1 PA159 - Pocitacove site a jejich aplikace - Uvod

Site

- spojovane: lehke QoS, analogie k stare telefonni siti
- nespojovane: internet

Standardizace

- de facto (implementace -> standard)
- de jurde (standard -> pokus implementace)

2 ISO/OSI

Modely

ISO/OSI	TCP/IP	Hodinovy
aplikacni	aplikacni	email, www, phone
prezentaci		smtp, http, rtp
relacni		tcp, udp
transparentni	transportni	ip
sitova	sitova	ethernet, ppp
linkova	vrstava sit. rozhrani	CSMA, async, sonet
fyzicka		copper, fiber, radio

2.1 Vrstvy

Komunikace jen s primym sousedem. Skutecna implementace casto odlisna.

2.1.1 Fyzicka vrstva

Sluzby

- Bit-to-signal (transofrmace)
- Bit-rate Control (rizeni poctu: b/s)
- Bit synchronization
- Multiplexing
  - Analogovy signal
    - Frequency-division Multiplexing (FDM)
    - Wawe-division Multiplexing (WDM)
  - Digotalni signal
    - Time-Division Multiplexing (TDM)
- Circuit switching (prepinani okruhu)[1]

2.1.2 Linkova (datoveho spoje)

Sluzby

- Ramcovani

[1] obycejne funkce fyzicke vrstvy, ne sluzba; prepinani paketu v linkove vrstve

- Adresace (MAC adresa)
- Kontrola chyb - zpravy chyb (redundance dat)
  - Automatic Request for retransmission ARQ (zadost o dalsi ramec)
  - CRC (L2 a L4 prochazi vice vrstvami)
  - Forward Error correction FEC (detekce na bazi Hamiltonova kodu)
- Rizeni toku
- Medium Access control (MAC) - sdielne prenosove medium

Protokoly
- random-access protocols: Aloha, CSMA/CD, CSMA/CA
- controlled-access protocols: based on reservations, polling, tokens, ...
- kanalove protokoly: FDMA, TDMA

Topologie
- Backward learning algorithm
  - mosty/switche nauci umisteni uzlu odposlouchavanim media
  - mozne vytvaret site s cykly - poizuva se Distr. span. tree alg.
  - Nevhodne pro vetsi site, nizka konvergence
- Distributed spanning tree algorithm
  -

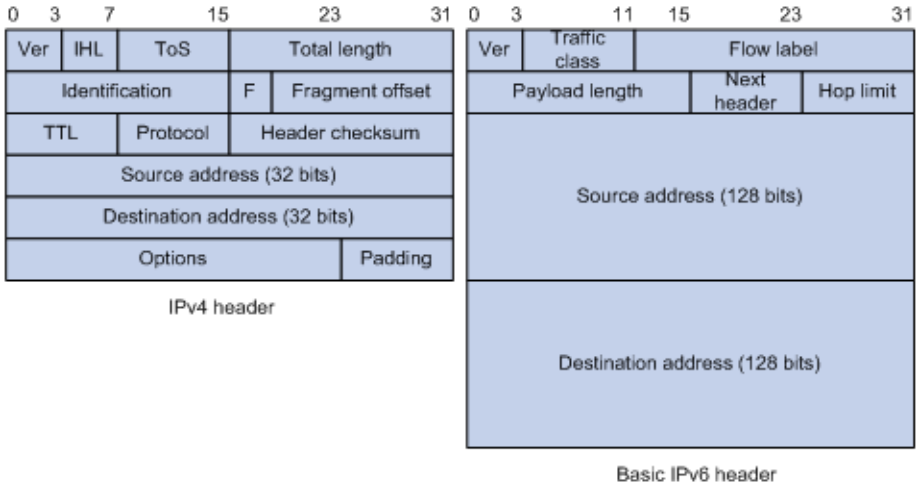
2.1.3 Sitova vrstva

Sluzby
- Vzajemna spoluprace
- Paketovani
- Fragmentace
- Adresovani (IP adresa)
- Rozlisovani adres
- Smerovani
- R.... zprav

Protokoly
- IPv4
  - typy ip adres: unicast, boradcast, multicast
- IPv6
  - typy ip adres: unicast, multicast, anycast (nejbl. clen.)
- Podpurne protokoly
  - ICMP (Internet Control Message Protocol)
    - Informace o chybach a stavu site behem dorucovani
  - ARP, RARP, IGMP

2.1.4 Transportni vrstva

Sluzby
- Paketovani



Obrázek 1: IPv4 a IPv6 datagramy

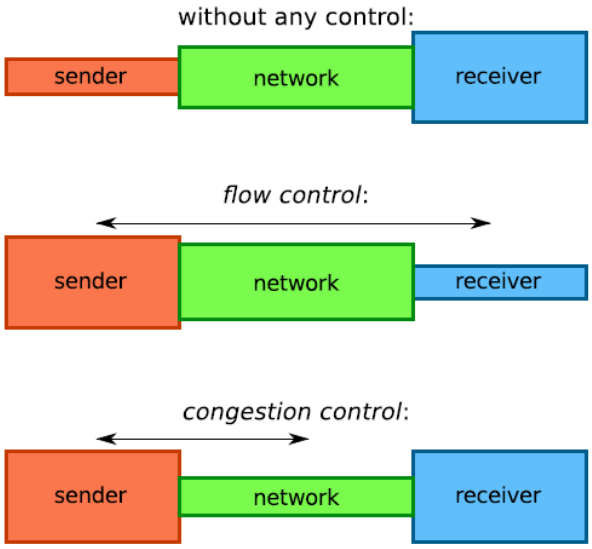
- Kontrola spojeni
- Adresovani (porty: zdrojovy a cilovy)
- Spolehlivost spojeni: flow a error control
- Kontrola zahlceni a zabezpeceni QoS

Spojeni

- Connection-oriented services COS
- Connection-less services CLS

Protokoly

- TCP (Transmission Control Protocol)
  - byte-stream oriented
  - podpora point-to-point
- UDP (User Datagram Protocol)
  - komunikace process-to-process



2.1.5 Aplikacni vrstva

Aplikacni protokoly soucasti sitovych aplikaci

- http - web
- smtp - email

2.2 Neighbour Discovery Protocol (NDP)

Soucast ICMPv6 - 5 ICMP zprav

- Router solicitation (RS)
- Router advertisement (RA)
- Neighbour solicitation (NS)
- Neighbour advertisement (NA)
- ICMP redirect

Mechanismy

- Duplicate addres detection (DAD)
- Neighbor Unreachability Detection(NUD)

2.3 Autokonfigurace

- Stavova (DHCP v IPv4)
- Bezstavova

2.4 IPv6 bezpecnost

dve tridy

- CIA: Confidentiality[2], Integrity, Avaiability
- AAA: Authentication, Authorization, Accounting
- + Nonrepudation[3]

Sifrovani
- Secret Key Cryptography (Symetric Cryptography)
- Public Key Cryptography (Asymmetric Cryptography)

Security Association (SA)
- Klic
- Sifrovani, nebo autentizacni mechanismus
- Dalsi parametry, upresnujici prochazeni

IPsec protokoly
- Internet Security Association and Key Managment Protocol (ISAKMP)
- Internet Key Exchange Version 1 (IKEv1)
- Internet Key Exchange version 2 (IKEv2) - soucasny

IPSec dva mody
- Transporntni
- Tunelovy

protokoly
- AH (Authenticatin Header) - autentizace, bez privacy[4]
- ESP (Encapsulating Security Payload) - sifrovani i autentizacie
  - ESP Header, Trailer, Authentication Data

2.5 IPv6 QoS

Dva pristupy
- Integrovane sluzby (Integrated Services) - spatne se skaluje => neujal
  - RSVP (Resources reServation protocol)
  - YESSIR (Yet another Sender Session Internet Reservations)
- Diferencované služby (Differentialed Services)

Hlavicky IPv6 pro QoS
- Traffic Class
- Flow label

2.6 IPv6 Transition

Problemy
- address parsing ('.' -> ':')

[2] Duvernost
[3] Nepopiratelnost
[4] neporusitelnost zpravy

- addres memory space (32bit -> 128bit)
- multiple address

Metody reseni
- Dual Stack
- Tunneling
- Transalotrs (NAT-PT)

3 Smerovani

Algoritmy centralizovane i distribuovane varianty
- Bellman-Ford (nejkratsi cesta do jedne destinace) - Distance Vektor
- Dijkstra's (nejkratsi cesty do vsech destinaci) - Link state

3.1 Zakladni pristupy

- Distance Vektor (DV)
  - Vsechny informace o siti jen svym sousedum
  - Problem zacykleni, Pro male site, Konverguje pomaleji, nez LS
- Link State (LS)
  - Info o mych sousedech vsem
  - Musi znat vsechny uzly (multicast)
  - Velke routovaci tabulky, Pro velke site
- Path Vector (PV)
  - Varianta DV, posilaji se i cesty do uzlu, detekce cyklu
  - Definice pravidel smerovani

Autonomni system AS mensi oblasti = domeny

3.2 Smerovani v AS

- Interior routing - Interior Gateway Protocols (IGP)
  - DV protocoly
    - RIP (Routing information protocol)
      - RIPv2: + nekolik vlastnostni (authenication of routing info)
      - RIPng: + podpora IPv6
    - IGP (Interior Gateway Routing Protocol): CISCO
    - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - LS protokoly
    - OSPF (Open Shortest Path First)
      - OSPFv2: autentizace zprav
      - OSPFv3" IPv6
    - IS-IS (Intermediate System To Intermediate System)
      - Puvodne ne pro IP ale pro CLNS (Nonnectionless Network Service) -> Dual IS-IS

- Exterior Routing - Exterior Gateway Protocol (EGP)
  - PV protokoly
    - BGP (Border Gateway protocol)
    - IBGP (Internal BGP)

3.3 Funkce routeru

Dve zakladni ulohy
- Smerovani (vytvari pohled na topologii, smerovaci tabulky, ...)
- Predavani paketu (urcuje celkovy vykon routeru)

Smerovaci funkce
- Trideni paketu
- Prokladani paketu
- Rizeni provozu

3.4 IP Filtrovani paketu a klasifikace

- Traffic engeneering
  - Discovering Network Utilization
    - Simple Network Managment Protocol (SNMP)
    - Net Flow
      - sFlow, ntop, ...
  - Dicovering Network Topology
  - Dicovering Net Flow Modelin - Single commodity net flow
- Multiprotocol Label Switching (MPLS)
  - LDP protokol
- GMPLS - rozsiruje MPLS
- G^2MPLS

3.5 QoS-Based Routing

Typy algoritmu
- Source-based routing
- Hop-by=hop routing
- Hiearchical routing

Protkoly
- PNNI
- QOSPF

4 TCP protokoly

- Tradicni
  - Tahoe

  - Reno
  - TCP Vegas
- Vylepseni
  - Multistream
  - Web100
- Konzervativni rozsireni
  - GridDT
  - Scalable TCP
  - HSTCP
  - H-TCP
  - BIC-TCP
  - CUBIC-TCP
- Vylepseni TCP
  - Guick Start a Limited slowstart
  - ETCP
  - FAST
- Odlisne pristupy od TCP
  - TSUNAMI
  - RBUDP
  - XCP

5 P2P site, Klient-server architektura

P2P architektura
- Base Overlay Layer
- Middleware
- Aplikacni vrstva

Nove uzly
- Staticka konfigurace
- Dynamicka konfigurace
- Inicializace clenskeho adresare

Overene toplogie
- Random Mash
- Tiered structure
- Usporadana matice

Taxanomie P2P P2P architektura
- Centralized
- Decentralized
  - Structure
    - Flat
    - Hiearchical
  - Topology

        * Unstructured
            · Static configuration
            · Re-configurabl
        * Structured
            · Precie
            · Probabilistic
- Hybridni (kombinace centralizovanych a decentralizovanych)

5.1 Smerovani v P2P

- V nestrukturovanych sitich
  - Heuristicke strategie
    * Directed BFS and Intelligent searching
    * Local indicies search
    * Random walk
    * Adaptive probabilistic search (APS)
- V strukturovanych sititch
  - DHT
    * CHORD
    * CAN
    * Pastry
    * Tapestry
  - Skip list
    * Skip graph
    * Skipnet
  - Tree-based
    * P-Grid
    * P-tree
    * Baton
- Hybridni site

6 Ad-hoc site

(L2 a L3 pro uzly a senzory a mobilni pocitace)
Site bez infrastruktury (GSM, UMTS, WLAN, ...)

- Mobile Ad-hoc Networks (MANTEs)
- Vehicular Ad-hoc Networks (VANETs) - auta po silnicich
- Wireless Sensor Networks (WSNs) - interakce mezi sebou, dulezita energeticka narocnost

6.1 Medium Acces control (MAC)

Koordinace pristupu uzluk sdilenemu prenosovemi mediu
Protokoly (efektivita vyuziti energie)

- Souperici s rezervacnim mechanismem (synchronni x asynchronni)
  - Busy tone protocol
  - BTMA (Busy tone multiple access)
  - MACA (Multiple Access Collision Avoidance)
  - PCM (Power-Control MAC)
- Souperici s planovacim mechanismem
  - S-MAC (Sensor-MAC)
  - LEACH
  - TRAMA
- Soperici protokoy - dva typy
  - sender-initiated
  - receiver-initiated

6.2 Ad-hoc smerovani

- Address-based routing
- Data-centic forwarding

Klasifikace smerovacich protokolu

- Proaktivni
  - DSDV (DV smerovani)
  - OLSR (LS smerovani)
- Reaktivni
  - DSR
  - AODV

7 Multimedia

7.1 Real-time charakteristiky

- Zpodeni zpracovani paketu
- Zpodeni odevzdani paketu
- Propagation delay
- Smerovani do fronty a zpozdeni