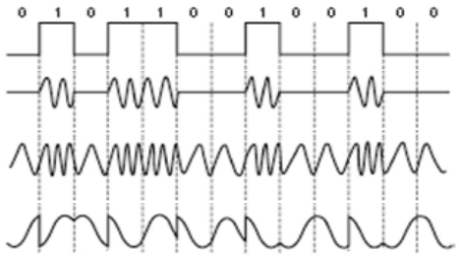
**Dátová komunikačná sieť** je súhrnné označenie technických prostriedkov, pomocou ktorých je realizované prepojenie a výmena dát medzi komunikujúcimi zariadeniami.
**Protokol** je množina pravidiel, ktoré používajú programy, operačné systémy alebo komunikačné zariadenia na komunikáciu medzi koncovými bodmi komunikačného systému.
**Sieťová architektúra** štruktúra riadenia celej komunikácie v sieti, spolu s technickými a programovacími prostriedkami.
**Vrstvový model sieťovej architektúry** reprezentácia štruktúry komunikácie pomocou vrstiev (layers) a k ním prislúchajúcich služieb a protokolov.
**Protokolový zásobník** skupina spolupracujúcich protokolov (jeden, príp. viac protokolov na vrstvu), ktoré riadia celú komunikáciu, ktoré riadia celú komunikáci u medzi uzlami.
**Taxonometria** simplexný / half duplexný / full duplexný prenos, paralelný *(viaceré komunikačné kanáli)*/ sériový prenos *(jeden kanál)*, synchrónny *(presný časový interval)* / asynchrónny *(rôzne časové odstupy)* prenos, analógový / digitálny prenos, spojovo / nespojovo orientovaný prenos, siete s prepájaním okruhov *(najprv je vybudovaná fyzická cesta)* / správ *(centrálny prvok na určenie cesty)* / paketov *(blok dát obsahuje adresnú informáciu),* fixné (metalické /optické) / mobilné siete, rozdelenie podľa veľkosti WAN (*50-1000km, celé štáty*)/MAN *(1-50km, viac LAN)/LAN (10m-1km)/PAN (do 10m),* rozdelenie podľa topológie, siete typu klient-server / peer-to-peer, broadcast (*zdroj→celá sieť*) / multicast *(zdroj→skupina)/* unicast *(zdroj→jednotlivec)* sieť.
**Topológia siete –** zbernica, hviezda, kruh, strom, mriežka, ad hoc
**Služba** – špecifikácia množiny poskytovaných operácií nižšej vrstvy vyššej vrstve
**Vrstvový model sieťovej architektúry -** každá vrstva vykonáva presne definované komunikačné funkcie, každá vrstva má definované rozhranie so susednými vrstvami, vrstvy pracujú podľa definovaného protokolu, vzájomne komunikujúce časti tej istej vrstvy sa nazývajú *rovnocenné (rovnoľahlé) entity* (peers alebo peer entities), každá vrstva vymieňa správy (dáta a riadiace informácie) s rovnocennou (peer) vrstvou na vzdialenom počítači, dáta vymieňané medzi dvoma *peer entitami* (prostredníctvom protokolu) sa nazývajú *protokolové dátové jednotky* (*PDU* Protocol Data Unit)
**Hlavné organizácie pre tvorbu štandardov -** *ISO* (International Standards Organization), *ITU-T* (International Telecommunication Union), *IEEE* (Institute of Electrical and Electronics Engineers), *ANSI* (American National Standards Institute), *IETF* (Internet Engineering Task Force)
**Modely sieťových architektúr –** RM OSI *(pokus o univerzálnu architektúru)*, TCP/IP
**RM OSI –** 7 vrstiev: *fyzická* (prenos a príjem bitov), *linková* (prenos rámcov, oprava chýb, fyzická adresa), *sieťová* (prenos paketov, logická adresa), *transportná* (prenos segmentov, komunikácia medzi koncovými užívateľmi), *relačná* (riadenie relácie), *prezenčná* (interpretovanie dát, konverzia), *aplikačná* (rozhranie medzi programom a sieťou)
**TCP/IP –** 4 vrstvy: *aplikačná* (pripojenie k užívateľskej aplikácii), *transportná* (prenos medzi dvomi koncovými uzlami, protokoly:UDP, TCP), *internetová* (adresovanie, smerovanie v sieti, dáta v blokoch), *sieťová* (transformácia dát a prenos prenosovým médiom)
**Fyzická vrstva**

- **komponenty –** *pasívne* (súčasti na prenos signálu, káble apod.)*, aktívne*(signál generujú/zosilňujú/modifikujú/ distribuujú, transceiver, opakovač)
- **modulácia** definuje, ako sú reprezentované jednotlivé informačné bity
- **synchronizácia –** vysielač a prijímač musia rozpoznať hranice prenášaných znakov
- **multiplexovanie** – viacnásobné využitie spoločného prenosového média, *SDM* (priestorový), *TDM* (časový), *FDM* (frekvenčný), *WDM* (vlnovo-dĺžkový, optika)
- **šírka prenosového pásma** – $f_{min}$ a $f_{max}$ sú hranice skreslenia, ktoré je ešte akceptovateľné, $f_{min}$-$f_{max}$ = šírka prenosového pásma (dvojlinka-GHz, koaxiál-desiatky GHz, optika-THz)
- **linkové kódy –** prispôsobenie signálu na prenos, druhy: *unipolar, NRTZ, manchaster....*
- **modulácie** – *aplitúdová* (2.), *frekvenčná* (3.), *fázová* (4.)
- **modulačná rýchlosť –** počet zmien za sekundu, Baud [Bd]
- **prenosová rýchlosť –** objem dát za čas, bit za sekundu [bps], $v_{prenosova}=v_{modulacna}*\log_2(n)$




- **prenosové cesty –** *pevné* (metalické/optické), *bezdrôtové*
- **vlastnosti prenosových médií –** impedancia [Ω], útlm [dB/m], vlnová disperzia [ns/km], presluch [dB]
- **koaxiálny vodič –** vodič uložený v dielektriku, obalené tienením, typy: *hrubý, tenký*
- **krútená dvojlinka –** skrútené dva vodiče, kategórie: *Cat1-Cat7,* typy: *UTP* (netienený)*, FTP* (tienený fóliou)*, STP* (každý pár tienený)*, SFTP* (tienený fóliou a opletením)*, SSTP* (každý pár tienený, fólia + opletenie)
- **optický kábel –** jadro pokryté obalom s menším indexom lomu, skupiny: *O-,E-,S-,C-,L-,U-band,* delenie: *jednovidové* (jedna cesta, !ohyby)*/multividové* (viacej ciest, !skreslenie)*, skoková* (jednoduchší)*/postupná* (nižší útlm) *zmena indexu lomu*
- **HUB –** preposiela pakety na všetky výstupy
- **krížený kábel –** spojenie žíl 1-3,2-6,3-1,6-2

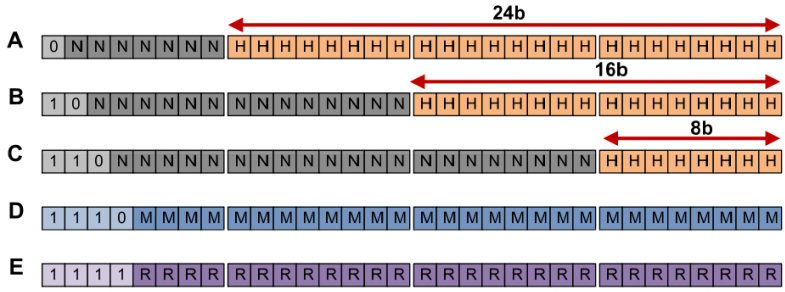
**Linková vrstva**

- **základne funkcie –** využíva služby fyzickej vrstvy, *rámcová synchronizácia* (dáta vysielané v rámcoch), *kontrola chýb* (detekcia a oprava chýb), *riadenie toku dát* (nezahlcovanie pomalších prijímačov)
- **MAC podvrstva –** riadi prístup k médiu *deterministické/stochastické*, fyzické adresovanie, hardvérovo závislá
- **LLC podvrstva –** (de)multiplexácia, riadenie toku, zabezpečenie proti chybám (CRC, parita ….)
- **služby –** *nepotvrdzovaná* (nie je vytvorené log. spojenie), *potvrdzovaná* (úsekové potvrdzovanie prenosu), *potvrdzovaná spojovo orientovaná* (vytvorené log. spojenie, rámce sú potvrdzované)
- **rámcovanie –** veľkosť dátových blokov je obmedzený, segmentácia/fragmentácia, jednoznačné označenie začiatok a koniec rámca, *bit stuffing* (zabezpečenie aby sa v dátach nenachádzalo návestie začiatku rámca)
- **kontrola chybovosti –** *dopredný prístup* (korekčné kódy FEC, Hamming, RS), *spätnoväzbový prístup* (detekcia chýb CRC/parita, riadenie chybovosti vyžiadanie rámca), *hybridný prístup*
- **CRC –** podľa generujúceho polynómu sa vypočíta kontrolný súčet vo vysielači a v prijímači sa kontroluje
- **riadenie chybovosti –** *ARQ* (automatické znovu vyžiadanie), *Stop&Wait* (čakanie na potvrdenie rámca), *Go-Back-N* (v prípade chyby sa vysiela chybný rámec + nasledujúce rámce), *Selective repeat* (po zistení chybného rámca sa vysiela opäť), *Sliding window* (vysiela sa určité množstvo rámcov bez potvrdenia)
- **riadenie toku dát –** zabezpečenie nezahĺtenia, *preventívne metódy, reaktívne metódy*
- **riadenie zahĺtenia –** 3 typy kolízií: *lokálna, vzdialená, oneskorená,* čas vysielania rámca > 2τ
- **CSMA/CD –** metóda prístupu viacerých zariadení, detekcia či niekto nevysiela, ak nie vyšle sa, pri kolízii je vyslaný *JAM signál*
- **CSMA/CA –** vysielač najprv informuje o úmysle vysielať, až potom vysiela
- **CSMA/CR –** každý uzol ma prioritu, pri výskyte kolízie sa určí, kto bude vysielať
- **HDLC protokol –** vznikol z SDLC, metódy prenosu: *ABM* (full duplex, nerušia sa), *NRM* (half duplex, riadiaca stanica určuje kto vysiela), *ARM* (podobne ako NRM, podriadená stanica nečaká na povolenie), formáty rámcov: *I-rámec* (informačný potvrdzovací reťazec), *S-rámec* (rámec na riadenie a dohľad), *U-rámec* (nepotvrdzovaný rámec, zostavenie a zrušenie spojenia)
- **PPP protokol –** podporuje dynamické nastavenie klienta, zabezpečenie pomocou hesla, kompresia prenášaných údajov, využíva U-rámec HDLC, súčasne prenášanie viacero protokolov po jednej linke
- **Ethernet –** prenos údajov medzi 2 bodmi, adresácia pomocou MAC adresy

**Sieťová vrstva**

- 3. vrstva RM OSI, zodpovedá 2. vrstve TCP/IP, využíva logickú adresu, prenáša pakety, zabezpečuje smerovanie
- **IP protokol –** prenos dát sieťou zdroj→cieľ, nespoľahlivé nespojovo orientované, spájanie sietí medzi sebou, prenáša *pakety* (niekedy *datagramy*), *IPv4* (štandard, adresa 32b), *IPv6* (nástupca v4, adresa 128b)
- **IPv4 –** hlavička: *Version* 4b (verzia protokolu), *Header Length* 4b (počet 4B blokov), *Type of Service/TOS* 8b (preferencie prenášaných údajov), *Total Length* 16b (celková dĺžka paketu, max. 65535B), *Idetification* 16b (jednoznačná identifikácia paketu, všetky fragmenty majú rovnaký identifikátor), *Flags* 3b (*DF* don't fragment, *MF* more fragments), *Fragment Offset* 13b (udáva koľko bajtov bolo vložených do predchádzajúcich fragmentov), *Time to live/TTL* 8b (životnosť paketu), *Protocol* 8b (aký protokol je prenášaný), *Header Checksum* 16b (kontrolný súčet hlavičky, nie CRC!), *Sender address* 32b (odosielateľ), *Destination address* 32b (prijímateľ), *Options + padding* max. 320B (voliteľné položky), *Data* (dáta, hlavička + dáta max. 65535B)
- **IPv6 –** rozšírenie adresácie, zmenšenie smerovacích tabuliek, zrýchlenie spracovania paketov, vyššia bezpečnosť, nekompatibilita s IPv4, hlavička: *Version, Header Length, Total Length* (24b), *Identification, Flags* (8b), *Fragment Offset* (8b), *Sender address* (128b), *Destination address* (128b)
- **fragmentácia –** každý fragment má osobitnú hlavičku a je smerovaný nezávisle, pri *total length* je dĺžka fragmentu a nie pôvodného paketu, veľkosť fragmentu podľa *MTU* (Maximum Transmission Unit)
- **ICMP –** prenos chybových a riadiacich správ, hlavička: *Type* 8b (typ správy), *Code* 8b (presné označenie typu správy), *Checksum* 16b (kontrolný súčet), *Data* 32b (doplňujúce dáta)
- **IGMP –** šírenie multicast správ, vždy TTL=1, hlavička: *Type* 8b (typ správy), *MRT* 8b (max. čas odpovede), *Checksum* 16b, *Group address* 32b (adresa multicast skupiny)
- **identifikácia zariadení –** *fyzická adresa* (MAC, jedinečná a unikátna, daná pri výrobe, 1 zariadenie len 1 adresa), *logická adresa* (IP, môže sa meniť, 1 zariadenie viac adries), prideľovanie: *RIPE, ARIN, APNIC*
- **ARP –** IP→MAC adresa, adresy sú ukladané a aktualizované v *ARP Cache*, hlavička: *Hardware type* 16b (typ linkového protokolu), *Protocol type* 16b (typ sieťového protokolu), *Hardware length* 8b (dĺžka linkovej adresy), *Protocol length* 8b (dĺžka sieťovej adresy), *Operation* 16b (operácia), *Sender/Target Hardware/Protocol Address* 48b,32b (linková/sieťová adresa príjemcu/odosielateľa),
- **RARP –** MAC→IP adresa, dnes už nevyužívaný, formát totožný s ARP
- **IP adresácia –** prideľovanie: *staticky* (natrvalo)*/dynamicky* (pri štarte alebo nadviazaní spojenia, DHCP), adresa sa skladá z 2 častí: *adresa siete* a *adresa zariadenia v sieti*

- **Classful addressing –** delenie IP adries do 5 tried, triedy: *A* (0.0.0.0-127.255.255.255, M:255.0.0.0), *B* (128.0.0.0-191.255.255.255, M:255.255.0.0), *C* (192.0.0.0-223.255.255.255, M:255.255.255.0), *D* (224.0.0.0-239.255.255.255), *E* (240.0.0.0-255.255.255.255)




- **Classless addressing –** kvôli nedostatku adries sa prestali deliť na triedy, maska môže mať aj iné hodnoty ako 0 a 255, *subsieť* (maska má viac „1“ ako štandardná maska)*/supersieť* (maska ma menej „1“ ako štandardná maska)

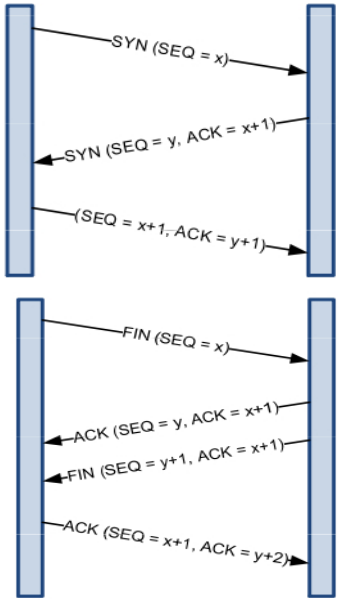
**Internetworking –** základný mechanizmus spolupráce viacerých sietí
**Smerovacia tabuľka –** uchováva adresnú informáciu, podľa ktorej sú pakety smerované, obsahuje len informáciu o nasledujúcom kroku (next hop)
**Smerovací algoritmus –** mechanizmus zodpovedný za rozhodnutia, ktorou výstupnou linkou odoslať pakety, druhy: *algoritmus vektorov vzdialeností, stavov liniek, vektorov liniek*
**Metódy prepínania –** *Store-and-forward* (príjme rámec, vypočíta CRC, detekcia chýb, určí port, odošle), *Cut-through* (analyzuje adresu ešte pred prijatím celého rámca, určí port a odošle)
**Switch (prepínač) –** prepínanie na základe MAC adresy, každý užívateľ má k dispozícii celkovú šírku komunikačného pásma, full duplex, riadenie toku dát, vytváranie záložných trás
**Router (smerovač) –** pracuje s topológiou celej siete, určuje najvhodnejšiu cestu, prepájania sietí: *so spojením* (každá podsieť môže zriadiť virtuálny kanál medzi dvoma koncovými bodmi), *bez spojenia* (datagram je smerovaný od zdroja k cieľu cez viacero smerovačov)
**Smerovanie –** *priame* (paket je smrovaný priamo cez swicth/hub bez použitia smerovača), *nepriame* (paket je smerovaný cez prestupné smerovače), komunikačné protokoly: *smerovateľné* (protokoly určené na prenos dát, ktoré v hlavičke obsahujú adresnú informáciu), *nesmerovateľné* (protokoly určené na prenos dát ale neobsahujú adresnú informáciu), *smerovacie* (určené na zisťovanie najvhodnejšej cesty k cieľu a výmena informácií medzi smerovačmi), smerovanie: *statické* (nakonfigurované manuálne, nevie dynamicky reagovať), *dynamické* (smerovacie algoritmy, pomocou ktorých zisťujú topológiu siete)
**Klasifikácia smerovania –** *neadaptívne/adaptívne (statické/dynamické), jednoduché/viacnásobné, na báze zdroja/hop-by-hop, centralizované/distribuované/izolované*
**Smerovacie protokoly –** zabezpečujú komunikáciu v sieti s inými smerovačmi, implementujú smerovacie stratégie, aktualizujú smerovacie tabuľky, vyhľadávajú najlepšiu cestu pre prenos údajov
**Metrika –** počet hopov, zaťaženie siete, cena, oneskorenie, priepustnosť, šírka prenosového kanálu, vzdialenosť,...
**Autonómny systém –** je skupina sietí a smerovačov, ktorá je pre účely smerovania riadená jednou autoritou
**Vnútorné smerovacie protokoly (IGP) –** smerovanie vo vnútri autonómnych systémov, RIP, IGRP, E-IGRP, OSPF, DVMRP, MOSPF, PIM
**Vonkajšie smerovacie protokoly (EGP) –** smerovanie medzi jednotlivými nezávislými autonómnymi systémami, EGP, BGP, CSPF,...

**Transportná vrstva**

- 4. vrstva RM OSI, komunikácia medzi aplikáciami koncových bodov, *segmenty TCP* alebo *datagramy UDP*
- **port -** číselné označenie SAP, identifikácia aplikačného protokolu, slúži na adresáciu a rozlíšenie konkrétneho komunikačného aplikačného procesu, *známe porty* (0-1023, pevne definované od IANA), *registrované porty* (1024-49151, pre bežné užívateľské aplikácie, registruje IANA), *dynamické/súkromné* (nikde neregistrované), známe: *7* (ICMP), *20-21* (FTP), *22* (SSH),*23* (Telnet),*25* (SMTP),*53* (DNS),*67-68* (DHCP),*80* (HTTP),*110* (POP3),*179* (BGP),*443* (HTTPS),*465* (SMTPS),*995* (POP3S)
- **socket –** jednoznačné určenie komunikačného procesu/služby, pätica: *transportný protokol, zdrojová IP, zdrojový port, cieľová IP, cieľový port,* primitívy: *SOCKET* (vytvor nový), *BIND* (pripoj lokálnu adresu), *LISTEN* (informuj o ochote akceptovať spojenie), *ACCEPT* (akceptuj spojenie), *CONNECT* (nadviaž spojenie), *SEND* (odošli dáta), *RECEIVE* (prijmi dáta) , *CLOSE* (ukonči spojenie)
- **UDP –** nespojovo orientovaný protokol, odosielanie dát bez potreby vytvorenia spojenia, pre služby kde sa nevyžaduje spoľahlivý prenos a pre broadcast (RTP, SNMP, DNS, DHCP, ICMP, RIP, TFTP, BOOTP), hlavička: *Source/Destination port* 16b, *Length* 16b (dĺžka celého segmentu), *Checksum* 16b (nepovinný)
- **TCP –** spojovo orientovaný, spoľahlivý full duplexný prenos, riadenie chybovosti a toku dát, súvislý tok dát po vytvorenom kanále, kanál je identifikovaný socketom, používa sa pre služby ktoré vyžadujú spoľahlivý prenos dát ale nie sú citlivé na oneskorenie (TELNET? FTP, HTTP, ...) hlavička: *Source/destination port* 16b, *Sequence number* 32b (poradové číslo prvého oktetu, náhodné), *Acknowledgement number* 32b (poradové číslo oktetu, ktorý sa očakáva), *Offset* 4b (dĺžka hlavičky), *Flags* 8b (CWR, ECE, URG, ACK, PSH, RST, SYN, FIN), *Window* 16b (počet oktetov bez priebežného potvrdenia), *Checksum* 16b, *Urgent pointer* 16b (posledný

oktet urgentných dát ak URG=1), *Options* max. 320B (doplnkové informácie), *Data* x32b

- **nadviazanie spojenia –** pred začatím prenosu je potrebné nadviazať spojenie (3 way handshake), klient port volí dynamicky, server používa známy port
- **prenos dát –** segmenty sú číslované, prvý segment má náhodne číslo, oba smery majú nezávislé číslovanie, číslovanie od 0 po $2^{32}$-1, zlé segmenty sú znova vyžiadané
- **ukončenie spojenia –** môže iniciovať ktorákoľvek strana




**Relačná vrstva**

- 5. vrstva RM OSI, nezávislá od technológií podsietí a topológie, hlavná funkcia je riadenie relácie, nadviazanie spojenia, spôsob komunikácie, ukončenie prenosu, v TCP/IP je v aplikačnej vrstve, RTP, SSL, TLS...
- **synchronizácia –** vkladanie synchronizačných bodov v prípade výpadku, zabezpečenie (šifrovanie)
- **RTP –** prenos dát v reálnom čase, rekonštrukcia dát v čase, prenos audio a video dát, doručenie segmentov v správnom poradí, umožňuje unicast a multicast, využíva UDP, multiplexovanie viacerých signálov, neposkytuje riadenie chybovosti, riadenie toku dát, hlavička: *Version* 2b (verzia, v2), *Padding* 1b (ak je =1 na konci dát je viacero bajtov výplne na zarovnanie), *Extension* 1b (ak =1 nasleduje aj rozšírená hlavička), *Marker* 1b (označenie začiatku prenášaných dát), *CSRC Count* 4b (počet viacerých zdrojov), *Payload Type* 7b (typ prenášaných dát), *Sequence number* 16b (číselné označenie paketu, detekcia strát), *Timestamp* 32b (čas navzorkovania prvého B v pakete), *Synchronization source identifier* 32b (identifikátor zdroja), *Contributing source Ids* x32b (identifikátory zdrojov ak ich je viac)
- **RTCP –** podporný protokol pre RTP, neprenáša dáta, poskytuje spätnú väzbu o kvalite prenosu, periodické vysielanie riadiacich paketov, zisťovanie počtu účastníkov a rýchlosť odosielania, prenos doplnkových informácií, typy: *SR* (Sender report, kvalitatívne parametre o vysielaní od aktívnych účastníkov), *RR* (Receiver report, kvalitatívne parametre o príjme od neaktívnych účastníkov), *SDES* (popis zdrojov dát), *BYE* (ukončenie komunikácie), *APP* (prenos špecifických informácii aplikácii)
- **komprimovaný RTP** – kompresia v *dátovej časti/hlavičke, CRPT* (pre spoľahlivé dvojbodové spoje), *ECRTP* (pre VoIP a málo spoľahlivé siete s dlhými odozvami)
- **TLS –** šifrovanie dát, nasledovník po *SSL,* využíva TCP, mechanizmy na overenie dôveryhodnosti (autentifikácia): *jednostranná* (len jedna strana, najčastejšie server)/*obojstranná* (aj server aj klient), šifrovanie: dohodnutie algoritmov šifrovania, výmena šifrovacích kľúčov, šifrovanie pomocou kľúčov; možnosti: *asymetrické šifrovanie* (RSA,DSA), *symetrické* (DES,AES,IDE,RC2), *jednosmerná transformácia/hash* (MD5/4/2, SHA1/2), TLS využívajú HTTPS, IMAPS, POP3S, SFTP...

**Prezenčná vrstva**

- 6. vrstva RM OSI, rovnaké interpretovanie rovnakých dát, konverzia, kódovanie znakov, formát číslic, šifrovanie, kompresia
- **ASCII –** kódovací štandard bitovej reprezentácie jednotlivých znakov, každý znak =8b, viacero kódovacích tabuliek: *ISO 8859-2, Windows-1250, CP852, UTF-8/16* (súčasne nahrádza staršie)
- **ASN.1 –** mechanizmus na reprezentáciu dátových objektov aby ich význam bol jednoznačne definovaný, umožňuje: definovať jednotlivé údajové položky, ich typy, prideliť názov

**Aplikačná vrstva**

- **DHCP –** slúži na automatické nastavenie sieťových parametrov, nástupca BOOTP a RARP, server poskytuje klientom sieťové parametre, využíva UDP, server port 67, klient port 68, nastavenie: *IP adresa,maska, gateway, DNS....,* proces získavania: *DHCP DISCOVERY* (žiadosť, broadcast, klient, zisťovanie dostupnosť DHCP serverov), *DHCP OFFER* (ponuka, unicast, server, poslanie voľnej adresy), *DHCP REQUEST* (výber, broadcast, klient, zaslanie vybratej adresy), *DHCP ACK* (pridelenie, unicast, server, konfigurácia aj s časom zapožičania), ešte aj *DHCP NAK/DECLINE/RELEASE/INFORM,* hlavička: *OP* 8b (typ správy), *htype* 8b (typ linkovej adresy), *hlen* 8b (dĺžka linkovej adresy), *hops* 8b (počet uzlov cez ktoré správa prešla), *xid* 32b (identifikácia transakcie), *secs* 16b (počet sekúnd od začiatku transakcie), *flags* 16b (ak najnižší bit=1 odpovede sú broadcast), *ciaddr* 32b (Client address), *yiaddr* 32b (pridelená adresa), *siaddr* 32b (adresa ďalšieho serveru ktorý ma klient použiť), *giaddr* 32b (gateway), *chaddr* 128b (linková adresa klienta), *sname* 512b (meno serveru ktorý ma klient použiť), *file* 1024b (názov súboru ktorý si má klient vyžiadať), *options* (voliteľné polia)

**DNS (Domain name system)**

- preklad IP↔doménové meno, záznamy sú uchovávané v doménových serveroch (*name server)*
- **doména –** skupina názvov uzlov, ktoré k sebe logicky patria, môže byť rozdelená na viac subdomén, úrovne:

*1.* posledná časť doménového mena (.com,.sk), *2.*spravujú registrátori, správcovia národných domén, konkrétny názov domény (google.sk), *3.* spravuje majiteľ domény 2. úrovne, označujú subdoménu alebo uzol (mail.google.sk)

- **typy name serverov –** *primárny server* (uchováva autoritatívne dáta pre danú doménu), *sekundárny server* (záložná kópia primárneho serveru, vždy aspoň jeden), *pomocný server* (uchováva odpovede a opätovne poskytuje, cache), *koreňový server* (záznamy na autoritatívne servery všetkých domén 1. úrovne)
- **vyhľadávanie –** ak klient potrebuje IP adresu obracia sa na lokálny DNS server, ak ju nemá ani on obracia sa na koreňový server, koreňový pošle zoznam autoritatívnych serverov pre danú doménu, lokálny server kontaktuje autoritatívny server; záznam ktorý poskytuje primárny/sekundárny name server je vždy správny
- **reverzné domény –** slúžia na preklad IP→doménové meno, IP adresa sa zapíše v opačnom poradí a pridá sa koncovka *in-addr.arpa*
- **záznamy prostriedkov –** záznamy uložene v autoritatívnych DNS serveroch, údaje: *Domain name, Time to live* (platnosť záznamu)*, Class* (pre internet IN)*, Type, Value* (hodnota záznamu, meno, IP adresa....)
- **DNS záznamy -** *A záznam* **(**obsahuje IPv4 adresu), *AAAA záznam* **(**obsahuje IPv6 adresu), *CNAME záznam* (alias na iné doménové meno), *MX záznam* (meno serveru pre príjem elektronickej pošty a jeho priorita), *NS záznam* (meno autoritatívneho serveru pre danú doménu), *PTR* (záznam pre reverznú zónu), *SOA záznam* (základný záznam definície zónových záznamov), *SRV záznam* (všeobecný záznam, ktorá služba je dostupná na ktorom koncovom zariadení), *TXT záznam* (ľubovolný text)
- **protokol DNS –** používa sa *UDP* (pri žiadostiach o preklad doménových záznamov) a *TCP* (výmena medzi primárnym a sekundárnym serverom), pracuje na princípe otázka→odpoveď, port 53
- **DNS operácie –** *QUERY* (získanie záznamu), *NOTIFY* (pre sekundárne servery o zmene na primárnom serveri), *UPDATE* (aktualizácia záznamov v databáze autoritatívnych serverov)

**WWW (World Wide Web)**

- princíp klient↔server, požiadavky spracované pomocou HTTP protokolu, správa štandardov W3C, protokol: *URL* (jednoznačná identifikácia zdroja), *HTTP* (komunikačný protokol medzi klientom a serverom), *MIME* (popis typu obsahu prenášaného dokumentu), *HTML* (jazyk pre formátovanie hypertextových dokumentov)
- **URI –** syntax zápisu reťazca znakov, používaný na identifikáciu zdroja, formát: <scheme name> : <hierarchical part> [?<query>][#<fragment>], *scheme name* (spôsob prístupu k záznamu), *hierarchical part* (hierarchicky usporiadaná identifikácia zdroja informácie), *query* (voliteľné), *fragment* (voliteľná časť s bližšou identifikáciou určitej časti), zahrňuje: *URL* (identifikácia zdrojov na základe umiestnenia, forma: schéma://užívateľ:heslo@host:port/cesta?parametre#fragment), *URN* (identifikácia zdrojov na základe globálne jednoznačného mena, **urn:nid**(menný priestor)**:nss**(jednoznačný názov vrámci menného priestoru))
- **HTTP –** textovo orientovaný protokol určený na prenos dát, kroky: vytvorenie spojenia, vyžiadanie obsahu, odpoveď servera, ukončenie spojenia, požiadavky: *REQUEST* (požiadavka o zaslanie informácií, *METHOD* (postup zaobchádzania s informáciami), *HEADER* (voliteľná hlavička), *DATA* (doplňujúce informácie)),*GET* (žiadosť o obsah špecifikovaný v URI)*, POST* (žiadosť o spracovanie zaslaného obsahu špecifikovanou v URL, odosielanie formulárov, dáta sú v tele správy)*, HEAD* (žiadosť o hlavičku špecifikovaného obsahu, nemá telo)*, PUT* (nahranie obsahu)*, DELETE* (zmazanie obsahu na strane servera)*, OPTION* (informácie o podmienkach)*, TRACE* (testovacie účely)*, CONNECT,* odpovede: *RESPONSE* (odpoveď na požiadavku), *STATUS CODE* (informácie o type odpovede, 3ciferný identifikátor)*, MIME* (formát prenášaných dát), HTTPv1.1: *multihoming, range request* (požiadavka na časť dokumentu), *chunked data* (dáta zasielané po častiach), *perzistentné spojenie* (keep-alive), *(de)komprimácia dát*
- **proxy –** server slúžiaci najmä na zvýšenie bezpečnosti filtrovaním a kontrolovaním obsahu
- **HTTP server –** web server, zabezpečuje spojenie klient↔aplikácia, predáva externým aplikáciám informácie
- **HTTP klient –** aplikácia schopná nadviazať http spojenie, vyžiadať informácie a následne ich prijať
- **HTTPS –** spojenie SSL/TLS + HTTP, port 443, server musí byť autorizovaný
- **HTML –** značkový jazyk určený na zápis formátových dokumentov prehliadateľné vo webovom prehliadači, navrhnutý pre štruktúrovanie dokumentu (odstavce, tabuľky, zoznamy,...)
- **web** – *statický* (html dokumenty, nie je možná dynamická zmena)/ *dynamický* (obsah html sa mení dynamicky)
- **e-mail –** elektronická podoba klasickej pošty, *MUA* (Mail User Agent, klientský poštový klient, napr.: thunderbird, outlook, eudora), *MTA* (sieťový poštový server, napr.:sendmail, postfix, exim), adresa: *názov_schránky@poštový_uzol;* pracuje na princípe *store and forward*
- **SMTP –** prenos e-mailov medzi stanicami, doručenie správy do poštovej schránky, polia správy: *from, to, cc* (kópia)*, bcc* (skrytá kópia)*, subject*
- **MIME –** doplnenie štandardu SMTP, umožňuje vložiť netextové dáta (obraz, video, zvuk), spôsoby kódovania: *7bit, quoted-printable, base64, 8bit, binary, x-token*, typy dát: *text, multipart* (viac typov v jednom), *message, application, image, video, audio, video*
- **POP3 –** zabezpečuje výber správ z poštovej schránky umiestnenej na MTA, pošta uložená aj u klienta
- **IMAP4 –** umožňuje prístup k správam a manipuláciu s nimi, nedokáže odosielať správy
- **FTP –** umožňuje obojsmerný prenos súborov a obmedzenú prácu so súbormi na serveri, nezabezpečené
- **Telnet –** všeobecný obojsmerný prostriedok komunikácie, emuluje terminál vzdialeného počítača

**Bezpečnosť –** zahŕňa: informovanosť užívateľov, správu prístupových opatrení, sieťovú infraštruktúru, aplikácie a OS, rozdelenie procesu: *prevencia, detekcia, náprava*

- **pojmy -** *utajenie* **(**útočník nerozumiem získaným dátam), *autorizácia* (overenie oprávnenia), *integrita* (dôvera, že dáta neboli pri prenose modifikované), *nepopierateľnosť* (zdroj dát nemôže poprieť odoslanie dát)
- **oblasti zabezpečenia –** *fyzická bezpečnosť* (prístup k systému fyzicky obmedzený len pre oprávnených užívateľov, kľúčová pri riešení bezpečnosti v sieťach), *bezpečnosť OS* (pravidelná aktualizácia, vytvorenie interakcie OS na servery a na klientoch), *bezpečnosť služieb a aplikácií* (odstraňovanie bezpečnostných dier z aplikácií, zabrániť zneužitiu), *bezpečnosť komunikačných sietí* (oddelenie lokálnej siete od vonkajších, filtrovanie (firewall, proxy server), informovanie užívateľov)
- **spôsoby zabezpečenia -** *šifrovanie* (pred prenosom kryptovať dáta tak aby ich nik okrem správneho príjemcu nemohol správne interpretovať, možnosti: *utajiť algoritmus, využitie šifrovacích kľúčov*), *filtrácia komunikácie* (*bezstavová* (paketové filtre)*, stavová* (na základe rekonštrukcie dátových tokov sa robí filtrácia)), *detekcia útokov* (monitorovanie prevádzky, rozpoznávanie podozrivých vzorov komunikácie, )
- **symetrické šifrovanie –** *zdieľaný* kľúč, šifrovanie a dešifrovanie sa robí rovnakým kľúčom, DES, 3DES, AES
- **asymetrické šifrovanie –** existuje *verejný* a *privátny/súkromný kľúč,* odosielateľ aj príjemca majú vlastnú dvojicu kľúčov, dáta šifrované verejným kľúčom je možné rozšifrovať len privátnym kľúčom, RSA, Diffie-Hellman
- **možnosti šifrovania –** *linková vrstva* (tunelling), *sieťová vrstva* (nezávislé na prenosovom médiu aj na použitých protokoloch vyšších vrstiev, IPSec), *relačná vrstva* (SSL, TLS, SRTP), *prezenčná* a *aplikačná vrstva* (šifrovacie algoritmy DES,AES)
- **firewall –** zariadenie (aplikácia), ktoré slúži na riadenie a zabezpečenie sieťovej prevádzky, podľa *ACL* (pravidlá aplikované na jednotlivé sieťové rozhrania pomocou ktorých sa filtruje) rozhoduje o tom ktorú prevádzku povolí, rozdelenie oblastí: *vnútornú* (chránenú), *vonkajšiu* (nebezpečnú) a *demilitarizovanú* (nezabezpečenú vnútornú) *sieť,* delenie firewallov: *paketové filtre, aplikačné brány, stavové paketové filtre, stavové paketové filtre s kontrolou známych protokolov*
- **VPN –** virtuálne privátne siete, budovanie súkromnej siete s použitím zdieľanej infraštruktúry siete, virtuálne spojenie je tvorené tunelmi, na zabezpečenie sa používa šifrovanie a autentizácia
- **IPsec –** protokol sieťovej vrstvy, vytvára tunel medzi dvoma komunikujúcimi zariadeniami, prevádzka je šifrovaná pomocou 3DES a AES
- **SSL/TLS –** protokoly relačnej vrstvy, poskytujú šifrovaný prenos pre protokoly aplikačnej vrstvy
- **spôsoby útokov –** *man in the middle* (aktívne odpočúvanie medzi dvoma zariadeniami, prevádzka smerovaná cez útočníka)*, eavesdropping/sniffing* (pasívne odpočúvanie komunikácie na spoločnom zdieľanom médiu), *denial of services* (zahltenie servera veľkým množstvom falošných požiadavviek), *zneužitie nedokonalosti protokolov* (využitie nedokonalosti v návrhu protokolov, každé hovno má svoje muchy), *zneužitie slabých miest systému* (využitie bezpečnostných dier aplikácii a OS)
- **útoky na sieťovú infraštruktúru –** *ARP spoofing* (presvedčiť odosielateľa, že IP adrese príjemcu zodpovedá MAC adresa útočníka, robí sa pomocou ping-u s falošnou MAC adresou), *DHCP spoofing* (zaslanie falošnej konfigurácie skôr ako ich zašle dobrý DHCP server), *MAC floding* (v prípade zaplneniu pamäte switchu falošnými MAC adresami sa switch prepne do režimu fail open a preposiela všetko ako HUB)*, port stealing* (modifikáciou tabuľky switchu pomocou zaslania paketu s obrátenými MAC adresami (útočník má MAC adresáta a naopak) je možné odpočúvať komunikáciu), *DNS spoofing* (podvrhnutie modifikovanej DNS správy)