Počítačové sítě

vypracované státnicové otázky

1 Model ISO/OSI a přenosové protokoly TCP/IP, popis a vlastnosti

- referenční komunikační model označený zkratkou slovního spojení "International Standards Organization / Open Systen Interconnection" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů)
- rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev
- úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě

1.1 Popis vrstev

1.1.1 Fyzická vrstva

- specifikuje bitový přenos z jednoho zařízení na druhé prostřednictvím fyzického média
- definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení.
- vrstva zajišťuje synchronizaci (synchronní vs. asynchronní komunikace) a multiplexing – několik logických spojení lze realizovat jedním fyzickým médiem

1.1.2 Linková vrstva

- přístup ke sdílenému médiu a adresaci na fyzickém spojení – tj. v jednom síťovém segmentu
- datové jednotky přenášené linkovou vrstvou jsou rámce (frame).

1.1.3 Síťová vrstva

- zajišťuje adresaci v rámci síťového prostředí s více fyzickými segmenty
- používá logické adresy a prostřednictvím nich přenos dat z jednoho zařízení na druhé i z jedné sítě do jiné
- datové jednotky přenášené síťovou vrstvou jsou pakety (packet)

1.1.4 Transportní vrstva

- zajišťuje spolehlivost a kvalitu přenosu jakou požadují vyšší vrstvy
  - spojově orientované (connection-oriented) služby (TCP)
  - nespojové (connectionless) služby (UDP)
- datové jednotky TPDU (Transport Layer Protocol Data Unit)

1.1.5 Relační (spojová) vrstva

- pravidla pro navazování a ukončování datových přenosů mezi uzly na síti
- služby typu překlad jmen na adresy nebo bezpečnost přístupu.
- datové jednotky SPDU (Session Layer Protocol Data Unit)

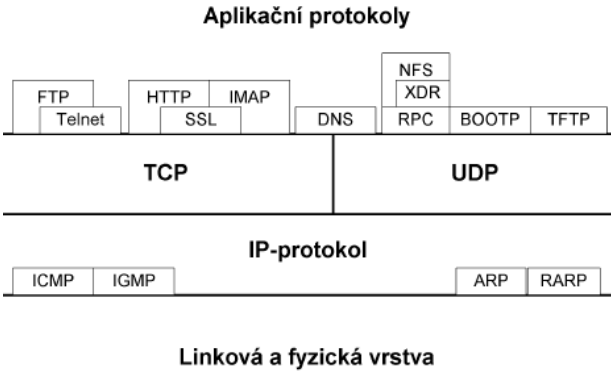
1.1.6 Prezentační vrstva

- formátování a syntaxe dat
- šifrování /dešifrování a komprese/dekomprese dat
- Datové jednotky PPDU (Presentation Layer Protocol Data Unit)

1.1.7 Aplikační vrstva

- nejvyšší vrstva v modelu
- souborové přenosy, sdílení zdrojů, přístup k databázím, prohlížení webových stránek, ovládání programů, apod.
- datové jednotky APDU (Application Layer Protocol Data Unit)

1.2 Přenosové protokoly TCP/IP



1.2.1 IP (Internet Protocol)

- prakticky odpovídá síťové vrstvě
- identifikace uzlu IP adresou
- přenáší IP datagramy (s adresou příjemce) -> mohou dorazit v jiném pořadí než byly odesílány

1.2.2 TCP a UDP protokoly

- odpovídají transportní vrstvě
- TCP – TCP segmenty, spojované služby
- UDP – UDP datagramy, nespojované služby
- adresování pomocí portu

1.2.3 Aplikační protokoly

- odpovídají vyšším vrstvám modelu ISO/OSI

Uživatelské protokoly

- FTP/TFTP (File Transfer Protokol / Trivial FTP)
  - přenos souborů mezi počítači
  - FTP – TCP, TFTP – UDP
- HTTP/HTTPS (Hypertext Transfer Protocol)
  - určený původně pro výměnu hypertextových dokumentů ve formátu HTML
  - v současnosti pomocí rozšíření MIME umí přenášet jakýkoli soubor

    - HTTPS - zabezpečená nadstavba nad HTTP, zabezpečení SSL nebo TLS
- TELNET
    - terminálový provoz
    - nešifrovaná komunikace
- POP3 / IMAP / SMTP
    - protokoly pro práci s elektronickou poštou

Služební protokoly

- směrovací protokoly
- spravovací protokoly (SNMP)

2 IP adresování a jmenné služby, pomocné protokoly (ICMP, BOOTP, DHCP) a protokoly pro interní a externí směrování

2.1 IP adresování

- IP adresa jednoznačná identifikace konkrétního zařízení v prostředí internetu

2.1.1 IPv4

- délka adresy 4 bajty – oddělují se tečkou
- 2 části – adresa sítě, adresa počítače
- třídy adres:

Třída	Začátek	1.B	Standardní maska	Bitů sitě	Bitů stanice	Sítí	Stanic v každé síti
A	0	0-127	255.0.0.0	8	24	128	16777216
B	10	128-191	255.255.0.0	16	16	16384	65536
C	110	192-223	255.255.255.0	24	8	2097152	256
D	1110	224-239	Multicast				
E	1111	240-250	Rezerva				

- privátní adresy (nesmějí být přiřazeny na vnějších zařízeních):
  - A: 10.0.0.0 až 10.255.255.255
  - B: 172.16.0.0 až 172.31.255.255
  - C: 192.168.0.0 až 192.168.255.255
- speciální adresy:
  - 127.0.0.1 – loopback
- **síťová maska:**
  - určení adresy sítě (určuje, které bity v IP adrese tvoří adresu sítě)
- v současnosti nedostatek IPv4 adres:
  - používání dynamicky přidělovaných adres
  - používání privátních sítí (-> překlad adres NAT/PAT)

2.1.2 IPv6

- délka 128 bitů – osm skupin po čtyřech hexa číslicích
  - 2001:0718:1c01:0016:0214:22ff:fec9:0ca5
  - posloupnost „0“ může být vypuštěna a nahrazena „::“
- rozšíření adresního prostoru (min. 65536 subsítí pro každého, třída A z IPv4 pro každou stranu)
- bez překladu adres
- 3 typy adres:
  - *Individuální (unicast)* která identifikují právě jedno síťové rozhraní.
  - *Skupinové (multicast)* označují skupinu síťových rozhraní, jejímž členům se mají data dopravit. Skupinově adresovaný datagram se doručuje všem členům skupiny.
  - *Výběrové (anycast)* označují také skupinu síťových rozhraní, data se však doručují jen jejímu nejbližšímu členovi.
- speciální adresy:
  - ::1 – localhost

- ::0 – nespecifikovaná adresa (používá se během inicializace)
- ff00::/8 – skupinové

2.2 Jmenné služby (DNS – Domain Name System)

- hierarchický systém doménových jmen -> servery DNS
- celosvětově distribuovaná databáze
- vzájemné převody doménových jmen a IP adres uzlů sítě
  - A záznamy – převod IPv4 adresy
  - AAAA záznamy – převod IPv6 adresy
  - PTR záznamy - zpětný překlad
- dělení na domény a subdomény
- kořen stromu - „.“
  - pod ní **Top-Level-Domain** (com, cz, sk, eu …)
    - atd...

2.2.1 DNS servery

Primární server

- udržuje data o své databázi na disku
- pouze zde má smysl editovat databázi
- autoritativní

Sekundární server

- automatická kopie primárního serveru
- slouží i jako záloha nebo i pro rozklad zátěže u frekventovaných domén
- autoritativní

Caching only server

- není pro žádnou zónu primárním ani sekundárním serverem
- data, která jím prochází uchovává do vypršení jejich životnosti

Root name server

- obsluhují root doménu
- popisují kde se nachází autoritativní servery pro domény nejvyšší úrovně

2.3 Pomocné protokoly

2.3.1 ICMP (Internet Control Message Protocol)

- služební protokol, součást IP protokolu
- slouží k signalizaci mimořádných událostí
- př. ping – zjištění dostupnosti uzlu (Echo Request, Echo Response)

2.3.2 BOOTP a DHCP

- slouží k automatickému nastavování síťových parametrů bez zásahu uživatele
- DHCP je založený na BOOTP, je zpětně kompatibilní
- rozdíly:
- BOOTP umožnuje nastavovat pouze IP adresu, masku, adresu brány a adresu DNS
- BOOTP neumožňuje dynamické přidělení adresy (adresa musí být předem nakonfigurována na BOOTP serveru)
- DHCP umožňuje nastavit expiraci přidělení adresy

2.4 Interní a externí směrování

2.4.1 IGP

- interní směrování v rámci autonomního systému
- **RIP (Routing Information Protocol):**
  - RVP (Routing Vector Protocol)
  - používá se metrika (max. 15 hopů, 16 je nedostupný)
  - pro menší sítě
  - routery si vyměňují tabulky každých 30 sekund
- **OSPF (Open Shortest Path First):**
  - LSP (Link State Protocol)
  - berou v úvahu i stav linek
  - výměna tabulek na základě změny stavu v síti
  - pro nejkratší cestu se používá Dijkstrův algoritmus

2.4.2 EGP

- externí směrování, mezi autonomními systémy
- protokoly umí zohlednit směrovací politiku
- BGP (Border Gateway Protocol):
  - dle LSA (Link State Algorithm)
  - vyměňují se pouze informace o změnách

3 Skupinové adresování a směrování (multicast)

- směrovací technologie – 1 zdroj, více cílů (1 data odeslány celé skupině)
- výhody: menší objem přenášených dat -> menší zatížení sítě
- Určení rozsahu doručování:
  - *Implicitní*
    - Použiti link-local adresy
    - Neopustí podsíť
  - *Omezení rozsahu založené na TTL*
    - Multicast směrovače maji nastaven práh (TTL prah)
    - Jestliže je TTL ≤ TTL práh, je datagram zahozen
  - *Administrativní omezení*
    - Použití skupiny adres 239.0.0.0 až 239.255.255.255
    - Omezení na administrativní doménu
    - V IPv6 je rozsah součastí atributu uvedeného v adrese

3.1 IGMP

- protokol pro přihlašování do skupin

3.1.1 IGMPv1

- pouze registrace / uvolnění
- výzva poslána na 224.0.0.1, TTL=1
- odpověď: posílána jen jedním hostem ze skupiny na skupinovou adresu, pokud se nikdo neozve skupina neexistuje

3.1.2 IGMPv2

- připojení / odpojení ze skupiny zprávou
- host posílá zprávu o opuštění na 224.0.0.2 (all routers) -> zkrácení doby pro detekci prázdné skupiny
- směrovač reaguje specifickou výzvou aby zjistil jestli je skupina prázdná

3.1.3 IGMPv3

- podpora SSM (Source Specific Mcast)

3.2 Směrovací protokoly

- existují dva typy:
  - **Dense Mode** (hustý režim):
    - push model, multicastový provoz se „tlačí“ do všech větví stromu
  - **Sparse Mode** (řídký režim):
    - pop model, směrovače explicitně „vytahují“ multicastový provoz od zdroje

3.2.1 DVMRP (Distance Vector Mcast Routing Protocol)

- hustý režim (dense mode)
- záplavové doručování
- explicitní připojení do subsítě
- source-based distribuční stromy

3.2.2 MOSPF (Mcast OSPF)

- hustý režim
- připojování pomocí Join
- není třeba šířit data záplavou od každého zdroje do každé subsítě

3.2.3 PIM-DM (Protocol Independent Mcast – Dense Mode)

- **hustý režim** = implicitně doručuje do všech subsítí
- libovolný směrovací protokol pro zajištění Reverse Path Forward (zjištění nejkratší cesty ke zdroji)
- routery používají záplavu s odřezáváním (flood and prune)

3.2.4 PIM-SM (Protocol Independent Mcast – Sparse Mode)

- **řídký režim** = použití explicitní Join zprávy pro připojení toku do subsítě
- RPF nezávislé na protokolu
- doručovací stromy se zavádí mezi příjemcem a RP (Randezvous Point)

3.2.5 CBT (Core Based Tree)

- charakteristiky jako PIM-SM, ale efektivnější při hledání zdrojů
- vytváří infrastrukturu pro doručování Mcast zpráv
- komerčně se nepoužívá

4 Mobilní IP

- protokol aplikační vrstvy
- **Mobile IP**
  - mobilita uzlů při přesunu ze sítě do sítě bez změny IP adresy pro udržení spojení na transportní a vyšší vrstvě.
- **Home Agent (domácí agent)**
  - směrovač v domácí síti mobilního klienta
  - udržuje informaci o momentálním výskytu klienta v intersíti
  - posílá pakety tunelem když se nenachází v domácí síti
- **Foreign Agent (cizí agent)**
  - směrovač v cizí síti kde je mobilní klient na návštěvě s náhradní adresou
  - poskytuje služby směrování po dobu registrace
  - zakončuje tunel od domácího agenta
  - odpouzdřuje datagramy a doručuje je mobilnímu uzlu
- Registrace:
  - uzel žádá FA, FA žádá HA, HA odpoví FA, FA odpoví uzlu
- Přenos zprávy:
  - uzel A pošle uzlu B, HA slyší, zabalí, pošle FA, FA zjistí adresu B přes ARP, FA rozbalí, pošle B.

5 Protokoly pro přenos v reálném čase

5.1 RTP (Real Time Protocol)

- představuje pouze mechanismy
- protokolově neutrální
- oddělené řízení a data
- bezpečnost (šifrování, ověřování)
- **funkce:**
  - fragmentace / defragmentace, znovuuspořádání (pokud je potřeba)
  - detekce ztrát, obnova
  - synchronizace uvnitř média (odstranění chvění zpoždění, vyrovnávání vzorkovacích hodin, synchronizace audia a videa, QoS zpětná vazba a adaptace rychlosti)
  - identifikace zdroje
- použití UDP, lib. port, RTCP = RTP+1
- **řízení: RTCP (Real Time Control Protocol)**
  - řízení RTP relace
  - sledování kvality, QoS zpětná vazba
  - odhad členství
  - detekce smyček

5.2 RTSP (Real Time Streaming Protocol)

vlastnosti:

- hrubá synchronizace (doladění – RTP sender report)
- virtuální prezentace = synchronizování přehrávání od několika serverů
- vyrovnávání zdrojů
- podpora ovládání zařízení
- vyrovnávací paměti (obdoba http)
- 1 TCP spojení na relaci

podobnosti s http:

- formát protokolu: text, MIME záhlaví, typ požadavek – odpověď
- stavové kódy, formát URL, bezpečnostní mechanismy

odlišnosti od http:

- stavový server, odlišné metody
- data přenášená mimo pásmo
- odstranění http chyb (požadavky s relativními cestami, kódování 8859-1)

6 Elektronická pošta, přenos souborů, vzdálený přístup, protokoly pro informační službu, LDAP

6.1 Elektronická pošta (e-mail)

- odesílání a přijímání zpráv přes elektronické komunikační systémy
- formát zprávy:
  - **Obálka**
    - informace důležité pro doručení zprávy
    - adresa odesílatele a adresa příjemce zprávy
  - **Hlavička**
    - řídící informace zprávy – schéma <klíč>: <paramtery>
    - např. původce zprávy, adresát zprávy, identifikace zprávy, datové a časové razítko (označující okamžik zpracování zprávy emailovým serverem), předmět, klíčová slova, nestandardní hlavičky apod.
    - aktualizována každým emailovým serverem, přes který email prochází
    - přidává se řádek Received: adresa MTA serveru + další jeho informace
  - **Tělo zprávy**
    - vlastní text zprávy

6.1.1 Protokoly

SMTP (Simple Mail Transfer Protocol)

- přenos e-mailových zpráv od klienta na server a výměna e-mailů mezi servery
- směrování na základě záznamů MX v DNS (pokud MX neexistuje, použije se A záznam)
- příkazy: HELO, MAIL, RCPT, DATA, RSET, NOOP a QUIT.

POP3 (Post Office Protocol)

- přenos e-mailových zpráv uložených na serveru na klientský počítač

IMAP (Internet Message Access Protocol)

- vzdálený přístup k elektronické poště z klientského počítače
- práce se zprávami na straně serveru

MIME (Multipurpose Internet Mail Extensions)

- rozšíření těla zprávy z původního textového na několik typů
- Typy zpráv MIME:
  - TEXT – vlastní tělo zprávy
  - IMAGE – přenos obrazu
  - AUDIO – přenos zvuku
  - VIDEO – přenos videa
  - APPLICATION – přenos jiného typu dat, neinterpretovaná binární data.
  - STRUCTURED – někdy se nazývá vícedílný (multipart). Ve strukturovaném typu se nepřenášejí data jako taková, ale určitá kombinace již uvedených typů.

- MESSAGE – přenos vlastní zprávy. Definuje podtypy RFC 822 (běžná zpráva), Partial (zpráva je částí celku, takto se odesílají zprávy delší než 64kB) a External Body (představuje odkaz na soubor, který je vůči emailové zprávě externí)

6.2 Přenos souborů

6.2.1 FTP (File Transfer Protocol)

- protokol aplikační vrstvy TCP/IP
- přenos souborů mezi počítači (rozdílné OS apod...)
- klient – server: porty 20 (samotný přenos) a 21 (řízení)
- řízení přístupu (přihlašování)
- v současnosti ne moc bezpečný -> rozšíření

6.2.2 TFTP (Trivial FTP)

- odlehčený FTP, protokol UDP
- vlastní způsob řízení spojení
- port 69
- omezení oproti FTP:
  - nelze procházet adresáře
  - neumožňuje přihlášení uživatele ani zadání hesla
  - maximální velikost přenášeného souboru je 32 MB

6.3 Protokoly pro vzdálený přístup

6.3.1 Telnet

- klient/server protokol, TCP/IP, port 23
- využíván především pro vzdálenou administraci
- tři základní služby:
  - síťový virtuální terminál (NVT – Network Virtual Terminal), který poskytuje standardní rozhraní, transparentnost vůči uživateli
  - vyjednávání klienta/serveru o nastavení určitých voleb
  - symetrické zobrazení terminálu a procesů

6.4 Protokoly pro informační služby

6.4.1 Gopher

- uspořádání v podobě hierarchického menu
- jednotlivé položky mohou ukazovat buď na další podobné menu, nebo již na samotný koncový obsah

6.5 LDAP (Lightweight Directory Access Protocol)

- protokol pro ukládání a přístup k datům na adresářovém serveru
- záznamy uspořádány do hierarchické struktury
- každý záznam popisuje nějaký objekt
- vhodný pro udržování informací o uživatelích
- odvozen od X.500 („odlehčený“)
- v aplikaci funguje jako klient-server, synchronní i asynchronní mód
- **záznam:**
  - atribut – hodnota
  - musí odpovídat přípustnému schematu
- **schema:**
  - soubor povolených tříd a knim náležících atributů
- **operace:**
  - aktualizační:
    - add, delete, rename, modify
  - autentizační:
    - bind, unbind, abandon
- příklady některých syntaxí:
  - bin – binární informace
  - ces – case exact string (directory string), při porovnávání rozlišuje malá/velká písmena
  - tel – telefonní číslo, reprezentace jako řetězec, mezery jsou ignorovány
  - dn – rozlišující jméno (distinguished name)

7 HTTP, proxy, vyrovnávací paměti

7.1 HTTP protokol

- původně určený pro výměnu hypertextových dokumentů ve formátu HTML
- obvykle používá port 80, případně 8080
- v současnosti pomocí rozšíření MIME umí přenášet jakýkoli soubor
- společně s využitím XML je používaný pro webové služby
- URL (Unified Resource Locator) – jednoznačně identifikuje uměstění zdroje v internetu
- HTTPS - zabezpečená nadstavba nad HTTP, zabezpečení SSL nebo TLS
- funkce:
  - dotaz – odpověď
  - bezestavový protokol – neumí uchovávat stav komunikace
    - vyřešeno pomocí HTTP cookies -> informace se ukládají na klientský počítač

7.2 Proxy servery

- prostředník při komunikaci klient – server
- klient posílá požadavky na server, požadavky však obslouží proxy server, který je přepošle dotazovanému serveru
- odpověď se posílá zpět přes proxy server klientovi
- účely použití proxy serveru:
  - ochrana soukromí
    klientem se stává proxy server, skrytí informací o klientu, některé proxy však předávají pozměněný požadavek i s informacemi o původním klientu
  - zvýšení výkonu komunikace
    některé opakované požadavky může mít proxy server uložen ve vyrovnávací paměti a obsloužit tak klienta bez poslání dotazu na server -> hrozí neaktuálnost odpovědí
  - bezpečnost
    filtrování obsahu, odstraňování reklam apod.

8 Protokoly pro řízení sítě (SNMP a RMON), ASN.1 a BER

8.1 SNMP (Simple Network Management Protocol)

- získávání různých dat pro potřeby správy sítě
- model klient – server (tzv. Agent)
- agent může sám vysílat data (např. informace o událostech) – **Trapy**
  - nutné předem definovat cílovou adresu
- komunikace na portu 161
- ukládání hodnot do datové struktury zvané MIB

8.1.1 SNMPv1

- pouze metody get, get next, set, trap
- ochrana pouze heslem – community string

8.1.2 SNMPv2

- přidána metoda getbulk – pro lepší získávání informací z tabulek

8.1.3 SNMPv3

- přidáno šifrování, ochrana dat pomocí algoritmu DES

8.1.4 MIB (Management Information Base)

- dovoluje jednoznačně identifikovat informace využívané systémem správy
- objektově orientovaná databáze
- každý objekt může obsahovat jiné objekty či jiné třídy
- MIB je tvořena jedním stromem
  - data uložena v listech stromu
  - každý uzel stromu má číselné i jmenné označení
- MIB definuje typ a velikost uložených dat a cestu k nim
- 3 mechanismy pro přidání
  - přidání nových objektů pomocí definice nové verze MIB-II
  - přidání nestandardních objektů přidáním experimentální větve
  - přidání vlastních objektů v rámci podstromu soukromé větve

8.1.5 Příkazy

- **get-request** - získání informace z MIB
- **get-next-request** – získání informace o objektech v MIB bez znalosti jejich přesných jmen, umožňuje postupné procházení celým hierarchickým stromem
- **set-request** - změna hodnoty proměnné agenta
- **trap** – vysílána agentem jako reakce na specifikovanou událost, zpráva zůstává nepotvrzená
- **get-response** - reakce agenta na předchozí příkazy - odpověď agenta managerovi, obsahuje i dotaz, protože protokol nezajišťuje souvislost mezi dotazem a odpovědí
- **get-bulk** - součástí SNMP v2, umožňuje vyžádat si k přečtení celou skupinu informací z MIB, urychlení komunikace

- **inform** - komunikace dvou managerů mezi sebou

8.2 RMON (Remote Monitoring)

- velmi podobný SNMP
- umožňuje hlubší analýzu – historické údaje a statistiky (SNMP pouze aktuální hodnoty)
- odlehčení komunikace přesunutím vetší části činnosti na agenta
- dokonalé detekce poruch v síti
- sledování ethernet i token-ring segmentů
- klientem je možnost konfigurovat sondu ke sběru informací
- využívá se SNMP datové struktury složené ze statických tabulek – ty jsou dosažitelné snmp příkazy
- **RMON sonda:**
  - oznamuje vyjímky
  - naslouchá promiskuitně LAN
    - statistiky hostitelských systému (MAC adresy)
    - historie pro analýzu trendu
    - statistiky kdo s kým hovorí (pouze v MAC Adresách)
    - zachycování paketu pro statistiku
- v rámci RMON MIB jsou tabulky označeny jako skupiny
- skupina původně definována pouze pro Ethernet
  - *Statistiky* – ukazuje statistiky LAN segmentu, neprochází přes switche
  - *Historie* – ukazuje časové statistiky LAN segmentu
  - *Alarmy* – monitorování jakýchkoli statistik podle MIB, je-li překročena vnitřní prahová hodnota -> RMON událost
  - *Host. systémy* – ukazuje kdo přenáší (pouze MAC adresy)
  - *Prvních N hostů* – kdo přenáší nejvice (pouze MAC adresy)
  - *Matice* – kdo s kým komunikuje (ukazuje pouze MAC adresy)
  - *Filtry* – podle parametrů v paketu (protokol, adresa apod.)
  - *Zachycování* – podle parametrů definovaných ve filtrech
  - *Události* – vznikne při překročení alarm prahu, spojení s akcemi jako logování apod.

8.3 ASN.1 - Abstraktní Syntaktická Notace verze 1

- formální jazyk pro popis strukturovaných dat pro komunikační protokoly distribuovaných systémů
- obsahuje binární data
- velmi úsporný – šetří každý bit (páteřní sítě telekomunikačních oparátorů)
- veškerá data musejí mít definovaný typ – silnější vazby mezi komunikujícími stranami
- využití v jazyce LISP

```
Zaznam ::= SEQUENCE {
      jmeno  PrintableString (SIZE (1..30) )
      vyska  INTEGER
      stav   ENUMERATED { svobodny (0),
                          zenaty(1),
                          rozvedeny(2),
                          vdovec (3)}
      }
```

8.3.1 BER (Basic Encoding Rules)

- základní kódovací pravidla
- reprezentace v bytové formě
- každá hodnota se zapisuje ve struktuře T-L-V => tag-length-value (cedulka-délka-hodnota)
  - cedulka – indikace typu obsahu
  - délka – délka kódovací hodnoty
  - hodnota – vlastní obsah

9 Bezpečnost v sítích, šifrování, otisky, ověřovací schémata a protokoly, ochrana proti útokům typu DoS, DDoS

9.1 Bezpečnost v sítích

- **Počítačová síť – otevřený systém**
  - napadení sítě
  - napadení počítačů
  - odposlech přenášených informací

9.1.1 Způsoby napadení sítě

- **pasivní**
  - odposlech (data, hesla)
  - analýza přenosu (odkud kam, délka, atd...)
- **aktivní**
  - modifikace – změna obsahu, adresy, pořadí atd...
  - zadržování – opožděné posílání zpráv
  - zahlcení požadavky
- **cíle obrany**
  - prevence pasivního útoku
  - detekce aktivního útoku

9.1.2 Ohodnocení bezpečnosti

TCB (Trusted Computing Base)

- úplný obranný mechanismus ve výpočetních systémech
- zahrnuje software, hardware, firmware.
- podpora výrobců spolehlivých OS
- **klasifikace:**
  - *D* – bez zajištění obrany (MS-DOS)
  - *C* – volná ochrana
    - ponecháno na uvážení (UNIX)
    - systémy s ověřováním uživatele
  - *B* – nařízená ochrana
  - *A* – verifikovaná ochrana
    - úplný formální návrh systému

9.1.3 Typy ochran

- **ochrana zdrojů**
  - přístupovou maticí
  - přístupovým seznamem
  - seznamem schopností

- **bezpečná komunikace**
  - zaměření na linku
  - zaměření na koncové uživatele
  - zabezpečení na úrovni spojení
- **ověřování uživatelů** – Kerberos

9.2 Šifrování

- Symetrické šifrování
  - kódování i dekódování využitím pouze 1 klíče (DES, AES, IDEA).
- Nesymetrické kódování (př. SSL)
  - využití 2 klíčů - 1 klíč je veřejný a druhý je tajný
  - veřejným klíčem je zpráva kódována a privátním klíčem se provádí dekódování

9.3 Otisky

- zakódovaná zpráva hashovací funkcí (např. MD5) – neexistuje dekódovací klíč
- hashovací funkce – vždy stejná délka (např. 128b)
- neměli by se vyskytnout dva stejné otisky
- k poslané zprávě se přiloží její zahashovaná varianta – **Otisk**
- pokud zprávu někdo změní, otisk bude jiný

9.4 Ověřovací protokoly

- **Kerberos**
  - symetrické šifrování
  - centralizovaná databáze uživatelů
  - základem je ověřovací server
- **SSL (Secure Socket Layer)**
  - asymetrické šifrování
  - ověřování certifikáty
- **SSH (Secure Shell)**
  - protokol pro vzdálenou správu
  - šifra využitím relačního klíče (RSA
- **IPSec (IP security)**
  - zabezpečení na síťové úrovni
  - ověřování původu
  - transparentní a přizpůsobivý
  - režimy činnosti
    - transportní – mezi koncovými uživateli, vložení AH (auth. Header) mezi IP header a data
    - tunelový – mezi dvěma síťovými prvky, celý packet se obalí novým

9.5 DoS, DDoS útoky a ochrana

9.5.1 DoS (Denial of Service)

- založeny na přetížení systému -> omezení výkonnosti serveru nebo úplný výpadek
- zaměřen na síťové komponenty nebo na hostitelské systémy
- ztlumení skutečného provozu „odpadním“ provozem
- **SYN Flood**
  - zahlcení SYN požadavky
- **Smurf Attack, Fraggle Attack**
  - velké množství ICMP echo paketů na broadcast adresu s falešnou zdrojovou adresou
  - zdrojová adresa (cíl útoku) je zaplavena odpověďmi
  - Fraggle Attack – použití UDP paketů
- **Ping of Death**
  - nelegální ICMP echo pakety delší než 65536 slabik
- **Teardrop**
  - IP fragmentace
- **Application Attack**
  - využití zranitelných míst aplikací

9.5.2 DDoS (Distributed DoS)

- automatizace útoků (skenování obětí, generování seznamu apod.)
- instrukce pro útok umístění přímo do oběti

9.5.3 Ochrana proti útokům

- neuchování stavu dokud se nepřijme ACK
- užití kryptografie
- zachycení na firewallu
- IP metody zpětného trasování
- **Snort (Open Source Intrusion Detection System)**
  - systém pro detekci útoků
  - analýza toku dat v reálném čase
  - informování o útoku v reálném čase

10 Obranné valy, principy, filtrování, architektura, NAT

10.1 Obranné valy – Firewally

- ochrana sítě před síťovými útoky
- odděluje uživatele (nespolehlivý článek) od prvků ochrany
- vlastnosti:
  - filtrování paketů
  - různé úrovně přihlašování
  - transparentnost a přizpůsobení uživatelům
  - rozlišení požadavků dle klientů nebo sítí
- kategorie:
  - filtrování na síťové úrovni (IP filtrování)
  - filtrování na transportní úrovni (úroveň spojení)
  - filtrování na aplikační úrovni (aplikační filtry)

10.1.1 Filtrování na IP úrovni

- analýza paketů a jejich následné filtrování
- filtrovací kritéria
  - IP adresa
  - port
  - typ paketu (IP, jiný)
- aplikační data nejsou filtrována
- bezestavové filtrování
- nejsou k dispozici údaje o spojení klient/server
- nezávisle filtruje přicházející pakety a odcházející pakety
- výhody
- transparentnost
  - podpora libovolného protokolu
  - není třeba modifikovat klienta ani sevrver
- vysoká propustnost
- nevýhody
- méně bezpečné
  - bezestavové
  - založené na omezeném filtrování
  - slabé ověřování
  - nebrání „prosakování“ IP paketů
- složitá pravidla filtrace

10.1.2 Aplikační filtry

- klient se spojuje s obranným valem, ne přímo se serverem
- na obranném valu umístěn Proxy, který přijímá a kontroluje pakety
- ověřování klienta v širokém rozsahu

- výhody
  - vysoké zabezpečení
    - informace o stavu spojení
    - ověřovací techniky
    - filtrace protokolu klient/server
  - logování a účtování
  - méně složitá pravidla
  - možno rozšířit o cache – pro zachycování často používaných dat (klient nemusí komunikovat přímo se server ale s proxy – rychlejší zpracování)
- nevýhody
  - méně transparentní
    - klient si může proxy uvědomit
    - pro každý protokol speciální proxy
  - náročnost na HW

10.1.3 Filtrování na úrovni spojení

- v zásadě podobné jako filtrování na aplikační úrovni
- odlišnosti:
  - slabší ověřování
  - nezajišťuje filtrování protokolu na úrovni aplikace klient/server

10.1.4 Socks

- tzv. spojky mezi klientem a serverem – klient komunikuje se socks, přenese adresu , port cíle, typ spojení a id uživatele -> socks vytvoří vlastní kanál pro komunikaci se serverem
- model (základní operace)
  - požadavek na spojení
  - nastavení proxy spojení
  - přepínání aplikačních dat
  - ověřování

10.2 NAT / PAT (Network / Port Address Translation)

10.2.1 NAT

- překlad adres 1:1
- statické i dynamické

10.2.2 PAT

- překlad adres N:1
- tabulka překladů na směrovači: lokální adresa – port (náhodný)
- výhody:
  - připojení na 1 IP adresu více počítačů do venkovní sítě (internet), úspora IP adres
  - bezpečnost stanic za tímto NATem
- nevýhody:
  - stanice za NATem nemají přímé spojení do internetu a nemusí fungovat nějaké protokoly

11 Síťové API (sockety, RPC), příklady