOS vs UEFI

| **BIOS - Basic Input-Output System** | **UEFI - Unified Extensible Firmware Interface** |
| --- | --- |
| - | Rychlejší boot a vypnutí |
| teoreticky grafický, prakticky ne | grafické rozhraní |
| - | Secure boot |
| - | síťové možnosti - troubleshooting a vzdálená konfigurace |
| při startu zkoumá všechny komponenty | inicializuje základní hardware, další se poté může aktivovat paralelně |
| při bootu prohledává všechna úložiště | rovnou ví kde co je |
| nemůže | může pomocí shellu spouštět software |
| MBR (disk max. 2TB, max. 4 partitions) | GPT (nemá omezení jako MBR), tabulka zapsaná v druhém sektoru |



Zaváděcí tabulky

* Jedná se o soubory obsahující informace o tom, jak je disk rozdělený na oddíly a jak k nim má operační systém přistupovat.
* **MBR** (Master Boot Record)
  + Zastaralá zaváděcí tabulka
  + umí pracovat jen s disky do 2 TB a podporuje maximálně čtyři oddíly
* **GPT** (GUID Partition Table)
  + oproti MBR novější
  + poskytuje teoreticky neomezený počet oddílů a velikost o 9.4 Zettabytů
  + GUID (Global Unique Identifier) je náhodný unikátní identifikátor oddílů, každý GPT oddíl na světě lze podle něj identifikovat.
  + GPT zapisuje data na několik míst na disku (bezpečnější), v čase zkoumá, zda nejsou poškozena (pokouší se je kdyžtak opravit)
  + Může obsahovat jednu MBR tabulku pro zpětnou kompatibilitu

Stavba počítače

* Využití/cena/specifické požadavky
* Vybírat komponenty postupně
  + **CPU** (od něj se odvíjí patice/socket na MB)
  + **Deska** (Socket, kompatibilita s CPU!, vhodné rozmyslet i typ čipové sady - odvíjí se od něj funkce MB)
  + **RAM** (typ (DDR5, DDR4, ...), velikost, rychlost, časování - na základě MB!)
  + Grafická karta (ne vždy potřeba)
  + **Zdroj** (nutné vybrat ten, který má požadované konektory)
    - Výpočet kapacity zdroje = Maximální spotřeba sestavy \* 1.5
* Při stavbě je vhodné
  + Uklidit pracoviště
  + Nepoužívat oděv z umělého vlákna
  + Připravit si potřebné nástroje předem
  + Před prací se uzemnit (například dotek s radiátorem nebo zemnící kolík)

2FA (HW)

* Více stupňové ověření
* Slouží k bezpečnějšímu přihlašován
* Můžeme dělit na:
  1. moduly v PC (HW)
  2. 3. strana - šipy (???)
  3. USB Klíčenka
     + USB rozhraní
       - Sériová komunikace
     + USB paměť (flash)

Operační systémy, základní funkce, možnosti konfigurace uživatelského rozhraní

* **Základní programové vybavení počítače**
* Při startu PC zaveden do operační paměti a zůstává v činnosti až do jeho vypnutí
* Hlavní funkce
  + **Efektivní využití systémových zdrojů** (HW prostředků)
    - Systémové zdroje:
      * CPU
      * RAM
        + Správa paměti
      * Paměťové úložiště
        + Filesystem
      * I/O
      * Multiuser
    - Využití
      * Přidělení, správa, odebrání procesů -> Instance úlohy (aplikace)
    - Efektivní
      * multitasking
  + **Možnost ovládat počítač uživatelem**
  + **Vytvoření rozhraní pro aplikace** (API - lze instalovat programy a následně s nimi pracovat) **a správa softwaru**
  + **Organizuje přístup k datům**
* Skládá se z **jádra** (kernelu) a **pomocných systémových nástrojů**

Základní pojmy

* **Multitasking**
  + Schopnost operačního systému “provádět několik procesů současně” (v reálu se jedná jen o rychlé střídání běžících procesů na procesoru)
  + Druhy
    - **Preemptivní** (moderní, o přidělování a odebírání systémových prostředkům jednotlivým úlohám plně rozhoduje operační systém)
    - **Kooperativní** (vyžaduje aktivní spoluúčast běžících úloh, každá úloha je povinna předávat řízení zapůjčených prostředků zpět systému (chybně naprogramované aplikace mohou způsobit zamrznutí celého OS))
* **Druhy uživatelského rozhraní**
  + **CLI** (Command-Line Interface)
    - Terminál pro zadávání příkazů
  + **TUI** (Text-based User Interface)
    - Pokouší se o grafické prvky tvořené textem
    - Nepodporuje využití myší
    - Např. BIOS
  + **GUI** (Graphical User Interface)
    - umožňuje uživateli ovládat počítač pomocí interaktivních grafických prvků (ikony, tlačítka, formuláře, panely,...).
    - základní prvky: pointer, icons, widnows, menus, scroll bars, input device
* **API** (Application Programming Interface)
  + Rozhraní pro programování aplikací.
  + Konkrétně se jedná o sbírku procedur, funkcí a tříd určité knihovny, kterou může programátor využívat při tvorbě aplikací.
* **Bootloader** (zavaděč)
  + Malý program, který v sobě nese informaci o nynějším umístění operačního systému, aby ho mohl následně nahrát z disku.
  + např. GRUB (Linux)
* **Kernel**
  + jádro operačního systému, které je rozbaleno (před spuštěním je vždy komprimováno!!!) a zavedeno při startu počítače
  + Hlavní funkce
    - **správa multitaskingu** (určuje, jaký proces bude procesor právě zpracovávat)
    - **správa souborového systému**
    - **přiděluje aplikacím prostor na operační paměti a zpracovává jejich požadavky na používání dalšího hardwarového vybavení**
  + Druhy kernelu (jader), od kterých se odvíjí typy systémů
    - **Mikrokernel**
      * Zajištuje pouze základní funkce (např. správa CPU, RAM)
        + Skládá se z:

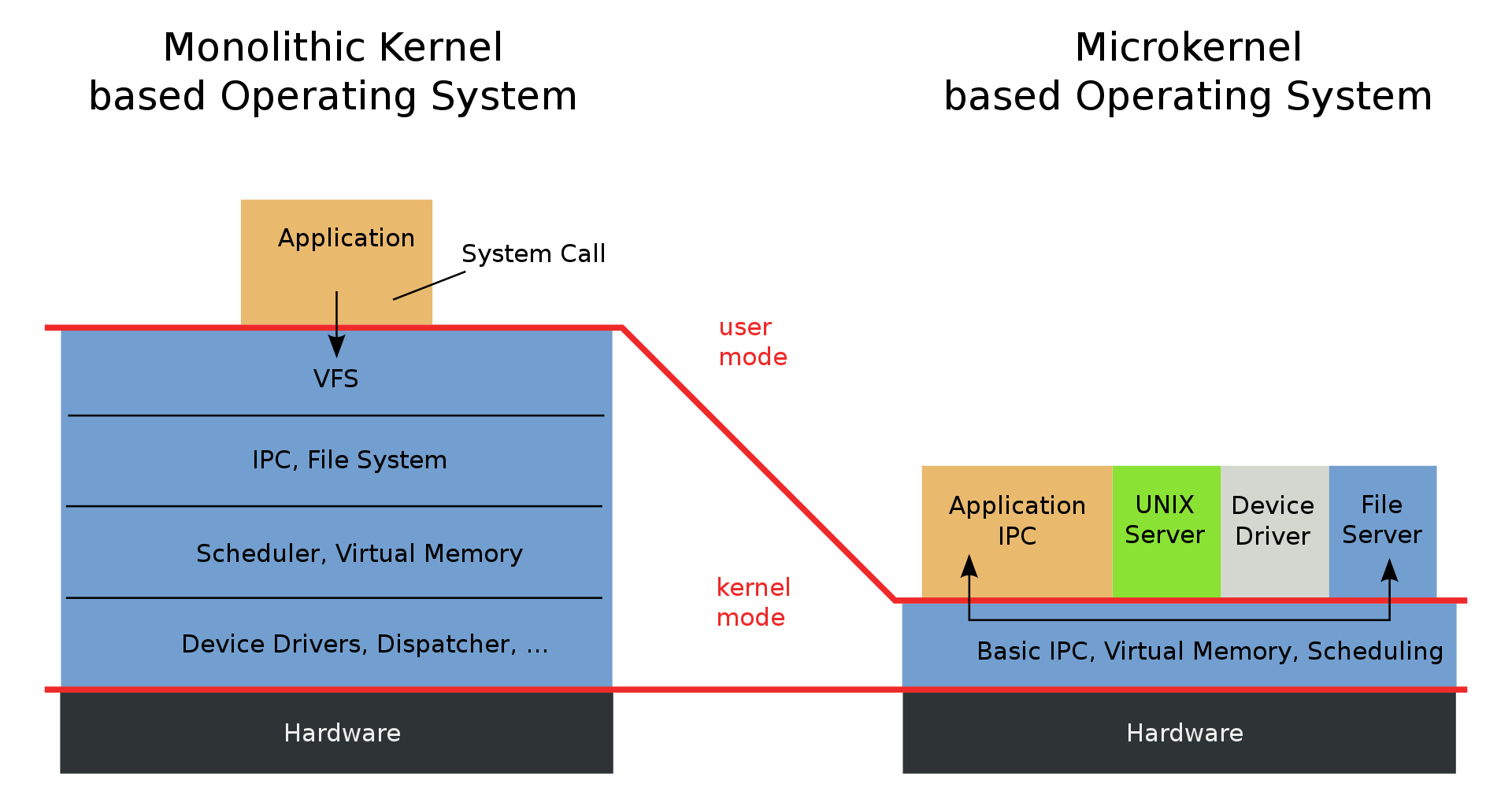
IPC (komunikace mezi procesy/vlákny)

přerušení

správa virtuální paměti

časování

* + - * správa ovladačů a další služby operačního systému jsou prováděny odděleně, v případě chyby se daný proces automaticky restartuje
      * bezpečný a spolehlivý, těžké ho optimalizovat (pomalejší)
      * Modulární: musím donahrát všechny moduly, které potřebuji
      * Systémy: - Minix, Symbian, MacOS 8, Arduina/ESP
    - **Monolitický kernel**
      * Jádro ovládá vše
      * **Všechny služby operačního systému běží spolu s hlavním vláknem jádra** (díky tomu mají neomezený a efektivní přístup k hardwaru, to ale způsobuje závislost mezi systémovými komponentami a chyba v libovolném ovladači může shodit celý systém)
      * Skládá se z:
        + vše jako u mikrojádra
        + zavaděče
        + správa paměti a souborového systému
        + ovladačů
      * Systémy: Windows, většina Linuxů (s prvky hybridního kernelu)
    - **Hybridní kernel**
      * Kombinuje rychlost a jednoduchost monolitického kernelu s bezpečností a spolehlivostí mikrokernelu.



* **HAL** (Hardware Abstraction Layer)
  + **zajištuje abstrakci nad HW** (tzn. programu, který běží na OS je jedno, jaký HW používáme -> program může bez problému využívat prostředky HW)

Rozdělení systémů

1. **Windows X GNU/Linux**
   * licence: Closed source X GPL v.2.0
   * modulárnost: není X velká (lze zvolit části systému)
2. **Monolitické X mikrojádra**
3. **Desktop X Server**
   * Server poskytuje služby
   * Desktop využívá služby
   * Server vyžaduje síťové připojení
   * GUI X TUI
   * Gnome (hezčí) X KDE (potřeba konfigurace)

Windows

* Obecné označení pro sérii komerčních operačních systému společnosti Microsoft, podporující grafické rozhraní a multitasking
* Novější verze jsou rozděleny na různé edice (Home, Pro, Enterprise, Education,...), jež poskytují odlišné nástroje a podporu
* nejpopulárnější OS

MacOS

* Obecné označení pro sérii komerčních operačních systému společnosti Apple, podporující grafické rozhraní a multitasking
* silně spjatý s Apple hardwarem (vždy je dodáván již nainstalovaný na daném Mac počítači a není možné ho legálně nainstalovat na jakýkoliv neautorizovaný hardware)

Linux

* Obecné označení pro rodinu svobodných open-source operačních systémů založených na unix-like kernelu
* Šíří se zpravidla zdarma v podobě distribucí (distribuce obsahují linuxový kernel, jsou ale doplněny o různé nástroje a aplikace - např. Debian, Ubuntu, Mint Linux, Arch Linux, Raspberry Pi OS, Kali Linux,...)
* Modifikované Linuxové jádro je také hojně využíváno pro mobilní operační systémy (Android, KaiOS,...) a širokou škálu smart zařízení (televize, bílé elektrospotřebiče, palubní systémy v autech,...)
* Existují i placené edice (resp. placená podpora od RedHatu a placené repozitáře)
* Dominuje na serverch

Historie (nuda, lze přepsat do bodů ??????????? - jestli se ti chce 🤷‍♂️)

Unix

První verze Unixu byly vyvíjeny v 60. letech 20. století společností Bell Laboratories jako operační systém pro sálové počítače. Unix neměl daný žádný určitý plán, podle kterého se postupovalo, velká část jeho funkcí se přidávala na základě žádostí od zákazníků a nápadů vývojářů. Postupně začaly na základě Unixu vytvářet své operační systémy společnosti jako HP (HP-UX), IBM (AIX) nebo Microsoft (Xenix). V roce 1983 vytvořil Richard Stallman svobodný unix-like systém GNU. Mezi moderní unix-like operační systémy patří například MacOS, Linux, Minix, NetBSD a další.

Linux

Autorem je Linus Torvalds, původně psal software pouze pro svůj osobní počítač. První verze Linuxového jádra byla vydána v roce 1991, postupně se do jeho vývoje zapojovalo mnoho dalších dobrovolníků. Již z počátku pracoval Linuxový kernel s GNU nástroji, ty ale nejdříve nebyly v distribuci zahrnuty, později byl Linux vydán pod GNU GPL (General Public Licence), načež začali vývojáři Linux a GNU integrovat do sebe, čímž stvořili plně funkční svobodný systém. Důležitým milníkem byl rok 1992, kdy byl na Linux portován framework X Window System, který dovoloval využití GUI. Postupně Linux nabíral na popularitě, začalo vznikat mnoho komerčních i nekomerčních distribucí.

MacOS

Jeho první verzi (System 1) vydal Apple společně s počítačem Macintosh 128K v roce 1984, od verze 7 byl přejmenován na Mac OS. Bez Jobse, který firmu opustil, se Mac OS kvůli absenci inovací postupně stával zastaralým. Z toho důvodu Apple koupil Jobsovu firmu NExT, společně portovali velkou část systému NExTSTEP do Mac OS, čímž vznikla verze Mac OS X 10.0, první verze, která používala unix-like kernel. V roce 2006 (Mac OS X 10.4.4 Tiger) se Apple rozhodl pro přechod z PowerPC na Intel procesory pro jejich vyšší výkon a efektivitu, Intel ale používal jinou architekturu, funkčnost starého softwaru byla zajištěna nástrojem Rosetta (překlad PowerPC instrukcí na Intel). Přechod byl kompletně dokončen v roce 2012 verzí Mac OS X 10.7 Lion, která již nepodporovala Rosettu. Po dlouhodobých problémech s efektivitou Intel procesorů přešel Apple v roce 2020 na vlastní ARM procesory. Překlad instrukcí zajišťuje Rosetta 2.0.

Windows

První verzi vydal Microsoft v roce 1981, téhož roku si IBM koupilo licenci a modifikovanou verzi prodávalo se svými počítači pod názvem PC DOS. Samotný MS-DOS byl vyvíjen až do roku 2000, ale již v roce 1985 Microsoft vydal Windows 1.0 (s MS-DOS kernelem), svůj první operační systém s GUI. V této linii pokračoval verzemi 2.x a 3.x, které byly následně nahrazeny Windows 95, 98 a Windows Me. V roce 2000 Microsoft systémy běžící na MS-DOS kernelu opustil, podpora Windows Me byla kompletně ukončena v roce 2006. V roce 1993 vydal Microsoft systém Windows NT 3.1, který nabízel stejné uživatelské prostředí jako o rok starší Windows 3.1, byl ale postaven na novém kernelu, který měl řadu výhod (především 32-bitovou architekturu, MS-DOS jádro používalo 16-bitovou). Tato linie pokračovala verzemi 3.5 a 4.0, které byly následně nahrazeny Windows 2000. Microsoft vyvíjel i 64-bit verzi Windows 2000, ale ta nebyla nikdy vydána. Oficiální podpora 64-bit přišla až se speciální edicí Windows XP. Windows XP také přinesl mimo zlepšeného výkonu a stability také první velkou změnu ve vzhledu UI. Další verze byla vydána až po pěti letech v roce 2006, a to Windows Vista. Ačkoliv přinesla další velkou změnu ve vzhledu UI a spoustu nových funkcí, které používáme dodnes (User Account Control, Windows Defender, Windows Update zabudovaný do systému, Disk Management, Windows Search,...), sklidila mnoho kritiky především za špatnou stabilitu a vysoké hardwarové nároky. Většina problémů byla vyřešena o tři roky později s verzí Windows 7. Její velkou oblíbenost můžeme pozorovat dodnes, stále (Q4 2020) ho používá ~16 % Windows uživatelů, jedná se tak o jediný zastaralý Windows, který si stále drží svou popularitu. O další tři roky později vyšel Windows 8, který přinesl mnoho bezpečnostních vylepšení (opravy přihlašovacích exploitů, secure boot, vylepšení Defenderu), byl silně kritizován za jeho UI, které bylo sice velmi užitečné pro uživatele tabletů, na bezdotykových zařízeních ale zaostávalo. Chyby se snažil Microsoft opravit verzí 8.1, ale ani ta nikdy nebyla příliš populární. Definitivní verzí je Windows 10 z roku 2015, která je neustále vyvíjena a vylepšována pravidelnými updaty. Uživatelům verzí 7 a vyšší byl nabízen zdarma, dokonce je možné ho legálně používat bez licence, za to se ale platí osobními údaji, které jsou sbírány v mnohem větším množství než na jakékoliv starší verzi.

Konfigurace OS

Windows

* v Nastavení (základní nastavení vzhledu atp.) nebo v Ovládacích panelech (pokročilejší nastavení jako správa disků, správa zařízení - tzn. driverů atp.)
* Části ovladacích panelů
  + Síť
  + Systém
  + Zabezpečení
  + Programy
  + Hardware
  + Usnadnění přístupu
  + Uživatelé

MacOS

* Všechna nastavení jsou lokalizovaná v panelu Systémových preferencí, do kterého často vlastní záložku přidává i nainstalovaný software.

Linux

* Ačkoliv je každá distribuce jiná, u většiny distribucí pro běžné uživatele platí, že konfigurace lze provádět v centralizované aplikaci pro nastavení.
* Co nelze konfigurovat v dané aplikaci, je možné vyřešit skrz příkazový terminál.

Doména

* Síť počítačů se stejnými nastaveními
* Spravuje uživatele a jejich nastavení
* V dnešní době se používá s AD
* Více domén: autonomní X trust
* Vyžaduje doménový řadič (Windows Server) a DNS server

AD - Active Directory

* Slouží k administaci domén
* Umožňuje efektivně uspořádat síťové prostředky
* Umožňuje používat stromovou strukturu
* Více info na: [Wikipieii](https://cs.wikipedia.org/wiki/Active_Directory)

Group Policy

* Správa systému
* Skupina -> Uživatelé -> Konfigurace OS

Mail

* <https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mda-smtp-dkim-spf-dmarc>
* Protokoly
  + POP3 (Post Office Protocol version 3)
  + IMAP (Internet Message Access Protocol)
  + SMTP (Simple Mail Transfer Protocol)
* Služby
  + MTA (Mail transfer agent)
  + MDA (Mail Delivery Agent)
  + MUA (Mail User Agent)

Zálohování

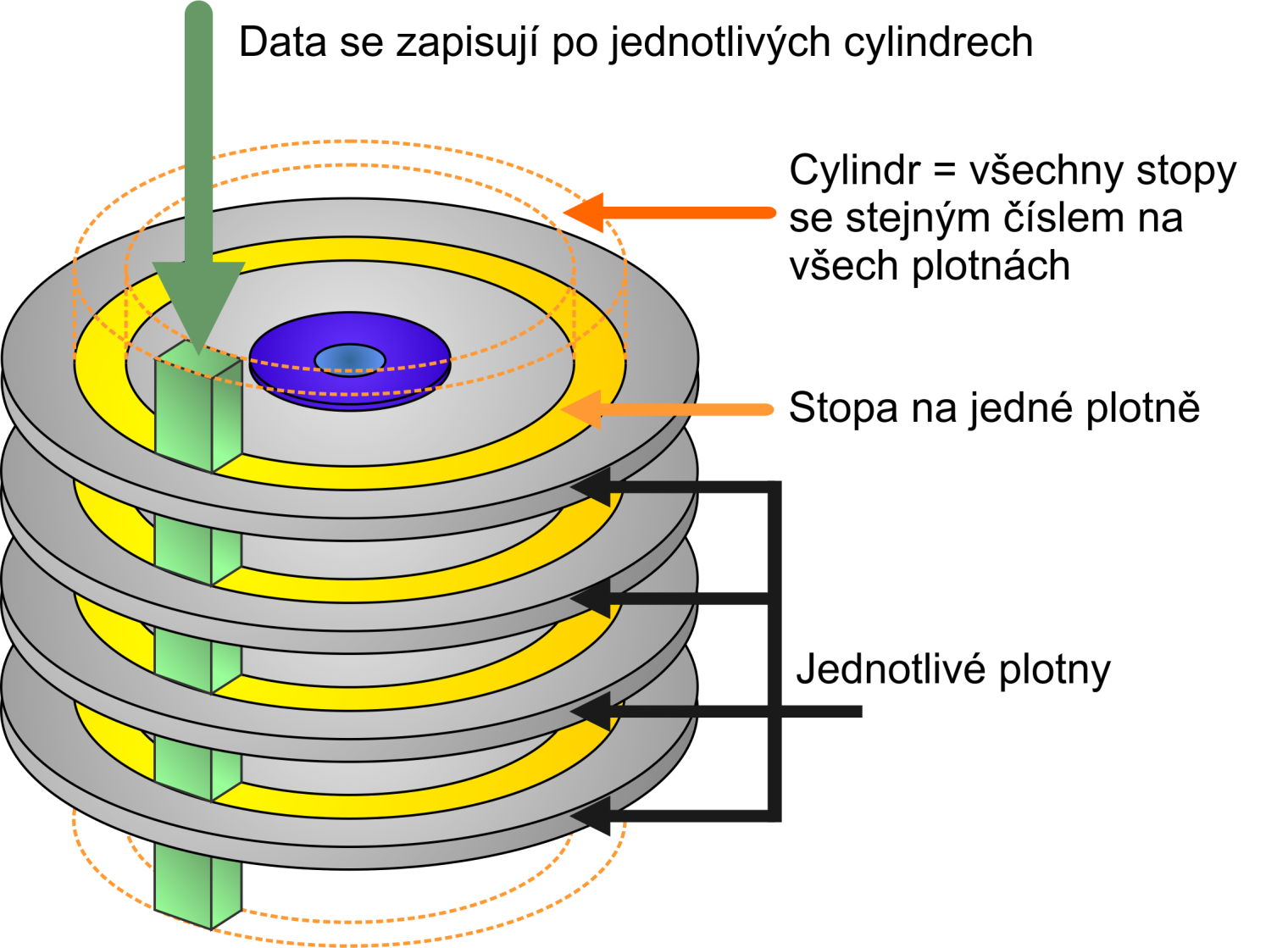
* Typy
  + Uživatelská data
  + Konfigurace
* Jedna z možností zálohy jsou **pásková mechanika**

# Instalace, konfigurace operačního systému

## Boot

* HDD(SSD), LiveCD, USB, Síť
* Hledání zavaděče
* Pozice: 001 - hlava, cylindr, sektor
* Zavaděč -> najde jádro -> vykomprimuje
* Na Linuxu - spuštění init systému (moderně SystemD)
* Jádro systému je zabaléné

## Podrobnosti HDD

* 
* Souborový systém -> datový typ
  + Soubor -> jméno
  + Metadata
  + Stromová architektura
    - Rozlišujeme pomocí parametru
    - Soubor **-**
    - Složka **d**
  + Čítač souborů
  + Synchronizační metoda semaforu
  + Cluster
    - je to nejmenší uložitelná část
    - definován souborovým systémem
  + Indexování
  + Maximální velikost partition
* Standardy pro souborové systémy
* Oddíl - logické členění disku - slouží k:

## Partition (oddíl)

* Rozdělení fyzického disku na logické disky
* Slouží k:
  + **Více OS**
  + Zrychlení OS na HDD (tím, že rozdělíme disk, můžeme fyzicky zarovnat OS k vnějšímu okraji diskového kotouče. Právě na obvodu disku je přenosová rychlost nejvyšší)
  + **Organizace a snazší zálohy** (mít OS na jednom oddílu a data s aplikacemi na druhém)
  + **Ochrana dat** (při potřebě naformátování systémového oddílu zachováme ten s daty, to samé platí při instalaci systému)
  + Nastavení kvót
* Při více operačních systémech je potřeba tomu uzpůsobit zavaděč, aby bylo možné přepínat mezi nimi

## Image

* Bitová kopie (klon) -> slouží např. k analýzám dat na disku
* Každý počítač je při instalaci z bitové kopie stejný

## Instalace Windowsů

* **Instalace jádra systému**
* **Aktualizace z internetu** (s tím souvisí **správa a stažení ovladačů** - Správce zařízení)
* **Aktivace systému**
* **Nastavení samotného systému** - Windows má předpřipravené "expresní nastavení" (např. automatické stahování aktualizací). Je ale vhodné provést další nastavení:
  + **Konfigurace uživatelů a uživatelských rolí**
    - Vytvoření běžného uživatelského účtu nebo možnost použít účet Microsoft (podpora synchronizace mezi zařízeními)
    - Je vhodné vytvořit běžný účet pro uživatele (s nižšími pravomocemi) a administrátorský účet
    - Také lze vytvořit speciální účet tzv. "Power User" (pravomoce mezi běžným uživatelem a administrátorem)
  + **Zabezpečení systému**
    - Antivirus
    - Firewall
    - Body obnovy a zálohování
  + **Další nastavení** např.
    - Síť
    - Vizuální stránka

## Účty a profily ve Windows

### Profily uživatelů

* Sada nastavení, díky kterým OS vypadá a pracuje podle představ uživatele. Zajišťuje, že uživatel po přihlášení získá stejný vzhled a nastavení jako při minulém přihlášení. Obsahuje nastavení plochy, spořič obrazovky, oblíbené položky apod.

#### **Místní profil**

* Je uložen **lokálně** na disku PC, změny profilu se projeví pouze v daném PC.

#### **Cestovní profil**

* Je uložen **na síťovém serveru**, je dostupný uživateli po přihlášení k libovolnému PC v dané síti.

#### **Povinný profil**

* Změny se neukládají, profil zůstává konfigurovaný **ve výchozí podobě**.

### Uživatelské účty

* Sada informací a práv, které určují, do jakých složek či ke kterým souborům má uživatel přístup a jaké konfigurace OS může provádět.

#### **Správce**

* **Nejvyšší úroveň oprávnění v OS**, může vytvářet a spravovat účty, měnit veškerá nastavení, instalovat SW apod.

#### **Standardní**

* **Záleží na nastavení účtu**, vlastní své přihlašovací údaje a je na něj vázán unikátní profil.

#### **Guest**

* **Nemá přístup k osobním souborům**, může používat jen určité programy instalované jinými uživateli.

### Skupiny

* Soubor oprávnění, která lze přiřazovat uživatelským účtům. Pokud je účet členem více skupin jeho oprávnění se sčítají, když jsou v jedné skupině zakázána a v druhé povolena, zůstávají zamčená.

#### **Administrators**

Skupina **s nejvyššími právy** pro práci s OS.

#### **Users**

Umožňuje **využití standardních prostředků** PC.

#### **Power Users**

Vše co může User + základní konfigurace systému a instalaci běžných aplikaci.

## Typy instalace

### Čistá instalace

* Provedeno formátování disku a následné nahrání systému
* přijdeme o veškerá nastavení (tzn. nastavení jsou v defaultu)
* Bezobslužná instalace (tichá)
  + Využívá dávkový soubor/skript, podle kterého se doplňují odpovědi za uživatele při instalaci OS
  + často zneužit pro instalaci škodlivého SW

### Inovace/Aktualizace systému (upgrade)

* Nahrazení stávajícího OS novým (systém se snaží zachovat co nejvíce nastavení, což se týká i zachování aplikací)

### Instalace z sítě

### Instalace z bitové kopie

* Instalace a konfigurace OS a všech požadovaných aplikací, často se používá jako záloha, ale také pro co nejrychlejší instalaci OS na větší množství počítačů.
* Dochází ke klonování, je vhodné bitovou kopii instalovat na stejný hardware, ze kterého se bitová kopie vytvářela

Periferní zařízení, členění, konektivita zařízení, způsob instalace a konfigurace

Pojmy

Vstupní periferie

* Zařízení rozšiřující možnosti použití počítače (tzv. přídavná zařízení). Počítač skrz ně pořizuje data a s nimi poté pracuje. Např. myš, klávesnice, mikrofon apod.

Výstupní periferie

* Rozšiřují možnosti použití PC, slouží k výstupu dat z počítače. Např. sluchátka či reproduktory, monitor apod.

Vstupně-výstupní periferie

* Hardware pro výměnu dat mezi uživatelem a počítačem, který kombinuje vlastnosti vstupních a výstupních zařízení.
* Např. dotykové displeje, podsvícené klávesnice, tiskárny se skenerem, gamepady s vibrací apod.

Firmware

* Mikroprogramové vybavení, které slouží pro řízení nějakého vestavěného systému.
* Firmware řídí například semafory, kalkulačky, počítačové díly (pevný disk, Wi-Fi čip), digitální fotoaparát, komponenty v PC atp.

Driver

* označení pro software, který umožňuje operačnímu systému pracovat s hardwarem.
* Některé ovladače jsou součástí operačního systému, jiné jsou distribuovány s hardwarem.

Interní rozhraní

* **Pinové headery**
  + Konektory, do kterých zapojujeme například konektory pro USB, audio a startovací tlačítka z počítačové skříně, RGB ovládání apod.
* **AGP** (Accelerated Graphics Port)
  + Zastaralé rozhraní pro grafické karty.
* **PCI-E** (Peripheral Component Interconnect Express)
  + Náhrada starší PCI a AGP
  + na rozdíl od svých předchůdců používá sériový přenos dat, díky tomu může nadále zvyšovat přenosovou rychlost.
  + Má několik různých délek (x1, x2, x4, x8, x16) pro různé typy karet.
  + má několik verzí (PCI-E 1.0 - 6.0 - rozdíly v rychlostech v jednotkách GB/s)
  + Grafické karty v dnešní době využívají výhradně x16.
* **IDE** (Integrated Drive Electronics) a **PATA** (Parallel AT Attachment)
  + Zastaralá rozhraní pro pevné disky, CD/DVD a disketové mechaniky.
  + Kšandy
* **SATA** (Serial AT Attachment)
  + Nástupce PATA, jedná se o rozhraní pro velkokapacitní paměťová zařízení jako jsou HDD, SSD, ale i mechaniky.
  + 3 verze (1,2,3) - liší se v rychlosti (v2 až 300 MB/s, v3 až 500 MB/s)
* **M.2**
  + Jedná se o rozhraní pro SSD, především NVMe, ta většinou používají PCI-E sběrnici.
  + Ačkoliv SSD v tomto portu mají limitovanou maximální kapacitu, jejich rychlost se odvíjí právě od PCI-E (rychlosti v GB/s)

Externí rozhraní

(Obraz)

* **VGA**
  + Od roku 1987, vydaný IBM
  + Přenáší analogový signál – vhodný pro CRT monitory, ale ne pro LCD
  + Není moc odolný analogovému rušení
  + Nezvládá přenést signál na delší vzdálenosti bez deformování
* **DVI**
  + Navržen pro nahrazení portu VGA
  + Nekomprimuje přenášená data, čímž se zaručuje vyšší kvalita obrazu
  + Rozšířený hlavně u LCD obrazovek a projektorů
  + Typy konektorů
    - DVI-I pro přenos digitálního i analogového signálu
    - DVI-A pro přenos analogového signálu
    - DVI-D pro přenos digitálního signálu
  + Dual Link je určen pro přenos obrazu s vysokým rozlišením
* **HDMI**
  + Vývoj začal v roce 2002
  + Nekomprimovaný přenos digitálního obrazového a zvukového signálu
  + Použití u televizí, monitorů, set-top boxů, DVD a Blue-Ray apod.
  + Vychází z rozhraní DVI
  + Dnes standard, nejpoužívanější video port
  + Nejnovější verze podporuje vysoká rozlišení obrazu, vylepšené funkce obnovovací frekvence, přenos ethernetu
* **DisplayPort**
  + Kompatibilní s HDMI a DVI
  + Od roku 2008
  + Používá se hlavně u počítačů

(Data)

* **RS-232** - sériový port
  + komunikační rozhraní osobních počítačů a další elektroniky umožňující sériovou komunikaci dvou zařízení. (myš, PDA aj.)
  + dnes nahrazeno rozhraním USB
* **LPT** – paralelní port
  + Představen v 80. letech
  + Navržen pro komunikaci s tiskárnou
  + Lze spojit PC se zařízením na max. 5 metrů
  + Lze používat i pro starší skenery, webkamery, zip mechaniky a staré zvukové karty
  + Přenosová rychlost až 12 Mbit/s
  + Nahrazeno USB
* **PS/2**
  + Představeno roku 1987
  + Pomocí tohoto konektoru se připojuje myš (zelený) a klávesnice (fialový), nelze je zaměnit
  + Při častém vypojování a zapojování může dojít k ohnutí pinů
  + Musí být připojeno před startem PC, nelze vyměnit za chodu
  + Dnes nahrazeno USB
* **FireWire** (IEEE 1394)
  + Dříve soupeř USB, dnes ho USB nahradilo
  + Používané hlavně pro přenos souborů z videokamer
  + Rychlé připojení externích disků, optických mechanik, čteček paměťových karet…
* **eSata**
  + Pro připojení externích HDD
  + Rozhraní, které podporuje stejnou technologii a nabízí stejnou rychlost jako SATA
  + Maximální délka kabelu jsou 2 metry
  + Zatěžuje méně procesor než USB
  + Nemá moc velkou podporu od výrobců základních desek, protože konektor neobsahuje vodiče s napájením, nahrazen USB
* **USB** (Universal Serial Bus)
  + První specifikace v roce 1995
  + Nahrazuje připojení pro myši, klávesnice, tiskárny, externí HDD atd.
  + Zařízení Plug & Play
  + Lze s ním tvořit stromovou strukturu (pomocí propojování zařízení)
  + Novější verze jsou zpětně kompatibilní (např. 3.2 Gen Xe{1;2}, 2.0, 1.1 - rozdíly v rychlostech)
  + Konektory jsou navrženy tak, aby je bylo nemožné zapojit obráceně, na jedné straně konektoru je USB značka, která musí mířit nahoru, pokud chcete konektor zapojit (to neplatí u USB-C)
* **Thunderbolt**
  + Konektor vizuálně stejný jako USB-C
  + kombinuje PCI-E a DisplayPort do dvou sériových signálů a poskytuje DC napětí – vše v jednom kabelu
  + Vyvinul ho Intel ve spolupráci s Applem
  + Disponuje lepšími vlastnostmi než USB 3.2 (rychlost až 40Gb/s, podpora více monitorů)

(Ethernet)

* **RJ-45**
  + Koncovka ethernetových kabelů
  + Běžně používaná pro síťové propojení, mezi PC a modemy, routery atp.
  + 8 pinů (existuje starší RJ11 se čtyřmi - pro pevné linky)
  + Používané kabely
    - UTP – nestíněná kroucená dvojlinka
    - STP – stíněná kroucená dvojlinka – každý pár kabelů je stíněný zvlášť

Zobrazovací zařízení

* Základní parametry monitorů:
  + Rozlišení
  + Obnovovací frekvence
  + Svítivost
  + Kontrast
  + Hloubka barev
  + Velikost
  + Pozorovací úhly

CRT (Cathode Ray Tube)

* Zobrazovací zařízení, které funguje na principu katodové trubice (typ urychlovače elektronů) se stínítkem, které je uzavřena do vakuové baňky.
* Obraz na monitoru vzniká pomocí vysílání tří elektronových paprsků ze tří elektronových děl, které jsou usměrňovány pomocí elektromagnetického pole vychylovacích cívek. Paprsky dopadají na stínítko potažené fosforem, elektrony díky usměrnění dopadají přesně na určené místo, které se na určitou chvíli rozzáří.

LCD (Liquid Crystal Display)

* Displej z tekutých krystalů je tenké a ploché zobrazovací zařízení skládající se z počtu barevných nebo monochromatických pixelů seřazených před zdrojem světla nebo reflektorem.
* Tekuté krystaly jsou rozmístěny pod dvěma průhlednými elektrodami a polarizačními filtry, vlivem elektrického napětí molekuly krystalů mění strukturu, díky čemuž lze regulovat průchod světla. Pixel je rozdělen do tří subpixelů (RGB), jejich kombinací vznikají miliony barev, průhlednost se ovlivňuje tranzistory; pro zobrazení je třeba pixely podsvítit (LED diody).
* Druhy: TN, VA, MVA, PVA, IPS

OLED (Organic Light-Emitting Diode)

* Typ LED diod, kde se jako elektroluminiscenční látka využívají organické materiály.
* Mezi průhlednou anodou a kovovou katodou je uloženo několik vrstev organické hmoty, ve které se přivedením elektrického napětí vyvolávají náboje, jenž produkují světelné záření. Jelikož záření vzniká přímo v jednotlivých pixelech, nepotřebují OLED displeje žádné podsvícení, díky čemuž mohou vytvářet dokonalou černou (v černém místě se pixely zhasnou), absence podsvícení také zajišťuje skvělé pozorovací úhly.

Myš

* Vstupní polohovací zařízení.
* Zajišťuje ovládání kurzoru, který se pomocí myši pohybuje po obrazovce.
* Druhy
  + Kuličkové (zastaralé)
  + S optickým snímáním polohy
* Dříve se připojovaly PS/2 portem, dnes se používá výhradně USB.

Klávesnice

* Odvozená od klávesnice psacího stroje či dálnopisu.
* Určena ke vkládání znaků a ovládání počítače.
* Dělí se podle typů spínače
  + membránové
  + mechanické
  + optické.
* Dříve se připojovaly PS/2 portem, dnes se používá výhradně USB.

Tiskárny

* Tiskárna je výstupní zařízení PC, převádějící informace z elektronické podoby na papír.
* Komunikace je zajištěna např. přes LPT, USB, LAN, Wi-Fi, Bluetooth
* Druhy
  + **Jehličková**
    - Řada 9 až 24 jehliček, vyťukává přes barvící pásku na papír jemné body, ze kterých se skládají písmena a obrázky po jednotlivých řádcích
  + **Inkoustová**
    - Tisková hlava tryská z několika desítek mikroskopických trysek na papír miniaturní kapičky inkoustu
  + **Laserová**
    - Laserový paprsek vykresluje obrázek na fotocitlivý, polovodivý (obvykle selen) válec, na jeho povrch se poté nanáší toner (jemný prach s vysokým obsahem barevného pigmentu), ten se uchytí jen na osvětlených místech, obtiskne se na papír a na závěr procesu tisku je k papíru tepelně fixován
  + Termální
    - Tisková hlava je tvořena malými odpory s malou tepelnou setrvačností, které zahřátím v určitém místě papíru docílí změny barvy
  + **3D tisk**
    - 3D tisk je proces, při kterém se prostřednictvím speciálního zařízení vytvářejí trojrozměrné objekty z vhodného materiálu, tisk po vrstvách je řízen ovládací elektronikou na základě předlohy vytvořené softwarem na počítači

Plug-n-play

* Technologie pro připojování dalších periferíí k PC
* Nepotřebuje restart systému
* Proces připojení
  + Připojení zařízení k hardwaru
  + HAL rozpozná typ zařízení
  + Nalezení ovladače
    - Linux - sysfs nebo příslušný package
    - Windows - .sys

Bluetooth

* Typ sítě - PAN (Personal Area Network - dosah cca 10m)
* Bezdrátová komunikace
* Ke spojení je nutný párovací kód (napříč např. telefony)

# Počítačové sítě, hierarchie, topologie, komunikace v síti – referenční modely a standardy

## Základní pojmy

* **Symetrický vs asymetrický přenos dat**
  + Při symetrickém přenosu dat je stejná rychlost upload/download, naopak při asymetrickém se liší.
* **Redundance**
  + nadbytečnost (označení situace, kdy je použito více prvků, než je nutné)
* **P2P** (Peer-to-Peer)
  + označení typu počítačových sítí (komunikují spolu přímo, rovnocenně jednotliví klienti)
* **Topologie sítí**
  + zabývá se zapojením různých prvků do počítačové sítě (zachycením jejich skutečné a logické podoby)
  + fyzická (rozdělení prvků do místností,...) a logická (rozdělení prvků do sítí, do VLAN,...)
* **ISP** (Internet Service Provider) - poskytovatel připojení k internetu a služeb s tím spojených
* **Server**
  + označení pro počítač, který poskytuje služby
* **Klient**
  + označení pro počítač, který využívá služby
  + druhy:
    - **Tlustý klient** (Obsáhlý klient)
      * provádí všechny operace sám (nemusí spoléhat na server - nejčastěji v podobě osobního počítače, laptopu)
    - **Tenký klient**
      * využívá zdrojů hlavně z hostitelského počítače (víceméně jen zobrazuje grafické data poskytované aplikačním serverem - vyhodou je ovladatelnost a pružnost)
    - **Hybridní klient**
      * směs modelů klienta (sám zpracovává operace, ale spoléha i na server)
* **Služba**
  + realizuje spojení a výměnu informací mezi počítači (komunikuje podle určitých pravidel, za účelem sdílení společných zdrojů nebo výměny zpráv)
* **Agregace**
  + spojování, seskupování, shlukování (udává se x:y - x → minimální podíl; y → maximální podíl z rychlosti)
* **Bezstavovost**
  + vztahuje se k implementaci protokolů (protokol je jednoduché implementovat a představuje malou zátěž pro server)
  + jednotlivé požadavky na server položené spolu nejsou nijak svázány, server neví, zda jsou od téhož uživatele, zda spolu nějak souvisejí
* **Síťová karta**
  + HW k vzájemné komunikaci v PC síti
* **Firewall**
  + kontrola a omezení komunikace počítače po síti

## Počítačové sítě

* souhrnné označení pro technické prostředky (např. PC, switch, router, kabely), které realizují spojení a výměnu informací mezi počítači (umožňuje komunikaci podle určitých pravidel - sdílení prostředků, výpočetního výkonu, výměny zpráv…)

### Součásti sítě

* Síťové uzly
  + každý uzel musí mít svojí MAC adresu nebo adresu řízení datového spoje (např. IP)
  + výkonná zařízení (servery, stanice)
  + propojovací zařízení (aktivní, pasivní)
* Síťová propojení
  + Drátově (fyzicky)
    - metalický kabel
    - optický kabel
  + Bezdrátově
    - rádiové vlny
    - satelitní/optický přenos
* Síťové služby (příklady)
  + webové
  + poštovní
  + tiskové
  + souborové
  + pro vzdálenou práci s počítačem
  + servisní
* Síťový software
  + prohlížeče internetových stránek
  + poštovní programy
  + chat
  + torrent klienty
  + firewall
  + vzdálená plocha
* Zabezpečení sítě
  + skrytí SSID
  + firewall
  + filtrování MAC adres
  + statické IP adresy
  + šifrování komunikace pomocí min. WPA2 nebo WPA3
  + rozdělení sítě na VLANy
* Sledované vlastnosti sítě
  + způsob přenosu signálu
  + bezpečnost
  + instalační požadavky
  + šířka pásma
  + útlum
  + vzájemné ovlivňování a rušení (EMI)
  + aktivní síťové prvky
  + cena

### Typy vzajemných vztahů stanic v síti

* Client-Server
  + odděluje klienta a server (komunikují přes počítačovou síť)
  + při vyšším počtu klientů klesá průměrná přenosová rychlost
  + nejčastější klienti jsou dnes webové prohlížeče (Chrome, Brave, Firefox)
  + klient (aktivní, posílá žádosti serveru, čeká a dostává odpovědi) X server (pasivní, naslouchá síti/reaguje na žádosti, při přijetí požadavku jej obslouží)
* P2P
  + např. sdílení složek v místnosti se vzájemně propojenými počítači
  + torrent, blockchain
  + při vyšším počtu roste přenosová kapacita

### Hierarchický model sítě

* propojení zařízení v menší nebo střední firmě
* zajišťuje přehledný chod sítě, rychlejší opravy, snadně se síť spravuje
* dovoluje efektivně přidělovat adresy a lehce je sumarizovat (zpřehledňuje toky dat)
* spočívá v rozdělení sítě na samostatné vrstvy (zajištěna modulárnost)
  + **Přístupová vrstva**
    - obsahuje koncová zařízení (PC, tiskárny, IP telefony)
    - poskytuje přístup do zbytku sítě (obsahuje směšovače, přepínače, bridge a přístupové body - AP)
    - hlavním účelem je připojit koncová zařízení k síti a kontrolovat, která zařízení mají povoleno v síti komunikovat
  + **Distribuční vrstva**
    - agreguje (slučuje) datový provoz, kontroluje síťový provoz lokální sítě
    - v této vrstvě nalezneme obvykle velmi výkonná zařízení (mají vysokou dostupnost a redundanci k zaručení bezporuchovosti)
  + **Jádro**
    - představuje vysokorychlostní páteř sítě
    - musí být velmi spolehlivá
    - je připojena k Internetu (často více linkami - musí být schopna posílat velký objem dat velmi rychle)

### Základní topologie sítě

* Sběrnicová topologie (**BUS**)
  + nejjednodušší způsob zapojení počítačů do sítě (skládá se z jediného kabelu hlavní kabel/segment/páteř, která propojuje všechny PC)
* Kruhová topologie (**RING**)
  + propojuje počítače pomocí kabelu v jediném okruhu (neexistují zakončené konce - signál putuje po smyčce v jednom směru a prochází všemi PC)
* Hvězdicová topologie (**STAR**)
  + každý počítač je připojený pomocí kabelu k centrálnímu prvku (mezi dvěma stanici existuje vždy jen jedna cesta)
* Stromová topologie (**TREE**)
  + vychází z hvězdicové topologie spojením aktivních síťových prvků
* Smíšená topologie
  + spojení více topologii do jednoho funkčního celku (např. TREE + STAR)

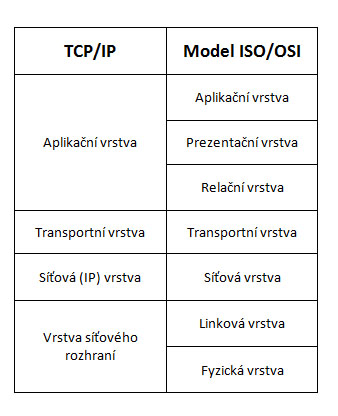
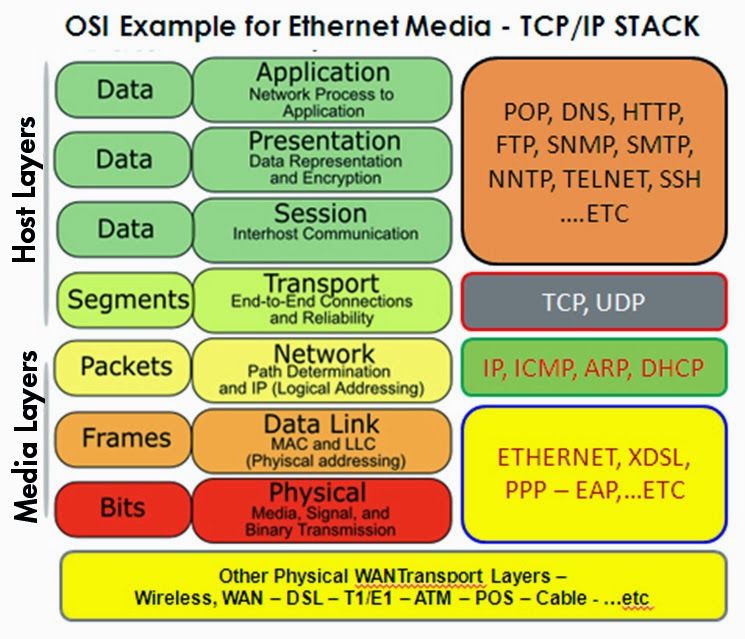
### Logické topologie sítě

* **Token ring**
  + Používají token -> kdo má token může komunikovat, pokud nepotřebuje posílá dál
  + V síti musí být řídící prvek - klasická máma, chápeš ne?
* **Ethernet**
  + Dva spolu komunikují, pokud dojde k chybě (např. rušení jiným prvkem), je komunikace na domluvenou dobu přerušena, dokud se neuvolní pásmo
  + Vinnetou, Old Shatterhand a ukecaná Ribana

### Síťové modely

* souhrn pravidel a úmluv - standardizace prvků sítě např.
  + standard pro podobu a tvorbu kabelů a konektorů
  + standard pro stanovení napěťové úrovně logické 0 a logické 1
  + protokol pro opravu chyb
  + protokol pro zasílání požadavků a příjem souborů ze serveru
  + protokol pro přenos dat mezi klientem, serverem a klientem
  + protokol pro internetové telefony
* příkladem je např. ISO/OSI (spíše teoretický) či TCP/IP (praktický)

#### **ISO/OSI a TCP/IP model**

Aktivní a pasivní síťové prvky, typy, parametry, konfigurace

Pojmy

* **Útlum**
  + ztráta signálu vedením
* **EMI** (elektromagnetická interference)
  + negativní vnější vliv
* **Terminátor**
  + ukončující spoj koaxiálního kabelu
* **Síťový uzel**
  + zařízení v počítačových sítích, které je připojeno jako součást počítačové sítě (počítač, server, mobilní telefon)
* **Propojovací zařízení**
  + aktivní či pasivní prvky sítě, zajišťující vzájemné propojení a provoz sítě (switch, router, bridge)
* **LAN**
  + lokální počítačová síť (uvnitř firem, budov, kanceláře, domácnosti)
  + skládá se z připojených zařízení, z rozvodů signálu a aktivních prvků (nejdůležitější je router - primárně pro komunikaci ven)

Aktivní síťové prvky

* pracují přímo s paketem a signál nějakým způsobem zpracovávají tzn. mění
* Výčet aktivních zařízení
  + **Repeater** (opakovač)
    - přijímá data na úrovni fyzické vrstvy, modulovaná a zesílená je posílá dál
    - slouží jako digitální zesilovač (zesiluje signály, tvaruje signály)
    - je možné umístit maximálně dva mezi uzly
  + **Switch** (přepínač)
    - síťový provoz je "inteligentně" směrován od odesílatele k adresátovi
    - linková vrstva (inteligentní varianta mostu)
    - síťová vrstva (rychlý směrovač, v síti lze adresovat)
    - lze ho brát zároveň jako pasivní prvek, jelikož dokáže směrovat provoz k adresátovi
  + **Bridge** (most)
    - spojuje dvě části sítě na linkové vrstvě (odděluje provoz různých segmentů sítěí)
    - lze využít pro spojení sítí s různou technologií (sám se učí topologie sítě)
  + **Router** (směrovač)
    - spojuje dvě sítě a přenáší mezi nimi data (úroveň síťové až aplikační vrstvy)
    - zná topologii sítě (v síti lze adresovat)
    - rozhoduje o směrování paketů v síti nebo ven ze sítě (zajišťuje NATování)
  + **Modem** (modulátor-demodulátor)
    - převod mezi analogovým a digitálním signálem
    - přenosová trasa může být telefonní linka, koaxiální kabel, rádiový přenos…
    - modemy pro širokopásmové kabelové připojení k internetu - CableDSL
    - modemy pro širokopásmové telefonní připojení k internetu - ADSL
    - GSM, UMTS modem/karta pro datové propojení přes síť GSM, UMTS viz připojení do digitální telefonní sítě
    - terminálové adaptéry - TA někdy též nesprávně zvané “ISDN modemy” pro připojení do digitální telefonní sítě
  + **Firewall** (hořící stěna 🥱)
    - slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení
      * Paketové filtry
      * Aplikační brány
      * Stavové paketové filtry
      * Stavové paketové filtry s kontrolou známých protokolů a popřípadě kombinované s IDS

Pasivní síťové prvky

* zajišťují pouze přenos signálu
* síťové propojení (kabeláž, konektory, Wi-Fi, vysílač, Hub)
* Výčet pasivních zařízení
  + **Hub** (rozbočovač)
    - data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny porty
    - úroveň fyzické vrstvy
    - lze rozšířit počet připojených větví pomocí spojování (kaskádování, stohování, stromová struktura)
    - v dnešní době existují rozbočovače, které patří mezi aktivní síťové prvky, jelikož jsou součástí jiného síťového prvku a jsou daleko modernější
  + **Metalické spoje** (většinou měď)
    - Druhy
      * **Kroucená dvoulinka**
        + levná, dosah maximálně 100m
        + problémy s odolností vůči elektromagnetickému záření, mechanické poškození
        + třídy kvalit 1-8.2 (běžně Cat5e nebo Cat6)
        + Druhy

nestíněná **UTP** (Unshielded Twisted Pair)

nestíněný kabel, velmi oblíbený

stíněná **STP** (Shielded Twisted Pair)

stíněný kabel, větší odolnost vůči rušení

stíněná FTP (Foiled Twisted Pair)

stíněná kroucená dvojlinka, stínění je kolem všech párů kabelu

* + - * **Koaxiální kabel**
        + velmi levný (maximální přenosová rychlost 40Mb/s)
        + dobře odstíněn, ale běžně nepoužitelný kvůli náročnosti tvorby koncovky
        + využit např. pro satelitní příjem pro TV
        + typy (Tlustý 10Base-5, Tenký 10Base-2)
  + **Optické spoje**
    - přenosová rychlost v rozsahu 10Gb/s - 111Gb/s
    - typy vláken (potřebuje revizi)???????????
      * mnohovidové vlákno
        + signál tvořen LEDkou
        + tvořeno z plastu
      * jednovidové vlákno
        + signál tvořen laserem
        + tvořeno ze skla
    - vyšší náklady na instalaci
    - velmi vysoká odolnost vůči EMI
  + Další možnosti propojení
    - mikrovlnný přenos
      * volné pásmo 10-155 Mb/s, licencované pásmo 10-900 Mb/s
      * přenos pomocí parabol
    - **Wi-Fi**
      * má několik typů - dnes nejrychlejší Wi-Fi 6 (maximální rychlost 9600 Mbit/s)
    - WiMax
      * přenos na 40-70 km (není nutná přímá viditelnost, 70 Mb/s)
    - **Bluetooth**
      * frekvenční pásmo 2,4 GHz (rychlost až 50 Mbit/s)
      * dělí se na třídy a verze
    - optický bezdrátový přenos (infračervený, laserový)
      * infračervený (laserový), maximální rychlost až 2,5G b/s
      * podmínkou je přímá viditelnost na 500m-5km (bezpečný a bez vzájemného rušení)

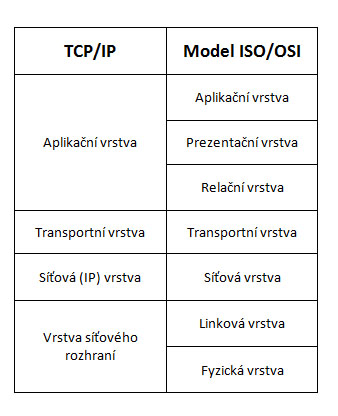
# TCP/IP, síťové služby a jejich konfigurace

## TCP/IP (Transmission Control Protocol/Internet Protocol)

* rodina protokolů TCP/IP obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet (od sdružení IET)

### Architektura

* je rozdělena do několika vrstev, komunikace mezi vrstvami je přesně definována
* každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší
* model TCP/IP je oproti ISO/OSI zjednodušený (na model TCP/IP se lépe aplikovali nové standardy a tím se prosadil)



#### **Aplikační vrstva**

* jedná se o protokoly, které slouží k přenosu konkrétních dat (FTP, HTTP, POP3, IMAP, SMTP, SSG, HTTPS, DHCP, DNS, SSH)
* doplnit porty u těchto služeb????????????

##### **DHCP (Dynamic Host Configuration Protocol)**

* umožňuje dynamické přidělování IP adres (+ masku, default gateway, DNS) počítačům na předem určenou dobu
* výhodou je bezpečnost, snadnost konfigurace, prevence konfliktů adres
* funguje ve čtyřech krocích
  + **DISCOVER** (počítač vyšle L2 broadcast, který vyhledá DHCP server)
  + **OFFER** (DHCP obdrží požadavek a rezervuje IP adresu pro klienta, tu vysílá na unicast klientovi)
  + **REQUEST** (Klient vyšle L2 broadcast (musí dát vědět i ostatním DHCP serverům o zapůjčení IP) s žádostí o přidělení nabídnuté adresy)
  + **ACK** (server posílá unicast zprávu ACK se souhlasem k používání vybrané adresy)

##### **DNS (Domain Name Server)**

* hierarchicky distribuovaná databáze
  + hierarchická (rozdělá do sobě nadřazených skupin - domény a subdomény)
  + distribuovaná (rozmístěna na více místech - name servery)
* jeho hlavnímí úkoly a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě
* např. pes.seznam.cz - nejprve se vyhledá skupina .cz, ve které se nalezne .seznam, ve které se nalezne pes - toto se poté převede na IP

##### **Telnet (Telecommunication Network)**

* umožňuje připojení ke vzdálenému počítači (absence šifrování dat, dnes nahrazen protokolem SSH)

##### **SSH (Secure Shell Protocol)**

* kryptografický protokol, který umožňuje bezpečné připojení i přes nezabezpečenou síť (náhrada za Telnet)

##### **FTP (File Transfer Protocol)**

* protokol pro přenos mezi klientem a serverem (nejčastěji se využívá pro sdílení dat - hudba, videa - a správu účtů internetových stránek)
* výhodou jsou možnosti nastavení práv, mazání, upload
* nevýhodou jsou hesla a soubory, která jsou zasílána jako běžný text -> FTPS, má delší odezvy

##### **HTTP (Hypertext Transfer Protocol)**

* internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML
* neumožňuje šifrování ani zabezpečení integrity dat
* zabezpečená alternativa je HTTPS (ta umožňuje ověřování identity protistrany)

##### **Poštovní protokoly**

###### **POP3 (Post Office Protocol)**

* slouží k přijímání elektronické pošty poštovním klientem (nelze pracovat s poštou na poštovním serveru, umožňuje stažení, přečtení a smazání pošty)
* ze vzdáleného serveru se všechny emaily stahují na zařízení, tím pádem funguje i offline

###### **IMAP (Internet Message Access Protocol)**

* slouží k přijímání elektronické pošty poštovním klientem (podporuje práci na poštovním serveru, vyžaduje trvalé připojení sítě, umožňuje připojení více uživatelů najednou)

###### **SMTP (Simple Mail Transfer Protocol)**

* slouží k odesílání elektronické pošty poštovním klientem (protokol zajišťuje doručení pošty pomocí přímého spojení mezi odesílatelem a adresátem)
* jeden z nejstarších protokolů určených pro elektronickou poštu

#### **Transportní vrstva**

* implementována až v koncových zařízeních (provádí převod adres na síťové, nestará se o směrování - NetBEUI, TCP, RTP, AppleTalk)

##### **TCP**

* zajišťuje spojení mezi propojenými počítači (opravuje chyby, součástí paketu je hlavička)
* spolehlivý, drží relaci, pokud příjemci data nepřijdou, posílají se znova

##### **UDP**

* je vhodný pro nasazení, které vyžaduje jednoduchost, nebo pro aplikace pracující systémem otázka-odpověď (DNS, sdílení souborů v LAN)
* jeho bezstavovost je užitečná pro servery, které obsluhují mnoho klientů nebo pro nasazení, kde se počítá se ztrátami paketů, není vhodné, aby ztrácel čas odesíláním nedoručených zpráv (VoIP, online hry, stream videa)

###### **Porty**

* využívány především protokoly TCP a UDP - jednoznačně identifikují službu na zařízení, která komunikuje
* kladné 16bitové číslo
* celkový rozsah portů je 0-65535 (port 0 je rezervován pro odesílající proces - neočekává odpověď)
* porty jsou rozčleněny do třech skupin
  + dobře známé (1-1023, porty různých základních/známých protokolů)
  + registrované (1024-49151, porty přiřazené společností IANA specifickým službám)
  + dynamické/privátní (49152-65535, porty privátní pro identifikaci např. v lokální síti)

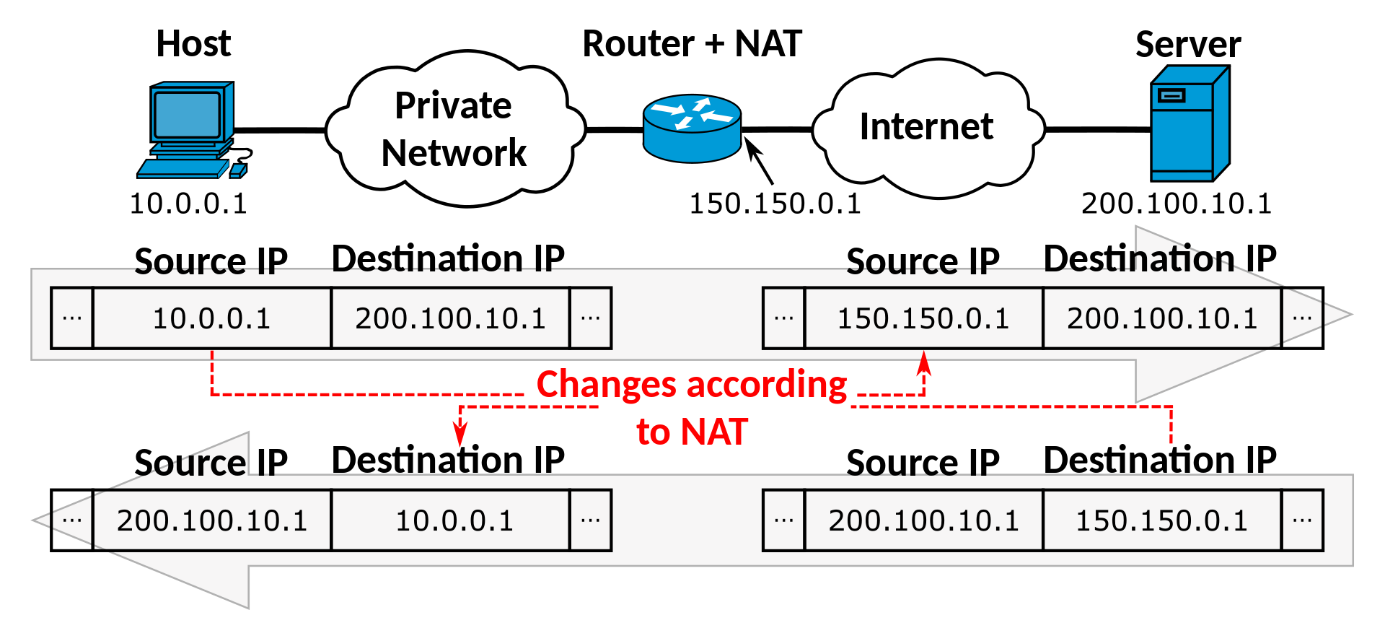
#### **Síťová vrstva**

* stará se o směrování v síti a síťové adresování (poskytuje spojení mezi systémy, které spolu přímo nesousedí)
* obsahuje funkce, které umožňují překlenout rozdílné vlastnosti technologii v přenosových sítích (IP, IPsec, ARP, RARP, ICMP, IGMP, IGRP)

##### **IP**

* je základní protokol síťové vrstvy a celého Internetu
* definice logického adresování a směrování
* vysílá pakety na základě IP adres obsažených v jejich záhlaví (každý paket je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesílateli)
* doručení paketu není zaručeno (spolehlivost musí zajistit vyšší vrstvy TCP)
* způsob komunikace
  + každé síťové zařízení komunikuje prostřednictvím IP (zařízení musí mít unikátní identifikátor - IP adresu)
  + na základě těchto adres pak router rozhoduje, kam paket pošle (routing)
* využívá IP adresy
  + **IPv4** = **32bit**
  + **IPv6** = **128bit** (snadnější automatická konfigurace, vyšší bezpečnost, velký rozsah adres)

###### **NAT (Network Address Translation)**

* způsob úpravy síťového provozu procházejícího přes router přepisem zdrojové nebo cílové IP adresy (prostě překlad adres)
* většinou používán pro přístup více počítačů z lokální sítě do internetu prostřednictvím jediné veřejné IP adresy 

##### **ARP (Address Resolution Protocol)**

* používá se pro získání MAC adresy sousedního stroje z jeho IP adresy (používá se v situaci, kdy je třeba odeslat paket na adresu ležící ve stejné podsíti jako odesilatel - data se tedy pošlou přímo adresátovi, u něhož však odesilatel zná pouze IP adresu), pro odeslání potřebuje znát cílovou adresu

##### **RIP (Routing Information Protocol)**

* směrovací protokol umožňující routerům komunikovat mezi sebou a reagovat na změny topologie počítačové sítě (sběrnicová, kruhová, hvězdicová)

##### **ICMP**

* jeden z nejdůležitějších protokolů (používají ho operační systémy počítačů v síti pro odesílání chybových zpráv - služba není dostupná, počítat nebo router není dosažitelný)

#### **Vrstva síťového rozhraní**

* poskytuje spojení mezi dvěma sousedními systémy (switch-PC)
* seřazuje a formátuje přenášené pakety a opatřuje jim MAC adresu (stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby)
* Podvrstvy
  + **LLC** (Logical Link Control)
    - umožňuje použití několika síťových protokolů v jedné síti
    - řídí tok a zabezpeření proti chybám
    - není hardwarově závislá
  + **MAC** (Media Access Control)
    - umožňuje přístup k fyzickému přenosovému médiu - Ethernet, Token ring, FDDI, 100BaseVG, X.25, SMDS

## Druhy vysílání

### Unicast

* zasílá zprávu pouze jedinému cíli

### Multicast

* zpráva je zaslána z jednoho zdroje skupině více koncových stanic

### Broadcast

* zpráva, kterou v síti přijmout všechna připojená síťová rozhraní (šíří se tak například informace o sdílení nebo identifikace zařízení)
* L2 Broadcast
  + datový rámec je přijat všemi síťovými zařízeními ve stejném segmentu sítě (segment je ohraničen routerem)
  + tento broadcast tedy projde přes switch i hub

# Návrh a realizace jednoduché sítě, připojení počítače k lokální síti

## Druhy počítačové sítě

### PAN (Personal Area Network)

* osobní síť pro připojení elektronických zařízení (počítač x tiskárna - BlueTooth/Wi-Fi, připojení přes USB)
* dosah cca 10m

### LAN (Local Area Network)

* sítě pokrývající oblast několika místností, maximálně budov (učebna, škola, společnost - metalické spoje, bezdrát)
* dosah cca 100m

### MAN (Metropolitan Area Network)

* rozšiřuje působnost sítě LAN (poskytovatelé internetového připojení - dalekosáhlý bezdrát, optika)

### WAN (Wide Area Network)

* sítě pokrývající většinu území (za hranice města - mobilní operátoři)

## Podle čeho se řídit při návrhu počítačové sítě

* musíme si ujasnit k čemu budeme síť využívat (dnes nemusí sloužit jen k připojení PC - můžeme díky ní využívat chytrá zařízení jako TV, tiskárnu, vlastní síťové uložiště... )
* Pro návrh topologie lze využít buď papír nebo specializovaný software (Páča Tráča \*mucq\*)

### Sledované vlastnosti při návrhu sítě

#### **Přenos signálu**

* elektromagnetické vlnění, viditelné světlo, infračervené světlo, mikrovlny, radiové vlny

#### **Instalační požadavky**

* musíme brát v potaz vlastnosti budovy, místnosti (kde budeme síť realizovat)
* množství uvolněných prostředků na realizaci a co budeme od sítě očekávat

#### **Šířka pásma**

* kapacita média (kolik je možné po médiu přenést dat)

#### **Útlum**

* slábnutí signálu při přenosu po médiu (rozdíl napětí na jednom konci vedené oproti druhému konci - čím menší útlum, tím kvalitnější a přesnější přenos signálu)
* hodnota útlumu u křemenných vláken (skleněná optika) se řadově pohybuje v desetinách decibelu na kilometr (plastová vlákna mají útlum větší)

#### **Vzájemné ovlivňování (NEXT-near-end-crosstalk)**

* NEXT je hodnota, která určuje, jak hodně je připojení odolné proti crosstalku
* čím vyšší hodnota NEXT, tím více je připojení odolné na crosstalk.
* Označuje se jako near end (“ke konci”), protože interference mezi dvěma signály v kabelu se měří na stejném konci kabelu jako rušivý vysílač.

#### **Elektromagnetická interference (EMI)**

* signál/emise, vysílané/vyzařované do volného prostoru nebo vedené podél napájecích či signálních vodičů, vedoucí k ohrožení/zhoršení správné funkce rádiové navigace či jiné bezpečnostní služby

#### **Elektromagnetická kompatibilita (EMC)**

* spočívá v tom, že neovlivňuje jiný objekt včetně sebe samotného a odolává působení ostatních přístrojů

#### **Rozsah sítě**

* dle její velikosti správně volíme jednotlivé uzly a technologie k její správné funkčnosti

## Kroky realizace počítačové sítě

* zjištění nároků klienta na síť
* nákup komponent
* instalace síťových komponent/programového vybavení
* nastavení sítě (sdílení prostředků, ochrana sítě)

## Konfigurace síťového prvku (Windows)

### Kontrola HW

* ve správci zařízení ověříme funkčnost síťového adaptéru
* provedeme fyzické připojení, zpravidla pomocí kabeláže
* v OS provedeme IP konfiguraci

### Nastavení jména PC

* zjistíme a nadefinujeme jméno počítače (musí být unikátní), provádíme ve vlastnostech systému

### Nastavení domény či pracovní skupiny

Bezdrátové technologie, parametry, konfigurace

Pojmy

* **Bezdrátová síť**
  + Bezdrátová síť je typ počítačové sítě, ve které je spojení mezi jednotlivými účastníky sítě uskutečňováno pomocí bezdrátové komunikace.
* **Mobilní síť**
  + Mobilní síť je telefonní síť, jejíž uživatel není vázán na místa, kde je k dispozici telefonní přípojka.
  + Telefonní přístroj komunikuje se sítí pomocí rádiových vln.
* **Pásmo**
  + rozsah frekvencí nebo skupinu rozsahů frekvencí
* **Licencované a bezlicenční pásmo**
  + Bezlicenční pásma jsou pásma pro rádiové vysílání v oboru průmyslovém, vědeckém a zdravotnickém - tyto sektory se musí řídit nařízeními ČTÚ (Český telekomunikační úřad).
  + Na licenční pásmo je potřeba licence od ČTÚ, většinou tato pásma slouží k širšímu použití v celoplošných sítích národního měřítka.
* **xG, kde x∈<1,5>** (Generace x)
  + Rozlišení mobilních systémů, využívající různých standardů a technologií
  + Číslo označuje verzi systému (v některých případech můžeme u technologií vyššího typu nalézt odkaz na starší technologie v kombinaci s novou, např. 3G, 5G)
* **Ad-hoc sítě**
  + Decentralizovaná síť, ve které se navzájem spojuje více klientů, kteří jsou v rovnocenné pozici
  + Vzájemná identifikace probíhá pomocí SSID
  + Oba body musí být v přímém rádiovém dosahu

Bezdrátová technologie

* Bezdrátová komunikace spočívá ve spojení dvou subjektů jiným způsobem, než mechanicky (kabelem).
* Podle typu nosného média můžeme rozlišovat mezi komunikací optickou (světlo), rádiovou a sonickou (zvuk).
* Vzdálenost mezi komunikujícími body může být od několika metrů (infračervený ovladač televize) do milionu kilometrů (komunikace družic v kosmickém prostoru).

Členění dle velikosti

* Soukromé sítě (WPAN – Wireless Personal Area Network)
  + Bluetooth
* Místní sítě (WLAN – Wireless Local Area Network)
  + Lokální síť v rámci jedné budovy nebo několika blízkých budov ve vzdálenosti stovek metrů až km
* Metropolitní sítě (WMAN – Wireless Metropolitan Area Network)
  + obvykle zasazená do města - spojení více menších sítí
* Rozsáhlé sítě (WWAN – Wireless Wide Area Network)
  + Rozlehlá síť, spojuje LAN sítě na libovolné vzdálenosti (stát, státy, kontinent)

Členění dle mobility

* Mobilní
  + umožňují transparentní pohyb uživatele a jeho zařízení v rámci jedné bezdrátové sítě i mezi sítěmi.
  + V LAN zajištěno např. pomocí APček a Controlleru (WLC)
  + Příkladem také může být mobilní síť - při telefonování nemusíme staticky stát na místě, můžeme se pohybovat
* Fixní
  + umožňují pouze „pevné bezdrátové“ připojení k dané síti
  + Příkladem lze uvést bezdrátové připojení k ISP

Členění dle šířky pásma

* Úzkopásmové
* Širokopásmové

Členění dle typu signálu

* Rádiové sítě
  + nejčastější, mají malý až střední dosah (jednotky až stovky metrů)
  + vhodné pro domácí i podnikové sítě.
* Infračervené sítě
  + malý dosah s neprůchodností neprůhledných překážek.
  + vzniká omezení na prostor mezi zdmi, ale zároveň větší bezpečnost vůči možnému odposlechu.
* Optické bezdrátové sítě
  + velký dosah, rozumíme stovky metrů, v přímé viditelnosti.
  + Vysoká kapacita přenosu dosahující rychlostí světla.
  + Řešení vhodné pro podnikové sítě a komunikaci mezi budovami nebo pro sítě domácí sloužící pro přístup k Internetu.

Bezdrátové standardy

IEEE 802.11 (Wi-Fi)

* Wi-fi Standard pro lokální bezdrátové sítě (WLAN).
* Využití bezlicenčního frekvenčního pásma (2,4 i 5 GHz)
* Levná, ale výkonná síť
* Nejpoužívanější modulace jsou 802.11a, 802.11b, 802.11g a 802.11n.
* Nejnovějším standardem je 802.11ax (označováno jako WiFi 6 - rychlost až 9600 Mbit/s)

Bluetooth

* Standard IEEE 802.15.1
* Komunikace na krátké vzdálenosti (do 100 m; u Bluetooth 5.0 až do 400 m)
* Typ sítě: PAN
* Zabezpečení probíhá přes párování – uživatel musí u obou zařízení potvrdit žádost o párování, které si mezi sebou vymění klíč, díky kterému si potom mezi sebou posílají data
* Pro minimalizaci rušení využívá FHSS (Frequency Hopping Spread Spectrum) – pravidelně provádí změnu frekvence

GSM (Global System for Mobile Communications)

* Druhá generace celulární radiové sítě (2G)
* Mobilní síť
* Registrace zařízení do sítě pomocí SIM karty
* Vysoká dostupnost v ČR

GPRS (General Packet Radio Service)

* Datová mobilní síť
* Přenos dat pomocí GSM
* Nízká přenosová rychlost, poměrně vysoká latence

ZigBee

* Pro komunikaci vytváří síť velikosti PAN (podobá se Bluetooth)
* Určeno pro spojování nízkovýkonových zařízení na krátké vzdálenosti – do 100 metrů
* Využití
  + Automatizace budov (ovládání světel, zabezpečení, …)
  + Počítačové periferie (bezdrátové myši a klávesnice, …)
  + Průmyslová automatizace

NFC (Near Field Communication)

* Komunikace na velmi krátkou vzdálenost – cca 4 cm
* Možnost komunikace buď se dvěma aktivními body (např.: 2 mobilní telefony), tak i s jedním aktivním a jedním pasivním bodem (platební terminál a bezkontaktní platební karta)
* Využití: bezkontaktní transakce, zjednodušená konfigurace spojení např. s Wi-Fi, vstupní čipy do budovy

RFID (Radio Frequency Identification)

* Vysílače (čtečky) opakovaně vysílají do okolí elektromagnetické pulsy. - Pasivní RFID čip si touto energií dobije kondenzátor a odešle odpověď.
  + Odpověď může být např. jedno číslo (např.: elektronické číslo produktu v obchodě, …)
* Aktivní RFID čipy – vysílají svou identifikaci bez nutnosti dobití kondenzátoru přes čtečku
* např.: elektronické peněženky, Pardubická karta, …

WiMAX

* Standard 802.16
* Levný a jednoduše rozšiřitelný (40 - 70 km)
* Přenosová rychlost 70 Mb/s
* Není nutná viditelnost

Souborové zdroje v síti, správa dat pomocí NTFS teorie/praxe

Pojmy

* **Cluster**
  + Minimální jednotka uložení dat v souborovém systému. Jeden cluster obsahuje pevný počet sektorů.
* **Vlastník**
  + Osoba, která soubor či složku vytvořila. Má právo povolit nebo odepřít přístup.
* **Převzetí vlastnictví**
  + Administrátor může odebrat práva vlastníkovi.
* **Oprávnění**
  + Určení přístupu k souborům a adresářům. Slouží pro zabezpečení.
* **Dědičnost**
  + Vnořené složky a soubory dědí oprávnění složky nadřazené.
* **Autentizace**
  + Ověření identity uživatele (kdo je to)
* **Autorizace**
  + Ověření práv uživatele (co může)
* **Kvóty**
  + Limity nastavené správcem systému. Určitým způsobem omezují použití souborového systému uživateli na základě nastavené kvóty.
* **Metadata**
  + Data, která poskytují informace o jiných souborech.

Souborový systém

* označení pro způsob organizace dat ve formě souborů tak, aby k nim bylo možné uživatelsky přistupovat
* je uložen elektronické paměti, která je umístěna přímo v počítači
* software, který realizuje souborový systém, je obvykle součástí OS
* Všechny soubory musí být v souborovém systému
* složky se soubory tvoří stromovou strukturu
* Příklady souborových systémů (+ běžná vazba na OS)
  + Linux – ext2, ext3, ext4, btrfs, zfs
  + Windows – NTFS
  + Windows Server – ReFS
  + macOS – HFS, HFS+, APFS
* souborový systém obvykle disponuje:
  + dědičností oprávnění
  + žurnálováním
  + virtuálním file systémem
* typy objektů souborového systému (popsat pipe, socket)
  + **soubor** (datový typ)
    - standardní vlastnosti
      * název
      * typ souboru
      * cesta k souboru
      * velikost
      * metadata a atributy
        + běžná (datum vytvoření atp.)
        + oprávnění
  + **složka**
  + **Pipe**
    - Přeposlání výstupu jednoho programu do druhého
    - Příklad:
      * příkaz grep dokáže fitrovat řádky
      * příkaz less dokáže zobrazit skrolovatelný výstup příkazu
  + **Socket**
    - Je to virtuální soubor, který umožňuje síťové spojení
    - Napadá mě, třeba, že příkaz docker komunikuje s backendem právě pomocí socketů. Když služba dockeru neběží, socket neexistuje a při spuštění příkazu docker ... vyhodí chybu: *Cannot connect to the Docker daemon at unix:///var/run/docker.sock. Is the docker daemon running?*
* Smazání souboru - smaže se pouze reference z tabulky filesystému, ne fyzicky z disku (k tomu musí být přepsán)
* Vypuštění souboru - odstraní se obsah souboru, ale atributy se nechají (např. PDFko s knihou - smaže se veškerý text, nechají se jen atributy jako datum vytvoření atp.)

NTFS (New Technology File System)

* označení pro souborový systém, který vyvinula firma Microsoft pro svoje operační systémy řady Windows NT
* navržen na konci 80. let 20. století jako rozšiřitelný souborový systém, který je možné přizpůsobit novým požadavkům
* při vývoji NTFS Microsoft vycházel z vývoje HPFS, na kterém spolupracoval s společností IBM
* Vlastnosti
  + **žurnálování**
    - změny souborů na disku se zaznamenávají do speciálního souboru (žurnál)
    - jeho účelem je ochránit data před ztrátou integrity
  + **access control list**
    - podpora pro přidělování práv k souborům
  + **komprese**
    - z podstaty samozřejmě bezztrátová
  + **šifrování**
    - umožňuje chránit data uživatele
  + **diskové kvóty**
    - umožňují nastavit místo na diskovém oddílu (pro uživatele)
  + **podpora dlouhých jmén souborů**
  + **pevné a symbolické linky**
    - odkaz na soubory na úrovni filesystémů
* Důvody použití NTFS
  + kontrola přístupu k souborovým datům
  + řízení přístupu ostatním
  + zamezení náhodného odstranění
* Oprávnění k souboru/složce (dále jako objekt)
  + Atributy (teor. metadata) souborů, které jsou obsaženy v tomto souborovém systému
  + můžeme měnit, pokud je sdílená složka umístěná na svazku naformátovaném na NTFS, FAT nebo FAT32
  + pro změnu potřebujeme mít pro svazek dostatečné oprávnění – být členem skupiny Administrators nebo Power Users (Win)
  + Základní typy oprávnění pro objekt
    - **Full Control** – čtení, spuštění, úpravy, mazání a nastavení oprávnění
    - **Modify** – čtení, spuštění, úpravy a mazání
    - **Read & Execute** – čtení a spuštění
    - **List Folder Content** – zobrazení obsahu adresáře
    - **Read** – čtení
    - **Write** – čtení a úpravy
    - **Oprávnění ke zvláštnímu přístupu**
  + Nastavení oprávnění pro objekt
    - oprávnění na souboru nebo složce může být přímo nastavené nebo zděděné
    - oprávnění, které je zděděné není možno smazat – pokud ho chceme upravit, je potřeba zrušit dědění
    - při nastavování oprávnění složky se standardně dědí na nižší úrovně
    - práva můžeme nastavovat pomocí hodnoty povolit a odepřít – odepření má vždy větší váhu
* Sdílení
  + sdílení znamená, že je možné k souborům přistupovat z jiného počítače
  + účelem je snížení nákladů na pořízení zařízení nebo usnadnění správy pomocí centralizace
  + využívá se pro vytvoření infrastruktury mezi počítači bez využití externí cloudové služby
  + Sdílet lze
    - Soubory
    - Složky
    - Tiskárny
    - Připojení k internetu
    - Počítače
  + Oprávnění na úrovni sdílení dáváme úplné řízení pro skupinu everyone a přístup jednotlivým uživatelům omezujeme až prostřednictvím oprávnění na úrovni NTFS.
  + Administrátorské sdílení
    - přístup do složek potřebných pro administraci
    - tyto složky jsou standardně nepřístupné
    - administrátor má v těchto složkách Full control
    - skryté (administrátorské) sdílení provedeno znakem dolaru $ na konci názvu objektu
* Parametry kvóty
  + **hard limit**
    - maximální možné obsazení diskového prostoru, nad tuto hranici není možné nic uložit.
  + **soft limit**
    - hranice nižší než u hard limitu, lze ji překročit, poté bude uživatel varován a poběží mu grace period.
  + **grace period**
    - uživatel může dočasně uložit na disk více, než je uvedeno v parametru soft limit na dobu zadanou parametrem grace period. Po uplynutí této doby se uživateli nepodaří na disk uložit více, i když ještě nepřekročil hodnotu zadanou parametrem hard limit.

Doména X Workgroup

* Doména síťová X lokální
* Doména je hostována na Serveru s Active Directory

NTFS

* Stromová struktura
* Windows X Linux (lseek)
* Kvóty

File servery

* Kvóty
* Přístupy
* SMB (pro Windows), FTP (většinou pro hosting), NFS (pro Linux)

Zabezpečení v sítích LAN, bezpečnostní model, zpracování autorizace, bezpečnost VPN

Pojmy

* Hacker
  + osoba, která využívá své počítačové znalosti k tomu aby narušila počítačovou síť nebo se dostala k citlivým informacím
  + existují druhy hackerů
    - **Whitehat** (*Hodnej*)
      * hovorový název hackera nebo specialisty na počítačovou bezpečnost, který se zaměřuje na penetrační a další testy pro zajištění bezpečnosti informačních systémů (získaná data nezneužívá, naopak hledá bezpečností chyby)
    - Grayhat
      * cracker, který získaná data nezneužívá a informuje administrátora systému o bezpečnostní chybě
    - **Blackhat** (neboli Cracker - *Zlej*)
      * působí škody vůči ostatním či firmám (lze posuzovat jako trestní čin)
      * využívá průniků ke kriminální činnosti
    - Blue hat
      * bezpečností specialisté z firem zabývajících se bezpečností počítačových sítí a poradenstvím
      * hledají a testují chyby systémů a zajišťují jejich nápravu
      * Microsoft tak začal nazývat white hat hackery, které si pozval na testování softwaru, např. Windows
* Sociální inženýrství
  + způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace (je účinná, propracovaná, plánovaná)
* Kryptografie
  + obor, zabývající se šifrováním a metodami šifrování (využívá algoritmy k šifrování a dešifrování dat)
* Bezpečnostní model sítě
  + tři hlavní zásady o zajištění bezpečnosti (detekce, prevence a náprava)
* DMZ (demilitarizovaná zóna)
  + fyzická nebo logická podsíť, která je z bezpečnostních důvodů oddělena od ostatních zařízení (jsou zde umístěny služby, které jsou k dispozici většinou z celého Internetu)
  + jakákoli služba, která je poskytována uživateli přes externí síť, může být umístěna do DMZ > nejčastěji webový server, poštovní server, FTP server, proxy server
* **Bruteforce** (útok hrubou silou)
  + metoda útočníků, slouží k rozluštění zašifrovaných dat či účtů, u kterých neznají dešifrovací klíč (nejvíce používán při zjištění loginu a hesla)
  + prevence před tímto útokem je složité heslo či i samotný login (dlouhá kombinace písmen, čísel a speciálních znaků)
* Wetware (liveware či meatware)
  + označení pro člověka ovládající počítač
  + ideologie “nejslabším článkem bezpečnosti je vždy člověk”
  + v praxi je zbytečné prolamovat hesla, když je možné zmanipulovat člověka, který má dostatečná práva v počítači či systému, aby útočníkovi poskytl přístup k jeho cíli
* **Phishing**
  + podvodná technika používána na internetu k získávání citlivých údajů (vyhledávání či získávání informací díky Internetu o určité osobě), hledá především citlivá osobní data (čísla kreditních karet, účtů, hesel a dalších)
  + útočník se většinou chová a prezentuje jako administrátor či správce internetového portálu

Počítačová bezpečnost

* zabezpečení před neoprávněnou manipulací s HW a SW
* ochrana informací před krádeží nebo poškozením
* zabezpečení přenosu dat (kryptografie)
* bezpečnost úložiště dat
* celisvost dat a nepodvrhnutelnost
* **Co udělat, aby se do sítě nikdo nepovolaný nedostal?**
  + Vrstvená bezpečnost (více prvků na ochranu sítě, oblastí)
  + Řízení přístupu (přihlašování, oprávnění)
  + Zabezpečení podle konkrétní role (podle organizační struktury)
  + Uvědomění uživatelů (školení, poučení, přednášky)
  + Monitorování (kamerový systém, software, strojové učení)
  + Aktualizace, Obranný tým (odpovědnost > omezený přístup uživatelů)

Bezpečnostní model sítě

* Součásti
  + Prevence
    - SW či HW výbava pro zajištění ochrany před možnými hrozbami útoku
  + Detekce
    - odhalení neoprávněných činností či slabých míst v síti
  + Náprava
    - odstranění zjištěných slabých míst, zamezení práv k možnostem neoprávněných činností

Potencionální cíle a důvody útoků

* cílem může být server (např. webová stránka) i client (člověk)
* důvodem k útoku může být např.:
  + odcizení bankovního účtu
  + spouštění jiných útoků
  + ovládání osobního počítače
  + získání osobních údajů např. k vydírání
* Útoky pomocí internetového připojení
  + možnost připojit se pomocí internetového připojení k nějakému serveru přes jiného klienta, konkrétně jeho IP
* **Botnet** (softwarové útoky, malware)
  + označuje síť počítačů infikovaných speciálním softwarem, která je centrálně řízena z jednoho místa
  + Botnet pak provádí nežádoucí činnost, jako je rozesílání spamu, DDos útoky apod.

Zabezpečení podle ISO/OSI modelu (Průnik především s PSkama)

L1

* Zabezpečení portů
  + Fyzické porty
  + Vypnutí portů
* Zamknutí serverové místností
* Prokazování fyzického přístupu k serverům a žurnálování těchto aktivit

L2

* Zabezpečení portů
  + Filtrování MAC adres
  + Nastavení módu: Trunk X Access
  + Port security
* Zabezpečení přístupu
  + Použití hesel
  + Šifrované protokoly (SSH (RSA))
* VLAN

L3

* **Firewall** (podrobně níže)
  + ACL
    - pravidla na adresu
    - protokoly
    - přeportování
* ARP útoky
  + ARP spoofing
* **NAT** (podrobně níže)
  + Komunikace mezi porty v jiných sítích
  + Překlad privátních adres na veřejné
  + IPv4 (kdo tam nebyl tak podle obrázku moc nemá nárok pochopit Horálkův myšlenkovej pochod...)

Zabezpečovací prvky

* **Firewall**
  + provádí analýzu paketů, sleduje vstupní a výstupní provoz
  + povolení a zákaz aplikací či služeb
* **NAT** (překlady síťových adres)
  + funkce, která adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro přístup do jiné sítě (Internet)
  + může způsobit problémy v komunikaci mezi klienty a snížit rychlost přenosu
  + na venek vypadá celá LAN jako jeden počítač s jednou veřejnou IP adresou
* Proxy a ochrana na úrovni aplikace
  + postarší technologie k využití připojení, například ke sdílenému připojení k internetu
  + nahrazuje technologie NAT (využívá technologii Triple A)
* **Technologie AAA**
  + zajišťuje ochranu služeb a komunikace v otevřených sítích
  + **Autentizace** - identifikování klienta
  + **Autorizace** - definice privilegii klienta
  + **Účtování** (Accounting) - shromáždění informací o účtech klientů a proběhlých relacích (žurnálování)
* IPSec (IPsecurity)
  + zabezpečení na úrovni síťové vrstvy
  + autentizace a šifrování každého paketu
  + skládá se ze dvou protokolů (AHP - autentizace, ESP - šifrování)
* GRE (Generic Routing Encapsulation)
  + uzpůsobené pro přenos paketů různých nosných protokolů
  + oproti IPSec má bohatší funkce pro tunelování, ale je méně zabezpečený
* AES (Advanced Encryption Standard)
  + narozdíl od starší technologie DES, nehrozí útok hrubou silou
  + délka klíče 128, 192 a 256 bitů
  + symetrický algoritmus - využívá sdíleného klíče k šifrování a dešifrování dat
* **VPN** 👇

VPN

* virtuální privátní síť
* spojení více vzdálených počítačů
* bezpečné (spojení je obvykle šifrováno), přitom transparentní spojení
* druhy
  + LAN2LAN
    - propojení dvou či více lokálních sítí
    - nejčastější použití pro propojení poboček s centrálou firmy
  + Vzdálený přístup
    - přístup vzdálených uživatelů do sítě
    - po navázání spojení má stejný přístup jako kdyby byli ve stejné lokalitě
  + Kombinované
    - kombinace LAN2LAN a vzdáleného přístupu
    - nejčastěji budovaný VPN
* zajištění integrity
  + pomocí jednosměrné hashovací funkce - kontrolní součet
  + pomocí MACs - přiřadí klíč k hashovacím funkcím
  + pomocí digitálního podpisu - odesílatel podepíše dokument jeho privátním klíčem a příjemce ho ověří pomocí veřejného klíče odesílatele
* využívá několik protokolů
  + přenášecí protokol (TCP, UDP, IPX)
  + obalový protokol (OpenVPN, GRE, PPTP)
  + nosný protokol (IP)

Zabezpečení Wi-Fi sítě

* SSID
  + název Wi-Fi sítě
  + možnost skrytí SSID
* MAC
  + možnost nastavení přístupu do sítě pouze vyhrazeným MAC adresám
* Šifrování
  + ochrana před odposlechem
  + data se nedají zachytit a zneužít
  + typy zabezpečení
    - **WEP** (Wired Equivalent Privacy)
      * zastaralý (prolomen v roce 2001)
      * šifrování RC4
    - **WPA** (Wi-Fi Protected Access)
      * nástupce WEP
      * od roku 2002 (prolomen)
      * šifrování RC4
    - **WPA2**
      * nástupce WPA
      * šifrování AES (poskytuje utajení, integritu a autentizaci - protokol CCMP)
      * prolomeno
    - **WPA3**
      * představen počátkem roku 2018
      * šifruje každé připojení samostatně
      * možné přes něj na dálku konfigurovat zařízení

Instalace serverového OS a rolí serveru. Základní role - uživatelé a skupiny, servery DHCP a DNS a souborový server

Základní zásady instalace

* **Příprava instalace systému**
  + před instalací je dobré rozdělit diskovou oblast na jednotlivé oddíly pro systém a pro data
  + vzhledem k bezpečnosti dat umístěných na serveru by rozdělení mělo být samozřejmostí
  + je dobré předem určit licenční model (doporučuje se však využití modelů Per Device nebo Per User)
* **Nastavení přístupové licence**
  + po instalaci je určen model přístupu
  + model lze po instalaci měnit pouze 1x
    - Druhy modelů
      * Per server (dříve)
        + určuje kolik uživatelů může být maximálně připojeno k serveru
      * Per seat (dříve)
        + licence na sídlo jednoho serveru, počet klientů definován dodatečně
        + výhodnější pro větší podniky s více servery
      * Per user (dříve)
        + kolik jednotlivých uživatelů může být v jediném okamžiku připojeno k serveru
      * Per device/core
        + licence udávaná na celkový počet počítačů, které se budou připojovat k serveru
* **Výběr edice**
  + Standard – pro Fyzická nebo minimálně virtualizovaná prostředí
  + Essentials – pro malé podniky až s 25 uživateli a 50 zařízeními
  + Datacenter – určeno pro datacentra a cloudová prostředí s vysokou mírou virtualizace
* **Nastavení a zabezpečení systému** (viz otázka 3)

Základní role systému

* **Server DHCP** (Dynamic Host Configuration Protocol) (viz otázka 7)
* **Server DNS** (Domain Name System) (viz otázka 7)
* **Active Directory** - Domain Services (AD-DS)
  + Jedná se o škálovatelnou adresářovou službu pro systémy řady Windows NT.
  + Kromě informací o objektech v síti (uživatelské účty, počítače, tiskárny apod.) umožňuje používat stromovou strukturu objektů, nastavovat systémové politiky, instalovat programy na počítače atd.
  + Pro funkčnost vyžaduje instalaci služby DNS (Win Server)
  + Je založena na standardních internetových protokolech
  + Definuje strukturu sítě
  + Organizuje skupiny počítačů a domén
  + **Domény**
    - Jedná se v podstatě o skupinu počítačů, které sdílí společnou adresářovou databázi.
    - Každá doména služby Active Directory má název DNS.
    - Hierarchické spojení domén vytvořené vztahem rodič-potomek se nazývá strom.
    - V případě, kdy jedna nebo více domén sdílejí stejná adresářová data, říkáme jim les.
  + **Organizační jednotky**
    - Jedná se o podskupiny v rámci domén, které často odráží řídící nebo obchodní strukturu organizace.
    - Jsou definovány v uvnitř domén. Můžeme si je představit jako logické kontejnery, do kterých můžeme umístit uživatelské účty, uživatelské skupiny, sdílené prostředky apod.
* **Souborový server**
  + označení pro počítač (server), který je připojen k počítačové síti a jeho hlavním úkolem je poskytovat přístup k souborům, které jsou na něm uloženy (klient-server)
  + výhodou souborového serveru je centralizovaná správa, úspora nákladů, snadnější zálohování, údržba, podpora sdílení dat a podobně
* Terminálový server
  + umožňuje převzít kontrolu nad vzdálenými počítači nebo nad virtuálními stroji přes síťové připojení
* **Tiskový server**
  + zařízení, které propojuje tiskárnu s klientem přes počítačovou síť
* Aplikační server
  + software specializovaný pro provozování nějaké sdílené aplikace (typicky pro podnikový software)
* **Poštovní server**
  + internetový protokol určený pro přenos zpráv elektronické pošty mezi přepravci elektronické pošty
* Vzdálený přístup/server **VPN**
  + prostředek k propojení několika počítačů prostřednictvím nedůvěryhodné počítačové sítě (veřejný internet)
  + lze dosáhnout stavu, kdy počítače budou moci spolu komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní sítě
  + při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, veškerá komunikace je šifrována

ISO/OSI

* **L7** Aplikační
* **L6** Prezentační
* **L5** Relační
* **L4** Transportní
* **L3** Síťová
* **L2** Datová/Linková
* **L1** Fyzická
  + Modulace
    - Analogová
    - Digitální

TCP/IP

* Aplikační
* Transportní
* Síťová
* Síťové rozhraní/Datová

Neřeší se zde fyzická zařízení

Typy komunikace

* Broadcast - Všichni v lokální síti (L2 a L3)
* Unicast - 1:1
* Multicast - 1:N

Standardy

* IEEE
* ITU

Fyzická

* L3 switch X Router

Typy kabelů

* Optika
  + Typy:
    - Single mode
      * Větší délka
      * Sklo + laser
    - Multimode
      * Menší délka
      * více signálu
      * Polymery + diody
      * Větší přenosová kapacita
* Metalika
  + Koax
    - Dobé stínění
    - Špatná práce s ním (krimpování, ...)
  + Kroucená dvoulinka
    - V páru kvůli stítění
    - STP
      * stítěný
      * Max 100m
    - UTP
      * nestítěný
    - Křížený
    - Přímý
      * Jiná zařízení na ISO/OSI modelu
    - MDIX - automatické rozpoznávání přímý/křížený
    - 802.3

Pojmy

* Duplex
  + Full
    - Oba směry v jeden okamžik
  + Half
    - Jden směr v jeden okamžik

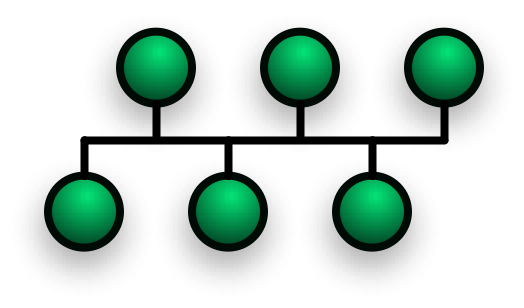
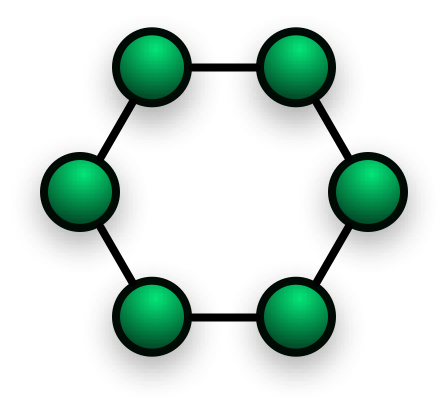
Bezdrátové sítě

* WiFi, Bluetooth, Infračervený, Zigbee
  + Frekvence
  + Vlnová délka
  + Menší frenkvece -> větší vzdálenost
* Typy
  + PAN
  + WAN

WiFi - 802.11

* 2.4GHz a 5GHz
* Normy
  + a, b, g, n, x
  + Určená kanály a frekvence
* Router vs AP
* Šifrování
  + TKIP
  + AES
* Zabezpečení
  + Nic
  + WEP
  + WPA
  + WPA2
  + WPA3
  + WPS tlačítko
* Typy autorizace
  + Personal
    - Lokální
  + Enterprise
    - Radius server
* SSID
  + Pasivní - Vysílá
  + Aktivní - Nevysílá
    - Ochrana před náhodným útokem
* Funkce routeru
  + Konfigurace routeru
  + Filtrování MAC adres
  + DMZ
  + Firewall
* Access point
  + Řídí ho **controller**

Fyzické topologie

* Sběrnicová topologie 
* Ring topologie 
* Star topologie

Kódování

* 4b/5b

Spojení vrstev

* Síťová vrstva -> HAL -> Ovladač -> Uživatel
* Zjištění hardwaru - daemon (systemd, udev)

Využití velikostí bitů

* 16 bitů
  + Nemáme
* 32 bitů
  + IPv4
* 48 bitů
  + MAC
* 64 bitů
  + Nemáme
* 128 bitů
  + IPv6

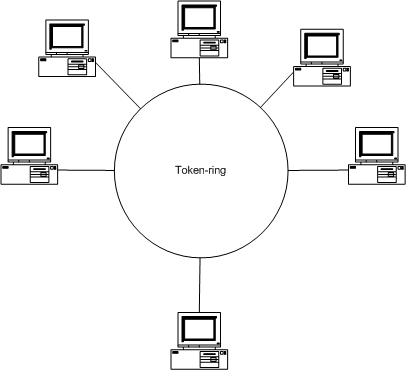
Strukturovaná kabeláž

* Konvergované sítě - pos tejných kabelech lze posílat více přenosů
* Komplexní návrh datových rozvodů (IPTV, VoIP, ...)

Linková/Datová

* LLC
  + FSC
  + Mac adresa
* MAC (Media Access Controll)
  + Modulace signálu kabelu
* MAC adresa
  + Hexadecimální
  + UID
  + První půlka - výrobce
  + Druhá půlka - náhodná
  + Link local adresy
* Frame
  + Head
    - Source MAC
    - Destination MAC
  + Data
  + Footer
    - FSC
    - Kontrolní součet
* Platnost DEST/SRC MAC adresy - každá síť má svou DEST/SRC MAC adresu
* Přepínané sítě
* Etherchannel
* Vlan
  + Tvoření podsítí
  + InterVLAN Routing
  + Trunk
    - Přeposílání všechny VLANy
    - Management VLAN
* Switch X Hub
  + Switch
    - Pamatuje si MAC adresy
    - Zabezpečení - Port security
  + Hub
    - Posílá vždy všem
* Kolizní doménu ruší switch
* Broadcastovou doménu ruší router
* ARP
  + Tabulka IPv4 adres s Mac adresami
* EUI64
* ICMPv6 - podobné ARP

Logická topologie

* Token ring 
  + Používají token -> kdo má token může komunikovat, pokud nepotřebuje posílá dál
  + Řídící prvek
* Ethernet

Síťová

* IPv4
  + 32bit
  + Hlavička
    - Srouce
    - Destination
    - TTL
    - Checksum
  + Data
  + Typy
    - Veřejná
    - Privátní
  + Třídy
    - A
    - B
    - C
* IPv6
  + 128bit
  + Prefix je maska
  + Link local adresa
    - Generuje operační systém
    - FE80::...
  + Veřejná
    - Jednoznačná identifikace
  + Hlavička
* Maska podsítě
* ICMP
  + Ping
  + Tracert
* Nat
* Router
* Routy
* Protokoly
  + RIP - nejkratší
  + OSPF - nejrychlejší
  + EIGRP - něco mezi

Transportní

* TCP
  + Spolehlivý
  + Checksum
  + Three way handshake
    - Klient žádá o spojení
    - Server potvrdí spojení
    - Klient potvrdí přijetí
* UDP
  + Není zaručena integrita
* Druhy portů
  + Well know ports 0-1023
  + Registrované porty 1024-49151
  + Dynamické porty 49152-65535

Relační

* Udržuje relace
* Synchronizace
* Získání všech dat

Prezentační

* Rozbalení dat (dekomprese, ...)

Aplikační vrstva

* DHCP
  + Port: 67 UDP
  + Proces:
    - DHCP Discovery -> L2 Broadcast
    - DHCP Offer -> (Unicast) IP, DNS, Gateway, Lifetime
    - DHCP REQUEST -> L2 Broadcast
    - DHCP ACK -> (Unicast)
  + Obnova IP - DHCP REQUEST,...
* DNS
  + Překládání domény na IP adresu
  + Port: 53
  + Řády domény
    - **cz.**
    - **delta-skola.** cz.
    - [***www***](http://www/)***.*** delta-skola.cz.
* HTTP
  + Port 80
* HTTPS
  + Port 443
* SSH
  + Port 22
  + v1 vs v2
    - v1 - 512 bitů
    - v2 - 1024 bitů
  + Přihlašování
    - Local
    - Radius AAA
* FTP
  + Port 21 TCP
  + TFTP
    - Po UDP
    - Bez zabezpečení
* VPN
  + Vytvoření tunelu do cizí sítě
* EMAIL

PŘÍKAZY

# Notes

* Default Management VLAN1
* Security VLAN1 -> VLAN99
* Management VLAN on all ports
* If configuring from notepad int no sh
* Interface can have multiple ipv6
* SVI - Switch Virtual Interface
* Do not forget!
* PC must be powered on.
* Configure Gateway!
* SSHv2 key 1024 bits.
* Router do not have ipv6 by default
* Trunk desirable -> other site native vlan

## VLAN Delete

* assign ports to active vlans
* no vlan
* delete vlan.dat
* Switch ports have dynamic auto

## Save config

# copy running-config startup-config

# Movement

# configure terminal

(config)# interface <interface>

(config)# line {console/vty}

(config)# interface range <i0> - <i1>

# Troubleshooting

# show startup-config

# show running-config

## interface

# show interface <interface> [status]

## ip interface

// vlna, switchport, trunk, port-channel, etherchannel

# show ip[v6] interface <interface>

# show ip[v6] interface brief

## vlan interface

# show vlan [brief]

## routing table

# show ip[v6] route

# show mac address-table

## ssh

# show ip ssh

## DTP

# show dtp interface <interface>

## STP

# show spanning-tree

## Ech

# show etherchannel summary

# show etherchannel port-channel

## DHCPv4

# show ip dhcp pool

# show ip dhcp binding

# show ip dhcp server statistics

## DHCPv6

# show ipv6 dhcp pool

# show ipv6 dhcp binding

# show ipv6 dhcp interface

## Static route

# show ip[v6] route static

## Common

# ping <host>

# terminal history size <no>

# show history | section / include / exclude / begin

## wrong ipv6

(conf-if)# no ipv6 address <wrongIP>/<prefix> (conf-if)# ipv6 address <correctIP>/<prefix>

# Basic Configuration

## Switch

(config)# no ip domain-lookup

(config)# hostname <hostname>

(config)# service password-encryption

(config)# enable {password/secret} <password>

(config)# banner motd # <text> #

(config)# ip default-gateway <ip>

## Router

(config)# no ip domain-lookup

(config)# hostname <hostname>

(config)# service password-encryption

(config)# enable {password/secret} <password>

# Remote Management

## Console cable

(config)# line console <no>

(config-line)# logging synchronous

(config-line)# transport output telnet

(config-line)# password [password]

(config-line)# login

## SSH

(config)# ip domain-name [name]

(config)# crypto key generate rsa 1024

(config)# username <name> {password/secret} <password>

(config)# line vty <vty0> <vty1>

(config-line)# transport input ssh

(config-line)# login local

(config)# ip ssh version 2

## Telnet

(config)# line vty <vty0> <vty1>

(config-line)# transport input telnet

(config-line)# password [password]

(config-line)# login

# Routing

(config)# ip routing

(config)# ipv6 unicast-routing

# Interface

(config)# interface <interface>

(config-if)# ip address <ip> <mask>

(config-if)# ipv6 address <ip6>/<prefix>

(config-if)# ipv6 address <ipv6> link-local

(config-if)# description <text>

(config-if)# no shutdown

# Loopback

(config)# interface loopbak <no>

(config-if)# ip address <ip> <mask>

# VLAN

## Switch

### Create VLAN

(config)# vlan <vlanNo>

(config-vlan)# name <name>

### Create SVI VLAN

(config)# interface vlan <vlanNo>

(config-if)# ip address <ip> <mask>

(config-if)# ipv6 address <ipv6>/<prefix>

(config-if)# ipv6 address <ipv6> link-local

(config-if)# no shutdown

### Assign VLAN

(config)# interface <interface>

(config-if)# switchport mode access

(config-if)# switchport access vlan <no>

### Assign Voice VLAN

(config)# interface <interface>

(config-if)# switchport mode access

(config-if)# switchport access vlan <no>

(config-if)# mls qos trust cos

(config-if)# switchport voice vlan <voiceNo>

# Trunk

## Switch

### Assign Trunk port manually

(config)# interface <interface>

(config-if)# switchport mode trunk

(config-if)# switchport trunk native vlan <no>

(config-if)# switchport trunk allowed vlan {<no1>,<no2>}

### Assign Trunk via DTP

* auto + auto = access
* desirable + auto = trunk
* desirable + desirable = trunk

#### **Tabulka**

* |---- S1 ---|---- S2 ---|- swp --|
* | auto | auto | access |
* | desirable | auto | trunk |
* | desirable | desirable | trunk |
* |-----------|-----------|--------|

(config)# interface <interface>

(config-if)# switchport mode dynamic desirable

(config-if)# switchport trunk native vlan <no>

(config-if)# switchport trunk allowed vlan {<no1>,<no2>}

* Do not forget to add native vlan on other side!

### No DTP

(config)# interface <interface>

(config-if)# switchport mode trunk

(config-if)# switchport nonegotiate

# Inter-VLAN

## Router-on-a-Stick

### Router

(config)# interface <interface>.<subinterface>

(config-subif)# encapsulation dot1Q <vlanNo>

(config-subif)# ip address {A.B.<subnet>.1} <mask> [native]

### Switch

1. Create VLANs

(config)# vlan <vlan>

(config-vlan)# name <vlanName>

1. Configure Management VLAN

(config)# interface vlan <mngVlan>

(config-if)# ip address {A.B.<mngVlan>.D} <mask>

(config)# ip default-gateway <gatewayIP>

1. Configure access ports

(config)# interface <interfaceToHost>

(config-if)# switchport mode access

(config-if)# switchport access vlan <vlan>

1. Configure trunking ports

(config)# interface <interfaceToRouterOrSwitch>

(config-if)# switchport mode trunk

* Host - assign gateway to subnet IP

### Layer 3 Switch

1. Create VLANs

(config)# vlan <vlan>

(config-vlan)# name <vlanName>

1. Create SVI VLANs

(config)# interface vlan <vlanNo>

(config-if)# ip address {A.B.<vlanNo>.1} <mask>

(config-if)# no shutdown

1. Configure access ports

(config)# interface <interfaceToHost>

(config-if)# switchport mode access

(config-if)# switchport access vlan <vlan>

1. Enable IP routing

(config)# ip routing

## Trunk to Switch

(config)# interface <interfaceToTrunk>

(config-if)# switchport mode trunk

(config-if)# switchport trunk native vlan <nativeVLAN>

(config-if)# switchport trunk encapsulation dot1q

* Do not forget to configure static trunk on switch

## Connect L3S to Router

1. Configure the routed port

(config)# interface <interfaceToRouter>

(config-if)# no switchport

(config-if)# ip address <ip> <mask>

(config-if)# no shutdown

1. Enable routing

(config)# ip routing

1. Configure OSPF routing

(config)# router ospf <vlanNo>

(config-router)# network {A.B.<vlanNo>.0} <!mask> area 0

(config-router)# network <networkIPwRouter> <!mask> area 0

# STP

(config)# spanning-tree vlan 1 root primary

(config)# spanning-tree vlan 1 priority 24576

# EtherChannel

## Tabulka PAgP

* |--- S1 ---|--- S2 ---|- ECh -|
* | on | on | yes |
* | on | des/auto | no |
* | des | des | yes |
* | dis | auto | yes |
* | auto | auto | no |
* |----------|----------|-------|

## Tabulka LACP

* |--- S1 ---|--- S2 ---|- ECh -|
* | on | on | yes |
* | on | act/pas | no |
* | active | active | yes |
* | active | passive | yes |
* | passive | passive | no |
* |----------|----------|-------|
* both sides must have same configuration of speed, duplex an vlan
* shutdown configured interfaces because of STP (dont forget no sh)

(config)# interface range <int0> - <int1>

(conf-if-rng)# channel-group <no> mode <mode>

(config)# interface port-channel <no>

(config-if)# interface mode trunk

(config-if)# switchport trunk allowed vlan {<no1>,<no2>}

# DHCPv4

* DHCPDISCOVER -> DHCPOFFER -> DHCPREQUEST-> DHCPACK

## DHCP Server

(config)# ip dhcp excluded-address <ip0> <ip1>

(config)# ip dhcp pool <name>

(dhcp-config)# network <networkIP> <mask>

(dhcp-config)# default-router <routerIP>

(dhcp-config)# dns-server <dnsIP>

(dhcp-config)# domain-name <domain>

(dhcp-config)# lease {<day> <hour> <minutes> | [infinite]}

(config)# service dhcp

## DHCP Relay Agent

* over router without DHCP to DHCP server

(config)# interface <interfaceToHost>

(config-if)# ip helper-address <dhcpIP>

## DHCP Router Client

(config)# interface <interface>

(config-if)# ip address dhcp

# SLACC

* A - Autoconfigure - use SLAAC
* O - Other Configuration - stateless DHCPv6
* M - Managed - statefull DHCPv6
* SLAAC Only = A1 O0 M0
* SLess DHCP = A1 O1 M0
* SFull DHCP = A0 M1

# DHCPv6

(config)# ipv6 unicast-routing

## DHCPv6 Stateless Server

(config)# ipv6 dhcp pool <poolName>

(config-dhcpv6)# dns-server <ipv6>

(config-dhcpv6)# domain-name <name>

(config)# interface <interface>

(config-if)# ipv6 address <ipv6>/<prefix>

(config-if)# ipv6 address <ipv6> link-local

(config-if)# ipv6 nd other-config-flag // O = 1

(config-if)# ipv6 dhcp server <poolName>

(config-if)# no shutdown

## DHCPv6 Stateless Client

(config)# interface <interface>

(config-if)# ipv6 enable

(config-if)# ipv6 address autoconfig

## DHCPv6 Statefull Server

(config)# ipv6 dhcp pool <poolName>

(config-dhcpv6)# address prefix <networkIPv6>/<prefix>

(config-dhcpv6)# dns-server <ipv6>

(config-dhcpv6)# domain-name <name>

(config)# interface <interface>

(config-if)# ipv6 address <ipv6>/<prefix>

(config-if)# ipv6 address <ipv6> link-local

(config-if)# ipv6 nd managed-config-flag // M = 1

(config-if)# ipv6 nd prefix default no-autoconfig // A = 0

(config-if)# ipv6 dhcp server

(config-if)# no shutdown

## DHCPv6 Statefull Client

(config)# interface <interface>

(config-if)# ipv6 enable

(config-if)# ipv6 address dhcp

## DHCPv6 Relay Agent

(config)# interface <interface>

(config-if)# ipv6 dhcp relay destination <ipv6ToDHCP> [interface]

# IP Static Routing

## IPv4 route

(config)# ip route <network> <mask> <next-hop> [ad]

(config)# ip route <network> <mask> [next-hop] <exitif> [ad]

## IPv6 route

(config)# ipv6 route <network>/<pref> <next-hop> [ad]

(config)# ipv6 route <network>/<pref> [next-hop] <exitif> [ad]

### Next-hop

* only next-hop address is specified
* recomended

## IPv4 Next-hop Static Route

(config)# ip route <network> <mask> <next-hop>

## IPv6 Next-hop Static Route

(config)# ipv6 unicast-routing

(config)# ipv6 route <network>/<pref> <next-hop>

### Directly Connected

* only exit interface is specified
* recommended to use only with p2p serial

## IPv4 Next-hop Static Route

(config)# ip route <network> <mask> <exitif>

## IPv6 Next-hop Static Route

(config)# ipv6 unicast-routing

(config)# ipv6 route <network>/<pref> <exitif>

### Fully specified

* next-hop and exit interface is specified
* to use with multi-access connection (i.e. Ethernet)
* use with IPv6 link-local

## IPv4 Next-hop Static Route

(config)# ip route <network> <mask> <exitif> <next-hop>

## IPv6 Next-hop Static Route

(config)# ipv6 unicast-routing

(config)# ipv6 route <network>/<pref> <exitif> <next-hop>

(config)# ipv6 route <network>/<pref> <exitif> <link-local>

### Default route

* matches all packets
* Gateway of the last resort

## IPv4

(config)# ip route 0.0.0.0 0.0.0.0 <next-hop>

(config)# ip route 0.0.0.0 0.0.0.0 <exitif>

## IPv6

(config)# ipv6 route ::/0 <next-hop>

(config)# ipv6 route ::/0 <exitif>

### Floating

* Backup to primary
* higher administrative distance
* Def 1 => 2+
* EIGRP 90 => 91+
* OSPF 110 => 111+
* IS-IS 115 => 116+

(config)# ip route 0.0.0.0 0.0.0.0 {next-hop/exitif} <ad>

(config)# ipv6 route ::/0 {next-hop/exitif} <ad>

### Host Route

* Automatically on Connected (C)
* Automatically on localhost (Configuring interface with ip) (L)

## normal

(config)# ip route <hostIP> 255.255.255.255 <next-hop>

(config)# ipv6 route <hostIPv6>/128 <next-hop>

## link-local

(config)# no ipv6 route /128 (config)# ipv6 route /128

# Duplex

* Half - one way
* Full - simultaneous two ways

(config)# interface <interface>

(config-if)# duplex <auto/full/half>

(config-if)# speed <10/100/1000/auto>

# MDIX

* no need to worry about straight / cross

(config)# interface <interface>

(config-if)# mdix auto

# Security

* Shutdown unused ports and put inside unused VLAN
* Enable port security
* Disable DTP

(config)# security password min-lenght <no>

(config)# service password-encryption

## Timeout

(config-line)# exec-timeout <minutes>

## Attempts

(config)# login block-for <sec> attemts <no> within <seconds>

## Port security

(config)# int <interface>

(config-if)# switchport mode access

(config-if)# switchport port-security

### PS max MAC

(config-if)# switchport port-security maximum <no>

(config-if)# switchport port-security mac-address <MAC>

(config-if)# switchport port-security mac-address sticky

### PS aging

(config-if)# switchport port-security aging time <minutes>

(config-if)# switchport port-security aging type {i/a}

### PS Violation mode

(config-if)# switchport port-security violation {p/r/s}

## DHCP Snooping

(config)# ip dhcp snooping

(config)# interface <trustedInterface>

(config-if)# ip dhcp snooping trust

(config)# interface <untrustedInterface>

(config-if)# ip dhcp snooping limit rate <no>

(config)# ip dhcp snooping vlan {<vlan0>, <vlan1>}

## Dynamic ARP Inspection

(config)# ip dhcp snooping

(config)# ip dhcp snooping vlan <no>

(config)# ip arp inspection vlan <no>

(config)# ip arp inspection validate src-mac

(config)# ip arp inspection validate dst-mac

(config)# ip arp inspection validate ip

(config)# interface <trustedInterface>

(config-if)# ip dhcp snooping trust

(config-if)# ip arp inspection trust

## PortFast

(config)# interface <interface>

(config-if)# switchport mode access

(config-if)# spanning-tree portfast

(config)# spanning-tree portfast default

### BPDU Guard

(config)# interface <interface>

(config-if)# spanning-tree bpduguard enable

(config)# spanning-tree portfast bpduguard default

# FHRP - HSRP

* def priority 100; higher better

(config)# interface <interface>

(config-if)# standby version 2

(config-if)# standby <gNo> ip <virtualIP>

(config-if)# standby <gNo> priority <priority>

(config-if)# standby <gNo> preempt

* change default gateway on Devices

# Misc

# clock set <hh:mm:ss> <Mon> <d> <y>