Úvod

19. februára 2013 12:17

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*
- *Prenosné médium*: optický kábel, vzduch, ..
- *Protokol*: sada pravidiel

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 *%*
- *Zdržanie prenosu* (latency, delay): čas odoslania po prijatie správy (najčastejšie v *ms*)
- *Rozptyl* (jitter): variabilita v doručovaní paketov; rozdiel medzi najväčšou a najmenšou odozvou na požiadavok

Ideálne siete / skutočné:

- *dôvody*: preťaženie siete -> spomalenie; dĺžka cesty
- neobmedzená priepustnosť / obmedzená
- žiadne straty dát / dochádza k stratám
- žiadne zdržanie / dochádza k zdržaniu
- 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

Základné prístupy

Spojované siete

- 2 fázy: nadviazanie spojenia (udržuje sa počas celej komunikácie) -> prenos dát
- Nutnosť uchovávať stav
- Jednoduché zaručenie kvality
- Napr. analógové telefónne siete

Nespojované siete

- Dáta sú rozdelené na malé pakety, ktoré môžu byť ešte fragmentované, sú vysielané samostatne, v rôznom poradí
- Príjemca ich potom zloží do pôvodného stavu
- Problematická implementácia kvality služby
- Netreba uchovávať stav siete
- Napr.: Internet

End-To-End prístup (E2E)

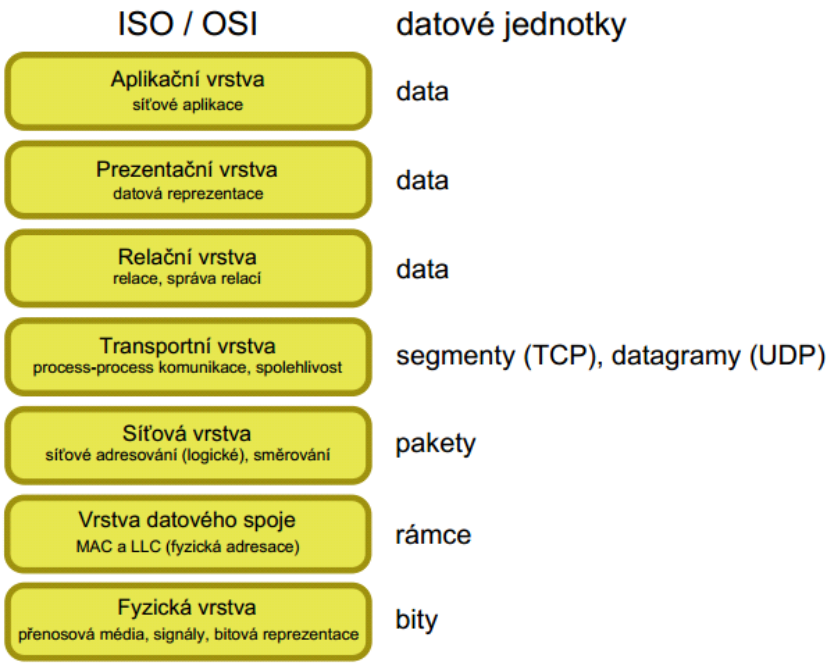
- Požadovanú funkcionalitu je možné zaistiť iba pomocou samotnej applikácie
- E-mail

Hop-To-Hop prístup (HbH)

- Opakovaním funkcionality je možné zvýšiť výkon
- Vyžaduje uchovávanie stavovaých informácií
- Vhodný pre real-time aplikácie

ISO/OSI Model

- **7 vrstiev**



- Každá vrstva je zodpovedná za určitú funkcionalitu
- Každá vrstva komunikuje len so susediacimi vrstvami
- Iný model: **TCP/IP**

Aplikačná vrstva
- Rozhranie medzi užívateľom a sieťou
- Zahrňuje sieťové aplikácie a protokoly

Prezentačná vrstva
- Zaisťuje jednotnú reprezentáciu dát
- Funkcionalita je zaistená samotnou aplikáciou

Relačná vrstva
- Spravuje relácie medzi komunikujúcimi aplikáciami
- Funkcionalita je zaistená samotnou aplikáciou

Transportná vrstva
- Zaisťuje identifikáciu a doručenie dát (segmentov) medzi dvoma komunikujúcimi procesmi

Sieťová vrstva
- Zaisťuje identifikáciu a doručenie dát (paketov) medzi dvoma komunikujúcimi uzlami

Spojová vrstva
- Zaisťuje prenos dát (rámcov) medzi uzlami prepojenými prenosovým médiom

Fyzická vrstva
- Riadi deje v prenosovom médiu: prenos dát, kódovanie, ..

Komunikačné protokoly

Priebeh komunikácie:

- Výzva
- Akceptácia
  - Akceptované
  - Odmietnuté
  - Time-out (opakovanie žiadosti)

- Komunikácie medzi HW/SW riadená protokolom
  - **Protokoly** riadia tok bitov, rýchlosť a smer paketov
  - Určujú: "*ČO?*", "*AKO?*", "*KEDY?*"
  - Definujú: syntax (formát dát), sémantiku (úkony vykonané pri odosielaní a príjimaní správ), časovanie (poradie správ)
  - Príklady: UDP, TCP, IP, IPv6, SSL, TLS, HTTP, FTP, SSH, ...

Štandardizácia

Typy:

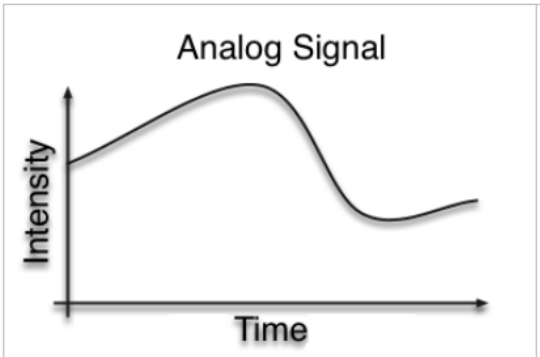
- **De facto**: technické riešenia, ktoré sa presadili na trhu a su všeobecne akceptované
- **De jure**: štandardy schválene normalizačným orgánom (napr.: ITU-T, ISO, IEC, IEEE, ANSI, EIA, IETF, ...)

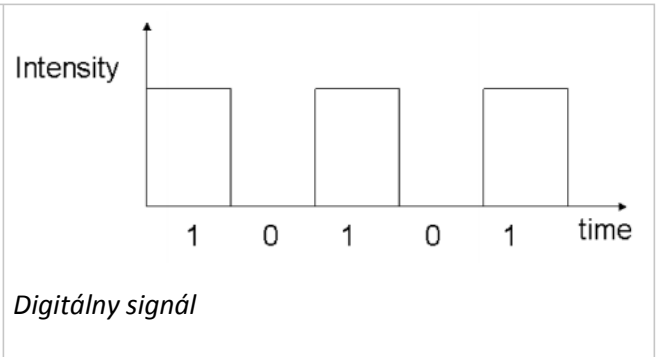
L1: Fyzická vrstva

26. februára 2013 12:32

- Len point-to-point spoje - nie je treba riešiť adresáciu, pretože neexistuje viac spojov
- Dáta sú vyjadrené 0, 1 zoskupené do rámcov
  - Prenášajú sa **analógovým** alebo **digitálnym signálom**
    - Analógový signál je možné modulovať (na to slúži *modem*)
- Fyzická vrstva transformuje bitový obsah rámcov
- **Hlavný cieľ**: prenos bitov (= obsah rámcov) medzi odosielateľom a príjemcom
- Dôležité sú **štandardy**: definujú parametry, význam a časový priebeh signálov, zapojenie konektorov, ...

- Dáta súmédiom prenášané elektromagnetickými signálmi
- **Signál**: časová funkcia reprezentujúca zmeny fyzikálnych vlastností
- *Analógové* (spojitý v čase)*, digitálne* (diskrétny v čase) *prenosy*

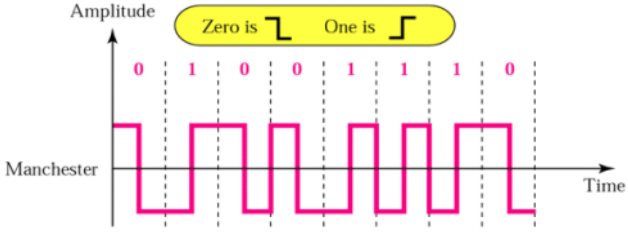




Digitálny signál

Digitálny prenos

- **Kódovanie**:
  - *Priame*: 1 = kladná amplitúda, 0 = záporná
  - *NRZ*: NRZ-L (1 = záporná, 0 = kladná) a NRZ-I (1 = zmena polarizácie, 0 = žiadna zmena)
  - *Manchester*:



  - *4B/5B*: substitúcia 4-bitových blokov na špeciálne 5-bitové vzorky

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

Defekty signálov

- **Slabnutie**, stráta energie: spôsobené napríklad odporom
- **Skreslenie**, stráta tvaru: spôsobené rozdielnou rýchlosťou signálov

- **Šum**: vplyv cudzorodej energie

Prenosové média

- Poskytujú prostredie
    - *Vodené média*: optický kábel, krútená dojlinka, koaxiálny kábel, ...
    - *Nevodené média*

Multiplexing

- Technika zdieľania dostupnej prenosovej kapacity
- Analógové signály:
    - *FDM: Frequency Division Multiplexing*
    - *WDM: Wave Division Multiplexing*
- Digitálne signály:
    - *TDM: Time Division Multiplexing*
- Zariadenie zabezpečujúce multiplexing: Multiplexor (MUX)
- Prevod späť na jednotlivé signály: Demultiplexor (DEMUX)

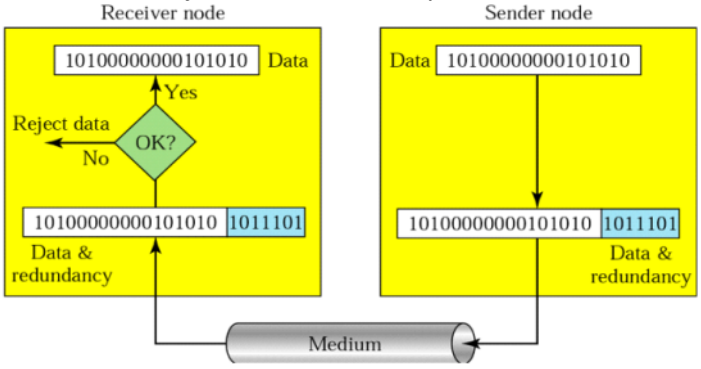
L2: Vrstva dátového spoja

26. februára 2013 13:18

- Lokálna sieť LAN
- Node-to-node delivery - prenos medzi uzlami
- Prijíma pakety zo sieťovej vrstvy, ktoré transformuje na rámce
- V spolupráci s fyzickou vrstvou zaisťuje prenos rámcov

Služby

- *Tvorba rámcov - framing*: pakety balené do rámcov
- *Adresovanie - addressing*: fyzické/MAC adresy
  - 

  - Každá stanica má unikátnu MAC adresu
- *Chybové riadenie - error control*
  - Chyba = zmena hodnoty bitu
  - L2 vrstva detekuje a robí korekciu chýb
  - 

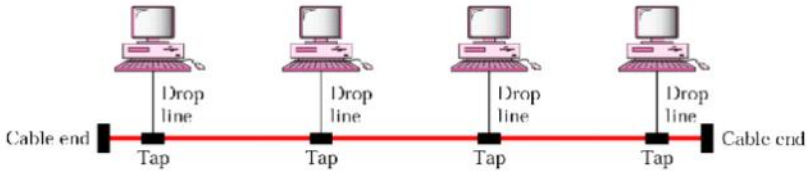
  - **Kódy pre detekciu chýb*:***
    - Párna/nepárna parita (veľmi slabá kontrola)
    - Cyklické kódy (silná kontrola)
    - CRC
      - Zo vstupných dát sa vypočíta číslo, ktoré príjemca podľa danej funkcie prepočíta a skontroluje správnosť dát
- *Riadenie toku - flow control*: zabraňuje zahlteniu príjemca (stop-and-wait)
- *Riadenie prístupu k médiu - MAC protokoly*
  - Cieľ: eliminovať konflikty pri vysielaní
  - Protokoly neriadeného prístupu (riešia kolízie až keď nastanú)
    - **Aloha**:
      - Stanica vysiela vždy, keď má pripravený rámec (dáta)
      - Predpoklad kolízii
      - Po kolízii istú dobu počká a tak znova vysiela
      - *Neefektívne*
    - **CSMA/CD**:
      - Upravená Aloha
      - Stanica vysiela, len ak je v médiu pokoj
      - CD = Collision detection
      - Aplikácia v klasickom LAN Ethernetu
    - **CSMA/CA**:
      - Obchádza kolízie
  - Protokoly riadeného prístupu
    - Stanica vysiela len ak má **právo**, v predom **dohodnutých intervaloch**, len ak je **vyzvaná centrálnou stanicou** a predáva ďalej **príznak indikujúci právo k vysielaniu** (metóda "pešiaka")
  - Protokoly multiplexovo-orientovaného prístupu

LAN

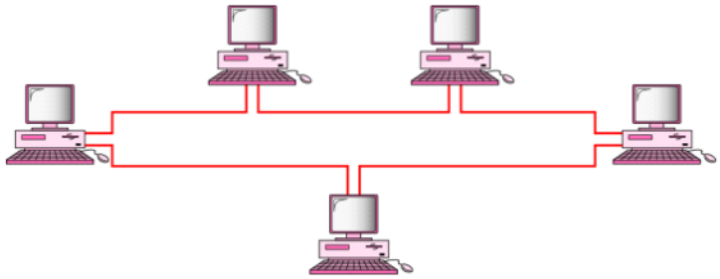
- Systematická topológia pre jednoduché siete (topológie = fyzické usporiadanie: zbernica, kruh, hviezda, strom, ...)

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

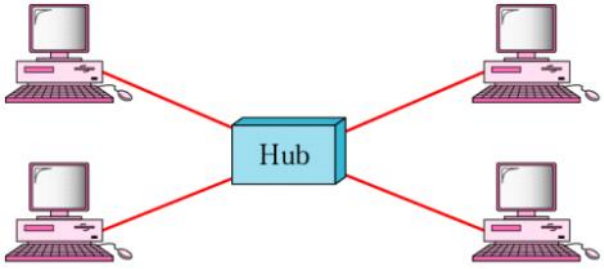
Zbernicová topológia

- Jednoduchá, nenáročná, lacná, ...
- CSMA/CD
- Náchylná k defektom (výpadok 1 kábla = výpadok celej siete)
- 

Kruhová topológia

- 1 smer, metóda "pešiaka"
- Náchylná k defektom (výpadok 1 kábla = výpadok celej siete)
- 

Hviezdicová topológia

- 1 centrálny prepojovací bod
- Zložitejšie inštalovaná
- *Hub*: operuje na L1
- *Bridge, switch*: na L2
- Nenachýlna k defektom
- 

L2 siete

- **Bridge**
  - Transparentné prepojenie v sieti, cez ktoré prechádzajú všetky dáta
  - **Switch** je viacportový bridge
- MAC adresy
- Cykly, *Spanning Tree Algorithm* pre výpočet kostry
- Nevhodné pre veľké siete

L3: Sieťová vrstva

5. marca 2013 12:59

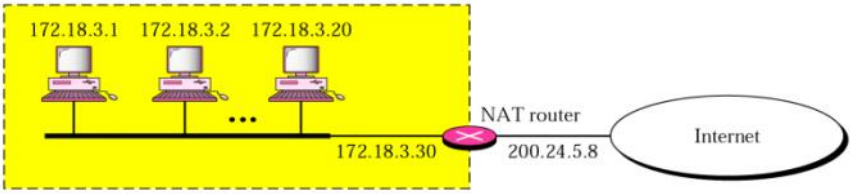
- Prepojenie lokálnych sietí do väčších komplexných sietí (internet)
- Príjima segmenty z transportnej vrstvy, ktoré transformuje na pakety
- Spojuje a zabezpečuje prenos paketov v LAN sieťach
- Adresácia: mapuje adresy sieťovej vrstvy na fyzické adresy (MAC), smerovanie, multicast

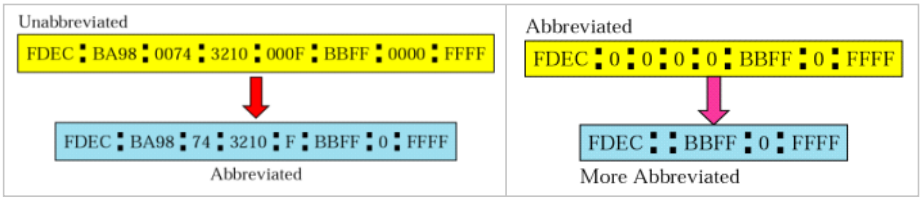
Internetworking - Prepojovanie sietí

- Vzájomné prepojenie viacerých sietí
- **internet**: prepojenie 2 a viac sietí
- **Internet**: meno 1 siete
- V sieťovej vrstve sa prepája pomocou **router**-u
    - *Prepínanie okruhov* (Circuit Switching)
        - Stanovenie priameho fyzického spojenia medzi odosielateľom a príjemcom
    - *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)

Adresácia

- Každé zariadenie má unikátnu adresu (systém k jednoduchému smerovaniu)
- **IPv4 adresy**
    - 32 bitov
    - Rozsah adries 2^32
    - *Individuálne adresy (unicast)* - identifikácia jedného sieťového rozhrania
    - *Broadcast adresy* - zasielanie dát všetkým príjemcom na danej LAN
    - *Skupinové adresy (multicast)* - skupina príjemcov, ktorí prejavili záujem o dáta
- **Prideľovanie adries**
    - **Classful Adressing**
        - Prvá metóda
        - Rozdelenie do 5 tried (A - E)
            - Každá trieda rozdelená ne pevny´počet sietí s pevnou maximálnou veľkosťou = plytvanie
            - A trieda = 20 971 552 adries
            - B trieda = 65 536 adries
            - C trieda = 256 adries
            - Nárast smerovacích tabuliek
            - Riešenie problému
                - Rozdelenie do podsietí (**subnetting**)
                    - 3 úrovne: sieť, podsieť, uzol
                - Znižovať veľkosť smerovacích tabuliek (**supernetting**)
                    - Združuje susedné samostatné sieťové IP adresy
        - **Maska siete/podsiete**
            - 32 bitový reťazec
            - 1 = sieťová adresa
            - 0 = relatívna adresa uzlu
        - **IP + Maska = adresa siete**
        - *NetID*: identifikácia siete
        - *HostID*: identifikácia uzlu v sieti NetID
    - **Classless Adressing**
        - Zavádza variabilnú dĺžku blokov (dovtedy bol najmenší počet pridelených adries 256 - trieda C)

        - Prideľovanie hierarchický
        - **CIDR**
            - Konvencie, "pravidlá hry"
            - 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)
        - **NAT**
            - Ďalší mechanizmus zníženia tempa čerpania adries
            - Skrýva vnútorné siete do jednej (čínska univerzita)
            - NAT smerovač prekladá adresy: prichadzajúce pakety podľa *Translation Table*, preklad odchadzajúcich paketov je triviálne
            - 

- **IPv6 adresy**
    - 128 bitová adresy
    - Hexadecimálny zápis
    - **Skracovanie zápisu**
        - 

    - Štruktúru adries definuje RFC 3587
    - Len *classless* (triedy neexistujú)
    - *Individuálne adresy (unicast)* - identifikácia jedného sieťového rozhrania (= IPv4)
    - *Výberové adresy (anycast)* - označujú celú sieť, ale dáta sa doručia iba jednému príjemcovi
    - *Broadcast adresy* - v IPv6 sa nevyužívajú
    - *Skupinové adresy (multicast)* - skupina príjemcov, ktorí prejavili záujem o dáta (= IPv4)

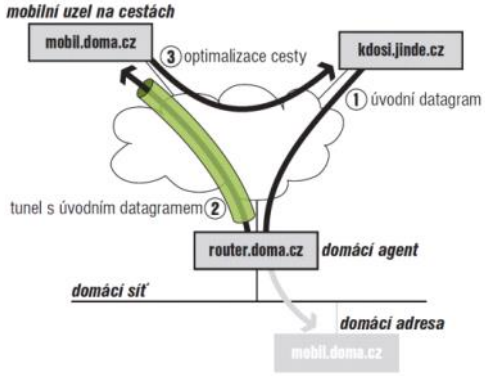
Interakcia L3 s L2 - mapovanie adries

- *Hop-by-hop* mechanizmus
- Predanie/doručenie správy na základe fyzickej MAC adresy
- LAN príjemca = LAN odosielateľa
    - IP a MAC príjemca
- LAN príjemca != LAN odosielateľa
    - IP príjemca, MAC smerovača
- Nutnosť **mapovať IP adresy** na fyzické MAC
    - *Statické mapovanie*
    - *Dynamické mapovanie*
        - **Address Resolution Protocol** (ARP)
            - Zaslanie *ARP request* **všetkým** uzlom na danej LAN
            - Paket sa spracova všetkými uzlami a odpovie len ten, ktorého IP adresa sa zhoduje s hľadanou
            - Odpoveď *ARP replay*
        - **Reverse Address Resolution Protocol** (RARP)
            - Opak ARP

IP protokol

- Najrozšírenejší protokol sieťovej vrstvy
- *Internet Protocol 4 (IPv4) - 1981, RFC 791*

- *Internet Protocol 6 (IPv6) - 1998, RFC 2460*
- *Doprava dát na miesto určenia - host-to-host delivery*
- Podporné protokoly: ICMP, ARP, RARP, IGMP
- **IPv4 datagram**
    - **Version (VER)**
    - **Header Length (HLEN)**
        - Dĺžka hlavičky IP datagrmu
    - **Differentiated Services (DS), Type of Services (TOS)**
        - Kvalita služby
    - **Total length**
        - Dĺžka celého IP datagramu
    - **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**
        - Protokol vyššej vrstvy využívajúci IP vrstvu
        - Nutné pre špecifikáciu cieľového protokolu
        - ICMP, IGMP, UDP, TCP, ...
    - **Header Checksum**
        - Kontrolný súčet hlavičky IP datagramu
    - **Source IP address, Destination IP address**
        - 32 bitová adresa identifikujúca odosielací/príjimací uzol
    - **Options**
    - **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
- **IPv6 datagram**
    - Rozšírený adresný priestor (2^128 jedinečných adries)
    - **Základná hlavička + rozšírujúca**
        - Len 40B (obsahuje iba najnutnejšie informácie)
        - **Version (VER)**
        - **Priority (PRI)**
        - **Flow label**
        - **Payload Length**
            - Celková dĺžka IPv6 datagramu (bez zakladnej hlavičky)
        - **Next header**
        - **Hop limit**
        - **Destination address**
    - **Zabezpečený prenos**
        - **IPSec**
        - Podpora v rozšírujucej hlavičke

        - *AH* - autentizacia datagramu
            - Overuje totožnosť odosielateľa
        - *ESP* - šifrovanie obsahu
    - **Mobilita**
        - Domáca adresa - nemenná adresa, na ktorej je stroj trvalo dostupný
        - Dočasná adresa - meniaca sa adresa
        - Domáci agent - smerovač v domácej siete (ak je potrebné, premseruje dáta na dočasnú adresu)
        - 

        : Ilustrace funkce domácího agenta v IPv6. (Satrapa P., IPv6)
    - **Autokonfigurácia**
        - Stavová a bezstavová konfigurácia (nová)
        - Klient pozná prefixy v sieti
        - 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
        - Nutnosť zistiť maximálnu veľkosť paketov
    - **Podporné protokoly**
        - ICMPv6
            - Formát je zhodný ako v ICMPv4
            - Správy sú rodelené na chybné a informačné
- **Mechanizmy na prechod IPv4 -> IPv6**
    - Dvojný zásobník
    - Tunelovanie
    - Translátory

Smerovanie (Routing)

- Nájdenie cesty medzi dvoma komunikujúcimi uzlami, ktorá musí spĺňať obmedzujúce podmienky
- **Smerovacia tabuľka**
    - Sada ukazovateľov, ktorá určuje čo robiť s ktorým paketom
- **Statický prístup**
    - Administrátorom ručne editované záznamy
    - Jednoduchšie, málo flexibilné
    - Smerovač nevytvára alternatívne cesty
- **Dynamický prístup**
    - Zložité algoritmy
    - Nezaručuje správne poradie doručenia
        - centralizované
        - izolované (RCC)
        - distribuované
            - výhody: pružné, robustné
- **Routing Control Center (RCC)**
    - Každý smerovač ho informuje o svojej situácií, z toho RCC vypočíta optimálnu cestu
    - Zle škáluje, nejde použiť vo veľkých sieťach, pomalé

Smerovacie algoritmy

- Sprostredkuvávajú funkcionalitu smerovania a výber komunikačnej cesty
  - Centralizované algoritmy (1 uzol)
  - Distribuované algoritmy (každý uzol)
- **Požiadavky:** správnosť, jednoduchosť, efektivita, škálovateľnosť, robustnosť, stabilita, spravodlivosť, ...
- **Distribuované smerovanie**
  - *Distance Vector (DV)*
    - Využ. Bellman-Fordov algoritmus
    - Susedné smerovače si vymieňajú kópie smerovacích tabuliek, podľa toho si doplňujú informácie
    - Protokol RIP (2 verzie)
      - Siete sú identifikované mechanizmom CIDR
      - Metrikou je počet hopov
      - Smerovače zasielajú informácie každých 30 sekúnd (časový limit 180 sekúnd = spojenie je DOWN)
      - Vhodné pre malé linky
  - *Link State (LS)*
    - Smerovače si posielajú len informácie o stave liniek, udržujú tak kompletné informácie o topológii sieti, z toho sa počíta najkratšia cesta (Dijkstra)
    - Vhodné i pre rozsiahlé siete
    - 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) - čím je číslo menšie, tým má cesta lepšiu metriku

Autonómne sytémy

Smerovanie

- *Interné* (vo vnútri systému)
  - Dôležité pre výkon
- *Hraničné*
  - Dôležité v škálovateľnosti
- Smerovače musia vedieť všetky cesty k sieťam
- Voľba cesty nie je závislá na lokálnych požiadavkách
  - *Exterior Routing Protocol (ERP I.)*
    - Prvý protokol medzimenového smerovania, dnes sa už nepoužíva
    - Neefektívne, navrhnutý pre stromovú štruktúru internetu
  - *Broder Gateway Protocol (BGP I.)*
    - Aktuálna verzia 4.
    - Navrhnutý pre komplexnejšie topológie, podporuje redundanciu a zvláda cykly
    - Pracuje nad TCP
- *Path Vector smerovanie*
  - Posielajú sa celé cesty, kratšie sa preferujú

IP Multicast - skupinová komunikácia

- Dáta sú prenášané k skupine príjemcov, je preto potrebná replikácia dát
- Príklady: streamované video, vieokonferencia (nízka latencia, obmedzenie počtu príjemcov)
- Klasické riešenie skupinovej komunikácie
  - Best effort, UDP, skupinová adresa, hop by hop, jedna kópia dát, time to live paketov (TTL)
  - IP adresa: IPv4 - *trieda D*, IPv6 - prefix *ff00::/81*
- Každý kto má multicastovú adresu, môže vysielať (stačí na adresu posielať pakety)
- Príjemca sa môže pridať aj odobrať z prenosu

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)

- Nekonečná škálovateľnosť, nezaťažuje sieť zbytočnými kópiami
- Problém so zaistením doručenia, jednoduchý terč útokov

L4: Transportná vrstva

2. apríla 2013 13:17

- Dokáže identifikovať konkrétne aplikácie
- Dáta transformuje do segmentov a ďalej ich predáva aplikácii
- *Proccess-to-proccess delivery*
- **Tvorba paketov (Packetizing)**
  - Utvorené pakety majú pridanú hlavičku
- **Riadenie spojení (Connection Control)**
  - Spojované (spojenie je udržiavané po celú dobu prenosu dát) a nespojované (pakety zasielané bez ustáleneho spojenia) služby
- **Adresácia (Addressing)**
  - Pakety obsahujú zdrojový a cieľový port
- **Zaistenie spoľahlivosti prenosu (Reliability)**
  - Riadenie toku a chýb
- **Riadenie zahltenia siete (Congestion Control)**

User Datagram Protocol (UDP)

- Najjednoduchší transportný protokol poskytujúci nespoľahlivú (nespojovanú = nazaistenú) službu
- Prenos blokov dát, ktoré hlavička UDP opatruje a posiela sieťovému protokolu
- Jednoduché, minimálna réžia, malá hlavička, nie je potrebné udržiavať spojenie
- **Hlavička paketov**
  - **Zdrojový port**
  - **Cieľový port**
  - **Dĺžka UDP paketov**
  - **Kontrolný súčet**
- Procesy komunikujú jednoduchým štýlom "požiadavka - odpoveď"
- Real-time prenosy (napr. multimediálne prenosy), multicastové prenosy

Transmission Control Protocol (TCP)

- Spojovaná, spoľahlivá služba
- Prenos prúdov bytov, 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*) - **point-to-point spojenie**
- **Hlavička segmentov**
  - **Zdrojový port**
  - **Cieľový port**
  - **Sekvenčné číslo segmentu**
  - **Číslo potvrdzovaného segmentu (acknowledgment number)**
    - Číslo nasledujúceho bajtu
  - **Dĺžka hlavičky**
  - **Rezervované pole**
  - **Riadiace dáta**
    - 6 bitov riadiacich informácií
  - **Veľkosť okna**
  - **Kontrolný súčet**
  - **Urgentné dáta**
    - Zasielanie dát mimo poradia
  - **Voľby**
- TCP zabráňuje zahlteniu príjemcu (Flow Control) a siete (Congestion Control)
- Množstvo dát, ktoré je možné zaslať = MIN (veľkosť okna príjemcu; veľkosť okna zahltenia)
- Varianty TCP (líšia sa len mechanizmom pre odhad dostupnej kapacity): *TCP Tahoe, TCP Reno, TCP Vegas, TCP Hybla, ...*

L5: Relačná vrstva

29. mája 2013 19:46

- Spravuje relácie medzi komunikujúcimi stranami
- Nachádza sa iba v ISO/OSI modelu (nie v TCP/IP)
- protokoly: SSL, RPC, ASP, H.245, ...
- Relácia = dialóg
- Naviazanie spojenia
- *Riadenie dialógu* medzi koncovými účastníkmi
  - Plne duplexné (obojsmerné)
  - Poloduplexné (striedanie obojsmerného a jednosmerného)
  - Simplexné (jednosmerné)
- *Synchronizácia (checkpointing)*
  - Ak je potreba vrátiť sa o kúsok späť (prerušenie tlače - zaseknutý papier)
  - Riešené mechanizmom kontrolných bodov
    - hlavné (major)
    - vedľajšie (minor)

L6: Prezentačná vrstva

29. mája 2013 19:56

- Na rôznych architektúrach sú **odlišnosti** vo vnútornej reprezentácie dát
- Nutnosť **jednotnej interpretácie dát =** úloha prezentačnej vrstvy
- Využíva jazyk **ASN.1**
- Aplikácia predáva prezentačnej vrstve dáta + ich popis v jazyku ASN.1
- Šifrovanie a kompresia dát
- Protokoly: AFP, ASCII, EBCDIC, LPP, XDR, ...

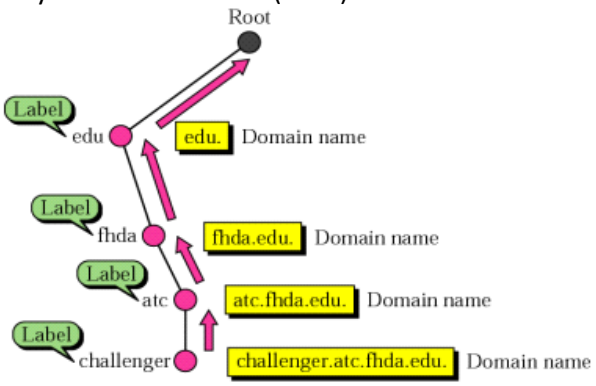
L7: Aplikačná vrstva

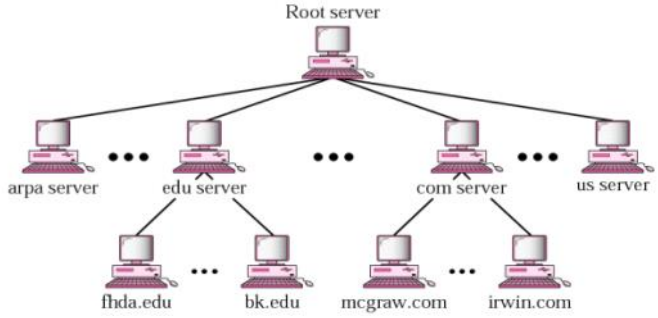
30. apríla 2013 12:03

- Služby pre užívateľa, aplikácie, programy, ...
- Aplikačné protokoly (HTTP, SMTP, ...) sú **súčasťou** sieťových aplikácií
  - protokoly definujú typy správ, syntax, sémantiku, pravidlá, ...
- *Client-Server model*
  - Spojenie inicializuje klient
  - Zasiela požiadavky na server, ten mu odpovedá
  - Po ukončení spojenia je kanál uzatvorený
  - WWW, FTP, DNS, SSH, ...
    - **Tenký klient (Thin)**
      - Na strane klienta sa vykonáva minimum aplikačnej logiky (väčšina na strane serveru)
      - Jednoduchšie, menšie nároky na HW
      - Menšia škálovatelnosť, väčší objem prenesených dát
      - Napr.: vzdialené terminály
    - **Tlustý klient (Fat)**
      - Opak tenkého klienta
      - Napr.: Firefox
- *Peer-to-peer model*
  - Klienti komunikujú priamo
  - Každý uzol poskytuje svoje zdroje a využíva zdroje ostatných uzlov
  - Skype, VoIP, ...
- *Pull model*
  - Prenos dát je inicializovaný klientom
  - Napr.: webový prehliadač
  - Asymetrický dátový tok
- *Push model*
  - Prenos dát je inicializovaný serverom
  - Napr.: streaming multimédií (IPTV)
  - Jednosmerný dátový tok
- Základné parametre z pohľadu aplikácií: strátovosť, priepustnosť, časové obmedzenie
- 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
- **DNS (Domain Name Space)**
  - Menný priestor = spôsob pomenovania entit
  - 2 varianty
    - *Plochý menný priestor*
      - Napr.: MojRouterDomaVBrne
    - *Hierarchický menný priestor*

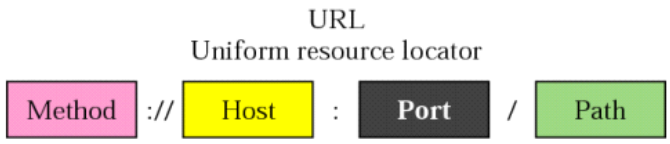
        - Napr.: MojRouter.DomaVBrne.cz
    - DNS = hierarchické usporiadanie
    - Štruktúra invertovaného stromu
    - Maximálny počet úrovní je 128
    - Každý uzol ma menovku (*label*) a doménové meno
    - 

    - *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
    - **Hierarchia menných serverov**
        - 

    - 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*

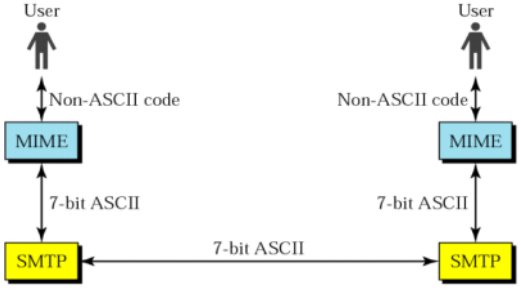
World Wide Web HTTP

- 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**
    - definuje zdroj, ktorý chce klient získať
    - metóda (protokol), host, port, path
    - 

- *Nepersistentné spojenie*
    - TCP spojenie uzavrené pre každú požiadavku
- *Persistentné spojenie*
    - TCP spojenie pretrváva dlhšiu dobu
- **WWW dokumenty**
    - *Statické*
        - HTML dokumenty, ...
    - *Dynamické*
        - Tvorené na webovom serveri
        - PHP, CGI skripty, ...
    - *Aktívne*
        - Bežia na strane klienta
        - Java aplikácie, ...

Elektronická pošta SMTP

- 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

- Mechanizmus internetu pre prenos súborov medzi uzlami
- Staršie ako SMTP
- Stanovuje **dva samostatné TCP spojenia**
    - Riadiace (TCP port 20)
        - Beží počas celého procesu
        - Musí byť stanovený typ súboru (textový alebo binárny), prenosový mód, vnútorná štruktúra súboru
    - Dátové (TCP port 21)
        - 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, ...
    - Kompresia - zníženie dátového objemu
    - MP3, OGG, WMA, RA, ...
- **Spracovanie obrazu**
    - Vzorkovanie a kvantovanie
        - Obraz je rozdelený na diskétne vzorky (768 x 576, 1920 x 1080, ...)
        - Kvantovanie určuje farbu/jas/intenzitu
        - *Framerate*: počet obrazov za sekundu, typicky 25 fps
    - Úprava jasu, vyváženie bielej, kompresia (dôležitá u videí)
    - MPEG, MJPEG, DV, HD, ...
- Prenosné protokoly
    - **TCP**
        - Zaistenie bezchybnosti na úkor latencie
    - **UDP**
        - Minimalistický, efektívnejší a rýchlejší
        - Viac využívaný
- Malá (= 1% - 20%) chybovosť nerobí nášmu oku problémy
- **Korekcia chýb**
    - XORovanie
        - Pakety rozdelené do skupín
        - Po každej skupine nasleduje XORovací paket
        - Strátu 1 paketu je možné opraviť, viac už nie
    - Posielanie druhého prúdu
        - Do prenášaných paketov sú vkladané posledne odoslané dáta
    - Prekladanie
- **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)**
    - Rozšíruje 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

30. apríla 2013 13:20

AAA

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

+

- **Confidentiality (Dôvernosť)**
- **Integrity (Integrita)**
- **Non-repudiation (Nepopierateľnosť)**

Authentication (Autentizácia)

- Overenie identity užívateľa
  - Podľa toho čo užívateľ **má, pozná, je, vie**

Authorization (Autorizácia)

- Oprávnenie použiť určitú službu alebo zdroj
- Udelenie oprávnenia alebo odoprenie

Accounting (Účtovanie)

- Sledovanie využívaných sieťových služieb užívateľom

Confidentiality (Dôvernosť)

- Ochrana dát pred neautorizovaným odhalením

Integrity (Integrita)

- Ochrana dát pred neautorizovanou modifikáciou

Non-repudiation (Nepopierateľnosť)

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
  - Pomalšie, vhodné pre kratšie správy
- *Certifikát*
  - Viaže identitu entity (užívateľ, server, ...) s verejným kľúčom
  - Obsahuje: meno, hodnota kľúča, doba platnosti, podpis vydavateľa
  - Vydávajú ich certifikačné autority (organizácie, ktorým sa dôveruje)

- **Digitálny podpis**
  - Správa je podpísaná (= zašifrovanie) súkromným kľúčom, overované (= dešifrovanie) verejným kľúčom
  - 2 metódy:
    - Podpis celého dokumentu
    - Podpis otisku dokumentu (najčastejšie používané)
- **Hashovacie funkcie**
  - Dôraz na jednosmernosť a one-to-one (2 rôzne správy nebudú mat rovnaký otisk)
  - MD5 (prelomená), SHA-256
- **IP Security (IPSec)**
  - Kolekcia protokolov pre zabezpečenie na sieťovej vrstve
  - 2 módy:
    - Transportný mód
    - Tunelovací mód
- **SSL, TLS**

Kvalita služby

29. mája 2013 18:37

Požiadavky

- Spoľahlivosť (tolerancia spoľahlivosti)
- Zdržanie (rozptyl zdržania)
- Prenosová kapacita

Mechanizmy zaisťujúce kvalitu služby

- **Plánovanie**
  - Obsluha vstupných/výstupných front na odosielateľovi, príjemcovi a vnútorných sieťových prvkov
  - *FIFO (First In First Out)*
    - Najjednoduchšie usporiadanie
    - Využ. iba 1 frontu
    - Žiadna podpora priority
  - *Priority Queuing*
    - Zoradenie paketov podľa prioritných tried
    - Každá priorita ma svoju FIFO frontu
    - Vyššia priorita = skoršia obsluha
    - Nevýhoda: pakety s nízkou prioritou nemusia byť nikdy oblúžené
  - *Weighted Fair Queuing*
    - Pakety su opäť zoradené do prioritných front
    - Frontám sú priradené váhy
    - Vyššie váha = vyššia priorita
    - Striedavá obsluha podľa váhy
- **Formovanie/obmedzovanie tokov**
  - Riadenie množstva a rýchlosti odosielania paketov
  - 2 mechanizmy:
    - *Leaky Bucket*
      - Využitie pre vyhladzovanie toku
      - Nepravidelný tok je priemerovaný (= konštantná rýchlosť)
      - 

    - *Token Bucket*
      - Penalizuje nečinné uzly
      - 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 smerovač zahadzovať

pakety náhodných tokov

- *Weighted Random Early Detected (WRED)*
  - To iste čo RED, ale záleží aj na priorite paketov

Kvalita služby internetu

- *Integrované služby*
  - Aplikácia oznámi sieti kvalitatívne požiadavky
  - Sieť overí, či sú požadované prostriedky k dispozícií
  - Ak nejde vyhovieť - spojenie je zrušené
  - Ak áno - komponenty siete rezervujú odpovedajúci objem prostriedkov
  - Nevýhoda: nutnosť udržovať stav (problémy so škálovatelnosťou)
- *Rozlišované služby*
  - Neoznamujú žiadne požiadavky
  - Paket je označený značkou, ktorá určuje kvalitu prenosu
  - jednoduché, žiadne stavové informácie a žiadne úvodné zdržanie