Úvod

Vlastnosti: prenos dát, zdieľanie hardwarových zdrojov, software, súborov, dát a informácií, komunikácia, ...

Delivery (správnemu príjemcovi), *Accuracy* (nepoškodené), *Timeliness* (včas)

Súčasti komunikačnéhoho systému

- *Odosielateľ*: mobil, videokamera, ..
- *Príjemca*
- *Správa:* vyměňovaná informace
- *Prenosné médium*: optický kábel, vzduch, ..
- *Protokol*: sada pravidiel řídících komunikací mezi zúčastněnými stranami

Parametry sieťových tokov

- *Priepustnosť* (bandwidth): kapacita prenosového kanálu (max. množstvo/jednotka času: *bps* (bit/sec), *kbps*, *Mbps*, *Gbps*, ..)
- *Strátovosť paketov* (packet loss): priemerný počet stratených paketov v *%*
- *Zpoždění prenosu* (latency, delay): čas odoslania po prijatie správy (najčastejšie v *ms*)
    - Zahrnuje zpoždění v přenosové trase a na zařízeních, které jsou její součástí
    - Někdy se také uvádí tzv. RTT delay (Round-Trip-Time delay) = zpoždění obousměrného přenosu
        - Tj. čas, který uplyne od odeslání zprávy zdrojovým uzlem, jejím přijetím na uzlu cílovém, zpětným odesláním na zdrojový uzel až po její přijetí na zdrojovém uzlu
- *Rozptyl/Kolísání zpoždění* (jitter): variabilita v doručovaní paketov na cílovém uzlu (tedy ve zpoždění při přenosu); rozdiel medzi najväčšou a najmenšou odozvou na požiadavok

Ideálne siete / skutočné:

- *dôvody*: preťaženie siete -> spomalenie; dĺžka cesty
- transparentní pro uživatele/aplikace (pouze tzv. end-to-end vlastnosti) / vnitřní struktura ovlivňuje doručení dat
- neobmedzená priepustnosť / obmedzená
- žiadne straty dát / (občas) dochádza k stratám
- žiadne zpoždění a jitter / dochádza ke zpoždění

- zachovanie poradia paketov / poradie nie je garantované
- nepoškodené dáta / môžu byť poškodené (napr. slnkom)
- *požadované vlastnosti:* maximálne využ. prenosových kapacít; rovnaká dostupnosť; decentralizovaná správa; rýchla adaptácia na nový stav topológie (po pripojení väčšieho počtu NB do siete nastáva zmena topológie) ; riadenie toku dát - ochrana; rozšíriteľnosť
- Efektivita, spravedlivost, decentralizovaná správa, rychlá konvergence při adaptaci na nový stav, multiplexing/demultiplexing, spolehlivost, řízení toku dat (ochrana proti zahlcení sítě a přijímacího uzlu)

Základní přístupy:

Spojované sítě (= přepínání okruhů)

- 2 fázy: nadviazanie spojenia (tzv. okruh; udržuje sa počas celej komunikácie) -> prenos dát
- Nutnosť uchovávať stav
- Okruh pevný (předvytvořený) nebo vytvářen na žádost
- Jednoduché zaručenie kvality
- Napr. analógové telefónne siete

Nespojované siete (= přepínání paketů)

- Dáta sú rozdelené na malé pakety, ktoré môžu byť ešte fragmentované nebo slučované, sú vysielané samostatne, v rôznom poradí
- Není předem známa cesta
- Príjemca ich potom zloží do pôvodného stavu
- Problematická implementácia kvality služby (tzv. best-effort služba)
- Netreba uchovávať stav siete
- Napr.: Internet

Implementace funkcionality:

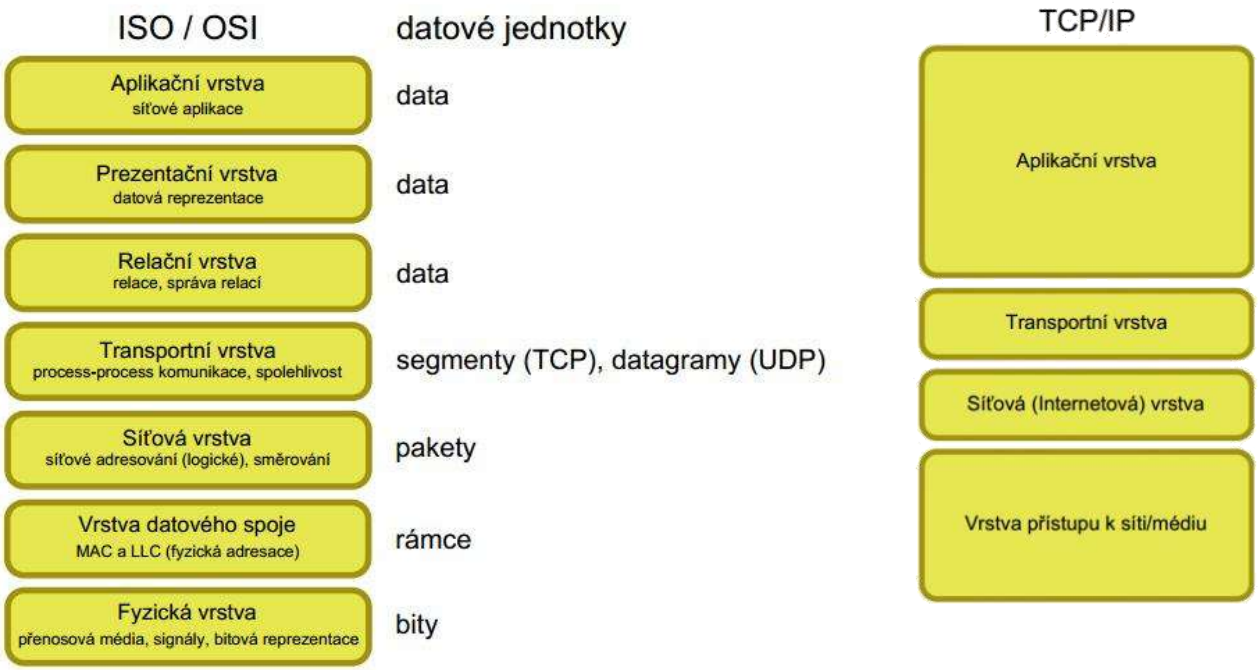
End-To-End prístup (E2E)

- Požadovanú funkcionalitu je možné zaistiť iba pomocou znalostí a prostřednictvím samotnej aplikácie
- Pokud je to možné, operace komunikačního protokolu provádět v koncových bodech systému, nebo co nejblíže k nim
- V nižších vrstvách systému mají být funkce protokolu implementovány pouze tehdy, pokud to

zlepšuje výkon
- E-mail; data musí být stejná a nevadí zpoždění

Hop-To-Hop prístup (HbH)
- Opakovaním funkcionality na úrovni každého dvoubodového přenosu je možné výrazně zvýšiť výkon
- Vyžaduje uchovávanie stavových informácií na vnitřních prvcích sítě → limitovaná škálovatelnost
- Vhodný pre real-time aplikácie: minimalizace zpoždění, menší věrnost dat

ISO/OSI Model
- **7 vrstiev**



- Každá vrstva je zodpovedná za určitú funkcionalitu – aby ji mohla zajistit, přidává do dat své řídící informace
- Každá vrstva komunikuje len so susediacimi vrstvami – funkcionalita izolována v rámci

příslušné vrstvy

- Komunikace se vlastně odehrává jen mezi stejnými vrstvami (peery)
- Iný model: **TCP/IP**

Aplikačná vrstva

- ♦ Rozhranie medzi užívateľom a sieťou
- ♦ Zahrňuje sieťové aplikácie a protokoly; data balena do aplikačních protokolů

Prezentačná vrstva

- ♦ Zaisťuje jednotnú reprezentáciu dát
- ♦ Funkcionalita je zaistená samotnou aplikáciou

Relačná vrstva

- ♦ Spravuje ustavená spojení (= relácie) medzi komunikujúcimi aplikáciami
- ♦ Funkcionalita je zaistená samotnou aplikáciou, resp. aplikačním protokolem

Transportná vrstva

- ♦ Zaisťuje identifikáciu (= adresaci) a doručenie dát (segmentov, datagramů) medzi dvoma komunikujúcimi procesmi, s případným zajištěním spolehlivosti přenosu

Sieťová vrstva

- ♦ Zaisťuje identifikáciu (= adresaci) a doručenie dát (paketov) medzi dvoma komunikujúcimi uzlami; součástí je také nalezení vhodné cesty (= směrování)
  - ▪ Nezávisle na použitých protokolech je pro identifikaci uzlů v síti (směrování) vždy užit IP protokol

Spojová vrstva

- ♦ Zaisťuje prenos dát (rámcov) medzi uzlami prepojenými prenosovým médiom, včetně řízení přístupu k tomuto médiu

Fyzická vrstva

- ♦ Riadi deje v prenosovom médiu: vysílání/příjem (prenos) dát, kódovanie do signálů, ..

Komunikačné protokoly

Priebeh komunikácie:

- Výzva
- Akceptácia (ustavení komunikačního kanálu)
  - Akceptované (dotaz na čas)
  - Odmietnuté
  - Time-out (opakovanie žiadosti, později ukončení)
- Komunikácie medzi HW/SW riadená protokolom
  - **Protokoly** riadia tok bitov (síťové karty), rýchlosť a smer paketov (směrovače)

- Určujú: "*ČO?*", "*AKO?*", "*KEDY?*"
- Definujú: syntax (formát dát), sémantiku (úkony vykonané pri odosielaní a príjimaní správ), časovanie (poradie správ, kdy je potřeba jakou odeslat)
- **Síťový protokol** definuje formát a pořadí zpráv vyměňovaných mezi dvěma či více komunikujícími entitami, stejně jako akce vykonané při odesílání/příjmu daných zpráv.
- Príklady: UDP, TCP, IP, IPv6, SSL, TLS, HTTP, FTP, SSH, ...

Štandardizácia

- Stanovení norem/standardů popisujících nejrůznější akce, formy komunikace atp.
- Hlavní cíle: kvalita, bezpečnost, kompatibilita, interoperabilita, portabilita

Typy:

- **De facto**: technické riešenia, ktoré sa presadili na trhu a su všeobecne akceptované
- **De jure**: štandardy schválene normalizačným orgánom (napr.: ITU-T, ISO, IEC, IEEE, ANSI, EIA, **IETF (vydává RFC),** ...)

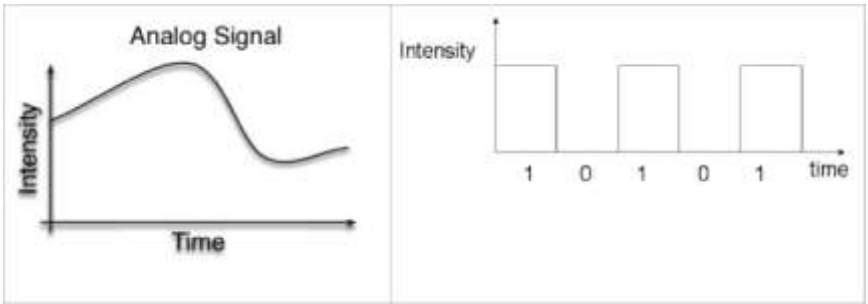
Reálné sítě: CESNET2 (ČR), GEANT2 (Evropa), Internet2/Abilene (USA)

L1: Fyzická vrstva

- Len point-to-point spoje - nie je treba riešiť adresáciu, pretože neexistuje viac spojov
- Data přenášena pasivním přenosovým médiem (žádná logika řízení)
- Poskytuje služby pro vrstvu datového spoje
- Dáta sú vyjadrené 0, 1 zoskupené do rámcov; fyz. vrstva transformuje jejich bitový obsah do signálů šířených přenosovým médiem
    - Prenášajú sa **analógovým** alebo **digitálnym signálom**
        - Analógový signál je možné modulovať (na to slúži *modem*)

- Řídí děje v přenosovém médiu, rozhoduje o: vysílání/příjmu, kódování do signálů, počtu logických kanálů přenášejících data z různých zdrojů souběžně
- **Hlavný cieľ**: prenos bitov (= obsah předaných rámcov) medzi odosielateľom a príjemcom
- Dôležité sú **štandardy**: definujú parametry přenášených signálů, význam a časový priebeh signálov, vzájemné návaznosti řídících a stavových signálů, zapojenie konektorov, ...
    - RS-232-C, CCITT V.24, CCITT X.21, IEEE 802.x

- Dáta súmédiom prenášané elektromagnetickými signálmi, musí na ně být transformována
- **Signál**: časová funkcia reprezentujúca zmeny fyzikálnych vlastností přenosového média
- *Analógové* (spojitý v čase)*, digitálne* (diskrétny v čase) *prenosy*
- Některá média vhodná pro oba přenosy – koaxiál, kroucená dvojlinka, optické vlákno

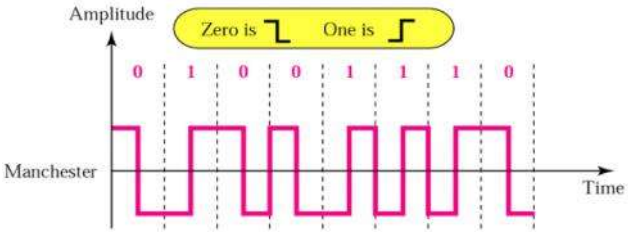


Analogový signál

- Spojitý v čase, mění se hladce; lze jej šířit jak vodiči, tak bezdrátovým prostředím
- Modulace nosného signálu digitálními daty
- Modulace:
  - ♦ Amplitudovou digitální modulací: mění se amplituda nosného signálu
  - ♦ Frekvenční digitální modulací – změna frekvence
  - ♦ Fázovou digitální modulací – změna fáze

Digitálny prenos

- Lze šířit pouze vodiči, mění se skokově
- Transformace kódování – proces konverze binárních dat do digit. signálu
  - **Kódovanie**:
    - ♦ *Priame*: 1 = kladná amplitúda, 0 = záporná, žádná samosynchronizovatelnost
    - ♦ *NRZ*: NRZ-L (1 = záporná, 0 = kladná; žádná samosync.) a NRZ-I (1 = zmena polarizácie, 0 = žiadna změna, řeší jen posl. 1, ne nul)
    - ♦ *Manchester*:
      - ▪ Každý bit kódován 2 prvky signálu, snížení efektivní přenosové kapacity
      - ▪ Plná samosynchrovatelnost



  - *4B/5B*: substitúcia 4-bitových blokov na špeciálne 5-bitové vzorky; nejvýše 3 nuly po sobě, vlastní přenos využívá NRZ-I (počet 1 nedůležitý)
    - Uměle zavedená redundance pro zabezpečení sync.; detekce chyb

4B	5B	4B	5B
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

- Problém – synchronizace vysílače a přijímače – změna (0→1, 1→0) lze využít pro synchronizaci hodin, ale neřeší dlouhé posloupnosti 0/1

Defekty signálov

- **Slabnutie**, stráta energie: spôsobené napríklad odporom

  Skreslenie, stráta tvaru: spôsobené rozdielnou rýchlosťou signálov na různých frekvencích
- **Šum**: vplyv cudzorodej energie; např. termální šum, indukovaný signál, přeslech

Prenosové média

- Poskytují prostredie pro činnost L1
  - *Vodené média*: optický kábel (páteře, stovky Gbps), krútená dvojlinka (LAN, 10Gbps), koaxiálny kábel, ...
  - *Nevodené média* – přenáší elmag vlny bez fyzického vodiče; éter

Multiplexing

- Technika zdieľania dostupnej prenosovej kapacity přenosového média souběžnými komunikacemi
  - ♦ Efektivnější využití médie; zejména optika a bezdráty
- Analógové signály:
  - ♦ ***FDM:*** *Frequency Division Multiplexing*
    - Každý přenášený signál modulován samostatným nosným signálem s unikátní nosnou frekvencí
    - Modulované nosné signály se kombinují do nového signálu, který se přenáší spojem
    - Např. telefonní spoje mezi ústřednami
    - Éter: netřeba fyzicky realizovat (de/)multiplexory, stanice mohou vysílat na různých frekvencích
  - ♦ ***WDM****: Wave Division Multiplexing*
    - Varianta FDM pro optické signály (opt. vlákna); použití více světelných paprsků o různých frekvencích, každá barva = 1 kanál
- Digitálne signály:
  - ♦ ***TDM:*** *Time Division Multiplexing*
    - V libovolném okamžiku kanál využívá výhradně jeden vysílající

    - Vysoká propustnost i při mnoha vysílajících
    - Nutnost precizní synchronizace vysílače a přijímače
- Zariadenie zabezpečujúce multiplexing: Multiplexor (MUX)
- Prevod späť na jednotlivé signály: Demultiplexor (DEMUX)

- Proč nastačí L1?
  - Nezajišťuje opakování chybně přenesené informace
  - Nepodporuje určení entity mající právo vysílat do média
  - Nepodporuje ovládání toku dat ze zdroje do média
  - Nepodporuje komunikaci mezi definovanými partnery

L2: Vrstva dátového spoja

- Lokálna sieť LAN (Local Area Networks), nutnost adresace stanic
- Node-to-node delivery - prenos medzi uzlami
- Prijíma pakety zo sieťovej vrstvy, ktoré transformuje na rámce
- V spolupráci s fyzickou vrstvou zaisťuje prenos rámcov mezi uzly sdíleným přenosovým médiem (tzn. pouze doručení na stejném segmentu, stejné LAN)
- Zajišťuje spolehlivost přenosu, nezahlcení přijímacého uzlu, řídí přístup ke kabelu

Služby

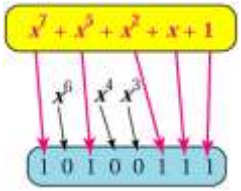
- *Tvorba rámcov - framing*: pakety ze síťové vrstvy balené do rámcov
- *Adresovanie - addressing*: fyzické/MAC adresy; zdrojová i cílová
  - Ethernetový rámec: 

    - Každá stanica (síťová karta) má unikátnu MAC adresu
    - Preambule – identifikace počátku rámce (sync. prvek)
- *Chybové riadenie - error control*
    - Chyba = zmena hodnoty bitu; např. optika 10^{-12}, wireless 10^{-5}
    - L2 vrstva detekuje a robí korekciu chýb – vysílač přidá bity, jejichž hodnota

je funkcí přenášených dat, přijímač stejnou funkci spočítá a v případě rozdílu se pokusí detekovat/opravit chybu. Detekce, ale neoprava = chce data poslat znovu.

- Error Detection, Automatic Request for Retransmission (ARQ) – detekce chyby a zajištění opakování přenosu, vhodné pro málo chybující přenosová média
- Forward Error Correction (FEC) – detekce chyb a snaha o jejich korekci (s využitím redundance), vhodné pro často chybující média nebo média s velkou latencí – např. Hammingův kód

- **Kódy pre detekciu chýb*:***
  - Párna/nepárna parita (veľmi slabá kontrola) – k přenášeným bitům přidán 1 bit tak, aby měla sudý/lichý počet 1; detekuje jen chyby v 1 bitu. Silnější ochrana – dvojdimenzionální parita
  - Cyklické kódy (silná kontrola)
  - CRC = Cyclic redundancy check
    - Zo vstupných dát sa vypočíta číslo, ktoré príjemca podľa danej funkcie prepočíta a skontroluje správnosť dát
    - Pro blok k-bitů se vygeneruje (n-k) bitová posloupnost, přidávaná ke k-bitům zprávy. Přenášená zpráva (rámec, n-bitů) reprezentuje polynom stupně (n-1)



- *Riadenie toku - flow control*: zabraňuje zahlteniu príjemca (mechanismy stop-and-wait, sliding-window)
- *Riadenie prístupu k médiu - MAC (Medium Access Control) protokoly*
  - Cieľ: eliminovať konflikty pri vysielaní do jednoho prostředí; nezbytné v síti s více entitami se sdíleným přenosovým médiem
  - Protokoly neriadeného prístupu (riešia kolízie až keď nastanú)
    - **Aloha**:
      - Stanica vysiela vždy, keď má pripravený rámec (dáta)
      - Predpoklad kolízii; detekovány nepřejetím potvrzení o přijetí v daném časovém intervalu
      - Po kolízii istú dobu počká a tak znova vysiela
      - *Neefektívne*
    - **CSMA/CD**:
      - Upravená Aloha – stanice vysílá, jen když zjsití klid v médiu
      - Současně na médiu naslouchá stanice pro detekci kolize (CD =

Collision detection)
        - □ Aplikácia v klasickom LAN Ethernetu; nepoužitelné v nevoděném médiu
    - **CSMA/CA**:
        - □ Obchádza kolízie
        - □ Použitelné v nevoděném médiu
- ○ Protokoly riadeného prístupu
    - Stanica vysiela len ak má **právo**, v predom **dohodnutých intervaloch**, len ak je **vyzvaná centrálnou(/jinou) stanicou** a predáva ďalej **príznak indikujúci právo k vysielaniu**

  (metóda "peška"); rezervace, vyzývání
- ○ Protokoly multiplexovo-orientovaného prístupu – zpřístupnění L1 multiplexingu do L2; FDMA, TDMA

L2 Sítě

LAN

- Systematická topológia pre jednoduché siete (topológie = fyzické usporiadanie: zbernica, kruh, hviezda, strom, ...)

Kolizná doména: ak dôjde k vysielaniu súčasne viacerých staníc, nastáva kolízia - znehodnotenie signálu, nutnost opakovat

Zbernicová topológia (bus)

- Jednoduchá, nenáročná, lacná
- Kolizní doména tvořena všemi připojenými stanicemi
- CSMA/CD jako protokol řízení přístupu k médiu
- Náchylná k defektom (výpadok 1 kábla = výpadok celej siete)

Kruhová topológia

- 1 smer, metóda "peška"
- Kolizní doména = všechny stanice
- Náchylná k defektom (výpadok 1 kábla/zařízení = výpadok celej siete)

Hviezdicová topológia

- 1 centrálny prepojovací bod (hub, brisge, switch)
- Zložitejšie inštalovaná
- *Hub*: operuje na L1, kolizní doména = všechny stanice
- *Bridge, switch*: na L2, kolizní doména = jen dvě sousední stanice
- Nenachýlna k defektom (jen výpadek zařízení, ne sítě)

L2 siete - budování

- **Bridge (můstek)**
  - Transparentné prepojenie v sieti, cez ktoré prechádzajú všetky dáta
  - Odděluje sdílená média (kolize se nepřenáší)
  - Může mít víc jak 2 připojení
  - **Switch** je viacportový bridge
- Založeno na MAC adresách
  - Backward Learning Algorithm – můstek se učí umístění stanic naslouchánim na médiu (sledováním zdrojových adres). Rámce se směrují dle cílové adresy.
- Lze vytvořit sítě s cykly, distribuovaný *Spanning Tree Algorithm* pre výpočet kostry
- Nevhodné pre veľké siete – přepínací tabulky rostou s počtem stanic, pomalá konvergence

- Distribuovaný Spanning Tree Algorithm:
  - Cíl: nepoužívat některé porty můstků (zabránit cyklům)
  - Každý můstek posílá periodické zprávy – vlastní adresa, adresa kořenového můstku, vzdálenost od kořene
  - Když dostane zprávu od souseda, upraví definici nejlepší cesty: preferuje kořen s menší adresou, menší vzdálenost; stejné vzdálenosti = nižší adresa
  - Mechanismus: volba kořenového stromu (nejnižší adresa). Postupný růst stromu – nejkratší vzdálenost od kořene (pref. uzly s nižší adresou). Nalezené nejlepší cesty definují aktivní porty můstků, všechny ostatní porty vypnout.
  - Fáze výběru kořenového můstku: po zapnutí všechny můstky ohlásí, že jsou kořenem, každý z nich zašle konfigurační informaci na všechny

porty, na základě toho je zvolen můstek s nejnižší ID
    - Fáze výběru kořenových portů: každý můstek si za svůj kořenový port zvolí ten s nejnižší cestou k Root Bridge. Stejná cesta = nižší Port ID, druhý se vypne (stane se non-designated)
    - Fáze výběru aktivních/neaktivních portů: Root Bridge nastaví všechny svoje porty jako aktivní (designated). Na všech spojích, kde nejsou Root porty, si přepínače vyměňují informace a zjišťují nejnižší Bridge ID; ten potom nastaví svůj port jako aktivní, druhý s vyšším Bridge ID se vypne

- Proč nestačí L2?
    - Nemožnost vybudování geograficky rozlehlé sítě
    - Neuniformní prostředí

L3: Sieťová vrstva

- Prepojenie lokálnych sietí do väčších, komplexných sietí (internet)
- Možnost propojit kterékoliv stanice v internetu skrze více samostatných fyzických LAN sítí (tzv. host-to-host delivery)
- Príjima segmenty z transportnej vrstvy, ktoré transformuje na pakety
- Spolu s L2 zajišťuje přenos paketů mezi komunikujícími uzly
- Logicky spojuje samostatné heterogenní LAN sítě, vyšším vrstvám poskytuje iluzi uniformního prostředí jediné velké sítě (WAN)
- Poskytuje možnost jednoznačné identifikace (adresace) každého zařízení
- Adresácia: ve spolupráci s L2 mapuje adresy sieťovej vrstvy na fyzické adresy (MAC), zajišťuje smerovanie, multicast

Služby:
Internetworking - Prepojovanie sietí

- Vzájomné prepojenie viacerých sietí i jednotlivých kabelových segmentů (hierarchie). Propojením vzniká internetwork, zkráceně internet.
- **internet**: prepojenie 2 a viac sietí

- **Internet**: jméno 1 konkrétní siete
- Důvody:
    - Překonání technických omezení (dosah kabeláže)
    - Optimalizace fungování sítě (regulace toku dat, zamezení zbytečného šíření provozu)
    - Zpřístupnění vzdálených zdrojů
    - Zvětšení rozsahu poskytovaných služeb (e-mail, telefonování, …)
- Rozdíly dle vrstvy:
    - L1 – opakovač (repeater)
    - L2 – můstek, přepínač
    - L3 – router (směrovač)
    - V budoucnu – brána (gateway)
- V sieťovej vrstve sa prepája pomocou **router**-u
    - *Prepínanie okruhov* (Circuit Switching)
        - Stanovenie priameho fyzického spojenia medzi odosielateľom a príjemcom bez potřeby paketizace; vrstva L1. Connection-oriented (spojovaná) služba
    - *Prepínanie paketov* (Packet Switching)
        - Zasielanie nezávislých dátových jednotiek - paketov cez *virtuálne kanály* (**Virtual Circuit Approach** - pakety jednej relácie cestujú rovnakou cestou) alebo *datagramovým prístupom* (Datagram Approach - každý paket obsluhovaný nezávisle). Cesta ustanovena na L2/L3. Využito ve WAN, Frame Relay, ATM
        - Datagramový přístup – používá internet. Komunikace je nespojovaná.

Tvorba paketů (packetizing)

- Přijaté segmenty transformovány na pakety (IP protokol)

Fragmentace paketů (Fragmenting)

- Rozdělování segmentů na pakety s délkou závislou na vlastnostech/schopnostech sítě

Adresace

- Adresy entit síťové vrstvy – tzv. IP adresy, jedinečné skrze celou síť
- Pakety obsahují zdrojovou a cílovou IP adresu komunikujících entit

Mapování IP z/na MAC (Address resolution)

- ARP, RARP protokoly

Směrování (routing)

- Nalezení nejvhodnější cesty mezi komunikujícími entitami, reakce na chyby

Základní monitoring sítě (Control messaging)

- Základní informace o nedoručitelnosti paketů, stavu sítě, uzlů, atd.; **ICMP** protokol

Adresácia

- Každé zariadenie má unikátnu adresu (systém k jednoduchému smerovaniu)
- Systematické přidělování adres
- **IPv4 adresy**
  - 32 bitov
  - Rozsah adries 2^32
  - *Individuálne adresy (unicast)* - identifikácia jedného sieťového rozhrania (příjemce/odesílatele)
  - *Broadcast adresy* - zasielanie dát všetkým príjemcom na danej LAN (zdrojová adresa diagramu je unicastová)
  - *Skupinové adresy (multicast)* - skupina príjemcov, ktorí prejavili záujem o dáta; data směrovači rozesílána všem. Zdrojová adresa je unicastová
- **Prideľovanie adries**
  - **Classful Adressing**
    - Prvá metóda přidělování adres
    - Adresní prostor rozdelen do 5 tried (A - E)
      = Každá trieda rozdelená na pevny´počet sietí s pevnou maximálnou veľkosťou = plytvanie (nedostatečná granularita)
      - A trieda = 2^7 sítí, každá 2^{24} uzlů (20 971 552 adries)
      - B trieda = 2^{14}, 2^{16} (65 536 adries)
      - C trieda = 2^{21}, 2^8 (256 adries)
      - D třída = multicastové adresy
      - E třída = rezervovaný prostor (pro budoucí použití)
  - Adresa sítě (NetID) – identifikuje danou síť (nemůže být přidělena uzlu/rozhraní). Tuto informaci lze použít pro směrování
  - Adresa uzlu/rozhraní (HostID) – identifikuje jedinečný uzel v síti NetID
  - Příklad: HostID = 147.251.48.1 → třída B → NetID = 147.251.0.0
    - A = 123.0.0.0
    - B = 141.14.0.0

- C = 221.45.71.0
- Možné řešení: přidělování více síťových adres menší třídy – ale zase nárust směrovacích tabulek (+jejich prohledávání)
- Riešenie problému
  - Rozdelenie do podsietí (**subnetting**)
    - Standardní IP adresa poskytuje 2-úrovňovou hierarchii (adresa sítě + uzlu)
    - 3 úrovne: sieť, podsieť, uzol
    - Využitelné v nějaké geograficky omezené oblasti (univerzity, …)
    - Síť rozdělena na podsítě – subnetworks(subnets)
    - Princip uzavřenosti – zvenčí se jeví jako 1 síť, podsítě se rozlišují až na hraničním směrovači
    - Lokální, ne gloubální platnost
  - Znižovať veľkosť smerovacích tabuliek (**supernetting**)
    - Združuje susedné samostatné sieťové IP adresy
    - Spojuje několik původně samostatných IP adres v jednu výslednou
    - Využívá toho, že organizace má přidělen jeden souvislý blok adres určité třídy
    - Musí se shodovat v určitém počtu vyšších bitů své síťové části a vyčerpávat všechny bitové kombinace v nižších bitech (síť. část)

(a) Subnetting (b) Supernetting

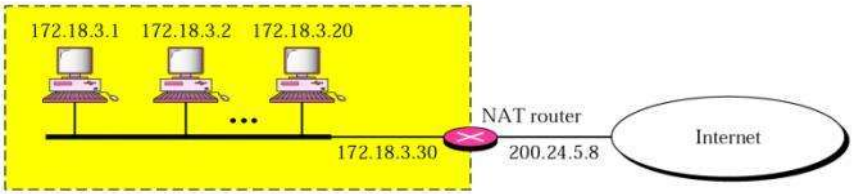
- **Maska siete/podsiete**
  - Identifikuje bity, které identifikují síť

- Subnetting – potřeba jen na hraničních směrovačích
- Supernetting – potřeba na všech směrovačích
- Maska sítě:
  - 32 bitový reťazec (v rámci IPv4)
  - 1 = síťová část adresy
  - 0 = relatívna adresa uzlu v rámci sítě
  - **IP adresa uzlu + maska sítě = adresa sítě**
    - A = 255.0.0.0
    - B = 255.255.0.0
    - C = 255.255.255.0
    - D = 255.248.0.0
    - E = 255.255.255.128

- **Classless Adressing**
  - Zobecnění a rozšíření subnettingu/supernettingu
    - Zavádza variabilnú dĺžku blokov (dovtedy bol najmenší počet pridelených adries 256 - trieda C)
    - Identifikace sítě = adresa + maska sítě
    - Prideľovanie adres hierarchicky – umožnění agragace směrování
    - **CIDR (= Classless Inter-Domain Routing)**
      - Konvencie popisující "pravidlá hry" – použití IP adres, významu masek, supernetting a subnetting
      - Nahradzuje pôvodné triedne prideľovanie (A, B, C, ...)
      - IP adresy prideľované po CIDR blokoch, ktoré majú variabilnú dĺžku, danú príslušnou maskou
      - Závislé na poskytovateľovi (zmena poskytovateľa = zmena adresy). Poskytovatel rozděluje CIDR blok dle uvážení
      - Snížení tempa vyčerpávání adresního prostoru
    - **NAT (= Network Address Translation)**
      - Ďalší mechanizmus zníženia tempa čerpania adries
      - Určeno pro domácí uživatele
        - Původně připojování modemy – možnost dynamického přidělování adres. Dnes většinou ADSL – trvalá alokace
      - Skrýva vnútorné siete do jednej (čínska univerzita) nebo několik externích

- ♦ V rámci sítě možnost využít mnoho interních adres
- ♦ Rezervované privátní adresy, unikátní v rámci organizace
- ♦ Vedlejší efekt: ochrana vnitřní sítě
- ♦ NAT smerovač prekladá adresy: prichadzajúce pakety podľa *Translation Table* (rozlišuje privátní/externí adresu), preklad odchadzajúcich paketov je triviálne

□



IPv6 adresy

- ○ 128 bitová adresy (16B)
- ○ Hexadecimálny zápis místo dekadického
- **Skracovanie zápisu**

▪

- Úvodní nuly lze vynechat, sekvenci nul taky (jen jednu skupinu!)
- Štruktúru adries definuje RFC 3587
- Cílem usnadnění směrování
- Globální směrovací prefix (adresa sítě, n bitů), adresa podsítě (64-n bitů), adresa rozhraní (64 bitů)
- Adresa podsítě obvykle 16 bitů – globální prefix 48
  - Prvních 16 = 2001_{16}, dalších 16 přiděluje RIR, dalších 16 LIR (regionální/lokální registrátory)
- Len *classless* (triedy neexistujú), popis s využitím notace CIDR
- **Typy adres:**

- *Individuálne adresy (unicast)* - identifikácia jedného sieťového rozhrania (=

IPv4)

- *Výberové adresy (anycast)* - označujú celú sieť, ale dáta sa doručia iba jednému príjemcovi (tomu, který je nejblíže)
- *Broadcast adresy* - v IPv6 sa nevyužívajú – nahrazeny speciálními multicastovými (např. všechny uzly na dané lince)
- *Skupinové adresy (multicast)* - skupina príjemcov, ktorí prejavili záujem o dáta (= IPv4), data vždy doručena všem členům skupiny, slouží pro adresování skupin počítačů a jiných síťových zařízení; prefix FF00::/8

Interakcia L3 s L2 - mapovanie adries

- *Hop-by-hop* mechanizmus doručení dat v IP sítích
- Predanie/doručenie správy na základe fyzickej MAC adresy
- 2 alternativy:
    - LAN príjemca = LAN odosielateľa
        - IP diagram obsahuje IP adresu příjemce, rámec L2 vrstvy MAC příjemce
    - LAN príjemca != LAN odosielateľa
        - IP diagram = IP adresa příjemce, rámec l2 = MAC směrovače
        - Směrovač po přijetí a zpracování diagramu jej vloží do nového rámce s MAC adresou dalšího směrovače ve snaze přiblížit se cíli
        - Po dosažení cílové LAN platí první možnost (lokálně)
- Nutnosť **mapovať IP adresy** na fyzické MAC
    - *Statické mapovanie*
        - Vytvoření statické tabulky párů (IP adresa, MAC adresa), obtížně spravovatelné
    - *Dynamické mapovanie*
        - **Address Resolution Protocol (ARP)**
            - Protokol pro zjištění MAC adresy uzlu/směrovače na základě IP adresy
            - Zaslanie *ARP request* **všetkým** uzlom na danej LAN (broadcast)
            - Paket sa spracova všetkými uzlami a odpovie len ten, ktorého IP adresa sa zhoduje s hľadanou; ostatní paket zahodí
            - Odpoveď *ARP replay*
            - ARP pakety baleny přímo do rámců L2 vrstvy
        - **Reverse Address Resolution Protocol (RARP)**

- Opak ARP – zpětný převod MAC adres na IP adresy; již se nevyužívá

IP protokol

- Najrozšírenejší protokol sieťovej vrstvy
- Doprava dat (diagramů) na místo jejich určení, a to i přes mezilehlé uzly – směrovače
- Tzv. Host-to-host delivery
- Uzly/rozhraní jednoznačně identifikovány IP adresami
- Využívá datagramový přístup k přepínání paketů, komunikace je nespojovaná
- Poskytuje nespolehlivou (best-effort) službu
- Doplněn dalšími protokoly (ICMP, ARP, RARP, IGMP) k ošetření nestandardních situací, identifikaci rozhraní na LAN apod.
- *Internet Protocol 4 (IPv4) - 1981, RFC 791*
- *Internet Protocol 6 (IPv6) - 1998, RFC 2460*

- **IPv4 datagram**
  - **Version (VER)**
    - Verze IP protokolu
  - **Header Length (HLEN)**
    - Dĺžka hlavičky IP datagramu, nezbytné kvůli poli Option
  - **Differentiated Services (DS), Type of Services (TOS)**
    - Třída datagramu v rámci kvality služby (QoS), odlišuje důležité datagramy
  - **Total length**
    - Dĺžka celého IP datagramu, max 2^{16} - 1
  - **Identification, Flags, Offset**
    - Fragmentácia: datagram prechádza rôznymi sieťami s rôznymi veľkosťami (*Maximum Transfer Unit)*
    - Rozdelenie na menšie fragmenty s vlastnou IP hlavičkou (na smerovači alebo zdrojovom uzle)
      - Je možné fragmentovať fragmenty
    - Zloženie fragmentov (len na cieľovo uzle):
      - Identifikácia fragmentu (**Identification**)
      - Znalosť počtu fragmentov (**Flags**)

- Znalosť pozície fragmentu v pôvodnom datagrame (**Offset**)

♦ **Time to Live (TTL)**
  - Riadenie maximálneho počtu smerovačov navštívených datagramom
  - Maximálny počet 255, pri každom hope -1 a ak je počet 0, paket je nedoručený/zahodený

♦ **Protocol**
  - Identifikace protokolu vyššej vrstvy využívajúci služeb IP vrstvy
  - Nutné pre špecifikáciu cieľového protokolu, forma de-/multiplexingu
  - Identifikátory určeny v online databázi IANA:
  - ICMP, IGMP, UDP, TCP, ...

♦ **Header Checksum**
  - Kontrolný súčet hlavičky IP datagramu bez dat – ta mají vlastní kontrolní součet
  - Zdvojení kvůli propočtu na směrovačích kvůli proměnným polím IP datagramu (TTL)

♦ **Source IP address, Destination IP address**
  - 32 bitová adresa identifikujúca odosielací/príjimací uzol

♦ **Options**
  - Volitelná součást IP datagramů, budoucí rozšíření IPv4

♦ **Data**
  - Vlastné prenášané dáta
  -

- Poskytuje nespoľahlivú (best-effort) službu, preto vytvorený *Internet Control Message Protocol*
  ♦ Príklady správ ICMP
    - Oznamy o chybách
    - Dotazy na stav siete/uzla
    - Časť paketov

- Fragmentace
  ♦ Datagram prochází po cestě různými sítěmi, ne všechny mohou přenášet data stejné velikosti
  ♦ Maximum Transfer Unit (MTU) – maximální velikost dat, které lze přenést využitým L2 protokolem
  ♦ Datagramy se mohou rozdělit na několik menších, každý s vlastní hlavičkou, na cílovém uzlu složeny zpět
- Využití polí IP hlavičky: Identification, Flags a Offset

- Identification – pole identifikuje původní datagram, kterému fragmenty náleží, tzn. mají všechny stejné identifikační číslo
- Flags – 3-bitová hodnota: 1 bit rezervovaný; do-not-fragment bit, fragment-more bit = pokud je 1, není posledním fragmentem
- Offset – relativní pozice fragmentu v původním datagramu
  - 13 bitů – offset max 8191, nelze pokrýt větší datagramy; jede po 8B

- Fragmentace se provádí na zdrojovém uzlu a na směrovačích, skládání jen na cílovém uzlu. Ztráta fragmentu = ztráta datagramu. Na směrovačích se neskládá, aby to zbytečně nezatěžovalo, a navíc mohou fragmenty putovat jinudy

Internet Control Message Protocol (ICMP)

- RFC 792, doprovodný k IP protokolu
- Poskytuje informace o chybách a informace o stavu sítě
- Zprávy nepředávány do síťové vrstvy, ale baleny do IP protokolu
- Zprávy o chybách (destination unreachable, time exceed), dotazy na stav sítě/uzlu (echo request/reply)
- Není generován pro chybu ICMP, broadcast/multicast zprávu, poškozenou IP hlavičku a chybu fragmentu (kvůli rekurzi)
- Zprávy obsahují část paketu, který způsobil chybu/na který se váže odpověď
- Ping, traceroute

- **IPv6 datagram**
  - Rozšírený adresný priestor (2^128 jedinečných adries)
  - IPv4:
    - Slabá podpora aplikací real-time
    - Nezabezpečená komunikace na IP úrovni
    - Nepodporuje autokonfiguraci zařízení
    - Nepodporuje mobilitu

  - Vlastnosti IPv6:
    - Rozšířený adresní prostor
    - Jednodušší formát hlavičky
    - Možnosti dalšího rozšíření - hlavičky
    - Podpora real-time – prioritizace provozu

- Podpora zabezpečení – autentizace, šifrování, verifikace integrity
- Podpora mobility – domácí agenti
- Podpora autokonfigurace
-

- **Základná hlavička + rozšírujúca**
  - Základní jen 40B (obsahuje iba najnutnejšie informácie)
  - Chybí kontrolní součet a options, fragmentační informace
  - **Version (VER)**
  - **Priority (PRI)**
  - **Flow label** – identifikuje proud od jednoho odesílatele k cíli (nevyužito, původně pro real-time)
  - **Payload Length**
    - Celková dĺžka IPv6 datagramu (bez zakladnej hlavičky)
  - **Next header** – hlavička transportního protokolu nebo rozšiřující
  - **Hop limit** = TTL v IPv4
  - **Destination address** – IP adresa zdrojového/cílového uzlu

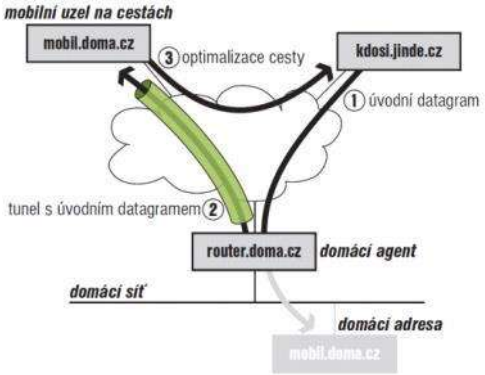
- **Zabezpečený prenos**
  - **IPSec**
  - V IPv6 povinná, v IPv4 doimplementováno později
  - Služby:
    - Autentizace a šifrování dat
  - Podpora v rozšírujucej hlavičke:
    - ***AH*** *(Authentication Header)*- autentizacia datagramu
      - Overuje totožnosť odosielateľa (autentizace)
      - Ochrana před vysíláním téhož
    - ***ESP*** *(Encapsulating Security Payload)* – autentizace/šifrovanie obsahu, ne současně
  - 2 režimy ochrany: **transportní** režim – bezpečnostní hlavičky vkládány přímo mezi ostatní rozšiřující
  - **Tunelující** – celý datagram zabalí jako data do nového datagramu, který má nové hlavičky, včetně bezpečnostních

- Bezpečnostní asociace (Security Association, SA)
  - Virtuální spojení dvou PC, které zajišťuje zabezpečený přenos
  - Součástí – použitý bezpečnostní protokol (AH/ESP) a jeho režim, šifrovací

algoritmus + klíče, čítače, doba životnosti, atd. Jednosměrné

- Dříve ISAKMP (RFC 2408), nyní Internet Key Exchange (IKEv2; RFC 4306)

- **Mobilita**
  - ♦ Domáca adresa - nemenná adresa, na ktorej je stroj trvalo dostupný – i když není momentálně v domovské síti
  - ♦ Dočasná adresa (Care-of address) - meniaca sa adresa
  - ♦ Domáci agent - smerovač v domácej siete (ak je potrebné, presmeruje dáta na dočasnú adresu)
- Stahuje na sebe datagramy směřující k mobilnímu uzlu a předává mu je tunelem
- Optimalizace cesty – seznámení vzdálené strany s aktuální dočasnou adresou mobilního uzlu pro zefektivnění komunikace



Ilustrace funkce domácího agenta v IPv6. (Satrapa P., IPv6)

- ♦ **Autokonfigurácia**
  - Stavová a bezstavová konfigurácia (nová)
    - ♦ Stavová – základem server spravující konfigurační parametry, které pak na požádání sděluje klientům; RARP → BOOTP → DHCP mechanismus; navrženo DHCPv6
    - ♦ Bezstavová – předpoklad, že směrovače ví vše, čas od času to ohlásí (Router Advertisement). Nově příchozí klient čeká na ohlášení, nebo si jej vyžádá, na základě toho pak vypočte svou IPv6 adresu (prefix + L2 adresa). Musí se doplnit třeba skrz DHCPv6

- Za prefix priloží 64 bitovú časť MAC adresy, počítač sa tak pripojí k sieti a IPv6 zistí všetky potrebné informácie

♦ **Fragmentácia paketov**
- Rovnaké ako v IPv4, rozdiel je vo vnútorných uzlov, ktoré nesmú fragmentovať , jen zdrojový může. Sníží to zátěž
- Nutnosť zistiť maximálnu veľkosť paketov – mechanismus Path MTU Discovery – zjištění minimálního MTU mezi dvěma uzly. Zjištěno před vlastní komunikací

♦ **Podporné protokoly**
- ICMPv6
  - Formát je zhodný ako v ICMPv4, stejné principy
  - Správy sú rozdelené na chybné (0,127) a informačné (128,255)
  - Zahrnuje funkcionalitu protokolů ARP a IGMP
  - IPv6 v hlavičce detekován hodnotou 58 v položce Next header

- **Mechanizmy na prechod IPv4 -> IPv6**

♦ Počítalo se s pozvolným přechodem – IPv4 a IPv6 musí koexistovat spolu
- ♦ Dvojný zásobník – zařízení podporuje oba IP
- ♦ Tunelovanie – IPv6 datagramy zabaleny jako data do IPv4 datagramu
- ♦ Translátory – Překlad IPv6 datagramů do IPv4 (klient → server) + odpověď

Smerovanie (Routing)

- Nájdenie cesty medzi dvoma komunikujúcimi uzlami, ktorá musí spĺňať obmedzujúce podmienky (topologie/zátěž sítě) a dopravit paket
- Problém teorie grafů – uzly směrovače, hrany - propojení, ohodnocení hran – cena komunikace; cíl: minimální cesta
  - Ohodnocení hran: všechny mají stejnou cenu, převrácená hodnota kapacity, zpoždění linky, využití linky, reálná platba
- Směrovač řeší jen jeden krok – komu paket předá dalšímu, blíže cíli. Hop-by-hop mechanismus. Ten pak určí, co s paketem bude dál
- **Směrování (routing)** – společná globální činnost směrovačů, proces vytváření a údržby směrovacích tabulek
- **Zasílání (forwarding)** – lokální pro každý směrovač. Vyžaduje přístup

ke směrovací tabulce

- **Smerovacia tabuľka**
  - Sada ukazovateľov, ktorá určuje čo robiť s ktorým paketom
  - Obsahují cesty k prefixům (počáteční IP adresa + blok)
  - Agragace záznamů – hledá se nejdelší prefix, který vyhovuje požadavku
- Problém získat znalost celé topologie, pořád se mění. Lokální představa o topologii = směrovací tabulka. Rozpor mezi lokální a globální znalostí může způsobit:
  - Cykly (černé díry)
  - Oscilace (adaptace na zátěž)

Základní přístupy:

- **Statický prístup (neadaptivní)**
  - Administrátorom ručne editované záznamy
  - Jednoduchšie, málo flexibilné
  - Smerovač nevytvára alternatívne cesty, pokud se cesta přeruší
- **Dynamický prístup (adaptivní)**
  - Reagují na změny v síti
  - Složité algoritmy
  - Nutnost aktualizace tabulek, možná dočasná nekonzistence
  - Nezaručuje správne poradie doručenia
    - centralizované – vše řídí centrum
    - izolované (RCC) – každý sám za sebe
    - distribuované – kooperace uzlů
      - výhody: pružné, robustné
- **Routing Control Center (RCC) – centralizované směrování**
  - Každý smerovač ho informuje o svojej situácií, z toho RCC vypočíta optimálnu cestu
  - Globální informace – optimální řešení, ulehčení práce směrovačů
  - Zle škáluje, nejde použiť vo veľkých sieťach, pomalé, při výpadku centra neaktuální
- **Izolované směrování**
  - Neposílají se informace o stavu sítě, každý sám za sebe
  - Příklady:
    - Náhodná procházka – paket poslán náhodně vybranou linkou; vysoká robustnost

- Horký brambor – paket poslán do linky s nejkratší frontou; vysoká robustnost
- Záplava – paket se pošle do všech linek kromě té, odkud přišel; enormní zátěž sítě, mimořádně robustní, vždy najde nejlepší cestu
- Zpětné učení – učí se z procházejících paketů

- **Distribuované směrování:**
  - Směrovací informace si vyměňují sousedé / malé skupiny
  - Výpočet mapy sítě, směrovací algoritmus
  - Pružné a robustní
  - Standardně používáno

- Internet / další členění
  - Distribuované — centralizované
  - Krok za krokem — zdrojové
  - Deterministické — Stochastické
  - Jedno — Více cestné
  - Dynamický — Statický výběr cest

Smerovacie algoritmy

- Sprostredkuvávajú funkcionalitu smerovania a výber komunikačnej cesty
- Proces vytvoření a údržby směrovacích tabulek
- Definice přesných pravidel komunikace a formátu zpráv nesoucích směrovací informace
- Rozdělení dle místa rozhodování:
  - Centralizované algoritmy (1 uzol)
  - Distribuované algoritmy (každý uzol)
- Dle okamžiku rozhodování:
  - Při uzavírání spojení (spojované služby, virtuální kanály)
  - Při příchodu paketu (nespojované služby, datagramy)
- **Požiadavky:** správnosť, jednoduchosť, efektivita, škálovateľnosť, robustnosť, stabilita, spravodlivosť, optimálnost

- Dle charakteru směrovací informace:
- **Distribuované smerovanie**
  - *Distance Vector (DV)*
    - Využ. Bellman-Fordov algoritmus
    - **Susedné** smerovače si v pravidelných intervalech nebo změně topologie vymieňajú kópie smerovacích tabuliek, podľa toho si doplňujú informácie a inkrementují své distance vektor číslo (počet hopů v síti)
    - Čili všechny informace jen svým sousedům
    - Úprava tabulek, aby se směrovalo co nejkratší cestou; problémy: pomalá konvergence, mnoho dat
    - Řešení pro to, aby nevznikaly cykly: dělení horizontu: směrovač nesděluje cestu zpět uzlu, od kterého se o ní dozvědel. Neřeší to při složitých topologiích
    - Protokol **RIP** (2 verzie)
      - Siete sú identifikované mechanizmom CIDR
      - Metrikou je počet hopov (nekonečno = 16)
      - Smerovače zasielajú informácie každých 30 sekúnd (časový limit 180 sekúnd = spojenie je DOWN)
      - Vhodné pre malé linky, nevhodné pro redundantní sítě
  - *Link State (LS)*
    - Smerovače si posielajú len informácie o stave liniek, na které jsou připojeny, udržujú tak kompletné informácie o topológii sieti, z toho sa počíta najkratšia cesta (Dijkstra)
    - Zaručená a rychlá konvergence
    - Vhodné i pre rozsiahlé siete
    - Čili informace o svých sousedech všem
    - Zložitejší algoritmus, väčšie nároky na CPU a pamäť smerovača
    - Zle kompromitovaný smerovač môže šíriť nesprávne informácie
    - Protokol **OSPF** (Open Shortest Path First)
      - Najpoužívanejsí protokol LS
      - Metrika je cena (číslo v rozsahu 1 až 65 535), přiřazené ke každému rozhraní směrovače - čím je číslo menšie, tým má cesta lepšiu metriku

- DV vs. LS
  - Složitost:
    - DV: Po změně ceny některé z linek je toto zapotřebí dát vědět jen nejbližšímu sousedovi, jindy jen při změně nejkratších cest
    - LS: Každý uzel zná cenu každé linky v síti a změna se musí oznámit všem
  - Rychlost konvergence:
    - DV: může být pomalejší než LS; problém s cykly
    - LS: trpí na oscilace
  - Robustnost:
    - DV: Nesprávný výpočet šířen sítí může zmást ostatní směrovače
    - LS: Šíření jen k sousedům, každý směrovač si přepočítává tabulky sám
  - Použití:
    - DV: Menší sítě
    - LS: Velké sítě

Autonómne sytémy

- Základní myšlenka: vzájemně propojené sítě, které spadají pod společnou správu, budou tvořit jediný autonomní systém, za který plně odpovídá jeho provozovatel
- V rámci svého AS lze dělat aktualizaci směrovacích údajů libovolně, navenek ale musí být stejný postup
- Cíl: snížení směrovací režie a zjednodušení srpávy sítě
- Autonomní systémy = domény
  - Každému AS přiřazen 16bitový identifikátor (ASN – AS Number) od společnosti ICANN
  - Odpovídají administrativním doménám – sítě a směrovače uvnitř jednoho AS spravovány jednou organizací (CESNET, PASNET, …)
  - Dělení podle způsobu připojení AS do sítě:
    - Stub AS – je připojen jen k dalšímu AS; směrovač A (hraniční) je výchozí
    - Multihomed / Transit AS; autonomní systém B je
      - Multihomed AS, pokud je připojen nejméně ke 2 dalším AS, mezi kterými neumožňuje přenášení provozu
      - Transit, pokud umožňuje (skrze LAN)

Smerovanie

- Oddělené směrování z důvodu škálovatelnosti
  - *Intradoménové (interior routing)* – uvnitř AS pod plnou kontrolou správce AS
    - Tzv. Interior Gateway Protocols (IGP), např. RIP, OSPF
  - *Interdoménové (exterior routing)* – mezi AS; Exterior Gateway Protocols (EGP), např. EGP, BGP-4
    - Směrovací pravidla dovolí třeba zakázat směrování přes jedno AS, pokud mezi dalšími dvěma vypadne spojení
    - Volba cesty nezávislá na lokálních požadavcích – asymetrie cest, kombinace nejlepších lokálních pravidel nemusí představovat globální optimum
    - **EGP** – první protokol mezidoménového směrování (1983); cílem dosažitelnost, nikoliv efektivita. Nepodporuje redundanci a neumí se vypořádat s cykly, už se nepoužívá
    - **BGP-4** (Border Gateway Protocol) – navržen kvůli růstu internetu, podporuje redundantní topologie i cykly. Používá path vector směrování, ale nevyměňuje ceny cest, ale popis cest včetně skoků. Umožňuje definici pravidel směrování, pracuje nad TCP, používá CIDR pro agregaci cest
    - **Path vector** – obdoba DV, posílají se celé cesty a ne jen koncové uzly. Definice pravidel (přátelské/nepřátelské AS), preferovány kratší cesty
      - Rozdíl DV: C je vzdáleno 2 hopy od A
      - PV přístup: cesta z A do C vede přes B
  - Nutná spolupráce interior a exterior směrovacích protokolů
- Jiné dělení:
  - *Interné* (směrovače vo vnútri systému)
    - Dôležité pre výkon
    - Znají cestu do všech podsítí
  - *Hraničné (border routers)*
    - Dôležité v škálovateľnosti
    - Sumarizují a zveřejňují cesty, aplikují směrovací pravidla
  - Jádro sítě nepoužívá implicitní cesty, směrovače musí znát cesty **ke všem** sítím

IP Multicast - skupinová komunikácia

- Dáta sú prenášané k skupine príjemcov, je preto potrebná replikácia dát. Kdyby byla součástí aplikace, musela by každá aplikace mít replikační modul, proto je to lepší řešit odděleně
- Príklady: streamované video, vieokonferencia (nízka latencia, obmedzenie počtu príjemcov), data produkovaná přístrojem
- Klasické riešenie skupinovej komunikácie
  - Best effort, UDP, skupinová adresa, hop by hop, jedna kópia dát, time to live paketov (TTL)
  - Jak identifikovat skupinu? Multicast IP adresa: IPv4 - *trieda D*, IPv6 - prefix *ff00::/8*
- 2 přístupy: Source based tree, shared tree (core based)
- Každý kto má multicastovú nebo skupinovou adresu, môže vysielať (stačí na adresu posielať pakety). Vysílajících je proměnný počet a nemusí být členem skupiny
- Príjemca sa môže pridať aj odobrať z prenosu, také proměnný počet; může patřit do více skupin současně

Source Based Tree

- Aktivita shora od zakládajícího
- Periodický broadcast
- Ořezávání větví bez členů
- Omezení šířky – TTL
- Pro úzce lokalizované skupiny
- Nevýhoda: režie, záplava broadcasty
- Protokoly: DVMRP (RIP), MOSPF (OSPF), PIM–DM

Core Based Tree

- Ustaveno jádro – body setkání (MP)
- Zájemce o skupinu kontaktuje MP
- Aktivita zdola od příjemce
- Redukce broadcastu $\longrightarrow$ lépe škáluje
- Nevýhoda: závislost na dostupnosti jádra
- Protokoly: CBT, PIM–SM (protokolově nezávislé)

- Vlastnosti multicastu:
- Nekonečná škálovateľnosť, nezaťažuje sieť zbytočnými kópiami
- Problém so zaistením doručenia, jednoduchý terč útokov (DoS, DDoS), problematické účtování, absence kontroly členství (nelze zjistit přijímající)

- Protokoly:
  - Správa skupiny:
    - pouze v rámci LAN
    - **IGMP** (Internet Group Management Protocol)
  - Směrování:
    - Mezi multicastovými směrovači
      - Source based tree: DVMRP (RIP), MOSPF (OSPF), PIM-DM
        - DVMRP – rozšíření unicastového DV směrování, používá RIP
        - MOSPF – rozšíření unicastového OSPF
        - PIM-DM – podobný DVMRP, ale nevyžaduje ke své činnosti RIP
      - Core based tree: CBT, PIM-SM
        - CBT – zdroj jako kořen stromu; AS rozdělen na regiony, pro každý zvolen bod setkání – vytvoření jádra
        - PIM-SM – předpoklad malé pravděpodobnost k multicastu; buduje záložní body setkání oproti CBT, v případě potřeby přepne do source based tree
- Správa skupiny – IGMP:
  - Spravuje informace o členech skupiny (pouze v rámci LAN), jen lokálně
  - Typy zpráv: přihlášení se ke skupině, odhlášení ze skupiny, monitoring skupiny

- Proč nestačí L3?
  - Nemožnost identifikovat aplikaci, které jsou data určena
    - Na každém uzlu by tak mohla běžet maximálně jedna aplikace
  - Neřeší defekty sítě – ztrátu/znásobení datagramu, zahlcení, …

L4: Transportná vrstva

- Dokáže identifikovať konkrétne aplikácie na uzlech (identifikované L3)
- Možnosti zajištění spolehlivého přenosu nad nespolehlivou (best-effort) IP sítí
- Dáta transformuje do segmentov a ďalej ich predáva aplikácii
- Spolu s L3 zajišťuje doručení dat (segmentů) mezi komunikujícími aplikacemi/procesy s případným zajištěním spolehlivosti přenosu
- *Proccess-to-proccess delivery*
- Nejnižší vrstva poskytující tzv. *end-to-end služby*
  - Hlavičky generované na straně odesílatele jsou interpretovány jen na straně příjemce; směrovače vidí data transportní vrstvy jako payload přenášených paketů

- **Služby:**

  - **Tvorba paketov (Packetizing)**
    - Utvorené pakety majú pridanú transportní hlavičku
  - **Riadenie spojení (Connection Control)**
    - Spojované (spojenie je udržiavané po celú dobu prenosu dát, pakety číslovány) a nespojované (pakety zasielané bez ustáleneho spojenia, nepotvrzovány) služby
  - **Adresácia (Addressing)**
    - Adresy entit transportní vrstvy – tzv. porty
    - Pakety obsahujú zdrojový a cieľový port
    - Aplikace jsou tak jedinečně detekované jako IP adresa:port
  - **Zaistenie spoľahlivosti prenosu (Reliability)**
    - Riadenie toku (Flow control) a chýb (Error control)
      - Na nižších vrstvách to bylo node-to-node, zde end-to-end
  - **Riadenie zahltenia siete (Congestion Control)**
    - A zajištění kvality služby (QoS)
- Adresy na L4 – čísla portů (adresy služeb); 16-bitové číslo (0 – 65535)
- Porty rozděleny do 3 tříd organizací IANA
  - Well-known: identifikují známou konkrétní službu (0 – 1023)

- Registrované porty (1024 – 49151) – lze je zaregistrovat
- Dynamické porty (49152 – 65535) – využity zejména jako zdrojové při odesílání

- Mechanismus adresace na L4 představuje formu multiplexingu a demultiplexingu
  - Na odesílající straně mnoho aplikací a jeden transportní protokol – MUX
  - Na přijímací straně jeden transportní protokol, výběr vhodné aplikace pro doručení – DEMUX; přijímací aplikace identifikována cílovým portem

User Datagram Protocol (UDP)

- Najjednoduchší transportný protokol poskytujúci **nespoľahlivú** (nespojovanú = nazaistenú) službu (best-effort)
- Ke službám IP vrstvy přidá jen process-to-process komunikaci a jednoduchou kontrolu chyb
- Zajištění spolehlivosti přenosu je na aplikaci
- Prenos blokov dát, ktoré hlavička UDP opatruje a posiela sieťovému protokolu
- Jednoduché, minimálna réžia, malá hlavička, nie je potrebné udržiavať spojenie ani staré stavové informace
- **Hlavička paketov**
  - **Zdrojový port** – identifikace odesílající služby/aplikace
  - **Cieľový port** – identifikace přijímací služby/aplikace
  - **Dĺžka UDP paketov**
  - **Kontrolný súčet** – hlavička + data
- Procesy komunikujú jednoduchým štýlom "požiadavka - odpoveď" (např. DNS)
- Interní řízení toku a kontrola chyb, např TFTP
- Real-time prenosy (napr. multimediálne prenosy, RTP), multicastové prenosy
- Aktualizace směrovacích tabulek RIP protokolem

- Proč se používá řízení chyb i zde? L2 vrstva to zařídí jen mezi dvěma uzly, ne mezi koncovými stanicemi
- Spolehlivost zajištěna mechanismem potvrzování:
  - pakety číslovány
  - Negativní potvrzování – zopakuj, prosím
  - Pozitivní potvrzování – doručeno v pořádku

- Pokud je chyba, data se znovu pošlou; mechanismus ARQ, musí se vypořádat s duplicitami
  - ♦ Stop-and-Wait ARQ – než dorazí p. potvrzení, nic jiného se nepošle; timeout pošle znovu; pakety střídat číslovány 0 a 1 pro potvrzení
    - Obousměrný provoz – **piggybacking**, místo 2 paketů (potvrzení, data) se posílá jen 1
    - Do sítě lze kdykoliv poslat jen 1 paket – degradace výkonu
  - ♦ Go-back-N – více paketů bez čekání na potvrzení, postupně číslovány, kumulativní potvrzení; lze použít piggybacking. Jeho varianta je v TCP
    - Informace o paketech uchovávány ve sliding windows – odesílatel 2^m
    - Neefektivní pro vysoce ztrátové linky, zahazuje pakety mimo pořadí
  - ♦ Selective-repeat – rozšíření Go-Back-N, místo 1 paketu v okně příjemce jich může pojmout více, out-of-order pakety u příjemce bufferovány; kumulativní potvrzení, lze udělat piggybacking, využívá p. i n. potvrzení

Transmission Control Protocol (TCP)

- Spojovaná, spoľahlivá služba
- Prenos prúdov bytov (x UDP – přenos bloků dat), ktore TCP segmentuje (veľkosť segmentov obmedzená *Maximum Segment Size (MSS))* a predáva sieťovému protokolu kompletne a v správnom poradí
- Každý prenášaný bajt je číslovaný
- Pred začiatkom prenosu je potrebné nadviazať spojenie medzi príjemcom a odosielateľom (tzv. *handshake* – výměna parametrů) - **point-to-point spojenie** – pouze dvojbodové (nepodporuje multicast)
- Spojení rozeznatelné jen na koncových uzlech (end-to-end)
- Možno využít pro duplexní komunikaci (piggybacking)
- MUX, DEMUX a detekce chyb stejná jako v UDP
- Přenos dat v UDP: aplikace předá bloky dat, UDP dá hlavičku a předá IP
- Přenos v TCP: aplikace předá proud bytů, TCP je segmentuje, dá hlavičku a předá je síťovému protokolu (IP). Aplikace mají iluzi roury
- Aplikací předaná data nutno uchovávat v bufferech (vyrovnání rychlosti)
- Segmentace: přijme proud bytů, IP očekává bloky dat, musí se tvořit segmenty (bloky dat) – omezeno MSS (definuje velikost uživatelských dat, ne celého segmentu); přidána TCP hlavička a předány IP
- Číslovány nejsou segmenty, ale jednotlivé byty

- **Hlavička segmentov**
  - **Zdrojový port**
  - **Cieľový port**
  - **Sekvenčné číslo segmentu** – každý byte, inkrementace o 1
  - **Číslo potvrdzovaného segmentu (acknowledgment number)**
    - Číslo nasledujúceho bajtu; piggybacking
  - **Dĺžka hlavičky** – délka TCP hlavičky ve 4B slovech
  - **Rezervované pole**
  - **Riadiace dáta**
    - 6 bitov riadiacich informácií
  - **Veľkosť okna** – pro řízení toku
  - **Kontrolný súčet** – hlavička + data
  - **Urgentné dáta** – zasílání dat mimo pořadí
    - Zasielanie dát mimo poradia
  - **Voľby**
- Full-duplex = obě strany musí inicializovat spojení; **3-cestný handshake**
- Ukončení inicializuje 1 strana, spojení uzavřeno oběma
- Error control: checksum, pozitivní potvrzení (kumulativní), timeout
  - Založen na Go-Back-N; buffer pro out-of-order segmenty je ale u příjemce
  - Timeout založen na Round-trip Time (RTT); typicky: timeout = 2 * RTT
- TCP zabráňuje zahlteniu príjemcu (Flow Control) a siete (Congestion Control)
- Množstvo dát, ktoré je možné zaslať = MIN (veľkosť okna příjemců (řízení toku); veľkosť okna zahltenia (řízení zahlcení))
- Flow control – explicitní zpětná vazba od příjemce – informuje o stavu svého přijímacího bufferu (zbývající místo)
- Řízení zahlcení (congestion) – zpětná vazba – síť dokáže informovat o blížícím se zahlcení (např. ATM); bez zpětné vazby – nutnost odhadovat (běžné IP sítě) – algoritmus AIMD
  - Proaktivní přístup – snaha předcházet zahlcení
  - Reaktivní přístup – jakmile je zahlceno, je to detekováno a sníží se rychlost
  - Kde dochází k zahlcení? Switche mají fronty, příchozí pakety potřeba zpracovat; příchod paketů rychlejší, než se zpracují, nebo výstup pomalejší než jejich zpracování
  - Zahlcení detekováno při ztrátě paketu (reaktivně); většina TCP je proaktivní

        - Odhadována velikost okna zahlcení; množství skutečně zasílaných dat v outstanding Windows
        - Odhadování velikosti:
            - Slow start – snaha o rychlé navýšení rychlosti po nějakou hranici
            - Additive increase – zpomalení rychlosti růstu, udržení vysoké rychlosti přenosu po co největší dobu
            - Multiplicative decrease – zahlcení sítě, snížení rychlosti přenosu
                - Zajišťuje férovou mezi TCP proudy
- Varianty TCP (líšia sa len mechanizmom pre odhad dostupnej kapacity): *TCP Tahoe, TCP Reno, TCP Vegas, TCP Hybla, TCP BIC, TCP CUBIC, Compound TCP*
- Jak dosáhnout lepšího využití sítě, zaručit rozumnou koexistenci s tradičním TCP a zajistit postupné nasazování nového protokolu? Protože TCP není připraveno na toto prostředí (San Diego – Brno: RTT = 205ms; TCP RTT 100ms)
    - Vliv RTT: řízení toku i zahlcení, použitá šířka pásma
        - problém „meziplanetárního" internetu – RTT vysoké, TCP nepoužitelné
- Víceproudové TCP – zlepšuje chování jen při izolovaných výpadcích paketů; komplikovanější než TCP, ne tak rychlý start, přetěžování front a cache (switch)
    - **Grid**DT – sbírka ad-hoc modifikací, rychlejší slowstart
    - Scalable TCP
    - High-Speed TCP – emuluje tradiční TCP v malých oknech/větších ztrátách
    - Early Congestion Notification **(ECN)** – tradiční rozšíření TCP; součást Advanced Queue Management (AQM); bit, který nastavují routery pro detekci zahlcení linky/fronty/bufferu. TCP má na ECN reagovat stejně jako na výpadek. ECN příznak musí být odzrcadlen přijímačem
        - E-TCP – odzrcadlení ECN bitu jen poprvé; umělé zavedení malých náhodných výpadků pro zajištění férovosti
        - Fast – používá end-to-end delay, ECN a ztráty paketů pro detekci a vyhýbání se zahlcení
- Přístupy odlišné od TCP:
    - Tsunami – TCP pro out-of-band řídící kanál, UDP pro přenos dat
    - Reliable Blast UDP – to samé; posílá uživatelem definovanou rychlostí
    - Dále: XCP, SCTP, DCCP, STP, Reliable UDP (spolehlivé in-order doručení)

L5: Relačná vrstva

- Spravuje relácie (dialogy) medzi komunikujúcimi stranami
- L1 – L4 orientovány spíš na přenos dat, vyšší vrstvy na potřeby síťových aplikací
- Nachádza sa iba v ISO/OSI modelu (nie v TCP/IP)
- protokoly: SSL, RPC, ASP, H.245, ...
- **Relácia** = dialog – spojení mezi dvěma koncovými účastníky na úrovni bezprostředně vyšší, než je vrstva transportní; analogie telefonního hovoru
- Zajištěno pomocí transportního spojení; jedno t. spojení může zajišťovat více po sobě jdoucích relací, nebo více t. spojení může zajišťovat jednu relaci
- *Riadenie dialógu* medzi koncovými účastníkmi (která aplikace smí vysílat)
  - Plne duplexné (obojsmerné; TWS, Two-Way Simultaneous)
  - Poloduplexné (striedanie obojsmerného a jednosměrného; TWA – Two-Way Alternate); řízen pomocí mechanismu předávání pověření k přenosu dat (**data token**)
  - Simplexné (jednosmerné; One-Way)
- *Synchronizácia (checkpointing)*
  - Ak je potreba vrátiť sa o kúsok späť (prerušenie tlače - zaseknutý papier)
  - Riešené mechanizmom kontrolných bodov (checkpoints), ke kterým se lze vrátit; hlavní (major), vedlejší (minor)

L6: Prezentačná vrstva

- Na rôznych architektúrach sú **odlišnosti** vo vnútornej reprezentácie dát
  - EBDIC kód (IBM) vs. ASCII
  - Jedničkový doplňkový (CBC Cyber) vs. dvojkový
  - Little Endian vs. Big Endian (Motorola, IBM 360/370)
- Nutnosť **jednotnej interpretácie dát =** úloha prezentačnej vrstvy
  - Přizpůsobení „každý s každým“ nebo převod do společného mezitvaru
- Předpoklad alternativy se společným mezitvarem
- Využíva jazyk **ASN.1** (Abstract Syntax Notation v.1)
  - Nutnost domluvy na vzájemném kontextu
- Aplikácia predáva prezentačnej vrstve dáta + ich popis v jazyku ASN.1; v TCP/IP se předpokládá, že úlohu prezentační vrstvy zvládne sama aplikace
- **Šifrovanie a kompresia dát**
- Protokoly: AFP, ASCII, EBCDIC, LPP, NDR, XDR, ...

L7: Aplikačná vrstva

- Proč nestačí L4 (transportní)? Z pohledu sítě stačí, z pohledu uživatele potřebujeme síťové aplikace
- Služby pre užívateľa, aplikácie (e-mail, WWW, DNS, …), programy, ...
- Aplikace = hlavní smysl existence počítačových sítí
- Aplikačné protokoly (HTTP, SMTP, ...) sú **súčasťou** sieťových aplikácií, včetně síťových aplikací a programů
  - protokoly definujú typy správ, syntax, sémantiku, časování
- **Základní členění**: Client-server / peer-to-peer; pull/push model; nároky na síť

- *Client-Server model*

Client-Server

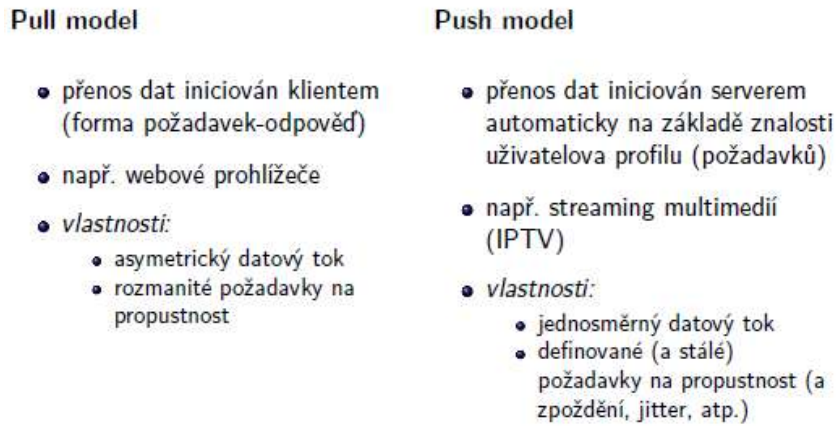
- komunikace iniciována klientem (klient = aplikační program ovládaný uživatelem)
- po ustavení komunikačního kanálu klient zasílá požadavky na server, ten mu odpovídá (mechanismus *request-response*)
- po ukončení komunikace je komunikační kanál uzavřen
- (centralizace zdrojů)
- valná většina aplikací v Internetu (WWW, FTP, DNS, SSH, ...)

Peer-to-peer

- jednotliví klienti spolu komunikují přímo (uzly jsou si rovnocenné)
- každý uzel poskytuje své zdroje (výpočetní síla, úložná kapacita, atp.) ostatním uzlům
- každý uzel využívá zdrojů poskytovaných ostatními uzly
- (decentralizace zdrojů)
- např. sdílení souborů (Gnutella, G2, FastTrack), Skype, VoIP, atp.

  - Klienty:
    - **Tenký klient (Thin)**
      - Na strane klienta sa vykonáva minimum aplikačnej logiky (väčšina na strane serveru)
      - Jednoduchšie, menšie nároky na HW - levnější
      - Menšia škálovatelnosť (moc práce dělá server), väčší objem prenesených dát, existence *Single point of failure* (server)
      - Napr.: vzdialené terminály
    - **Tlustý klient (Fat)**
      - Opak tenkého klienta – aplikační logika u klienta
      - Menší nároky na server (dobře škáluje), nižší objem dat, možnost *práce offline*
      - Komplexní provedení i instalace, velká spotřeba

lokálních zdrojů
    - Napr.: Firefox
- *Peer-to-peer model*
    - ♦ Klienti komunikujú priamo
    - ♦ Každý uzol poskytuje svoje zdroje a využíva zdroje ostatných uzlov
    - ♦ Skype, VoIP, ...
- *Pull / push model*



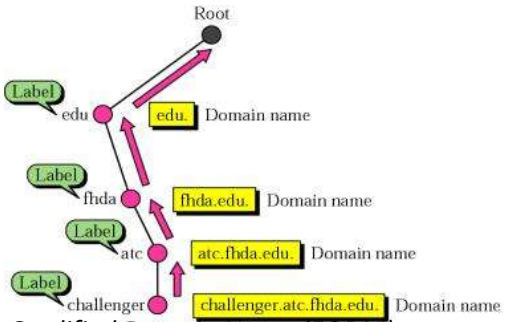
- Základné parametre z pohľadu aplikácií: strátovosť, priepustnosť (bandwidth), časové obmedzenie (delay / jitter)
- Z pohľadu programátora
    - ♦ Aplikácie komunikujú cez tzv. **sockety** (štruktúra jednoznačne popisujúca komunikujúcu aplikáciu)
        - **Family** (IPv4, IPv6, ...)
        - **Type** (prúdový, datagramový, základný)
        - **Protocol** (pre TCP a UDP nastavené na 0)
        - **Lokálna adresa socketu** (IP + číslo portu)
        - **Vzdialená adresa socketu** (IP + číslo portu)

- **Systém doménových mien DNS**
    - ♦ Služba na preklad doménových mien na IP adresy
    - ♦ V minulosti riešené pomocou **host** súborov (súbory s

dvojicami: doménové meno, IP adresa)

- Neefektívne s rastom internetu, neškálovatelné
- **DNS (Domain Name Space)**
  - Menný priestor = spôsob pomenovania předmětných entit
  - 2 varianty
    - *Plochý menný priestor* - bez jakékoliv vnitřní struktury
      - Napr.: MojRouterDomaVBrne
    - *Hierarchický menný priestor* - s hierarchickou vnitřní strukturou; možnost decentralizace správy (přidělování a kontrola jmen)
  - Varianta hierarchického uspořádání, max. počet úrovní = 128

- Každý uzol ma menovku (*label;* 63 znaků) a doménové meno (sekvence label, oddělená „ . “). Plné doménové jméno vždy končí „ . “



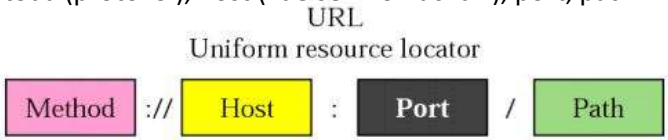
  - *Fully Qualified Domain Name (FQDM)*
    - Plné doménové meno končiace znakom "**.**"
    - Napr.: aisa.fi.muni.cz
  - *Partially Qualified Domain Name (PQDM)*
    - Neobsahuje všetky značky až ku koreňovému uzlu
    - Napr.: aisa.fi
  - **Doména**
    - Podstrom doménového menného priestoru
    - *Základné domény (generic)*

- *Národné domény (country)*
  - sk, cz, ca, us, ...
- *Reverzné domény (inverse)*
  - Slúžia pre mapovanie IP adries na doménové mená

- Rozoznávame
  - *Koreňové DNS servery*
    - Obsahujú informácie o top-level doménach
    - Aktuálne (máj 2013) 13 serverov po celom svete
  - *Primárne DNS servery*
    - Informácie o určitej doméne alebo jej časti
  - *Sekundárne DNS servery*
    - Redundantné servery získavajúce informácie o zónach
  - *Cache DNS servery*
    - Servery slúžiace na skrátenie doby odpovede na opakujúce sa dotazy
- Preklad doménových mien na IP adresy a späť sa nazýva *name-address resolution*

World Wide Web – HyperText Transfer Protocol (HTTP)

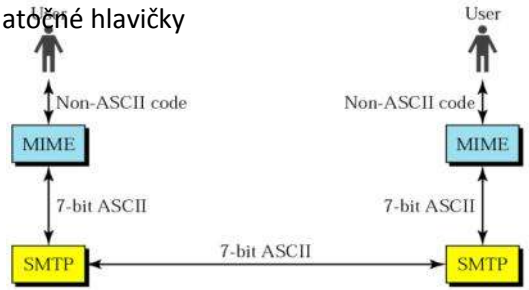
- protokol pre prístup k dátam na WWW (text, hypertext, audio, video, ...)
- klient zasiela požiadavku, WWW server zasiela odpoveď (TCP protokol na portu 80)
- **Hypertext -** text, ktorý obsahuje dodatočné informácie
- **URL** (Uniform ressource locator) – součást požadavku
  - definuje zdroj, ktorý chce klient získať
  - metóda (protokol), host (kde se info nachází), port, path



- *Nepersistentné spojenie*
  - TCP spojenie uzavrené pre každú požiadavku
- *Persistentné spojenie*
  - TCP spojenie pretrváva dlhšiu dobu
- **WWW dokumenty**
  - *Statické* - na serveru uložené dokumenty s pevným obsahem
    - HTML dokumenty, ...
  - *Dynamické* – neexistují v předem definovaném formátu
    - Tvorené na webovom serveri
    - PHP, CGI skripty, ...
  - *Aktívne*
    - Bežia na strane klienta, serverom poskytnuté programy
    - Java aplikácie, ...

Elektronická pošta – SMTP (Simple mail transfer protocol)

- Štruktúra:
  - *Obálka* - adresa odosielateľa, príjemcu, ...
  - *Správa* - hlavičky, telo správy, ...
- Adresa: **local_part@domain_name**
- Veľmi jednoduchý protokol, ktorý nedokáže posielať správy s diakritikou, non-ASCII dáta, súbory, ...
- Preto bol navrhnutý rozšírujúci protokol: **MIME (Multipurpose Internet Mail Extensions)**
- MIME nie je emailový protokol, ale iba rozšírujúci protokol, funguje iba s SMTP
- Obsahuje dodatočné hlavičky



- **Doručenie**
  - Lokálny poštový server stanový TCP spojenie (port 25) s poštový serverom
  - Po predáni správy je spojenie uzavrené
  - Predá email cieľovému poštovému serveru (mail.muni.cz)
  - Email môže byť nedoručený, ak sa adresa odosielateľa nachádza na black liste alebo ak príjemca neexistuje
  - Predá email cieľovému poštovému klientovi (something@mail.muni.cz) s využitím POP3 alebo IMAP4

- **POP3 (Post Office Protocol ver. 3)**
  - Jednoduchý protokol pre prístup k správam na poštovom serveri
  - využíva TCP port 110
  - Po autentizácií správy predáva a následne ich zmaže alebo ponechá v mailboxu
  - Predpokladá, že po každom spojení dochádza k zmazaniu mailboxu
  - Neumožňuje nahliadnúť do emailu pred stiahnutím

- **IMAP4 (Internet Mail Access Protocol ver. 4)**
  - Podpora organizácie správ na serveri, čiastočne stiahnutých emailov a náhľadov

Prenos súborov FTP

- Standardní mechanizmus internetu pre prenos súborov medzi uzlami
- Staršie ako SMTP
- Stanovuje **dva samostatné TCP spojenia**
  - Riadiace (TCP port 21)
    - Beží počas celého procesu
    - Musí byť stanovený typ súboru (textový alebo binárny), prenosový mód, vnútorná štruktúra

súboru
    - Dátové (TCP port 20)
        - Otvára a zatvára sa pri každom súbore

Multimediálne prenosy

- Požaduje relatívne veľke objemy dát
- Nároky na prenos (chybovosť, latencia, jitter, ...)
- Pr.: streaming audia/videa, videokonferencie (dôraz na minimálne end-to-end zdržanie), ...
- **Spracovanie zvuku**
    - Vzorkovanie a kvantovanie - prevod analógového zvuku do digitálneho
    - Použitie filtrov - odstránenie šumu/echa, ekvalizace, ...
    - Kompresia - zníženie dátového objemu
        - MP3, OGG, WMA, RA, ...
- **Spracovanie obrazu**
    - Vzorkovanie a kvantovanie
        - Vzorkování – odebírání vzorku signálu v definovaných časových intervalech (vzorkovací frekvence) – převod spojitéto průběhu signálu na diskrétní
        - Obraz je rozdelený na diskétne vzorky (768 x 576, 1920 x 1080, ...)
        - Kvantovanie určuje farbu/jas/intenzitu; diskrétní reprezentace hodnoty intenzity v okamžiku odebíraných vzorků
        - *Framerate*: počet obrazov za sekundu, typicky 25 fps
    - Úprava jasu, vyváženie bielej, kompresia (dôležitá u videí)
    - Komprese: MPEG, MJPEG, DV, HD, ...

- Prenosné protokoly
    - **TCP**
        - Zaistenie bezchybnosti na úkor zvýšení end-to-end latencie
        - Zajištění férovosti nedovoluje dostatečnou šířku

pásma na vytížených linkách

- **UDP**
  - Minimalistický, efektívnejší a rychlejší
  - Nemá režii spojenou s ověřováním bezchybnosti přenosu
  - Viac využívaný v případě přenosu multimediálních dat

- Nebylo na novějších slidech:
- **Videokonferencie**
  - Pri prenosu nejde používať buffery
  - Využíva kodeky s nízkou latenciou
  - Latencia a jitter sú najväčší problém
- **Streaming**
  - Vďaka jednosmernosti je možné použiť buffer
  - Latencia nie je problém (buffer)
- **RTP (Real-time Transport Protocol)**
  - Multimediálne prenosy využívajú UDP - UDP nepodporuje multimediálne aplikácie
  - Vznikol RTP, postavený nad UDP, obohacuje UDP
  - Identifikuje obsah, zadáva časové značky pre jednotlivé pakety
  - Nezaručuje kvalitu prenosu, len aplikáciam poskytuje prostriedky na prenos
- **RTCP (RTP Control Protocol)**
  - Rozširuje RTP
- **SIP (Session Initation Protocol), H.323, ...**
- **RTSP (Real-time Streaming Protocol)**
  - Založený na HTTP požiadavkách (GET, ...)
  - Ovládanie streaming serverov
  - Využíva RTP + RTCP protokoly
- **MMS (Microsoft Media Services)**

Bezpečnosť

Bezpečná síť by měla nabízet následující služby:

- **AAA**
  - **Authentication (Autentizácia)**
  - **Authorization (Autorizácia)**
  - **Accounting (Účtovanie)**

    +

    Zabezpečená komunikace:
  - **Confidentiality (Dôvernosť)**
  - **Integrity (Integrita)**
  - **Non-repudiation (Nepopierateľnosť)**

Authentication (Autentizácia)

- Overenie identity užívateľa (původce zprávy)
  - Podľa toho čo užívateľ **má, pozná, je, vie**

Authorization (Autorizácia)

- Oprávnenie použiť určitú službu alebo zdroj, následuje po autentizaci
- Udelenie oprávnenia alebo odoprenie přístupu

Accounting (Účtovanie)

- Sledovanie využívaných sieťových služieb užívateľom

Confidentiality (Dôvernosť)

- Ochrana dát pred neautorizovaným odhalením; zajištěno šifrováním

Integrity (Integrita)

- Ochrana dát pred neautorizovanou modifikáciou; zajištění, že během přenosu nedošlo ke změně dat

Non-repudiation (Nepopierateľnosť)

  - Příjemce dokáže protistraně dokázat přijetí (odesílatel odeslání) zprávy a tím zabrání pozdějšímu popření této akce protistranou

Kryptografia

- **Symetrická kryptografia**

- K šifrovaniu aj dešifrovaniu je použitý jeden kľuč
- Nízka náročnosť, vhodné pre dlhé správy
- Nutnosť zdieľania tajného kľuča
- DES, 3DES, IDEA, ...

- **Asymetrická kryptografia**
  - 2 kľuče (= pár kľúčov = keypair)
  - Šifruje sa verejným kľúčom, dešifruje súkromným kľúčom
  - Není potřebna nikam posílat šifrovací klíč – snížení rizika jeho vyzrazení
  - Pomalšie, vhodné pre kratšie správy
  - Např. RSA, DSA, …
- *Certifikát*
  - Viaže identitu entity (užívateľ, server, ...) s jeho verejným kľúčom
  - Obsahuje: meno, hodnota veřejného kľúča, doba platnosti veřejného klíče, podpis vydavateľa certifikátu
  - Vydávajú ich certifikačné autority (organizácie, ktorým sa dôveruje)
- Diffie-Hellman algoritmus – často používán pro zajištění důvěrnosti přenosu

- **Digitálny podpis**
  - Správa je podpísaná (= zašifrovanie) súkromným kľúčom, overované (= dešifrovanie) verejným kľúčom
  - 2 metódy:
    - Podpis celého dokumentu
    - Podpis otisku dokumentu (hash; najčastejšie používané)
- **Hashovacie funkcie**
  - Ze zprávy vypočten otisk (hash), který je pak podepsán (zašifrován soukromým klíčem odesílatele) a odeslán spolu s původním (nijak nešifrovaným) dokumentem
  - Dôraz na jednosmernosť (z otisku nelze získat zpět dokument) a one-to-one (2 rôzne správy nebudú mat rovnaký otisk)
  - Pro jakkoliv dlouhý dokument je vždy délka pevná
  - MD5 (prelomená), SHA-256

- **IP Security (IPSec)**
  - Kolekcia protokolov pre zabezpečenie na sieťovej vrstve; AH x ESP
  - 2 módy: transportní x tunelovací
  - Zabezpečení všech datových toků, netřeba upravovat aplikace; naopak zas žádné automatizované prostředky pro správu klíčů
- **SSL, TLS** – pro zabezpečení na L6, musí se upravit aplikace, aby šly na L7 (HTTP → HTTPS, FTP → FTPS)

Kvalita služby

- Všechny síťové toky jsou v TCP/IP obhospodařovány ekvivalentně, žádný není upřednostňován, na libovolném z nich může dojít ke ztrátě, zpoždění, …
- Jsou případy, kdy je nezbytné některé toky upřednostnit (prioritizovat) před jinými, resp. poskytnout jim definovanou kvalitu služby
  - Omezit ztrátovost, zpoždění, garantovat přenosovou rychlost, …
  - Nezbytné pro real-time, kritická řídící data, haptika (lékařství)

Požiadavky

- Spoľahlivosť – plná spolehlivost vs. tolerance ztrátovosti
- Zpoždění (rozptyl zdržania)
- Rozptyl zpoždění (jitter)
- Prenosová kapacita (bandwitdth)

Mechanizmy zaisťujúce kvalitu služby

- Plánování, formování/omezování toků, prevence zahlcení; zajistit na L2/3/4
- **Plánovanie**
  - Obsluha vstupných/výstupných front na odosielateľovi, príjemcovi a vnútorných sieťových prvkov
  - Struktura front a způsob jejich manipulace ovlivňují

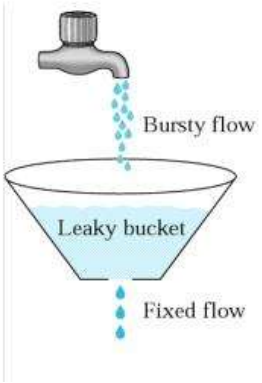
možnosti garance zpoždění přenosu, nutno kombinovat s dalšími přístupy

- *FIFO (First In First Out)*
  - Najjednoduchšie usporiadanie
  - Využ. iba 1 frontu pro obsluhu procházejících paketů
  - Žiadna podpora priority, agresivní proudy zvýhodněny
- *Priority Queuing*
  - Zoradenie paketov podľa prioritných tried
  - Každá priorita ma svoju FIFO frontu
  - Vyššia priorita = skoršia obsluha; nižší odešlou až po všech vyšších
  - Výhoda: garantována přednostní obsluha – nižší zpoždění
  - Nevýhoda: pakety s nízkou prioritou nemusia byť nikdy oblúžené, pokud existuje kontinuální tok (= **starvation**)
- *Weighted Fair Queuing*
  - Pakety su opäť zoradené do prioritných front
  - Frontám sú priradené váhy
  - Vyššie váha = vyššia priorita
  - Striedavá obsluha podľa váhy (Round Robin mechanismus)
  - Řeší problém starvation

- **Formovanie/obmedzovanie tokov**
  - Riadenie množstva a rýchlosti odosielania paketov
  - Kritéria: průměrná rychlost odesílaných paketů (average rate), špičková rychlost (peak rate), maximální počet paketů, které lze zaslat najednou (burst size); dlouhý časový interval/krátký/velmi krátký
  - 2 mechanizmy:
    - *Leaky Bucket*
      - Využitie pre vyhladzovanie toku, ovlivňuje average rate
      - Nepravidelný tok je priemerovaný (= konštantná rýchlosť)
      - Pokud je plno, nově příchozí pakety jsou zahozeny
      - Restriktivní, penalizuje nečinné uzly - nedovolí

nashromáždit tokeny

➢ •



- *Token Bucket*
  - Ovlivňuje peak rate a burst size, umožňuje krátkodobé špičky
  - Za prenesenú dátovú bunku je z koša odobraný token
  - Ak je uzol nečinný, umožňuje nazhromažďovať tokeny
  - Veľkosť koša ovplyvňuje veľkosť špičiek

- **Prevencia zahltenia**
  - Fronty sa môžu zaplniť a nové dáta sa zahadzujú
  - Preto boli vytvorené 2 metódy
    - *Random Early Detection (RED)*
      - Ak presiahne zaplnenie fronty určitú medzu, začne směrovač zahadzovať pakety náhodných tokov; odesílatel stáhne rychlost odesílání
    - *Weighted Random Early Detected (WRED)*
      - To iste čo RED, ale záleží aj na priorite paketov (toku)

Kvalita služby internetu

- *Integrované služby*
  - Oznamování parametrů QoS a rezervace zdrojů na vnitřních prvcích sítě (po cestě k příjmeci)
  - Aplikácia oznámi sieti kvalitatívne požadavky na přenos
  - Sieť overí, či sú požadované prostriedky k dispozícií
  - Ak nejde vyhovieť - spojenie je zrušené; aplikace může

slevit z požadavků a chtít méně náročné QoS
    - Ak áno - komponenty siete rezervujú odpovedajúci objem prostriedkov; rezervační protokol RSVP nebo YESSIR
    - Nevýhoda: nutnosť udržovať stav na vnitřních prvcích sítě (problémy so škálovatelnosťou)
- *Rozlišované služby*
    - Značkování paketů, jejich zařazení do tříd, prioritní obsluha na vnitřních prvcích sítě
    - Neoznamujú žiadne požadavky – vystačí si s garancí, že se kvalita přenosu výrazně nezhorší při změně zatížení sítě
    - Paket je označený značkou, ktorá určuje kvalitativní třídu přenosu
    - jednoduché, žiadne stavové informácie (dobrá škálovatelnost) a žiadne úvodné zdržanie, protože se nic nemusí rezervovat

Samoorganizující se sítě (P2P a ad-hoc sítě)

Překryvové sítě & P2P

- P2P síť je typicky virtuální síť utvořená nad existující síťovou infrastrukturou
    - Překryvová síť využita pro indexování a zjišťování sousedů (peerů); P2P síť nezávislá na topologii základové sítě
    - Nový peer musí za účelem připojení k P2P získat informaci nejméně o jednom jejím členovi
        - Nezbytné: IP adresa, port, …
- **Centralizované** – jeden nebo více centrálních serverů, poskytujících různé služby
    - Kombinace výhod centralizovaných (klient-server) a decentralizovaných distribuovaných systémů
    - Peerové zasílají centrálnímu serveru dotazy na vyhledání uzlu, který obsahuje požadované zdroje
    - Pokud peer získá kontakt na jiný peer, komunikuje s ním

přímo bez účasti centrálního uzlu
    - ♦ Citlivé na útoky, single point of failure, nevhodné pro mnoho účastníků, slabá škálovatelnost a robustnost
    - ♦ Vědecké výpočty, sdílení digitálních dat (Napster), Jabber, …
- **Decetralizované** (Pure P2P) – neobsahují žádné centrální servery – musí řešit strukturu (**plochá vs. hierarchická** (směrovací struktury se sestávají z více vrstev)) a topologie překryv sítě (**nestrukturovaná vs. strukturovaná**)
    - ♦ Každý z peerů má pouze částečnou představu o celé síti a poskytuje data, která mohou být relevantní pouze některým dotazům
    - ♦ Immuní vůči single point of failure, vysoký výkon, škálovatelnost, robustnost a další žádoucí výhody
    - ♦ Gnutella, Crescendo, PAST, FreeNet, Canon, …
    - ♦ **Nestrukturovaný** P2P systém – každý z peerů je zodpovědný za svá vlastní data a drží si info o svých sousedech, na které může směřovat vyhledávací dotazy
        - Lokalizace dat je výzvou, bez garance kompletní odpovědi, bez garance doby na odpověď
    - ♦ **Strukturovaný** – lokace dat je pod kontrolou určité, předem definované strategie (distribuované hashovaní tabulky – **DHT)**
        - Existuje mapování mezi daty a peery, na kterých jsou data uložena
        - Mohou poskytovat garanci odpovědi na úkor vyšší režie
- **Hybridní P2P systémy** – kombinace obou výše zmíněných; hlavní výhodou centralizovaných systémů jsou rychlé a přesné odpovědi na vyhledávací dotazy, na úkor škálovatelnosti sítě – ale hlavní výhodou decentralizovaných P2P systémů je škálovatelnost, na úkor delšího času pro vyhledávání
    - ♦ Neexistují centrální servery, ale některé peery jsou vybrány a prohlášeny za servery sloužící dalším peerům (*superpeers*)

- **Bezdrátové sítě** tradičně založeny na tzv. buněčné infrastruktuře – dané území, které má být pokryto, rozděleno na tzv. buňky, každá z nich pokryta základovou stanicí, mezi sebou propojeny

bezdrátově

- Veškerá komunikace mezi mobilními zařízeními jde přes stanici
- Např. GSM, UMTS, WLAN, …
- Nemožnost vybudovat klasickou bezdrátovou síť → wireless ad-hoc network
  - Vybudována pro speciální účely
  - Kolekce autonomních uzlů, komunikujících spolu přes multihop síť, která je spravována decentralizovaným způsobem
  - Každý uzel zároveň koncovým uzlem i síťovým směrovačem
  - Velmi rychlé vybudování, odolnost, efektivnější využití rádiového spektra než u buněčných sítí (každý může komunikovat s každým)
  - Neexistence centrální entity organizující uzly, omezený dosah, mobilita uzlů (→mobilní ad-hoc)
  - Otázky u řízení přístupu a směrování
- **Mobilní ad-hoc** – vyhýbání se dopravním zácpám, záchranné operace při katastrofách, vojenské operace, zasíťování osobních zařízení (hodinky, PDA, …)
- **Dopravní ad-hoc (VANETs)** – využívá pohybujících se aut jako uzlů/směrovačů pro vytvoření mobilní sítě

Bezdrátové senzorové sítě (MANETs)

- Místo lidí interakce s prostředím pomocí senzorů
- Záchranné akce, monitoring prostředí (požáry), inteligentní budovy, mosty (zemětřesení)
- Omezená životnost baterie, využité síťové protokoly musí být úsporné
- Využití bezdrátové multi-hop komunikace, samoorganizace sítě
- Podobnost s P2P: stejné paradigma, samoorganizace, dynamická topologie, neexistence centrální entity, zodpovědnost za směrování dotazů
- Spíše platformou pro P2P aplikace