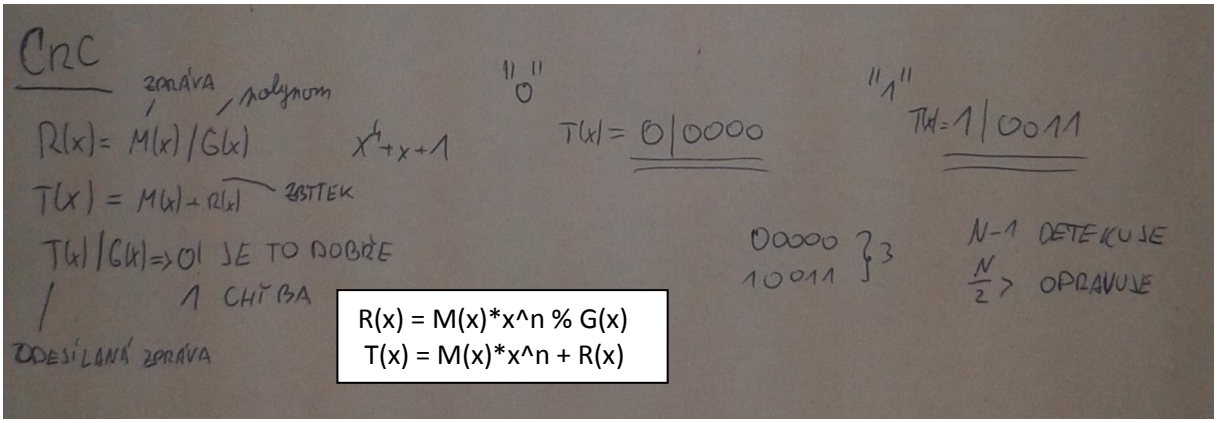
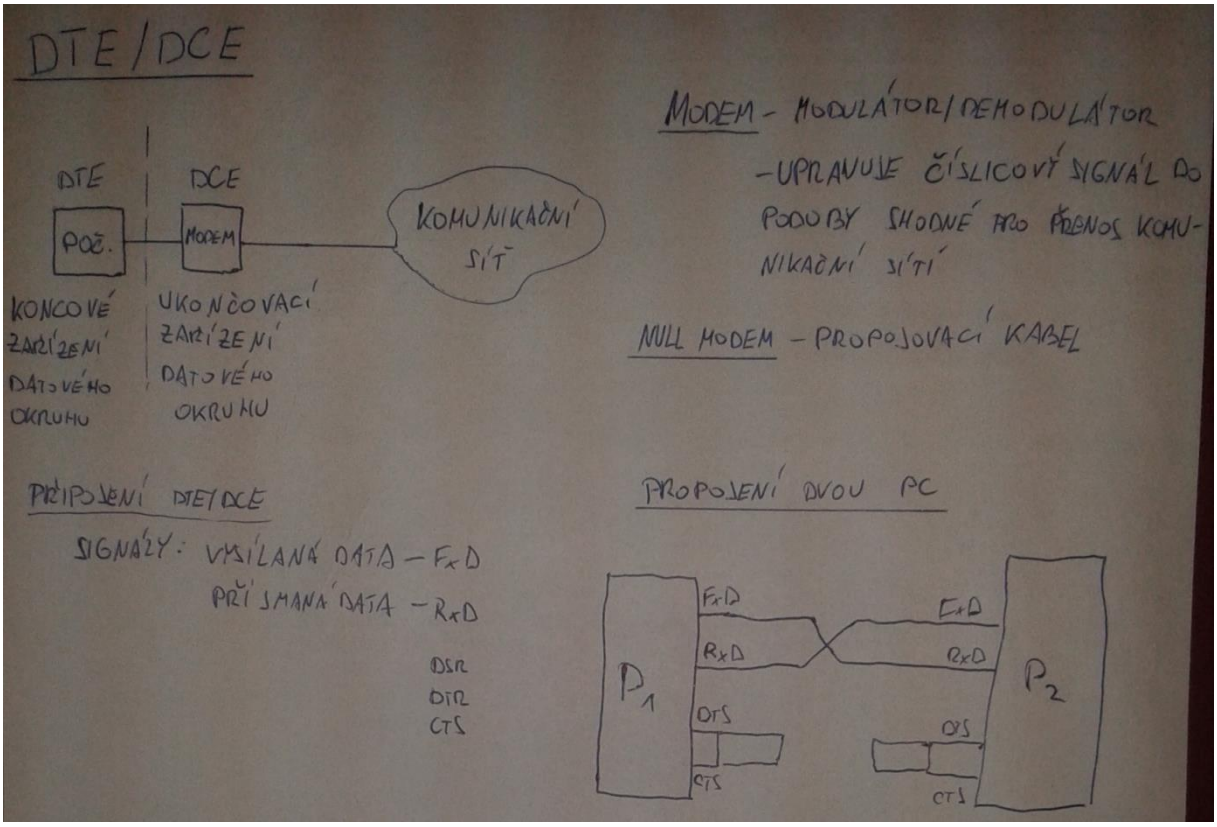
1. Spočíst CRC pro: zpráva "0" a zpráva "1", polynom x4+x+1. Uvést obecné vzorce.



2. Zařízení DTE a DCE, jak propojí dvě zařízení DTE. Null modem.



3. Co je to OPAKOVAČ, HUB, MOST, SMĚROVAČ, BRÁNÁ.

OPAKOVAČ - Opakovač je obousměrný číslicový zesilovač. Používáme jej pouze jako prostředek pro zvětšení vzdálenosti, jíž jsme schopni lokální síti obsáhnout. Nejedná se tedy v pravém smyslu slova o propojení dvou různých lokálních sítí, ale o tvorbu jedné větší lokální sítě z menších částí. Další možnou funkcí opakovače je propojení dvou částí lokální sítě, pracující s různými kabely.

HUB - je aktivní prvek počítačové sítě, který umožňuje její větvení. Chová se jako opakovač. To znamená, že veškerá data, která přijdou na jeden z portů (zásuvek), zkopíruje na všechny ostatní porty, bez ohledu na to, kterému portu (počítači a IP adrese) data náleží. To má za následek, že všechny počítače v síti „vidí“ všechna síťová data a u větších sítí to znamená zbytečné přetěžování těch segmentů, kterým data ve skutečnosti nejsou určena.

MOST – spojuje dvě části sítě na druhé (linkové) vrstvě referenčního modelu ISO/OSI. Most je pro protokoly vyšších vrstev transparentní (neviditelný), odděluje provoz různých segmentů sítě a tím zmenšuje i zatížení sítě. Most odděluje provoz dvou segmentů sítě tak, že si ve své paměti RAM sám sestaví tabulku MAC (fyzických) adres a portů, za kterými se dané adresy nacházejí. Leží-li příjemce ve stejném segmentu jako odesílatel, most rámce do jiných částí sítě neodešle. V opačném případě je odešle do příslušného segmentu v nezměněném stavu.

PŘEPÍNAČ - je aktivní síťový prvek, propojující jednotlivé prvky sítě. Switch obsahuje větší či menší množství portů (až několik stovek), na něž se připojují síťová zařízení nebo části sítě. Na rozdíl od HUBu neposílá přijatá data na všechny porty, ale pouze na ty, kterým data patří.

SMĚROVAČ - je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli. Routování probíhá na třetí vrstvě referenčního modelu ISO/OSI (síťová vrstva). Netechnicky řečeno, router spojuje dvě sítě a přenáší mezi nimi data. Router se podstatně liší od switche (přepínače), který spojuje počítače v místní síti. Rozdílné funkce routerů a switchů si lze představit jako switche coby silnice spojující všechna města ve státě a routery coby hraniční přechody spojující různé země.

BRÁNÁ - je obvykle kombinací softwaru a hardwaru, který propojuje dvě různé sítě pracující pod různými protokoly. Brány pracují zpravidla na síťové vrstvě nebo ještě výše. Některé brány kromě vlastního přenosu dat z jedné sítě do jiné zabezpečují současně s přenosem také převod do jiného protokolu; takovýmto branám se říká aplikační brány. Někdy se pojem brána používá i v situacích, kdy se neprovádí žádný převod mezi protokoly, ale kdy se data pouze přenesou z jedné sítě do jiné. Takovouto bránu tvoří software a hardware, který propojuje dvě různé sítě.

4. Vysvětlit syndrom hloupého okénka

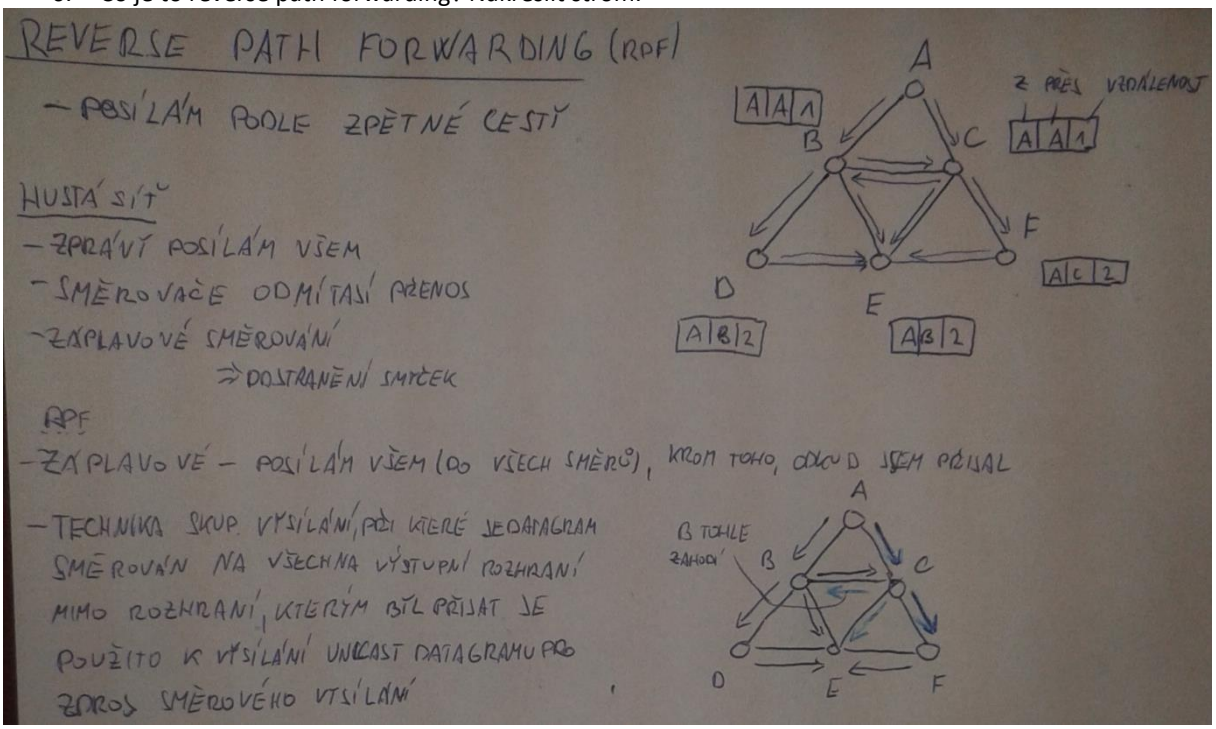
Při výměně segmentů nestejné velikosti může dojit k syndromu hloupého okna způsobeného odesilatelem, či příjemcem. V případě odesilatele tento problém nastává tehdy, když posílá male segmenty dat, i když je možno počkat a následně odeslat větší objem dat v jednom segmentu. U příjemce syndrom hloupého okna nastává v případech, když v potvrzovacích segmentech ohlašuje male velikosti svého dostupného okna, i když by bylo možno počkat a ohlásit větší velikost. Samotné zpožděné doručovaní potvrzování a Naglův algoritmus tomuto problému přímo nezabráni, ale specifikace protokolu TCP obsahuje posloupnost kroků, jak řešit odesílaní dat a potvrzení tak, aby problému s „hloupým oknem“ nedocházelo. Zasílaní krátkých segmentů dat vede k velmi neefektivnímu využití přenosového pásma, kde se navíc velká část spotřebuje pouze na režii samotného protokolu.

5. Co jsou sítě Personal Space Communication IEEE 802.15.8
Napojení na 3G sítě.

Hlavní vlastnosti:
čisté řešení, není třeba kombinované řešení
dynamické školování velkého rozsahu (100Kb/s až 50Mb/s, dosah do 30m)
rychlá synchronizace a připojování (rychlé vyhledávání sousedů a odpojování)
asymetrické připojení

PSC aplikace:
přizpůsobení pro smartphone (lokalizační služby, načítaní dat přístupových bodů, …)
bezdrátová interakce se všemi zařízeními v osobním prostoru (zvuk/video, Voip, web camera, ...)
zajišťuje pomalou i rychlou komunikaci (ovládání a řízení + prohlížení videa

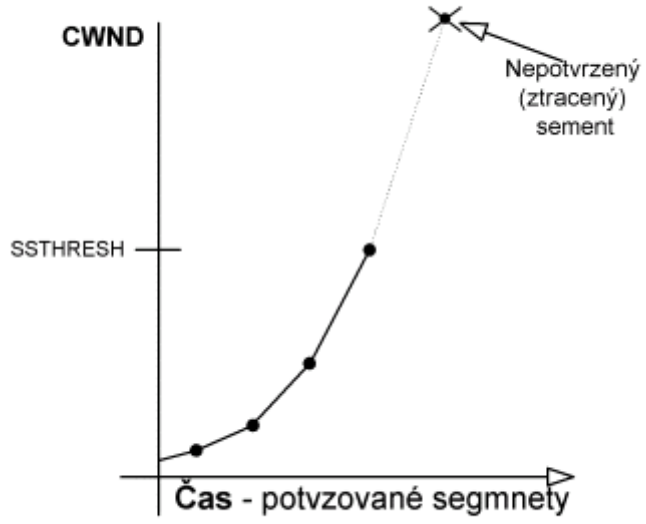
6. Co je to reverse path forwarding? Nakreslit strom.



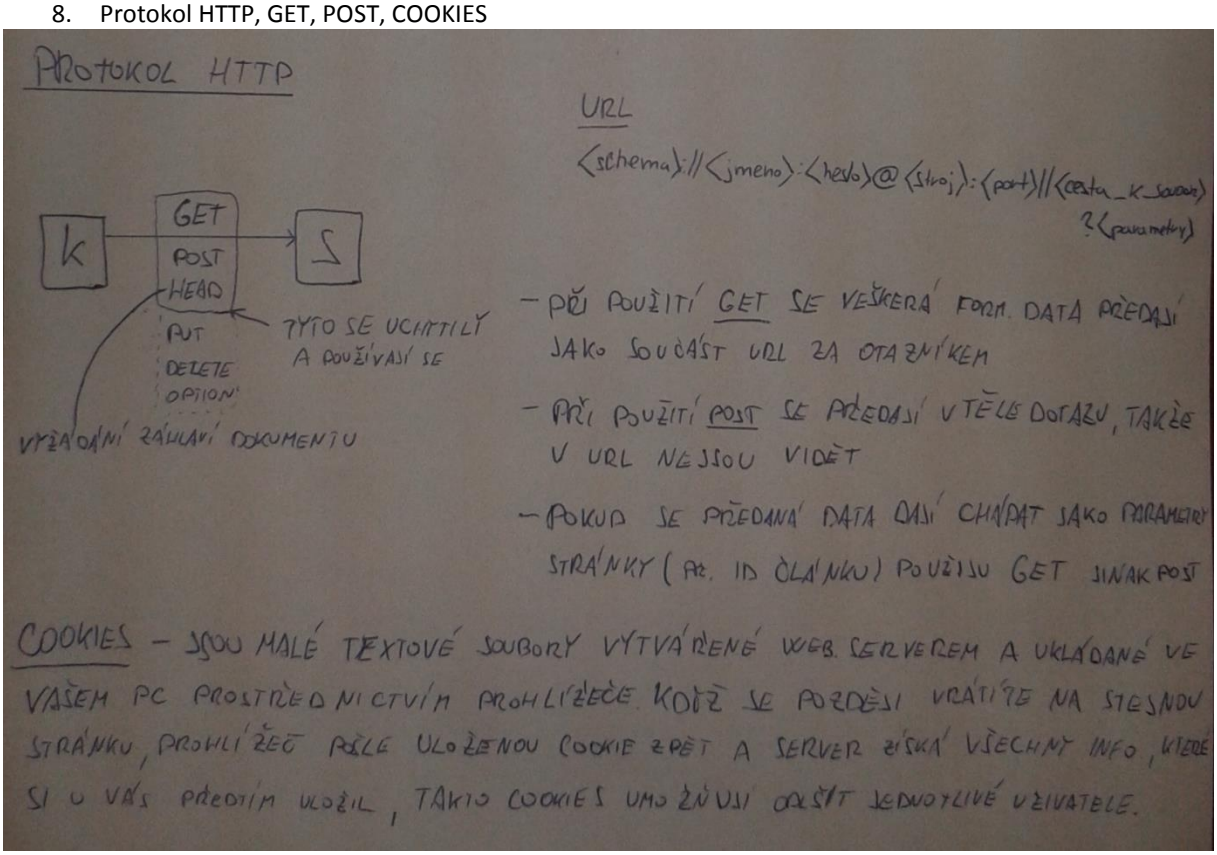
7. Pomalý start

- při zřizování nového TCP spojení možnost skokového nárůstu zátěže, zahlcení sítě a zneprůchodnění všech (i již navázaných) spojení.
- principem je přizpůsobení rychlosti vysílání segmentů do sítě rychlosti přicházejících ACK
- používá se jen pro spojení mimo LAN

Vysílač upravuje šířku vysílacího okna (CWND,"Congestion Window"), ta se udržuje v bajtech.
Také udržuje hodnotu SSTHRESH, což je hodnota velikosti CWND, od které již začíná hrozit zahlcení.
Cílem je udržovat CWND blízko nad hodnotou SSTHRESH, kde však ještě nedochází k zahlcení.

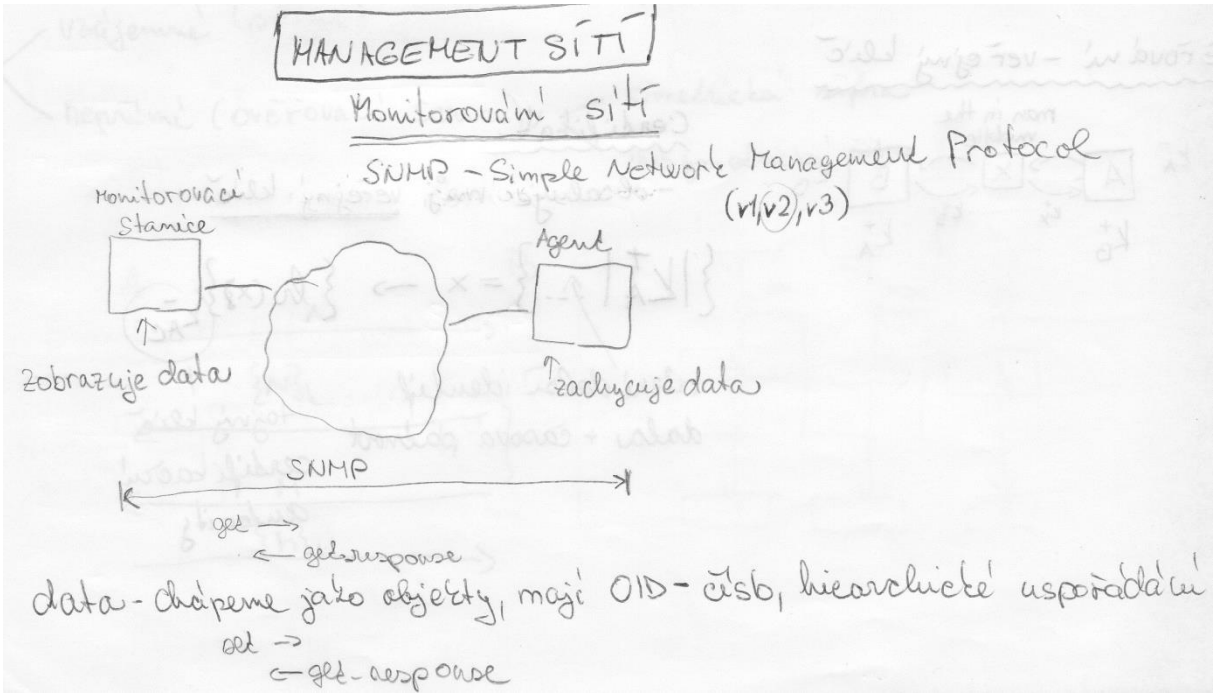


8. Protokol HTTP, GET, POST, COOKIES



9. Co je to SNMP? Jaký je rozdíl mezi jednoduchými objekty a sloupci tabulky

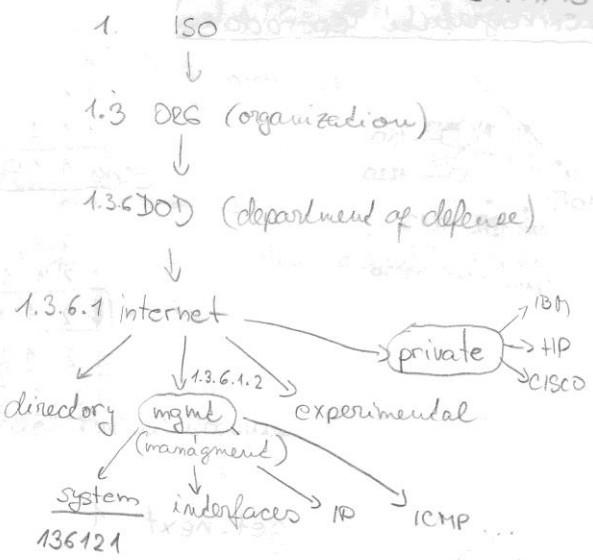
Je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě. Má tři verze: druhá obsahuje navíc autentizaci a třetí šifrování. Nejvíce zařízení podporuje druhou verzi.



29.11.13

ISO
CCITT/ITU } strom identifikátorů

- pro managment slouží ISO



Protokol

get - čtení hodnoty

set - zápis hodnoty

get_response - odpověď

get_next

trap - asynchronní zpráva

PŘ.

get 1.3.6.1.2.1.1.0 (jméno systému)

get_response 1.3.6.1.2.1.1.0 | router uc401
OID hodnota

identifikátor objektu - instance OID
OID OID.0

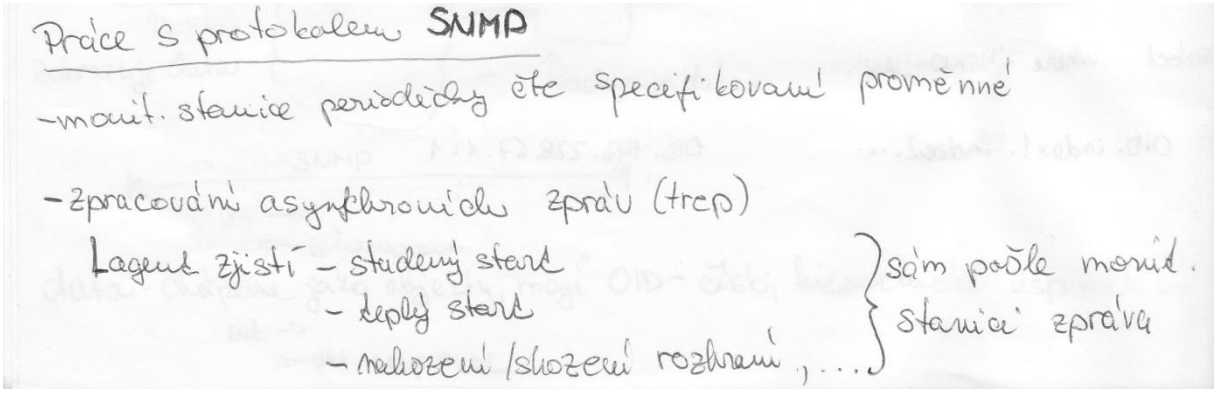
Práce s tabulkami

ARP tabulka

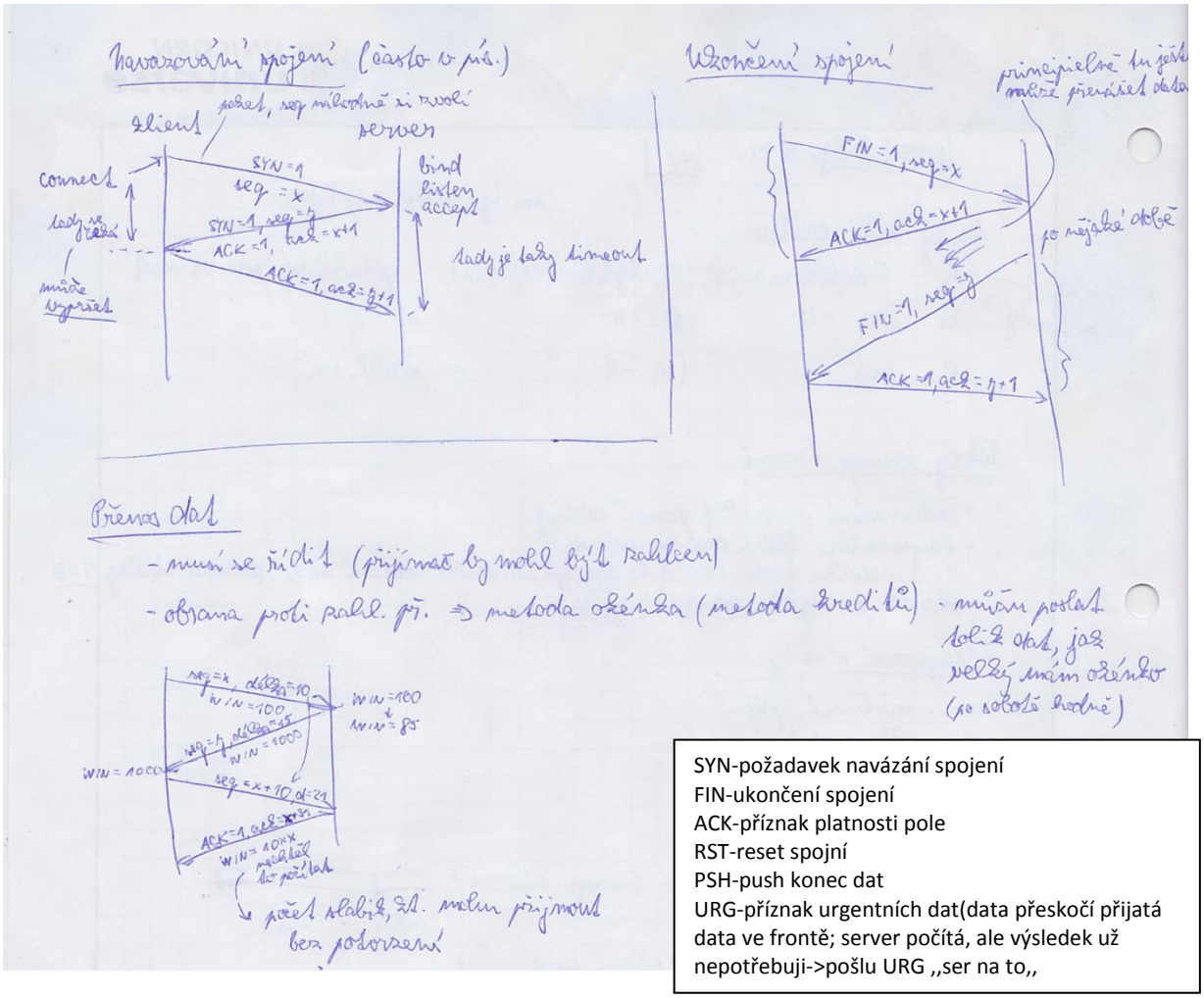
fyzická adr.	síťová adr.	interface
CO:AB:CD:01:02:03	147.228.67.1	1

SQL: select... where JMENO='JAN'...

SNMP: OID.index1.index2.... OID.147.228.67.1.1



10. TCP navázání spojení, ukončení spojení, přenos dat, nakreslit komunikace. Co jsou to urgentní data, kde se používají a jak se přenáší? Jak se řeší v TCP data přicházející z klávesnice a myši.



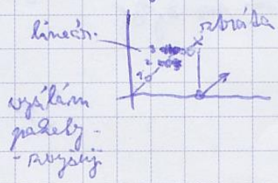
SYN-požadavek navázání spojení
FIN-ukončení spojení
ACK-příznak platnosti pole
RST-reset spojní
PSH-push konec dat
URG-příznak urgentních dat(data přeskočí přijatá data ve frontě; server počítá, ale výsledek už nepotřebuji->pošlu URG ,,ser na to,,

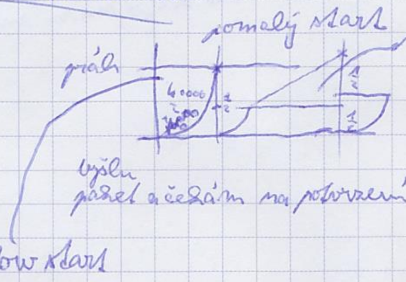
Nejdřív pošleš jednu klávesu, s nějakým bitem, který zajistí, aby tam nebyla taková režie a než ti dojde potvrzení o doručení, tak se naplní buffer se zbývajícími klávesy a ty se pak pošlou v jedné zprávě.

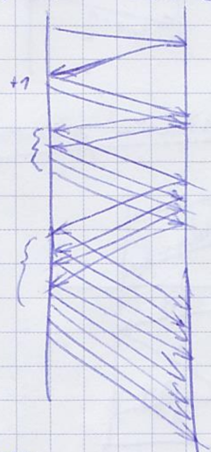
Ochrana proti zahlcení

- explicitní – přenáší se příznaky o zahlcení sítě
  (každý směrovač má fronty a jestliže dojde k zahl. fronty – požadavky zahodí)
- implicitní metody – provádí se testování průchodnosti sítě
  – detekce zahlcení = ztráta paketu

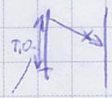
metody určení zatížení sítě





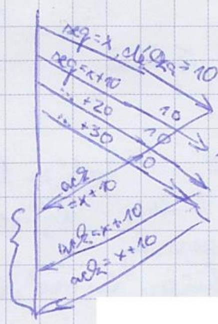


detekce zahlcení sítě

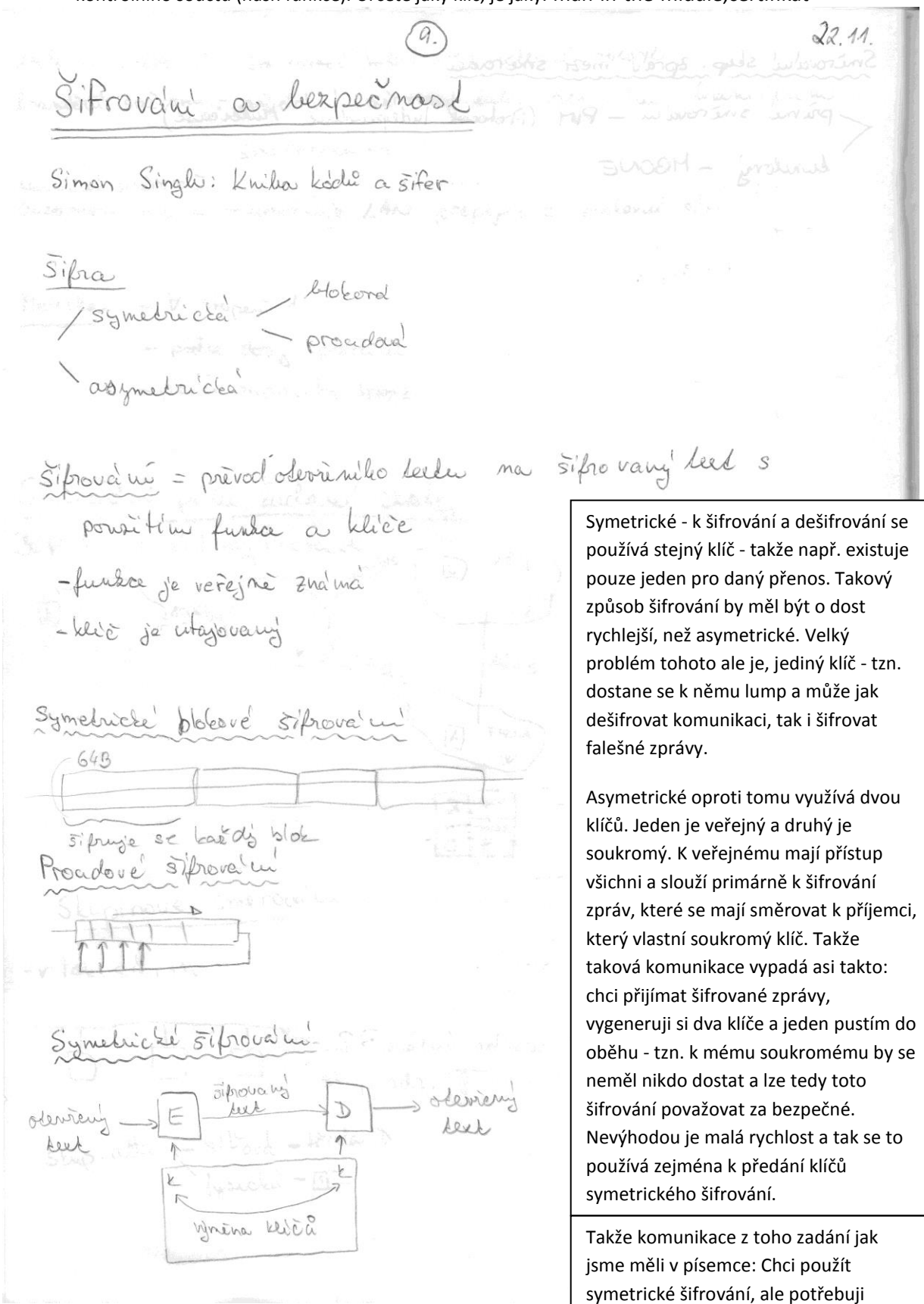


- T.O. (timeout) prechodu ACK
- duplicitní potvrzení

k abych si z toho odnesli:
→ běží po 2 úrovních
- řízení mezi 2 stanicemi
- řízení množství dat přenášených sítí (zahlcení)



11. Chceme poslat zprávu prostřednictvím symetrického šifrování a ověřit nepopiratelnost zprávy. Popište, jak bude vypadat komunikace s využitím symetrického, asymetrického šifrování a kryptografického kontrolního součtu (hash funkce). Určete jaký klíč, je jaký. man-in-the-middle,certifikat

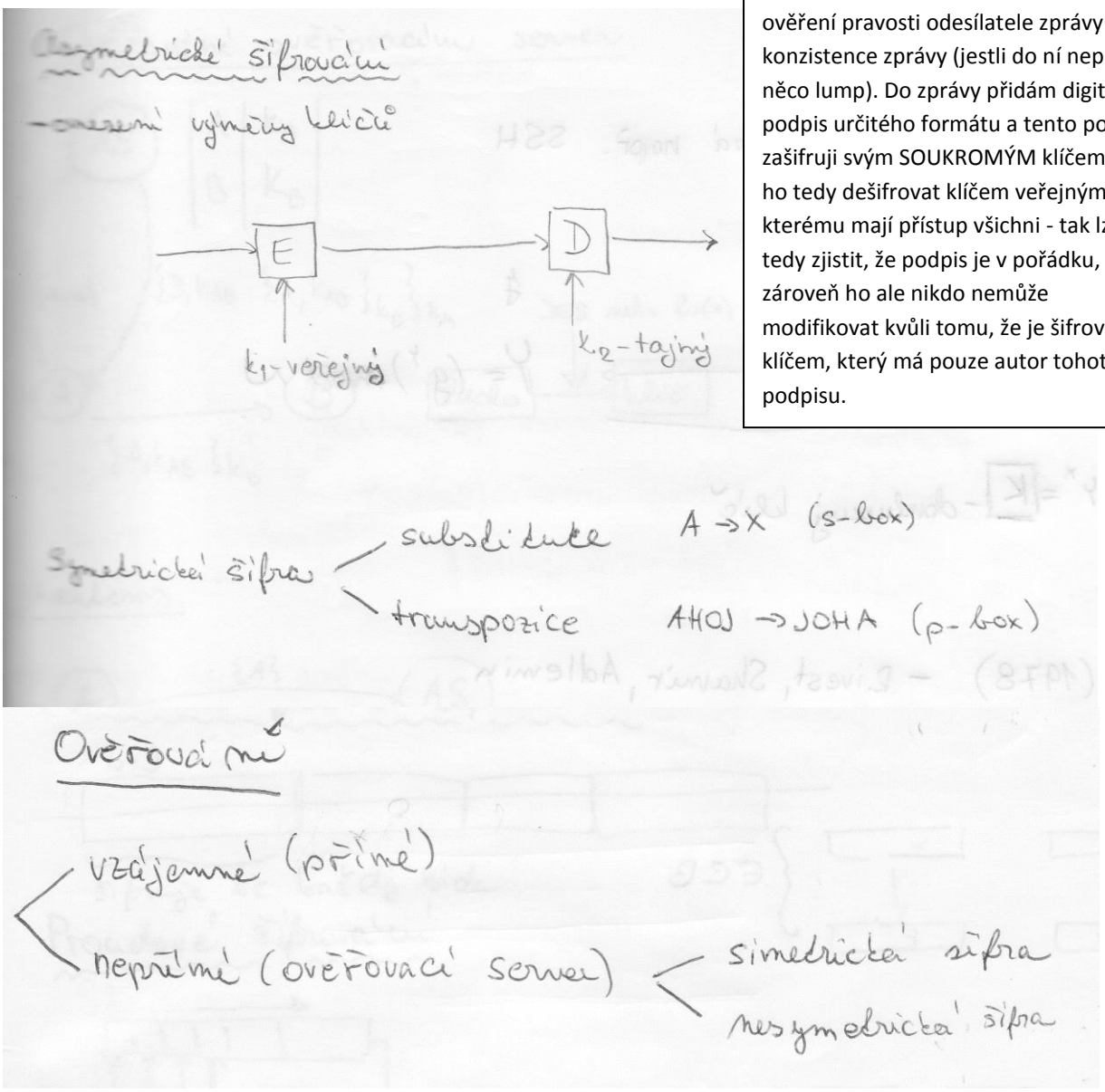


Symetrické - k šifrování a dešifrování se používá stejný klíč - takže např. existuje pouze jeden pro daný přenos. Takový způsob šifrování by měl být o dost rychlejší, než asymetrické. Velký problém tohoto ale je, jediný klíč - tzn. dostane se k němu lump a může jak dešifrovat komunikaci, tak i šifrovat falešné zprávy.

Asymetrické oproti tomu využívá dvou klíčů. Jeden je veřejný a druhý je soukromý. K veřejnému mají přístup všichni a slouží primárně k šifrování zpráv, které se mají směrovat k příjemci, který vlastní soukromý klíč. Takže taková komunikace vypadá asi takto: chci přijímat šifrované zprávy, vygeneruji si dva klíče a jeden pustím do oběhu - tzn. k mému soukromému by se neměl nikdo dostat a lze tedy toto šifrování považovat za bezpečné. Nevýhodou je malá rychlost a tak se to používá zejména k předání klíčů symetrického šifrování.

Takže komunikace z toho zadání jak jsme měli v písemce: Chci použít symetrické šifrování, ale potřebuji způsob, jak dostat klíč k tomu druhému, se kterým budu komunikovat. Použiji tedy asymetrické šifrování pouze k předání klíčů. Když máme oba klíče můžeme šifrovat symetricky.

Digitální podpis (hash, kontrolní součet všechno je to jeden pojem doufám) - k ověření pravosti odesílatele zprávy a konzistence zprávy (jestli do ní nepřipsal něco lump). Do zprávy přidám digitální podpis určitého formátu a tento podpis zašifruji svým SOUKROMÝM klíčem. Lze ho tedy dešifrovat klíčem veřejným, ke kterému mají přístup všichni - tak lze tedy zjistit, že podpis je v pořádku, zároveň ho ale nikdo nemůže modifikovat kvůli tomu, že je šifrovaný klíčem, který má pouze autor tohoto podpisu.



Kryptografická hašovací funkce je v kryptografii hašovací funkce s takovými vlastnostmi, které umožňují její použití v aplikacích zabezpečení informací, jako například autentizace nebo zaručení integrity zprávy. Kryptografická hašovací funkce je používána pro ochranu proti úmyslnému poškození dat a v dalších kryptografických aplikacích.

Známé hashovací funkce: SHA-1 a SHA-2

Certifikát je datová struktura (řetězec bitů) pomocí které se zveřejňují údaje o uživateli a zejména uživatelův veřejný šifrovací klíč (v případě RSA šifer). Certifikát je elektronicky podepsán (ověřen) certifikační autoritou. Z certifikátu je možné získat veřejný šifrovací klíč uživatele, který je možné použít k prokazování totožnosti uživatele. V případě, že certifikát obsahuje šifrovací klíč určený také k šifrování dat, pak je možné i tento klíč z certifikátu použít k šifrování dat odesílaných uživateli. Certifikát se často přirovnává k občanskému průkazu.

Ověřování ověřovacím serverem

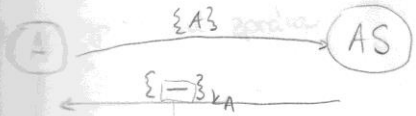
{a,b}

$\{B, k_{AB}, \{A, k_{AB}\}_{k_B}\}_{k_A}$

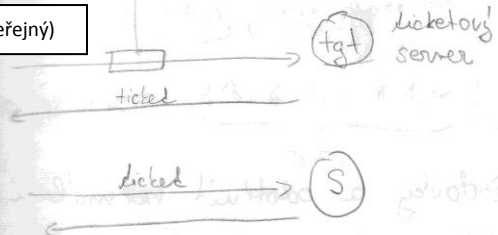
DES nebo hv(x)

$\{A, k_{AB}\}_{k_B}$

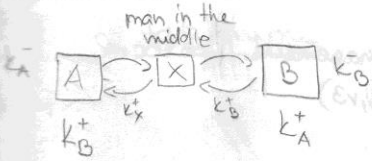
Kerberos



Heslo-Ka(veřejný)



Ověřování - veřejný klíč

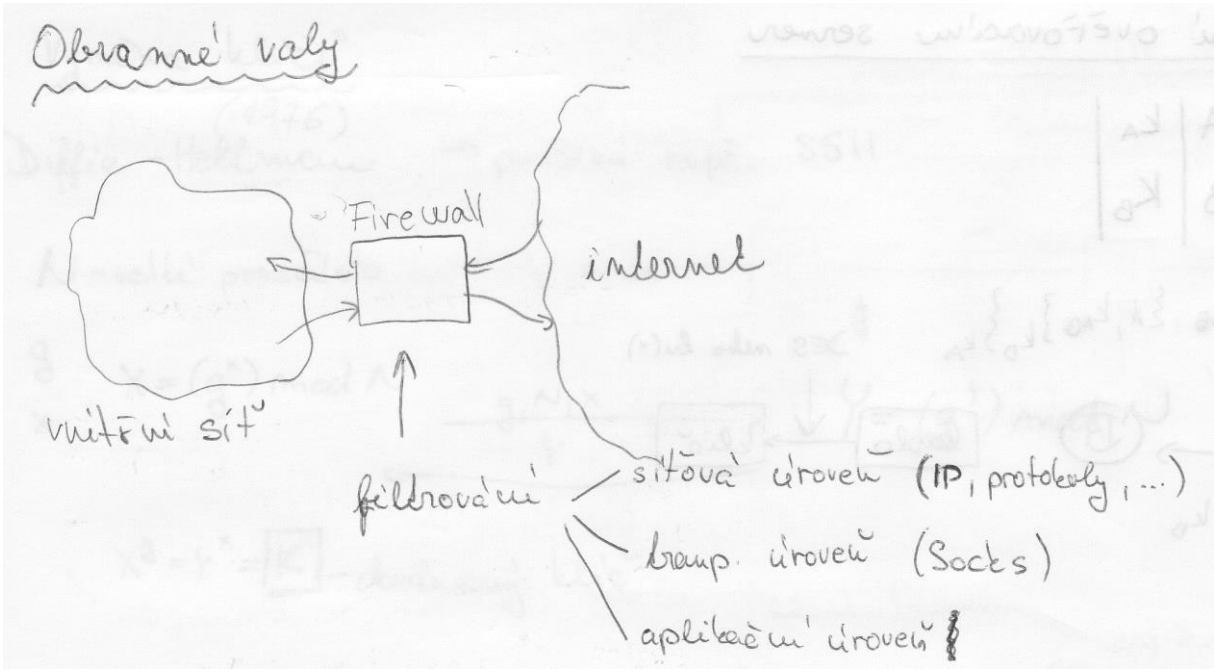


Certifikát:
- obsahuje můj veřejný klíč

$\{|K_A^+| \ldots\} = x \rightarrow \{hv(x)\}_{k_{AC}^-}$

různá další identif. data + časová platnost

tajný klíč certifikační autority



12. Nakreslete TCP/IP zásobník a zařaďte protokoly a ve stručnosti je popište.

1. TCP/IP zásobník

Aplikační vrstva

- DNS, BOOTP, DHCP, FTP, Telnet, SMTP, SSH

Transportní vrstva

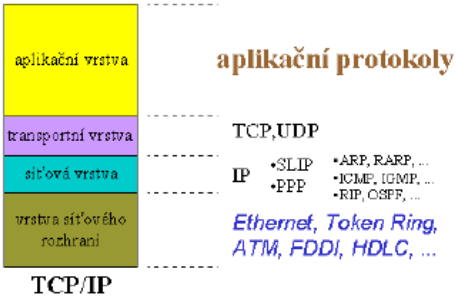
- TCP, UDP

Síťová vrstva

- IP, ARP, ICMP, IGMP

Přenosová vrstva

- Ethernet, HDLC



DHCP (Dynamic Host Configuration Protocol) – obdoba BOOTP, modernější, nepoužívá statické konfigurace (při každém připojení do sítě může uzel obdržet jinou adresu), umožňuje dynamickou změnu nastavení uzlu

BOOTP (Bootstrap Protocol) – pracuje nad UDP, slouží k získání IP adresy a dalších parametrů potřebných pro zapojení uzlu do sítě; získání síťového nastavení pro provoz uzlu

Telnet (Telecommunication Network) - pomocí stejnojmenné aplikace umožňuje uživateli připojení ke vzdálenému počítači, spojení typu klient-server protokolem TCP(duplexní spojení)

Ethernet – metoda náhodného přístupu, sběrnicová nebo hvězdicová topologie, rozlehlost stovky metrů až několik km, nejrozšířenější lokální síť, distribuovaná a neřízená metoda přístupu

FTP (File Transport Protocol) – přenos souborů, přístup ke vzdálenému serveru

DNS (Domain Name System) – převod jména na adresu a opačně, poskytuje id další informace

UDP (User Datagram Protocol) – nespojované služby, nepotvrzované

TCP (Transport Control Protocol) – spojované služby, potvrzované, obnova po chybě

ICMP (Internet Control Message Protocol) – přenos zpráv o chybách, test dosažitelnosti vzdáleného uzlu, přenos parametrů, synchronizace času

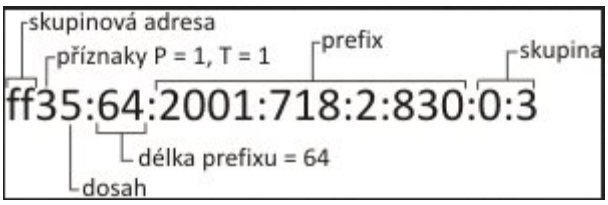
IGMP (Internet Group Management Protokol) – je protokol, který rozšiřuje požadavky na implementaci protokolu IP (IPv4) o podporu IP multicastu. Využívá se pro dynamické přihlašování a odhlašování ze skupiny u multicastového routeru ve své lokální síti. IGMP protokol řeší i situaci, kdy jsou v síti připojeny dva a více multicastových routerů, protože pak by mohlo dojít v síti k šíření nadbytečných informací.

ARP (Address Resloution protocol) – převod síťové adresy na fyzickou

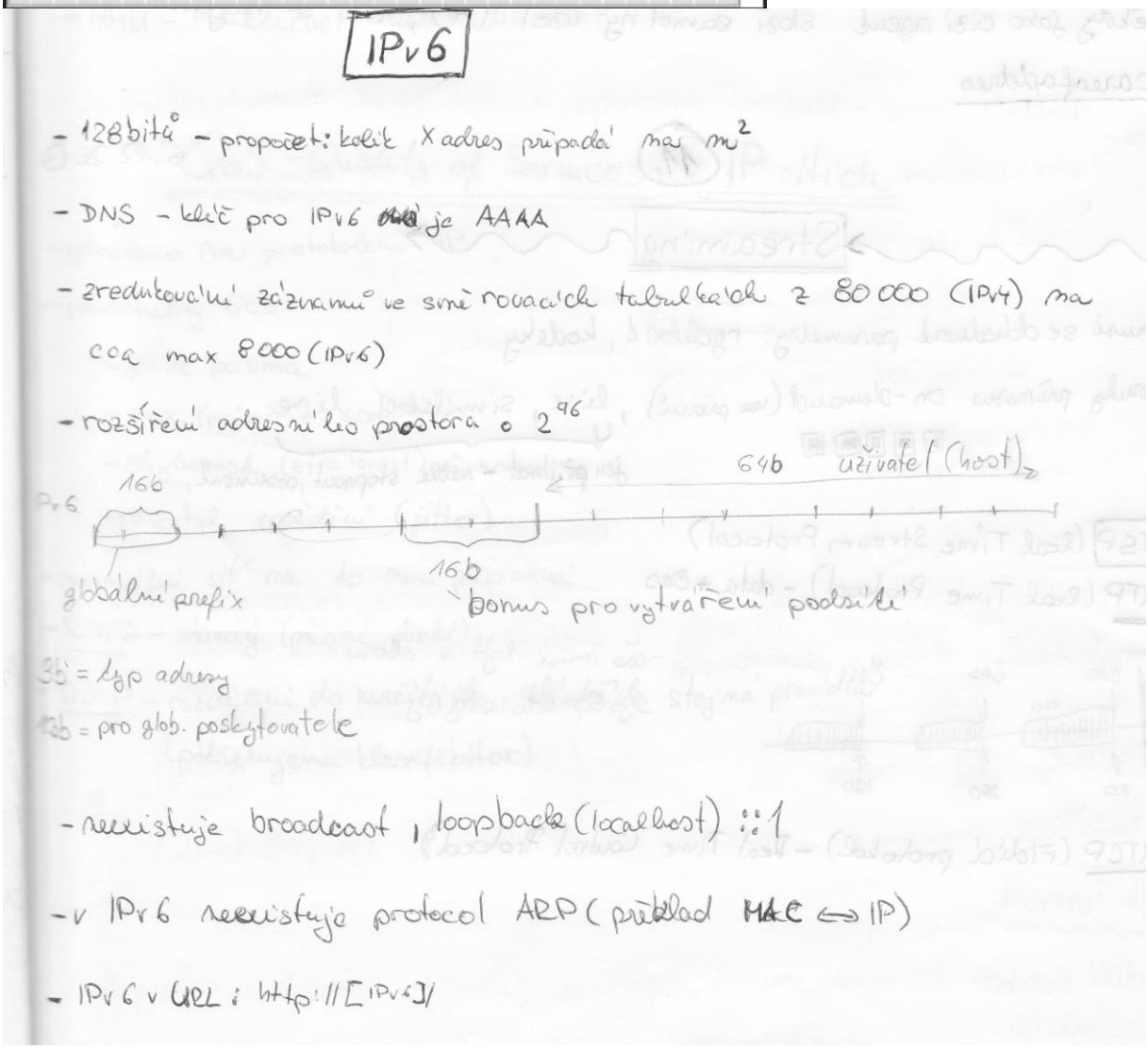
IP (Internet Protocol) – nespojovaný protokol, nepotvrzované služby, přenáší pakety a směruje je podle cílové adresy

13. IPv6 - jak vypadá záhlaví IPv6

128bitů



Základní záhlaví IPv6 protokolu

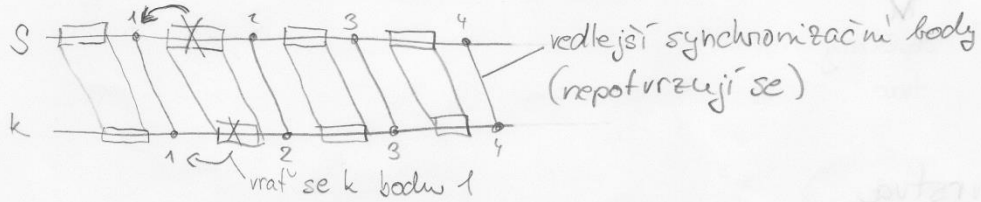


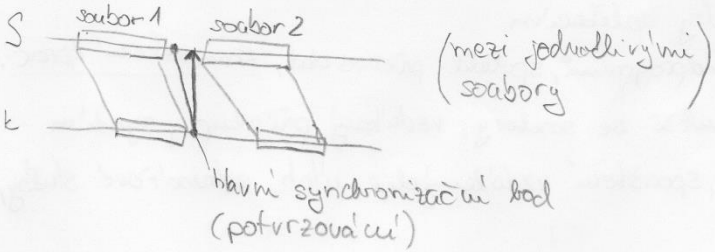
14. Relační úroveň, hlavní a vedlejší synchronizační body.

Relační vrstva

- řeší se problém: co s výpadkem transportního spojení?
- ∃ transportní spojení
- ∃ relační spojení
- vztahy 1:1 (T:R) – např. právě 1 HTML stránka v rámci HTTP protokolu
  1:N (T:R) – naváže 1 transp. spojení a realizuje více relací
  N:1 (T:R) – stahování souboru (dojde-li k výpadku ⇒ může stahování obnovit)

Obnova transp. ~~relace~~ spojení během relace

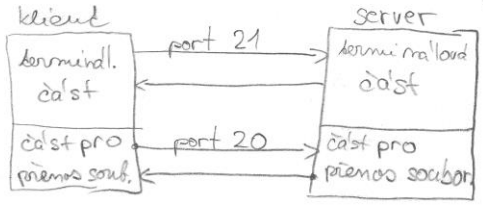




15. FTP - aktivni/pasivni

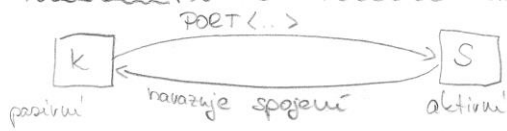
Přenos souborů

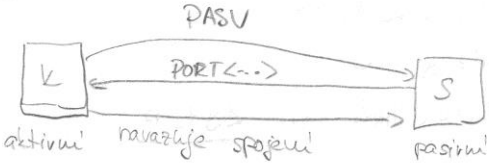
- FTP (File Transfer Protocol)
  - spolehlivý, TCP
  - vyžaduje přihlašování
  - sestává ze dvou částí ← terminálový provoz
    vlastní přenos souborů (GET, PUT)



ovládání klienta: !před příkaz

Aktivní a pasivní navázání spojení





Anonymní uživatelé

- ftp, anonymous – heslo: e-mailová adresa

Bezpečnost

- řeší scp (Secure copy) ← navázže šifrované spojení
  přenáší data

- SSH protokol
  - navazování spojení

Jeffie-Hellman schema

g — y – tajemství

N – velké prvočíslo ← $Y = (g^y) \bmod N$

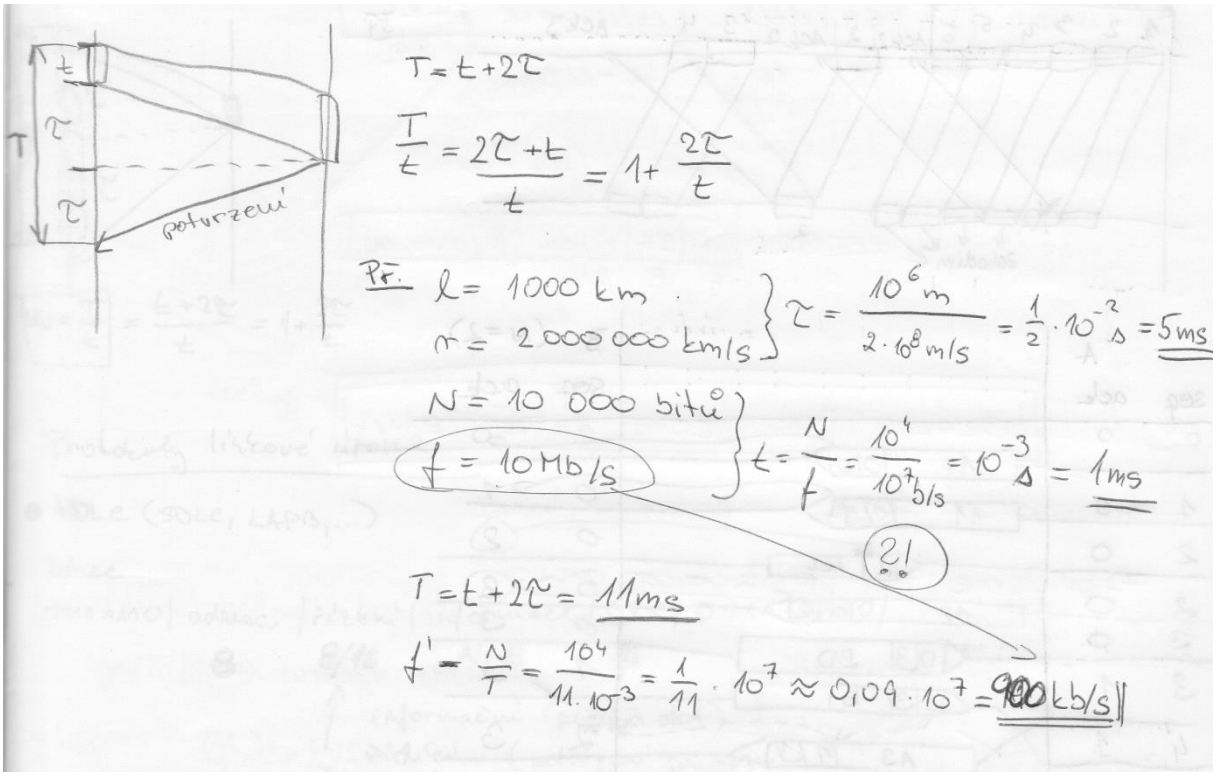
x – tajemství

$X = g^x \% N$ →

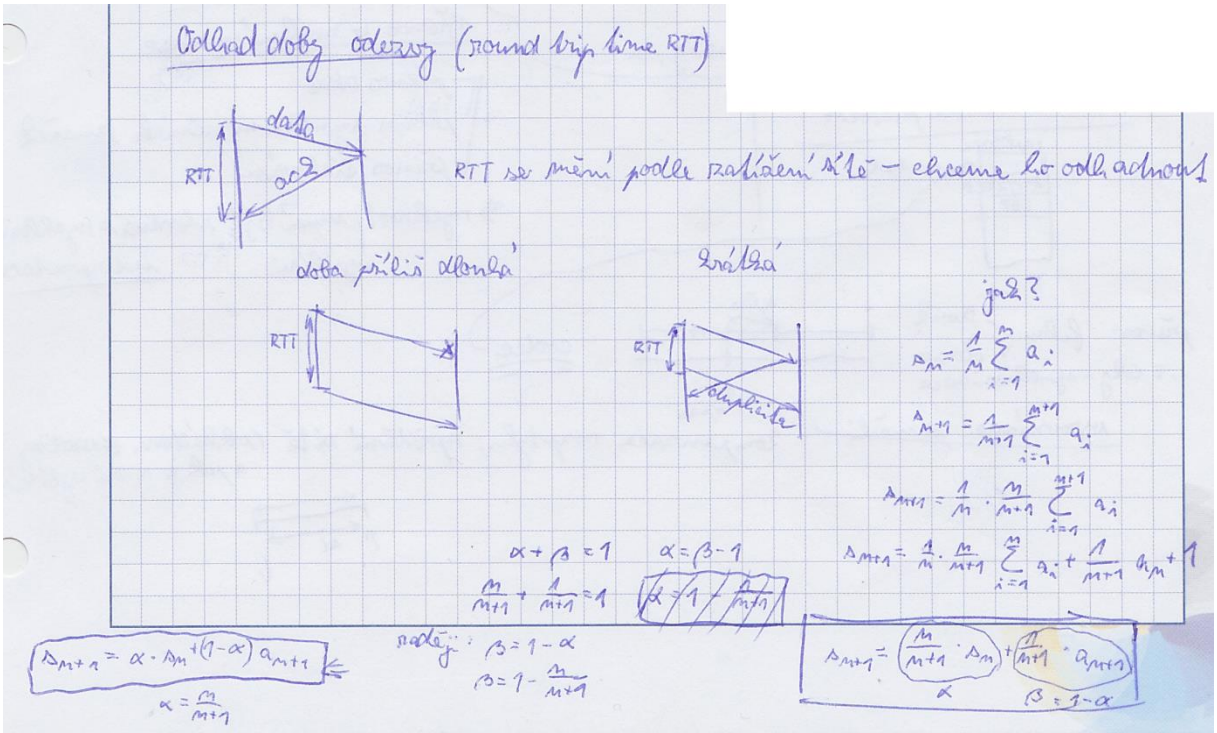
X, g, N

$(X^y) \bmod N = (Y^x) \bmod N = (K)$ – klíč používaný pro komunikaci

16. Určit průměrnou přenosovou rychlost u Stop and Wait. Doba vysílání je 1ms, délka zprávy 10000 bitů a doba odezvy je 5ms. Nakreslit obrázek vysílání.



17. Jak se zjišťuje (odhaduje) doba odezvy RTT při přenosu TCP.

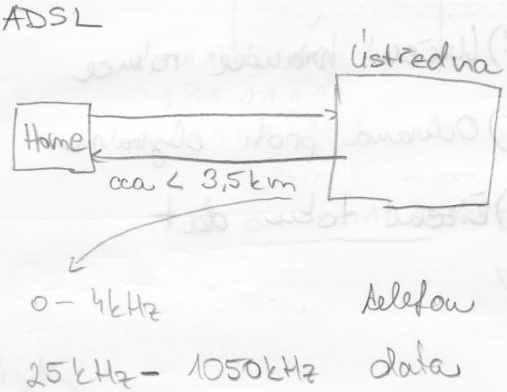


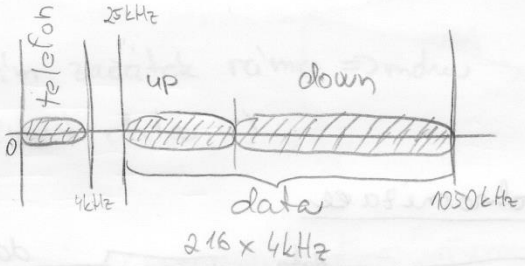
18. Co je ADSL, co je to splitter, díky čemu ADSL dosahuje vysokých rychlostí.

- AD převodník

ISDN – 2 kanály (64 kb/s) – volání + internet
1 kanál (16 kb/s)

ADSL





Kabelové sítě

- kabelová televize
- telefon
- kabelový modem < downlink
  uplink – sdílený