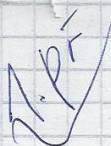
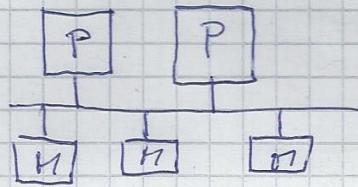


Výpočetní systémy ds topologie

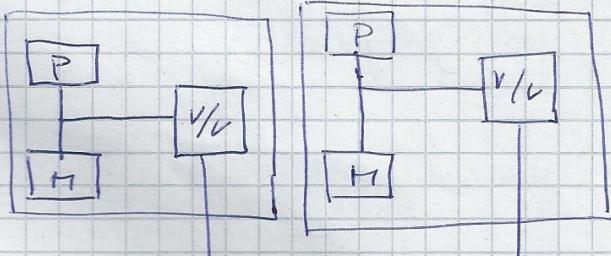


Výpočetní systém

centralizované
ob -||-



težká vazba - komunikace probíhá
volum - vazba - kon. sítí, zpráv

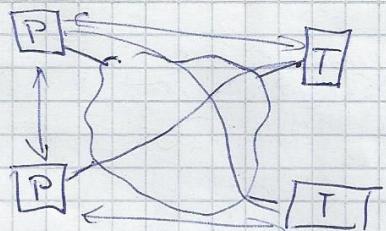


zprávy

Vývoj - vzdálený přístup (SSH)
- počítače v síti
- distribuovaný systém

Vzd. příst.:

Síť:



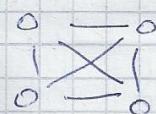
DS = poč. sítí + zdroje

distribuovaný výpočet (Ethernet)
data (web)

PC sítí $\begin{cases} \text{uzly} & - výpočetní prostory \\ \text{hrany} & - propojení \end{cases}$

Topologie

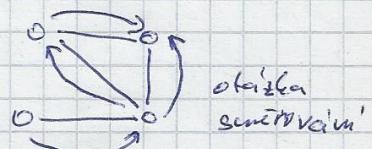
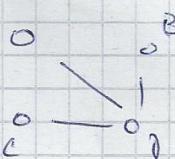
úplně polygonální síť



$$\frac{m \cdot (m+1)}{2}$$

Neplošná - " -

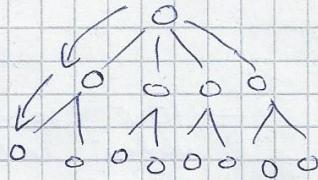
propojení s menším počtem spojů



Hierarchická síť kruhová síť lineární síť dvoubodový spoj mnohabodový spoj

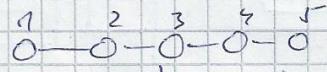
Hierarchická síť

tok dat
od štora dolů



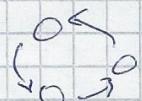
jasné dány cesty

Lineární síť

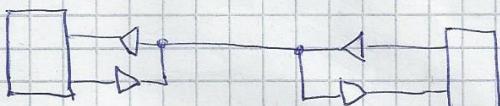
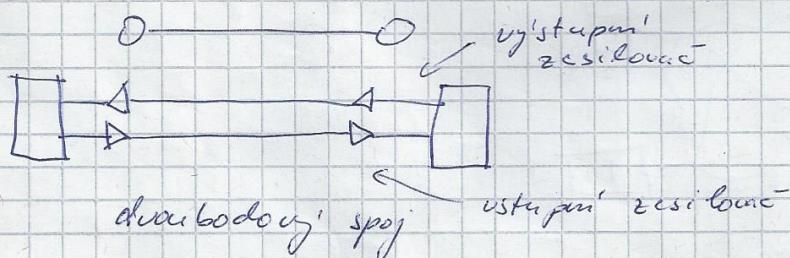


Vi, kam se posílá po celé
ochodnou cestou

Kruhová síť



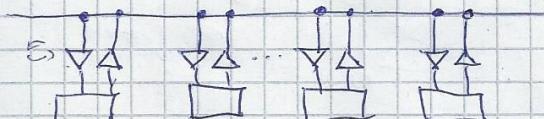
všichky všechny obdrží zprávu



dvoubodový polo duplexní spoj

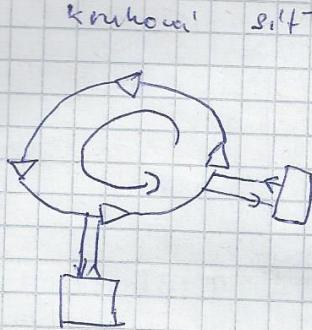
Mnohabodové spoje

aběrnicová síť



CAN
Ethernet

Kruhová síť, dělení sítí, pan lan man wan gan ban multiplexování přepínání kanálů



Dělení počítačové sítě

WAN - wide $\approx 100 - 1000$ km $1 - 10 \text{ Gb/s}$

MAN - metropolitní $\approx 10 - 100$ km $100 \text{ Mb/s} - 10 \text{ Gb/s}$
- kabelové sítě

LAN - local $\approx 100\text{m} - 1\text{km}$ $100 \text{ Mb/s} - 10 \text{ Gb/s}$

PAN - personal $\approx 10\text{m} - 100\text{m}$ $100 \text{ Mb/s} - 10 \text{ Gb/s}$
- radiové spoje

BAN - body $\approx 1\text{m} - 10\text{m}$ $10 \text{ Gb/s} - 100 \text{ Gb/s}$

Bezdrátové spoje - radiové vlny
- infra struktury

LAN \rightarrow WLAN

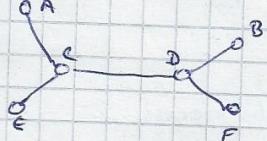
PAN \rightarrow WPAN

BAN \rightarrow WPAN

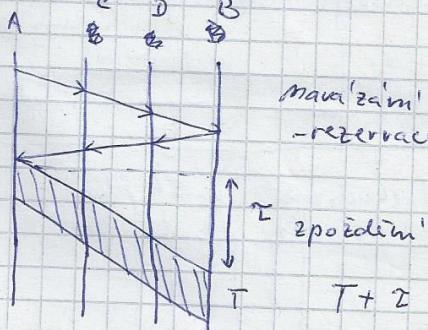
Multiplexování

- fyzický kanál - více spojů

- přepínací kanálů



$A \rightarrow B \dots C \rightarrow D$ multiplexování



multiplexování
- rezervace kanálů

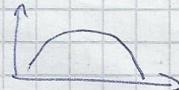
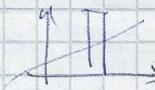
zpoždění

- vlnou' multiplex
- rámci "šarvy"
- vlnové čísla
- pomocí optických kabelů

~~W~~ multiplex. v rádiu ještě ~~W~~

Přenos v rozprášení pulzů

Sifrování



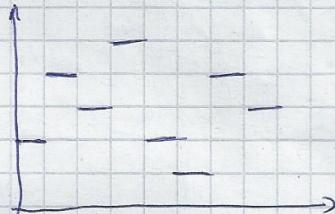
- ~~DSSS~~ - přímou modulací
- jeden bit se posílá jako posloupnost bitů
- sítové frekvence silnější

1 ... 100110101
0 ... 011001010

IEEE 802.15.4

- musí se znít v rámci frekvence, jinak ho nejde rozlišit - aranžmá

FHSS - frekvenční přeskoky



- mění se frekvence mezi časem
- sifrování + schéma bez interferencí
- ~~Bluetooth~~

CDMA

A (1 1 1 1)

1 - 1 1 - 1

1 1 - 1 - 1

B (1 - 1 - 1 1)

1 - 1 - 1 - 1

0 - 1 1 - 1 - 1

1 ... 1 1 1 1
0 ... - 1 - 1 - 1 - 1
1 ... 1 - 1 - 1 1
0 ... - 1 1 1 - 1

vezímejte ortogonální

V	U
V	⊕

Walshovy kódy

A	10	1 1 1 1	- 1 - 1 - 1 - 1
B	11	1 - 1 - 1 1	1 - 1 - 1 1
		2 0 0 2	0 - 2 - 2 0

výsledek je pro rozsifrování

výsledek

$$\oplus = 1$$

$$\ominus = 0$$

viz cv.

Protokol referenční model ISO OSI

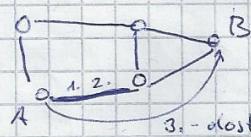
Protocol layer

- souhrn pravidel
- způsob kódování

Referenční model ISO / OSI

1. Fyzický - propojení počítače - být přenos
2. Linkový - přenos rámce - zpráv rozmanité délky, kontrola chyb
3. Sítový - sítovým, adresován, řízení toho, kde
4. Transportní - základní, adresování, řízení toho, kde
5. Relační - zajišťuje opravy po chybě
6. Prezentacní - záfrakování, komprese a kódování dat
7. Aplikace - aplikace

protokoly



3. - dostanu se ke správciem posítači

4. - spolehlivé / nespolehlivé

↳ jistotou

5. kódování ↗ ASN.1 - popis dat
BER - jak se konkrétně stane zakódování
integer ↗ 21C TLV Values

do roku 1980 v tom byl hordej

technical office protocol

Boeing & GFD ↗ TOP (transport) authentication
- MAP (manufacturing action protocol)

→ druhý, modernější se spíše využívá v síti

Tcp ip tcpip arp icmp bootp dhcp

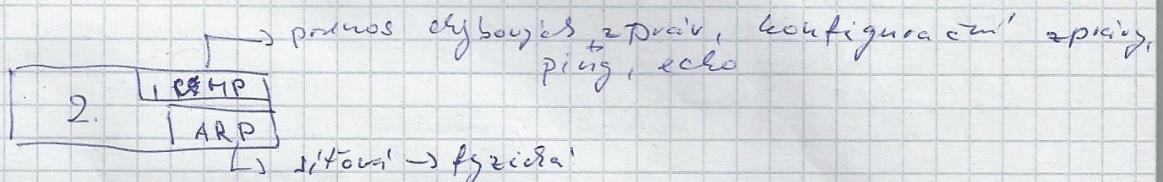
TCP / IP

4. Aplikacií - HTTP, FTP, DNS...

3. transportní - TCP, UDP

2. síťová - IP

1. přenosová - Ethernet, IEEE 802.* , PPP , SCIP, FDDI



2nd část

Základy TCP/IP

Používané prototypy

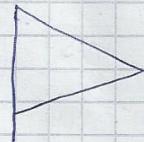
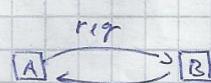
ARP > address Resolution protocol

sít. → fyz. adresy

ICMP - internet control message protocol

- přenos násobných zpráv
- echo - request
- respond

- time exceeded

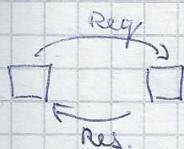


BOOTP - bootstrap protocol

- získání

- IP, HASHA, ADRESA ŠÍŘKOVIN A DNS)

- používá UDP a používá dat



TRACEROUTE

DHCP - dynamic host configuration protocol

- BOOTP + dyn. přidělování adres

- má nastavený rozsah adres, ze kterého může
přidělovat zadanou dynamickou
přiřazenou adresu danou výklopnou cloubou

Tcp udp telnet http ftp dns ns

TCP - spolehlivý, přenos dat

- HTTP, FTP, SSH

- vysoký reakční - navazání spojení přenos dat
a uchování spojení

UDP - nespolehlivý,

- malý reakční

- při ztrátě dat pak opakovat

- DNS, registrace čas... (TIME)

TELNET - terminálový přístup

- přenos dat v oddělené podobě

- program SSH secure shell
= šifrovací kanál

FTP - file transport protocol

- přenos souborů

- SCP - secure copy

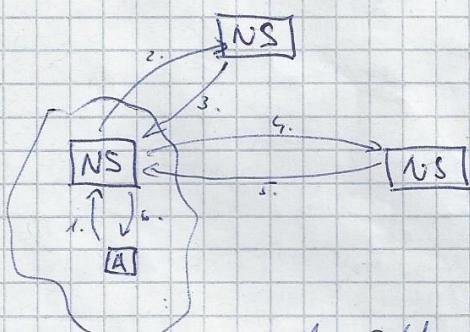
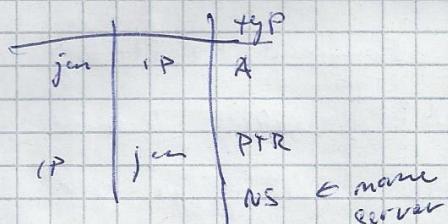
- přenos v oddělené podobě

HTTP = hypertext

- https (SSL) google

DNS - jmenování služeb

- jmeno \Rightarrow adresa



1. addr www.jcu.cz

2. NS ~~jcu.cz~~ jcu.cz

3. endpoint NS jcu.cz jmena xxx

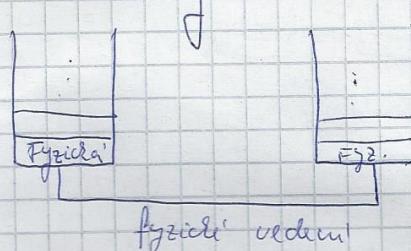
4. addr www.jcu.cz NS

5. endpoint

6.

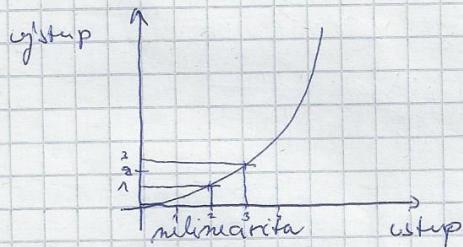
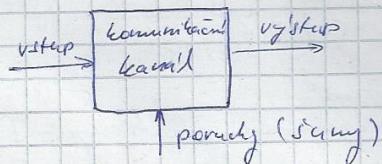
Fyzická úroveň šum Fourierova analýza

Záře



Fyzická čírověn - "nejvýšší črověn"

propojení s celu



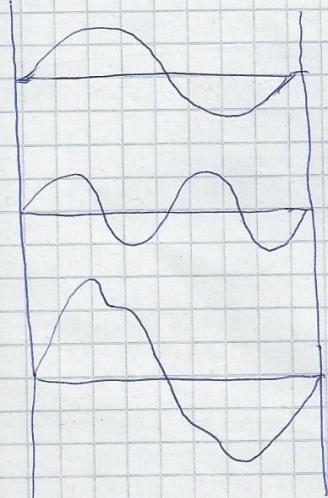
bílý šum - náhodný signál
- ohnisko bý

impulsní šum - jednorázový signál
- při zapnutí/vypnutí spotřebičů

Území modelu → aby vědět kolik info tím můžete prospat

Fourierova analýza

- analogický signál → frekvenční spektrum
- harmonický frekvence
- periodický signál - perioda \approx 1. harmonická
 - \approx 2. harmonická
 - \approx 3. harmonická



jakožkoli signál se dá

rozložit na jednotlivé harmonické

kanalem můžete prospat jakožko číslo harmonickou (území dleka písmo)

Pokud nestaci sítka prima můžete
např. snížit přenosovou rychlosť

Nyquist shannon kritérium

$$C = \text{počet bitů za zmín} \quad \text{# zmín/s}$$

Nyquist:

$$C = 2W \log_2(V)$$

kapacita pásem
[5/Hz]

šířka pásem # úrovní (kódování)
[Hz]

komun. nároky
nároky

počet zmín

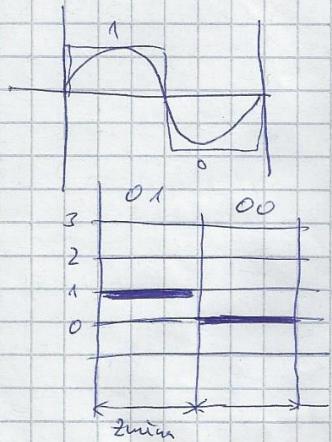
počet bitů které potřebují
zakódování V

$$\max \# \text{zmín} = 2 \cdot \text{šířka pásem}$$

$$V = 128 = 2^7$$

úrovní

na zakódování potřebuje V bitů



Shannonovo kritérium

$$C = W \log_2 \left(1 + \frac{s}{N} \right) \rightarrow \begin{array}{l} \text{signal ka sum} \\ \text{úrovní signálka} \\ -/- \text{ sum} \end{array}$$

$$P_f: \frac{s}{N} = 1000$$

$$W = 10^4$$

$$V = \sqrt{1 + \frac{s}{N}}$$

$$V = \sqrt{1001} = 32$$

$$C = 10^4 \log_2 \left(1 + 1000 \right)$$

cca $\log_2 2^{10} (1024)$

"stejně jde o teoreticky"

$$C = 10^4 \cdot 10 \text{ bits/s}$$

$$C = 2W \log_2 V = W \log_2 \left(1 + \frac{s}{N} \right)$$

$$\log_2 V^2 = \log_2 \left(1 + \frac{s}{N} \right)$$

$$V = \sqrt{1 + \frac{s}{N}}$$

za 1 zmín posíláme 5 bitů

Výpočet přenosu

Příslušně:

$$W = 10^4 \text{ Hz}$$

$$\frac{S}{N} = 2000$$

$$V = \sqrt{2000} \approx 45$$

úrovní musí být
2x abý se to
než by vobdoválo

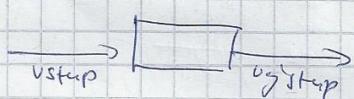
$$2^5 < 45 < 2^6 \quad \text{musíme si vybrat}$$

$$C = 2 W \log_2 45 = 2 \cdot 10^4 \cdot 5 = 10^5 \text{ s/m}$$

$$C = W \log_2 (1 + \frac{1}{2})$$

$$C = 10^4 \cdot 10^4 \approx 10^5 \quad (\text{náleží to ujít uva - teorie})$$

Vypočítat přenos

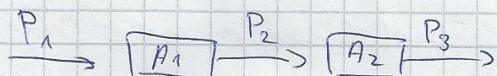
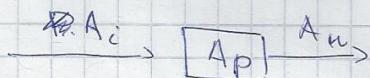


$$\frac{\text{výstup}}{\text{vstup}} = \text{průnos}$$

A_u ... zesílení napětí

A_i ... zesílení proudu

A_p ... zesílení výkonnosti



$$P_2 = A_1 \cdot P_1$$

$$P_3 = A_2 \cdot P_2$$

$$P_3 = A_3 \cdot A_2 \cdot A_1 \cdot P_1$$

$$\log(a_b) = \log_a a + \log_b b$$

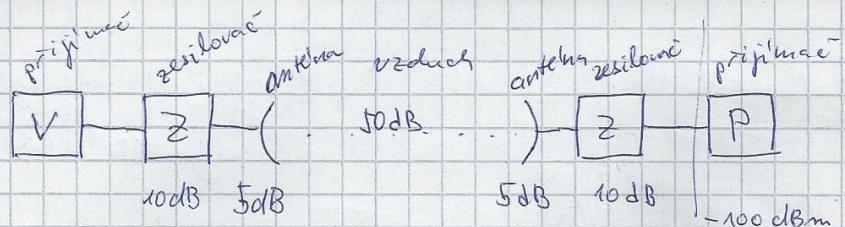
$$A_p = \frac{P_o}{P_i}$$

$$\log(A_p) = 10 \log \left(\frac{P_o}{P_i} \right)$$

[dB]

	[dB]
10	10
100	20
1000	30

Typy přenosů sériový přenos paralelní přenos



$$10 + 5 - 50 + 5 + 10 = -10 \text{ dB}$$

$$1 \text{ mW} = 0 \text{ dBm}$$

$$10 \text{ mW} = 10 \text{ dBm}$$

do přijímací

přijímací

$$0 \text{ dBm} \approx -20 \text{ dB} = -20 \text{ dBm} \geq -100 \text{ dBm}$$

$$10 \text{ dBm} - 20 \text{ dB} = -10 \text{ dBm} \geq -100 \text{ dBm}$$

musí být větší než přijem

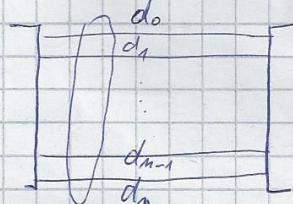
$$\text{Př.: } W = 10^4 \text{ Hz}$$

$$\frac{S}{N} = 30 \text{ dB} \Rightarrow 10^3$$

$$Q = W \log_2 \left(1 + \frac{S}{N} \right)$$

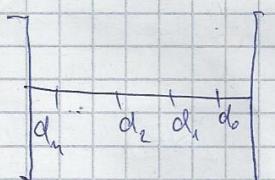
Typy přenosů

přenosové kanály na vodivé sítipr.



parallelní přenos

- rychlejší, více kanálů

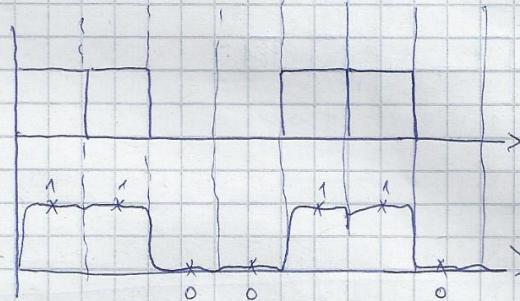


seriální přenos

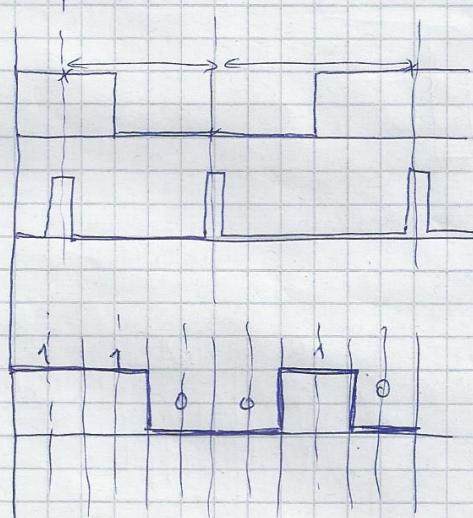
- dříve, 1 kanál

Asynchronní přenos synchronní aritmický

(asynchronní přenos)
charakteristiky okamžiky jsou od sebe různě daleko



obecně



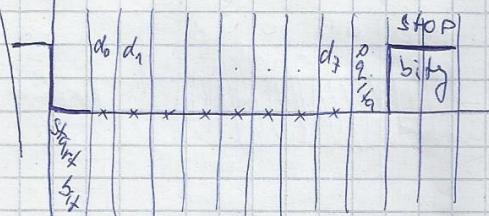
asynchronní

synchronizační signál
používá se u paralelního ...
(jeden drát matic)

synchronní

neplatí synchronní signál
(vygeneruje si to samy)

je ale nutná synchronizace
hodin vysílce a přijímače



asynchronní, (start-stop přenos)
člávečnice, myš...

bloky asynchronní
uvedené synchronní

z rychlosti přenosu si
vypočítat charakteristiky
okamžiků

za tak kritickou dobu
je hodin využitý

synchronizace u start bitu

$$T = \frac{N}{N + \text{START BIT} + \text{STOP} + \text{PARITA}} \rightarrow \text{max!}$$

počet dat bit | Parita | stop bit

$$(8 | N | 1) \quad \frac{8}{10}$$

max využití kanálu na 80%

Dvouúrovňový víceúrovňový přenos

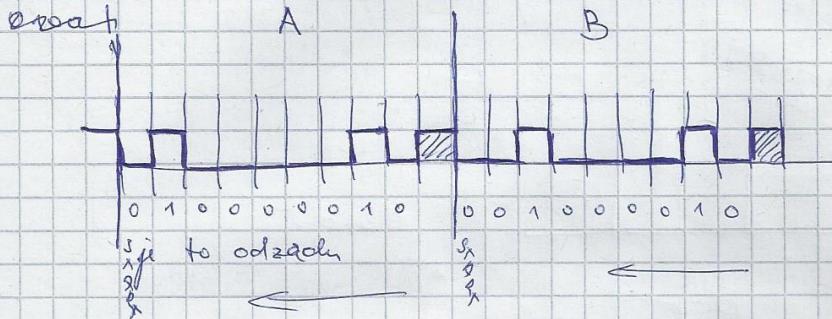
$$'A' = 0x41$$

$$'B' = 0x42$$

0100 10001

0100 10010

(8N1)

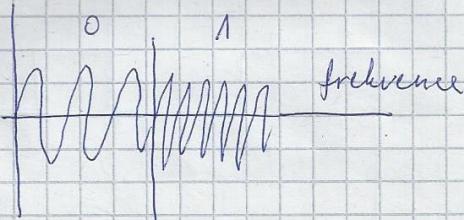
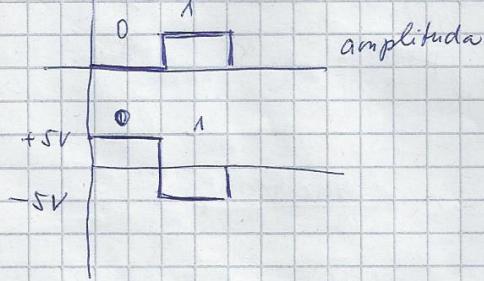


přenos

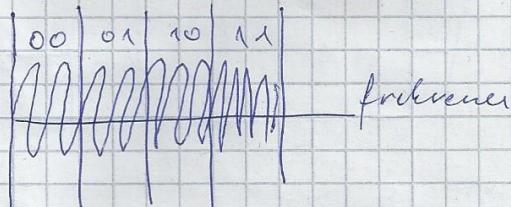
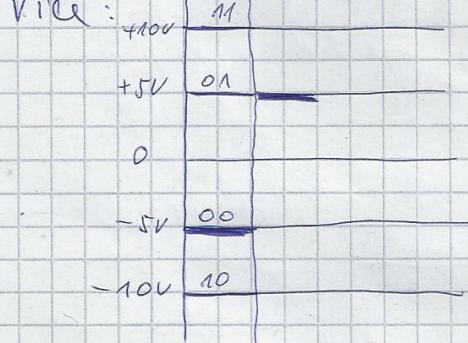
dvouúrovňový
víceúrovňový

$$C = 2W \log_2 V$$

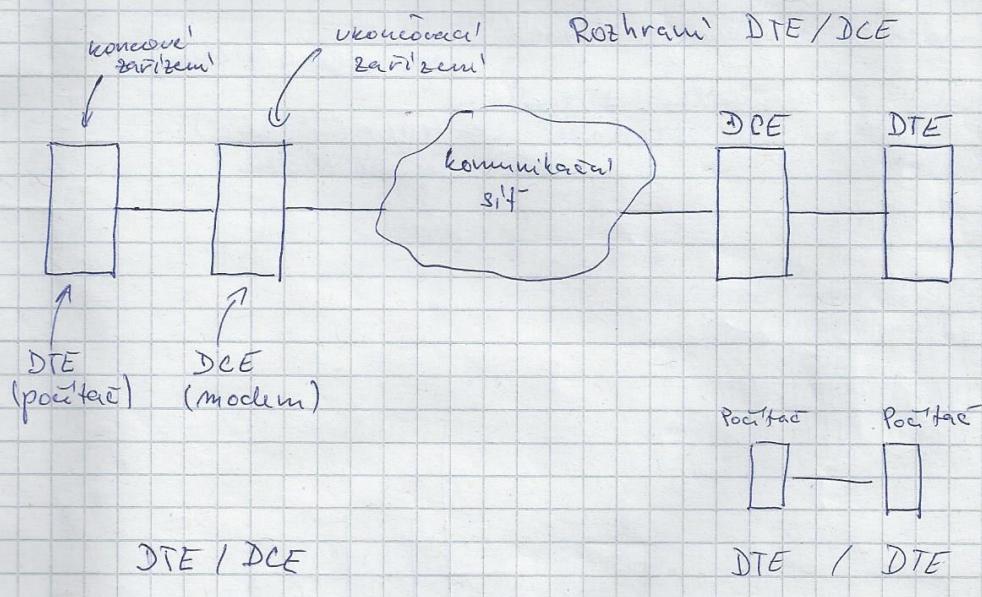
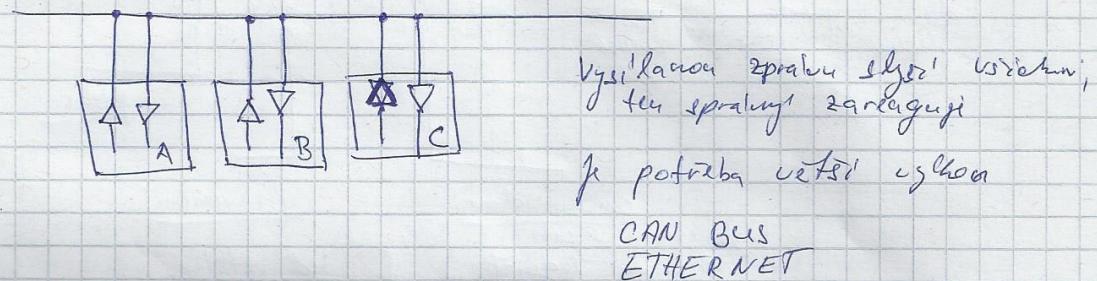
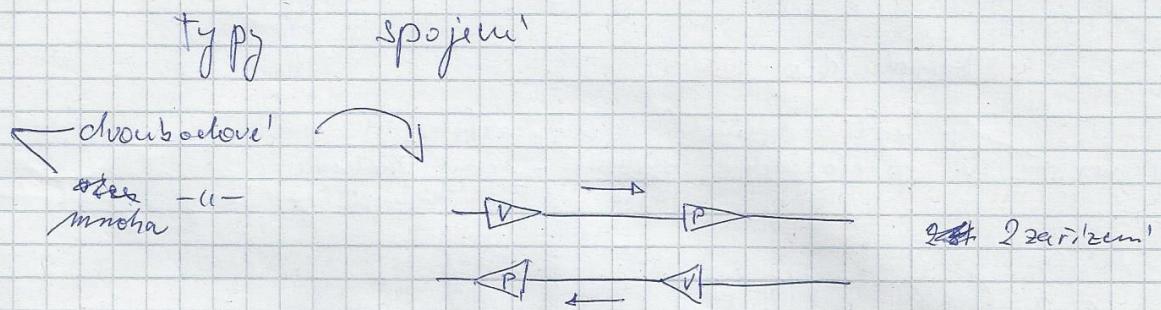
2:



Více:



Typy spojení dce dce dvoubodové mnohabodové



bylo se muset být správ (volit)
kabel mimo mít správ
počítač, co si to nemá
přesně (switch)

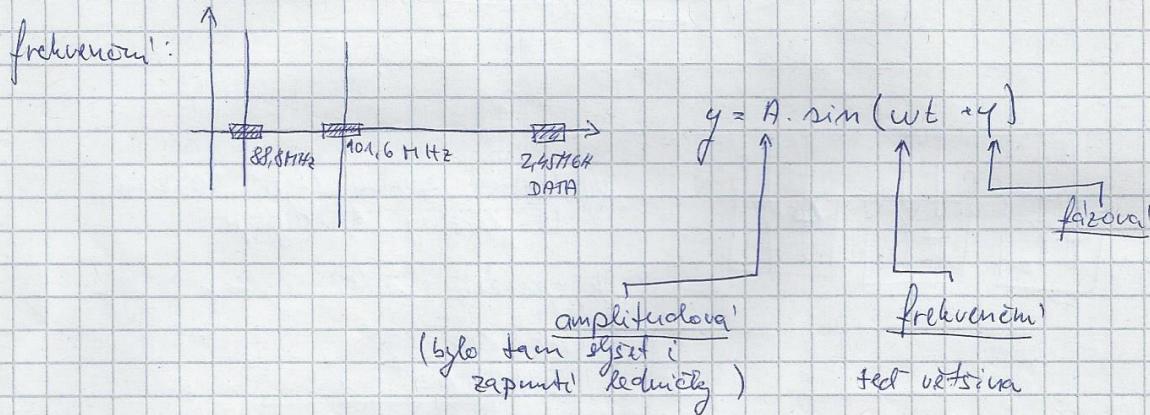
stejně tak DCE / DCE

(takže se to musí ořeřít)
switch to počítači auto.

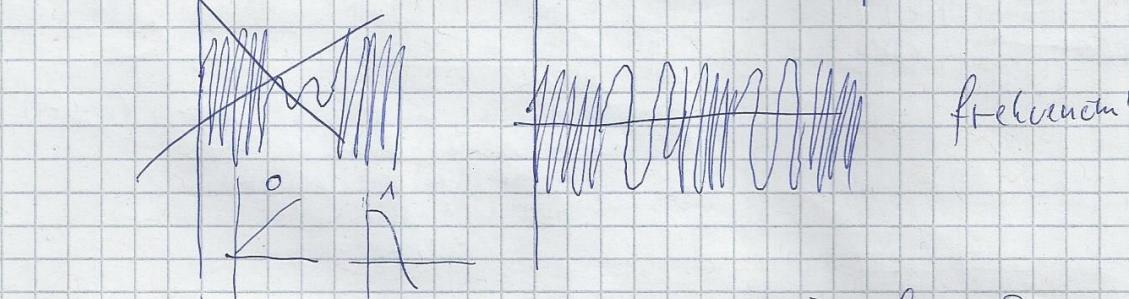
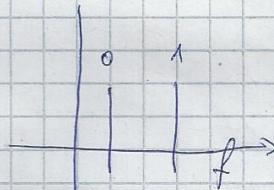
Modulace frekvenční modulace, amplitudová modulace, fázová modulace

Modulace

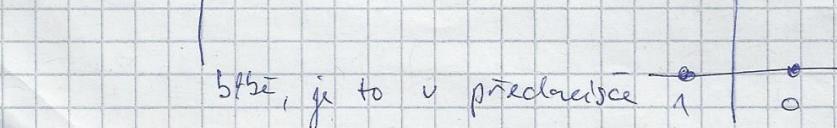
Přenos → zač. pasm (0 - 200 MHz)
 → přeloženek pasm - nosná frekvence
 má mi se manuálně nošený signál



modulaci - analogový signál ma nosnou frekvenci
 uložení - digitální signál
 - nízké skokové (v telegrafu klic)
 - malé tlakopy



1 - změna fáze } clifrenční
 0 - normálně



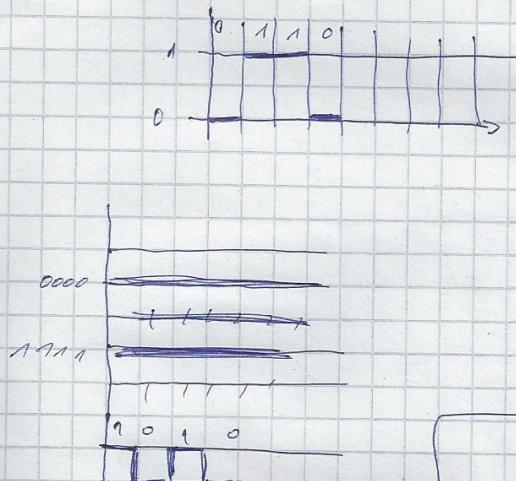
Kódování

Kódování

Přednáška 3

m m

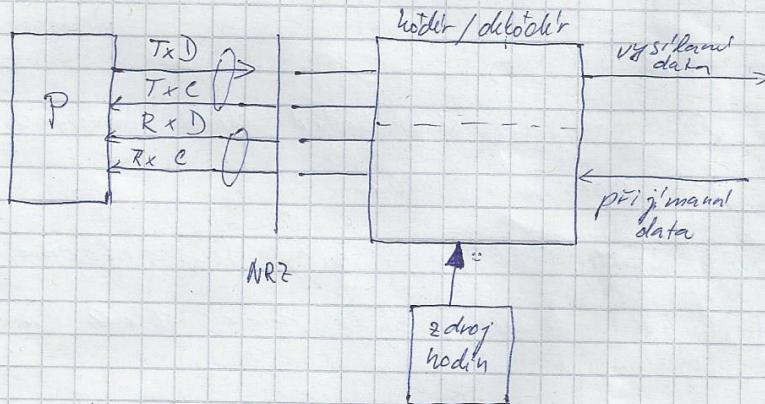
- výstup z počítače - NRZ - "bez návratu k nule"



- logická hodnota reprezentovaná urovni (nula než a menší než)
- může to být pouze
- existuje smejnosťné složky
- malý počet signálů

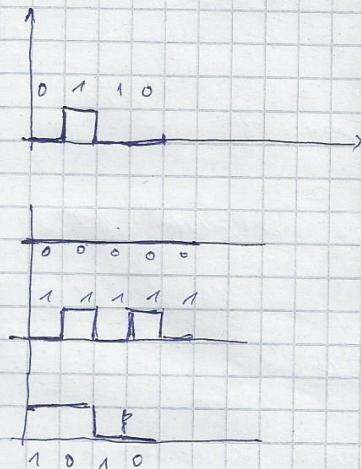
nem' to zase tak skuteč'

→ kódování



KÓDOVÁNÍ

NRZI - bez návratu k nule, s inverzí
(NRZ-M) - M - Marek - změnu při "1"



- log. hod. kodování změna
- oba hranice sú složené
- může jít o jednu a na druhou stranu
- malý počet změn

Dlouhé posl. nul.

- kódování: 8b → 5b s lichou paritou

0	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	

nejake jde 16 nul → pak príde 1 a tím se synchronizuje rozprádlení nuly

$$C = (2w) \cdot \log r$$

#2min

2 srovnat

$$C = 2w$$

$$w = 10442 \Rightarrow C = 20 \text{ bits/s}$$

Př.:

Kódování: 4B/15B

→ sít typu FDDI - fibre distributed data interface

- obs. optická sít, 100Mbit/s, ≈ 100 km
- dřívější kódování 5bity, ale jen 4 bity jsou informací
- Pošlu pouze 3 bity mohou byt max 3 nebo menší
- použití kódov. NRZI

00000
00001
00010
00011
00100
00101
00110
00111

- významné hodiny:

konečný za více nulaní
začínající za více nulaní

1	0	0	1

na přechod max 3

budeme mít více jak 16 možností, které
začínají 4 bity

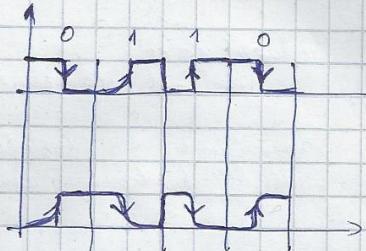
max. počet zmin: $\frac{1}{2} \Rightarrow$ max frekvence
min. $\frac{1}{15} \Rightarrow$ min bitového intervalu
 $120 : 5 = 24$

min frekvence

kódování dvojí fází dekódování

kódování dvojí fází
 metody
 Manchester (pri'ug', nupri'ug')
 Diferenciální Manchester

PM: uprostřed bit. int. je přechod: $0 \rightarrow$ přechod do 0
 $1 \rightarrow -1 - 1$



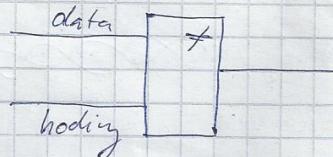
$$\begin{array}{c} 0000 \\ 1111 \\ 0101 \\ 1 \end{array} \Rightarrow w = c$$

$$2 \quad 2$$

$$0 = 2w$$

$$100 \text{ Mbit/s} \Rightarrow \begin{array}{c} 50 \text{ MHz} \\ 100 \text{ MHz} \end{array}$$

DM: $0 \rightarrow$ přechod do 1
 $1 \rightarrow -1 - 0$

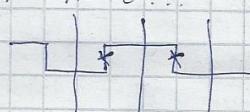


Dekódování



od poloviny bit. sig.
 $+ 3/4T$

středy hledáme tak, že poslu 1010...

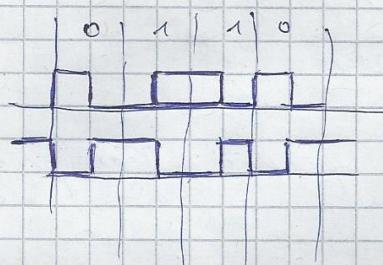


uprostřed bit. int. vědy

0 ... změna má zač. vědy
 1 ... konec změny

kroucená dvojlinka koaxiální kabel

dif. - mezikruží má polaritu sign.



obr. jde o správnu
(DH.)

85 sloučka - délka 1 sign.

10 Mbit/s ... 20 MHz
100 Mbit/s ... 200 MHz

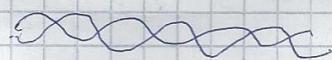
clouzí fází
(da je to snadno zjistit)

1 Gbit/s ... 2 GHz

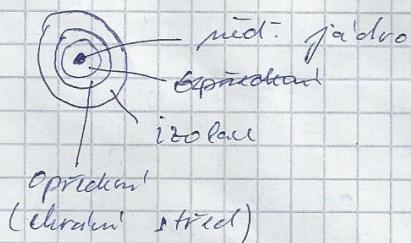
musíme to rozložit jinak,
velkým pásem může vzniknout

délší perioda
není problém se zbrutou synchronizací.

kroucená dvojlinka
(není to zvukový obraz --)

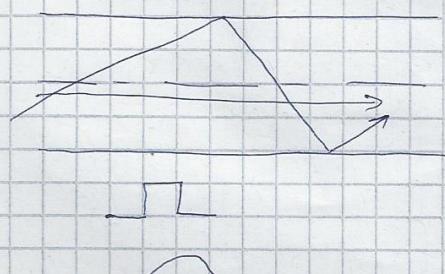


koaxiální kabel

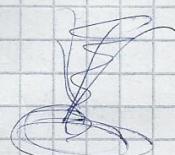


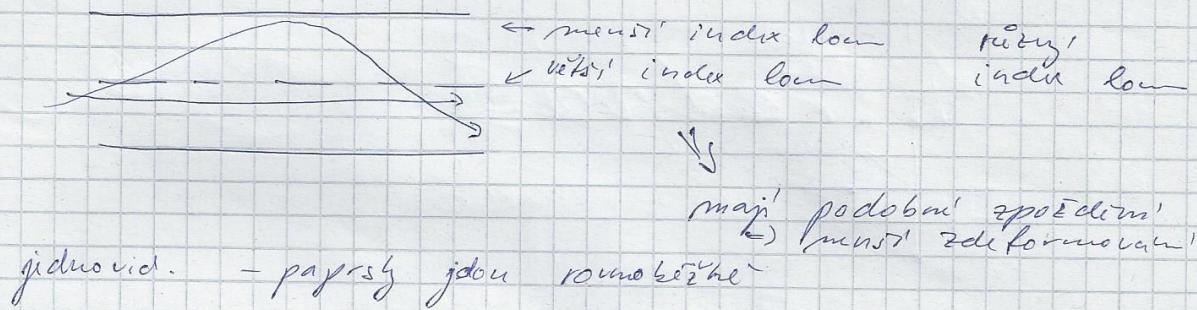
optické vlnění brásky

- ∅ monomodová ~ 50 μm → první index cca 10 Mbit/s - 1 km
- ∅ jednomodová ~ 5 μm → první index ~ 11 - cca 10 Gbit/s ... m - 1 km
- ~ 10Gb/s, stoky km



první index
⇒ řízení zpoždění





Rádiový přenos

- odraz od ionosféry

↳ aj. k plán

IEEE 802.11

15

BT

ovládání

stejný, co u staršího
jednotlivého protokolu

kabel - spolehlivost rychlosť
bezdrát. - mobilita

anténa - 3 výšky

geostacionální - stejná vzdálenost
rychlosť jde ze země
100 m/s (velké zpoždění)

nebude zkouset nic o chuzičích

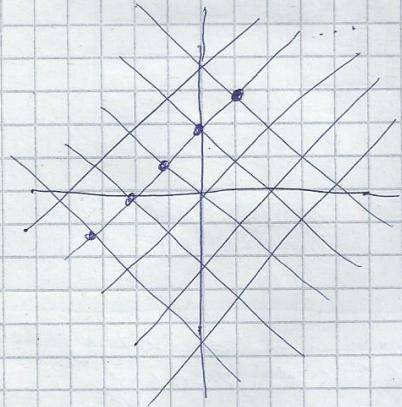
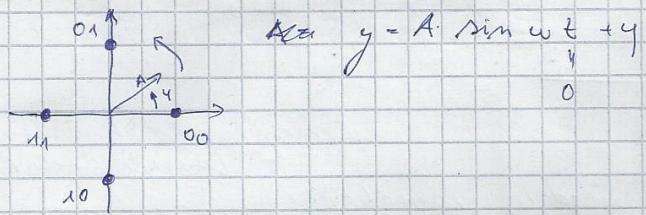
ADSL

asym. subscriber orig. lines
[4] síť, propojení
slabší, vysílání

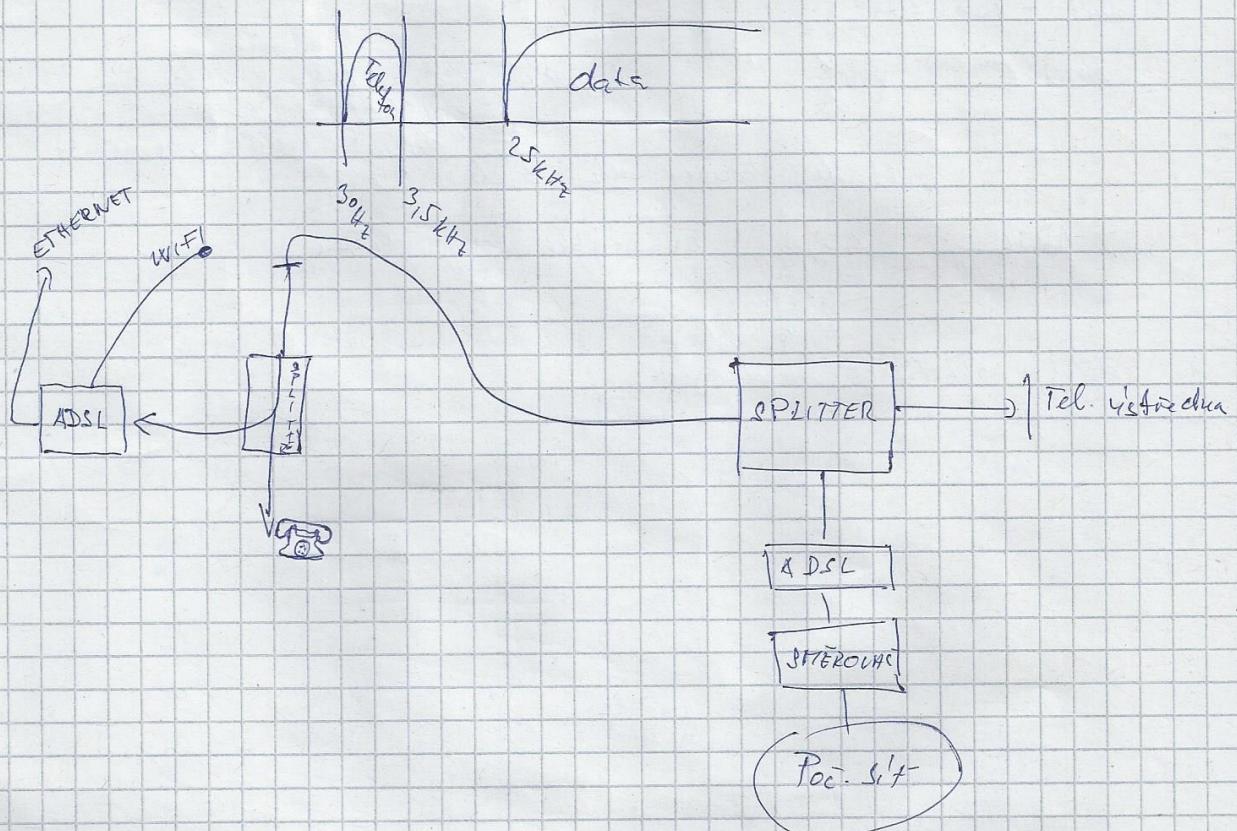
drive - akustická modulace

modulace

Modulace

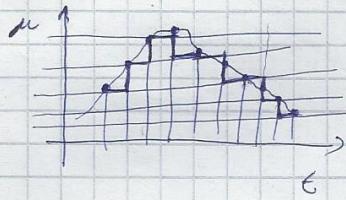


$\approx 1.1 \text{ MHz}$ - doba řezení přenosu počtu linky
- celou již můžeme rozložit pro rovnou



přenos zvuku sítí paletizace

Přenos zvuku poč. sítí



CD = dig. x anal. odesy

vzorkování $\rightarrow R$

analog

A/D převodník - klasifikace

\hookrightarrow koneční číslo - zaokrouhlit

převod

\hookrightarrow číslo urovni

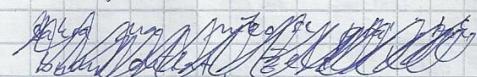
postupnost slabik

paletizace - (160 slabik = 1 pacet)

zvuk: 8000 vzorků/s \Rightarrow 1 pacet = 8 slibek
 $\Rightarrow 64\text{ ms}$

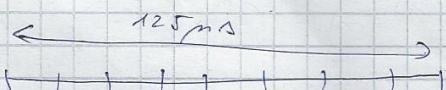
C = 2000 ... 4000 Hz

min. 2 vzorky na periodu - jinak neje možné obnovit zvuk
 (mimo 20 Hz - 2048 Hz)



strukturní časovadlo synchronizace

ji jedno jake zpoždění,
 ale stejné pořadí a rychlosť

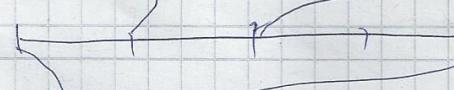


8 novor. pacet

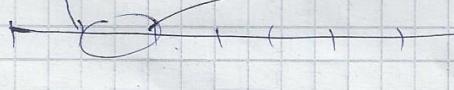
T1



24 T2



4 T3



7 T4

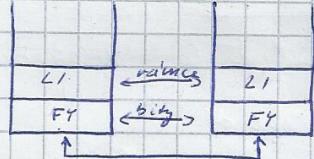
BTS - první stanice - telefon
 univerzální přes existující databázi



4. Prednáška



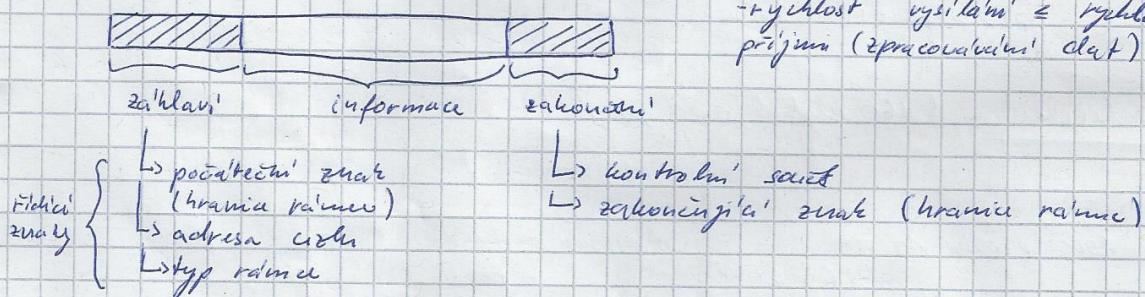
linková úroveň



Funkce

- stanovení hranic rámce
 - 128bit - značkové orient. protokoly
 - 16bit - bitové - " -
 - první čísla - dílkové - " -
- transparentnost přenosu
 - jednoznačný oddělení dat a řídících znaků
- detekce a odstranění chyb
- různé typy dat
 - rychlosť vysílání ≤ rychlosť příjemu (zpracovávání dat)

Format rámce



informace se musí přenášet tak, aby se neponáhalo

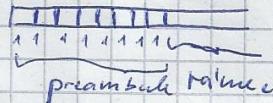
Stanovení hranic bitů

- posloupnost bitů
 - \Rightarrow bitová synchronizace
 - \Rightarrow aritmický přenos

start bit (start)

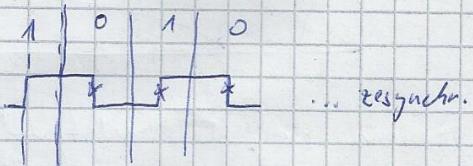
- \rightarrow synchronní přenos
 - závisí na kódování
 - NRZ (NRZ-M)

0 0 0 1 1 1



- ethernet

manchester



Značková synchronizace

- maléru záčátek rámcu
- rámcu musí začít jednoznačnou bitovou kombinací
- ↗ značkové orient. prot.
- bitová - " -

značkové orient. prot = STX (02) ← & ASCII
 ETX (03) - konec do 31> - fiktivní znaky

1 1 1 1 | 1 1 1 1 | 0 1 0 0 0 0 0 0
 ↓ ↓
 STX ETX
 ← kritické spracování ji je 2 ...
 záčátek rámcu základ výpočtu
 porovnává se mactejí výs.

bitové orient. prot.

1 1 1 1 1 1 1 1 | 0 1 1 1 1 1 0

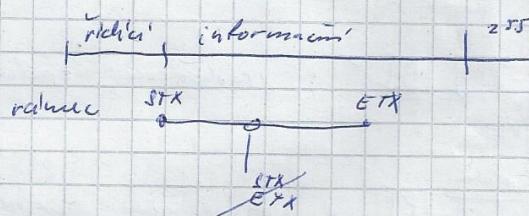
Transparentní přenos

- jednoznačný oddílum' dle od fiktivních značek

znač. orient. prot.

STX start rámcu
 ETX konec rámcu

ASCII kód 8-bitů



řádkové zavedení značek pro rozdílné informace
 násil. značek

DLE

data

02(STX) → DLE STX

03(ETX) → DLE ETX

DLE → DLE DLE

STX . . . DLE STX . . . ETX
 02

řádku

DLE STX . . . DLE DLE . . . DLE ~~ETX~~ ETX

bitově orient. prot.

ramec: 01111110 ————— 01111110

opět se to nesmí dostat dovnitř

- vložit do po poli jednotekých

0111110	data + 0
01111110	meziní znacka
011111110	chyba
0111111101	přerušení přenosu ↳ přijate "data" zahodi"

Př.: 01111101 → 011111001
↳ vložením

Detekce a korekce chyb

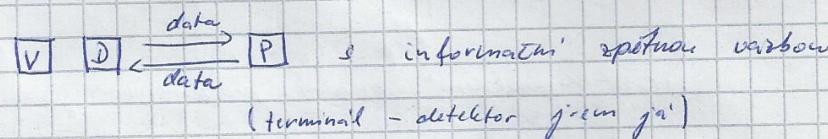
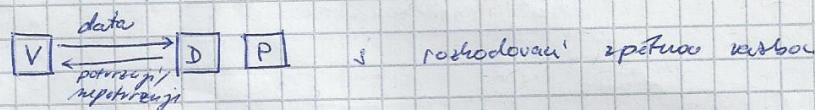
detektioní - rozpoznavání
samoopravní - můžete i opravit

- ARQ

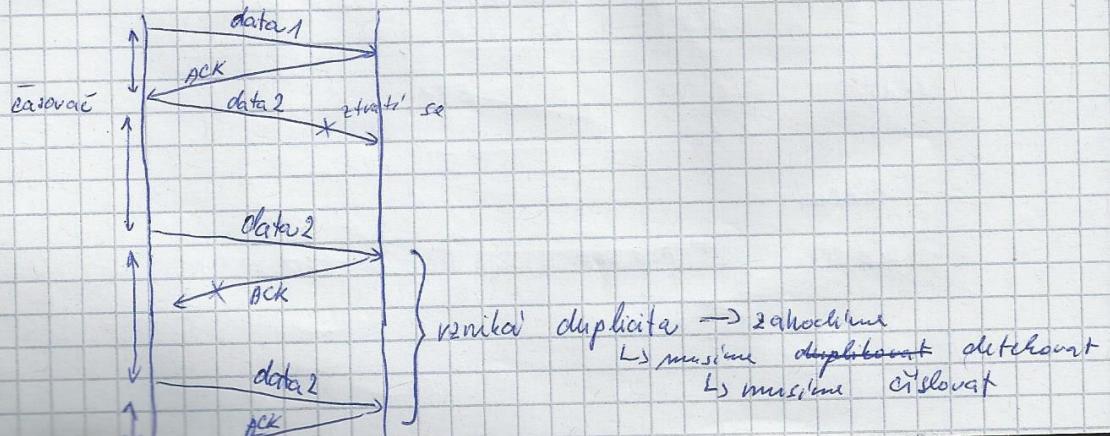
Schemata: ARQ = automatic request query
FEC = forward error correction
přenos v reálném čase
družice u planety

- Internet
- RT
↳ ↳ ↳

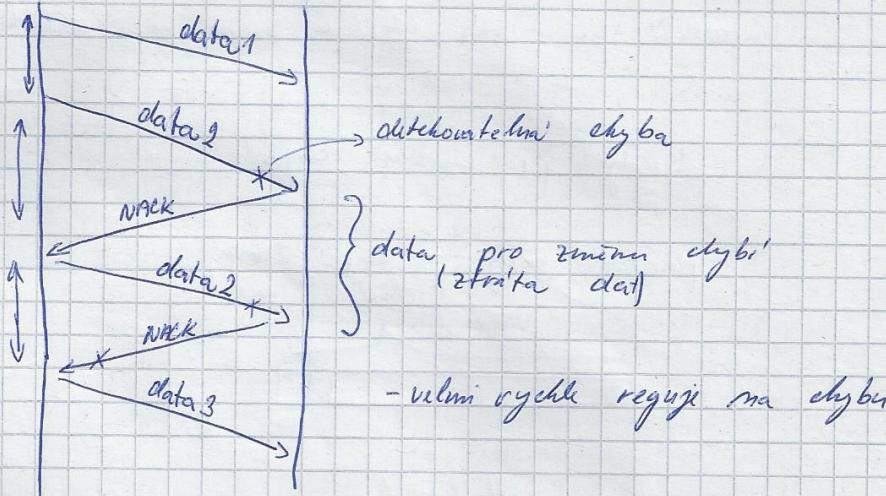
Metody ARQ (opakování přenosu)



↳ rozhodování zpětnou vazbou
• s klidým potvrzováním

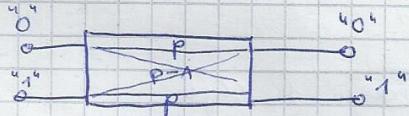


- se zapojením potvrzovačům



- obou stranné aktivity

Model kanálu



- binární kanál
- symetrický ($k=0$ se chová stejně jako $k=1$)
- bez paritěti (nemá, co bylo vysláno představí)

$$1 \text{ bit}: P_1 = p$$

$$2 \text{ bitů}: P_2 = p^2$$

$$n \text{ bitů}: P_n = p^n$$

$$P_n^k = \binom{n}{k} p^k (1-p)^{n-k}$$

mezi kritickou pozici chybného bitu

P chyby $\hat{=} q = 10^{-3}$
délka zprávy N pro kterou $P_n = 0,8$

$$\# P_n = p^N$$

$$\log P_n = N \cdot \log p$$

$$N = \frac{\log P_n}{\log p} = \frac{\log P_n}{\log(1-q)}$$

Bílý šum - & kvůli polohám elektronů ...

Impulzni šum - ráz, když se zapne něco elektrického

Kódy pro detekci chyb

- paritní kódy \leftarrow sudé (#1) liché (#1)



Hammingova vzdálenost

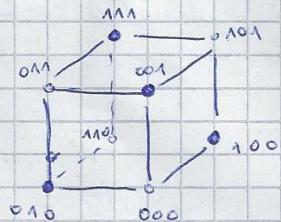
$$\begin{array}{r} 0 \ 0 \ 0 \ 1 \\ 0 \ 1 \ 0 \ 0 \\ 1 \ 0 \ 0 \ 0 \\ 1 \ 1 \ 1 \ 1 \\ \hline P_{\text{liché}} \end{array}$$

$\overbrace{\quad}^2 \overbrace{\quad}^2 \overbrace{\quad}^2 \overbrace{\quad}^2 \quad \text{min} \quad = HV.$

Detectér kód
detekuje d-1 chyb
pro d=2 ... detekuje 1 chyb

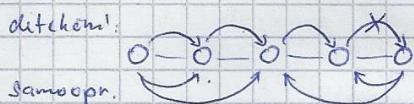
Samoopravny kód

detekuje $\frac{d}{2}$ chyb



vzdálenost jehnoufingových vrcholů = # různých bitů

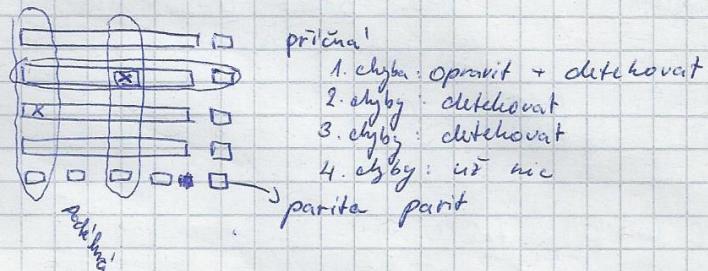
detekční:



samoopr.

opravujeme s tím, že víme, kolik je chyb

- iterativní kód



Hammingova vzdálenost $d = 4$

Cyklické kódy

máme přimájet číslo 6
číslo, aby výsledek byl dělitelný 7
→ kontrola musí být /7/

neboť funguje pro $11^7 \equiv 1$

$$6: \quad \begin{array}{r} 6+1=7 \\ 60+3=63 \end{array} \quad \text{nejdeme, co jsme poslali}$$

$157+4=161$ informace + zabezpečení

$$157: \quad \begin{array}{r} 157+5=162 \\ \text{inf záb.} \end{array} \quad \left. \begin{array}{l} \text{zabezpečení} \\ \text{systematický kód} \end{array} \right\}$$

č normalní matematika

$$\frac{M(x)x^n + R(x)}{P(x)} = Q(x) \cdot P(x)$$

zpráva posun zbytek číslo dělitelné něčím
 (zabezpeč.) (záb.) (zábezpečování polynomem)

$$\frac{M(x)x^n + R(x)}{P(x)} = Q(x) \oplus \frac{R(x)}{P(x)}$$

unormalní matematika
 (modulo 2)
 → vypadne \ominus
 normální přenosy do
 užšího řádu

$$\begin{aligned} \frac{M(x)x^n + R(x)}{P(x)} &= \frac{M(x)x^n}{P(x)} + \frac{R(x)}{P(x)} \\ &= Q(x) + \frac{R(x)}{P(x)} + \frac{R(x)}{P(x)} \end{aligned}$$

$$\begin{array}{r} 0010 \\ \text{zpráva} \quad 1101 \\ \hline \text{e+ zpráva} \quad 1111 \end{array}$$

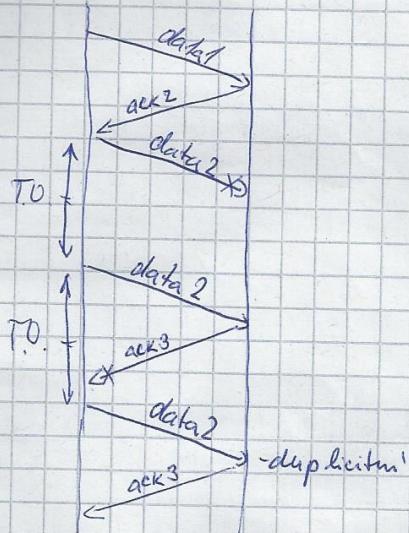
$$\frac{M(x)x^n + R(x) + E(x)}{P(x)} = Q(x) + \frac{E(x)}{P(x)}$$

když je chyba celosícelně
dělitelná $P(x)$, tak ji'
můžeme odstranit :

Voli se speciální (chybové) polynomy

5. přednáška

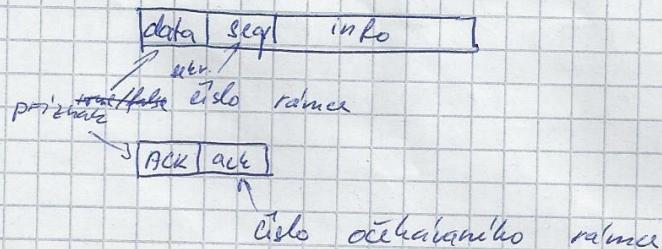
Simplexní protokol



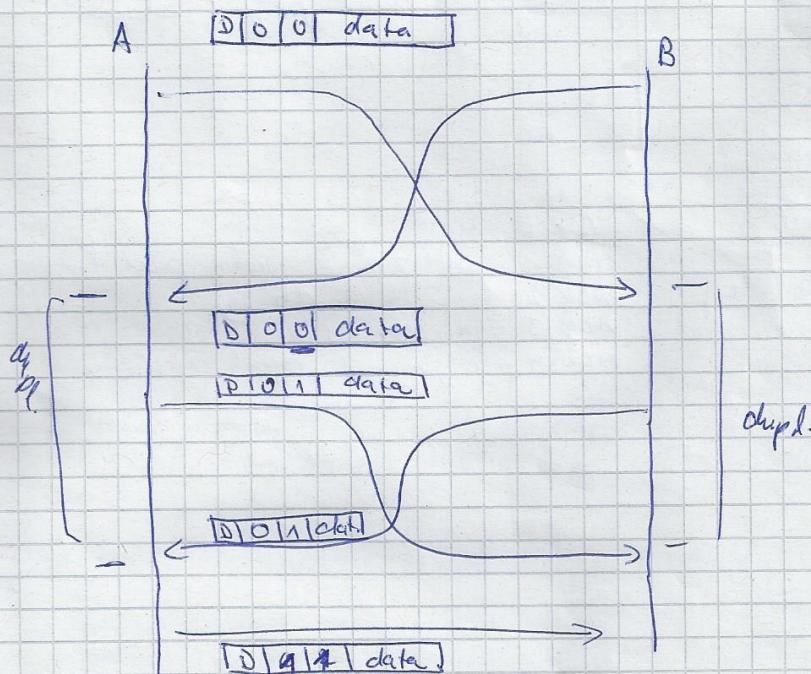
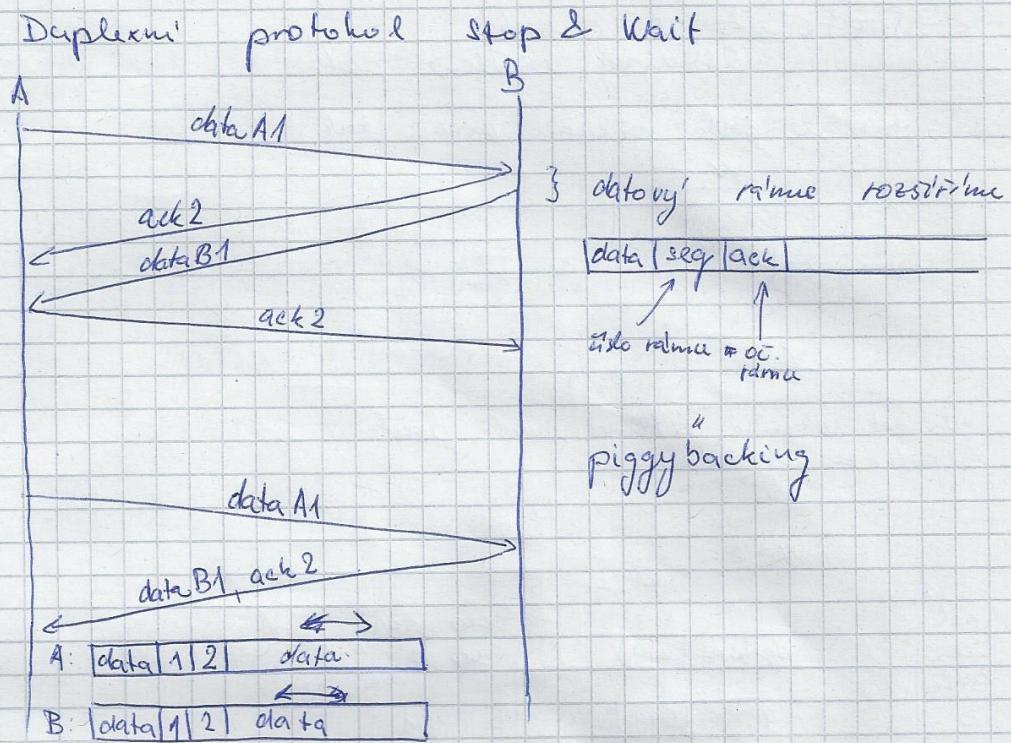
zabýval se

- řízení tohoto dat
- detekce chyb + opakování přenosu

- rámec datový
- rámec řídící
- přenos dat
- přenos říd. inf.



duplexní protokol stop wait stop&wait

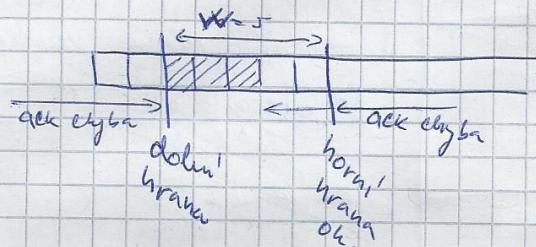


pokud použijeme S2W a začneme duplexním přenosem, tak všechno dojde rychleji 2x

protokol s okénky okénkem okénko

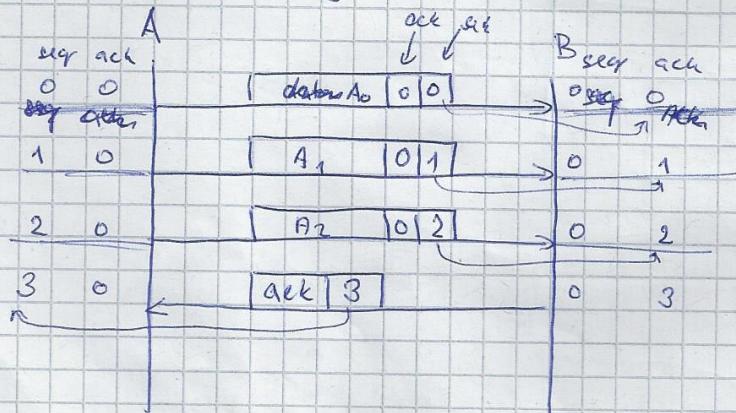
- Protokol s okénky
sliding window prot.

- meračka si li číslo očekáv. valence tak:

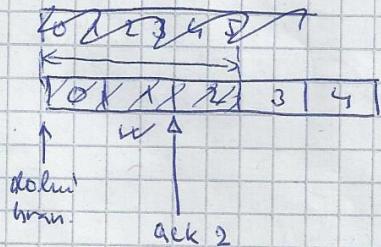


velikost okna ustanjuje max. počet nepotvrzených valencie

$$W = 3$$



musi prijít celou paří potvrz.



ACK 0 *

ACK 1 - potvrzuje se všechny před 1

ACK 2 - až do 1

ACK 3 - potvrzeno 0, 1, 2

ACK 4 - chyba, 3 nem' odeslana

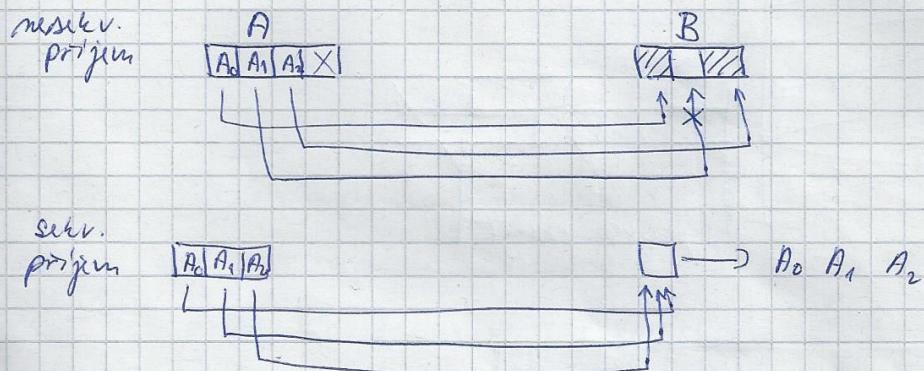
protkoly s okénkem číslování rámců

Protokoly s okénkem

- se sekvenčním přijímaním
 $w = 1$ (přijím. ok.)
- se mesekvenčním přijímaním
 $w > 1$ (přij. ok.)

Okénko

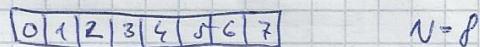
- přijímací - počet přijatých rámců málo počtu
- vysílání - # odeslaných rámců bez potvrzení



Číslování rámců
 $0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow \dots$

Omezení číslen. mod $\leq N$

sekv. přijm $N = 8$ $N = 12$
 ↳ jaká může být max. velikost okna?



ACK 0 - nepotvrďuji mi

ACK 8 → ACK 0 ↳ nepotvržuji mi
 ↳ potvržuji všechno



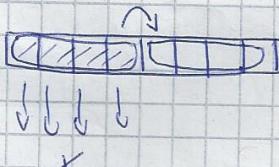
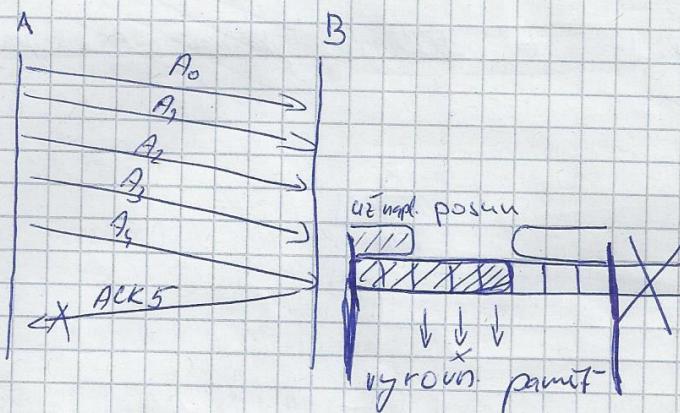
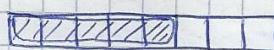
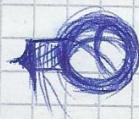
ACK - 0-7
 mi všechno

$$W \leq N-1$$

velikost vysílačeho okna
 musí být alespoň a 1 menší
 než rozsah číselování

Nestandardní příjem

$$W_{\text{vys}} = W - p \geq j$$

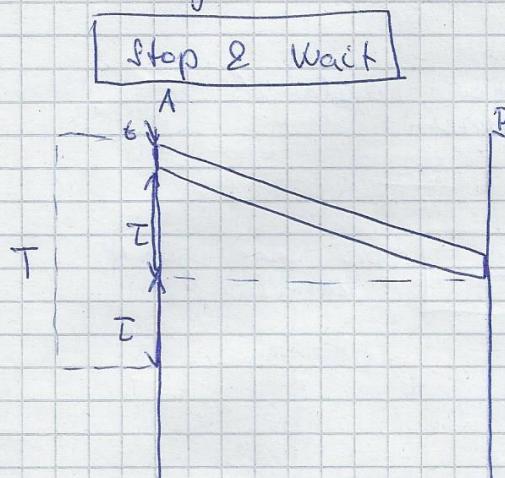


a může být

$$W \leq \frac{N}{2}$$

ocenka musí být disjunktivní, aby se mohly využít
ocenka pro pořadí

Využití komunikačního kanálu



$$T = 2\tau + t$$

$$\tau = \frac{l}{v}$$

$$t = \frac{N}{f}$$

l ... vzdálenost [m]

v ... rychlos sítí
sig. vedením
[m/s]

N ... délka zprávy [b]
 f ... frekvence [Hz]

rychlos [s]

Příklad: Přenos pomocí geost. družic

délka zprávy $N = 10^4$ bitů

rychlos přenosu $f = 10\text{ kHz}$

rychlos sítí $v = c = 3 \cdot 10^8 \text{ m/s}$

vzdálenost $l = 36\text{ 000 km}$

$$\tau = \frac{36 \cdot 10^6}{3 \cdot 10^8} = 12 \cdot 10^{-2} = 0,12 \text{ s} = \underline{\underline{120 \text{ ms}}}$$

$$t = \frac{10^4}{10 \cdot 10^6} = \underline{\underline{10^{-3}}} \text{ s}$$

$$T = \underline{\underline{0,241 \text{ s}}}$$

\rightarrow přenos mezi 10^4 dat

efektivní přenosová rychlos

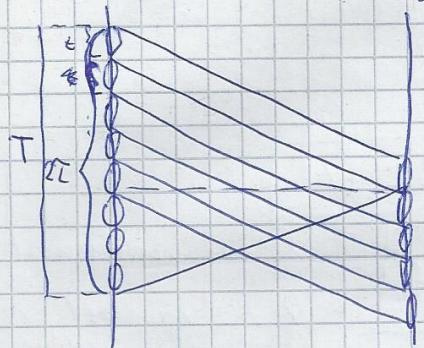
$$f_{\text{eff}} = \frac{N}{T}$$

$$f_{\text{eff}} = \frac{10^4}{0,241} = \underline{\underline{41\ 494 \text{ b/s}}} = \underline{\underline{41,5 \text{ kB/s}}}$$

$$\frac{f}{f_{\text{eff}}} = \frac{10^7}{41,5} = 241 \times \text{nižší}$$

přes protokol Stop & Wait

protokol A → klouzajícím okénkem B



pocet načtených poslanych
bez potvrzení

$$W = \frac{T}{E} = \frac{E+2E}{E}$$

$$W = 1 + \frac{2E}{E} \quad \text{pro max. využití kanálu}$$

S&W - hodi' se tam, kde je $\frac{2E}{E}$...

Příklady protokolů linkové úrovně

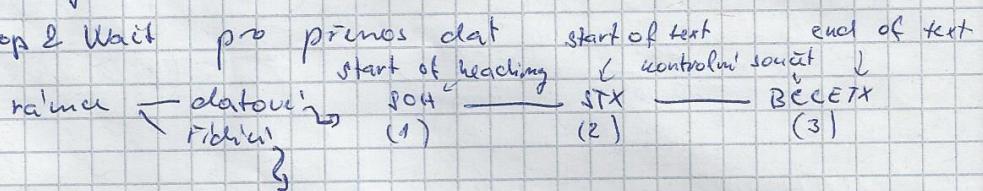
znakově orientované (BSC - IBM)

silově orientované (HDLC), SDC - IBM
LAPB

Znakově orient. prot.

BSC - BiSync Control

- Stop & Wait pro přenos dat



ACK - potvrzení

EOT - end of transmission

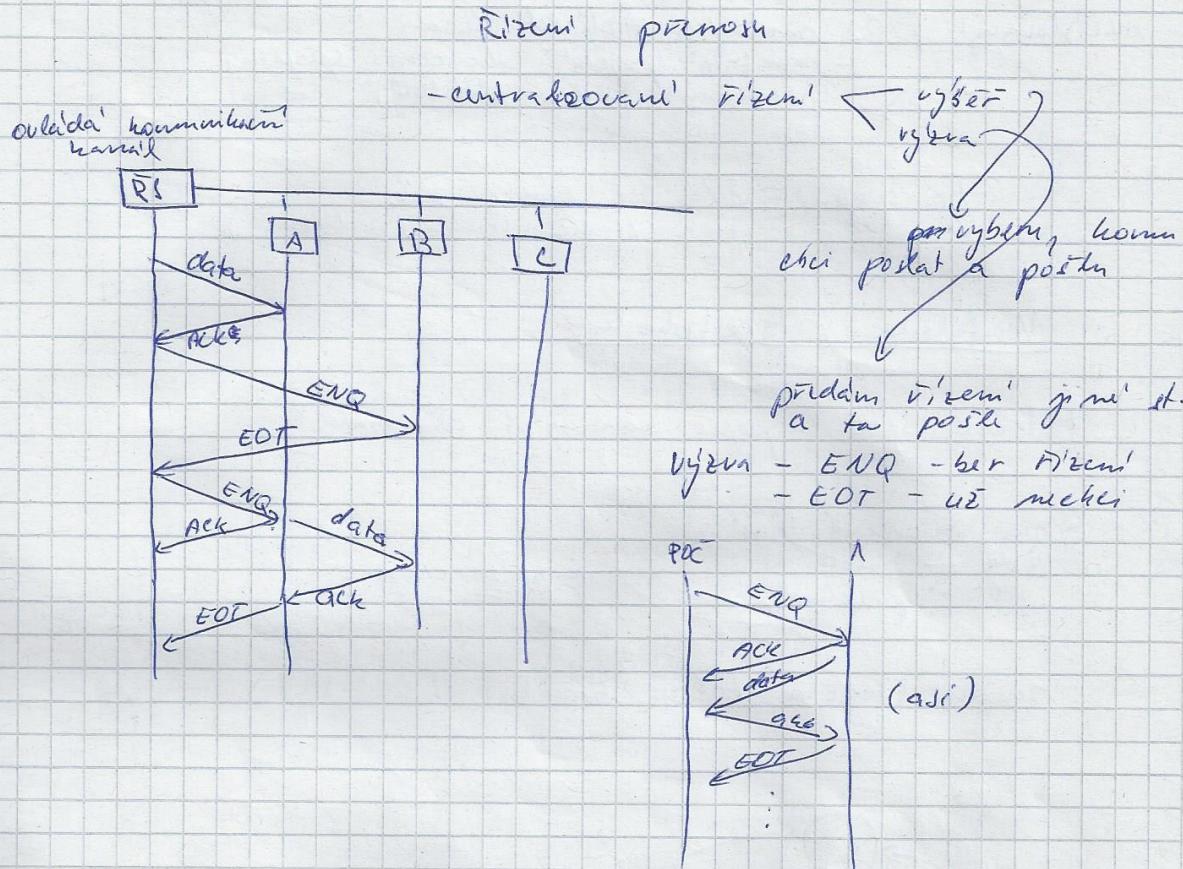
DLE - uvozovací znak dat datového znaku, který vypadá jeho řídce'



Transparentnost

- řídicí znak v datech
DLE + znak (DLE DLE)

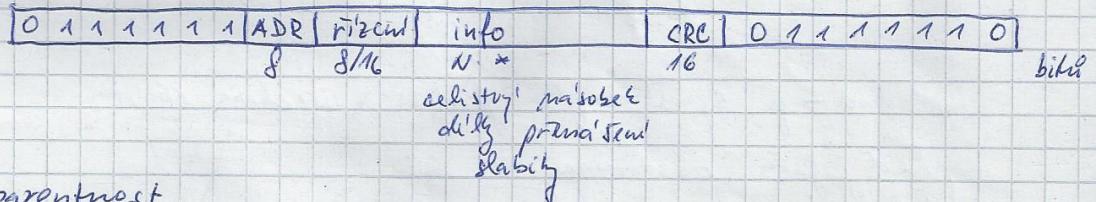
Rízení přenosu bitově orientovaný protokol transparentnost hdlc rr rnr rej srej



Bitově orientovaný prot.

HDLC - High data link control

ramec



Transparentnost

Po 5 jednotkách s výdeji složí Ø nulla

Rízení: typy ramečků
mečsloucí
řídící
informaci

1	1	P/F		
1	0	CMD	P/F	N(R)
0	1	/	P/F	/

n(s) n(r)

Příkazy (řídící - CMD)

RR - receive ready N(R)

RNR - receive not ready NR

↳ potvrzují dat, že nepotřebují

REJ - reject NR

↳ dodávají ramečko N(R)+a datový CMD - číslo příkazu

SREJ - selective reject N(R)

↳ když 1 ramečko - chybou → zopakování

prázdnat bezprostřední odpovídání
info
N(s) - seq (číslo ramečka)

N(R) - ack (číslo oček. ramečka)

verifikace protokolu petriho sítě

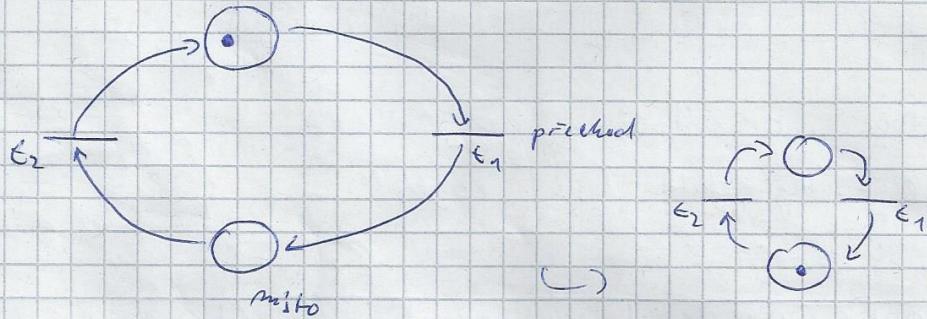
necílový - 32 možných řídicích kódů
- nanečekání spojení, ukončení spojení,
prinášení spojení (RESET) - (chyba)

- typ spojení - 8/16 bit různé slabika
- stav stanice (řídící) / podstavce ()

Verifikace protokolu

Petriho sítě - popis komunického automatu

- hrany - orientovaní
- uzel → místa
přechody } může se střídat
- znaky (značka, token, brouk)

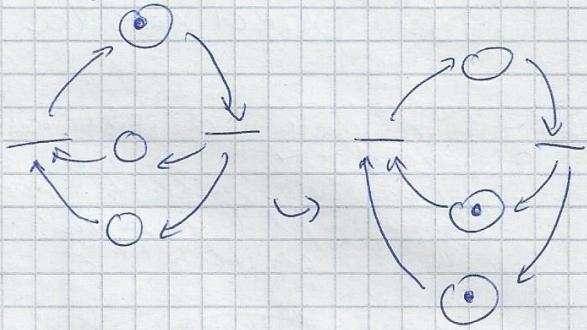
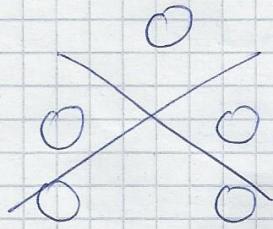


přechod - je spustitelný, jestliže všechna místá
před jím obsazena

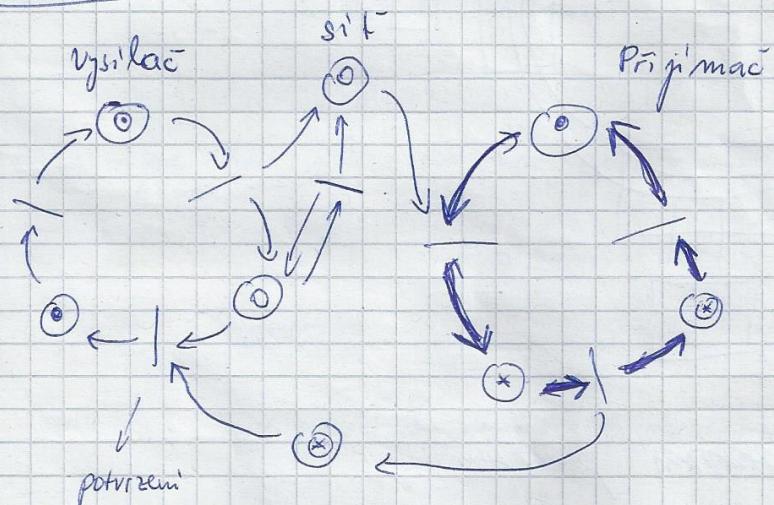
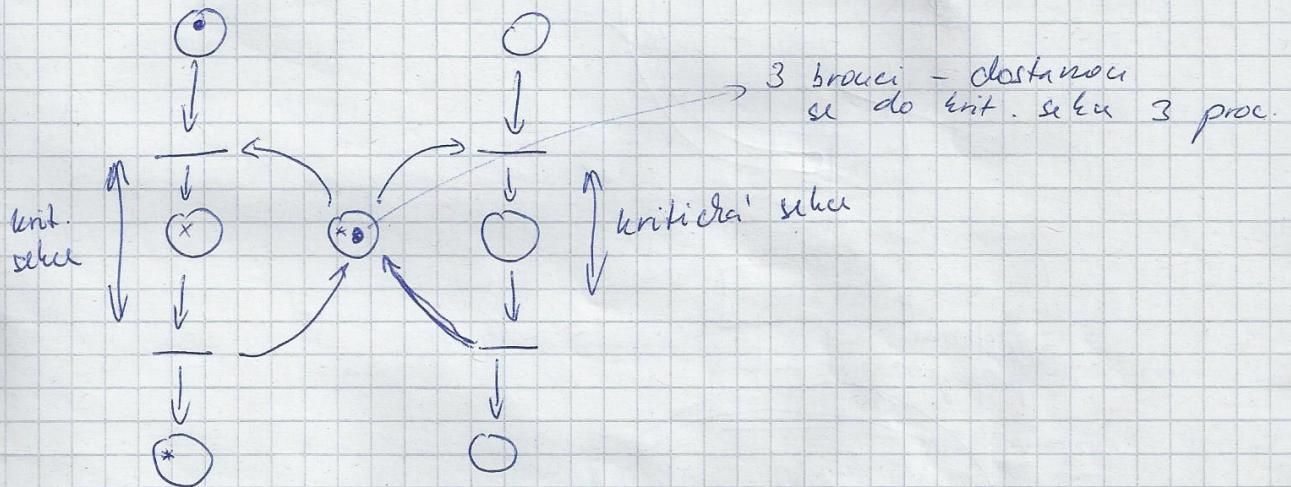
- jestliže ji má více přechodů spustitelných, tak
se vybere libovolný z nich

přechod ze stavu do stavu vypadá tak, že se
ubere jedno znaků ve všech místech před
přechodem a přidá se 1 znaků na všechna
místá za přechodem

synchronizace



Synchronizace :)



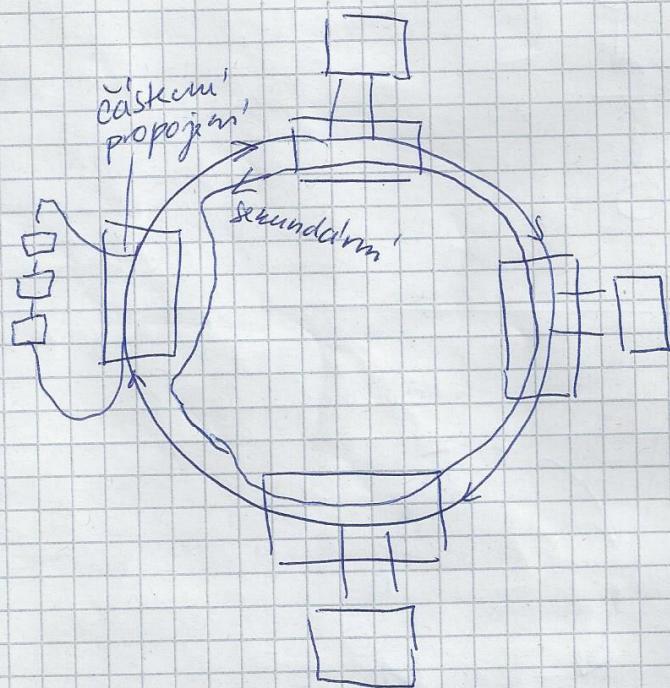
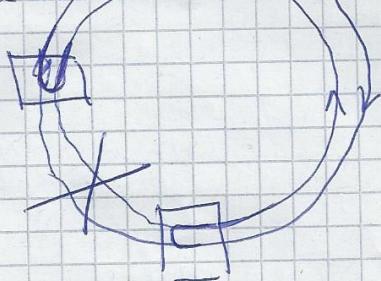
• zjistit se, zda vzniká deadlock mimo reálném cyklu epoch.

7. přednáška

FDDI - fibre data distributed interface

- optická síť, 200km, 2km
- přenosové rychlosti 100Mbit/s
- struktura \leftarrow plné propojení
částečná

- primární kruh - přenos dat
sekundární kruh - záložní

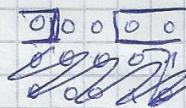


- předávání 'potiskem' pověření'
- kódování NRZI ($NRZI + 1$)
- kód 5B/4B

token bus

5b/4b

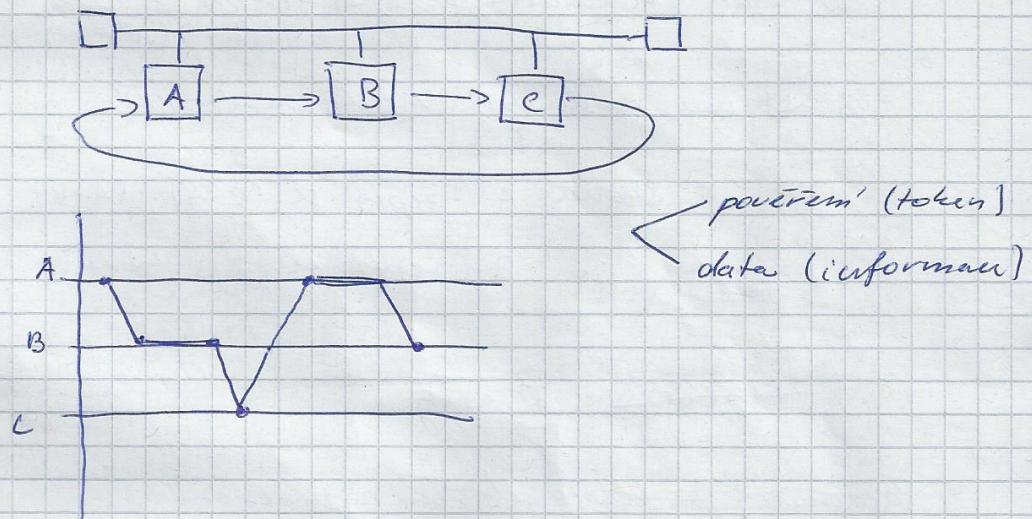
- 5 bitů, 4 informací
- max 3 můž po sobě



1	0	0	0	0	X
1	0	0	0	1	
1	0	0	1	0	
1	0	0	1	1	
1	0	1	0	0	
1	0	1	0	1	
1	0	1	1	0	
1	1	0	0	0	X

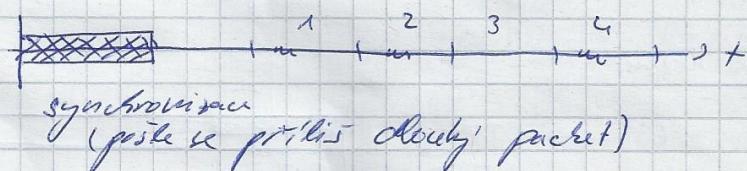
$$\begin{aligned} \text{min. \# zimutn} &= 2 \\ \text{max} &= 5 \end{aligned}$$

Token Bus

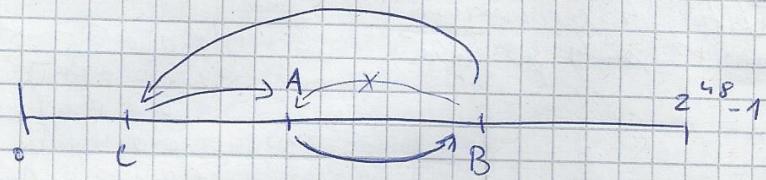


- problem jak obnovit povolení po jeho state-
- malo statické

1 - 3 - 4 vložit packet



Token Bus IEEE 802.4



Obnova priorit

1. stanice málochá → ticho → test na 3 jiné stanice
→ cíle!

2. stanice málochá → ticho → test na 3 jiné stanice →
→ krok (A + B)

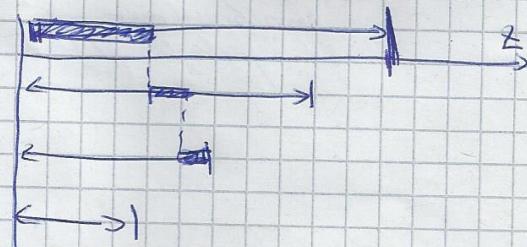
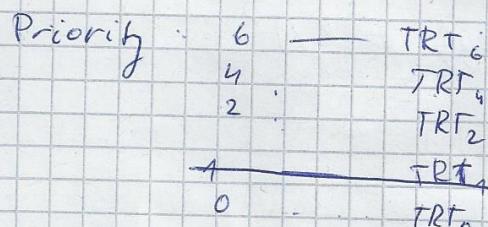
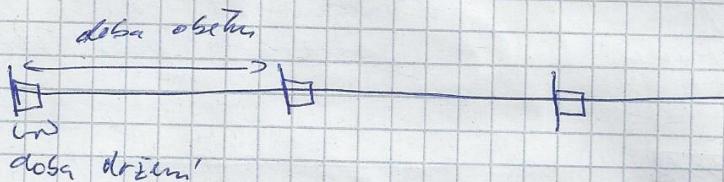
3. stanice málochá → ticho některý → cíle!

Stanice A - zepředu se (0-A), (A-B)

B - zepředu se (B-konec)

Principy Priority

Parametry → doba držení priorit
doba oběhu priorit



Stanice může využít následující čas pro vysílání zpráv s následující prioritou.

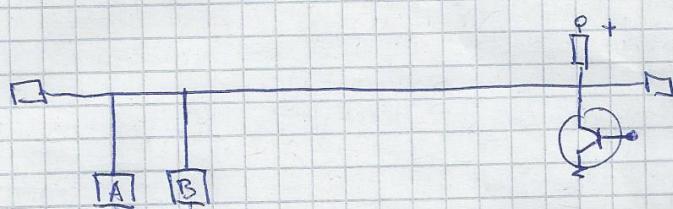
Stanice si o užitkový čas dělí.

Prioritní metody

'priorita zadána' kódem

ADM	test priorit + teor.
ZOB	12.2 - 1
GPA	
UPS	15.1
C	15.1
PSA	

'priorita zadána' kódem



A	B	S
0	0	1
0	1	0
1	0	0
1	1	0

$$S = \overline{A} + B$$

A	1	0	X
B	1	1	0
	↓	↓	
	S = 0	0	1

odčítání {
 A 01 - prioritá
 B 001 - výběr

Užívání → 1 - pokračují
 0 - slýší odcenu 0 - poloh.
 1 - slýší odcenu 1 - končí

A	4	4	4	4
B	5	5	5	5
	6	6	6	6

Monopolizace - stanice S
 máj prioritou využívá
 pořad

→ dynamická + statická
 priorita

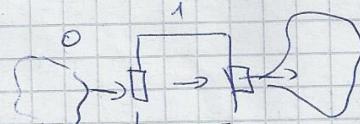
A	0	4	1	4	2	4
B	0	5	1	5	0	5
	6	6	6	6	6	6

dyn. stat.

Dynamická priorita

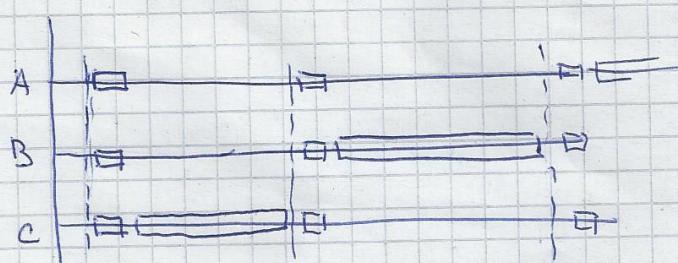
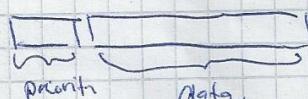
0 - něco
 1 - výběr

0/1.



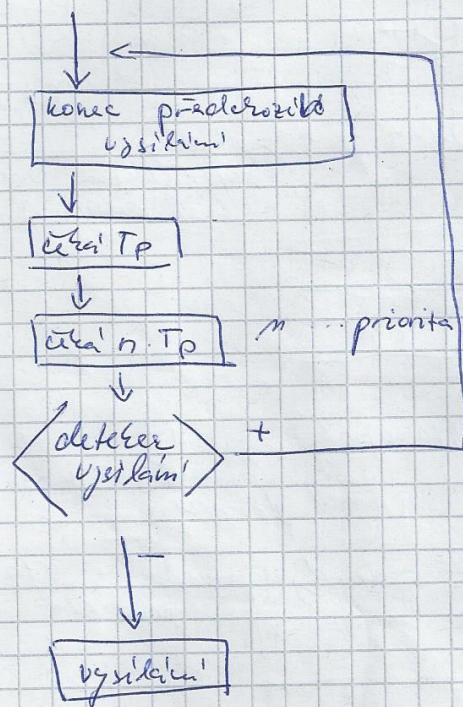
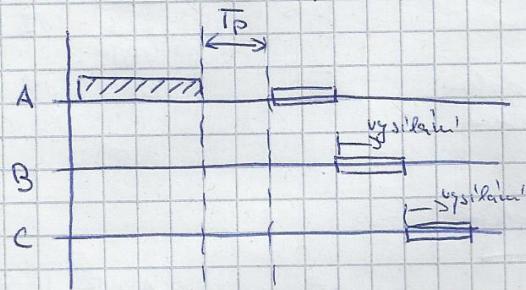
A	0	4	1	4	1	4
B	0	5	1	5	0	5
	6	6	6	6	6	6

Realizace



priorita zadána časem

Priorita zadána časem

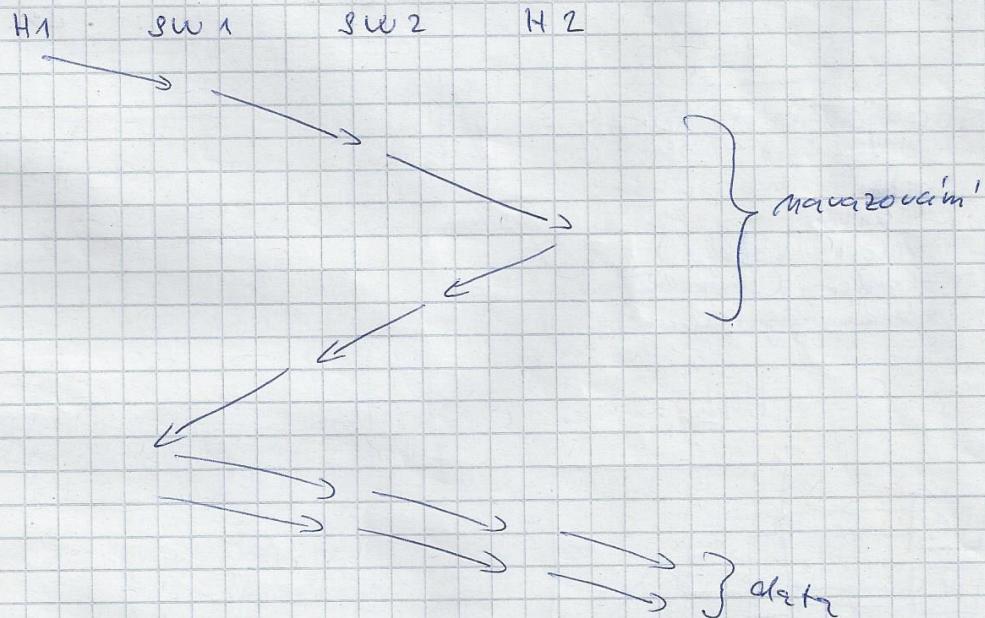
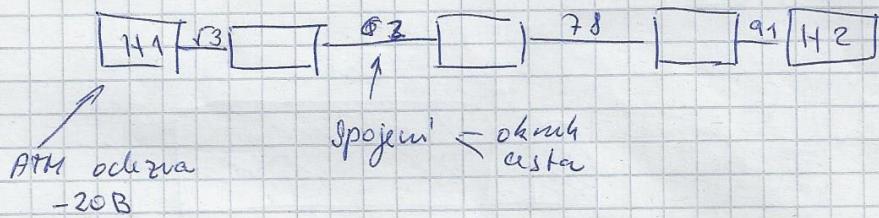


ATM - ~~asynchronous~~
Asynchronous Transport Block

AT&T - synchronous' režim

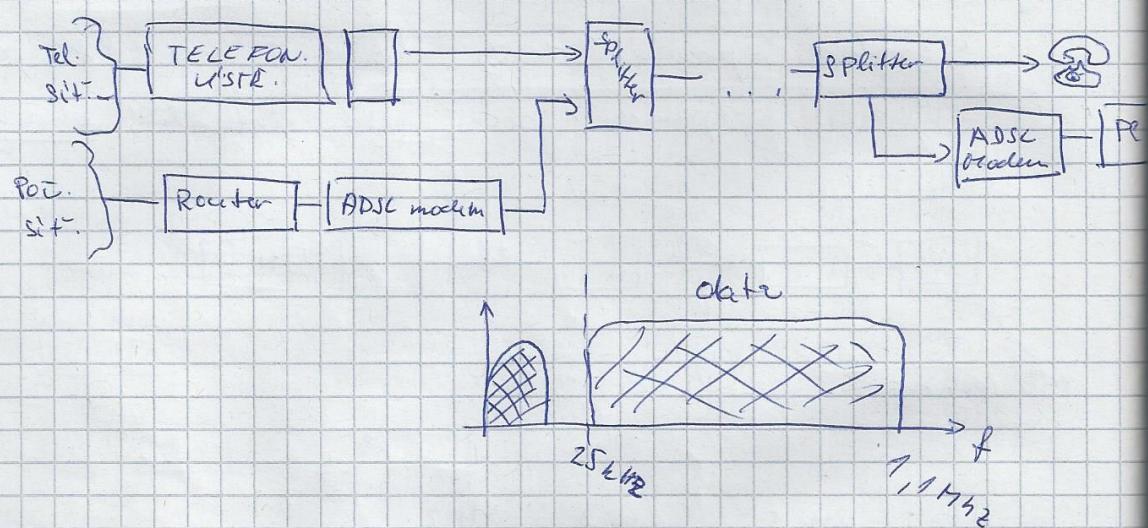
plane → ⊗ ⊗ →

- základ - prínos bývá 5 bytů za časový slot → 48B data
- využití přepnutí + posun mezi virtuální okny



Přenosové rychlosti - 100 - 1000 Gbit/s

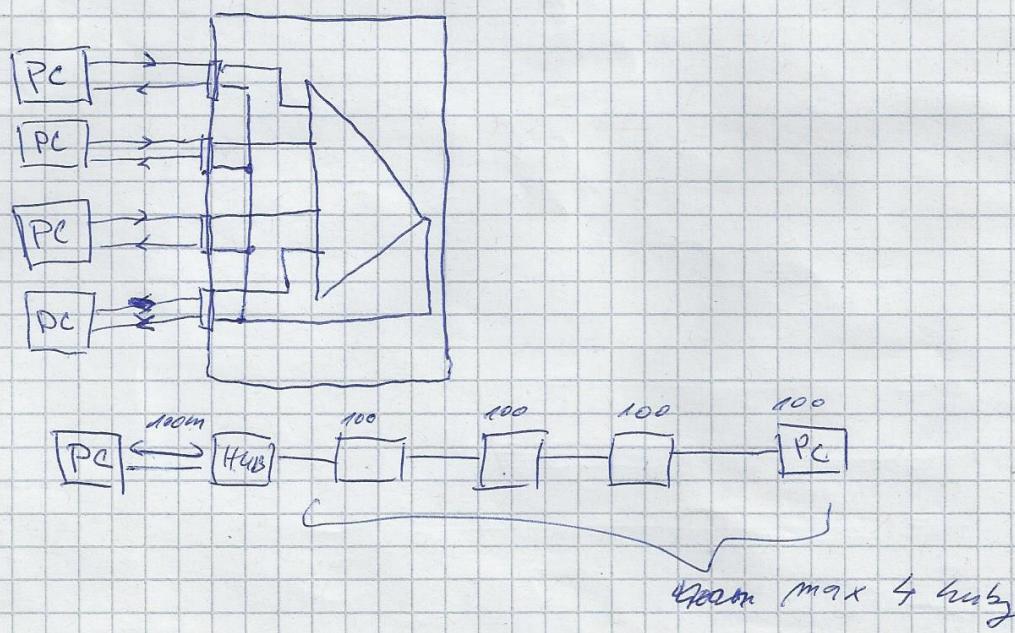
přenos
zpráva
dat



Propojovací prvky síti

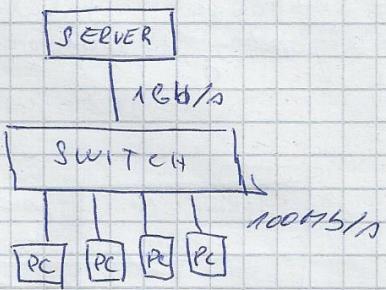
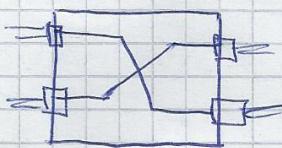
- hub
- switch
- most (bridge)
- router (směrovač)
- brána (gateway)

Hub



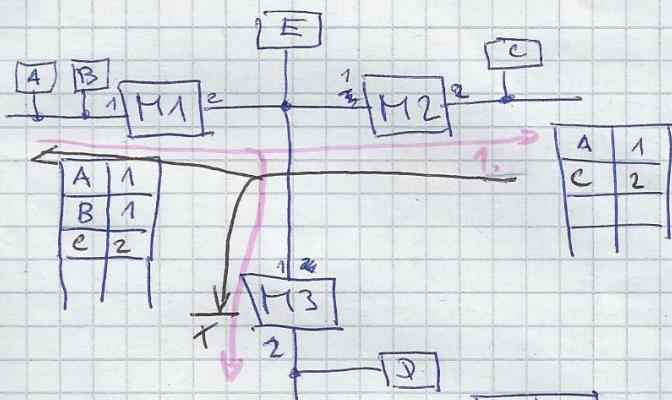
switch bridge most

SWITCH

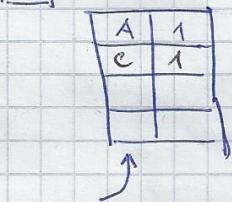


HOST

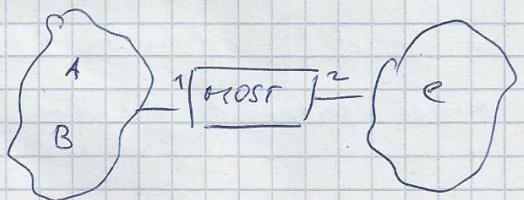
- propagácia' $(A - C)$
- filtrovanie' $(A - B)$
- výber



1. A \rightarrow C
2. C odpovedal'



MAC adresy
(fyzické)



A	1
B	1
C	2

kedy toto musí mať tabuľku - kde je kde

když mení adr. zdroj, si to rozloží wieder

Směrovací

= směrovací tabulka
- algoritmy směrování

slíkna' (IP adresa)	metrická matice	port (rozhraní)
127. 228. 67.0	1	1
147. 228. 73.0	2	1

na rozdíl od mostu (samosítě) u této tab.

musí vytvářet - rachní nebo směrovacím alg.

Brahna (gateway)

= přenáší na aplikativní úrovni

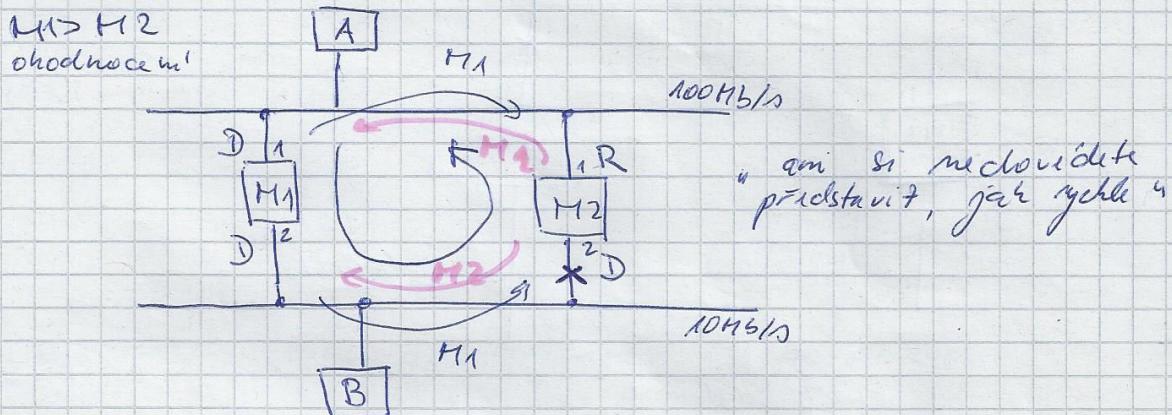
= poštovní brahma

- přenos pošty mezi různými systémy

spanning tree algoritmus algorithm

Spanning tree algorithm

- = např. Ethernet, odstraňení redundancí cest
- = vytvořit se kostra grafu - strom



1) malému kořen strom

(uzel s největším odnoscem)

-zaplňové doručování

M2 spustí ST-alg. - výše správ z 1 a 2
(m užastník u počítače mosty)

D = designated (na usta nevadí ke kořeni)

2) vyberi rozhram 'D' na spojku sběrnici

(problem se spojku sběrnici)

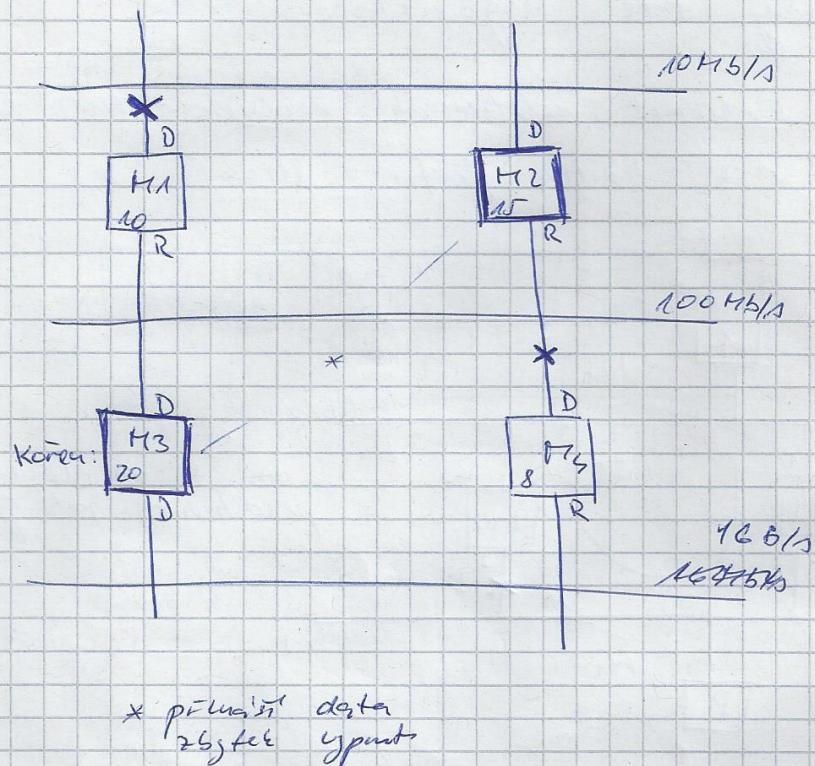
X je dál od Rooty

Porty ke kořeni: R
od D

Pokud na sběrnici 2x D ten ktery
je dál od kořen li port 'odpoji'

ten když výhru' musí periodicky vyzídat ze svého alg.

spanning tree algoritmus algorithm



cca 11

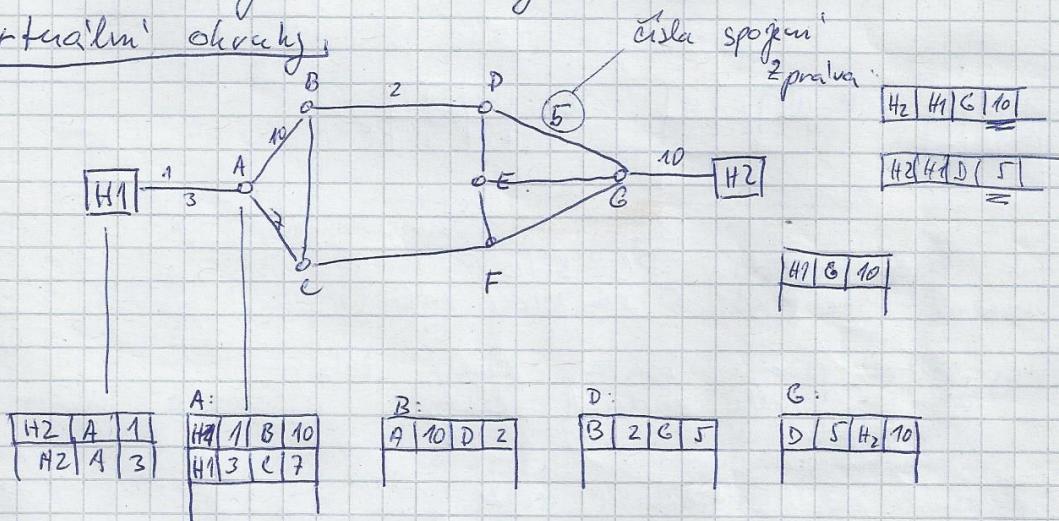
Síťová úroveň

síťová	- propojení koncových lišti
cílová	- propojení sousedních uzlů
fyzická	

virtuální okruhy ← (spojuvání) (nespojování)

datagramové služby

Virtuální okruhy

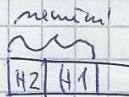


- nemí tak odozvu proti útokům → zničení užlu
- tvorí se dynamicky - přizadlává → vytvoření cesty

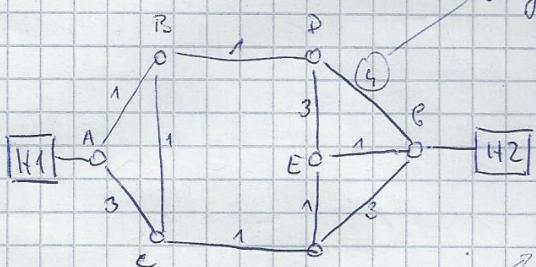
datagramové služby směrování

Datagramové služby

paquet:



metonymie



A:	H2	B	5	
	H1	H1	0	

B:	H2	C	4	
	H1	A	1	

G:	H2	H2	0	

C:	H2	F	3	
	H1	B	2	

F:	H2	E	2	

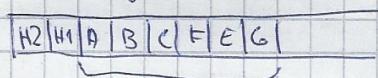
E:	H2	G	1	

V tab. jsou uvedeny PC sítě
směrování → ve všech směrovacích tab.

Směrování → podle obsahu směrovací tab
podle zadanej cesty

Směrování podle zadanej cesty

→ do rámečku paquetu (valence) se zadají adresy
určující cestu



můžeme cestit přes které uzel zpráva pojde (jako
u virtuálních okruhů)

Vytváření obsahu směrovacích tabulek

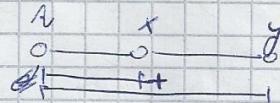
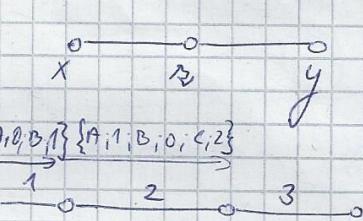
podle vektoru vzdálenosti (DVA - Distance Vector Algorithm)
 podle stavu linie (LSA - Link State Algorithm)
 směrování podle zadání cesty

Algoritmus DVA

- jednotlivé sousední uzel si periodicky vyměňují vektory vzdálenosti
- Bellman - Fordův algoritmus

$$d(x, y) = \min \{ d(x, z) + d(z, y) \}$$

min $\neq z$

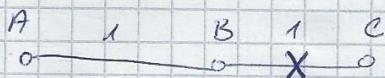


A	A	0	A	1	B	0	A	B	3	A	C	6
B	B	1	B	B	0	B	B	B	2	B	C	5
C	C	2	C	C	0	C	C	C	0	C	C	3
D	D	3	D	D	3	D	D	D	3	D	D	0

souří vektor

posílají si vektory
 vzdálenosti a dopočítávají
 si už které předtím
 měly

Problém: cílový uzel neznáma



A	A	0	A	1	B	0	A	B	2	A	B	1
B	B	1	B	B	0	B	B	B	1	B	C	0
C	C	2	C	C	0	C	C	C	0	C	C	3

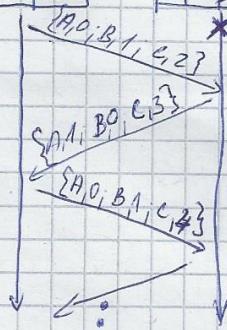
* nestíhá poslat info

Hoj, přes Aho je vzdálenost jen 2 !!

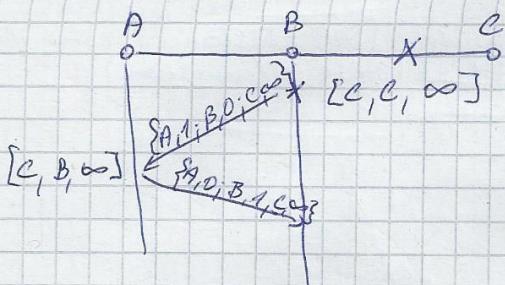
je čas si zmínit tabulku.

C	A	3
---	---	---

C	B	4
---	---	---



C	A	5
---	---	---



Algoritmy pro odstranění 'čísla' do ∞

= okamžitá oprava (trigger update)

- uzel při zjištění změny topologie posílá informaci vektor ihned

- ale i tak by mohl být rychlejší a aby to zase postál

= rozdělený horizont



informaci odl uzel \times může nesít
poslat zpět do \times

= rozdělený horizont s "otvorenou" zprávou cestou

- uzel posílá do "má druhého" následnou cestu s vahou ∞

Protocol

- algoritmus DVA

- RIP (Routing Internet Protocol)

- opakování správ po 30s

- detekce výpadku cesty po 180s

- nekonečno 16

RIPZ

- umožňuje overování správ

- nekonečno > 16

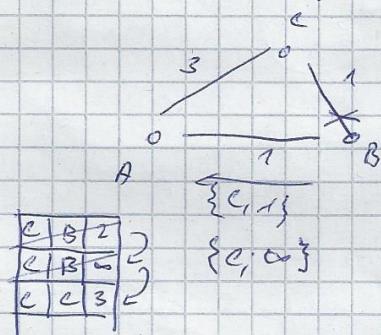
Algoritmus určování vzdálenosti

$$d(x, y) = d(x, z) + d(z, y)$$

$novel < stava!$ \Rightarrow oprava

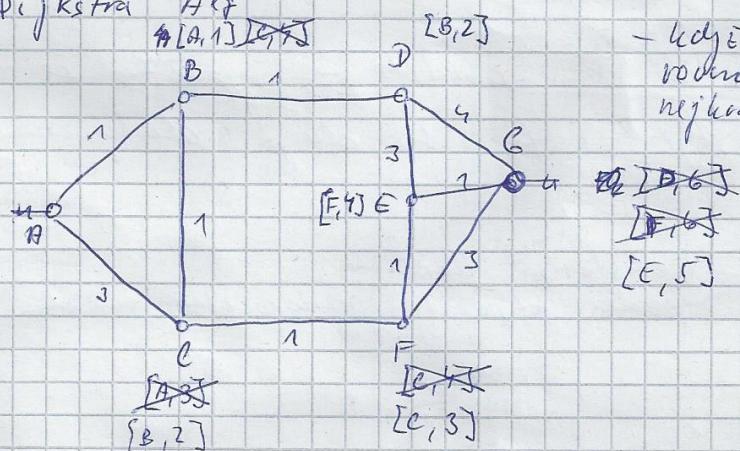
$novel = stava!$ \Rightarrow nic

$novel > stava!$ - pokud ji od uzel, který má
ji méně \Rightarrow oprava
- jinak nic



Algoritmus LSA

- Link State Algorithm
- Dijkstra

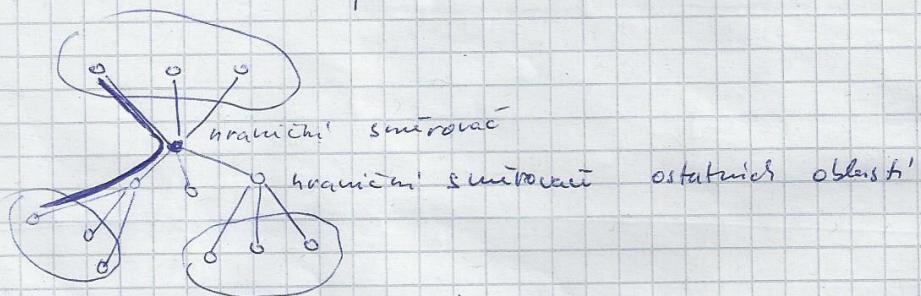
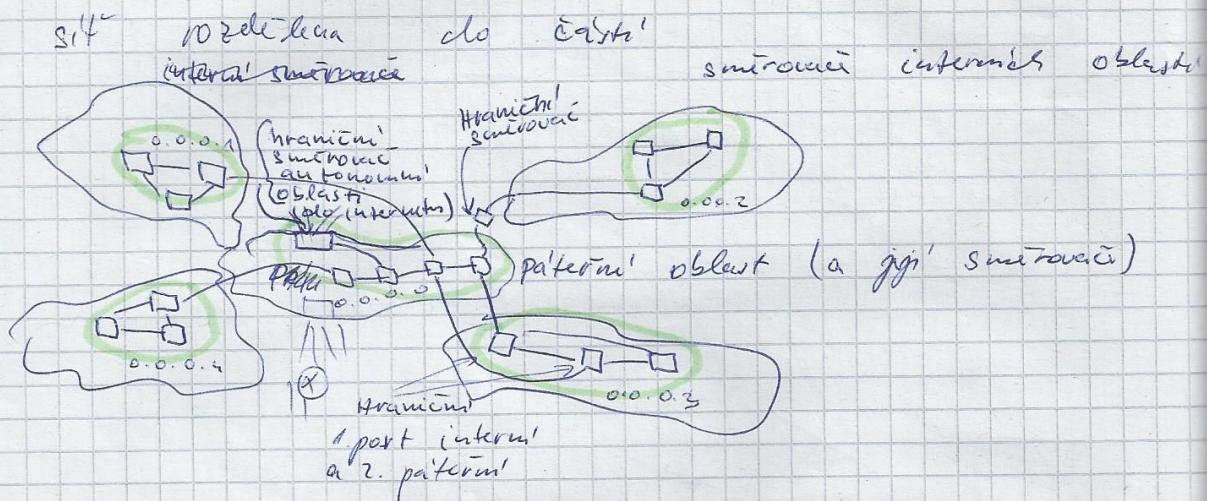


- když vypadne uzel
rozhodnou vypočítat
nejkratší cestu

B-F - pouze, že v tomto směru je vzd. ∞

ospf open shortest path first metrika

OSPF - Open Shortest Path First



aby tabulkám hraničních směrovaců se cesty
dají jednoznačně vypočítat.

Oblast se rozdělí na oblasti \rightarrow vypočta se
směrovacím \rightarrow tyto info se dají do konsolidace

metrika → konstantní hmotnost
podle kapacity přenosového mezinárodní
max 1
min > 1
1Gb/s ... 1
10Gb/s ... 100
průměrný hod.
podle reálné propustnosti

směrování podle zadané cesty směrování v internetu ospf bgp asn

Směrování podle zadané cesty

Směrování v internetu

mitrování (OSPF, RIP)
implicitní směrování (default)

nejít (BGP)

propojení autonomních oblastí

statické tabulky

protokol TCP

velikost tab. ~ 70 000 - 80 000

založené na poloze

zadanou implicitní směrování

* Cíla autonomních oblastí

= ASN 165 / 32 b

používají se místo IP adres

npr. Cesnet (~13 univerzit)
1 ASN

X

Směrování podle zadané cesty

(ne vždycky je třeba výplňovou nejít objevit cestou jinou
je to jen z interního hlediska)

V tab. není jen cíl, ale
i cesta k tomu sítí

má koncovou
část cílu do něj

IPv6 - agregace adres
jedno adres
162

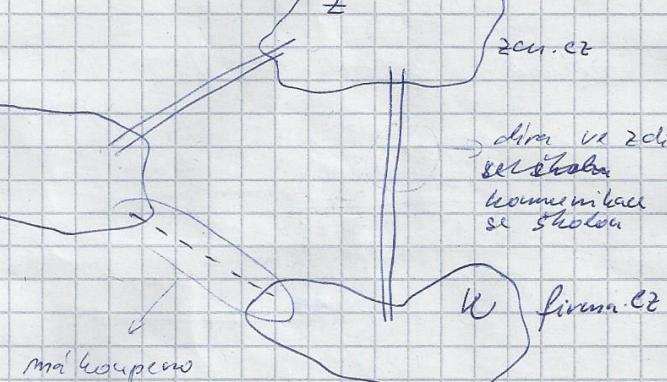
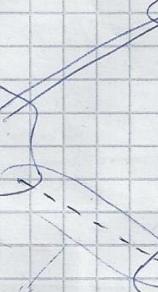
obr. ve zde
se zde
komunikace
se řeší

firm. cz

zcu.cz

z

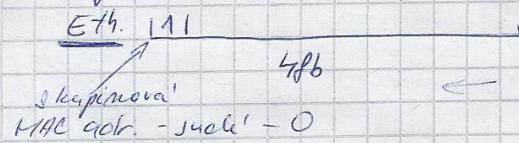
zcu.cz



skupinové adresy skupinové adresování

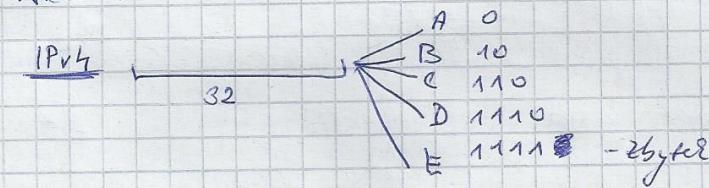
Skupinové adresy, Skupinové adresování

Skupinová adresa - fyzická ukoven

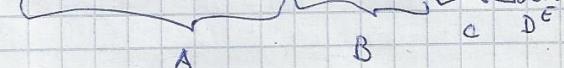


výdejno 1 - broadcast

IPv4
32

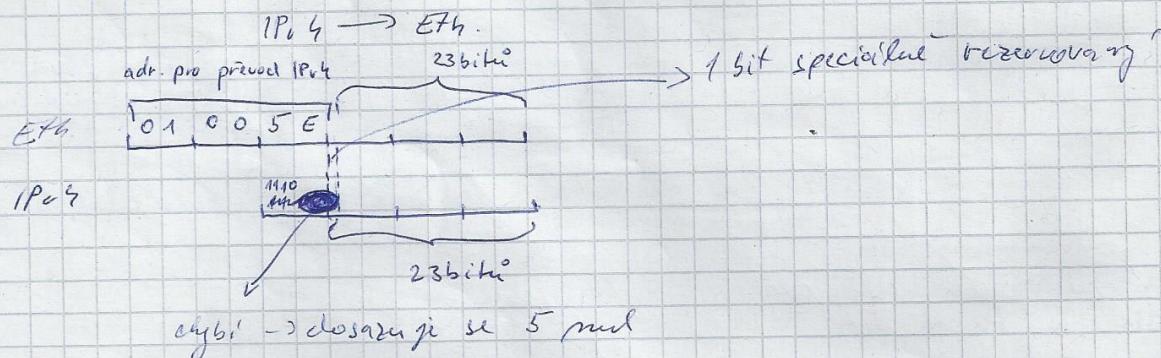


$2^{32} - 1$

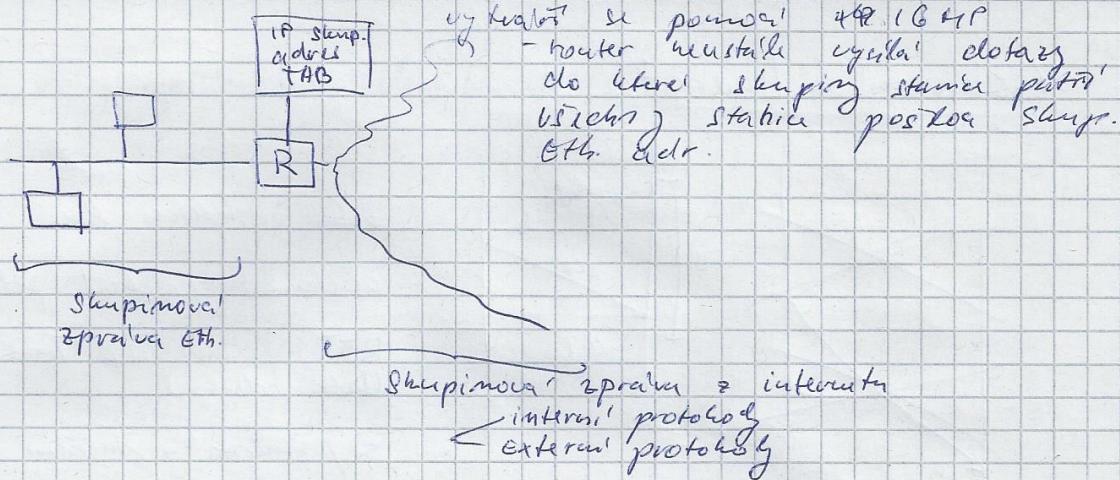


D-s skupinové adresy - 1110 - 2^{2^8} adres

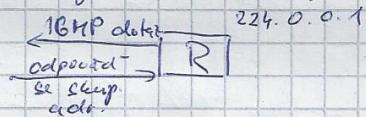
Převod : E�. \rightarrow IPv4



igmp internet group management protocol



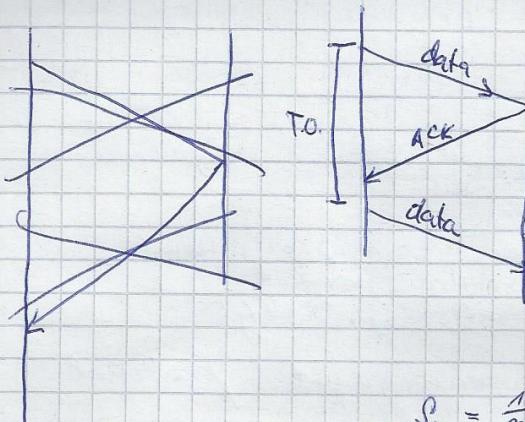
IGMP - Internet group management protocol



Příjem menší adresy v tab. → zpráva se zahodi'

rtt round trip time

Nastavení timeoutu



Doba, za kterou bude
ocíklat potvrzení

RTT - Round Trip Time
(Doba odkazy)

\Rightarrow průměrná + mřížová RTT

$$S_m = \frac{1}{m} \sum_{i=1}^m a_i$$

$$S_{m+1} = \frac{1}{m+1} \sum_{i=1}^{m+1} a_i = \frac{1}{m+1} \sum_{i=1}^m a_i + \frac{1}{m+1} a_{m+1}$$

$$S_{m+1} = \frac{m}{m+1} S_m + \frac{1}{m+1} a_{m+1} = \frac{m}{m+1} S_m + \frac{1}{m+1} a_{m+1} = d S_m + (1-d) a_{m+1}$$

$$\frac{m}{m+1} = x \quad \frac{1}{m+1} = 1-x$$

$$m=7$$

$$m+1=8$$

$$x=\frac{7}{8}$$

$$1-x=\frac{1}{8}$$

$$S_{RTT+1} = \frac{7}{8} S_{RTT} + \frac{1}{8} \cdot RTT$$

= průměrná hodnota
= průměr rozptylu

Problém volby optimální velikosti paketu

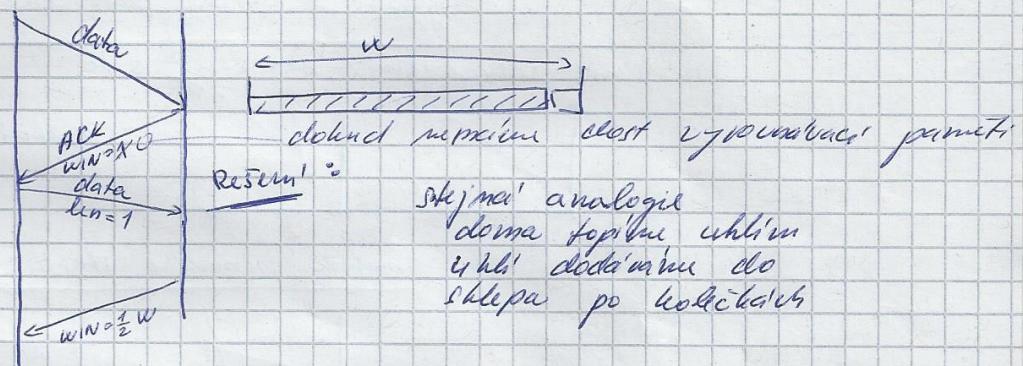
- snaha → co nejdéle, paket

$$\text{za'klad'} - \text{IP} + \text{TCP za'klad'} = 40$$

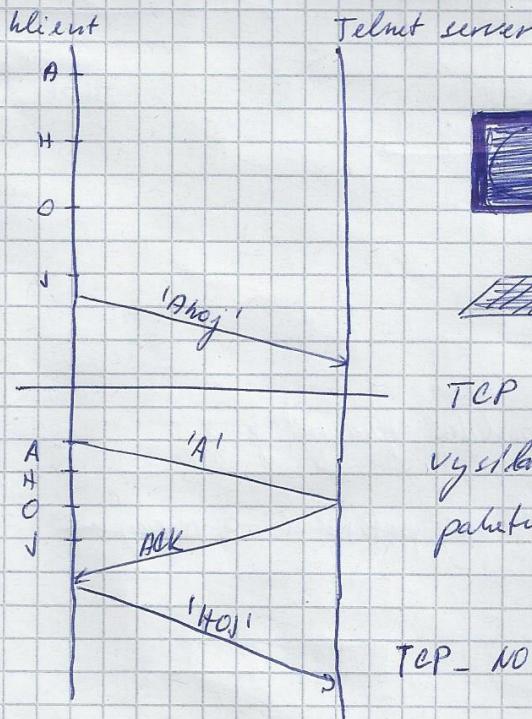
Syndrom hloupého okna

vysílací s velmi vysokou rychlosťí generování dat

přijímací s velmi nízkou rychlosťí zpracování dat



Problém znakových zařízení'



TCP přejde do režimu

vysílání pouze 1 mimořádného paketu

TCP - NO DELAY

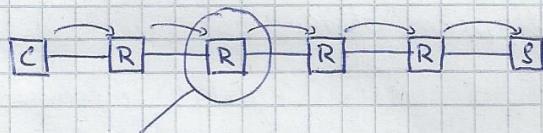
"příliš pomalý generování dat"

řízení toku dat zahlcení okénko fast retransmit rychlé opakování zatížení

Řízení toku dat; a obrana proti zahlcení'

Řízení toku dat - pomocí okna

Obrana proti zahlcení'

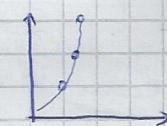
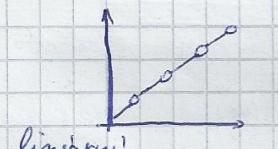


pretilen

(zahazuje nové data)

→ výhnutí = obrana proti zahlcení

Problém stanovení zatížení sítě

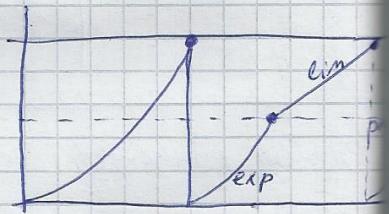
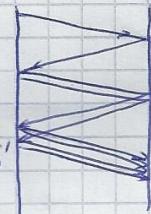


... výhousitnice

, metoda pomalého startu

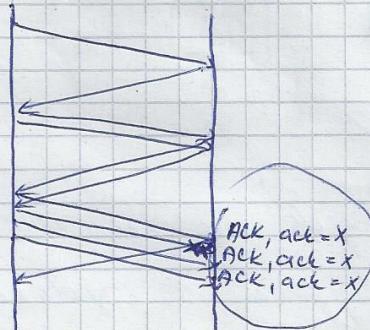
($\frac{1}{2}$ od kolik směrbači zahazují
datu)

zjistitelné prehl



pomalý start předchá
konflikto

Fast retransmit (rychle opakování);

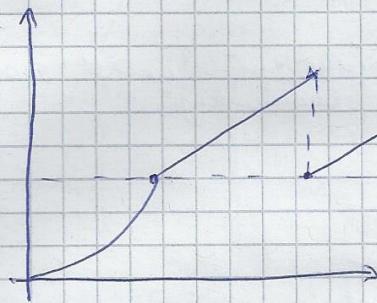


poslední správou je X

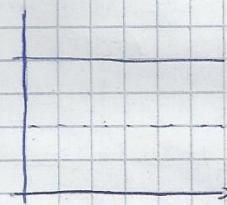
Z duplicitní potvrzení → reagujeme

fast recovery rychlá obnova rtt

Fast recovery (rychlá obnova)



prah - padá jen k prahu



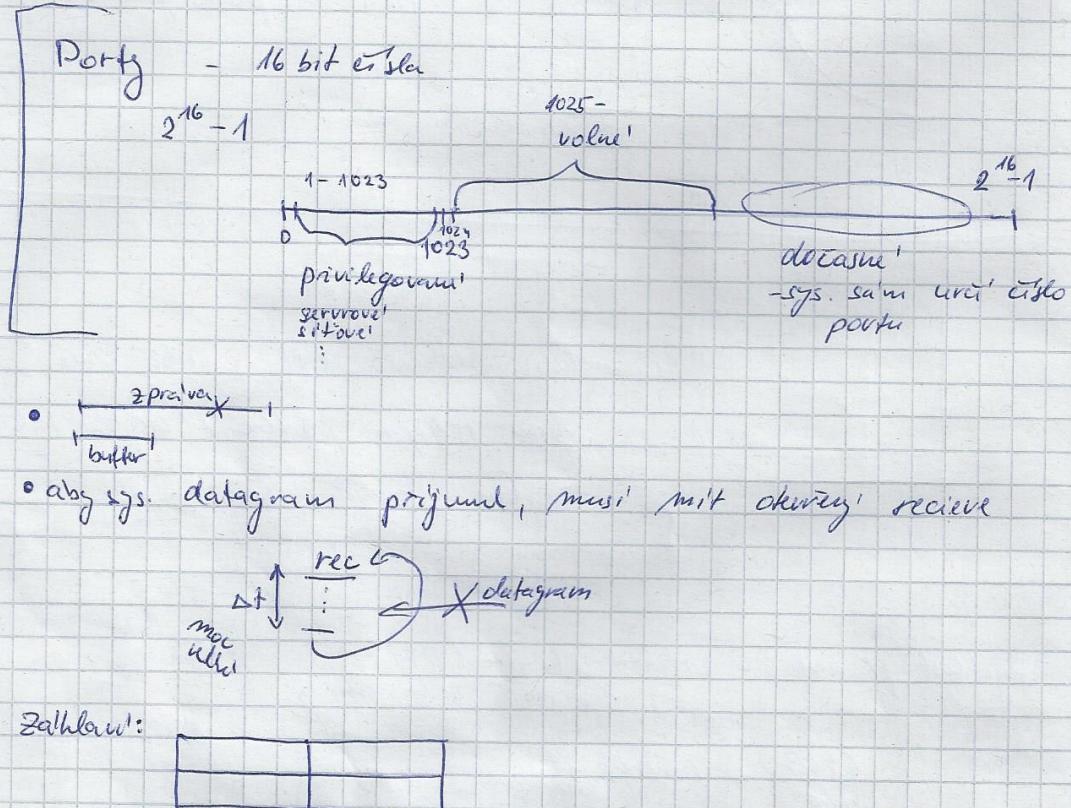
WAN když máme větší okno, než
jsme schopni přeslat dat, tak
vnitru „pseudo okno“?

Rychlosť prazsnu - velikosť okna / RTT
dáve, když 2^{31} cloba odebry
 $\frac{64KB}{0.1s} = 640KB/s$

UDP

~~real time~~

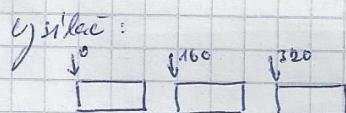
- datagramy
- max. port 64 KB
- základ: čísla portů - zprostředkování určuje aplikaci, kterou spondu komunikují



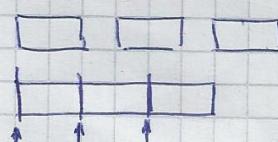
RTP (protocol)

Real Time Transport Protocol

- přenos v reálném čase
- nad UDP
- kromě dat přenos
- čísla verzí
- časoví zálohy
- když se data ztratí, tak se nezajíma o datost
- prostě je přesnost

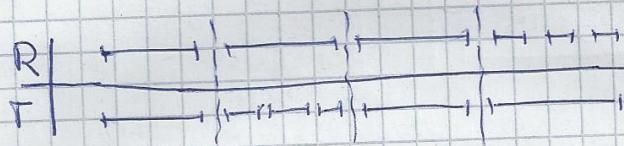


přijímací



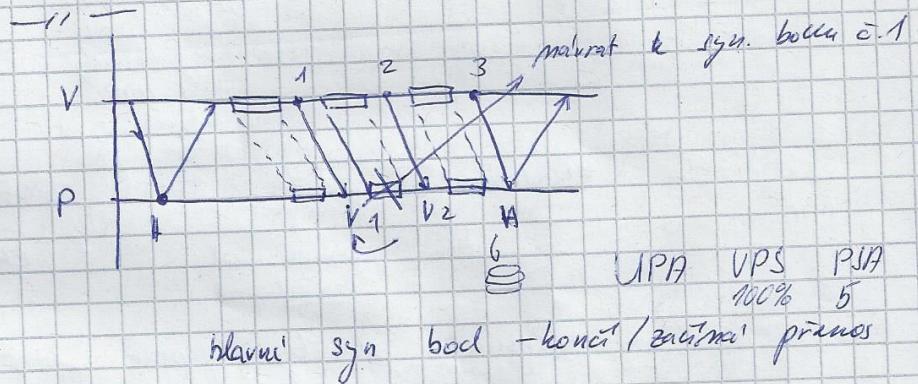
Relační úroveň

- slouží k zabezpečení oprav přenosu
- maci transportní úroveň



= hlavní synchronizační body

= vzdálost



Prezentační úroveň

- připravování dat přenosu

- komprese

- řízení

- uprava dat na univerzální formát

- popis dat - jazyk ASN.1
abstract symbolic notation?

- typy, délka...

- kodovační algoritmus - BER

(basic encoding rules)

Aplikační úroveň

- firičky obecné prostředky potřebné aplikacemi pro přenos dat

- volání vzdálených podprogramů

- transakční zpracování

- spolehlivý přenos dat

- adresování služby (LDAP)

- tabulkové služby

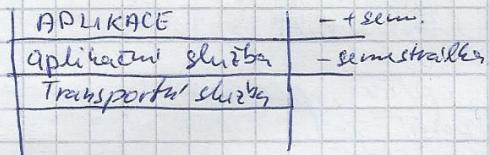
- přenos souborů

- terminálové služby

- přenos e-mailu

- implementované funkce ...

služby tcp ip tcip telnet ssh protokol ftp tftp scp smtp pop imap http gopher dns ldap bootp dhcp snmp rmon



Služby TCP / IP

- PROTOCOLOVY
open / sifr.

uživatelskej = vzdálený přístup - Telnet, SSH protokoly

= prenos souboru - FTP, TFTP, SCP

soubor / jednotky' / sifrovani'
načel UDP
matahovací OS

= elektronická pošta - SMTP, POP, IMAP

simple mail
transf. prot.
čtení el. pošty

= informační služby - gopher, http

zobrazování
dat na síti
přes
data
informace
o čl. a PC
na síť
v DB

= systémové služby - adresářové služby - DNS, LDAP

zjistit info o PC → adresa a adr.

- konfigurace PC - BOOTP, DHCP

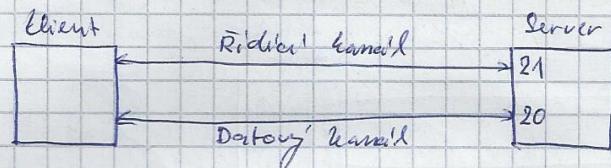
ar
- síťový management - SNMP, RMON
simple network management proto
velké dat... shromažďování

- Bezpečnostní prot. - ~~SSL~~

IPsec, SSL, SSH
sifrování na síti /
výrobců / na transp. vr. /
apl. vr.

Všechny tyto protokoly patří na APL. VR.

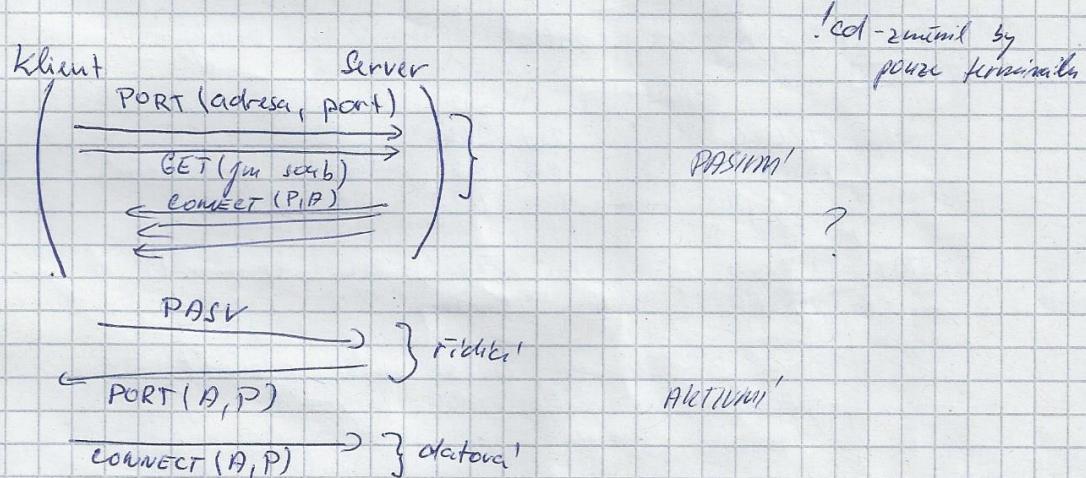
FTP - File Transport Protocol



Ridicí kanál - řídíci protokol přenos
- obdobec terminálových protokolů
+ get, mget, put, mput
stázení nahražení

Dátový kanál - přenos souborů, přenos listingu adresáta

Vypočítaný systém ↘ lokální (Client) !emel !ls, lcd
vzdálený (Server) ls, cd

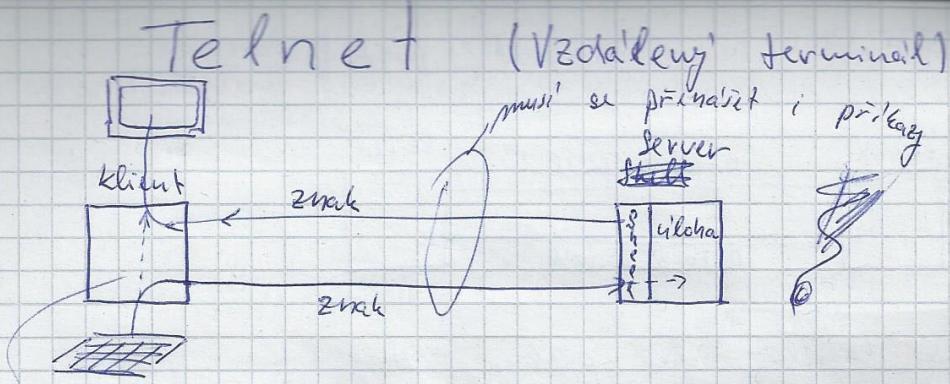


Anonymní FTP

= FTP- uživatel se musí přihlásit (jmeno, heslo)

- uživatel = anonymous, ftp
heslo = email

Používá TCP protokol



Po spuštění úlohy naší shell propouští znak abychom mohli poslat uživateli - urgentní data TCP komunikovat se shellom

Urgentní data: Předložka fronty dat - přednostně zpracování
- nastaví se příkaz
OOB - out of band

IAC - interpret as control ~ řídíci znaky
255 [eod]

CTRL+C 255 234
 IAC kód příkazu poslat uživateli
video terminal

TERM = vt 100 obyčejná, jaký terminál to je
= vt 250 posun kurzoru

Program si, co si máte dělat
- přenáší se jeho řídící signál

12. přednáška

Prostředky pro řízení sítí
(management)

- icmp ↗ echo (ping)
time exceeded (traceroute)
- logické (softw.) analyzátory
 - zazývavání paketu + jeho zobrazování
 - Wireshark, tcpdump, ...
- Zad. 90. tel

- na ISO/OSI vrstvi

- pro TCP/IP - SNMP

SNMP záč

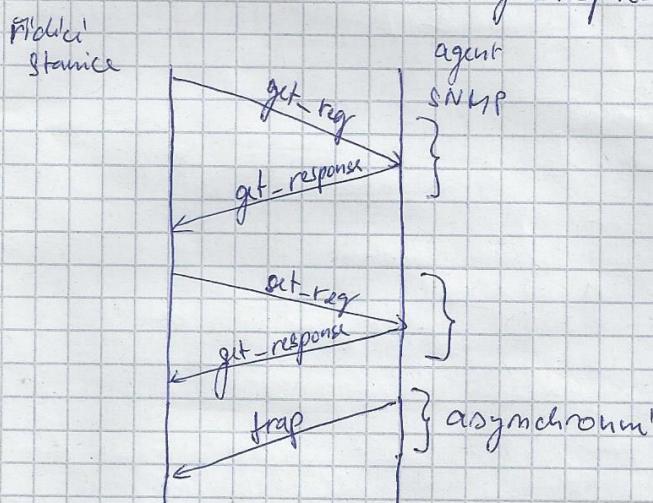
- simple network management protocol

- základ

- operace - čtení, zápis

get-request

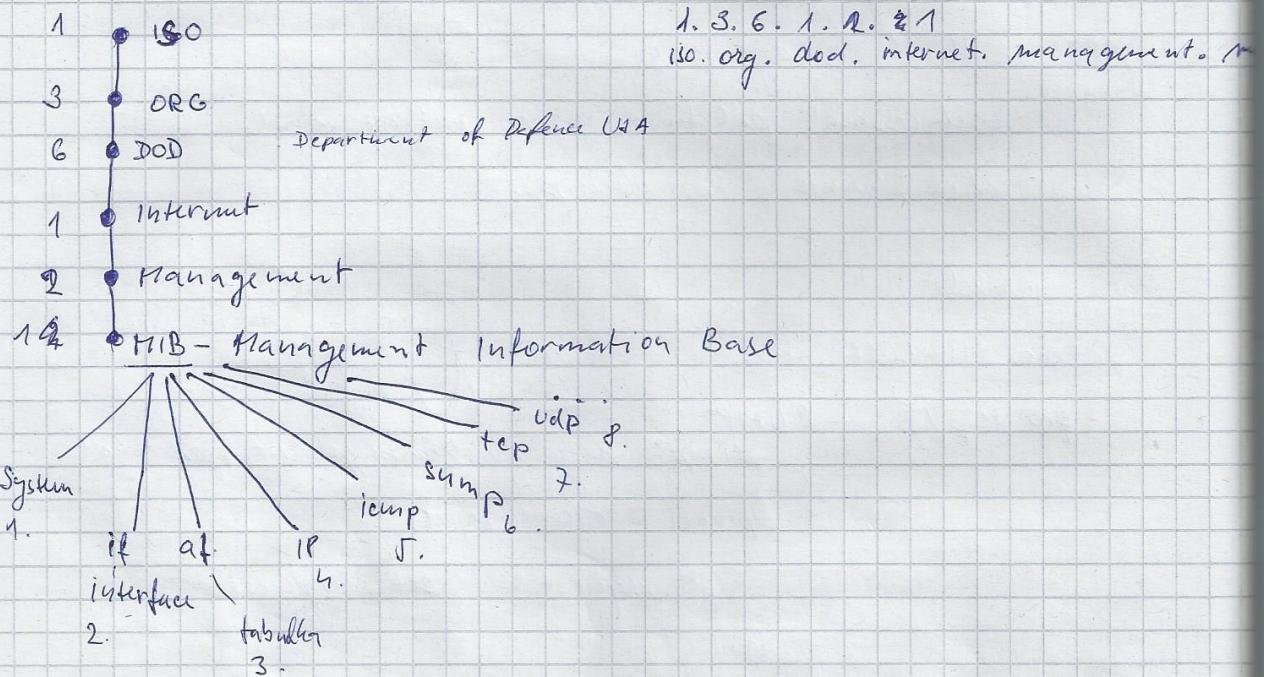
set-request



Basic Encoding Rules
kódování: BER
structure of management information

Problém: - reprezentace dat (podmnožina ASN.1, SMI)

- označování primitivních
- tečková notace
- hierarchický strom



System: jmeno systému

jmeno správce

umístění

oba provoz

:

if: číslo rozhraní

typ rozhraní

přenosová rychlosť

množství přenášených dat

chyby

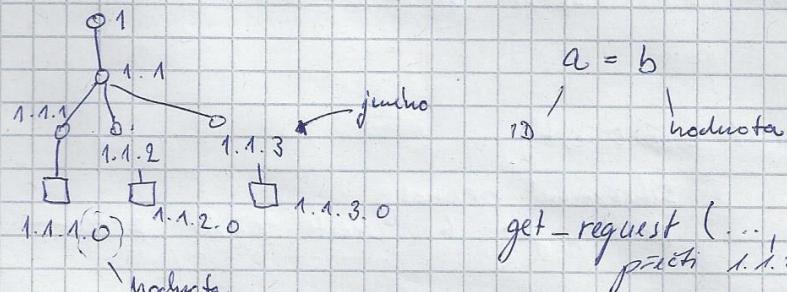
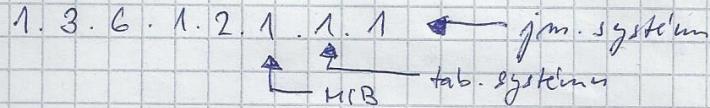
:

oid get_request set_request snmp

Manipulace s promeny

↳ jednoduché tabulky
tabulky

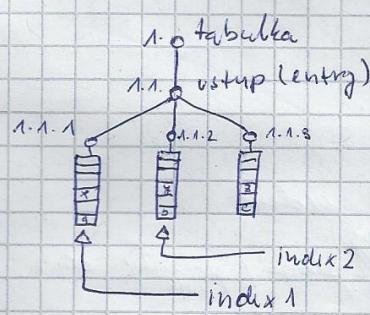
Identifikace: identifikátor objektu OID



get-request (... , 1.1.3.0)
právě 1.1.3.0

set-request(..., 1.1.3.0, [])

Tabulka



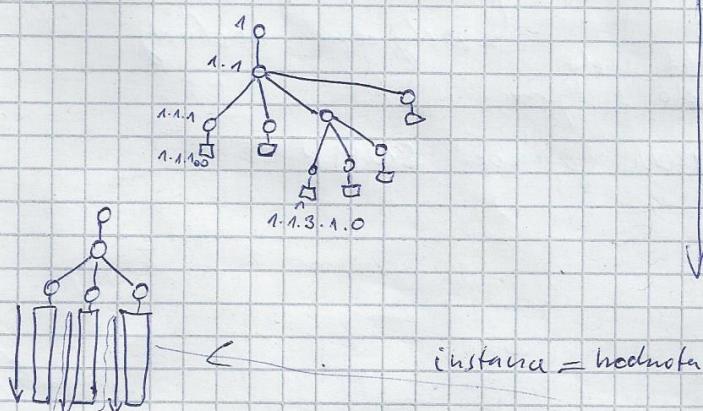
Select [] from tab where □ = hod;

OID . index1 . index2

1.1.3.x.y → z

1.1.2.a.b → b

Sequenční prohlížení tabulek
podle abecedního pořadí



1
1.1
1.1.1
1.1.1.0
1.1.2
1.1.2.0
1.1.3
1.1.3.1
1.1.3.1.0
1.1.3.2
1.1.3.2.0
:

SNMP:
get-next-request
OID → další instance
míti

case
1 → 1.1.1.0
1.1.1 → 1.1.1.0

snmp rmon remote monitoring sonda

Zabezpečení (poradí foto prot.)

SNMP v1

- heslo (v otevřené podobě)
- přístupová pravla → čtení etem' (writable) zapisu

heslo - public - čtení
- private - zapis + čtení

používání → čtení (čítací počet slabší)
čtení + zapis (spustit něco zastavit rozhraní)

SNMP v2 } větší bezpečnost

SNMP v3 } větší bezpečnost

difuzního průnosu
přístup je už víceméně dán strojem

Datovačení → příliš zátěžuje přenosovou linku

SNMP - konec (zakončení)

RMON - začátek

Remote monitoring

sonda - autonomní čítačka

- zachycuje data na určeném vedení (Ethernet, Token Ring)
- sleduje zátěžovou linku (cyklování/ přijaté data, časy...)
- mechanismus aby marnické konfigurace

spoj. tabule → filtri (počet vzorků (číslo záhl.),
datová) rychlosť (vzorek/s), OID
(co chceme záhl.)

- dále určovat akt. uživ. (TOP 10%, kdo s čím...)

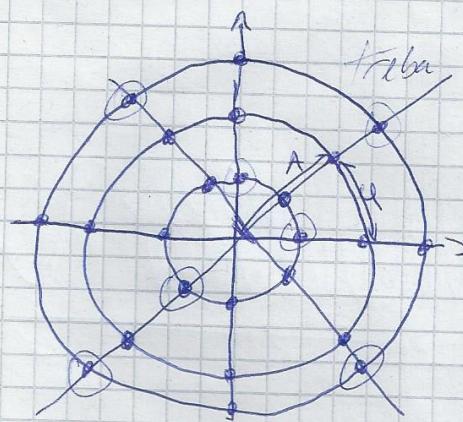
- čtení dat z RMON pomocí SNMP

~~bily papir...~~

QAM

- graf

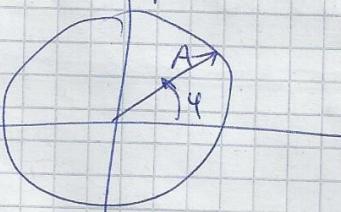
kombinace Amp. a fáz.



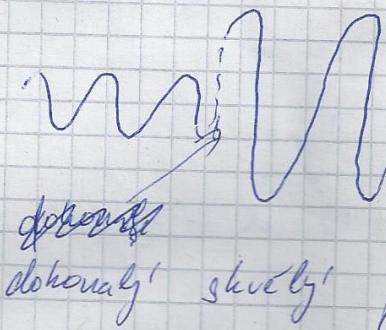
úhlu $\frac{\pi}{4} \cdot 3$ úrovni = 24

- dají se prakticky
využít jen ty, co
jsou od sebe dál

místo uvažovat 2



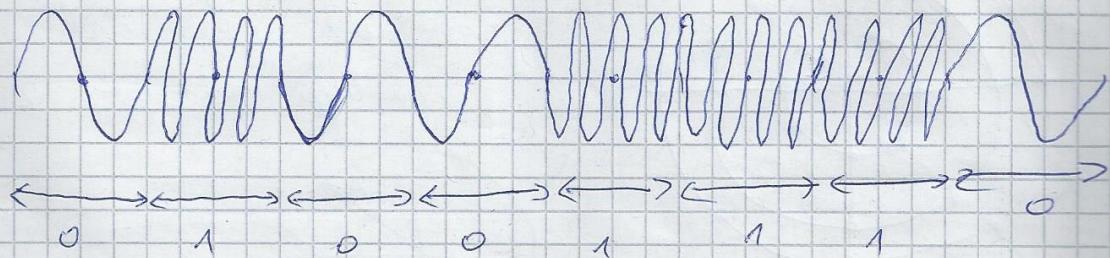
Dá se pak do přenosu množit vše



dobrý

dohodnout skvělý přeskok :)

Navrhnute sig.
frekvenčná mod. sig.
0 1 0 0 1 1 1 0



bit - jednotka info (0, 1)
baud - jednotka modulacie (počet stavov/s)
vyslaný
počet stavov za 1 tick

4 stavy - 1 baud - 8 bitů

modulačná rýchlosť
koľko zmien za tick [baud]

Ethernet 2 zmien na bit
počet v signál / Vmodulacie
1 zmiena = 1 baud

$$V_{\text{prin.}} = V_{\text{mod.}} \log_2(1)$$

2/1

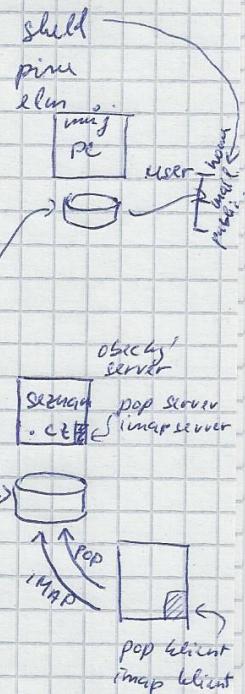
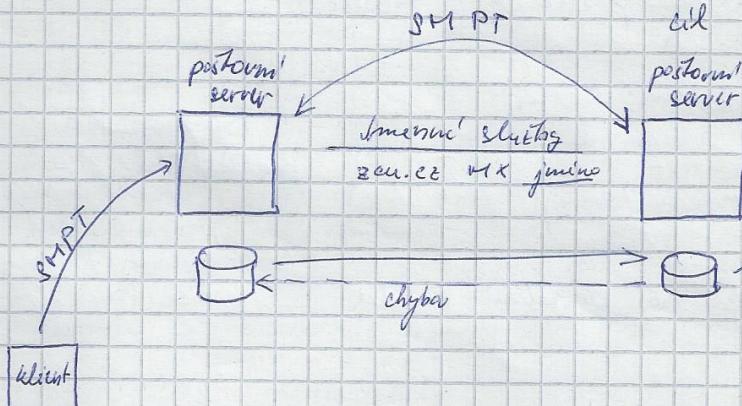
UPS

11. týden

Prednáška

Elektronická Pošta

(systém domácími offline)



SMTP - simple mail transfer protocol

- přenosu mail me post server
- přenos

POP - post office prot.

IMAP - internet message access prot.

} lokální prototypy

POP - user

- password - Pass
- RETR
- LIST
- DELE
- BYE

} přihlašení

} účet

} seznam poskyt

} zpráv (seznam)

} odklizení

IMAP

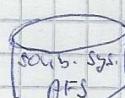
} lokální seznam

} uživatelův seznam

} přihlašení

jméno @ adresa

na zkuš

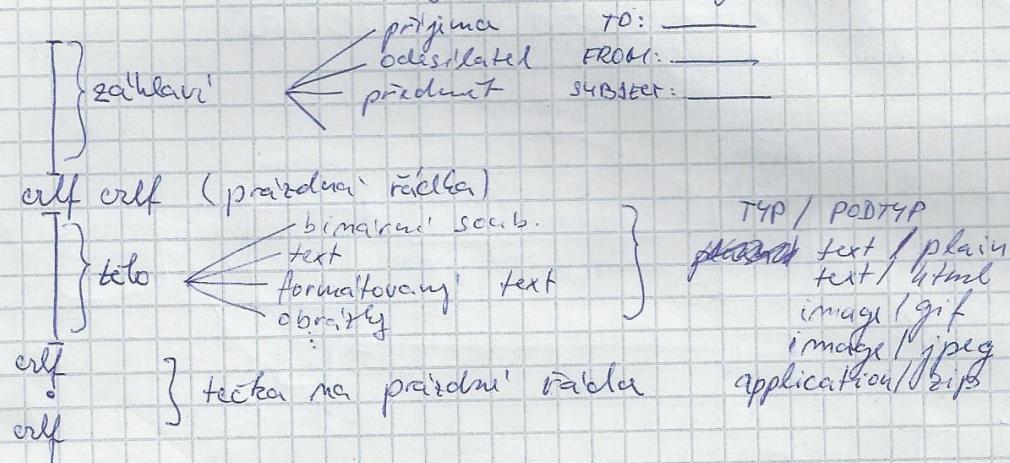


jedno PC užek

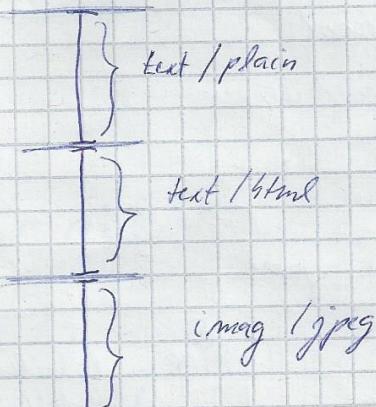
Students. zcu. cz - alias - Mapovací tab.

Students. zcu. cz → uživatel "jméno" poštovní *ejx.zcu.cz*

Struktura zprávy el. pošty



Rozdílení těla zprávy do bloků



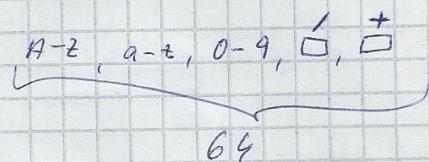
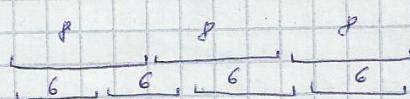
Zobrazí u to, co umí
nařídit zobrazit

To, co nemůže se ukáže
jako příloha

Kódování

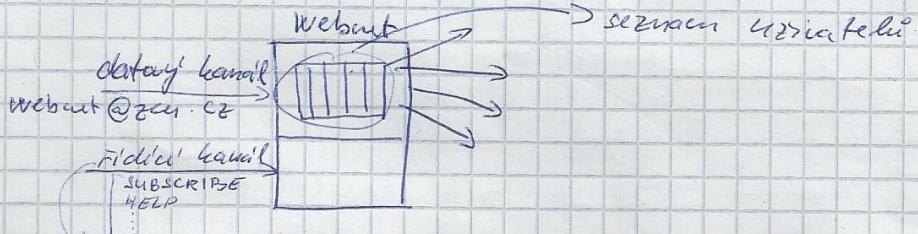
7-bit ASCII

BASE 64 - zakódovanou binární zprávu tak, aby byla prenositelná
v ASCII



Elektronická konference

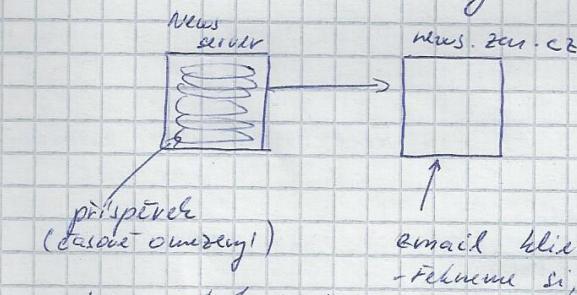
- = list server
- = ~~napřímo~~ zprávy jsou přenášeny jako zprávy el. pošty



el. mail k řídícímu datačnímu kanálu
pošle se zpráva → server odesíle faktel zpráv el. pošty

el. mail server → musí se vygenerovat obsah novostí pošty

News - novinky



příspěvek
(článek omezený)
ve stranu → kde má noviny
email klient (nastavení v konfiguraci) příspěvek
- řídíme si, co chceme → když je nový zpráv
se mi → když ho chci → stáhnout si ho

HTTP, HTML, URL

HTTP - protokol pro přenos web. stránek

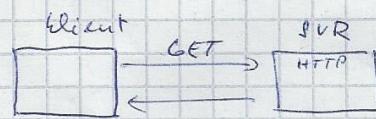
- metody
GET
HEAD
POST

GET - přečtení - URL - web. stránky

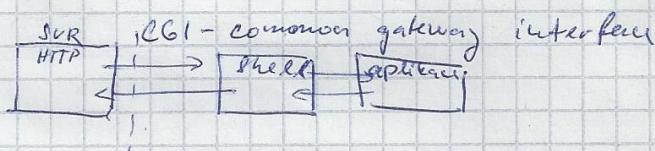
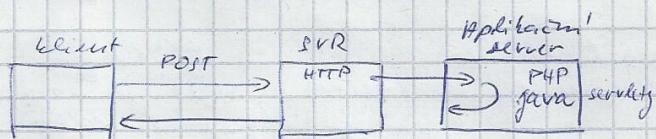
HEAD - mísťem za 'blan' stránky
- sčítání - následný přečtení záhlaví → už ji máme?

POST - odeslání dat na SVR URL + data

zpracování počítače



HTTP SVR - umí zpracovat jin URL



Webové stránky

popisují značkový jazykem (HTML, XHTML)

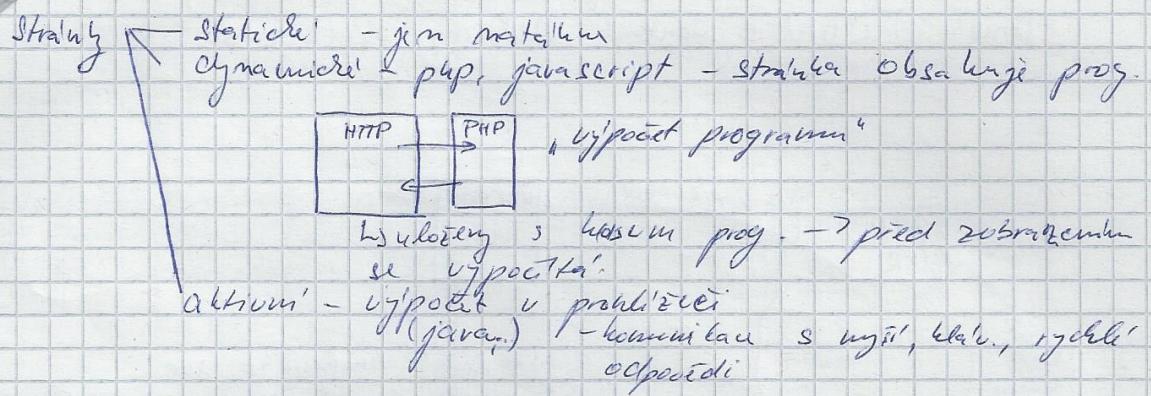
značky ← píšeme <p> . . . </p>
například

formát:

```
<html>
  <head>
    :
    </head>
  <body>
    :
    </body>
</html>
```

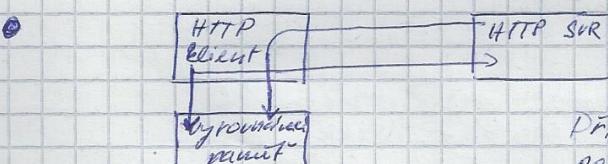
→ typ HTML...

vyrovnávací paměť http transparentní vyrovnávací paměť



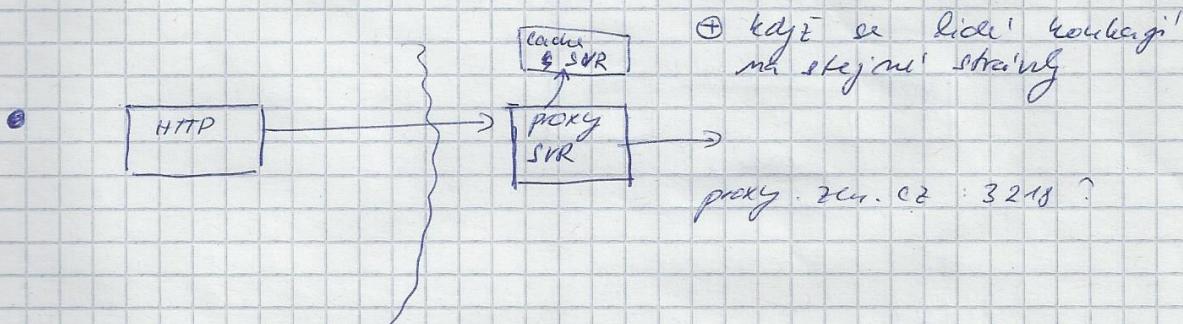
Vyrovnávací paměti

- uvažování procesu zobrazení informací
- snížení zátěže sítě

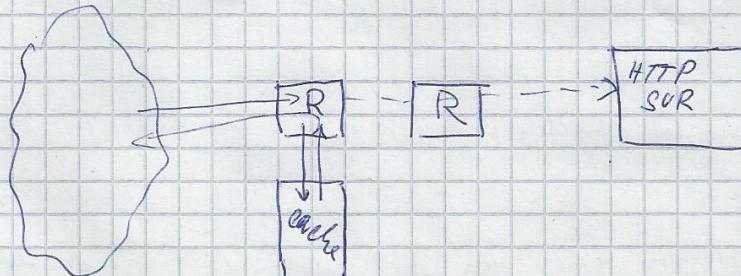


Při něj se klient spojí pořád požadován, zkouší najít se
vyrovnávací pamět

v RAM nebo na disku

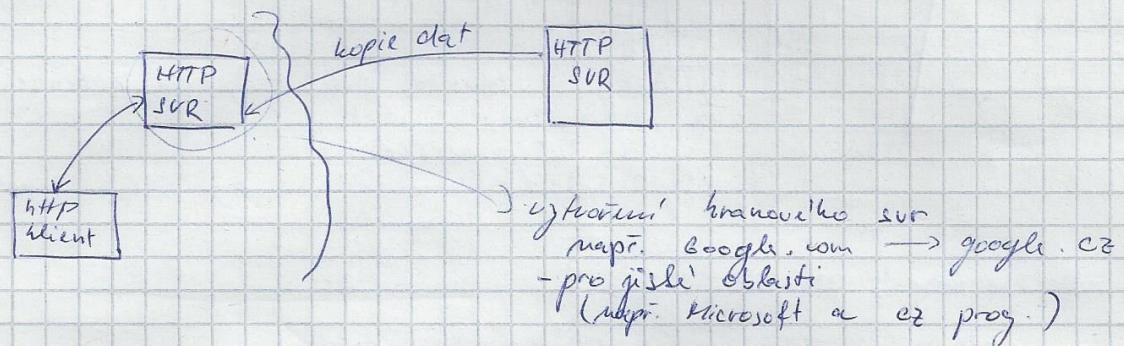


- transparentní vyrovnávací paměť



cdn content delivery networks http cookies url

Dnes: CDN - Content Delivery Networks

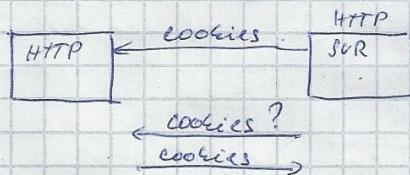


Cookies

= uchovávání stavové informace na místním PC
datový soubor (4KB)
HTTP - bezstavový

pořadové → odpověď (zapsání)

např. můjupní kód, rozšíření knížka



URL

schema: // uživatel:heslo @ stroj : port / cesta-k-souboru /soubor ?param

↓
http

↓
80

není uveden soubor → index.htm
·html
·php

úprava adresár

mailto:// jmeno @ students.zcu.cz

telnet:// stroj

- musí to být na konfigurovaném v prohlížeči

rmi:// [] . stroj
jmeno služby

file:// zobrazení soub. na lok. pc

divov' adresy

- můžu uvidět jenom IUR → doplňuji auto

kaskádové styly - potřeba oddělit obsah a forum

css - nastavím styly

Oznámení o změnách stránky

RSS - Really Simple Syndication

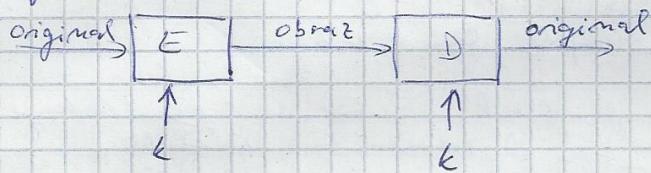
- má IUR je XML, auto se ~~ne~~ stačí
a povídám → změna → indexace

Šifrování a bezpečnost

- = Šifrování original $\xrightarrow{\text{funkce}} \text{obraz}$
- = kryptografický kontrolní součet original $\xrightarrow{\text{funkce}} \text{kont. souč.}$

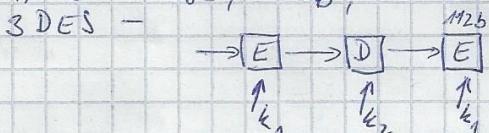
Šifra. $\begin{cases} \text{symetrická} \\ \text{asymetrická} \end{cases}$

Symetrická Šifra



DES - 56 b

AES - 128b, 192b, 256b

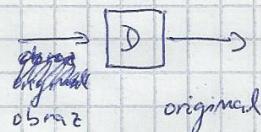


operace = substituce - nahrazení znaků
permutace - prohozují znaky }
opakování - 24, 32 otáček

(opakování když se zvyšuje P prolomitelnost)

prolomitelnost řady

- hromadný kód - zhodnocení všechny možnosti



↓

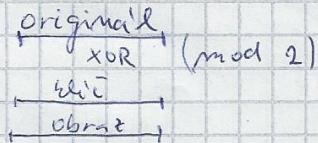
zhodnocení

"Ahoj Pavle!"

- zpravidla počítá se, že odpovídají originalu

neprolomitelnou řadu

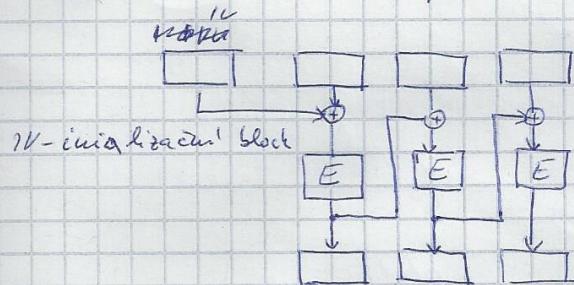
- jednorázový klíč - stejně dlouhý jako original



šifra → bloková - blok první díly → kódované - ECB
 procesová - každý bit je kódován

ECB - Electronic Code Block - $O \rightarrow O$

CBC - Chain Block cipher



Problem: distribuce šifrovacího klíče

Diffie, Hellmann

malé číslo g
 tajné číslo g_x
 velké procesní číslo N

$$g^x \bmod N = X$$

$$X, g, N \rightarrow Y = g^y \bmod N$$

$$K = (Y^x \bmod N) = (X^y \bmod N)$$

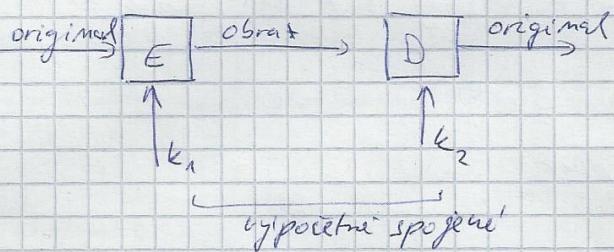
1 strana 2. strana

šifrovací klíč man in the middle



asymetrická šifra RSA šifrování klíč

Asymetrická šifra - různí klíče



RSA

klíče - velká čísla q, p
 $p, q, N = (p-1)(q-1)$... atd.

$$K_p \cdot K_s = C = M^{kp} \pmod{N}$$

\downarrow

public key tajný klíč

$$M = C^{ks} \pmod{N}$$

= šifrování, realizace el. podpisu

$$\hookrightarrow h = H(M)$$

hashovací funkce $\{h\}_{K_s}$
 kontrolní součet zasífravany
 tajným klíčem

$M, h(M), \{h(M)\}_{K_s}$

A $\xrightarrow{M, \{h(M)\}_{K_s}} B$

$$\{h(M)\}_{K_s} \xrightarrow{K_p} h(M)$$

$$M \rightarrow h(M)$$

počít se nevadí, fakt mohou
 dle toho mít stejný klíč

hash zprávy zajišťuje
 souborné privátní a
 klíče

Rozifr. zasífr. zprávy
 využívají klíče

každý už. má 2 klíči
tajný a veř.

A → B
 $\{M\}_{K_p^B}$ (zpráva pro B - zašifrovaná B - publický klíčem)

podpis: $\{h(M)\}_{K_A}$ (mý podpis zašifrovaný mým tajným klíčem)

El. pošta - symetricky zašifrovaná + asym. klíč.

$\{M\}_K$ $\{K\}_{K_p^B} \rightarrow \{K\} \{M\}$

(public má ji všechny, ale nemá ho rozšifrovat pouze teh, kdo má privátní)

$\{M\}, \{h(M)\}_{K_A} \rightarrow \{h(M)\} \{M\}$

PGP - používal RSA (bylo potřebné chránit)

zvolil si 1 klíč, aby generoval si 2.

Certi fi káty

- obsahuje VEREJNÝ KLÍČ
- ID vydavatele
- ID uživatele
- platnost
- ID certifikátu
- použití
podpis

{ inf. { h() } }
K_p
vydavatel
siceva

v pořeji chladisté vydavateli ←
potřebují veřejný klíč → stáhnu se certifikát → kontrolu
musíme mít jeho veřejný klíč →
nakonec si uživatel musí podepsat
svůj certifikát sám

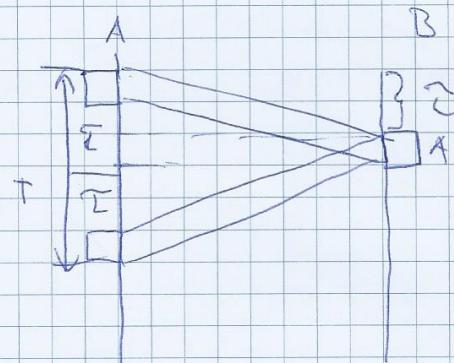
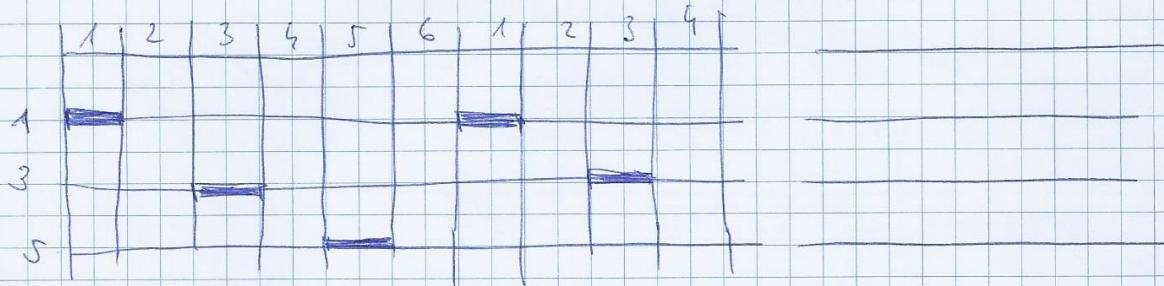
HTTPS ← anonymous přístup jsi ← SVR
anonimní přístup certifikát ← certifikát
všem jistě, že se přihlásíme ke správnému serveru
délky ověření certifikátu, co už poslou
tajný klíč znám jen jsi.

Metody rovnoměrného přístupu

- = predeem neplánuje pořadí vysílání
- = TDMA - časový multiplex
- = metoda s řídoucím okruhem



Korespondenční seminář z programování



$$T = \overbrace{t}^{\text{délka jednoho signálu}} + 2\overbrace{t}^{\text{délka intervalu (obrůstka)}}$$

$$t = \frac{T}{3}$$

$$T = \alpha T + 2T$$

$$T = \frac{2T}{1-\alpha}$$

délka intervalu (obrůstka)

aby stanice odeslala signál
a všechny stanice ho slyšely
v tom samém okamžiku

algoritmus hierarchického přidělení algoritmu sítí s přidáváním pověření

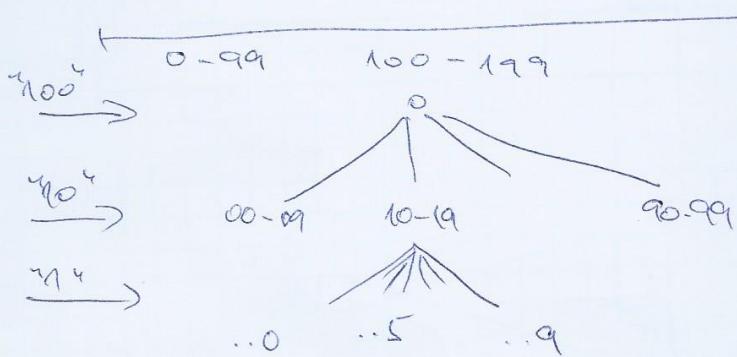
Algoritmus hierarchického přidělení
komunikačního karty

N... číslo stanice 0-999

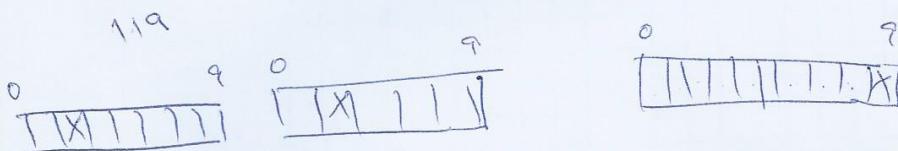
= nejdříve "100"

= pro ujistit "100" poslat "10"

= pro nejistu "10" poslat "1"



$$\begin{array}{r} 10 \\ 100 \\ 1000 \\ \hline 1110 \end{array}$$

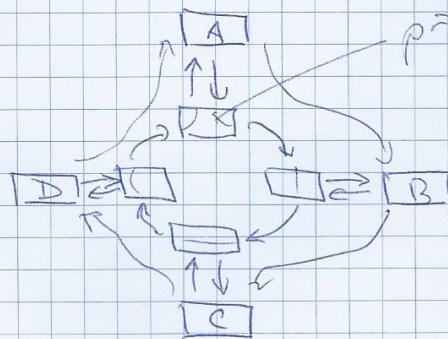


síť s předvolenou pověřením

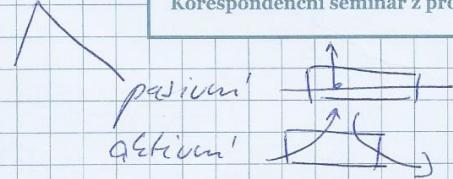
krabové síť s předvolenou pověřením
(TOKEN RING)

sběrnicové síť s předvolenou pověřením
(TOKEN BUS)

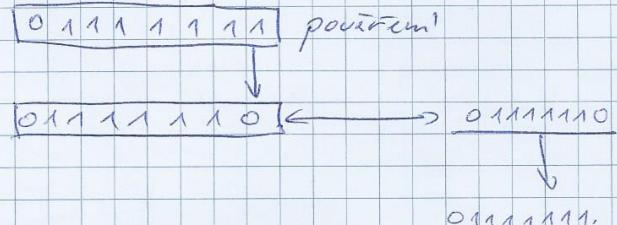
TOKEN RING



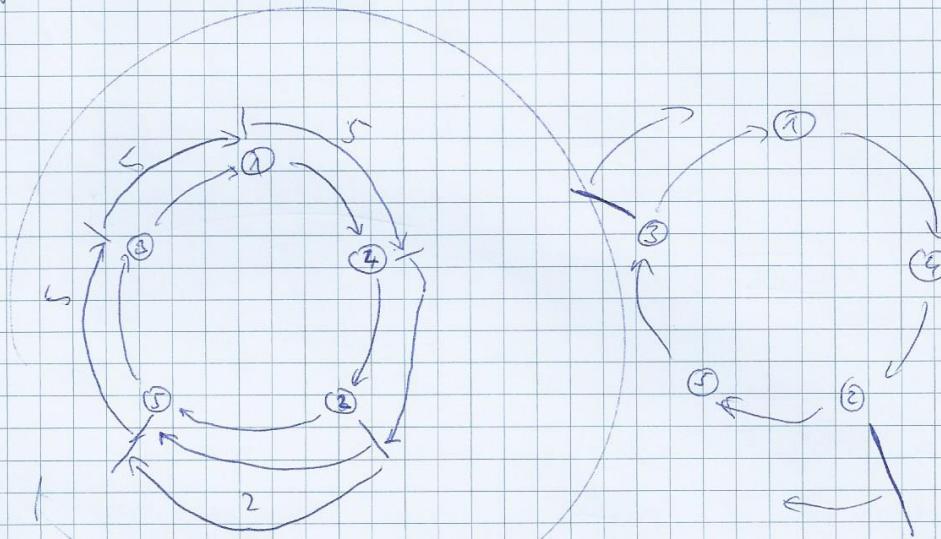
přistupuje uzel A



Korespondenční seminář z programování



Algoritmus obnovy pověření
= výběr $1 \leq N$



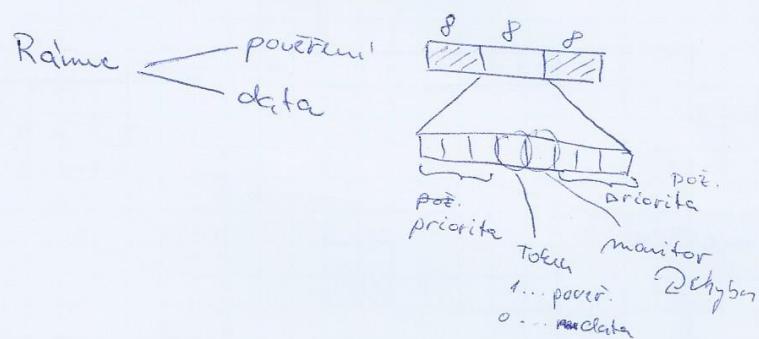
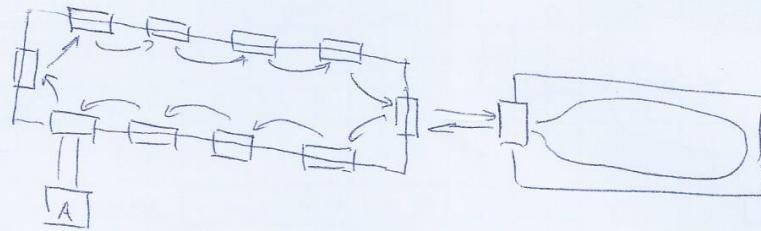
Korespondenční seminář z programování Matematicko-fyzikální fakulty UK

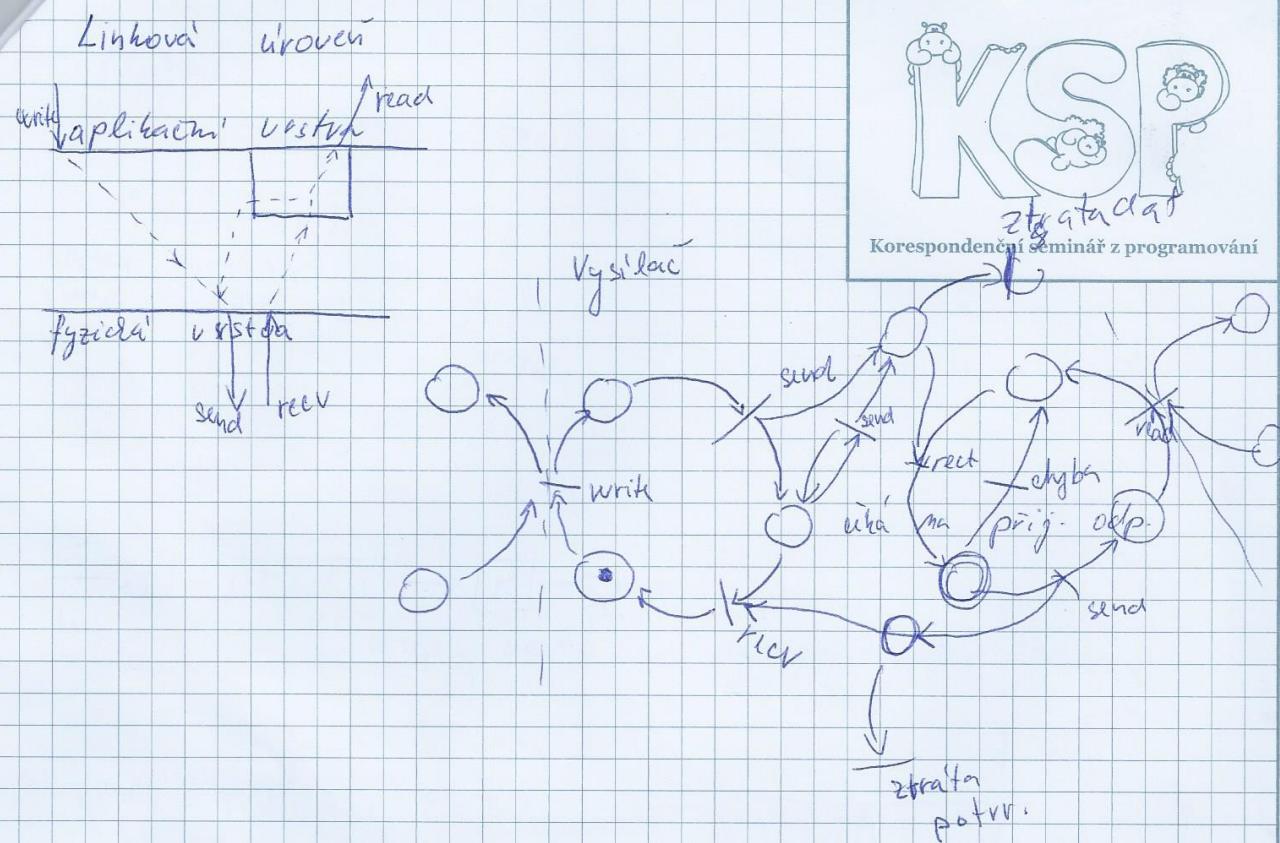
<http://ksp.mff.cuni.cz/>

sít token ring ieee 802.5 ibm rámc

Příklad typu token ring

- IEEE 802.5
- IBM TOKEN RING
- pravostranná rychlosť 4 Mbit/s, 16 Mbit/s
- jidloňka: MDA





Lokální počítačové sítě

- mnohabodové spoje



- přístup k ke komunikační mediu

- ↳ s centralizovaným rozdelením - jednoduchy x správní řízení
- ↳ s decentralizovaným - II - - složitý x řízení - II -
- + s plánovacím alg.

Decentralizovaný řízení

= s náhodným přístupem

= s rovnoměrným přístupem
(z rozvrhovacím)

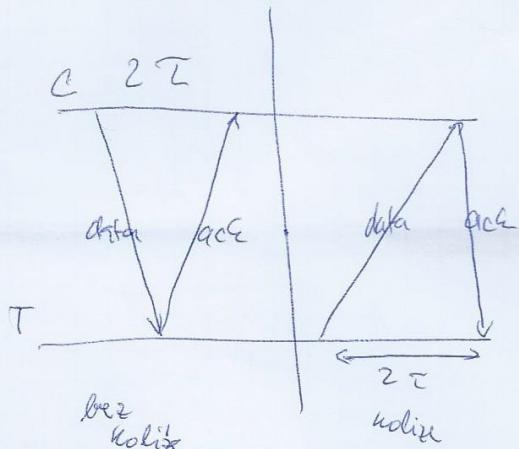
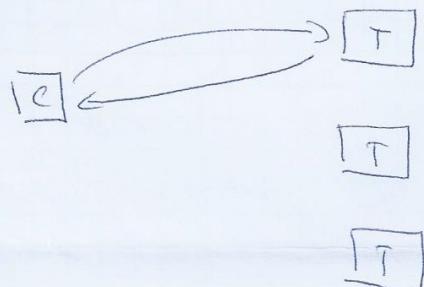
= s pravutím přístupem

1) metody s náhodným přístupem

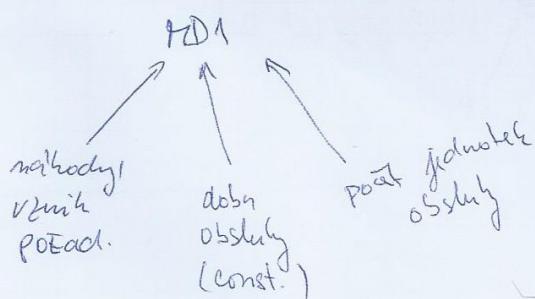
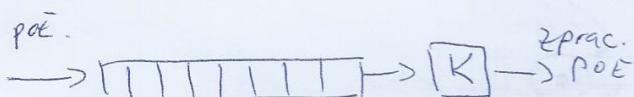
- připojení vznik kolize

= Aloha

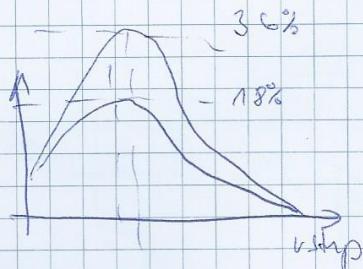
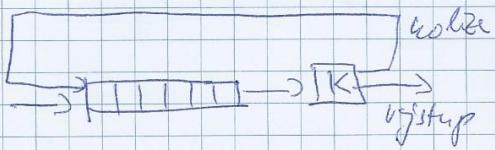
když chceme vysílat
vyšší sílu, kontroly
 pomocí ACK



Model hromadného obsluhy

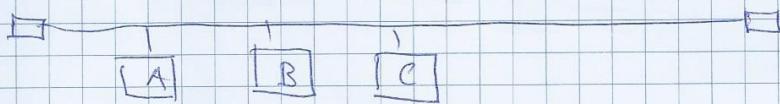


Aloha

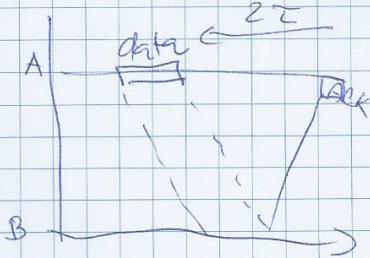


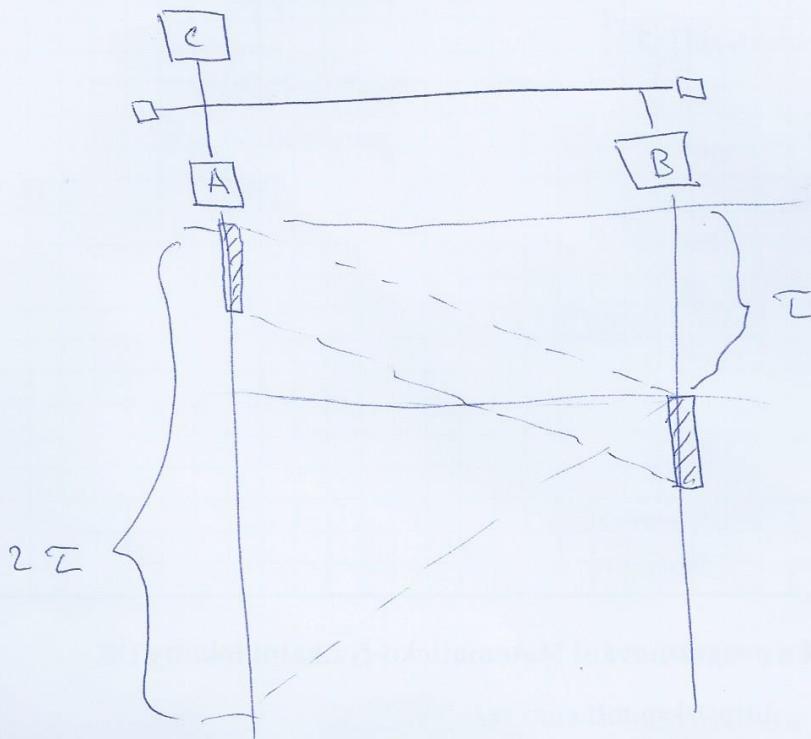
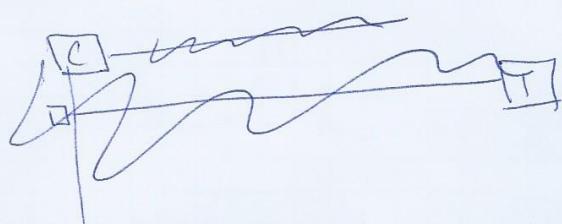
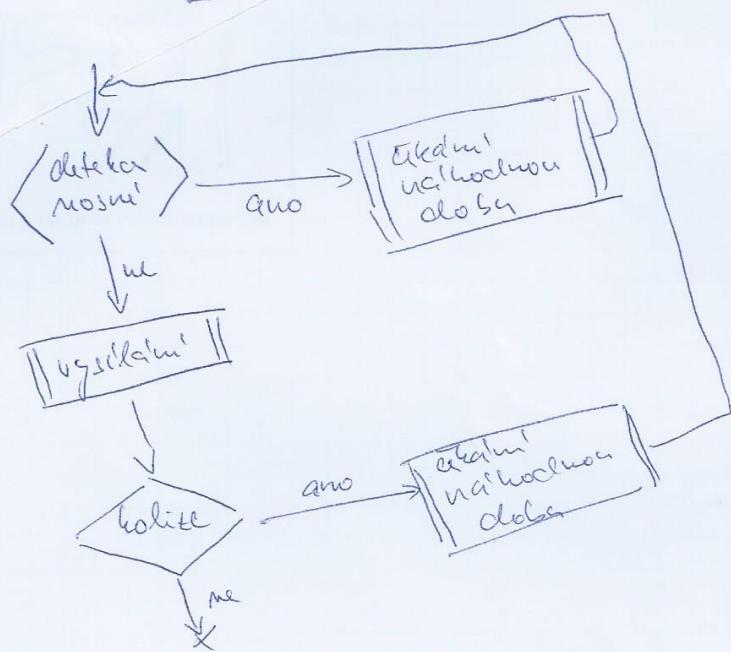
CSMA - carrier sense multiple access

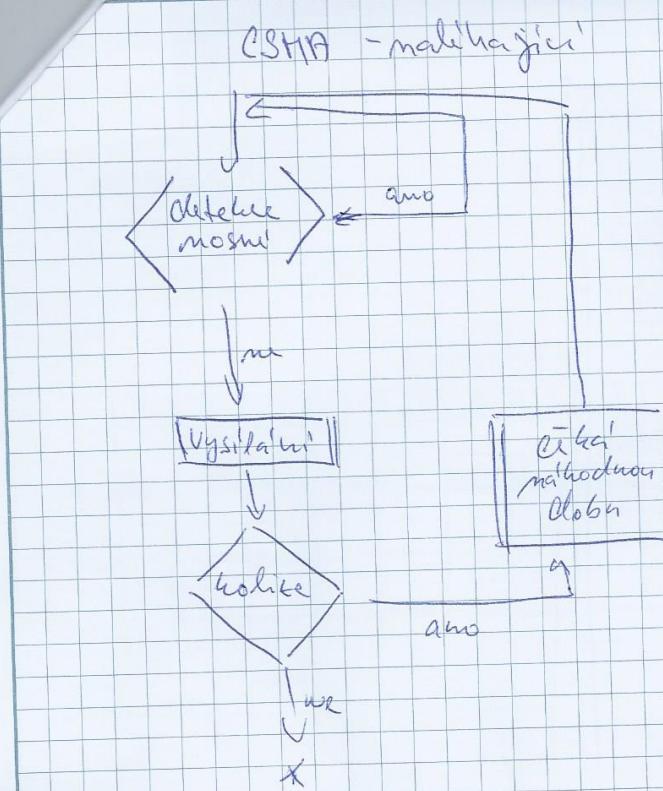
vícenásobný přístup → přenos & detekce náruží



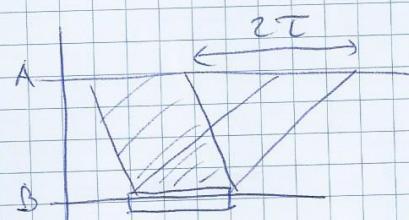
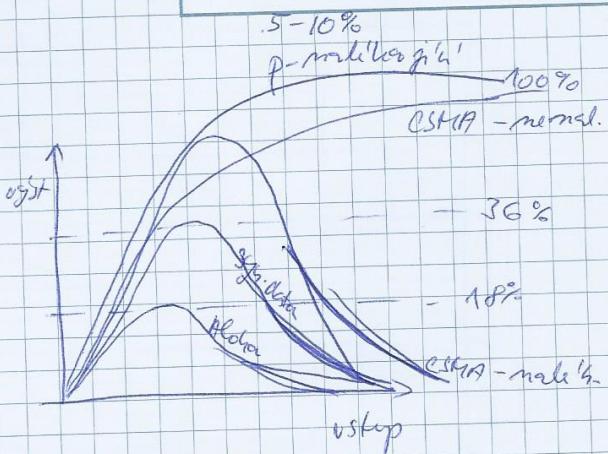
= malým čekáním → vysoká účinnost
čekání → CSMA malým čekáním
ne malým čekáním
p-malým čekáním



CSMA - nenaléhajíci

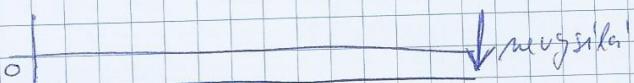


Korespondenční seminář z programování



CSTMA / CD

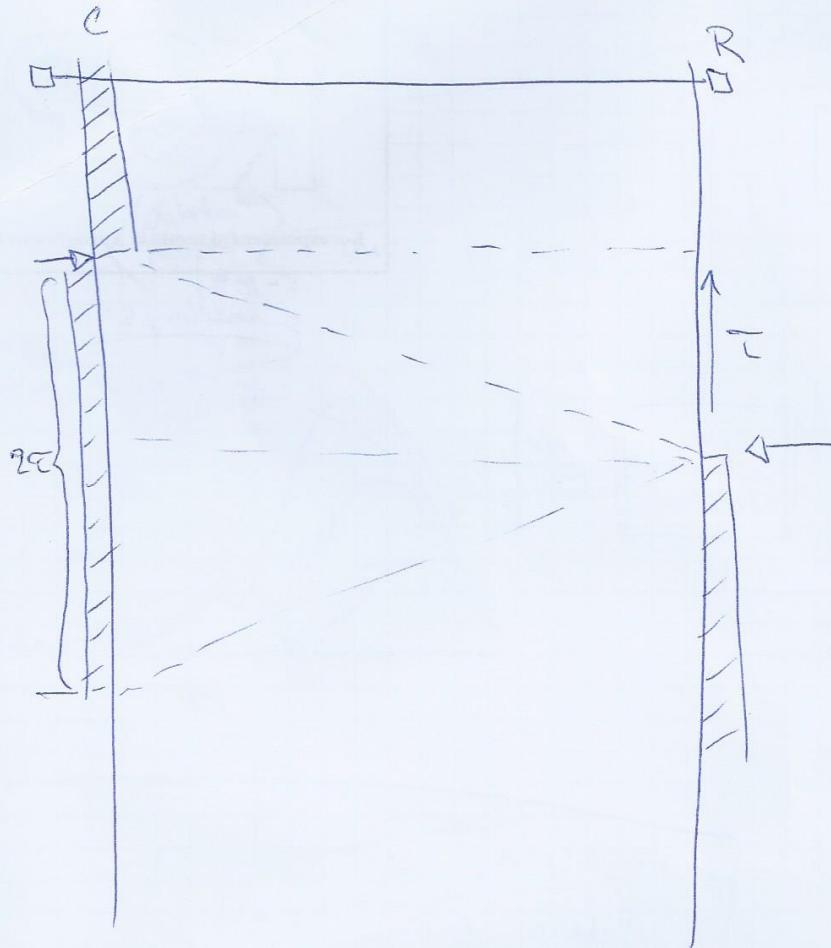
Detectice kolize



SGS - vysílání
A = kolize

Korespondenční seminář z programování Matematicko-fyzikální fakulty UK

<http://ksp.mff.cuni.cz/>



SÍŤ ETHERNET

- CSMA/CD - malé hající
- určení doby opakovaného

1. detekce kolize z rozsahu $2^8 T$

$$T = 2^9 \cdot \frac{1}{f}$$

2

$$4T^2$$

3

$$8T$$

:

$$2^{10} T$$

11

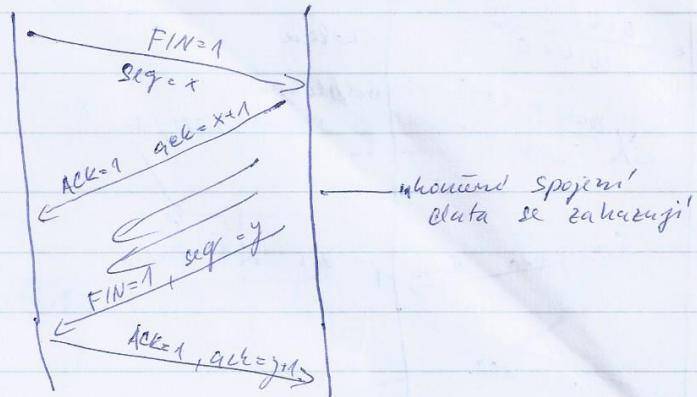
$$2^{11} T$$

16

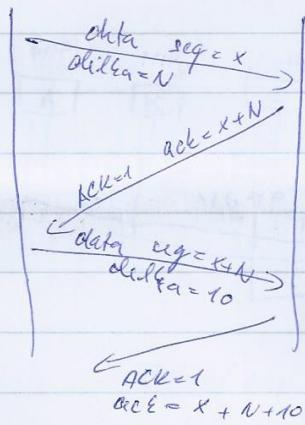
chyba

ukončení spojení přenos řízení toku dat

v koučení spojení



Prenos Oblat

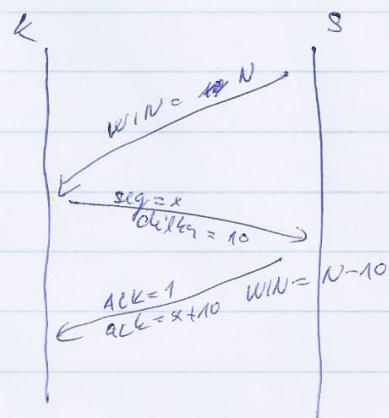


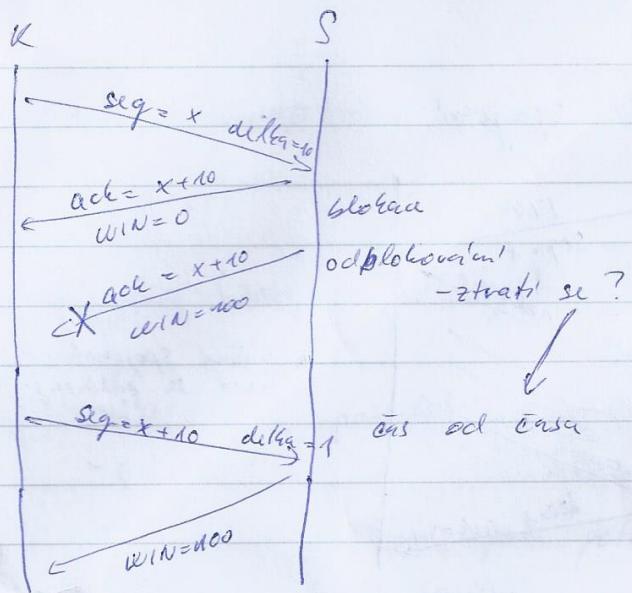
Rízení toku oblata

- okno WIN

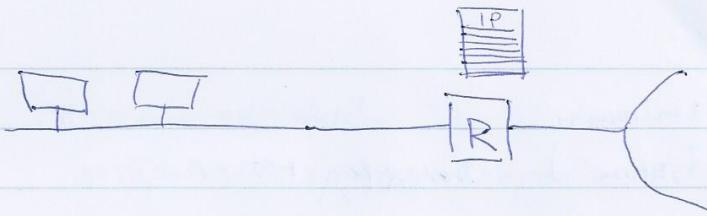
- vyznamenací paket

- kredit





skupiny ip adres igmp

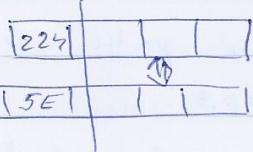


Registration skup. IP adres

Skupinová adresa

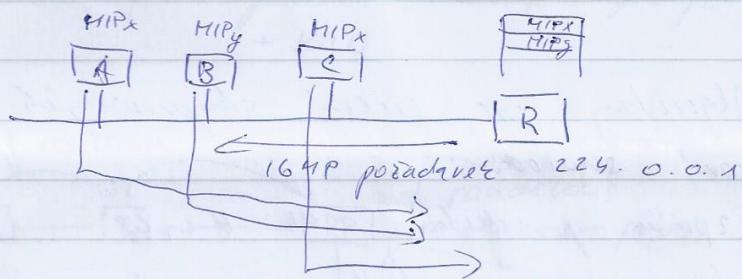
- síťová třída D

- fyzická EII ~~10.90.80.5E~~ | | |



R&a

Protokol IGMP - internet group management protocol



IGMPv1

dotaz/ odp.

IGMPv2

manuč odhlásení

IGMPv3

rozlišení zdroj signálů

skup.	zdroj
MIPx	IPa
OTIPx	IPB

Ch

Skupinové směrování:
 - vnitřní (interní) - DVMRP, MOSPF, PIM
 - venkovní (externí) - BGP

DVMRP - distance vector multicast routing prot.

DVA - směrování podle vektora vzdáleností

MOSPF - multicast OSPF

PIM - Prot. independent Multicast

BGMP - border gateway multicast prot.
 - BGP ← exteriér

Algoritmy pro strom skupinových zpráv
 = záplavové směrování

- zpráva je odeslána do každého toho, ze kterého je zpráva přijata
- Základ v grafu \Rightarrow odstranění sítě
- = vytracení doručovacího stromu
 - zdroj vysíláčem trvá kořen stromu
 - reverse path forwarding

B:

A	A	1
---	---	---

 říká f. 8

C:

A	A	1
---	---	---

 pouští

D:

A	B	2
---	---	---

 obrácení

E:

A	C	2
---	---	---

 :

F:

A	C	2
---	---	---

G:

A	D	3
---	---	---

H:

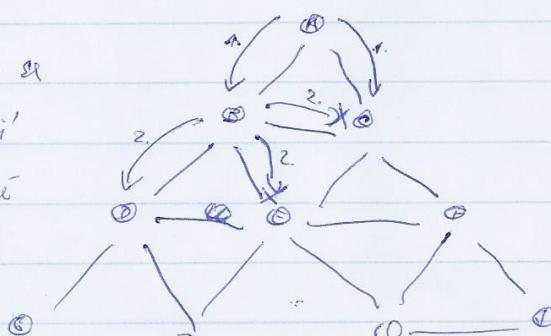
A	D	3
---	---	---

I:

A	F	3
---	---	---

J:

A	F	3
---	---	---



D - zpráva od B

C - zpráva od B, ale mila přijít
od A \Rightarrow záhazovat

PRUNF - odříznuti'

špatná zpráva → zpráva PRUNF ⇒ přidání do blacklista
aby

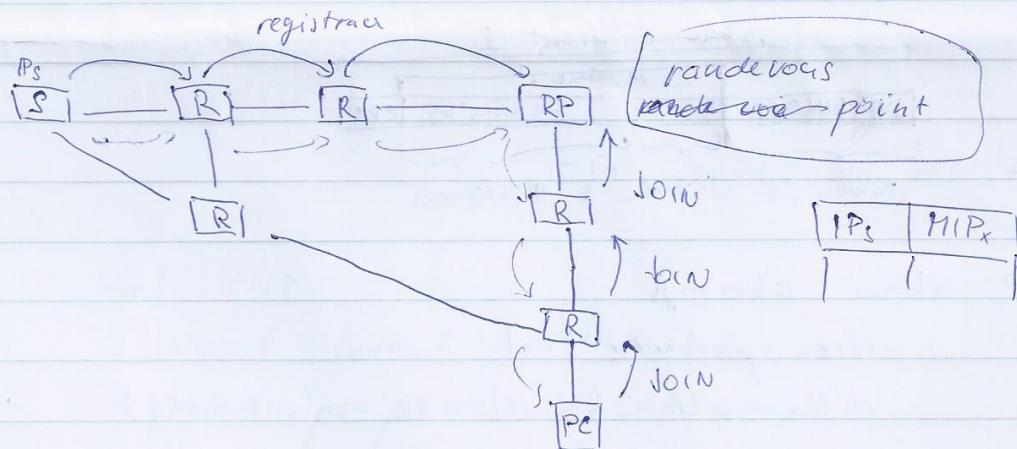
chvílikočko

DVMRP

PIM - protocol independent multicast

Routing - hrdly' - je možné pořídit
zprávy do tří vrstev + PRUNF
malo uživatelů

Fidelity - je možné o zprávách požádat
+ JOIN



Problemy

- přidilování s kroupinových adres

- cesta skupinových adres je rozdílná

- jde o 2 metody vybrat, z ASN - autonomous system number

233. X. Y. 0

147.228.0.0

CESNET

1 adresa

další problem:

určení dosahu sítění skup. zprávy

definice doby života

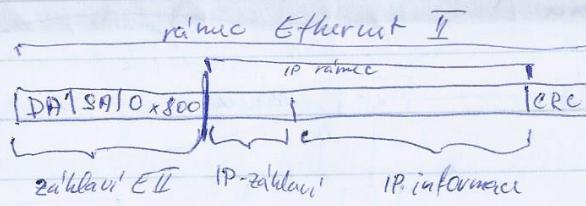
určení dosahu podle MCAST adresy

určení kam až se má vracet

Protocol IP - Internet protocol

síťová vrstva - zakladní datova jidlo - packet

IPv4
IPv6

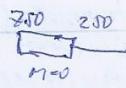
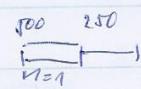
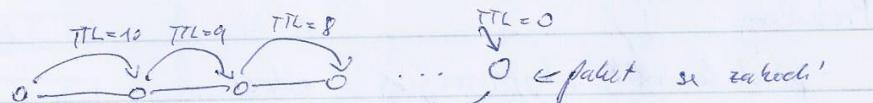


- IP - zakladní obsahuje

- verze protokolu (v4)

- délka zakladní (5-15) \times 4B = (20B ÷ 60B)

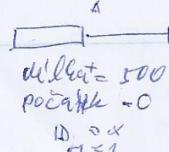
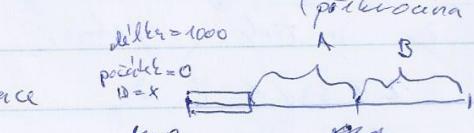
- TTL - time to live - počet povolených přeskočů



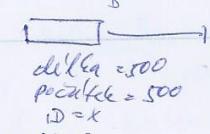
- fragmentation

rozložení v zakladání

TIMEOUT - když nedorazí
celá \rightarrow zakladání je



TCP/IP zpráva (řídce, 1)
(překročená doba života)



icmp protocol protokol

- vodíčka parametry

zpráva - struktura směrování - předem známé cesta

X — A — B — Y

A | B

zařízení

číslo portu uživitele

cílová cesta

- volná směrování

X — A — B — Y

C

může jít přes několik cest

T C

lze cestu

- zařízení cesta - do zařízení se vydává
směrování (max 9 byte)

- zařízení časové zálohy

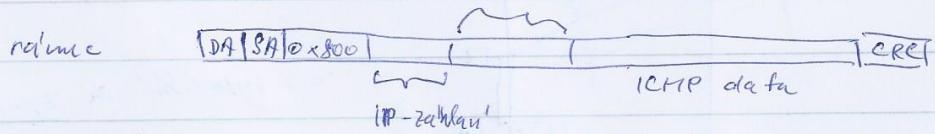
- jak to produktovi přes užly

Protocol ICMP

Internet Control Message Protocol

- protokol pro přenos obecných zpráv

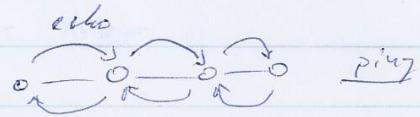
ICMP zařízení



ICMP je nesen IP prot. → jeden typ směrování
když dojde k chybě, tak se nesmí hledat

Typy řídících zpráv

- echo request



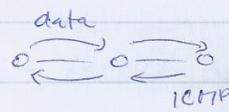
- echo reply

- = dosažitelnost

 - uživ.

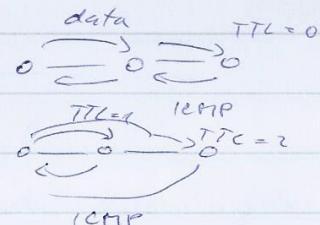
 - síť

 - služby



- = výkonného určení TTL

 - trace route

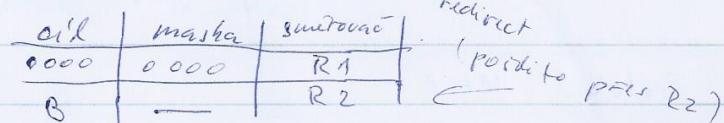
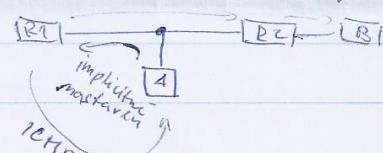


 - data dorazí - port > 2000

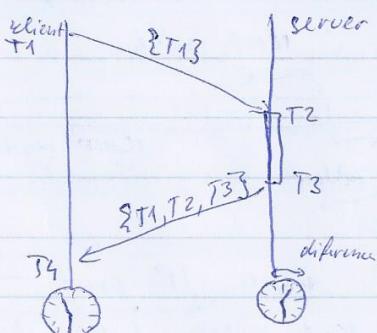
 - nesenzitivní

- redirect

 - redirect



- = synchronizace času

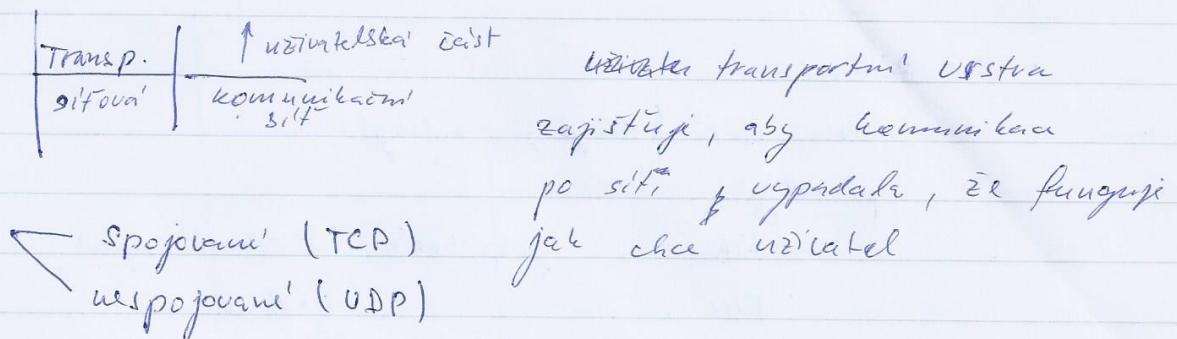


 - \Rightarrow hypotéza se zpředstaví

 - přenosu a o časovou diferenci

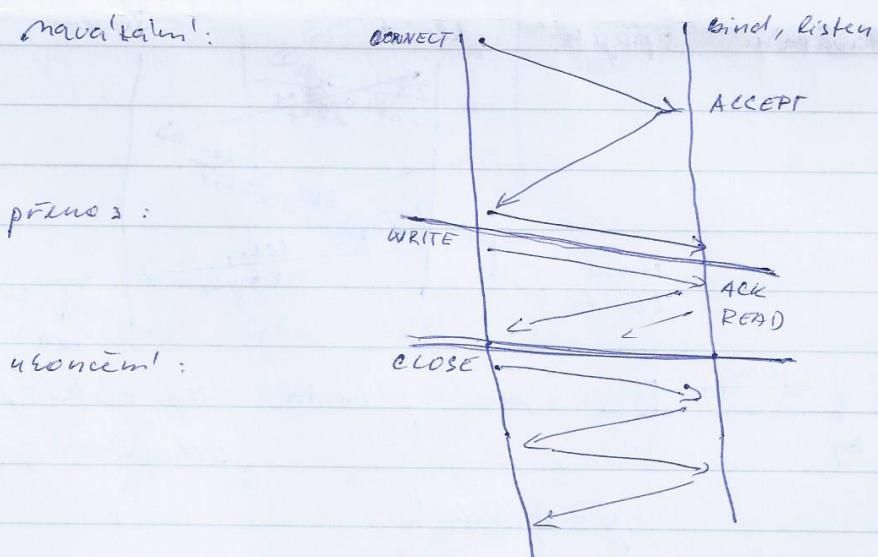
předpoklad: doba přenosu $K \rightarrow S$ = d.p. $S \rightarrow K$

Transportní úroveň



TCP - transport control Protocol

navazání spojení
prenos dat
ukončení spojení



navázání spojení

- TCP záhlaví

- čísla portů (zdrojový, cílový)

- přenosy

- SYN ... požadavek navázání spojení

- FIN ... ukončení

- ACK ... platnost pole potvrzení dat

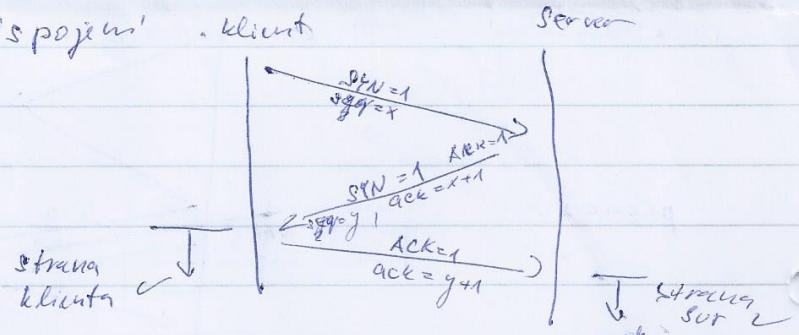
- RST ... reset spojení

- URG ... urgentní data (ETRIC)

- na straně příjemce producent spracování

- PSH ... okamžité spracování přijatých dat

navázání spojení - klient



x, y - m'hoodací
mali' příjemka - seq. čísla pro
ochranu spojení

$x, y - m'hoodací$

