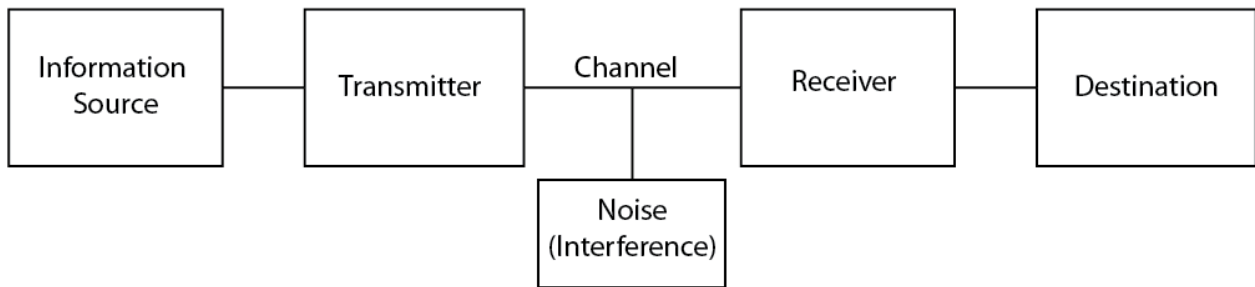


Shannon–Weaveri mudel, ISO-OSI mudel, TCP/IP protokollistik.



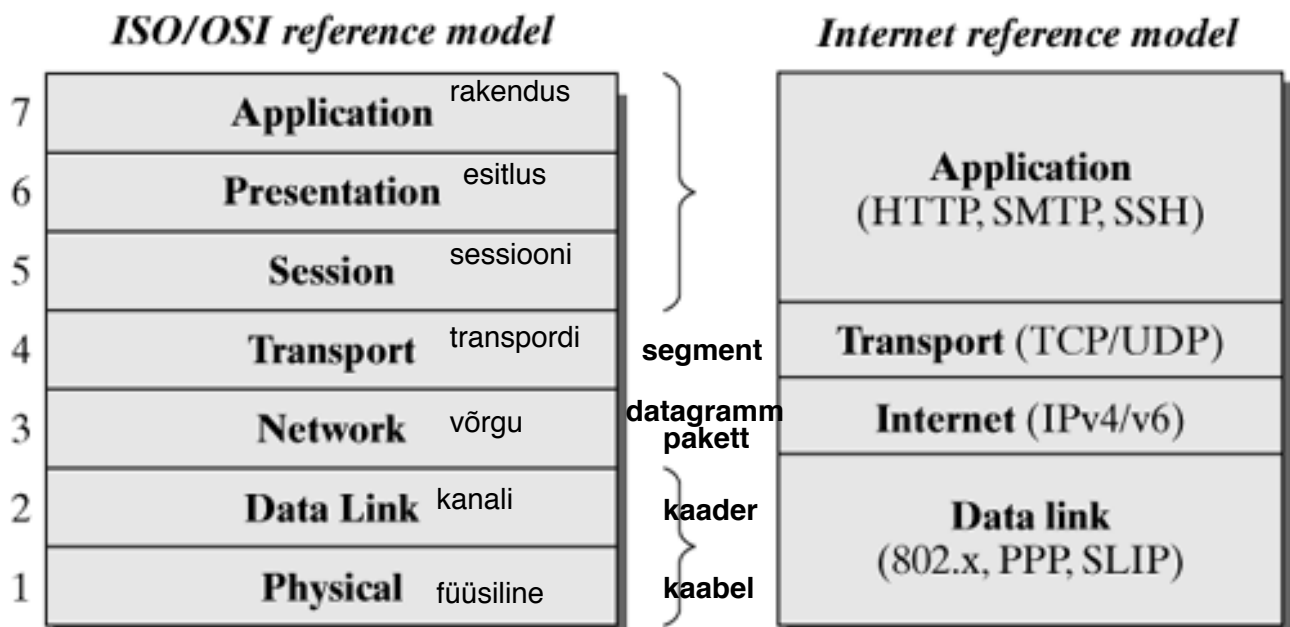
allikas

- A-D muundur - juhul kui on analoogandmed, muudet need digit
- allika kodeerimine - võtab ära kõik ülearuse
- kanali kodeerimine
- modulatsioon - abstraktne digitaalseks

kanal - kuhu tuleb sisse müra

- demodulaator - peab ka müra "ära arvama", digit abstraktseks
- kanali dekooder - paarsusbiti kasutamine
- allika dekooder

sihtkoht



TCP - Transmission Control Protocol lõhub paketid tükkideks ja paneb jälle kokku
IP - Internet Protocol kommunikatsioon arvutite vahel, aadressidega tegeleb

HTTP - Hyper Text Transfer Protocol viib kliendi requestid serverisse ja serverist toob veebimaterjali kliendile

HTTPS - Secure HTTP sama mis HTTP, aga nt kaardimaksete puhul jms

FTP - File Transfer Protocol failiedastus arvutite vahel

Informatsiooni mõõtühikud: bitt ja bait, nende detsimaalliited.

- 1 byte (B) = 8 bits (b)
- 1 Kilobyte (K / KB) = 2^{10} bytes = 1,024 bytes
- 1 Megabyte (M / MB) = 2^{20} bytes = 1,048,576 bytes
- 1 Gigabyte (G / GB) = 2^{30} bytes = 1,073,741,824 bytes
- 1 Terabyte (T / TB) = 2^{40} bytes = 1,099,511,627,776 bytes

bit - b - 0 or 1

byte - B - 8 bits

informatsiooni hulk $I = \log_a = (1 / P)$, kus $a=2$ siis kasutatakse byte ja bit, P on tõenäosus

kõvaketaste ja cd-de tootjad kasutavad 10 astmeid nt KB = 1000 B

Signaali mõiste ja selle erinevad tüübid: audio, pilt, video, tekst, digitaalsed andmed. Pidevad ja diskreetsed signaalid, aja ja väärtuse järgi. Ajalised ja ruumilised signaalid, mitmemõõtmelised signaalid.

signaal on andmete esituseks kasutatava füüsikalise suuruse variatsioon

1D - heli

2D - pilt

3D - video

pidevad (analoog, kogu aeg muutub, müra rikub ära) ja diskreetsed (väärtus omistatakse ainult kindlatel taktidel, müra ei riku eriti) signaalid, digitaalne signaal on selline diskreetne signaal, millel on ainult 2 väärtust - 1 või 0

Elektrilised signaalid, vool ja pinge. Takistus, Oomi seadus.

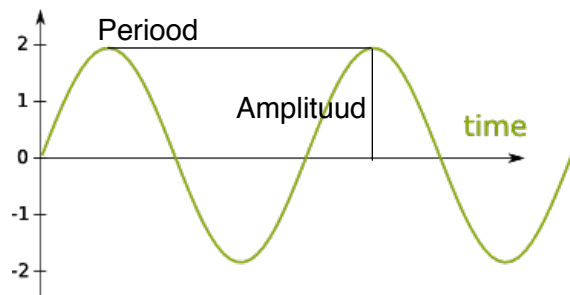
$$U = IR \quad \text{või} \quad I = \frac{U}{R} \quad \text{või} \quad R = \frac{U}{I}.$$

I on ahelaosa läbiva voolu tugevus, mida mõõdetakse amprites (A);

U on pinge, mida mõõdetakse voltides (V);

R on vooluahela lõigu takistus, mida mõõdetakse oomides (Ω).

Siinussignaali, amplituud, sagedus ja periood.



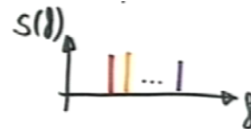
$$f = 1/T \text{ on sagedus (Hz)}$$
$$\omega = 2 * \text{Pii} * f \text{ on ringsagedus}$$

$$s(t) = A * \sin(2 * \text{Pii} * f * t)$$

Peamised signaali parameetrid: võimsus, sagedus ja spekter.
Logaritmilised mõõtühikud, suhtelised dB ja absoluutsed dBm.
Tehted logaritmiliste mõõtühikutega.

p - elektriline võimsus $p(t) = |s(t)|^2$ - ajaühikus ülekantud energia

spekter, parameetrik on sagedus $f = 1/T$ Hz-des
 $B = f_{\max} - f_{\min}$ (riba laius)



Logaritmilisi mõõtühikuid kasutatakse väga suurte ja väikeste suuruste esitamisel nii, et nad nii palju ei erineks.

Suhtelised dB nt SNR mõõtmisel

Absoluutsed dBm detsibelle milliwati kohta (absoluutse võimsuse mõõtmine)

mW saab alati teha dB (valemid paberil) **0 dBm-i on 1 mW**

$$\log(a * b) = \log a + \log b$$

Müra sidekanalis, AWGN müra. signaal- müra suhe SNR. Shannoni valem.

kanali mahutavus:

B on Hz-ides.

$\text{SNR} = S/N$ on kordades.

SHANNONI VALEM

$$\text{SNR} = \frac{S}{N}$$
$$C = B \cdot \log_2(1 + \text{SNR})$$

Additive white Gaussian noise - kasutatakse infotehnoloogias looduses esineva suvaka müra matkimiseks

Allika kodeerimine, entroopia mõiste, kadudega ja kadudeta kodeerimine: kompreseerimistegur (code rate) ja liiasus, kompressiooni-moonutuse suhe (rate-distortion function).

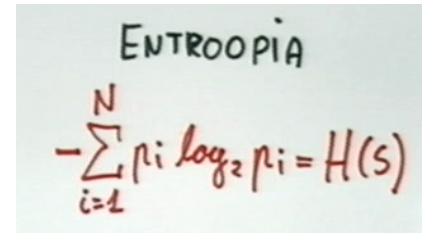
Soovime eemaldada võimalikult palju ebavajalikku infot, et kasutada võimalikult hästi ära kanali suutelisust.

Allikas S on n sümbolit, mille igal sümbolil on tõenäosus p_i .

Entroopia on juhuslikkuse määr, minimaalne info hulk, mis on vaja üle kanda, et info kadudeta jõuaks. Lühemaks kui entroopia ei saa koodi muuta.

Koodi keskmine pikkus $R = p_i \cdot n_i + \dots$

Liiasus - $L = R - H$

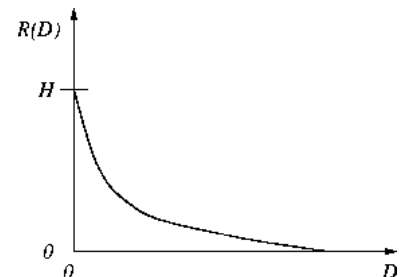


ENTROPIA

$$-\sum_{i=1}^N p_i \log_2 p_i = H(S)$$

Kui on olemas liiasus (rohkem infot kui entroopia), on tegu kadudeta kodeerimisega.

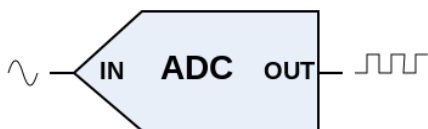
Kui kantakse infot üle vähem kui entroopia, on see kadudega kodeerimine. (me ei saa aru, sest meie enda nägemis- ja kuulmiselundid pole täiuslikud)



kompressiooni-moonutuse suhe \rightarrow

$R(D)$ on kiirus - kui on mega moonutatud, siis ka kiirus on suur.

Analoog-digitaalmuundus, Nyquisti kriteerium, signaali-kvantimismüra suhe, dünaamiline diapasoon. Audio kodeerimine. Psühhoakustiline mudel, MP3, maskeerimise efekt, diferentsiaalne kodeerimine, sigma-delta modulaator.



Sample & Hold - kondensaator (analoogmälu)

Kui kiiresti peab kondensaatori lülitiit avama ja sulgema? **Nyquisti**

kriteerium - kõik info jääb alles, kui avatakse ja sulgetakse vähemalt kaks korda kiiremini kui on signaali maksimaalne sageduses.

Ja siis kvantitakse pinget - pannakse kõrvale joonlaud (diskreetne seade), siis nüüd saab selle pinge panna kirja diskreetsete suurustena.

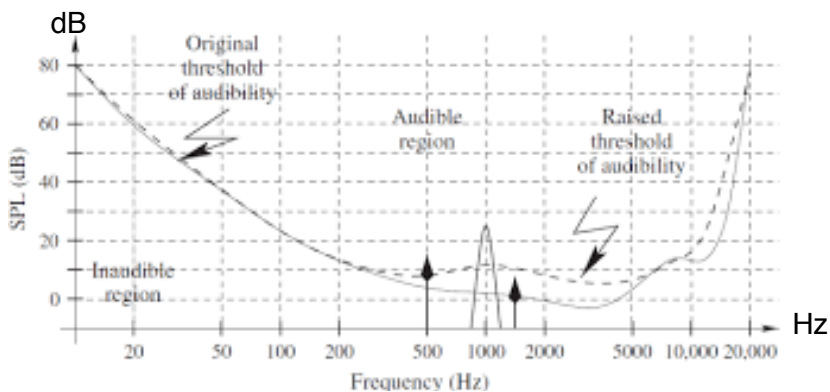
Kvantimismüra on siis kirjapandud ja tegeliku väärtuse vahe.

Signaali ja kvantimismüra võimsuste suhe on $SNR = 6 \text{ dB/bit}$

dünaamiline diapasoon on süsteemi või seadme puhul mingi parameetri lubatud maksimaalse väärtuse ja selle parameetri minimaalse registreerimist võimaldava väärtuse suhe. Nt inimese kõne diapasoon on 70...7000 Hz.

Audiotailide kokkupakkimisel kasutatakse ära inimkõrva puudujääke (Psühhoakustiline mudel) ja eemaldatakse helid, mida inimkõrv nkn ei kuule. Veel kuna kõvem heli katab inimese jaoks

nõrgema heli ära, siis võetakse ka need nõrgad helid välja, mis on kaetud "maskeeritud" tugevama heli poolt. See on maskeerimise efekt.



diferentsiaalne kodeerimine - ei panda kirja mitte signaale endid, vaid nende vahed, mis on väiksemate arvude hulga kirjutatavad.

sigma-delta modulaatorit kasutatakse analog->digital ja ka digital -> analog transleerimisel, samamoodi pannakse kirja signaalide vahed

Teksti kodeerimine. ASCII kood. Muutuva pikkusega kood, Huffman'i kood, sõnastikuga kodeerimine, kontekstipõhine kodeerimine.

ascii kood seab igale tähemärgile vastavusse 7 bitilise binaarkoodi

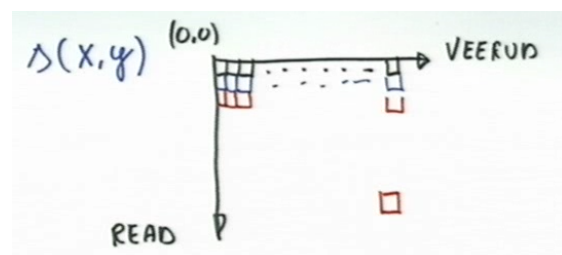
muutuva pikkusega kood on nt Morse kood, kus tihedamini esinevaid sümboleid esitatakse vähemate märkidega.

Huffmanni kodeerimise idee on asendada olemasolev sümboleid kirjeldav bitijada ümber nõnda, et **informatsiooni** hulgas tihedamini esinevad tähemärgid saaksid kirjeldatud lühema bitijadaga.

kontekstipõhine kodeerimine - ennustatakse konteksti põhjal järgmisi sümboleid

Pildi (RLE, DCT, JPEG) ja video kodeerimine (interkaadrid, liikumise kompenseerimine).

Pilt edastatakse pikslitena.
pixel sisaldab infot heleduse kohta,
8 bit sinise heledus,
8 bit punase heledus,
8 bit roheline heledus
000 - must, 444 - tumehall



RLE - run length encoding - rida rea kaupa hea must-valgete piltide puhul, sest kui järjest palju piksleid on nt mustad, ei pea seda ütlema iga piksli kohta, vaid võib öelda, et pikslid nr 10-130 on mustad.

DCT - diskreetne koosinusteisendus - reasignaaside jaoks mõeldud Fourier' teisendus. Arvutab pildisignaali spektri ehk kui kiiresti heledus piki pilti muutub (8x8 matriks tuleb). Ruutudel on koefitsendid. Ebavajalikud koefitsendid visatakse minema, mis võib pildi muuta "ruuduliseks". Jagatakse pilt 8x8 pix ruudukesteks, vasakul üleval suuremad väärtused ja all paremal väikesed, väärtusi skaneeritakse siksakis.

JPEG - kadudega kompressseeritud fail, tehakse DCTga

interkaadrid - video kompressseerimiseks kasutatakse interkaadreid, mis tuletatakse eelneva ja järgneva kaadri põhjal

liikumise kompenseerimine - tuletatakse video liikumine eelneva ja järgneva kaadri liikumise põhjal

Koodeki, multimeedia konteineri ja metafaili mõisted.

koodek - surub heli ja video multimeedia konteinerisse ja ka pakib need lahti

multimeedia konteiner - fail nt avi, kus on nii heli kui ka videopilt

metafail - failitüüp, mis võib endas hoida mitmeid erinevaid tüüpi andmeid, nt graafikafailide puhul nii vektor- kui ka rastergraafikat

ISO-OSI Mudeli füüsiline kiht. Meediumid: Koakskaabel, keerdpaar (UTP, STP, CATx), fiiberoptiline kaabel, raadiokanal.

koakskaabel - faraday puuriga varjestatud juhe, faraday puuris on elektriväli, mis kaitseb sisemist juhet ja selle voolu

vampiiriliides - lõikab koakskaablistse augu, millest läbi võtab "hambaga" voolu. Hiljem hakati kasutama **T-otsikut**.

terminaator - märgib juhtme lõppu, sinna sumbub vool.

keerdpaar - ei kiirga palju välja, sest mõlema keerdunud juhtme ümber keerleb vool vastassuunas

STP - shielded twisted pair (varjestatud)

UTP - unshielded twisted pair (pole varjestatud)

CATx - (UTP) category ja kvaliteedi nr, nt CAT3 on kõige lahjem - telefon; ka internetiühendus, mida suurem nr, seda parem ühendus

fiiberoptiline kaabel - valgus liigub murdudes läbi kaabli, väga väga kiire ühendus, kuid kallis kaabel. Annabki infot edasi on-off valgusega (1-0). Suures kaablis võib tulla ette moonutusi, sest kiirel on mitu teed. Mitu erineva värviga kiirt saab ka korraga läbi minna - kiirus ja mahutavus on suured.

raadiokanal - nt bluetooth, raadio, wifi, ei pea kasutama juhet, vaid läbi õhu lähedavad lained, painduvad Maa kumeruse järgi ja peegelduvad ioniseeritud õhukihilt või satelliidilt. Pealtkuulamise oht!

Asünkroonne andmeedastus. RS-232 liides ja selle põhiparameetrid. Nullmodem, paarsuskontroll.

RS232 on ühenduse standard, mis määrab põhiparameetrid: Kiirus, Andmebitte, Paarsuskontroll, Stopp-bitte, Voo juhtimine.

Null modem ühendab kaks seadet ilma vahepealse modemita kasutades RS-232 liidest.

Korraka vähe bitte: saadetakse startbitt – nüüd hakkab edastus. Siis mõned andmebitid ja siis kontrollbitid.

Paarsuskontroll – kas on paarisarv 1sid või on mõni bitt sassi läinud, võimaldab tabada bitivigu.

Teenindamisest keeldumise tõenäosus, Erlangi valem.

$$P_{\text{keeldumine}} = \frac{\frac{\rho^L}{L!}}{\sum_{k=0}^L \frac{\rho^k}{k!}}$$

Siin $\rho = \frac{\lambda}{\mu}$ tähistab sisendvoo taandatud intensiivsust,
 λ kirjeldab sisendvoogu ja
 μ ühe teenindaja väljundvoogu.
 L on liinide arv

Ethernet, ajalugu ja levinumad standardid: 10BASE5, 10BASE2, 10BASE-T, 100BASE-TX, 1000BASE-T.

Ethernet on juhtmetega kohtvõrgu tehnoloogia, mis vastab Elektri- ja Elektroonikainseneride Instituudi standardile **IEEE 802.3** ja kasutab juhuslikku pöördumisviisi CSMA/CD. Alates 1990ndatest põhiline ja mainstream, odav ja ühilduv. 10 Mbit/s kuni 10 Gbit/s. Robert Metcalfe. Nimi tuleb sõnast "eeter".

10 BASE 5 (10 Mbit/s, -500 m pikkune juhe võib olla) arvuteid saab panna 2,5 m vahega

10 BASE 2 (10 Mbit/s, -185 m pikkune juhe võib olla) kastuab T-kujulist otsikud host-arvutiga ühendamiseks

10 BASE T (10 Mbit/s, T - twisted pair)

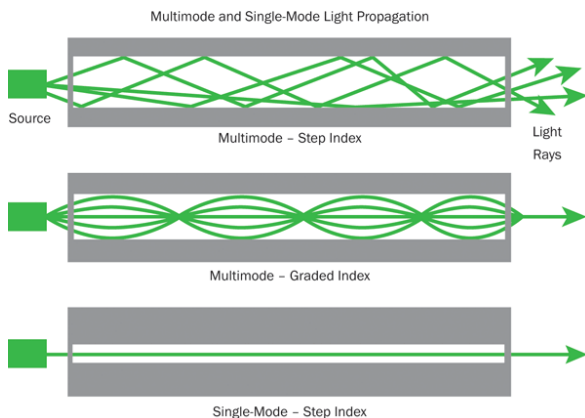
100 BASE TX (100 Mbit/s, T - twisted pair, X näitab versiooni)

1000 BASE T (1000 Mbit/s, T - twisted pair) 1Gbit Ethernet

Fiiberoptilise kaabli ehitus ja tööpõhimõte, mono- ja multimodaalne fiiber, graded index fiiber. Fiiberoptilise kaabli eelised ja puudused, dispersioon fiiberoptilises kaablis.

fiiberoptiline kaabel - valgus liigub murdudes läbi kaabli, väga väga kiire ühendus, kuid kallis kaabel. Annabki infot edasi on-off valgusega (1-0). Suures kaablis võib tulla ette moonutusi (dispersioon), sest kiirel on mitu teed. Mitu erineva värviga kiirt saab ka korraga läbi minna - kiirus ja mahutavus on suured, sumbuvus väike. Ei talu tolmu, võib olla ohtlik paigaldada.

Graded index - murdumisnäitaja muutub sujuvalt ja tekitab vähem moonutust modaalne dispersioon - signaali kuju muutub madalamaks, laiemaks. Kui on graded index v single mode, siis on kiirel vähem moonutust.



Raadiolevi - peegeldused, hajumine ja dispersioon, mitmekiireline levi, feeding, sümbolite vaheline interferents raadiokanalis. DRM - Digital Radio Mondiale ja 802.11 WiFi. Antenn ja selle võimendus dBi, EIRP.

Pigem ühepoolne edastus. Elektromagnetkiirgus. Läbi õhu lähevad lained, painduvad Maa kumeruse järgi ja peegelduvad ioniseeritud õhukihielt või satelliidilt. Pealtkuulamise oht!

feeding - signaali tugevuse kõikumine, signaalid liituvad peegelduste tõttu ja hajuvad

sümbolite vaheline interferents raadiokanalis - kui osa uuest signaalist jõuab vastuvõtjasse ajal, mil saabub alles eelmise signaali lõpp, suurendab vigade tekkimise tõenäosust. Seda põhjustab nt mitmekiireline levi.

mitmekiireline levi - peegelduste tõttu jõuab vastuvõtjani mitu erinevat kiirt

DRM - suure kompressiooni tõttu võimaldab väga hea kvaliteediga heli edastada

IEEE 802.11 Wifi-standard (WLAN) - töökaugus u 100 m. Sagedus 2,4 GHz peal on 13 kanalit. Osaliselt kohakuti, sama sagedus samal ajal mõnikord. Ei sega teineteist, igal jaamal oma kood (CDMA - Code Division Multiple Access).

Antenn võib olla **isotroopne** - igale poole kiirgav, kaugemal muutub signaal nõrgemaks; **raadiorelee** - ühele poole läheb signaal ja väga hea, aga on võimalus tema asukoht tuvastada; **satelliidilt** on samuti võimalik

signaali peegeldada, aga satelliit tuleb panna 36 000 km kaugusele Maast, siis liigub ta Maaga samas tempos ja ei pea antenniga teda otsima.

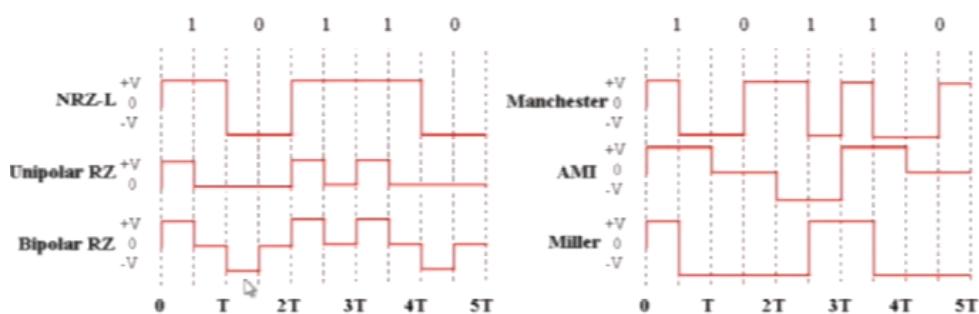
ISO-OSI füüsilise kihi seadmed repiiter, jaotur(hub) ja modem.

repiiter - loeb sisse ja taastab signaali tugevuse seda korrates

jaotur - signaal tuleb ühest august sisse ja läheb mitmest august välja, saadab igale poole edasi

modem - muudab ühe signaali teiseks, et saaks kasutada erinevaid kaableid ja signaale (translaator). Moduleerib, demoduleerib.

Liinikoodid (NRZ, RZ, Manchester, AMI), signaali taastamine.



NRZ - No return to zero: miinusega arv - 0, plussiga arv - 1

RZ - Return to zero: 1 puhul läheb nulli

Manchester - frontidega, 1le vastab langus, 0le tõus.

AMI - 1 vastab vaheldumisi madalale ja kõrgele nivoole

Et tiksumine oleks sünkroonis, on vaja kas saata alg-ja lõppsignaale või siis eraldi signaaliga sünkrosignaale (topelt ribalaius...). Signaali taastamiseks kasutatakse repiiterit koos otsustusnivooga, millest üleval olevad signaalid tehakse 1ks ja all olevad signaalid 0ks.

Modulatsiooni mõiste, modulatsiooniviisid. Amplituud-, sagedus- ja faasmodulatsioon.

Vanasti töötasid modemid läbi telefoniliini ja saatsid signaale helidena.

Modulatsioon on siinusfunktsiooni parameetrite muutmine (kas amplituudi, sageduse või faasi)

Amplituudmodulatsioon - kõrge piiks - 1, madal piiks - 0

Sagedusmodulatsioon ehk sagedustihendus FDMA - ühte kanalisse mitme signaali toppimine, sagedusriba efektiivne kasutamine, nt raadiol saad valida ühe sageduse (jaama), kuigi kõik jaamad on samaaegselt eetris

automatic link establishment - automaatne ühendus kahe lühilaine aparaadi vahel, kasutab nt 8 erinevat sagedust ja saab 3 bitti korraka saata.

faasmanipulatsioon - cos graafik - 1, -cos graafik - 0

Ressursijaotuse viisid: sagedustihendus FDMA (lainepikkuse järgi WDMA), aegtihendus TDMA, koodtihendus CDMA, ruumiline tihendus SDMA.

FDMA - ühte kanalisse mitme signaali toppimine, sagedusriba efektiivne kasutamine.

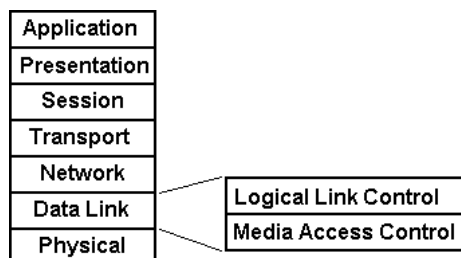
WDMA - ühte kanalisse mitme kiire toppimine valguskaablis.

TDMA - ajapilude kasutamine, hästi pisikesed pilud, kasutaja ei märka, 2G võrkudes.

CDMA - kanali jaotus, kus sama kanalit saavad kasutada mitu saatjat, kasutades erinevaid koode. 3G, GSM, wifi

SDMA - ruumi paralleelne kasutamine (suund, kaugus), nt wifi ruuteril kaks antenni

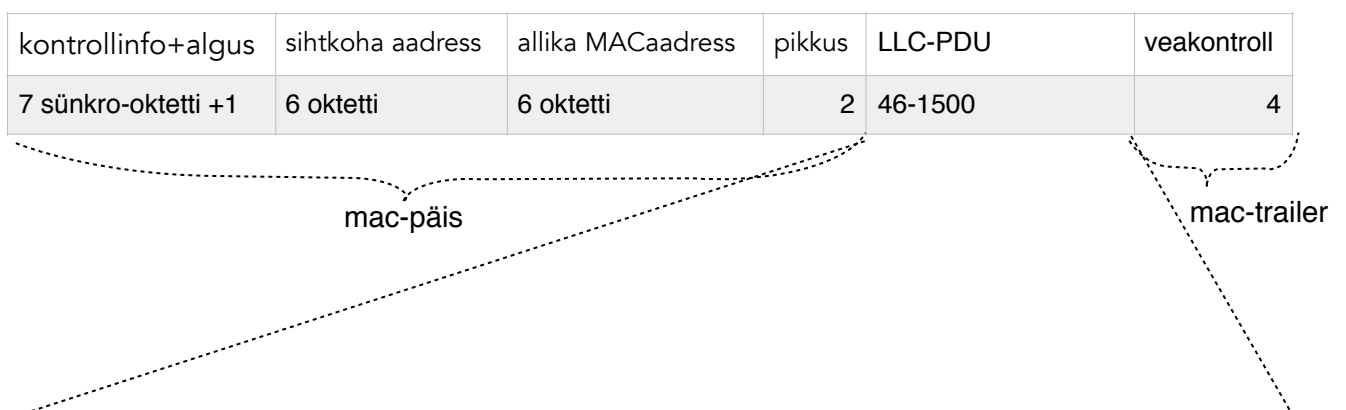
ISO-OSI mudeli kanalikiht. TCP/IP mudeli MAC ja LLC alamkihid. Kanalikihi adresseerimine (MAC aadress) ja põrkedomeenid. MAC kaader, selle struktuur. LLC-PDU. LLC teenuse juurdepääsupunkt (LSAP). Veatu vastus (CRC, FCS). Meediumi jagamine: ALOHA, CSMA/CD. Vookontrolli meetmed: Stop-and-Wait, Sliding Window. Veakontrolli meetmed: Stop-and-Wait ARQ, Go-Back N ARQ ja Selective Reject ARQ.



48bit MAC aadress, mis on igal võrku ühendatud seadmel erinev.

põrkedomeen: võrgu saab jagada põrkedomeenideks (sillaga, repiiteriga, kommutaatoriga). Sild näeb, kust pordist pakett tuli ja kontrollib tabeli abil, kuhu porti peab saatma (kus pordis on saaja MAC), kui ei ole vaja seda edasi saata, siis põrkab pakett tagasi samasse porti. Saab kasutada ka turalisuse eesmärgil (tabelise teha mingi black list)

MAC kaader



LLC-PDU logical link control - protocol data unit - LLC päis + kasutaja info, selle sees allika ja sihtkoha service access pointid,

kontrollbitt	sihtkoha SAP	kontrollbitt	allika SAP	LLC kontroll	informatsioon
1 bit	7 bit	1 bit	7 bit	8-16 bit	

LLC teenuse juurdepääsupunkt (LSAP) - filtreerivad, millise rakenduse jaoks paketid on

Veatuuvastus (CRC, FCS) mingi kontrollsumma, mida kontrollitakse, kui pakett on kohale jõudnud. Nt CRC: tähtedel on koodid, mille summa on antud. Kui koodid on valeks läinud, siis summa enam ei klapi ja teatakse, et on viga.

ALOHA edastad kaadri, millal tahad, ootad kinnitust. Kui kinnitust ei tule proovid uuesti n korda, siis loobud. Kanali kasutus väike.

CSMA kuulad, kas meedium on vaba. Kui on, edastad kaadri. Kui on kinni, ootad suvaka aja ja kuulad uuesti.

CSMA/CD collision detect (möödab pidevalt pinget) kuulad, kas on vaba. Kui on vaba, edastad. Kui pole, kuulad edasi ja kohe kui vabaneb, saadad. Kui on kokkupõrge, alustad uuesti.

Vookontrolli meetmed: Stop-and-Wait (saadab ära ja ootab kinnitust, kui ei tule, saadab uuesti) **Sliding Window** (mitu tk saadetakse korraga, oodatakse kinnitusi. Kui nt 2. paketi jaoks kinnitust ei tule, saadetakse paketid alates 2st uuesti)

Veakontrolli meetmed: Stop-and Wait ARQ (tagasi saadetakse kontrollid Ack1 ja Ack0 vaheldumisi, ootab time-outi ja siis kui pole Acki tulnud v tuli vale Ack, siis saadab vastavalt uuesti), **Go-Back N ARQ** (saadab mitu korraga ja järjest kontrollib Acke, kui mõni on vahelt ära jäänud, saadetakse alates ärajäänud paketist) ja **Selective Reject ARQ** (saadab mitu korraga ja järjest kontrollib Acke, kui üks jääb vahelt ära, siis saadetakse ainult see uuesti, muidu ikka edasi).

Kanalikihi seadmed kommutaator (Switch) ja sild (Bridge)

kommutaator teeb seadmetel MAC-aadresside põhjal järgi, teab, et pordis 1 on arvuti A jne, saadab infot ühelt seadmelt teisele, tagab mitme seadme vahelise üheaegse ühenduse (jaoturis saadetakse sõnum laiali kõigile, kommutaator aga teab, kes kellele tahtis saata)

sild on vähemalt kahe pordiga osa kahe pörkedomeeni (LANi) vahel, tänapäeval on sillaks ikkagi kommutaator. Sild kontrollib, kuhu porti on vaja saata ning ei saada midagi ebavajalikku porti.

Hargneva puu protokoll (STP).

Konfigureeritakse võrku ehk genereeritakse graaf, kus on juursõlm, millel on kindlad juurpordid, kust leitakse optimaalseim tee. Mitteoptimaalsed teed blokeeritakse, kuid neid saab uuesti kasututsele võtta, kui optimaalse teega midagi juhtub. Et ei tekiks kinnist ringi, on samuti

mõned lingid blokeeritud. Konfigureeritakse vanima võrgukaardiga (väikseima MAC-aadressiga) seadme järgi, sest see seab kiiruse piirangu.

Võrkude topoloogiad. Siin- ja tähtvõrk, joon, puu, ring, täielikult ühendatud (Metcalfi seadus ja võrguefekt) ja mesh võrgutopoloogiad. Superarvutites kasutatud "paks puu" ja hüperkuubi võrgutopoloogiad. Võrkude hierarhia suuruse järgi: LAN, MAN, RAN, WAN. Ahel- ja pakett-kommunikatsioon.

siin: probleem - mitu seadet korraga omavahel rääkida ei saa 10BASE2, 10BASE5

täht: kui keskmisega midagi juhtub, on terve võrk katki 10BASE-T

joon: kui ühega midagi juhtub, ei saa ka teised suhelda, raadiorelee

puu: nagu hargnev graaf, paks puu (ülemised "oksad" on paksemad ja nendes ühendus kiirem, sest neist käib läbi kogu liiklus)

ring: kui 1 läheb katki, saab minna ringiga

täielikult ühendatud: kalleim, aga töökindlaim

Metcalfe'i seadus: igasuguse võrgustiku väärtus on võrgusõlmede arv ruudus

mesh võrk: kui 1 on katki, saab teist teed pidi tavaliselt

hüperkuup: suurem kui kolmas dimensioon, mitu kuupi üksteise sees

LAN – local area network, kohtvõrk. Füüsilised mõõtmed paarsada meetrit. Võimalik suurendada vaheseadmetega. Kuulub omanikule, haldurile.

CAN – campus area network. Mõõtmed suuremad, TTÜS 1–1.5 km.

MAN – metropol area network. Leviala kümned kilomeetrid. Palju kasutajaid.

RAN – rural area network. Paikneb nt maakohtades, kus on asustus hõre. Vähe kasutajaid, suur ala.

WAN – Wide Area Network – suurim – terved kontinendid, Maa (pm Internet). Ei kuulu kasutajatele endale.

ahelkommunikatsioon: ühendus luuakse ainult edastuse ajal, kanalit pole kogu aeg olemas (nt telefoniühendus), peab maksma ainult kasutatud aja eest.

pakettkommunikatsioon: kuni 1 MAC-kaadressisse pakitud pakett liigub, on meedium hõivatud, kohe kui ta enam ei liigu, on meedium vaba. Võib luua virtuaalse kanali või visata (datagrammide puhul).

ISO-OSI võrgukiht ja TCP/IP internetikiht. Protokollid IPv4, IPv6. DHCP, ARP ja NAT. IP- aadress, aadresside klassid, CIDR ja võrgumask, privaatvõrk, multicast ja leviaadress (broadcast).

võrgukiht kasutab pakettkommunikatsiooni, adresseerib sihtkohta IP aadressiga, edastab datagramme.

internetikiht valib järgmise sõlme saatmisel, fragmenteerib datagrammi ja edastab selle kanalikihile,

IPv4 aadress (32 bitti) esitatakse kümnendarvu kujul: 172.16.254.3

IPv6 aadress (128 bitti) esitatakse kuueteistkümnendarvudena:
2001:db8:85a3:0:0:8a2e:370:7334

DHCP dynamic host configuration protocol – kleindi-serveri vaheline protokoll, kui võrku ühendatakse uus seade annab kohe talle ühe vabast IP aadressidest, ei pea ise midagi konfigureerima.

ARP – address resolution protocol – arvuti saadab kaadri kõikidele arvutitele küsimuse, kellele kuulub vastav aadress. Vastav arvuti vastab oma MAC-aadressiga. ARP jätab mingiks ajaks MAC aadressid meelde.

NAT – network address translator. Mitmel masinal võib olla sama IP aadress, NAT translaator muudab seda üldaadressi masina enda aadressiks ja vastupidi

Võrguaadresside klassid:

- **A** – standartne/algne. võrgu määrab esimene bait
- **B** – võrgu määravad kaks esimest baiti
- **C** – võrgu määravad kolm esimest baiti, neid on palju
- **D** – **multicast** edastuseks – ühelt aadressilt kõigile, kes tahavad
- **E** – mõeldud tulevikurakendustele, katsetamiseks.

Klass	Esimesed bitid	Võrgunumber bittides	Ülejäänud bitid	Võrkude arv	Aadressi võrgus	Aadressi klassis	Esimene aadress	Viimane aadress
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	2,147,483,648 (2^{31})	0.0.0.0	127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	1,073,741,824 (2^{30})	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	536,870,912 (2^{29})	192.0.0.0	223.255.255.255
D	1110	-	-	-	-	268,435,456 (2^{28})	224.0.0.0	239.255.255.255
E	1111	-	-	-	-	268,435,456 (2^{28})	240.0.0.0	255.255.255.255

broadcast – paketi edastamine kõigile võrgu arvutitele

Tänapäeval on klassideta võrk **CIDR**, kus saab aadressi piire nihutada, piiri nägemiseks kasutatakse **võrgumaski** – nagu sõel, mis laseb läbi ainult seda, mida parajasti vaja on. Mask on 1-de ja 0-de jada, kus 1 on auk (tuleb läbi) ja 0 ei lase läbi.

Privaatvõrk – kolm aadressivahemikku privaatkasutuseks (nt firmasisese interneti jaoks), aga arvuti ei tohi olla marsruuter välisesse võrku

- 10.0.0.0 – 10.255.255.255 (üks A klassi võrk)
- 172.16.0.0 – 172.31.255.255 (16 B klassi võrku)
- 192.168.0.0 – 192.168.255.255 (256 C klassi võrku)
-

Võrgukihi analüüsivahendid ICMP (ping) ja traceroute.

ping käsk saadab paketi teele ja ootab vastust, saab teada, kas võrgusõlm töötab ja kaua läheb aega vastuse saamiseks erinevate pikkustega pakettide puhul.

traceroute töötab nagu ping, aga näitab kõigi marsruuteriteni jõudmiseks kulunud aega eraldi.

Võrgukihi seadmed: marsruuter, tulemüür.

marsruuter ehk default gateway on seade kahe võrgu vahel, leiab õige tee ja saadab andmeid edasi.

tulemüür ehk firewall on turvaeesmärgiga seade sise- ja välisvõrgu vahel, mis piirab liiklust andmetele, mis ei peaks sealt läbi liikuma. Piirab suvalise Interneti kasutaja sisenemist sisevõrku/kohtvõrku. Võib olla riistvaraline, tarkvaraline või mõlema kombo.

IP-datagramm ja selle päis. Paketi eluiga TTL.

	okt	0								1								2								3							
okt	bitt	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Versioon				IHL				DSCP				ECN				Kogupikkus															
4	32	Identifitseerimine																Lipud				Fragmendi nihe											
8	64	TTL								Protokoll								Päise kontrollsumma															
12	96	Saatja IP aadress																															
16	128	Sihtkoha IP aadress																															
20	160	Valikulised väljad (kui IHL > 5)																															

versioon: mis internetiprotokoll? IPv4, IPv6

IHL: internet header length, millal päis lõpeb ja andmed algavad

DSCP: different service code point, mis teenus

ECN: valikuline, annab teada, kui on tekkinud ummik

kogupikkus: kui pikk on päis + andmed baitides

identifitseerimine: vajalik, kui on fragmenteeritud, et oskaks jälle kokku tagasi panna

lipud: ühebitised muutujad (1 v 0) nt DF (don't fragment, kui vajab lõikumist, ei saadeta üldse), MF (more fragments, ehk see pole viimane fragment)

fragmendi nihe: esimesel seda pole, muul juhul näitab kus kohas reaalses pakettis asub konkreetne fragment

TTL – time to live (lubatud hüpete ehk edasisaatmiste arv), kui see läbi saab, ei saadeta seda paketti enam edasi, see piirab pakettide vohamist, et nad ei ringleks võrgus igavesti ja ei koormaks seda

protokoll – mis kõrgema kihi protokollid on datagrammis (ICMP, UDP, TCP, AX.25)

päise kontrollsumma – vigade tuvastuseks

Marsruutimine võrgus. Fikseeritud, üleujutamine, juhuslik ja adaptiivne marsruutimine. Minimaalse kuluga marsruutimine ja Dijkstra algoritm.

marsruuter ehk default gateway on seade kahe võrgu vahel, leiab optimaalseima tee ja saadab andmeid edasi.

fikseeritud marsruutimine - on teada kogu info võrgu kohta, mis on esitatud tabelis. Read ja veerud vastavad saatja ja saaja aadressile. Nende ristumispunktis on "õige tee".

üleujutamine - pole vaja nii palju inffi võrgu kohta. Kui tuleb sõlme pakett, siis ta saadab selle kõigile edasi, v.a. see, kust ta tuli. TTL tõttu ei ringle paketid igavesti.

juhuslik marsruutimine - valitakse marsruut juhuslikult, ei vaja palju infot võrgu kohta, ei leia tavaliselt kohe optimaalseimat teed, ei tuvasta võrgumuutusi

adaptiivne marsruutimine - tuvastab võrgumuutusi, teab ootejärjekordi ja lävesid

minimaalse kuluga - marsruutidel on "hinnad", leitakse vähima hinnaga tee

Dijkstra algoritm: iga sõlme koguhinna leidmiseks

```
for each sõlm u{  
    for each sõlm v{  
        if (v on u kõrval){  
            koguhind = u ja v vaheline hind;  
        }else{  
            koguhind = lõpmatus;  
        }  
    }  
}
```

Transpordikiht ja selle funktsioonid usaldusväärse ja ebausaldusväärse võrguühenduse korral. TCP protokoll. TCP segment ja TCP port. Vookontroll, libisev aken (parameetrid, ISN, SN, AN, W). TCP olekumasin. Ühenduse loomine ja katkestamine. Segmentide järjestamine, retransmissioon, duplikaatide tuvastamine. Võrgu ülekoormusele reageerimine.

Ülesanded:

- kujuteldava otsekanali loomine kahe masina vahel
- ühenduse alustamine ja lõpetamine (SYN, FIN)
- adresseerimine (pordid)
- segmentide õige järjekorra tagamine
- vookontroll
- usaldusväärse ühenduse loomine (ACK lipud, puuduvate segmentide uuesti saatmine kasutades taimerit, NACK lippu, segmentide kontrollsumma, kolmekordne käesurumine(saadetakse SYN, oodatakse vastu ACK-SYN, saadetakse kinnituseks veelkord ACK))

- multipleksimine
- peab avastama duplikaadid jrk järgi ja siis ühe neist kustutama

Saadetakse segmente, millel omaette päis. Pordi järgi saab teada, millise rakenduse jaoks segment mõeldud on. Protokollid on TCP (ühendusega) ja UDP (ühenduseta)

	okt	0								1								2								3							
okt	bitt	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Allika port																Sihtkoha port															
4	32	Järjekorranumber																															
8	64	Kinnituse number (ACK)																															
12	96	Päise pikkus				0 0 0				N	C	E	U	A	P	R	S	F	Akna suurus														
										S	W	C	R	C	S	S	Y	I															
										R	E	G	K	H	T	N	N																
16	128	Kontrollsumma																URG viit															
20	160	Valikulised väljad (kui Päise pikkus > 5)																															

lipud SYN - ühenduse alustamine, **ACK** - sain segmendi kätte, **FIN** - ühenduse lõpetamine **URG** - urgent, **RST** - reset, **PSH** - push

vookontroll - peab tagama andmete kohale jõudmise ja et ei tekiks ummik või ülekoormus

libiseva akna meetod: mitu segmenti saadetakse korraga, segmendid on nummerdatud, kui mõni ei jõua kohale, saadetakse see uuesti - see võib põhjustada pakettide saabumise vales järjekorras ja seetõttu vajatakse järjekorranumbreid

AN - mis nr on järgmisel segmendil

SN - praeguse segmendi nr

ISN - esimese segmendi nr

W - akna suurus ehk palju on saaja valmis infot vastu võtma. Rohkem pakette ei tohi saata. Niiõelda krediidi jaotuse süsteem: kui saadetakse andmed välja, läheb aken kitsamaks, kui saadakse kinnitus, läheb aken jälle suuremaks. Ülekoormuse ohu korral (kiirus väheneb, võrk umbes) lükatakse aknend vägisi väiksemaks, et vähem pakette saadetakse.

Final State Machine - TCP olekumasin on viis süsteemi kirjeldamiseks. põhiolek on "established". osapooled on active open (initsialiseerib ühenduse, saadab lipu - tavaliselt klient) ja passive open (kuulab, ootab, vastab - tavaliselt server)

UDP protokoll, UDP datagramm ja selle päis.

UDP on sarnane TCPga, aga pole nii veakindel (pakette võib kaduma minna), aga samas kiirem. Ühenduseta protokoll. Avastab vigu, kuid ei paranda neid, ei tegele võrgu ülekoormusega, datagramm lühem kui TCP oma, päis sisaldab sihtkoha ja lähtekoha IP aadresse, kontrollsummat ja segmendi pikkust.

Küberturvalisuse mõiste.

Oma riist- ja tarkvara kaitsmine andmete kahjustamise ja varguse eest.

Pahavara ja selle liigitus: viirus, uss, troojalane, tagauks, käomuna.

viirus: nakatab faile, paljundab ennast ise, kui on sattunud masinasse

uss: iseseisev tarkvaratükk, mis teeb halba

troojalane: tundub nagu hea asi, ise installeerid, tegelikult on uss v viirus

tagauks: mingi auk on süsteemile sisse jäetud, mis alguses välja ei paista, aga hiljem võib anda kurjamitele ligipääsu sinu süsteemile

käomuna: kõige halvem, administraatori õigustega tarkvaratükk masinas, mis saab ise pahavara installida

Levinumad rünnakute viisid: pealtkuulamine, spoofimine, õngitsemine, klikkide kaaperdamine, DoS rünnak ja selle võimendamine.

pealtkuulamine - pildi kuvamine rida rea haaval toodab raadiosignaale, mida on võimalik antenniga kinni püüda. Peab kasutama segajaid.

spoofimine - võltsitakse porti või IP aadressi

õngitsemine - nigeeria kirjad, abipalved, vale aadress on pandud lingile

klikkide kaaperdamine - kasutaja meelitatakse kuskile klikkima (download/next nupud nt)

DoS - denial of service; aetakse süsteem umbe nt hakatakse saatma 2GB paketti kiirusega 1 bitt minutis või trükkima järjest musti lehti (must faks), saadetakse suvakatelt portudelt SYN signaale nii palju, et arvutil pole enam võimalust ühendada, pannakse liiga suur pakett teele (surmav ping)

smurfi rünnak - DoSi võimendamine, saadetakse pakett kõigile võrgu arvutitele, saatja aadressiks ohvri aadress. Tagasiside saadavad kõik võrgu arvutid ohvri arvutile. Rünnak tuleb paljudest masinatest korraga ja mitte ükski neist pole ründaja oma.

domain name service - saadetakse päring, saatja aadressiks ohvri aadress, mille vastus on päringust sada korda pikem

network time protocol - küsitakse kella kogu aeg internetist

Kaitsemeetmed: tulemüür, proksi, NAT.

tulemüür ehk firewall on turbaeesmärgiga seade sise- ja välisvõrgu vahel, mis piirab liiklust andmetele, mis ei peaks sealt läbi liikuma. Piirab

suvalise Interneti kasutaja sisenemist sisevõrku/kohtvõrku. Võib olla riistvaraline, tarkvaraline või mõlema kombo.

proksi: puhverserver, mis kontrollib sisenevat andmevoogu, pahalane ei jõua sinu arvutini, vaid ainult puhvrini

NAT: sõel, mis ei näita sinu tegelikku IP-aadressi internetti välja

Krüpteerimine ja autentimine. Krüpteerimine ja krüptoanalüüs. Räsifunktsioon (hash). Sümmeetriline ja avaliku võtmega krüpteerimine, autentimine, digitaalallkirjastamine. IPsec ja SSH.

krüpteerimine - andmete salvestamine ja edastamine viisil, mis tagab juurdepääsu vaid valitud inimestele

autentimine - kaitseb spoofimise, andmete muutmise vastu, krüpteerimine on hea viis autentimiseks, kuid alati pole see tõhus, sest võtab liigselt ressursse

digiallkirjastamine - krüpteeritakse teade salajase võtmega ja dekrüpteeritakse avaliku võtmega. autentitakse, et kasutaja oleks ikka ID kaardi omanik

krüptoanalüüs - algse teksti või krüptovõtme välja mõtlemine ilma võtit teadmata

räsifunktsioon - suurte andmebaaside ja pangaparoolide kaitsmiseks, praktiliselt võimatu lahti murda, sekstistringide kodeerimine

krüpteerimisel on kaks algoritmi: **sümmeetrilised** (salajase võtmega, võtit kaasa ei panda, kellel võti teada, saab alati infole ligi) ja **avaliku võtmega** (asümmeetrilised, krüpteerimisel ja dekrüpteerimisel kasutatakse eri võtmeid, nt kõik saavad avaliku võtmega krüpteerida, aga lahti teha saab ainult see inimene, kellel on salajane võti)

IPsec: võrgukihis töötav IP turvalisuse tagamiseks loodud protokollistik, mis krüpteerib, autentib, kooskõlastab algoritme

SSH: secure shell, krüpteerib ühenduse, turvakest HTTP -> HTTPS

Traadita kohtvõrk 802.11 (Wi-Fi) ja selle turvalisuse tagamine WEP ja WPA.

wifi liiklust peab krüpteerima, sest see on kergelt pealt kuulatav

WEP: -2003, kasutab 64 v 128 bitiseid võtmeid, ei tohiks kasutada ruuteris

WPA: alates 2003, kasutab 256 bitiseid võtmeid, efektiivseks toimimiseks vaja kasutada vähemalt 13 sümbolilist parooli, WPA2 alates 2004 ja selle vastu pole teada ühtli rünnakut, samuti toetab uuemat riistvara

Hajaspektriside. Sagedushüplemine (FH-SS) ja otsene sageduse hajutamine (DS-SS). Juhuslikud binaarsed jadad, M-jadad ja nende genereerimine. Ortogonaalne sagedustihendus OFDM.
Rakendused: GPS, IEEE 802.11 Wi-Fi, Bluetooth.

Hajaspektriside: määratakse spekter laiali mööda kanalit (kas otsese hajutamise või sagedushüplemisega), kasutatakse CDMA-d, see vähendab häirivusi, saab mitu sidepidajat kanalit korraga kasutada. Shannoni piir ($B/C = 1/2$, kus vigadeta edastus on veel võimalik) on palju suurem ühest $B/C \gg 1$

Otsene sageduse hajutamine: hajutav jada pannakse kohe kanali kooderi otsa, hajutatud sõnum viiakse kandesignaali generaatorisse.

Sagedushüplemine: isemängiv klaver (M-jada), mis järjest muudab sagedusi, millel saatmine käib, vähendab pealtkuulamist. Hajutav jada pannakse kandesignaali generaatori külge ehk õget sõnumit saadetakse hajutatud kanalil.

M-jada ehk pseudojuhuslik: mürataoline, kasutatakse nihkeregistrit, luuakse deterministlikult, entroopia võimalikult suur

Ortogonaalne sagedustihendus: laiaribalist digitaalsignaali (nt teleka) saadetakse osadekaupa paljudel lähestikku olevatel abisagedustel, need sagedused peavad olema omavahel risti (faasinihe 90°) ehk ortogonaalsed. et kõrvutiolevad signaalid üksteist ära ei kataks

GPS: satelliidid edastavad erinevaid signaale, neli tükki peab olema kogu aeg nägemisulatuses, et asukohta määrata nende ristumispunkti järgi

IEEE 802.11 Wi-Fi: ortogonaalne sagedustihendus, ruuteril mitu antenni (SDMA)

Bluetooth: sagedushüplemine

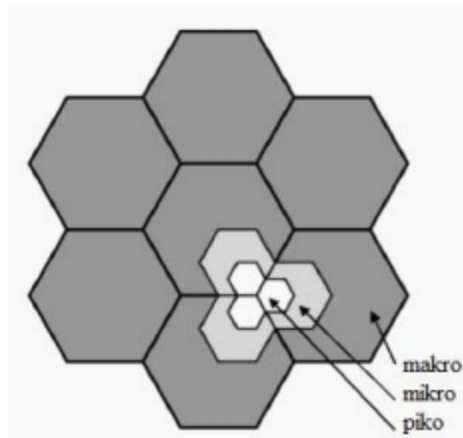
Mobiilside, kärgvõrgud, sageduste taaskasutus, kärgede jaotamine.

1 mast suure maa ala peal ei tööta hästi, sest see ei taluks kogu liiklust, signaal harjuks ja signaal ei paindu üle mägede, orgude ja Maa kumeruse.

Kärgvõrgud – kärjekujuliselt kaetakse ala mastidega, nende sagedused on kõigil erinevad

Sageduste taaskasutamine: pannakse järjest kärgedele sagedused nii, et ükski sarnane ei satuks kõrvuti (ei puutuks kokku)

Kärgede jaotamine: tihedalt asustatud kohtades tehakse kärjed omakorda väiksemateks kärgedeks ja pannakse iga kärje keskele taaskord pisike mast



Mobiilside standardid. Esimene põlvkond 1G NMT, 2G GSM, GPRS, EDGE, 3G UMTS (W-CDMA).

1G NMT: nordisk mobiltelefon, 80ndad, esimene täisautomaatne analoogmobiilseade, $B=25\text{kHz}$, kärje raadius 2...30 km, raadiokanaleid 180 tükki, mis oli vaja ära jagada kärgede ja operaatorite vahel, FM sagedused, lihtne oli pealt kuulata

2G GSM: global system for mobile communications, 90ndad, esimene täisdigitaalne mobiilseade, kaheksa ajapilu (TDMA), $B=200\text{kHz}$

GPRS: 2,5G, natuke internetti (WAP leheküljed), e-mail, MMS sõnumid, 56...114 kbit/s

EDGE: GPRSi edasiarendus, väga suur kiiruse kasv (470 kbit/s), inimesed tahavad internetti palju rohkem kui kõnelega

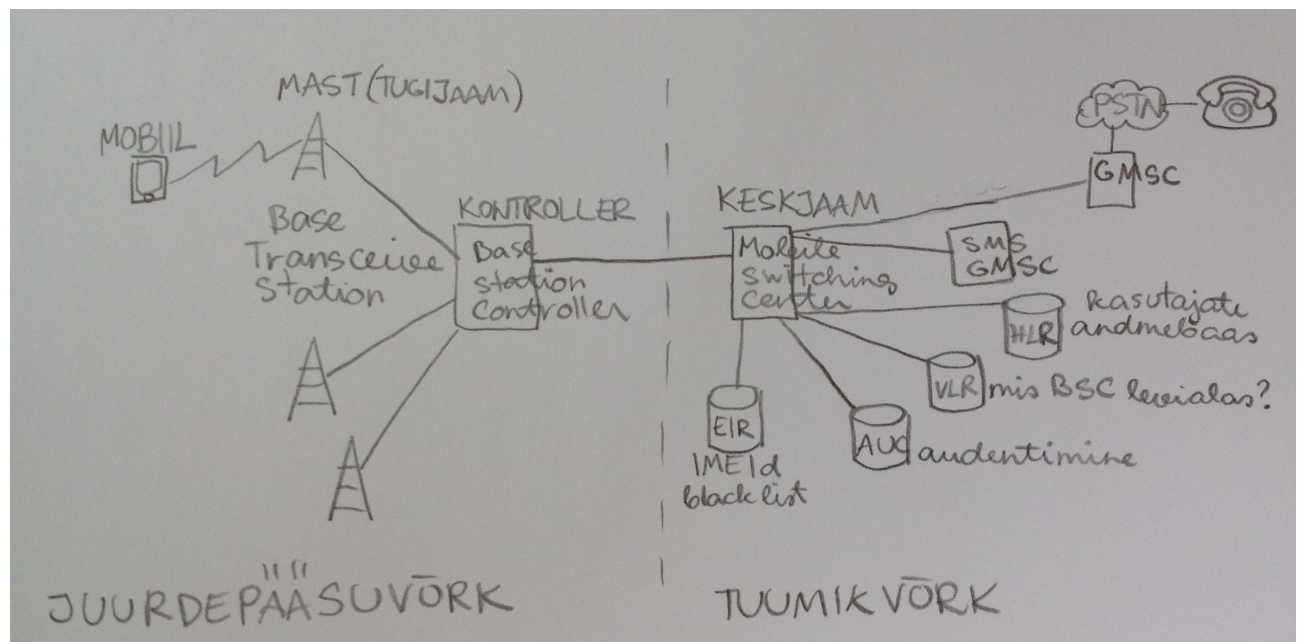
3G UMTS: 5MHz lai riba, allalaadimise kiirus 14Mbit/s, üleslaadimise kiirus 6 Mbit/s, parem kõnekvaliteet, hajasperktrimodulatsioon (kõik kasutavad sama kanalit järjest)

Mobiilsidevõrgu ehitus, mobiilterminal, juurdepääsu- ja tuumikvõrk, nende elemendid ja liidesed.

SIM kaardil on IMSI kood: 248 (Eesti), 01 (EMT), 02 (Elisa) või 03 (Tele2), mis identifitseerib võrgu kasutaja. Igal seadmel on veel IMEI kood, mis on riistvaras. IMEI koode hoitakse EIR baasis.

Ümberlülitumine (handover) ühelt mastilt teisele peab olema sujuv, sellega tegeleb BSC Base station controller.

Võrk on jagatud juurdepääsu- ja tuumikvõrguks.



Mobiilpositsioneerimine, kärje tunnus CI, kaugus tugijaamast
TA -timing advance.

Mobiilseadme asukohta geograafilise määramine raadiolainete abil.
Kasutatakse mitme erineva tugijaama TA-sid, on täpsem kui GPS ja töötab ka toas.

Kärje tunnus CI on Base Transceiver Stationi identifitseerimisnumber

kaugus tugijaamas TA - timing advance: saab teada, kui kaua läheb aega, et signaal jõuaks mobiilist mastini, selle järgi saab teada, millisele mastile mobiil kõige lähedamal on, 550 m laiune rõngas ümber masti