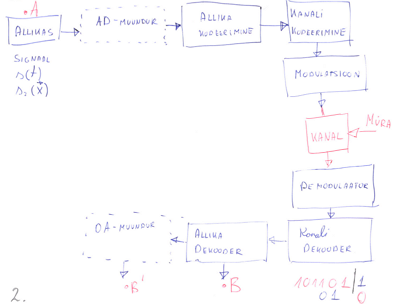
# Shannon-Weaveri mudel

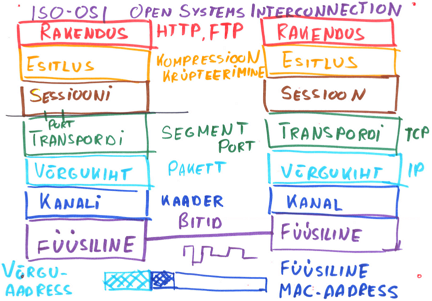
Signaal – mistahes ajas või ruumis muutuv suurus(võib olla nii analoogne kui digitaalne)  
Analoogne – pinge anduris muutub sarnaselt (nt. FM-raadio)  
Digitaalne – numbriline  
Müra – Juhusliku iseloomuga signaal kanalis



Allikas saadab signaali.   
AD – muundur muudab signaali analoogsest, digitaalseks(ei pruugi iga signaali puhul toimuda).   
Allika kodeerimine eemaldab kogu ülearuse, edastatakse vaid hädavajalik, andmed muutuvad haavatavaks, enam rohkem ei tohi ära kaduda.   
Kanali kodeerimisel lisatakse pahna, et sõnum ei oleks nii haavatav(Algsest ikkagi väiksem).   
Modulatsiooni käigus pannakse info edastatavale kujule.   
Kanalis toimub reaalne andmete edastus(nt. traadita side või juhe).   
Demodulaator teeb signaalist programmikoodi(0101), kui ei ole saadud signaalis täiesti kindel, siis pakub, mis see võiks olla.   
Kanali dekooder võtab vigadega bitirea vastu(kontrollib paarsusbiti).  
Allika dekooder teeb siirupist moosi ehk laiendab koodi tagasi.  
Kui vaja siis DA-muundur muudab digitaalse signaali tagasi analoogseks.

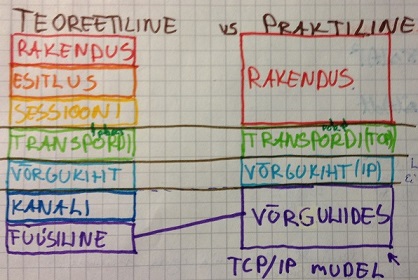
# ISO-OSI mudel

International Standard Organization – Open Systems Interconnection mudel  
Alumine kiht pakub järgmisele teenust ja ülemine kiht kasutab seda oma ülesande täitmiseks.



Füüsiline kiht määrab ära ühenduse tüübi ja konkreetse ühenduse ja signaali tüübi.  
Kanali kihi ülesanne on tagada kahe võrgusõlme vahel loogiline kanal. Füüsiline kiht pole oluline. Kaader on pakk andmetega. Kanali kihis kasutatakse füüsilist aadressi ehk MAC aadressi.  
Võrgukihis liiguvad paketid(datagram). Kaadrile lisatakse andmeid juurde(võrguaadress).(Hoitakse lõpp IP aadressi)  
Transpordi kiht tagab rakenduste jaoks virtuaalse kanali. Alg- ja lõpppunkti vahel. Teekond pole oluline. Kaasas on ka pordi number (millisele failile/rakendusele neid andmeid anda). TCP protokoll(Transmission Control Protocol)  
Sessioon – kasutatakse samal ajal youtube-i (Sessioon 1) ja facebooki (Sessioon 2). Hoiab nende erinevate sessioonide töö eraldi.  
Esitlus kiht – siia käib kokku surumine ja andmete ümbertöötlus ja krüpteerimine.

# TCP/IP protokollistik



# Informatsiooni mõõtühikud: bitt ja bait, nende detsimaalliited

Informatsiooni ei saa valgusest kiiremini edastada.

I = Informatsioon  
P = tõenäosus  
a = e => I [nat] kbit = 1000 bit  
a = 10 => I [hartley] kibit = 1024 bit  
a = 2 => I [**bit**] 8 bit = bait  
1 MB (megabait) = 1024 kB = 1 048 576 baiti.  
1 GB (gigabait) = 1024 MB = 1 073 741 824 baiti.  
1 TB (terabait) = 1024 GB = 1 099 511 627 776 baiti.

# Signaali mõiste ja selle erinevad tüübid: audio, pilt, video, tekst, digitaalsed andmed.

*Signaal* – signaal on mis tahes ajas/ruumis muutuv füüsikaline suurus. Igasugune elektri- või valgusimpulss või sagedus traadijuhtmes, valguskaablis või raadieetris.

*Audio* – igasugune heli, telefoni ja raadio ja televisioonivõrkudes edastatakse heli analoogsignaalina. Digitaalsignaalina salvestatuna tagab aga palju parema helikvaliteedi ja võimaldab paremini ära kasutada olemasolevate sidesüsteemida ribalaiust.

*Pilt* – Pilt salvestatakse arvutisse kui maatriks. Pilt kantakse üle ridade või veergude kaupa.  
must-valge: 8 bit tumeduse jaoks(valgest mustani)  
värviline: värvid salvestatakse punase, rohelise ja sinise tooniga (RGB). 8 punasele, 8 rohelsiele, 8 sinisele ehk 1 piksel = 24biti.  
Resolutsioon = ridade ja veergude arv nt 1920x1080, kokku pildis info 1920x1080x24 = 49,77Mbit =  
= 6.2 MB.   
Binaarne pilt- esitatakse vaid 2 värviga. Pildi pisklil on 2 võimalikku väärtust. 1 pixel vaid 1 bit.

*Video* – Video hõlmab endast liikuvat pilti ja heli. Mõlemat osa surutakse kokku eraldi, vastavalt kuidas kumbagi osa töötletakse. Toores video 300 MB/s

*Tekst* – selline tekst, mis on salvestatud ASCII koodis

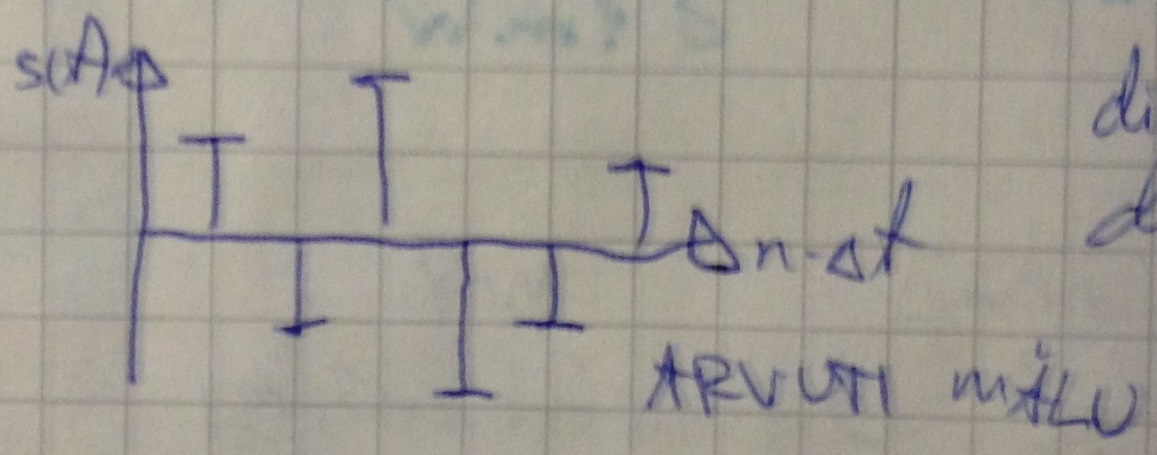
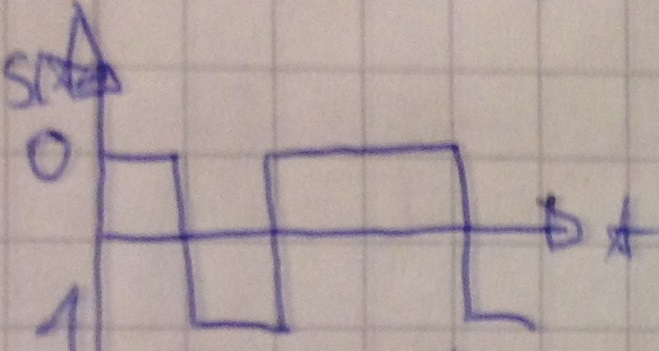
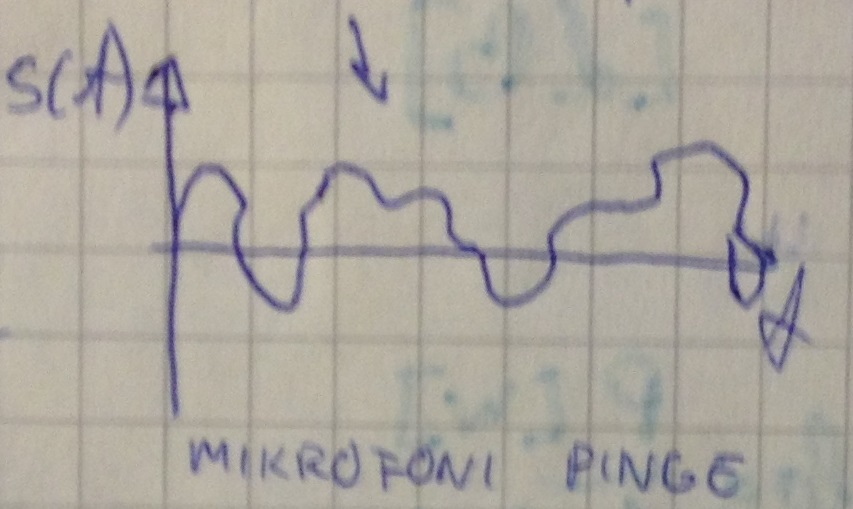
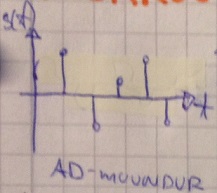
*Digitaalsed andmed* – diskreetsete väärtuste või tingimuste kujul esitatud andmed

*Pidevad ja diskreetsed signaalid, aja ja väärtuse järgi* – Pidev signaal muutub ühtlaselt, pole katkestuskohti (nt inimese kõne/miktofoni pinge), väärtuse poolest pidev aga määratud kindlal ajal väärtus (diskreetne signaal, aeg diskreetne, omab väärtusi konkreetsetel aja hetketel) (nt analoog-digitaal muundur), ajas pidev aga lõplik hulk väärtusi (trepina kujutatav) (PAM-5 1000 base-T, info edastus kaablite kaudu), omab ainult mingitel diskreetsetel hetketel mingit diskreetset väärtust (nt arvutimälu)

# Pidevad ja diskreetsed signaalid, aja ja väärtuse järgi

Signaal – mistahes ajas muutuv suurus, analoogne või digitaalne.

diskreetses ajas pidevad väärtused  
pidev signal  
pidevas ajas diskreetsed väärtused  
diskreetseetel hetkedel diskreetne väärtus



# Ajalised ja ruumilised signaalid, mitmemõõtmelised signaalid.

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

*Elektrilised signaalid* – ehk analoog signaal on pidev signaal, millel on lõpmata arv olekuid ning mida saab igal ajahetkel mõõta. Esitavat infot läbi voolutugevuse, pinge, sageduse või kogulaengumuutuse. Informatsiooni muundatakse mingist füüsikalisest suurusest elektriliseks signaaliks kasutades muundurit, mis muundab energiat ühest liigist teiseks nt mikrofon.

*Vool* – võrdub ajaühikus elektrijuhi ristlõike pinda läbinud elektrilaenguga

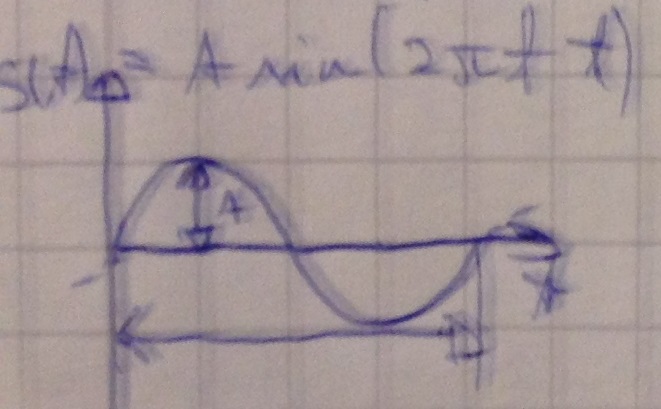
*Pinge* – iseloomustab kahe punkti vahelist elektrivälja potendsiaalide erinevust ning määrab ära, kui palju tööd tuleb teha ühiklaengu ümberpaigutamiseks ühest punktisst teise.

*Takistus* – iseloomustab juhi omadust avaldada elektriaengute liikumisele takistavat mõju.

*Oomi seadus* – I = U/R

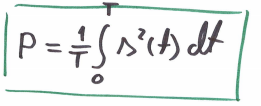
# Siinussignaal, amplituud, sagedus ja periood.

Siinussignaal

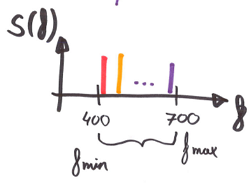


A – amplituud  
T – periood = 1/f  
2πf = w – ringsagedus

# Peamised signaali parameetrid: võimsus, sagedus ja spekter.

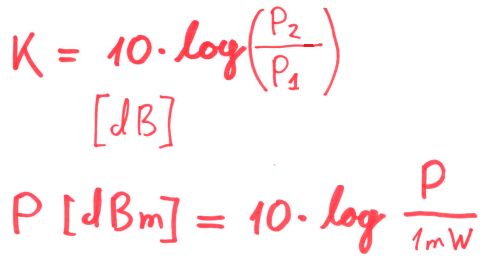
Võimsus - Raadiolained levivad ruumis igas suunas, võimsus väheneb aina. aja jooksul tehtud töö (võimsus), aja ühikus üle kantud energiat (P (power) või S(f) signaali võimsus , wifi ruuter max 100 mW, bluetooth 1 mW, HAARP 3,6 MW) võimsuste vahed väga suured ja see tõttu võrdlemiseks kasutatakse logaritmilisi mõõtühikuid.  
Sagedus – Kui mitu korda aja ühikus ta ennast kordab  
Spekter ehk valge valgus – on elektromagnetilise signaali võimsusspekter.

B – bandwith ehk ribalaius.

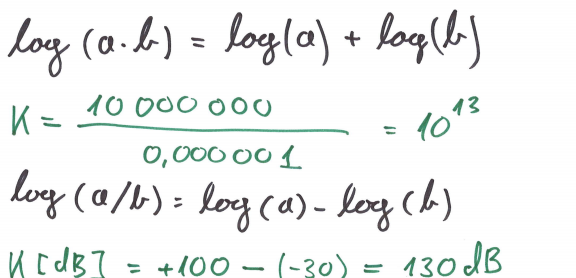


# Logaritmilised mõõtühikud, suhtelised dB ja absoluutsed dBm. Tehted logaritmiliste mõõtühikutega. Müra sidekanalis, AWGN müra. signaal- müra suhe SNR. Shannoni valem.

Detsibell näitab kui palju üks suurus teisest erineb.  
dB ja dBm



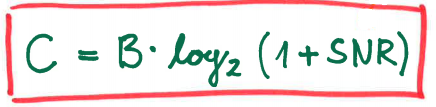
tehted logaritmiliste mõõtühikutega



Müra on juhusliku iseloomuga signaal.   
SNR ehk signal to noise ratio, näitab kui müra ja signaali vahekorda, eelkõige kui palju on signaal mürast tugevam.



Shannoni valem

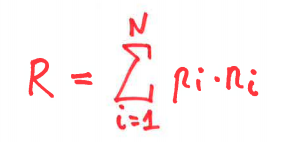


C – Kanali mahutavus. (sidesüsteemi kvaliteet) Kui palju bite sekundis võiks sinna kanalisse teoreetiliselt mahtuda.

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

Allika kodeerimine tähendab ülearuse eemaldamist nii et ainult hädavajalik edastatakse.

Allika entroopia - Mitu biti läheb vaja ühe tähe jaoks, et informatsiooni kadudeta edastada. Liiga suur entroopia -> allika kodeerimine.

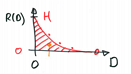
kompreseerimistegur (code rate) – Koodi keskmine pikkus

liiasus – näitab kui palju on edastatud informatsiooni lisaks vajalikule hulgale. Muutuva pikkusega koodi kasutamine aitab liiasuse vähenemisele  
L = R-H, R – koodsõna keskmine pikkus, H –(allika entroopia) vajalike bitide arv, et info kadudeta edastada.

kadudega kodeerimine – ehk kui jääb alla entroopia piiri, siis osa ebaolulist informatsiooni kaob

kadudeta kodeerimine – ehk kui ületatakse entroopia piir ja kõik info edastatakse vigadeta. Kadudeta peavad olema kodeeritud nt raamatud ja programmikood.

kompressiooni-moonutuse suhe (rate-distortion function). - joonealune ala on võimatu.



Teisendusega kodeerimine (Analoog TV) – Kantakse üle siinuse amplituud tõus ja preiood, mitte iga väärtus vastavad diskreetsel ajahetkel. Võib kanda ka, et on 5 siinust ja nende andmed, sellisel juhul on üle kantavate andmete hulk ikkagi väiksem.  
Diskreetne koosinus teisendus(Digi TV) – Pilt või video kaader jagatakse 8x8 bit ruutudeks  
Ridadele ja veergudele tehakse diskreetne koosinus teisendus(must-valge), Toores info blokis 8x8x8=512 bit.  
Pannakse kirja vaid 0st erinev väärtus. Täidetakse diagonaalse sik-sak’i pidi.

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

AD-muundus - Analoog signaal muutub pidevalt ajas. Kasutatakse seadet salvesta ja hoia.  
Lüliti pannakse lühikeseks ajaks kinni, mille jaoks kondensaator laadub vastaval ajahetkel oleva pingeni. Kondensaator hoiab seda pinget endas. Lüliti avamise ja sulgemise kriteerium : NYQUIST – Lülitit tuleb avada ja sulgeda vähemalt kaks korda kiiremini, kui on signaali maksimaalne sagedus. Sellisel juhul jääb kogu info alles.

Kvantimine – Salvestatud pinge mõõdetakse ära lõpliku täpsusega. Väikseim mõõtude vahe = kvantimissamm q. Nivoode arv (palju kriipse on joonlaual) 2...60000 tk.  
ADC bittide arv

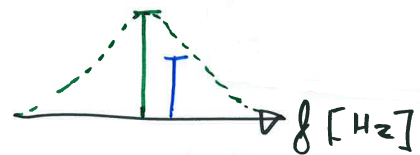
Kvantimismüra – kvantimise käigus arvu ümardamisel tekkinud erinevus  
signaali-kvantimismüra suhe - SNR = 6dB/bit

Dünaamiline diapason – süsteemi või seadme puhul mingi parameetri (võimsus, voolutugevus, pinge, sagedus jne) lubatud maksimaalse väärtuse ja selle parameetri minimaalse registreerimist võimaldava väärtuse suhe. X\_max/x\_min (dB 10log(x\_max/x\_min))

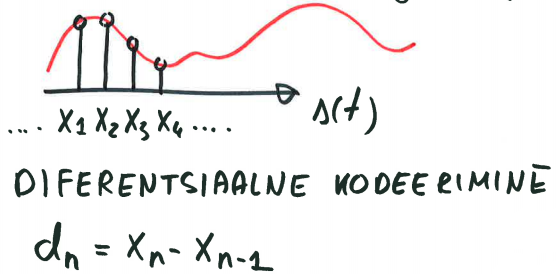
# Audio kodeerimine

1)eemaldatakse need helid mida inimesed nagunii ei kuuleks

2) Maskeerimise nähtus - Kuna neid kahte tooni kõrvuti ei kuule, siis kõik rohelise joone all olev visatakse ära.



3) Diferentsiaalne kodeerimine - Pannakse kirja vaid väärtuste erinevused



Psühhokaustiline mudel - Kõrva kuulde vahemik ei sõltu ainut sagedusest vaid ka dB’st

*MP3* – f\_s = 44,1 kHz mõõdetakse heli väärtust, n\_B = 16, kaks kanalit ehk 1,4 Mbit/s. muusikast tehakse spekter ja vaadatakse millist osa ei kuule inimene ja see osa visatakse välja. Keskmine laul on 300 Mbit/laul. Digitaalse helifailide tihendamise algoritm, mille tihedustegur on kuni 12. helikvaiteet seejuures ei kannata, sets siin arvestatakse inimese kõrva tajumisvõimet nii helisageduste kui dünaamisise diapasooni osas ning kogu mittevajalik info jäetakse välja.

*Maskeerimisefekt* – Kui on spekter, siis mingi noot maskeerib teise noodi ära ja see visatakse ka välja. Kõrva võimekus eraldada testsignaali juhul kui kas samal ajal või ajas ähestiku rakendatakse teine maskeeriv heli

*Diferentsiaalne kodeerimine* – pannakse kirja ainult signaalide erinevused mitte väärtused, kuna need võivad olla liiga suured d\_n = x\_n – x\_n-1

*SIgma-Delta modulaator* – muudab suure resolutsiooniga digitaalse signaali madala resolutsiooniga digitaalseks signaaliks (osa AD-muunurist)

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

Teksti kodeerimine - on teksti kokkuvõtmine ja selles sisalduva info lühikese koodi alla panemine. Korduvalt esinevad andmelõigud edastatakse ühe koodiga

ASCII kood - 128-märgiline keelemärkide tabel, mis sisaldab inglisekeelseid tähemärke, numbreid, keelemärku, klaviatuurifunktsioone.

Huffman’i kood - asendada olemasolev sümboleid kirjeldav bitijada ümber nõnda, et informatsiooni hulgas tihemini esinevad tähemärgid saaksid kirjeldatud lühema bitijadaga.

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

*RLE* – binaarne pilt sisaldab ainult musta ja valge infot. Pildi info antud ainult ühe bitiga. 512x512 suurus pilt on 32 kB. Kui nt terve rida omab sama väärtust, siis saab määrata et terve veerg on must. Run Length Encoding. Et määratakse ära palju musti on järjes ja palju valgeid. See hoiab paju kokku vb ka ei hoia kui pilt on liiga kräbuline.

*DCT* – Signaali kuju esitamine koosimussignaalide kaalutud summana. Toimub andmete tihendamine kadudega.

*JPEG* – kadudega andmetihendusalgoritm ja sobib eelkõige värvifotodele

*Video kodeerimine* – Toored andmemahud väga suured. Signaal on nelja mõõtmeline, laius, pikkus, värvus, aeg. Multimeedia (video, heli, subtiitrid jne koos). Video koodek surub kokku video ja heli (avi, mp4 jne) koodek pakib ka lahti, et välja mängida video.Video kodeerimine:

* vaja selleks, et nt digitaalset televisioonisignaali oleks võimalik olemasolevate kanalite kaudu üle kanda.
* edastatava info mahtu vähendatakse kõigepealt videosignaali digiteerimisel. Nimelt kasutatakse nägemistaju omadust hinnata kuva teravust peamiselt heleduse järgi ja vähemal määral värvide järgi.
* kodeeritakse peamised võtmekaadrid ja neile järgnevates kaadrites olevad pidlierinevused. S.t et jäetakse ülekandmata see osa infost, mis jääb kaadris eelmisega võrreldes samaks.

edastatava videovoo mahtu on võimalik vähendada kuni 200-kordselt

# Koodeki, multimeedia konteineri ja metafaili mõisted.

Koodek – surub kokku kõik erinevad multimeedia osad ja pakib sama vormi järgi lahti  
Multimeedia konteiner – mitu erinevat informatsioon koos(liikuv pilt + heli)  
metafail - failiformaadi termin, mis hoiab endas erinevat tüüpi infot.

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

Kõik kaablid on lainejuhid.

Koakskaabel – kaasteljeline. 2 juhti, mille mõtteline telg on sama.  
Pealmine juhe kaitseb sisemises juhtmes kulgevat voolu. Voolu juhtiva keha sees ei saa elektrivälja olla. Kui peaks sinna sisse tekkima elektriväli, siis osaksesed kompenseerivad.

Keerdpaar – balanseeritud liin. Ei taha väliseid laineid vastu võtta ega siseseid välja lasta. Juhtmestes vool eri suunades. Ühe võrgukaabli sees 4 keerdpaari. 2 interneti, 1 lauatelefoni ning 1 power over LANi jaoks. Juhtmete vahel tugev magnetväli, ümber nõrgem. Max 100 m. pikk.  
UTP – Unshielded twisted pair  
STP – Shielded twisted pair – kaitse väliste mõjutuste vastu kaablis.  
CATx – erinevad kategooriad kaablitele, kvaliteedi järgi.  
Simpleks – ühesuunaline side  
Dupleks – kahepoolne side  
Pooldupleks – üks saab korraga rääkida  
täisdupleks – mõlemad võivad samal ajal edastada.

Fiiberoptiline kaabel – valguskaabel. Laseb läbi valgust, läbimõõt nii pisike, et valgusel vaid üks tee läbimiseks. Otstel tavaliselt tolmukaitse. Kuna kaablist on võimalik eri värvi valguseid läbi lasta siis aab ka mitu kanalit ühest kaablist läbi lasta.(kuni 370)

Raadiokanal – Toimib elektromagnet kiirgusega. 0 < f < 300GHz, kaugus R = 0 ... 100 va(teoreetiline), reaalne 17 vh. Leviedastus, läbi signaalitornide.  
Kaabliga on vaja iga uue kasutaja saamiseks reaalne kaabeldus vedada. Point to point.  
Raadiorelee, sõjaväes – raadioside saadetakse kindlas suunas.  
Satelliitside – side kosmoses olevate satelliitidega.

Raadioside + : Madala sagedusega raadiolained pöörlevad maa ümber. Madalad sagedused peegeldab atmosfäär tagasi.

Raadioside - : 1) Mitmekiireline levi- raadiolained levivad teieni otsa v pindade peegelduste pealt, mille tõttu jõuab teieni signaal mitu korda. Lained siis liituvad ja sellega raadiosignaal nõrgeneb.  
Feeding- signaal nõrgeneb  
2)Doppler effekt – kui objekt, mis kiirgab laineid liigub teie suunas, siis signaalid jõuavad ksteisele järele ja sagedus läheb suuremaks. Sõidate mastist eemale, siis sagedus läheb väiksemaks.

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

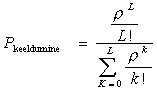
# Asünkroonne andmeedastus ehk start/stop bitid.

# RS-232 – järjestikliidese standard. Peaaegu kõik modemid on sele standardiga ühilduvad (vana asi tglt), Standardis määratakse ühenduse elektrilised omadused, signaalide ajastused, signaalide tähendused, ühenduspesade füüsikalised suurused ja kontaktide jaotus. RS-232 standardil on aga mitu puudust: piiratud andmete edastuskiirus, suhteliselt kõrged pingete tasemed ja liiga suured ühenduspesad.

# Nullmodem – kaabel kahe arvuti kokkuühendamiseks läbi jadaportide ´. Kaabe ühendatakse modemi jaoks mõeldud pistikupessa ja see võimaldab arvutil andmeid välja saata ja vastu võtta, ei toimu moduleerimist ega demoduleerimist.

# Paarsuskontroll – kui on paaris arv ühtesid, siis 1 vastupidi 0

# Teenindamisest keeldumise tõenäosus, Erlangi valem.

Taani inseneri Agner Krarup Erlang (1878-1929) nime kannab valem  mis annab teenindamisest keeldumise tõenäosuse (kõik teenindajad hõivatud), kui on teada teenindajate arv L ning sisendvoo taandatud intensiivsus http://www.lr.ttu.ee/side/labor/side_labor5_html_m53dcc705.gif kus λ kirjeldab sisendvoogu ja μ ühe teenindaja väljundvoogu.

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

Ethernet tuleneb sõnast eeter – tundmatu substants kus electromagnet lained levivad.  
10BASE5 – max 10 mbit/s,Kasutatakse hästi paksu koaks kaablit. 1 võrgusegmendi max pikkus 500 m. Ühendus kaablisse toimus vampiirliidese abil. See hammustas kaablisse augu, ning hammas jõuab juhtmeni ja ühendub võrku. Võis ühendada iga 2,5 m. tagant, kuni 100 arvutit.

Terminaator – lõpetab ära signaali edastamise.(juhtme otsas). Takisti, et signaalid tagasi ei põrkuks. Takistus sama suur kui kaablil.

BASE – põhiriba. Sagedused vahemikus 0-. Teised RIBA (PASS BAND) signaalid.

10BASE2 – kaabel oli peenem kui base5. Vampiirliite asemel kasutati T liides. Lõpus terminaator. Kuni 30 arvutit.

10BASE-T – Twisted pair kaabel.

100BASE-TX – 100 mbit keerdpaar  
1000BASE-T – 1 GBit Ethernet  
Kaabli sumbuvus – Signaali nõrgenemine juhtmes. Sõltub sagedusest ja kaabli pikkusest. Peenema kaabliga suurem sumbuvus.

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

Fiiberoptiline kaabel – valguskaabel. Laseb läbi valgust, läbimõõt nii pisike, et valgusel vaid üks tee läbimiseks. Otstel tavaliselt tolmukaitse. Kuna kaablist on võimalik eri värvi valguseid läbi lasta siis aab ka mitu kanalit ühest kaablist läbi lasta.(kuni 370)

WOMA – wavelength Division multiple access – Eri värvi valgus ühes sama fiibris eristatav lainepikkuse järgi. (infrapuna tavaliselt)

Monomodaalne fiiber – Kaabli materjalid on selliste murdumisnäitajaga, et kogu valgus põrkub tagasi.

Multimodaalne fiiber – Kaabel nii lai, et valgusel on läbimiseks mitu teekonda -> info võib eri aegadel tagasi jõuda.

Graded index fiiber – valgus levib kõveralt, kahe eelneva vahepealne.

Moddalne dispersioon – valgus levib eri teekondi pidi.

# 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.

Peegeldused – Kõrgetel sagedustel saadetakse signaal sateliidini, see võimendab seda ja saadab tagasi maa peale, sihtkohta.  
Iga signaal hajub pika peale nii ka raadiolevi, selleks on loodud tornid, mis võimendavad signaali ja saadavad seda edasi.

DRM, Digital Radio Mondiale – digitaalne standard, mis võimaldab edastada heli, mis on sama hea kui CD plaat, kasutatakse raadiolaineid. Levib umbes 1000 km.

DAB Digital Audio Broadcasting – Sama hea kvaliteet nagu FM-raadiol, aga kallim. Põhimõtteliselt sama nagu DRM-raadiolainete abil CD kvaliteet.  
802.11 WiFi – Traadita kohtvõrk 2.4 GHz, Tööraadius ~100m. B = 22 MHz ühele kanalile.

Antenn – Kiirgab võrdselt igas suunas- ideaalis. Reaalsuses tugeva suunateguriga. Olemas igal tel. wifi-ruuteril jne.  
Gain – antenni võimendus.  
Võimendus – raadiolevis halb, hea kui tahadki ühte kohta suunata.

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

Repiiter – 2 auguga hub. Kõik, mis tuleb ühest august sisse saadetakse teisest välja. Pikkade võrkude juures vajalik, et signaali võimendada.  
Lihtsam variant lihstalt võimandab  
Keerulisem teeb lahti ja saadab uuesti. Võimaldab minna ühelt meediumilt üle teisele.

Jaotur – Kui infot tuleb sisse, siis jagab kõikide vahel laiali.

Modem – Vaja läheb selleks, et koodi signaali ümber teisendada. Võtab sisse üldise signaali(DSL) ja teisendab selle vaja minevale kujule.

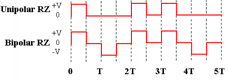
# Liinikoodid (NRZ, RZ, Manchester, AMI), signaali taastamine.

Digitaalne signaal ei pea olema vaid 1 ja 0.

NRZ(no return to zero) – nullist väärtust ei ole. Lihtne lugeda, aga kehv kanali kasutus, 8 andmebiti edastamiseks kasutatakse 12 biti. Keskmine väärtus 0 volti.



RZ(return to zero) – Unipolaarsel Pool biti väärtus ja pool biti 0, Saab aru 1-de puhul mitu biti edastatud, 0’e ei saa eristada.  
Bipolaarsel pool biti väärtus ja siis pool biti 0. Keskväärtus 0, saadetakse ka sünkrosignaal, ribalaius peab olema 2B(topeltsuur).



Manchester – Infot edastatakse nivoo muutusega. Langus +V, -V = 1 ja tõus on 0, bitide keskel toimub muutus.



AMI – 0’le vastab 0 nivoo, 1’le vastab üle ühe pos ja neg nivoo.



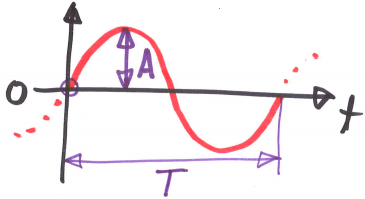
Miller – Kui signaal muutub, siis on tegemist 1-ga, kui ei muutu, siis 0.



Signaali taastamine – Tõmmatakse mõtteline 0-nivoo, kõik mis on kõrgemal on 1 ja madalamal on 0.

# C:\Users\randm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\signaali taastamine.png

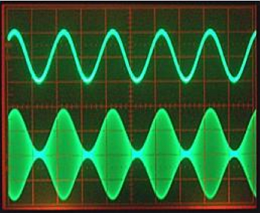
# Modulatsiooni mõiste, modulatsiooniviisid. Amplituud-, sagedus- ja faasmodulatsioon.



A – apmlituud – kõrvalekalle tasakaaluolekust.  
T – periood  
f = 1/T – sagedus  
ϕ – faasinihe. Kui palju on alguspunkt nihkes normaalist.

Modulatsioon – Andmeid kantakse üle sin funktsiooniga ja võib muuta ühte või mitut parameetrit.

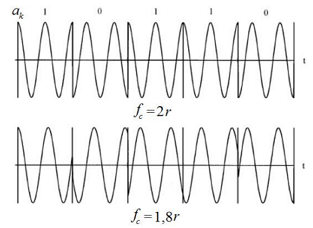
Amplituudi modulatsioon – roheline täidis on kandev signaal ja tema aplituud muutub signaali taktis.



Sagedusmoduleerimine – moduleerimine kanalis kindla sagedusega, ühe kanali saab ühte juhtmesse kokku panna, Raadios vahetad kanali vahetamisel sagedust nt. Sellel põhineb raadio ja telelevi.

C:\Users\randm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\sagedusmodulatsioon.png

Faasmodulatsioon – 1 asemel esitab cos, 0 asemel esitab –cos.



BFSK – specter – kantakse üle 2 erinevat sagedust ja vastuvõtjas on “filter”. Ei pea olema vaid 2 erisagedust.

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

FDMA - Mitu signaali saab edastada ühes kanalis, kuna need on eri sagedustel ja võnkesse on võimalik kokku panna mitu erinevat kanalit,

TDMA – GSM-süsteemi võrkudes kasutatav võte võrgu läbilaskevõime suurendamiseks. Erakdab peakanalis perioodiliselt igale allkanalile oma ajaintrevalle. Töötab nii, et peakanal jaotatakse ajaintervallideks ja seejärel edastatakse üht ja sama kanalit mööda mitu kõnet, eraldades igale ühele neist teatud ajaintervalle. Nii on võimalik ühel ja smaa sagedusel tekitada mitu samaaegselt toimivat andmekanalit.

CDMA – koodijaotusega hulgipöördus, kus mitu saatjat kasutab samaaegseks signaalide edastamiseks ühele vastuvõtjale üle ühe ja sama sageduskanali mingit spektrijaotuse varianti sellest, et signaalidevaheline interferents puudub või oon minimaalne.

SDMA - is a channel access method based on creating parallel spatial pipes[clarification needed] next to higher capacity pipes through spatial multiplexing and/or diversity, by which it is able to offer superior performance in radio multiple access communication systems.

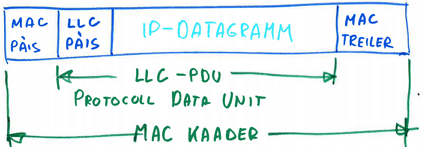
# ISO-OSI mudeli kanalikiht. TCP/IP mudeli MAC ja LLC alamkihid. Kanalikihi adresseerimine (MAC aadress) ja põrkedomeenid. MAC kaader, selle struktuur. LLC-PDU. LLC teenuse juurdepääsupunkt (LSAP). Veatuvastus (CRC, FCS). Meediumi jagamine: ALOHA, CSMA/CD. Vookontrolli meetmed: Stop-and-Wait, Sliding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

LLC – pole vahet kuidas füüsiline kiht on ühendatud, peaasi, et oleks mingi ühendus. LLC teeb selles piltlikult “toru”, kus informatsiooni saaks edastada.  
Liides kõrgema kihi protokollide jaks. Andmete multipleksimine(LSAP)  
vookontroll(Stop and Wait, Sliding window)  
Vigade tuvastus ja parandamine (ARQ, FEC)

MAC – meediapöördus alamkiht. Kuidas me füüsilise media poole pöördume ja seda jagame. LLC Service access point ehk LSAP. Loogiline aadress, mis ütleb täpselt millise rakenduse jaoks see andmepakett on.

Kaader – Seal sees on lisaks vajalikule infole palju lisandeid, tagamaks kaadri kohalejõudmise õigele kohale.

Alumine osa on MAC päise ja MAC traileri ehitus.



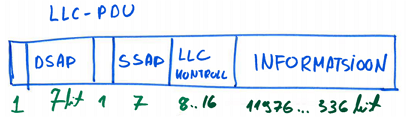
MAC konteiner  
7 - 101010…, vajalik selleks, et saatja ja vastuvõtja kellad ühtlustuksid   
1 – 01111110, annab märku kaadri algusest. Selline kombo tuleb ainult kaadri alguses või lõpus. Kui andmete keskel tuleb selline bitide järjestus, siis pannakse iga viie 1 järele 0. 011111010.

Sihtkoha MAC-Aadress  
Kui vastuvõtja loeb ja tegu on tema mac-aadressiga, siis vastuvõtja loeb edasi. Vastasel juhul ignoreeritakse.

2 – antakse teada kaadri pikkus, et vastuvõtja saaks buffri valmis panna.  
LLC-PDU – Kui tegelik pikkus on väiksem siis lisatakse täidet.



MAC-aadress – tehases igale seadmele antud identifitseeriv aadress. 48-bit. Kokku umbes 2.81x10^14 erinevat aadressi. Veel otsa ei saa. Vanu saab uuesti kasutada. 16nd süsteemis unikaalne.



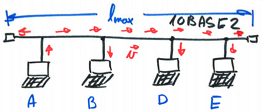
LLC service Access points ehk LSAP loogilised aadressid, mis ütlevad, mis rakendusele on paket mõeldud.

DSAP – destination service access point – millisele rak. See info läheb  
SSAP – source SAP – millisest rakendusest andmed tulid.

Veatuvastus CRC – Cyclic Redundancy Check  
veatuvastus b  
Näide. Edastame TERE väärustega 21+4+19+4, kontrolli jaoks paneme iga tähe võrdume tema asukohaga Eesti tähestikus.  
Kontrolliks liidame kõik tähtedele vastavad arvud kokku CRC = 48  
Kui arvutatud CRC admetest ei klapi edastatud CRC’ga, siis on teada VIGA  
Lõpus veel ka 01111110 või järgmine kaader, siis lõpu oma ei panda.

MAC-kihi ülesanded  
Saatmisel andmete jaotamine kaadriteks, füüsilise aadressi ja veatuvastusväljade lisamine  
vastuvõtul andmete eraldamine kaadrist, aadressi ja vigade tuvastamine  
kaadrite sünkroniseerimine  
Füüsilisele meediumile juurdepääsu tagamine.

Sama info jõuab igasse masinasse  
kui A suhtleb D-ga, siis B ja E on ka hõivatud  
Kui A ja E saadavad samal ajal, siis teisteni jõuab ennde kahe saadetud paketi summa.  
Eelnevate probleemide lahenduseks on erinevad meediapöördus protokollid.



ALOHA – edasta kaader millal tahad, Peale kaadri edastust oota mingi aja, kui vastest ei saabu, saada uuesti. Kui mingite katsete järel endiselt ei saabu vastust, anna alla.  
max kanali kasutus 18%

Pesastatud Aloha – võib saatma hakata hetkel, mis on täisarv kordne , n=1,2,3... muu sama nagu tavalisel alohal. Pesastatud aloha korral kanali kasutus 37%

CSMA – carrier sense multiple access  
Kuula, kas keegi teine edastab  
Kui meedium on vaba, siis edasta kaader  
kui meedium ei ole vaba, siis oota juhulikult valitud aeg ja seejärel alusta  
ühe paketi algusesse ja eelmise lõppu vahele jääb tühi auk.

Järjekindel CSMA – Kui meedium pole vaba, siis kuula ja edasta kaader niipea, kui meedium vabaneb.

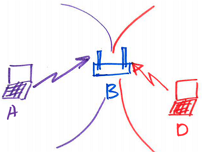
Parim on kahe eelneva vahepealne.

CSMA/CD – collision detect.  
Kuula, kas keegi teine edastab  
kui meedium on vaba, edasta kaader  
kui meedium ei ole vaba, siis kuula edasi, alusta kaadri edastamist niipea kui meedium vabaneb, kuulamist jätkatakse ka edastamise ajal.  
Kui tuvastatkse kokkupõrge, siis edasta lühikene teavitussignaal ja lõpeta seejärel edastus.  
oota juhulikult valitud aja jooksul ja seejärel alusta uuesti esimesest paketist.

Kuidas tuvastada, et teine ka räägib?  
sõltub topoloogiast  
siinvõrk  
iga vastuvõtja mõõdab pinget ja kui see on suurem kui tema suudab tekitada, siis on kokkupõrge  
sarnaselt kuulamine – kui on pinget, siis keegi suhtleb  
täht-topoloogia  
jaotur tuvastab kokkupõrke.

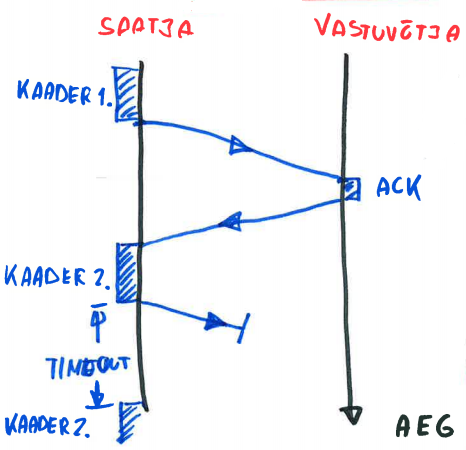
Raadiovõrgus

A ja D küsivad B käest edastuseks luba.



Vookontroll  
Saatja tahab saata palju andmeid ning vastuvõtja hoiustab neid oma bufferis, et neid töötlema hakata. Võib juhtude, et vastuvõtja ei jõua nii palju andmeid ära töödelda ning juhtub bufferi ületäituvus. Vookontroll tegeleb selle probleemi ärahoidmisega.

Stop-and-Wait  
  
Pane andmed teele  
oota  
peale kinnitust pane uus teele  
kui kinnitust ei tule, siis oota ära timeout ja saada uuesti  
vastuvõtja ootab ära kuni ta andmed ära töötleb ja siis saadab ACK(aeg lühem kui timeout).  
häda tekib, kui side link on megapikk nt. Satelliit side. Siis on side link enamasti tühi.



Sliding-window  
Kui kanal on enamus ajast tühi, siis saadetakse mitu paketti korraga. Kinnitused tulevad ka iga paketi kohta eraldi. Saadetakse vajadusel osad uuesti. Saadetakse uuesti kõik paketid alates katkisest.

Vigade parandus ja tuvastus  
FEC – Forward Error Correction  
andmeid on võuimalik kodeerida nii, et kaotsi läinud andmeid on võimalik alles olevate põhjal taastada  
ARQ – automatic repeat request  
veatuvastus välja põhjal on võimalik öelda kas pakett tuli kohale vigaselt või ei. Kui tuli vigaselt, siis palutakse uus pakett teele panna.

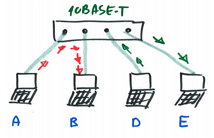
Stop-and-Wait ARQ  
ACK 1 – sain kätte saatke pakett nr 2.  
vaid numbrid 0 ja 1

Go-Back-N ARQ  
1, 2, 3, 4  
Ack 5 – kõik neli tulid, saada 5’s  
5, 6(fail), 7, 8  
ACK 9 – uuesti alates 6’ndast.  
  
Selective reject ARQ  
5, 6(fail), 7, 8  
öeldakse, et saada 6’s uuesti, mitte 7’s ja 8’s.  
6, 9...

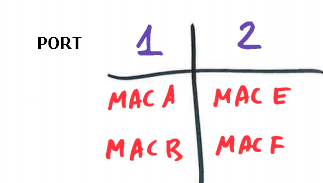
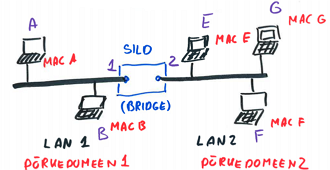
# Kanalikihi seadmed kommutaator (Switch) ja sild (Bridge).

Koomutaator – Switch  
Väliselt nagu jaotur

Andmed edastatakse vaid sellele, kellele see mõeldud on. Teeb vahet MAC-aadresside abil.(Teab kõigi enda külge pandud asjade MAC-aadresse.)  
LAN – Local area network ehk kohtvõrk, max ulatus ~200 m  
Põrkedomeen



Sild – Bridge  
ühendab kahte kohtvõrku.  
  
Kui F saadab kaadri teele ja sild tuvastab, et see on E-le mõeldud, siis ta seda Lan 1 poole üle ei kopeeri. Vahet teeb MAC-aadresside abil.  
Sillal on tabel MAC aadressidega. Porte võib olla tuhandeid.  
  
Andmed tulid pordist 1. Mõeldud arvutile MAC B. See on pordis 1, järelikult sild ei tee nende andmetega midagi. Kui andmed tulevad pordist 2 ja arvutile MAC B siis sild saadab edasi vaid porti 1.  
- on sillale tuleb ise öelda kõik MAC-aadressid.  
lahendus:  
1)Algoritmid teevad tabeli ise  
2)Sillal on alguses tühi tabel. Kui tuleb pakett, siis sild paneb ise kirja, et see arvuti mis saatis on pordis x. Saadab kõik tundamata saatjaga paketid kõikjale edasi.



Miks kasutada silda?  
Füüsiliselt pikem võrk, kui kaablid lubavad.  
Töökindlus – iga alamvõrk saab omavhael suhelda, ilma et teisi segaks.  
Turvalisus – saab hoida 2te võrku eraldi ja öelda, et omavahel ei saaks suhelda osad arvutid.

# Hargneva puu protokoll (STP).

Eriline MAC  
FF-FF-FF-FF-FF-FF – leviaadress  
pakett on mõeldud kõigile(sisevõrgu piires)

Kinnine võrk  
Lan 1 -> Lan 2 -> Lan 4 -> Lan 1

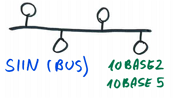
Arvuti A saadab paketi välja. See hakkab ringi liikuma, igavesti.

STP – Spanning Tree Protocol  
hargneva puu protkoll  
kuni 4096 arvutit võimalik konfigureerida.  
BPDU – Bridging Protocol Data Unit  
Igale sillale saadetakse leviaadressiga käsklus end konfigureerida.  
võtab aega 30-50 sekundit  
üks juursõlm millest kogu liiklus hakkab läbi käima.  
Kasutatakse kõige väiksema MAC-aadressiga silda, kuna ta on arvatavasti kõige vanem ja kehvem  
hakatakse vaatama, mis kuhu on ühendatud  
Leitakse igasse alavõrku optimaalseim tee ja ülejäänud teed blokeeritakse ära.  
nii kaob ära kinnise võrgu probleem.

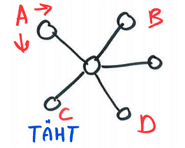
# Võrkude topoloogiad. Siin- ja tähtvõrk, joon, puu, ring, täielikult ühendatud (Metcalfi seadus ja võrguefekt) ja mesh võrgutopoloogiad. Superarvutites kasutatud "paks puu" ja hüperkuubi võrgutopoloogiad. Võrkude hierarhia suuruse järgi: LAN, MAN, RAN, WAN. Ahel- ja pakett-kommunikatsioon.

Viisid, kuidas seadmeid omavahel võrku ühendada.

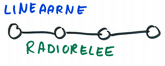
Siinitopoloogia (BUS)  
  
nt 10BASE2, 10BASE5.  
+  
lihtne  
-  
kasutatakse ühte meediumi ehk üks saab ainult korraga rääkida.  
nõrk koht  
kui peamine juhe katki teha, siis on kõik. Katkisest kohast enam suhtlus ei saa läbi minna.



Tähttopoloogia  
  
nt 10BASET  
+Kui üks kaabel on katki siis teisi see ei sega  
nõrk koht  
kui keskse sõlmega midagi juhtub, siis on võrguga kõik.



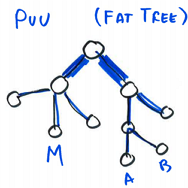
Lineaarne/Joon topoloogia  
  
Kasutatakse nt pika maa taha edastamiseks või raadiorelee liinid  
halb töökindlus – piisab ühe sõlme katki minekust ja terve võrk ei tööta  
-  
igal võrgusõlmel peab olema 2 ühendust ehk 2 võrgukaarti  
mõistlik siis, kui ühest otsast ei saa otse ühendada ja vaja seda korrata.

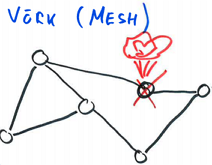


Ringvõrk  
  
Füüsiliselt nagu täht, ainult et saata saab vaid naabrile.  
+  
Kui üks kaabel puruneb, siis saab saata lihtsalt teiselt poolt.  
Füüsiline vs Loogiline Topoloogia  
Füüsiline – kuidas on kaablid veetud  
Loogiline – kuidas võrk seda näeb

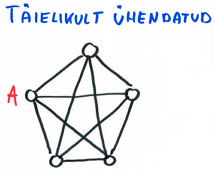


Puu  
  
Mida kõrgema kihi sõlm, seda olulisem.  
Mõistlik oleks kõrgemad ühendused teha kiiremad, kuna neid kasutatakse rohkem – Paks puu  
kasutatakse superarvutites.



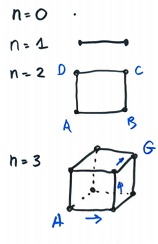
Võrk(Mesh)  
  
võrgusõlmed on ühendatud juhuslikult  
suuremad punktid ja nende vahelised liinid  
piisavalt töökindel- pole hullu kui üks juhe puruneb.  
Pärineb interneti algusaegadest II MS aegu, kui oli oht, et tuumapomm võib mõne ühenduse hävitada.

Täielikult ühendatud võrk  
  
eksisteerib otseühendus kõigi võrgusõlmede vahel  
N = 5 – võrgusõlmede arv  
võimalike ühenduste arv   
+  
Töökindlus on parim  
-  
Reaalselt selle tegemine on keeruline



Metcalf’i seadus  
Igasuguse võrgustiku väärtus on võrdeline võrgusõlmede ruuduga  
Teatud piirist alates ei anna enam see sõlmede nii palju kasu, kuna seda ei jõuta ära tarbida.  
Dunbari arv ehk ahviring  
Inimese aju – kui palju inimesi me suudame tajuda inimesena(et nad on mitmetahulised ja sügavad) – 160

Hüperkuup  
superarvutites  
  
Superarvuti CN-1 kasutas n=12 hüperkuupi



LAN- kohtvõrk Local Area Network ~200m  
CAN – Campus AN(Linnak, tehnopol) mõned km.  
MAN – Metropolitan AN – suurem linn, kümned km.  
RAN – Rural AN – MAN’is palju kasuatajaid ja tihedalt koos RAN’is vähe kasutajaid hõredalt.  
WAN – Wide AN – Võib katta riiki, kontinenti  
Internet  
LAN – palju inimesi ühendada  
WAN – suurte maade taga oleks ühendus

Kuidas luua ühendus  
1. püsib ühendus  
-  
Kallis, kui vaja pidevat andmevahetust mingi punktiga  
kui kontoris siis pole peale töötunde vaja.  
2. Liini on vaja siis kui vaja.

Ahelkommutatsioon  
Kõige vanem ühenduse viis – telefonides  
Kui teil on vaja, siis luuakse teie jaoks punktist-punkti fikseeritud kanal, mis on kogu ühenduse ajal teie. Muul hetkel pole teie. Maksad kasutatud aja eest.  
Ennekõike kõne edastuseks.  
Pole hea andmeedastuseks.

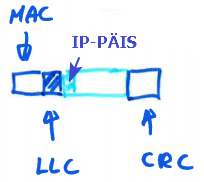
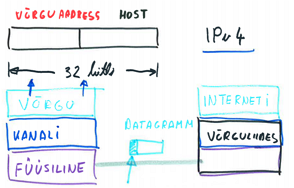
Pakett Kommutatsioon – andmeedastuseks  
Kui sul on midagi saata, siis need pakitakse kaadriteks  
ühendus on teie vaid paketide saatmise ajaks  
1.virtuaalne kanal  
töö alguses lepitakse kindel teekond kokku, niipea kui üks sõlm on vaba, saab kohe uued teele panna.  
2.Datagrammide edastamine  
Saatja viskab paketi võrku ja ütleb, kuhu see jõudma peab. Sõlmed ise on piisavalt targad ja saadavad selle edasi resurssi kõige tõhusamalt ära kasutades.

# 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 (ühenduseta kanal), pole füüsilist kanalit  
kui saadetakse mitu pakki siis nad võivad liikuda eri teid pidi ja seega võivad eri ajal kohale jõuda => peab olema info järjekorra kohta.  
Kanalikiht toimetab andmeid ühest sõlmest teise. Võrgukiht toimetab paketi algusest lõppu välja.

IP/TCP – best effort – võrk annab parima, et pakett kohale jõuaks, aga ei garanteeri seda.  
IP aadress annab aimu sihtpunkti asukohast

Võrguaadress(IP-aadress)  
andmepakett = datagram



Internetikiht  
pead edastamisel valima sõlme, kuhu pakett edasi saata. Edastamine LLC kihile.

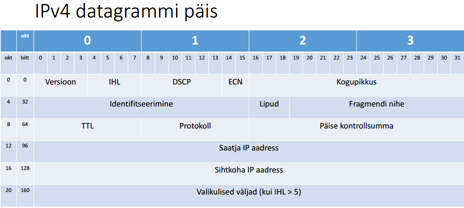
Fragmenteerimine  
Kui andmed on suuremad, kui õhte datagrammi mahub, siis see lõigatakse juppideks ja need saadetakse eraldi kaadritega üle.

Vastuvõetud andmete edastamine transpordikihile  
veatuvastus ainult päises oleva info kohta  
diagnostika, nt. Protokoll ICMP – Internet Controll. Message Protocoll-ping  
loll võrk – edastab andmed aga ei kontrolli nende õigsust

Pingimine – vastavale aadressile saadetakse lühike andmepakett ja mõõdetakse kas ja kui kaua selle kohale jõudmine aega võttis.  
TTL – Time to live

IPv4 – esitatud kümnendarvudega  
32 bit = 8 B, nt 172.16.254.1

IPv6 – 128 bit  
vajalik, kuna IPv4 on otsa saamas max 4.3x10^8 kujutatakse 16-nd arvuna.  
  
version – näitab ära interneti versiooni tüübi  
IHL – Internet header Length – päise pikkus 1 = 32 bit, 2 = 64 bit  
DSCP – millise teenusega on tegemist. Sellest sõltub selle paketi prioriteet  
ECN – optional. Saab anda teada võrgus toimuvast koormusest. Enamasti ei kasutata.  
Kogupikkus – kui pikk on datagram kokku , Päis + andmed.  
Identifitseerimine – vaja, kui IP datagram on fragmenteeritud. Annab teada mitmes pakett tuleb.



Lipud  
1. Reserveeritud  
2.DONT FRAGMENT – kui datagram on liiga suur saatmiseks ja fragmentida ei tohi siis see visatakse minema  
3. MORE FRAGMENT – rohkem fragmente tulemas

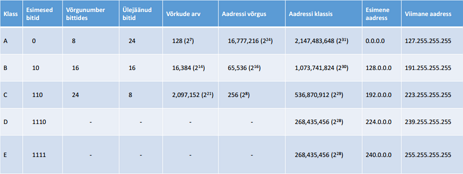
Fragmendi nihe – mitmendast baidist see kõik pihta hakkab.

TTL – pakette saadetakse ka suundades, kus pole vastuvõtjat.TTl annab ette kaua see pakett elab hüppeloenduri abil ehk mitu korda seda võib edasi saata. Iga sõlm vähendab seda 1 võrra.  
IPv6 nim Hop count

Protokoll – näitab mis kõrgema kihi andmed siin sees on  
nt. ICMP – ping  
TCP – transfer code protocol  
UDP – user datagram protocol

Päise kontrollsumma – igas sõlmes arvutatakse kontrollsumma ja võrraldakse seda kaasa antud kontrollsummaga, vigane visatakse ära.  
Saatja ja sihtkoha IP – kellele mõeldud ja kas saatis.

Võrguaadresside klassid  
  
Aadressi võrgus – palju asju sinna võrku saab ühendada



D – Multiast aadressid – paljudele mõeldud vaatamiseks. Siiamaani kasutatakse ühelt aadressaadilt mitmele saatmine.  
E – tulevikurakendustele ja ekperimenteerimiseks

Klassideta võrk  
bitimask  
1111 0000 – mask  
1011 0101  
1011 0000

Võrgumask – kuna kõik on jagatud alamvõrkudeks, siis võrgumaski ja IP-aadressi loogilise liitumisega saad alamvõrgu, kuhu see tuleb viia. Sealt läheb edasi vastavasse arvutisse.  
1 võimalik kirjapilt(CIDR kirjapilt)  
192.168.2.0/24  
IP-aadress

Võrgumaski esimesed 24 nr. On 1’d

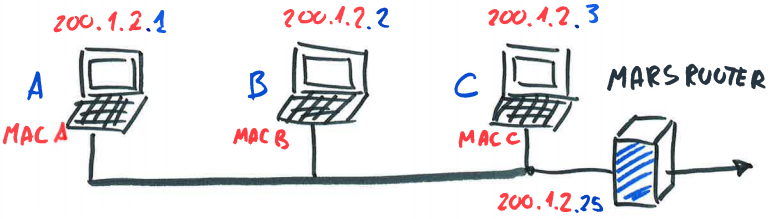
Privaatvõrk  
3 aadressi vahemikku igaühele kasutamiseks seni, kuni see välja ei paista internetis

BROADCAST 192.168.105.**255**  
IP-aadress millele paketti saates läheb info kõigile, kes seal kohtvõrgus on.

Multicast – ip aadress, mis saadetakse kõigile, kes tahavad.

Loopback 127.0.0.1  
Virtuaalne aadress, millele saab tarkvara saata pakette ja kõik saadetakse tagasi. Ei pea olema võrguühendust selle kasutamiseks.

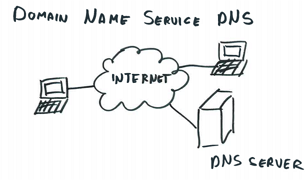
Default gateway – kui arvuti pole samas võrgus või ei tea kelle saata ja seal on targem võrgusõlm, mis teab mida teha.



Arvuti A tahab arvutile C saata midagi, kuid ta teab arvuti C IP-aadressi, kuid mitte MAC-aadressi. Kuidas arvuti A selle teada saaks?

Selleks on protokoll Adress Resolution Protocol  
Saadab kõikidele arvutitele broadcast aadressile paketti, küsimaks : Kellele kuulub aadress 200.1.2.3  
Kõik võrgus olevad masinad teevad selle paketi lahti ning kontrollivad seda IP-aadressi enda omaga  
Kui tegu on mingi arvuti IP-aadressiga, siis see arvuti vastab: 200.1.2.3 MAC-aadress on …  
Arvuti A jätab selle IP-aadressi siis meelde teatud ajaks  
Igale kaadrile pannakse ajatempel juurde  
selle abiga saab aimu kanali tööst  
et andmeid väljapoole edastada on vaja targemat seadet.

DNS Domain Name Service  
  
DNS-server pakub DNS teenust  
Inimene trükib veebilehitsejasse aadressi  
siis küsitakse DNS serverilt Selle aadressi IP-aadressi ja saadab selle sulle tagasi  
see info jäetakse mõneks ajaks meelde.



DHCP – protokoll, mis võimaldab võrguülematel ühest keskusest hallata ja automatiseerida dünaamiliste IP aadresside omistamist organisatsiooni võrku ühendatud hostidele. Internetiprotokollide TCP/IP kasutamise korral peab igal internetiühendust vajaval masinal olema oma unikaalne IP aadress. Kui organisatsioon soovib igale arvutikasutajale anda ligipääsu Internetile, siis on üheks võimaluseks igasse arvutisse käsitsi sisestada staatiline ehk alaline IP aadress ja kui antud arvuti paigutatakse samas võrgus kuhugi mujale, tuleks sisestada uus IP aadress. Igale organisatsioonile on eraldatud teatud kindel arv IP aadresse ja kui arvutite hulk selle organisatsiooni võrgus kasvab suuremaks kui olemasolevate IP aadresside arv, võimaldab DHCP omistada IP aadresse ainult neile arvuteile, mis parajasti sisse on lülitatud.

NAT

C:\Users\randm\AppData\Local\Microsoft\Windows\INetCache\Content.Word\privaatvõrk.png

Eravõrgu sisemiste IP aadresside asendamine avalike IP aadressidega. NAT annab organisatsioonidele suurema paindlikkuse aadresside kasutamiseks oma kohtvõrkudes ja lubab kasutajatel vastavalt vajadusele ühiselt kasutada piiratud arvu registreeritud IP aadresse. NAT’i kasutamine teeb ühtlasi raskemaks sisevõrgu ründamise väljastpoolt, sest sisemisi IP aadresse ei edastata üle Interneti. Võrguaadresside ümbernimetamine toimub harilikult marsruuteris või tulemüüris

# Võrgukihi analüüsivahendid ICMP (ping) ja traceroute.

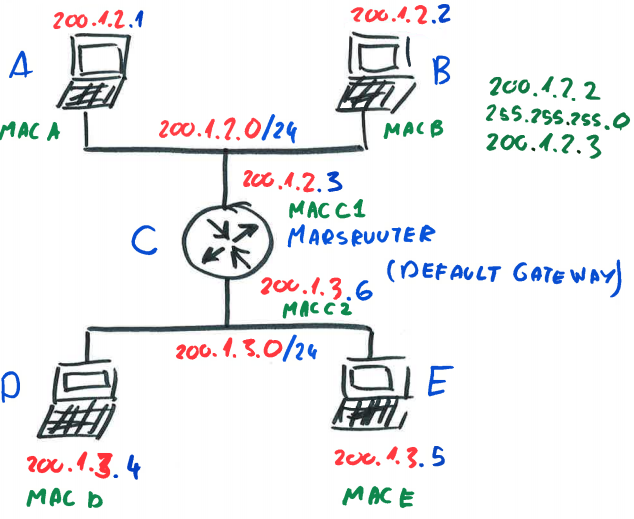
ICMP - Hooldusprotokoll TCP/IP protokollistikus, mis on nõutav igas TCP/IP realisatsioonis ja mis võimaldab kahel IP võrgu võrgusõlmel omavahel vahetada ja ühiselt kasutada IP oleku- ja veainformatsiooni.

Ping-utiliit kasutab ICMP protokolli kaugarvuti juurdepääsetavuse kindlakstegemiseks.

Traceroute - Utiliit, mis jälgib paketi teekonda teie arvutist kuni Internetis paikneva hostini ja näitab ära, kui mitu hüpet (hop) pakett peab tegema enne hostini jõudmist ja kui kaua aega iga hüpe võtab. Kui te külastate mingit veebisaiti ja teile tundub, et veebilehed jõuavad kohale liiga aeglaselt, siis see utiliit võimaldab teil kindlaks teha, kus nimelt viivitused tekivad.

# Võrgukihi seadmed: marsruuter, tulemüür.

Marsruuter -Võimeline andmeid edastama meie LAN-ist väljapoole ja internet  
Sellisel juhul saadad tundamtu IP-aadressi default gatewayle ning tema teab mida sellega edasi teha.



2 Mac- ja 2 IP-aadressi- üks esimese ja teine teise jaoks  
default gateway – marsruuteri IP

Marsruutimine  
Kui arvuti A tahab arvutile E saata andmeid, siis ta ARP päringule ei saa vastust.Siis saadetakse pakett E IP-aadressiga aga Mac c1 Mac-aadressiga  
marsruuter saadab selle paketi tesie võrku siis edasi.

Marsruutimise algoritmi omadused  
Marsruutimine peab tagama, et andmed jõuaksid sinna kuhu vaja  
lihtsus  
robustus – ta peab erinevates tingimustes hakkama saama  
aus ja õiglane – ei eelista kellegi pakette  
optimaalne – kasutatakse alati optimaalseimat teed  
effektiivsus – kui suur osa liiklusest on kasutajate ja kui suur osa vajalik võrgu enda ülalpidamiseks.

Marsruutimise kriteeriumid  
soorituskriteeriumid  
 min hüpete arv  
 hind  
 viide  
 läbilaskevõime

Otsustusaeg  
 pakettedastus(datagramm)  
 sessioon(virtuaalne ahel)

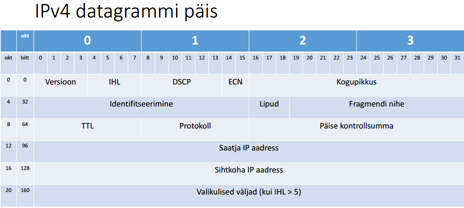
Otsustuskoht  
 igas sõlmes  
 keskses sõlmes  
 allikas

Info allikad  
 puuduvad  
 lokaalne  
 naabersõlmed  
 sõlmed marsruudi ulatuses  
 kõik sõlmed

Otsustusaeg  
 pidev  
 perioodiline  
 topoloogia muutumisel  
 olulise koormise muutuse korral

Tulemüür - Internetti ja kohtvõrku teineteisest eraldav spetsialiseeritud arvuti, nn. lüüsarvuti, mis ise ei sisalda tundlikke andmeid ja kaitseb kohtvõrku volitamata sissetungijate eest väljastpoolt. Tulemüüri võib kasutada ka selleks, et piirata firma töötajate võimalusi suhelda välismaailmaga üle Interneti ja niiviisi kaitsta firmasaladusi.

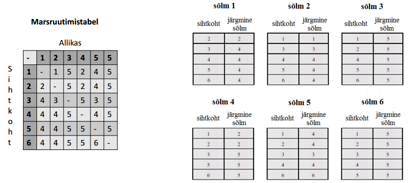
# IP-datagramm ja selle päis. Paketi eluiga TTL.

  
version – näitab ära interneti versiooni tüübi  
IHL – Internet header Length – päise pikkus 1 = 32 bit, 2 = 64 bit  
DSCP – millise teenusega on tegemist. Sellest sõltub selle paketi prioriteet  
ECN – optional. Saab anda teada võrgus toimuvast koormusest. Enamasti ei kasutata.  
Kogupikkus – kui pikk on datagram kokku , Päis + andmed.  
Identifitseerimine – vaja, kui IP datagram on fragmenteeritud. Annab teada mitmes pakett tuleb.

TTL – pakette saadetakse ka suundades, kus pole vastuvõtjat.TTl annab ette kaua see pakett elab hüppeloenduri abil ehk mitu korda seda võib edasi saata. Iga sõlm vähendab seda 1 võrra.  
IPv6 nim Hop count

# Marsruutimine võrgus. Fikseeritud, üle ujutamine, juhuslik ja adaptiivne marsruutimine. Minimaalse kuluga marsruutimine ja Dijkstra algoritm.

Fikseeritud Marsruutimine  
Eksisteerib marsruutimistabel, kus on kirjas see, kellele need andmed tuleb saata.  
  
Kui tahad saata arvutist 1 paketi arvutile 6  
alguses oled sõlmes 1 seega llika alt vaata pealkirjaga 1 rida. Siis võtad sõlme 6 veeru ja see kast ütleb, et mine sõlme 4.   
Nüüd oled sõlmes 4. Nagu eelmises punktis vaatad allika 4 realt ja endiselt sihtkoha 6 veerult arvu ning nüüd pead minema sõlme 5, jne.  
iga sõlm teab ainult seda, kuhu tema peab andmed saatma.



Üleujutus  
+  
ei pea võrgust midagi teadma  
pakett jõuab alati kohale  
pakett jõuab alati ka lühimat teed pidi kohale

pakett saadetakse kõigile edasi, peale selle, kust see tuli  
(TTL on oluline)  
Saab teha piisavalt targad sõlmed, mis korra tulnud paketti uuesti edasi ei saada.

Looduslikud marsruutimis algoritm  
eeskuju võetud spielgatest  
sipelgad uitavad juhulikult ümber pesa ringi ning varem või hiljem komistab millegi hea otsa  
mines eritab feromeene ning tagasitee leiab lõhna järgi  
kasutatakse lühemat rada, kuna see on kiirem ja lõhn jääb kauemaks, kuna edasi-tagasi tee on kiirem.

Fikseeritud marsruutimise miinused  
suuri võrke inimesel raske hallata  
iga sõlme kohta peab infot teadma  
kui midagi muutub, siis onv aja kõiki tabeleid uuendada

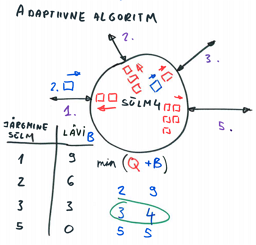
Üleujutuse miinuseks on suur koormus võrgul.

Juhuslik marsruutimine  
mitte ükski sõlm ei tea midagi  
pakett saadetakse suvalisse kohta edasi, varem või hiljem jõuab kohale  
võrgu kohta ei pea infot teadma  
võrreldes üleujutusega ei teha nii palju koopiaid  
aga ei jõua kõige otsemat teed pidi  
võib sissetulevaid ringiratast saata

Parem version  
kui on teada iga lingi läbilaske kiirus, siis marsruutimist saab teha tõhusamaks, kui eelistada suurema läbilaske kiirusega teed.

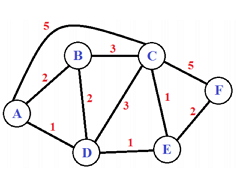
Staatiline algoritm – kogu aeg sama (üleujutus, juhuslik marsruutimine)

Adaptiivne algoritm  
oskab ennast vastavalt oludele ümber häälestada  
Isoleeritud – ligipääs vaid enda sõlmes toimuvale.  
  
Kuidas valida kuhu pakett saata?  
Kõige lühema ootejärjekorraga  
ootejärjekord tuleb sellest, et sõlm peab arvestama vastuvõtja buffriga  
Vookontroll  
saatja peab ise ka mõningaid andmeid ümber arvutama  
Võimalus on anda igale sõlmele lävi.  
min(Q + B)  
Q – ootejärjekorra pikkus  
B – lävi  
valitakse teekond kus Q+B on väikseim.

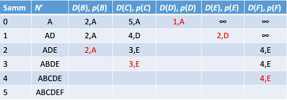


Vähima kulu algoritm  
On olemas info kogu võrgu kohta ning kui midagi muutub, siis arvutatakse mis teekond.

Graaf – suvalise sõlmende ja nende vaheliste ühenduste hulk  
  
Graaf G = (N;E)  
Sõlmede hulk  
N = {A, B, C, D, E, F}  
harude hulk(sõlmede vahelised ühendused)  
E = {(A, B),(A, C),(A, D),…,(E, F)}  
ühenduse hind(rahaline, viide jne.) väiksem, parem  
C(X, X’)  
C(A, C) = 5  
Tahame, et C(X, X’) oleks minimaalne

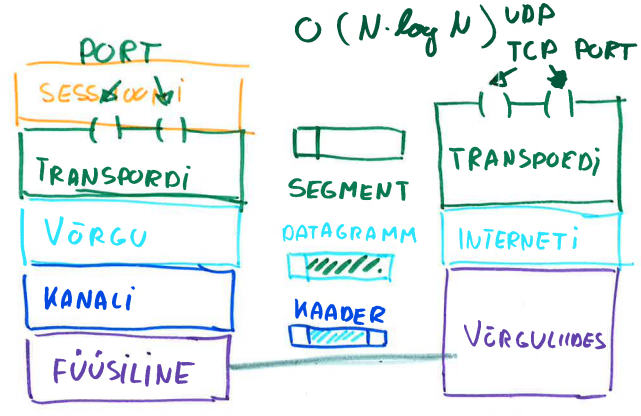


Dijkstra algoritm  
Adaptiivne – iga mingi aja tagant mõõdab ja arvutab uuesti kogu asja  
et muud infot teada saada siis lihtsalt küsib  
C(x, y) sõlmede vaheline hind. Kui pole naabrid, siis C(x, y) = ∞  
D(v) hetkel teadaolev koguhind allikast sihtkohani v  
P(v) viimane sõlm, teel allikast, enne sihtkohta v  
N’ – sõlmede hulk, milleni on teada vähima kuluga tee

Dijkstra algoritm - algväärtustamine   
N’ = {u} /\* Alustame teede leidmist sõlmest u \*/   
Kõigi sõlmede v jaoks, Kui v on u kõrval D(v) = c(u,v), muidu D(v) = ∞  
  
Tahan A-st F-ni odavaimat teed pidi  
Punkti F on min kulu 4 läbi E  
Punkti E on min. Kulu 2 läbi D  
Punkt D on otseühenduses punktiga A hinnaga 1.  
Selle algoritmi keerukus on N^2

# 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.

Transpordikiht



Transpordikiht tagab rakenduse jaoks ühenduse, mis rakendusele tundub, naug oleks otsekaabel  
Transpordikiht peab tagama häirevaba konkreetse ühenduse rakenduste vahel  
TCP/IP mudelis transpordikihi peal juba rakenduskiht  
Transpordikihis liiguvat paketidena segmendid  
transpordikiht suhtleb millisele rakendusele see segment on  
Osad pordi numbrid on fikseeritud ~200 tk  
ülejäänud vabad  
Port määrab ära selle, millise rakenduse jaoks pakett tuleb

Transpordi kihi funktsioonid  
ühendusele orienteeritud side. Virtuaalne otsekanal alg ja sihtpunkti vahel. Sõltumatus alumiste kihtide ülesehitusest ja protokollistikust  
segmentide õige järjekorra tagamine  
Ühenduse usaldusväärsuse tagamine  
segmendi kontrollsumma  
kinnitused ACK ja NACK  
Vigaste/puuduvate andmete uuesti saatmine ARQ  
vookontroll  
võrgu ülekoormuse vältimine  
Rakenduskihi andmete multipleksimine  
TCP protokoll on aeglane paljude kinnituste pärast  
Transpordikiht jagab info ise segemntideks annab need võrgukihile ja hiljem pärib ise info sealt lahti ka.

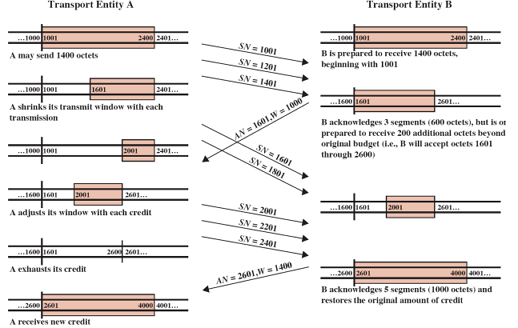
TCP segment

Järjekorranumber – andmete õigeks kokkupanekuks. Ühe segemndi järjekorranr.  
kinnituse nr(ACK) – teadmaks millised kinnitused on tulnud ja mis vaja uuesti saata  
päise pikkus – 5-15  
000 – tulevikurakendustele. Hetkel kõik nullid  
Lipud  
NS-  
CWR-  
ELE-  
URG-urgent, oluline  
ACK – kinnituslipp ühenduse loomisel  
PSH – käsk, et andmed kohe rakenduskihile edasi anda  
RST – reset, uus ühendus vaja luua  
SYN – sync, vaja ühenduse loomiseks  
FIN – ühenduse lõpetuse soov  
Akna suurus- segemndi + päise suurus  
kontrollsumma – kontrollimaks, kas segment on korrektselt kohale jõudnud  
UKG viit – kui on oluline, siis kui palju neid veel tuleb



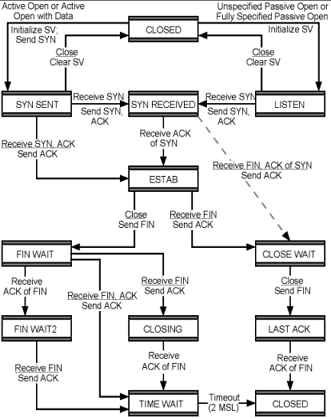
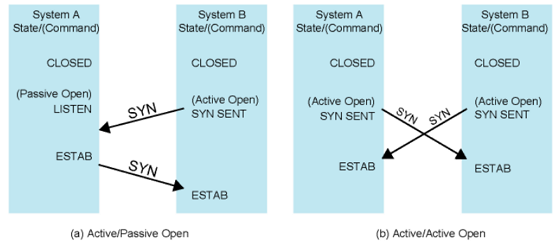
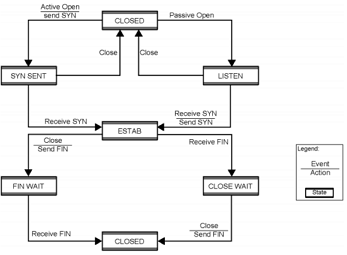
Usaldusväärse võrgukihi ülesanded  
adresseerimine  
peab teada andma kuhu andmed lähevad  
multipleksimine  
üks transpordikiht pakub samal ajal teenust paljudele rakendustele  
vookontroll  
libisev aken, sarnane transpordi kihiga  
SN-sequence number – millisest bitist alatest asjad tulevad.  
AN – acknowledgement number – esimese järgmine oodatava segmendi number  
ühenduse loomisel saadetakse ISN ehk esimene saadetava segmendi nr.(lipuke SYN = 1)  
W-kui palju infot saab vastuvõtja vastu võtta

TCP krediidijaotuse süsteem  
  
Mõlemad osapooled teavad, et saadetakse alustades baidist 1001 ja vastuvõtja saab hetkel vastu võtta 1400 baiti. A paneb teele 3 segmenti 1001-1401(baidid 1001-1600). A saab saata veel kuna vastuvõtja enamaks valmis. A saadab veel 2 paketti 1601 ja 1801. Sellel hetkel saab A vastuse, et kuni 1600 tuli ilusti ja 100 B saad veel saata ehk kuni 2601. Kuna 1601 ja 1801 on ka veel saadetud siis A saadab ära veel 3 paketti ning sellega kasutab ära kogu oma krediidi ning peab ootama B’lt kinnitust, et edasi toimetada. B annab teada, et saada pakett 2601 ja saan võtta veel 1400 B.



Lõplik olekumasin FSM  
FSM –final state machine

Abstraktne seadde, millega saab erinevaid olekuid kirjeldada  
lihtne TCP olekumasin  
  
passive open – serverid. Ootad et keegi suhtleks  
active open – loo ühendus  
ühenduse loomine  
  
Ebausaldusväärse võrguühenduse korral  
Segmentide õige järjekorra tagamine  
Retransmissioon, 1)vigane segment – kontrollsummaga test, 2)segment ei jõua kohale, 3)AN, taimer, kui mingi aja jooksul vastust ei tule, siis saada uuesti.  
Dublikaatide tuvastamine – ISN sama võrguga uuel ühendusel erinev  
vookontroll  
ühenduse loomine ja katkestamine  
tõrgetest toibumine  
ülekoormuse vältimine, kui võrk läheb aeglaseks. TCP annab siis enda poolt kõik, et end tagasi tõmmata



UDP päis – connectionless user datagramm protocol  
visatakse võrku ja loodetakse, et jõuab kohale. Ei kontrollita kohale jõumist.  
  
allika port – ei pea olema, võib olla   
ühepoolne  
kontrollsumma – veast teatatakse, aga seda ei parandata



UDP rakendused  
TCP on usaldusväärne, aga aeglane  
kui on kiire rakendus ja pole oluline, kui tuleb viga, nt. Internetitelefon  
TCP on alati kahe otspunkti vahel kui sama serveriga tahavad rohkem kui üks kasutaja, siis TCP puhul luuakse mitu ühendust.  
Identifitseerimine käib „socekt“i kaudu = IP:port, nt 192.168.105.31:80  
Kui mitu inimest vaatavad samal ajal sama asja, live TV, siis kasutatakse UDP  
Broadcasti jaoks kasutatakse UDP, võetakse multicast aadressi ja kõik kes tahavad, saavad sama paketi  
Sensorsüsteemides, termomeetrid  
TCP kasutatakse kriitiliste andmete puhul, kus andmete kadu pole lubatud. Nt. Rakenduste allalaadimine  
UDP ei taju võrgu ülekoormust

# UDP protokoll, UDP datagramm ja selle päis.

Sideprotokoll, mis pakub suhteliselt piiratud teenust andmete vahetamisel intentetiprotokolli (IP) kasutavasse võrku ühendatud arvutite vahel. UDP kujutab endast alternatiivi edastusohje protokollile (TCP) ja kuna ta vajab tööks internetiprotokolli, siis kasutatakse vahel ka tähistust UDP/IP. UDP kasutab internetiprotokolli selleks, et saata andmeüksust ehk datagrammi ühest arvutist teise. Erinevalt TCP-st ei tegele aga UDP sõnumi jagamisega pakettideks (datagrammideks) ja nende õiges järjekorras kokkuühendamisega vastuvõtupoolel. Kui võrgust saabub datagrammideks jagatud sõnum, siis UDP datagramme ei reasta. See tähendab, et UDP-d kasutav rakendusprogramm peab ise suutma kontrollida, kas kogu sõnum on kohale jõudnud ja kas datagrammid on õiges järjestuses. Seetõttu kasutatakse UDP-d sellistes võrgurakendustes, kus on tegu väga lühikeste, ühte paketti mahtuvate sõnumitega ja kus tahetakse töötlemisaega kokku hoida. Kokkuhoid tuleb sellest, et UDP kasutamisel puudub vajadus edastada igas paketis pakettide "kokkumonteerimiseks" vajalikku informatsiooni. Näiteks TFTP (Trivial File Transfer Protocol) kasutab TCP asemel UDP´d. UDP pakub aga ka kaht teenust, mida IP ei paku. Nimelt pordinumbreid ja vajaduse korral ka kontrollsummasid. Pordinumber võimaldab eristada erinevaid kasutajanõudeid ja kontrollsumma abil saab kindlaks teha, kas sõnum jõudis kohale vigadeta. OSI kontekstis asub UDP nagu ka TCP neljandas ehk transpordikihis

UDP päis – connectionless user datagramm protocol  
visatakse võrku ja loodetakse, et jõuab kohale. Ei kontrollita kohale jõumist.  
  
allika port – ei pea olema, võib olla   
ühepoolne  
kontrollsumma – veast teatatakse, aga seda ei parandata

UDP rakendused  
TCP on usaldusväärne, aga aeglane  
kui on kiire rakendus ja pole oluline, kui tuleb viga, nt. Internetitelefon  
TCP on alati kahe otspunkti vahel kui sama serveriga tahavad rohkem kui üks kasutaja, siis TCP puhul luuakse mitu ühendust.  
Identifitseerimine käib „socekt“i kaudu = IP:port, nt 192.168.105.31:80  
Kui mitu inimest vaatavad samal ajal sama asja, live TV, siis kasutatakse UDP  
Broadcasti jaoks kasutatakse UDP, võetakse multicast aadressi ja kõik kes tahavad, saavad sama paketi  
Sensorsüsteemides, termomeetrid  
TCP kasutatakse kriitiliste andmete puhul, kus andmete kadu pole lubatud. Nt. Rakenduste allalaadimine  
UDP ei taju võrgu ülekoormust

# Küberturvalisuse mõiste

Küberturvalisus – riistvara, tarkvara ja võrgus oleva info kaitsmine selle eest: 1) et neid ei kahjustataks  
2) et neid ei varastataks.

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

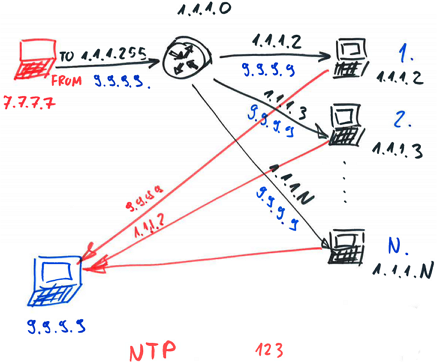
Pahavara – kurjade kavatsustega tarkvara  
viirus iseseisvalt ei ela, kopeerib end mingi koodi vms külge. Lähim asi hetkel tehiselule  
uss-Iseseisev tarkvara, mis teeb halba, tuleb ise su arvutisse.  
troojalane – esitleb end hästi. Ise paned oma arvutisse ja siis hakkab su arvutis halba tegema  
käomuna – paigtatakse arvuti juurde ja suudab administraatori õigustest mööda hillida  
lunavara – pahavara, millest lahti saamiseks peate kellelegi raha maksma.  
pahavara saab ka riistvara hävitada.  
man-in-the-middle – Kui Alice tahab Bobiga rääkida, siis nemad ei näe erinevust, kuid reaalsuses mõlemad räägivad Stuxnetiga ja stuxnet saab neile öelda mida teha.  
tagauks - võib olla sisse ehitatud, võib tekkida vigade tõttu süsteemi ehituses, hiljem saab seda lisada nii kasutaja kui ründaja poolt. Tagauks tagab ründajale ligipääsu su arvutile salaja.Sarnaneb maja tagauksele. Kui selle lahti jätad, siis saab igaüks sulle külla tulla ja võtta mida iganes ta tahab.

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

DOS-rünnak – Denial of Service  
takistab sihipärastel kasutajatel ligipääsu seadmele või võrgule  
Kuidas seda teha?  
pingi ujutus – pingib ühte arvutit suurte pakettidega palju. Kui kasutada zombie arvuteid(sinu poolt üle võetud arvutid, mis teevad mida iganes sa tahad samal ajal kui nende omanik ei tea midagi), siis saab rohkem kahju teha.  
surmav ping – kunagi sai teatud OS-iga arvutile kindlate parameetritega pingiga ära tappa  
SYN ujutus – Serverile saadetakse SYN palve, mitmete erinevate suvaliste IP-aadresside ja portide poolt ning server jääb vastust ootama, kuid seda ei tule. Serveril saavad võimalike ühenduste arvud täis ja tavakodanik enam sinna serverisse ligi ei pääse  
Püsiv kahju – tarkvara jupp vahetatakse pahavara vastu  
füüsilise kihi rünnakud – Kõige enam EW-Elektronic warefare, mis segavad vastase raadiosidet. Füüsilise kihi rünnakud on ainult lokaalsed  
Rakenduskihi rünnakud – banaanirünnak ei lase andmeid sisse, kuna kõik teie väljaminev info tuleb teile endale tagasi.  
HTTP POST rünnak  
post käsuga saadetakse palju andmeid teele ja siis keeratakse kiirus maha. Sina ootad ja ootad andmeid ja muud ei saa teha  
Must Fax – saaded kellelegi järjest musta lehe faxile  
Botnet – pahavaraga on su arvuti muudetud osaks ründavate arvuti hulgaks. Botneti või müüa või ise kasutada.  
Hajutatud DdoS  
Botnet  
vabatahtlikud zombied – inimesed ise korraldavad kambaga rünnaku millegi vastu, nt Anonymus.  
LOIC – low orbit ion cannon  
võrkude stressi testimise tarkvara, sarnane SYN ujutusele  
DdoS – võib ka heatahtlikult

Kuidas veel su masinale ligi pääseda?  
Arvuti kõige nõrgem tuvasüsteemi lüli on kasutaja.  
Pealtkuulamine, Juhtmete küljes harukarp => uitab krüpteerimine, tehakse ikkagi andmete analüüs => hoiatakse liine pidevalt töös, saab ka päiseid krüpteerida  
Van Eck phreaking – on võimalik kuulata teid pealt kuulates vaid kuvari tekitatud häiresignaalide põhjal, kuvarile tekitatakse pilt ride haaval ja see muutub pidevalt ning füüsika seaduste kohaselt kuvar eritab raadiolaineid. Saab suunata teie poole antenni, mille taga on raadio vastuvõtja ning singaalitöötlus, mis suudavad kuvarile näidata sama pilti, mis teil.  
Spootimine – esitlete end kellegi teisena. Nt. mees keskel – paned mingi teise allika IP.  
Kasutusõiguste suurendamine, pääsed arvuti adminnile ligi ja sellega suurendad enda õigusi  
Õngitsemine, nigeeria printsi kirjad jms.  
<a href=”http://www.pettus.org”>www.swedbank.ee</a>  
klikkide kaaperdamine – eda arust vajutad ühte aga teelt midagi muud, häkkerid on pannud nähtamatu lehe õige lehe alla

Dos rünnaku võimendamine  
Smurfrünnak ICMP  
  
ei toimi tänapäeval  
9.9.9.9 ohver  
paketile vastab iga võrgus 1.1.1.0 olev seade, mis kõik läheb tagasi ohvrile.  
DNS – annab veebilehtedele IP aadressi teatud päringule antakse 100 korda pikem vastus  
NTP – küsib netist üle palju kell on. Nt uuendatakse automaatselt 2048 s tagant. On olemas käsk, millega saab küsida nimekirja viimastest IP aadressidest, mille võimendus on 500 kuni paartuhat korda.



# Kaitsemeetmed: tulemüür, proksi, NAT.

Vastumeetmed  
Tulemüür – eraldi seade või arvutis sees, paketifilter – datagramme igaühte hinnati, et kas last läbi või mitte(whitelisting, blacklisting), keeratakse IP-aadressid kinni, mõned pordid, mõned protokollid.  
Olekupõhine tulemüür – vaadatakse kas paketid kuuluvad andmevoogu või mitte  
rakenduskihi – vaadatakse, mis rakendused käima tõmmatakse ja mida ta teha tahab.  
keylogger – loeb klahvivajutusi  
mikrofoni või veebikaamera tööle lülitamine  
võrguaadresside tõlkimine – väljast paistab teie IP-aadress teine ja õige IP-aadressi teada saamine pole kõige kergem  
proksi – sise ja välisvõrgu vahel, vahemälu väliselt pommitamisel võib pahalane vaid proksi leida.

NAT – Eravõrgu sisemiste IP aadresside asendamine avalike IP aadressidega. NAT annab organisatsioonidele suurema paindlikkuse aadresside kasutamiseks oma kohtvõrkudes ja lubab kasutajatel vastavalt vajadusele ühiselt kasutada piiratud arvu registreeritud IP aadresse. NAT’i kasutamine teeb ühtlasi raskemaks sisevõrgu ründamise väljastpoolt, sest sisemisi IP aadresse ei edastata üle Interneti. Võrguaadresside ümbernimetamine toimub harilikult marsruuteris või tulemüüris  
A-klass, mis on mõeldud suurtele võrkudele ja toetab 16 miljonit hosti  
B-klass, mis on mõeldud keskmise suurusega võrkudele ja toetab 65000 hosti  
C-klass on mõeldud väikestele võrkudele, kus on alla 256 hosti  
D-klass on mõeldud multiedastusvõrkudele

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

Krüptograafia – andmete salvestamise ja edastamise meetodid, mis tagavad juurdepääsu ainult neile kasutajatele, kellele see mõeldud on. Krüpteeritud teksti avamiseks vajalik võti. Krüptograafia ja sõnumite kodeerimine on väga VÄGA vanad.

Asendusšiffer – lahtise teksti sümbolite asendamine mingi reegli järgi šiferteksti sümbolitega  
  
võti peab olema salajane.



Šifri lahti murdmine  
krüptoanalüüs – krüptograafilise süsteemi väljundite ja sisendite analüüs võtme teada saamiseks.(selle krüpteerimis viisi murdmiseks)  
toore jõuga lahti murdmine – nt tabalukul lihtsalt koodide järjest läbi proovimine  
kõrvalkanali rünnatakse – ei rünnata otse seda krüpteerimise süsteemi vaid kõrvalkanaleid nt. programmi, mis seda jooksutab.

Kerckhoff’i printsiip  
Krüptosüsteem peab olema turvaline ka siis kui vaenlane teab: 1) Viimse detailini kuidas see töötab, 2) Krüpteeritud teksti

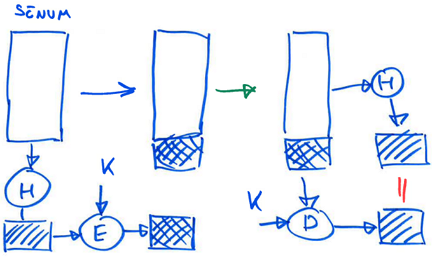
Ainus mis seda saab lahti murda on võti.

Ühekordne šiffer – OTP  
õige kasutamise korral lahtimurdmatu  
Tingimused:  
1) võti peab olema juhuslik  
2)võti peab olema sama pikk kui lahtine tekst  
3)võtit võib kasutada ainult 1 korra  
4)võtit tuleb hoida saladuses  
5)krüpteerimisel liidetakse iga lahtise teksti bitti mooduliga kaks kokku võtmega ühe ja sama sümboliga 2 korda annab algse summa XKK=X



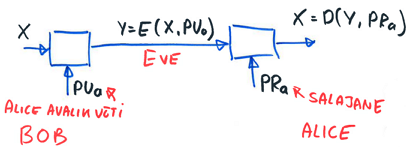
Sümmetriline krüpteerimine  
Ajalooline meetod  
krüptoks ja dekrüptiks vaja sama võtit + kuidas toimetada  
DES – Data Encryption Standard – 56 bit, al 1977, murti lahti 1998, 3DES – kasutati 3 kordset krüpteerimist  
AES – Advanced ES, 128 bit  
mida pikem võti seda kauem läheb aega selle lahti murdmiseks.

Autentimine  
Kaitseb aktiivse rünnaku eest, spoofimise ja andmete muutmise vastu  
kasutatakse räsifunktsioone  
matemaatiline funktsioon, mille sisendiks on muutuva pikkusega sisend ja ühepoolne, algsest saad räsi aga räsist algset ei leia.  
kasutatakse paroolide hoidmisel  
väljundiks fikseeritud pikkusega räsi.  
mida rohkem on parrelis erinevaid sümboleid seda kauem võta aega nende läbi proovimine  
MAC-message authentication code  
  
H – räsiks tegemine  
E – krüpteerimine  
D – dekrüpteerimine



Avaliku võtmega krüpteerimine A-sümmeetriline  
eksisteerib 2 võtit – 1 avalik ja 1 salajane

ID-kaart  
id-kaardis on sinu salajane võti, id-kaardiga saab ka teksti krüpteerida nii, et ainult valitud inimesed saavad seda avada.  
  
Y – Krüptoekst  
X – tekst  
E – algoritm  
võimaldab digiallkirjastamist  
krüpteerimiseks kasutatakse BOB’i sajast võtit ja igaüks saab BOB’i avaliku võtmega autentide, et see tõesti oli BOB.



IPsec ja SSH  
räsifunktsioon Krüptograafias kasutatav ühesuunaline funktsioon tekstistringide kodeerimiseks

nternetiprotokolli andmeturve Firma Cisco Systems juhtimisel arendatav andmeturbe standard võrgu- või paketitöötluskihi tasemel. Varem sisestati andmeturve sidemudeli rakenduskihti. IPSec on eriti kasulik virtuaalsete privaatvõrkude ehitamisel ja kasutajatele turvalise kaugpöörduse võimaldamisel virtuaalsetesse privaatvõrkudesse. IPSec’i suur eelis on selles, et andmeturbe tagamiseks pole vaja teha mingeid muudatusi individuaalkasutajate arvutites. Cisco varustab kõiki oma võrgumarsruutereid IPSec’i toega. IPSec pakub kaht turbeteenuse valikut: andmete saatja autentimist võimaldavat autentimispäist (AH) ning sõnumi kapselturvet (ESP), mis toetab niihästi saatja autentimist kui ka andmete krüpteerimist. Kummagi teenusega seotud spetsiifiline informatsioon sisestatakse sidekanalis edastatavasse paketti eraldi päisesse, mis järgneb IP paketipäisele. On võimalik valida mitme erineva võtmeprotokolli vahel, näiteks võib kasutada ISAKMP/Oakley protokolli (vt. ka IKE). IPSec sobib kasutamiseks nii Internetis, ekstranetis, intranetis kui kaugpöördusega privaatvõrkudes

turvaline kest, turvakest UNIX‘i-põhine käsuliides ja protokoll, mis võimaldab turvalist sisselogimist kaugarvutisse. Paljud võrguülemad kasutavad seda veebi- jt serverite kaugjuhtimiseks. SSH kujutab endast tegelikult komplekti kolmest utiliidist slogin, ssh ja scp, mis on varasemate UNIX’i utiliitide rlogin, rsh ja rcp turvalised versioonid. SSH käsud on krüpteeritud ja mitmes mõttes turvalised.

Klient-server ühenduste mõlema otsa autentimiseks kasutatakse digisertifikaati ja ka paroole edastatakse krüpteeritult.

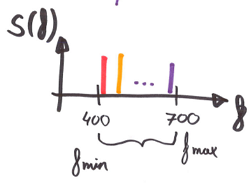
# Traadita kohtvõrk 802.11 (Wi-Fi) ja selle turvalisuse tagamine WEP ja WPA.

Tegemist on Etherneti protokolli kasutava kohtvõrguga, kus kaablid on asendatud raadiolinkidega. Wi-Fi on ühilduv PC-kaartidega ja Wi-Fi logot kandvate tugijaamadega.

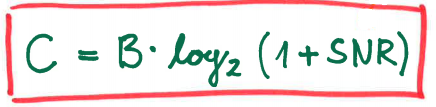
WEP krüpteerimismeetod (40-bitine RC4) projekteeriti selliselt, et see peaks tagama samal tasemel andmeturbe nagu fiksvõrkudes, kuid tegelikult osutus WEP kergemini haavatavaks kui loodetud (see murti lahti 2001.a.) ning 2003.a. tuli selle asemele WPA

Andmeturbe protokoll Wi-Fi alliansilt IEEE 802.11 standardile vastavatele raadiokohtvõrkudele (Wi-Fi võrkudele). Siin kasutatakse TKIP (Temporal Key Integrity Protocol) protokolli, et tagada tugevamat krüpteerimist kui varasema WEP protokolli puhul (WEP kasutas RC4 algoritmi, kuid WPA kasutab AES algoritmi). WPA on tuletatud IEEE 802.11i andmeturbe standardist ning kasutab autentimiseks EAP protokolli

# 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  
Shannoni valem  
B – bandwith ehk ribalaius.

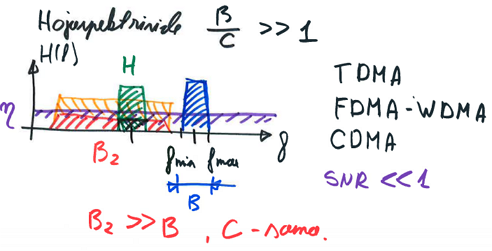
SNR ehk signal to noise ratio, näitab kui müra ja signaali vahekorda, eelkõige kui palju on signaal mürast tugevam.snr



C – Kanali mahutavus. (sidesüsteemi kvaliteet) Kui palju bite sekundis võiks sinna kanalisse teoreetiliselt mahtuda.  
B-looduslik piir tuleb ette

Shannoni piir   
B/C <= ½. Kui selline piir on veel täidetud, siis kõik liinis kulgevad andmed on üksteisest sõltumatud ja ei mõjuta teineteist kui c suuremaks ajada siis toimub interferents sümbolite vahel e järjestikused sümbolid hakkavad üksteist mõjutama

Hajaspektririda  
 B/C >> 1 tundub nagu raiskamine



Eelised:  
1. Kui hajaspektri kanali sisse tuleb tavaline kanal väikse ribaliausega (joonis punane ja roheline kanal), siis hajaspektrist lähevad kaduma vaid teatud bitid ja kõrgemad kanalid suudavad neid taastada. Seega hajaspektrimodulatsioon ei sega kitsaribalist, kuna kitsaribaline suudab end samuti parandada.  
2.Kui samas vahemikus samal ajahetkel on 2 hajariba signaali, siis nad ei sega üksteist.  
3. TDMA – time divisjon multiple Access. Üks kasutab ühe hetkel ja teine teisel hetkel  
FDMA – WDMA – samad kanalid erineval lainepikkusel/sagedusel  
CDMA – code divisjon multiple Access – hajaspekter kasutab seda ehk saad istuda samal lainepikkusel teiste kasutajatega ilma , et neid segaks.  
4.D on müra piir. Kanal on alla müra piiri SNR << 1. Hea, ei saa pealt kuulata , kuulda on müra ->  
-> Low Probability of Intercept – radarites ka

Kuidas spektrit laiali määrida?  
1)FHSS – Sagedushüplemine  
vahetame sidekanalit iga natukese aja tagant  
1) aeglane – kanali vahetamise kiirus on aeglasem kui info edastus kiirus  
2)kiire – ühe biti edastamisel vahetatakse kanalit mitu korda

Kuna oled ühel kanalil lühikest aega, siis ei eristata nii suurt võimsust, seega mitmest vahetuvast lühikest aega, siis ei eristata nii suurt võimsust, seega mitmest vahetuvast lühikest ja kõrgemast kanalist tundub olevat üks lai ja madalam kanal  
Kanalid saavad koos „ringi hüpata“, ilma et üksteist segaks kuna eaalselt on nad samal ajahetkel eri kanalites  
nt „bluetooth“  
sagedushüplemine on tõhus kui vaenlane ei tea sageduste vahetamise rütmi

Pseudojuhuslik jada  
Binaarne, statistiliselt sarnane juhuslikule jadale (mürataoline)   
Tegelik tekkeprotsess deterministlik, jada seega perioodiline  
M-jada: maksimaalse pikkusega N = 2 n -1  
Tekitatakse tagasisidestatud nihkeregistriga (pikkus n)

Vaja 0 ja 1 esinemise tõenäosus saada võrdseks  
vastuvõtjale vaja öelda nihkeregistri konfiguratsioon

Hajaspekter-sidesüsteemid – infosignaal hajutatakse laia sagedusribasse. On olemas kahte

tüüpi:

– Sagedushüplusega (FHSS) – edastus näivalt juhuslikult muutuvatel sagedustel, kus

vastuvõtja järgib saatesageduse hüppeid. Siin infosignaai ribalaius on võrdeline kanali

ribalaiusega, kuid igal kanalil toimub edastus teatud aja kestel. Sageduste kasutamise

järjekord on määratud pseudojuhusliku hajutatava koodiga. On olemas kiire ja aeglane,

vastavalt sellest, kui kiirelt muutub sagedus bitti ülekandmis aja suhtes.

– Otsejadaga (DSSS) – igale infobitile vastab edastatud signaalis mitu bitti, iga kasutajaga

on seotud unikaalne hajutav kood. Siin hajutamine toimub pseudojuhusliku bittijada abil

(müra taolisele).

ortogonaal-FDM Euroopas, Jaapanis ja Austraalias kasutatav digitaaltelevisiooni modulatsioonimeetod. 1990-ndate algul propageeriti seda esialgu 5 GHz juures töötava raadio-kohtvõrgu (WLAN) tehnoloogiana. OFDM’i spektrilaotusmeetod jaotab edastatavad andmed üle paljude kandevsageduste, mis erinevad üksteisest täpsete sageduste võrra. Selline eraldamine annabki meetodile "ortogonaalsuse", mis takistab demodulaatoritel "näha" teisi sagedusi peale enda omade. Kodeeritud OFDM (COFDM) puhul on OFDM-meetodile lisatud ka ennetav veaparandus

globaalne positsioneerimissüsteem Süsteem, mis võimaldab määrata asukohta Maa pinnal mitme satelliidi raadiosignaalide võrdlemise teel. Süsteem koosneb 24-st raadiosaatjate ja aatomkelladega varustatud satelliidist. GPS vastuvõtja asukoha määramiseks kasutatakse triangulatsioonimeetodit. Sõltuvalt vastuvõtja geograafilisest asukohast võrreldakse GPS-signaale kuni kuuelt satelliidilt ja arvutatakse välja aeg, mis kulub signaali jõudmiseks igalt satelliidilt vastuvõtjani ning selle alusel arvutatakse välja vastuvõtja asukoht

IEEE raadiokohtvõrgu (traadita kohtvõrgu) standardite perekond, millele pandi alus aastal 1997. Esimene praktikasse juurutatud standard 802.11b määrab ära andmekiiruse 1 kuni 11 Mbit/s vabas sagedusalas 2,4 GHz ning kasutab DSSS tehnoloogiat. WECA on sellele standardile vastavate toodete jaoks võtnud kasutusele kaubamärgi "Wi-Fi" ("Wireless Fidelity").

1998. a. Ericssoni, Inteli, Nokia ja Toshiba koostöös välja töötatud mobiilside spetsifikatsioon. See kirjeldab, kuidas mobiiltelefonid, sülearvutid ja elektronmärkmikud (PDA) saavad lihtsal viisil andmeid vahetada nii omavahel kui ka kodu- või töötelefonide ja lauaarvutitega lühikese vahemaa pealt (kuni 10m ).

Bluetooth võimaldab mobiiltelefonide, piiparite ja pihuarvutite või elektronmärkmike kasutajatel endale muretseda kõiki kolme funktsiooni ühendava mobiiltelefoni. Et taoline mobiiltelefon saaks suhelda lauaarvuti, printeri, faksiaparaadi, lauatelefoni vms seadmega, tuleb kõigisse neisse seadmetesse monteerida vastav mikroskeem. Esimesed Bluetooth’i spetsifikatsioonile vastavad tooted jõudsid turule 2000.a. teises pooles. Praegu on Bluetooth’i asutajatega ühinenud juba umbes 1200 riist- ja tarkvarafirmat, hiljuti ühines ka Microsoft.

Bluetooth põhineb raadioside standardil IEEE 802.15.1 ja töötab samas sagedusalas nagu WiFi. Lisaks andmesidekanalile on võimalik kasutada ka kolme kõnekanalit. Igal seadmel on oma unikaalne 48-bitine aadress. Ühendused võivad olla nii kakspunkt- kui multipunktühendused. Andmeedastuskiirus on 1 Mbit/s (teise põlvkonna seadmetel 2 Mbit/s). Sagedushüpitamise kasutamine lubab töötada ka piirkondades, kus esineb tugevaid raadiohäireid. Saab kasutada ka krüpteeritud andmevahetust

# Mobiilside, kärgvõrgud, sageduste taaskasutus, kärgede jaotamine.

mobiilside, traadita side Terminit "traadita side" kasutatakse telekommunikatsioonisüsteemide kohta, kus signaalikandjaks on mitte juhtmed nagu tavalistes telefonivõrkudes, vaid elektromagnetlained (raadio- või infrapunalained). Mõnikord kasutatakse traadita ühenduse tarvis ka helilaineid (näit. hoonete valvesüsteemides). Sageli kasutatakse termini "wireless" vastena sõna "raadio-", kuid see pole päris täpne. Näiteks haarab "wireless" ka infrapunasidet, "raadio" aga mitte.

A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. This base station provides the cell with the network coverage which can be used for transmission of voice, data and others. In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell.

This means that, in a standard FDMA system, there must be at least a one cell gap between cells which reuse the same frequency.

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

Põhjamaades (ka Eestis) enne GSM süsteemi kasutusel olnud analoog-mobiiltelefonisüsteem, mis töötab kas 450 MHz või 900 MHz sagedusalas ja mida on hiljem hakatud nimetama 1. põlvkonna mobiilsidesüsteemiks. On ka praegu veel käigus, kuigi kasutajaid jääb järjest vähemaks.

Teise põlvkonna mobiilside tehnoloogia nimetus. Kui esimese põlvkonna mobiilside oli analoogside (vt. nt. NMT), siis teise põlvkonna mobiilsides toimub kõnesignaali edastamine digitaalselt. Kuna aga sidetehnoloogiana kasutatakse ka siin kanalikommutatsiooni, siis võimaldab 2G edastada ainult digitaalset kõnesignaali ja abiinfot, andmeside võimalust see ei paku. Mõnes 2G süsteemis, nagu nt. GSM, on küll olemas SMS-sõnumite vahetamise võimalus.

Eestis hakkas EMT pakkuma GPRS teenust 2001.a. ja see võimaldab andmeedastust kiirusega 56 kuni 114 kbit/s ning pakub mobiiltelefonide ja personaalarvutite kasutajatele pidevat internetiühendust. Suur andmeedastuskiirus annab mobiilkommunikaatorite, pihuarvutite ja sülearvutite omanikele võimaluse korraldada videokonverentse ja kasutada interaktiivseid veebisaite ning muid taolisi lahendusi.

GSM mobiiltelefonisüsteemi kiirem versioon andmeedastuskiirusega kuni 384 kbit/s (EDGE on kolm korda kiirem kui GPRS), mis teeb mobiiltelefonide ja kaasaskantavate arvutite omanikele võimalikuks multimeedium- ja teiste lairibarakenduste kasutamise.

Kolmanda põlvkonna (3G) laiaribaline mobiilside tehnoloogia andmeedastuskiirusega kuni 2 Mbit/s. 3G teine nimetus on UMTS. Peale kõne- ja andmeside võimaldab 3G tehnoloogia edastada ka audio- ja videoinformatsiooni mobiilseadmetele üle kogu maailma läbi statsionaarsete, mobiil- ja satelliitsidesüsteemide

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

# Mobiilpositsioneerimine, kärje tunnus CI, kaugus tugijaamast TA –timing advance.

mobiil-positsioneerimissüsteem GSM-võrgus kasutatav süsteem mobiiltelefoni asukoha kindlaksmääramiseks võrgu tugijaamade suhtes. Eestis pakub seda teenust EMT

# Valemid

I – saadud informatsiooni hulk [bit]  
P – tõenäosus, et midagi juhtub

B – bandwidth ehk ribalaius

[dB]

Näitab kui palju üks võimsus erineb teisest

P – signaali võimsus [W]

Võimsuse võrdlemine 1mW võimsusega.

Logaritmiga võib ainult liita ja lahutada:

log(a b) = log a + log b  
log(a:b) = loga – log b

[kordades] =

Signaali ja müra suhe ehk kui palju on signaal mürast tugevam

SNR[dB] = S[dBm] – N[dBm] = 10 log()

Shannoni valem

C =

C – kanali mahutavus ehk sidesüsteemi kvaliteet [bit/s]

# Näiteülesanded

1. Visatakse kulli ja kirja. Kui suur on saadud informatsioon, kui tegu on tavalise mündiga, mida pole kuidagi mõjutatud?  
P= 0.5 => I = log2(1/0.5) = log22 = 1 bit

2. Wifi võimsus dBm’ides, kui P = 0.1W

P[dBm] = 10 log(0.1 / 0.001) = 20 dBm

3. Koakskaabel. D = 1.2”. l = 100m. F = 1200 MHz = 1.2GHz. S = 100mW = 0.1W

leida S[dBm] ja S0(signaal kaabli väljundis) nii kordades kui dBm?

Sumbuvus K = 8 dB – väljundis on signaal 8 võrra väiksem

S[dBm] = 10 log(S / 1mW) = 10 log 100 = 20 dBm

K[kordades] =

S0 = S/K = 100/6.3 = 16 mW

S0 = S[dBm] – K[dBm]= 20 – 8 = 12 dBm

4. Oletame et on arvuti A ja B ühendatud 10BASE2 võrku. A tahab saata Ble 7230B informatsiooni. Kasutatakse MAC/LLC protokolli. Kui kaua võtaks aega ja kui suur oleks andmeedastuskiirus?

C=10Mbit/s = 107bit/s

MAC/LLC protokoll

|  |  |  |  |
| --- | --- | --- | --- |
| Mac päis  22B | LLC päis  3-4B | Info | Mac treiler  4B |
| 46 – 1500B | |

LLC päise pikkus 4B

Infot saab korraga edastada 42 – 1496 B

7230:1496 = 4.92.

Tuleb saata 5 paketti: 4x1496 B + 1246 B

Päised annavad juurde 5x(22 + 4 + 4)

Kokku saadetakse 7380B = 59040 biti infot.

t = 59040 / 107 = 5.9 ms

info edastuskiirus

7380 B -------- 10 Mbit/s

7230 B -------- v Mbit/s

v = (7230 / 7380) \* 10Mbit/s = 9.8 Mbit/s

5. C = 50 Mbit/s = 6.25 MB/s

tahetakse saata 2MB fail. Andmeid saadetakse 1024B kaupa, ning selle sees on ja 64B päise infot. Kõik paketid saadetakse järjest ning nende töötlemise aega ei arvestata. Kui kaua seda faili saadetakse?

Mitu paketti on vaja saata?

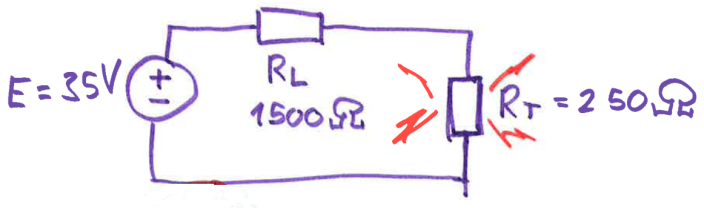
2MB = 2 x 106 : (1024 - 64) = 2083.333

Kuna tuleb alati saata 1024B infot, siis tuleb ümardada üles täisarvuni. Viimase pakti lõppu lisatakse lihtsalt täidet. Seega saadetakse 2084 paketti.

Saadetakse 2084 x 1024 = 2.134016B informatsiooni edasi.

t = 2.134016 : 6250000 = 0.34s

6.



PT=?

I=U/R P=UI=

PT=UT IT

R=RL + RT

I=IT=U/R=E:( RL + RT) = 0.02A

UT=IT RT => P = IT2 RT = 0.022 x 250 = 0.1W

7.

IP-aadress 186.172.10.0

Võrgumask: 255.255.255.0

Mitu aadressi selles võrgus saab olla? 256.

Võrgumask näitab ära mis osa IP-aadressist on võrgu aadress. Ülejäänustest saab moodustada kõik võimalikud kombinatsioonid saab teha kõikides ülejäänud kombinatsioonidest, jättes võrguaadressi kogu aeg samaks.

8. Kui kaua võtab aega, et 10BASE2 võrgus andmed kõigini jõuaksid?

C=10Mbit/s

Max pikkus l = 200m

v = 2/3 c

c(valguskiirus) = 3 x 108 m/s

t=l/v = 10-6s = 1 μs

Mitu biti jõuab saatja saata enne, kui kõige kaugemal asuv vastuvõtja esimese biti kätte saab.

t = 1 μs

v = C = 10Mbit/s = 107 bit/s

n = v t = 107 x 10-6 = bit

9. Värviline pilt 1000 x 860 pikslit.

1 piksel = 3x8bit = 3B (RGB)

np= 1000x 860 x 3 = 2.58 MB

Sama pilt video lõiguna

t = 30 kaadrit/s

nv = 2.54 MB x 30 = 77.4 MB/s

10. EDGE võrk

C = 600 kbit/s

SNR -?

Shannoni valemi kasutus.

On teada, et EDGE võrgu ribalaius on 200kHz

C =

11. Kärgside. Tugijaam P = 10 W. Telefoni TA = 20. Sumbuvus 10 dB/km

PV – võimsus telefonis

Terminali kaugus tugijaamast R = TA x 550m = 11 km

Võimsus telefonis on 11 x 10 = 110 dB väiksem

P[dBm] = 10 log (10/1mW) = 40 dBm

PV = 40 dBm – 110 dB = -70 dBm

12. GSM telefon. Väljundi võimsus P=2W. Aku pinge U = 5 V. Saatja kasutegur η = 30% = 0.3. Kui suurt voolu telefon tarbib I-?

P= η I U => I = = 1.33 A

13. Maa geostatsionaarsel orbiidil on üks satelliit mille kaudu kaks arvutit maal omavahel suhtlevad.

C = 100 kbit/s

Paketi suurus 1000 bit

Vastuse suurus 100 bit.

Kaua kestab andmeside, kui üks saaba paketi ja teine saadab vastuse. Töölemiseks kuluvat aega ei arvestata.

Geostatsionaalse orbiidi kaugus R = 36000 km

Signaali levimise kiirus v = c = 300000 km/s

Paketi edastamiseks kulub tpak = 1000/v = 0.01 s

Vastuse edastamiseks kulub tACK = 100/v = 0.001 s

Signaal levi õhus R/V = 0.12s

tsaatmine = 2R/V + tpak = 0.25s. saadetakse pakett korra stelliidile ja siis koheselt tagasi ning siis veel läheb aega paketi kohale jõudmiseks.

tvastamine = 2R/V + tACK = 0.241 s

T = tsaatmine + tvastamine =0.491 s