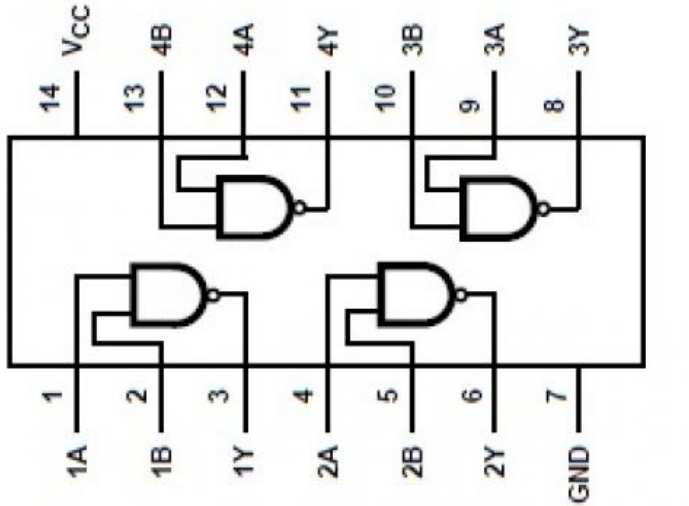
Elektrooniku sõber teab,et need on kõigest lihtsad NING-EI digitaalloogikaelemendid. Digipädevavatel rohelistel küberekspertidel pole aga tänapäeval sageli aimugi sellest, et nende abil on võimalik ära kirjeldada kogu nende digitarkus.



A	B	Y
0	0	**1**
0	1	**1**
1	0	**1**
1	1	**0**

(M.J.2024)

EET3010 JUHTIMIS - JA ANDMESIDETEHNIKA ALUSED

Kevad 2025

Digitaaltehnika- Arvutivõrgud

Martin Jaanus NRG-308
martin.jaanus@ttu.ee 56 91 31 93

Õppetöö : http://isc.ttu.ee
Õppematerjalid : http://isc.ttu.ee/martin

(Tele)kommunikatsioon

- Telekommunikatsioon (nimetatud ka: elektrooniline side, kaugandmeside, kaugside) tähendab informatsiooni edastamist ja sidepidamist pikemate vahemaade taha. (wikipedia)
- Oluline on infromatsiooni edastamine.
- Väiksem infoühik on bitt (0 või 1) See võib tähendada aga palju, näiteks:

  - Sõda võidetud (0-ei , 1 jah)
  - Kas „tasuta“ sõiduõigus on olemas (0-ei, 1 jah)
  - Inimese sugu (0- mees, 1 naine)
  - Jne.....

Tele (kreeka k. τῆλε) - tähendab kauget , kõik sõnad , millel on see ees tähendab, et midagi on eemal - Televiisor, telefon, telemehaanika , teleport, jne…

Kommunikatsioon /side

- Kommunikatsioon e. informatsiooni (andmete) vahetus
  - Informatsioon on jagatud sõnumiteks
  - Sõnumit kannab edasi signaal
  - Signaal on ajas või ruumis muutuv füüsikaline suurus

Meedia

Signaal - Ajas või ruumis muutuv füüsikaline suurus, kannab edasi informatsiooni (õhurõhk, pinge, vool , elektromagnetväli – raadiolained, valgus)

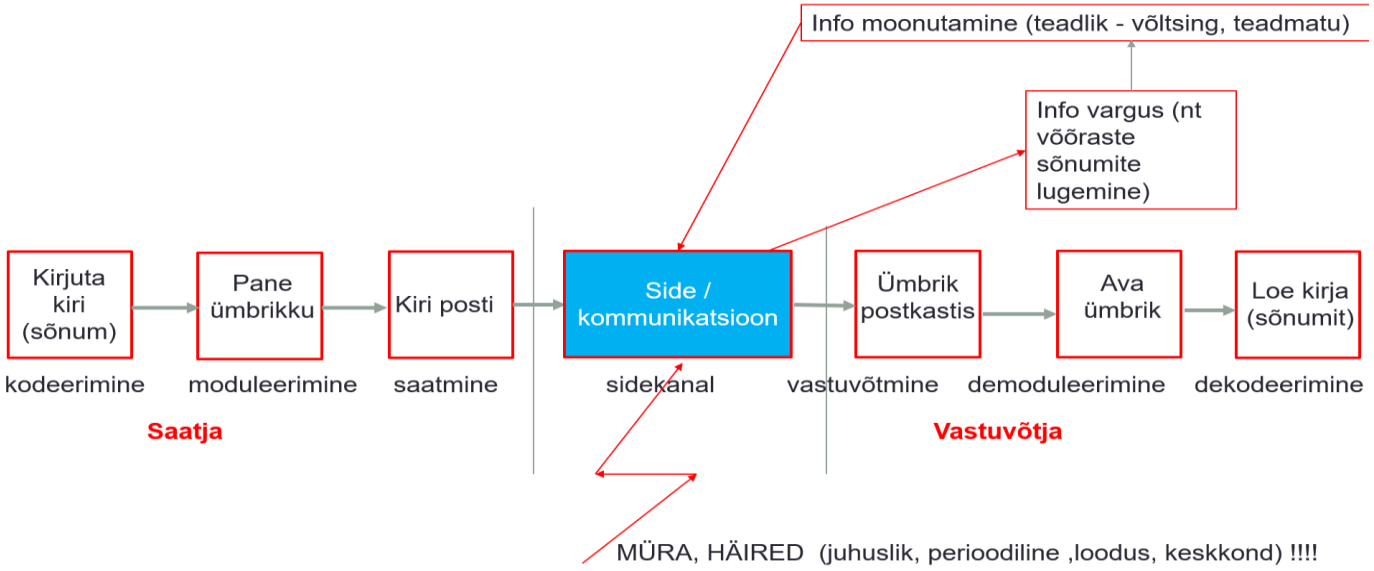
Kaksport, milles toimub signaali ülekanne, võib olla järgmistes meediates

- Liinid (kaks juhet, koaksiaal, juhitud meedia)
- Akustiline (allveeside), heli
- Fiiber(valgus)
- Vaba ruum (eeter, juhtimata meedia), elektromagnetlained (ka valgus)

- Siit tuleb ka sõna multimeedia (tarbime mitut eri liiki meediat korraga)

Sidekanal

- Saatja muudab signaali sidekanalile sobivale kujule
- Signaal muutub sidekanalis
- Vastuvõtja muundab kanalist tuleva signaali ja muudab selle esialgsele kujule
- Vastuvõtja peab taastama vastuvõetud signaalist saatja poolt saadetud esialgse sõnumi
- Nii saatja kui ka vastuvõtja peavad arvestama sidekanali omapära kui ka saate- ja vastuvõtu tingimustega



Andmeedastuskiirus

- Edastuskiiruse ühik bit/s – bitti sekundis
- kbit/s – 1024 (!) 2^{10} bitti sekundis
- Mbit/s – 1024 (!) 2^{10} kilobitti sekundis
- Gbit/s – 1024 (!) 2^{10} megabitti sekundis
- Kasutatakse ka ühikut B/s (bait sekundis) koos 2^{10} kordajatega
- Üks bait on 8 bitti ehk 1 B/s=8 bit/s
- Telekommunikatsioonis kasutatakse ka ühikut Baud (Bd) Émile Baudot – 1926, mis näitab tegelikku (kasulikku) sümboliedastuskiirust (sümbol võib olla ka 1 bitt/bait aga ei pea olema , võetakse arvesse ka tehnilisel eesmärgil saadetud bitid (kontroll, paarsus ,jms)
- Kasutatakse meetrilist prefixi 1kBd=1000 Bd jne

.

Kui kiiresti saab üldse andmeid edastada ?

- 1927 Nyquist avastas, et (telegraafi) ülekande kanali sagedusriba peab olema vähemalt 2 korda laiem edastatavate pulsside sagedusest. $f_p \leq 2B$
- 1940 ndad Claude Shannon formuleeris (digitaalse) infomatsiooniedastuse teooria.
- Claude Shannoni ja Ralph Hartley seadus :

C – maksimaalne bitiedastuskiirus (sh kontroll jms bitid) $C = B \log_2 \left(1 + \frac{S}{N}\right)$

B – ülekandeahela ribalaius (hertsides)

S – kasuliku signaali võimsus (vattides)

N – müravõimsus (vattides)

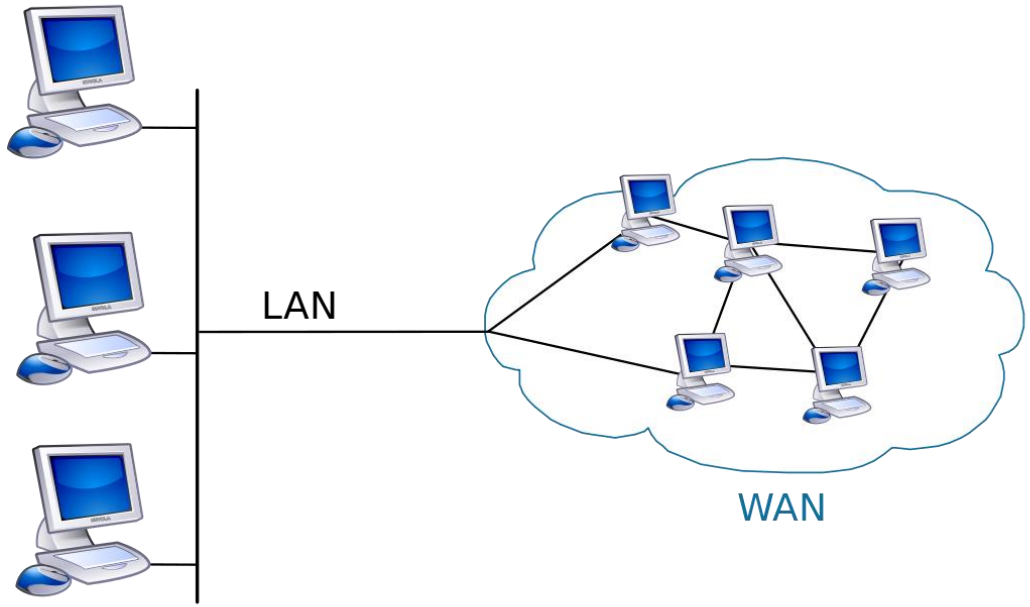
S/N tähistatakse ka kui signaali – müra suhet (ühikuta suurus), avaldatakse ka detsibellides.

Arvutivõrk

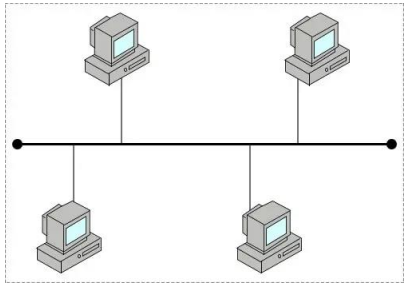
- Mõelge ämblikuvõrgule, aiavõrgule, elektroenergeetikud - elektrivõrgule
- Kohtvõrk (LAN) – Local Area Network
- Kaugvõrk (WAN) – Wide Area Network (ka Internet)
- Alates 1969.
- Toimimise idee – luua läbi võrgusõlmede , ruuterite abil kahe seadme vahele sidekanal , mis on seadmetele “nähtamatu”.

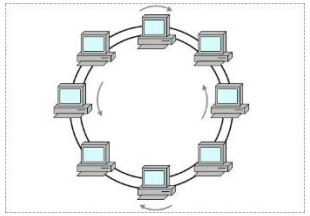
- Kuidas seadmed teineteist leiavad ?
- Kuidas levib sõnum üle arvutivõrgu ?

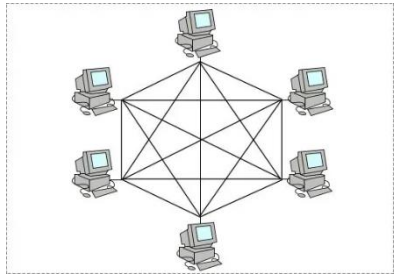
- Pilt – Wikipedia
- P.S. Selle temaatika pildid on üldjuhul arhailised

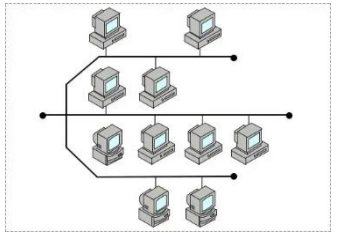


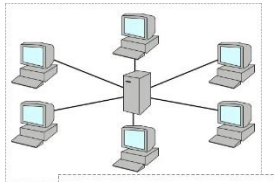
Arvutivõrkude topoloogia

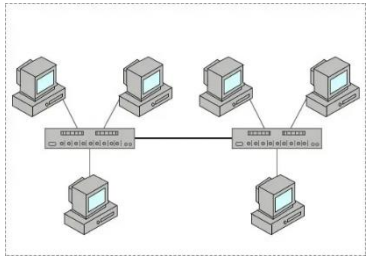


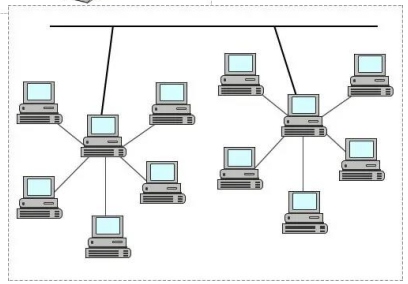












- Siinitopoloogia (bus) – nt koaksiaalkaablivõrgud
- Jagatud siinitopoloogia
- Ringtopoloogia (vananenud)
- Kõik kõigiga (mesh , vananenud)
- Tähttopoloogia (keskseadmega) , enamus kodulahendusi
- Hübriid ja puutopoloogia , suuremad võrgud , jne

- Igal juhul info peab jõudma ühest arvutist teise

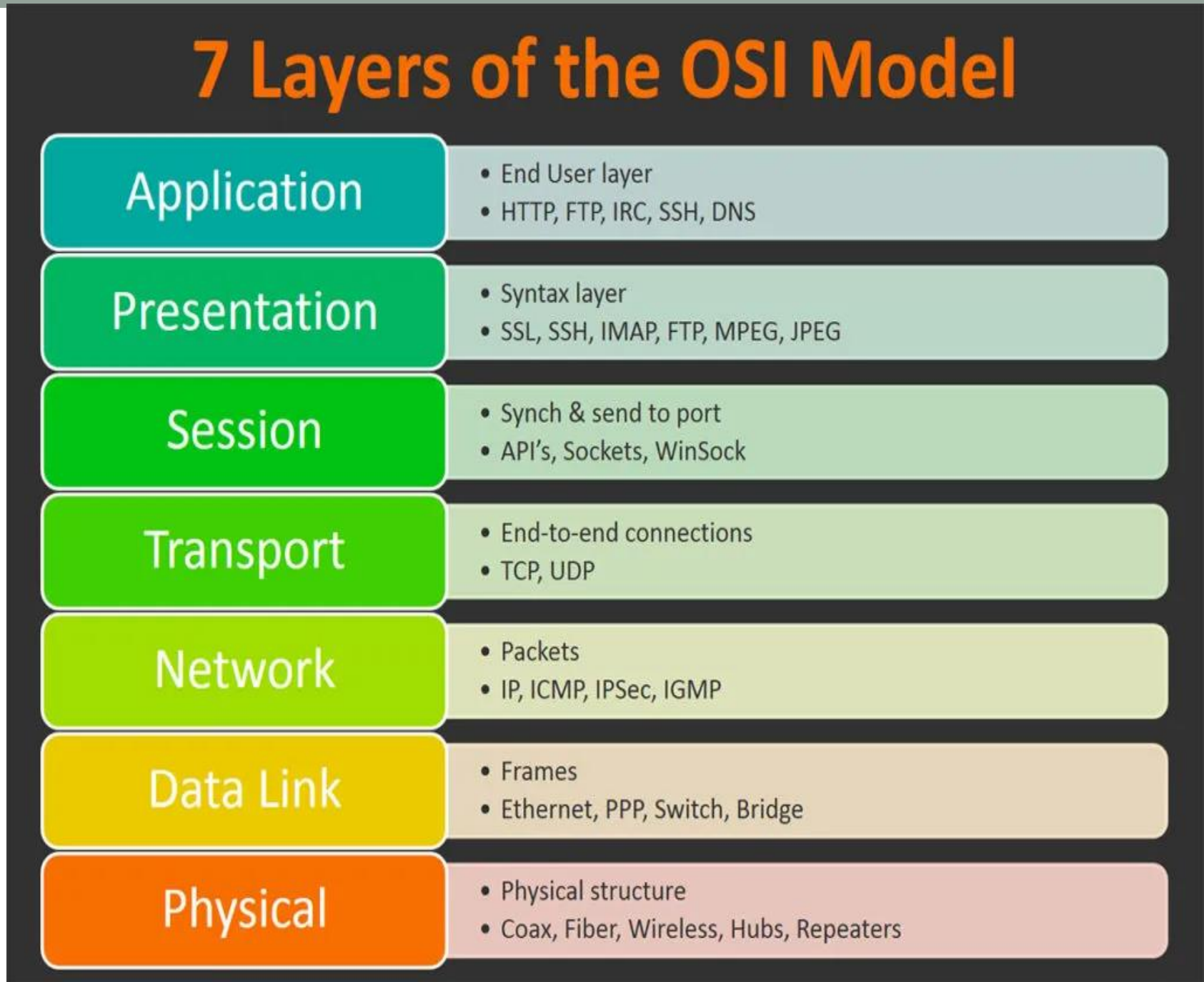
- Võrgusõlmedes on jaotorid (hub, switch, router,), mis suunavad liikluse õigesse kotha.

7 kihilline mudel

7 kihiline võrgumudel

- 7 – Rakendus
- 6 – Süntaks
- 5 – Session
- 4 – Transport
- 3 – Paketid
- 2 – Kaadrid
- 1 – Füüsiline media

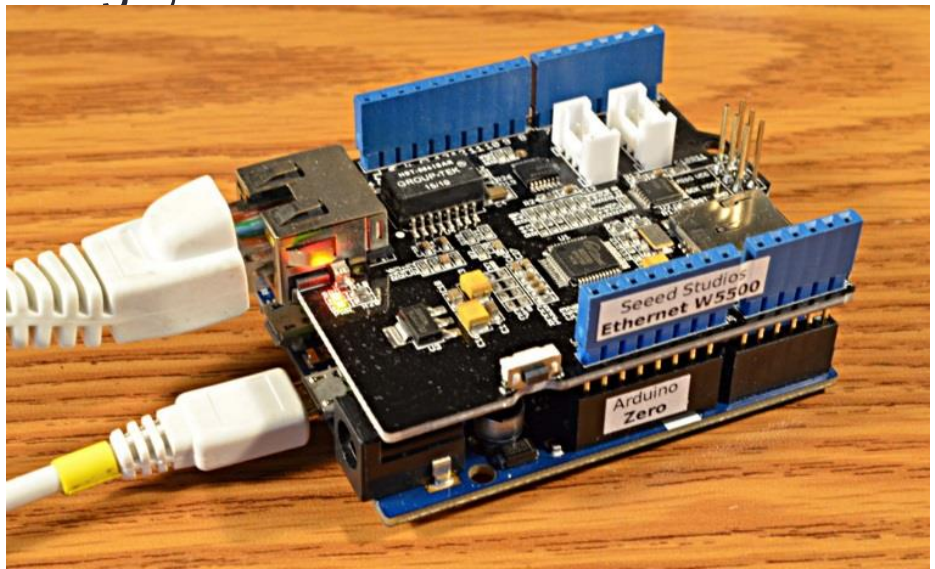
- Pilt -> Wikipedia



IEEE 802.3 (Ethernet)

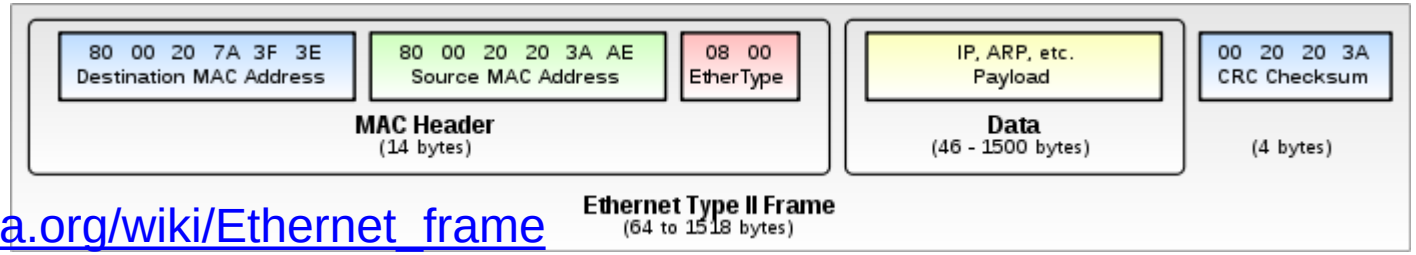
- Esmased standardid juba 1973
- IEEE 802.3 1983 ja on muudatustega püsinud tänaseni
- IEEE 802.3cc (2017) 25Gbit/s
- Ethernet määrab juhtmete ja pistikute tüübid, kirjeldab füüsilist signaali ülekannet ning määrab andmevahetuse formaadi.
- Ethernet on aluseks võrguprotokollidele nagu TCP/IP, millega tagatakse interneti ja muude võrkude toimimine.
- Selle standardid on tihedalt seotud OSI füüsilise kihiga, täites mudeli kahe alumise kihi (füüsiline kiht ja lülikiht) funktsioone.

Arduino plaat ja Etherneti moodul →



IEEE 802.3 (Ethernet)

- Etherneti põhised süsteemid jagavad andmevood väiksemateks kaadriteks (inglise k. frame).
- Iga kaader peab kindlasti sisaldama saatja ja vastuvõtja MAC aadressi ja andmeid veakontrolliks.
- Kaadri keskosas on piirkond andmete jaoks, mida üle kantakse. Andmed võivad sisaldada teiste protokollide päiseid, nagu näiteks IP protokoll (inglise k. Internet Protocol).
- Veakontroll on realiseeritud 32 bitise tsükkelkoodkontrolli meetodil, kus saatepoolel rakendatakse edastamisele kuuluvale andmeplokile 32-bitist polünoomi, mille tulemusena saadav kood lisatakse plokile.
- Vastuvõtupoolel rakendatakse andmeplokile sama polünoomi ja kui tulemused kokku langevad, loetakse andmeedastus õnnestunuks.

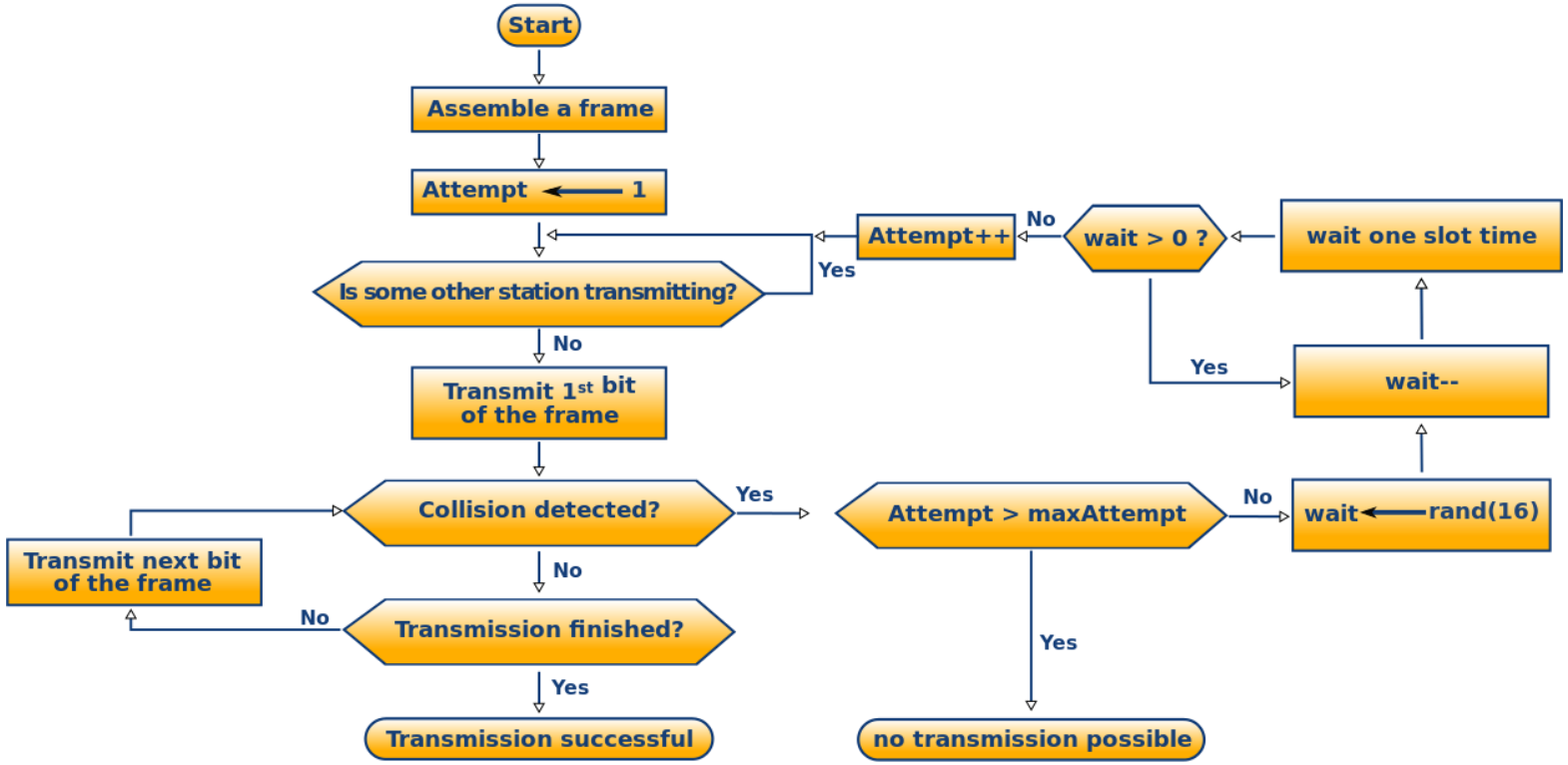


https://en.wikipedia.org/wiki/Ethernet_frame

IEEE 802.3 (Ethernet)

Füüsiline kiht – Palju seadmeid jagavad sama meediakanalit.

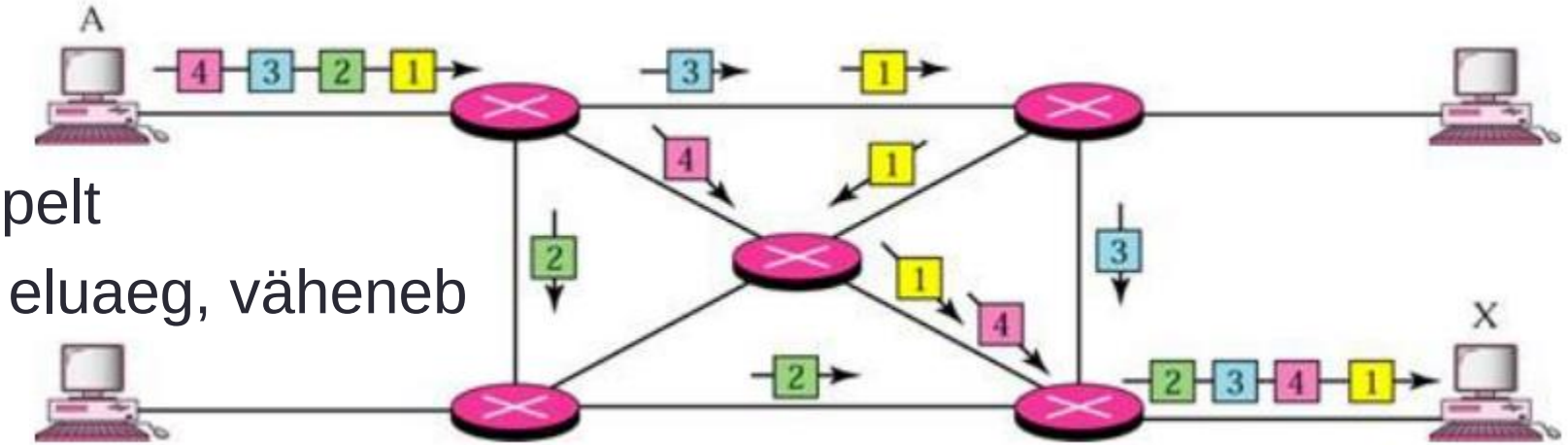
- CSMA/CD -Carrier-sense multiple access with collision detection .
- Kontrollitakse, kas kanal on vaba ning saadetakse pakett ära.



https://en.wikipedia.org/wiki/Carrier-sense_multiple_access_with_collision_detection

Pakettedastus (IP)

- Suurema hulga info (sõnumi) tükeldamine väiksemateks osadeks.
- Võib võrrelda kaubarongiga, kus vagunid võivad liikuda lõppjaama erinevates koosseisudes ja mööda erinevaid teid .
- Lõpus pannakse väiksematest tükkidest kokku saatmisele läinud info .
- Kui pakett läheb kaduma, saab anda käsu uuesti saata (see tegelikult on TCP ülesanne) .
- IP (Internet protocol) hooliseb selle eest , et oleks teada ,kust pakett pärineb ja kuhu see läheb.

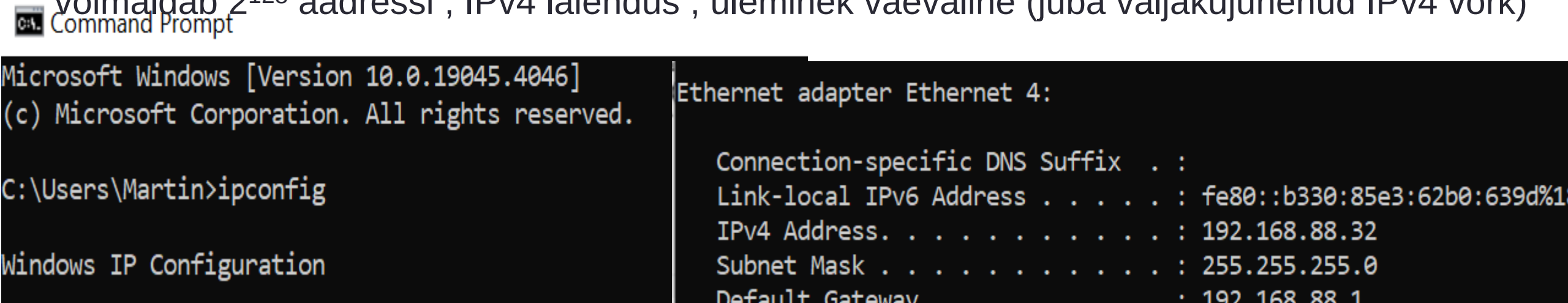


- Mõni pakett võib jõuda topelt
- TTL (time to live) –paketi eluaeg, väheneb

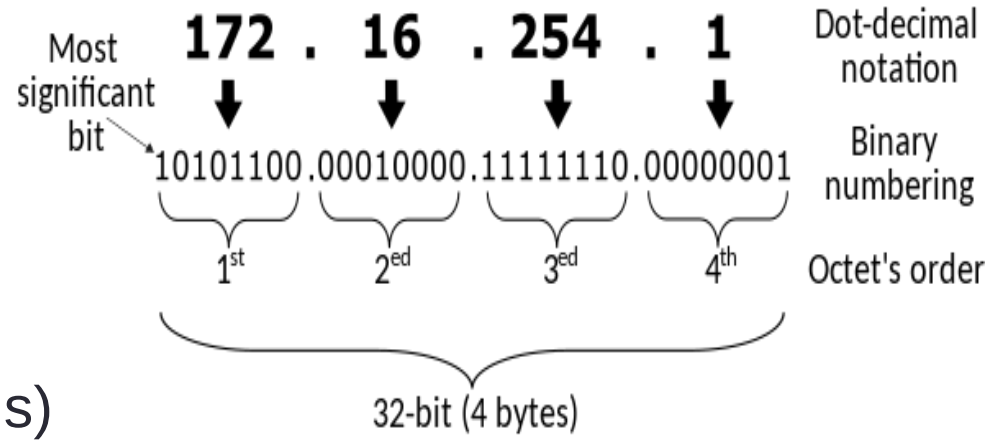
igas sõlmes

IP aadressid

- Jagab - Internet Assigned Numbers Authority (IANA), USA –aadressivahemikud teenusepakkujatele
- Seadmel on kaks aadressi – MAC , mis on seotud konkreetse füüsilise seadmega ja peab olema unikaalne.
- IP aadress – seotud arvutivõrguga, tavakasutaja saab tänapäeval automaatselt
- IP version 4 , (alates 1983) 4 baiti, edastatakse sageli kümnendarvuga (nt 192.168,1,5) algselt 2^{32} ehk 4294967296 unikaalset aadressi
- IP version 6 , (alates 1995) 16 baiti, edastatakse 16 arvuna 4FAC::553A:BB44:2215::55DA võimaldab 2^{128} aadressi , IPv4 laiendus , üleminek vaevaline (juba väljakujunenud IPv4 võrk)



IP aadressid (IPv4)



- Igal bitil on oma tähendus
- Nende bittide järgi teevad võrgusõlmed otsuseid andmevoo suunamisel (muide, lihtloogikat kasutades –kiirus)

- Kuni 1993:

Historical classful network architecture

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Number of addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16 777 216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16 384 (2^{14})	65 536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2 097 152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

Pildid -wikipedia

- Pooled IP aadressid asusid USAs
- edasi : Classless Inter-Domain Routing , CIDR (valitakse aadressisegnendi alguse pikkus vastavalt vajadusele Privaatvõrgud – aadressid võivad koduda

Privaatvõrgud

- Avalikke aadresse kõigile ei jätku. Loodud kolm vahemikku privaatvõrkudele
- Privaatvõrgud teineteist ei näe (kui ei kasutata erilahendust)
- Avalikes võrkudes on need aadressid keelatud !

Reserved private IPv4 network ranges[9]

Name	CIDR block	Address range	Number of addresses	*Classful* description
24-bit block	10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216	Single Class A
20-bit block	172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576	Contiguous range of 16 Class B blocks
16-bit block	192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536	Contiguous range of 256 Class C blocks

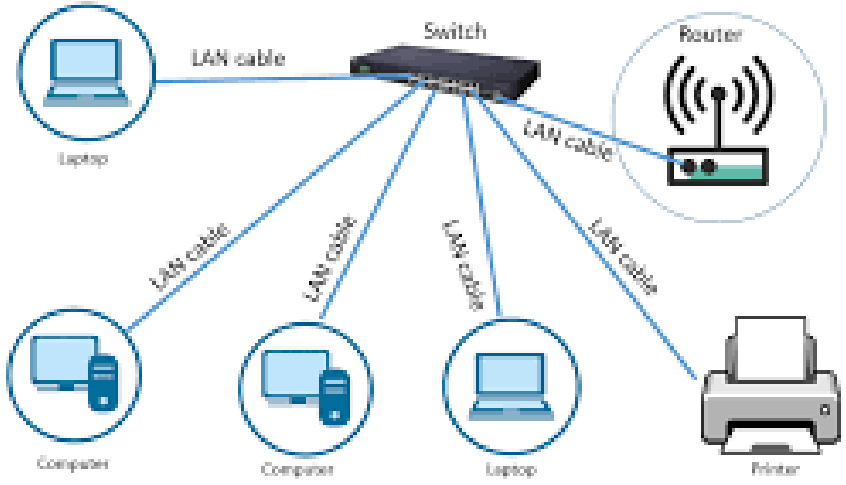
Bittide arv aadressi algusest, mis määrab ära võrgusegmendi siin esimesed bitid on 0000 1010(bin)

Privaatvõrgus

- Seadmel on olemas IP aadress, seotakse MAC aadressiga , füüsilise aadressiga seda teeb ARP (Address resolution protocol)
- DHCP - Dynamic Host Configuration Protocol , saab küsida IP aadressi
- Seadmed “näevad “ teineteist, saavad vahetult suhelda (kui IP aadressi algus on sama, mis kohtvõrgu algusel , vt eelmine slaid)
- Erinevad seadmed ühendatakse füüsiliselt kokku
- Või juhtmeta ühendusega (wifi)
- Seadmete arv sõltub võrgusegmendi suurusest

```
C:\Users\Martin>arp -a

Interface: 192.168.145.234 --- 0xa
  Internet Address      Physical Address      Type
  192.168.145.1         ec-b1-d7-53-6f-7e     dynamic
  192.168.145.8         9c-7b-ef-2b-03-71     dynamic
  192.168.145.12        50-7b-9d-3e-98-4b     dynamic
```



Local Area Network

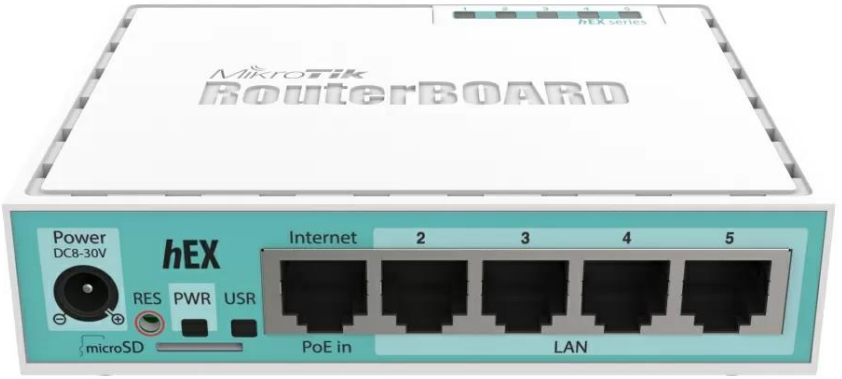
Privaatvõrgust välja

- Privaatvõrgust seadmed välja näha ei oska
- Vajalik on lüüs (gateway) – sellel on 2 füüsilist liidest
- Ja kaks aadressi, sisemine IP PEAB olema samas segmendis teiste seadmetega !
- Kirjad peal LAN ja WAN (või internet vms)
- Integreeritud sageli jaoturiga

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b330:85e3:62b0:639d%18
   IPv4 Address. . . . . . . . . . . : 192.168.88.32
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.88.1
```

Mikrotik HAP ruuter – kõik ühes seade, nagu tänapäeval kombeks sisaldab endas 4 pordiga LAN jaoturit
,
WiFi juurdepääsupunkti ja WAN liidest. Pilt mikrotik.com

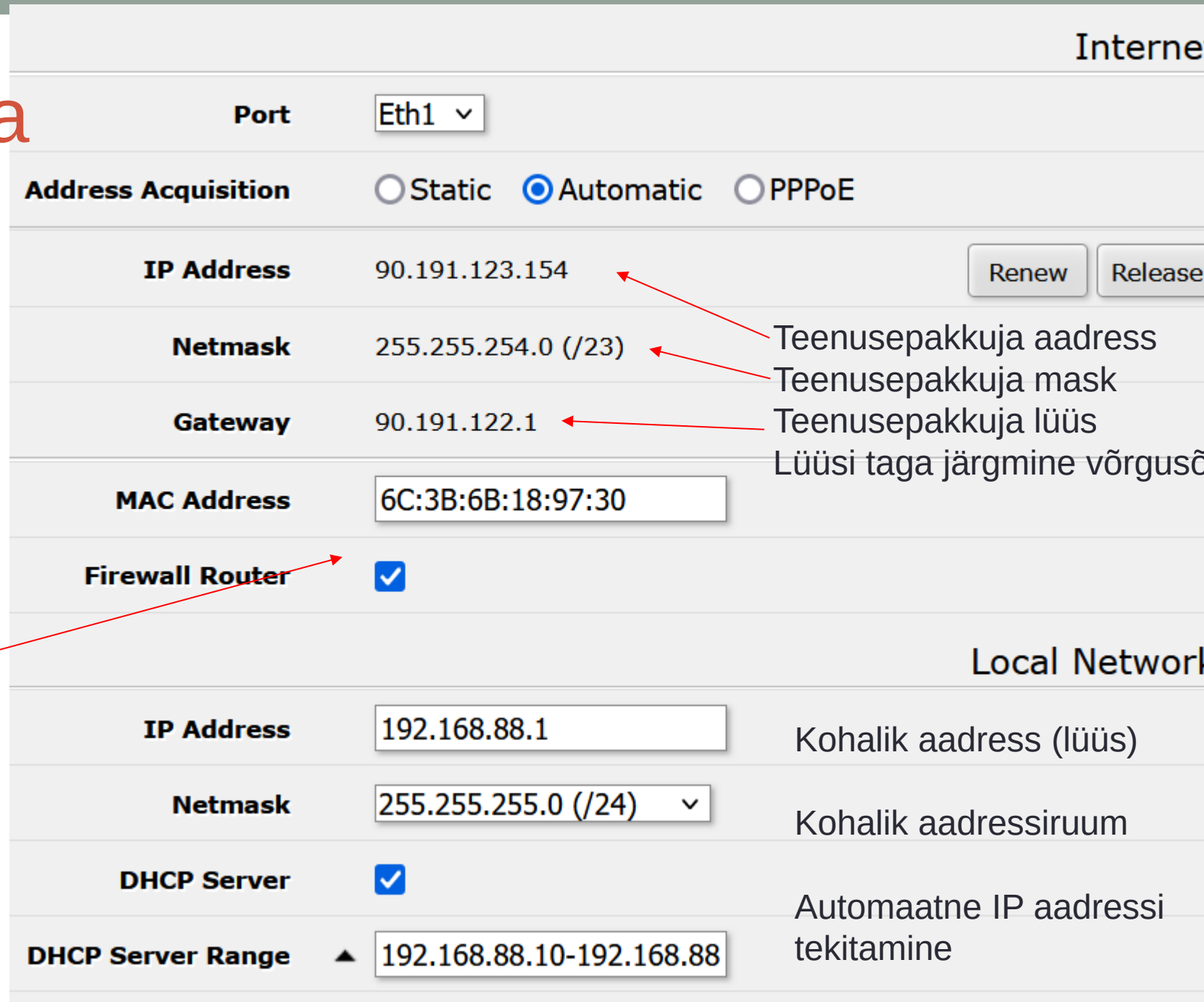


Privaatvõrgust välja

Järgmine võrgusõlm “näeb” privaatvõrku selle aadressina

Võrgumask (subnet mask /netmask määrab ära ,milline osa kuulub oma võrgule, mida edastama ei hakata

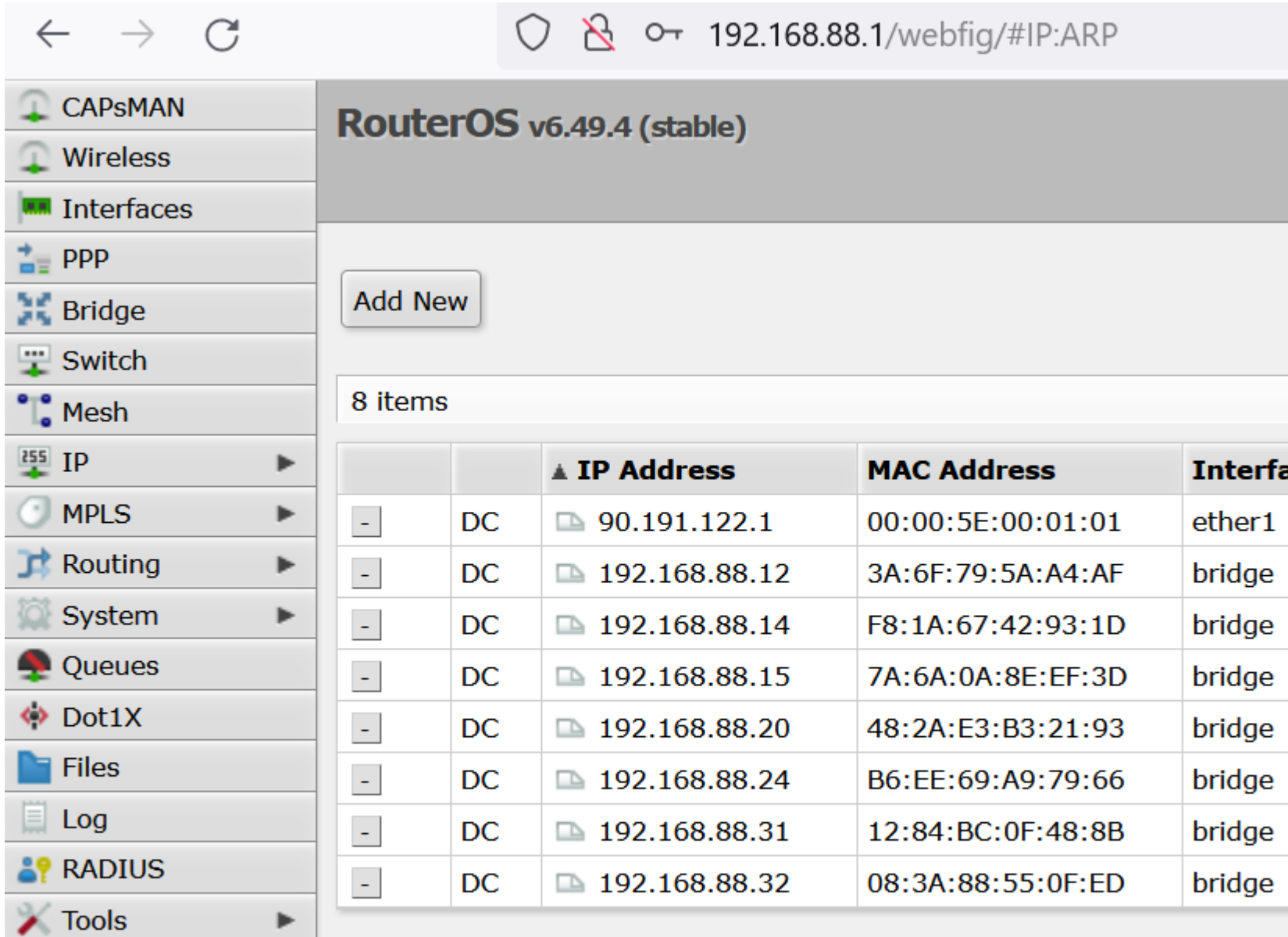
Osad (teadlikule kasutajale) mõeldud seadmed võimaldavad muuta füüsilist aadressi.
NB ! Kui ei tea, mida teed, ära torgi !!!!!



Teadlikele kasutajatele mõeldud võrguseadmete

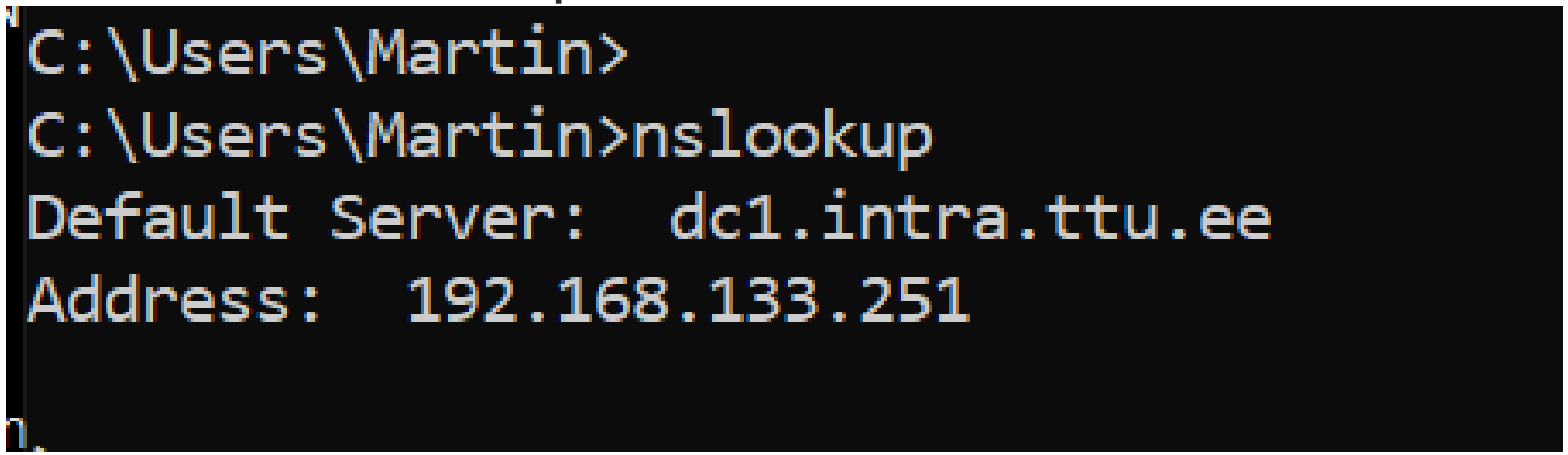
Võimalused on väga laiad

- Võimalus luua selline võrk, mida päriselt vajad, mitte selline, mis odava rendiseadmega tuleb.
- Nõuab oskusi, süvenemist
- Tea, mida teed !!!!



Nimeserver

- Kõik saab tehtud vaid ip aadresse kasutades, aga tavakasutajale on see ebamugav.
- Nimeserver NS (name server) , DNS (domain name server) on register mis seob omavahel nimed ja ip- aadressid (võrrelge oma telefonikontaktidega)
- Lahendab (domeeni)nime IP aadressiks.
- Olemas palju, kohalikke nimeservereid, et asi kiiremini toimiks
- Arvuti seadetes peab olema määratud.



Nimeserver

- Avalikud teenused (nt who.is)

isc.ttu.ee

DNS information

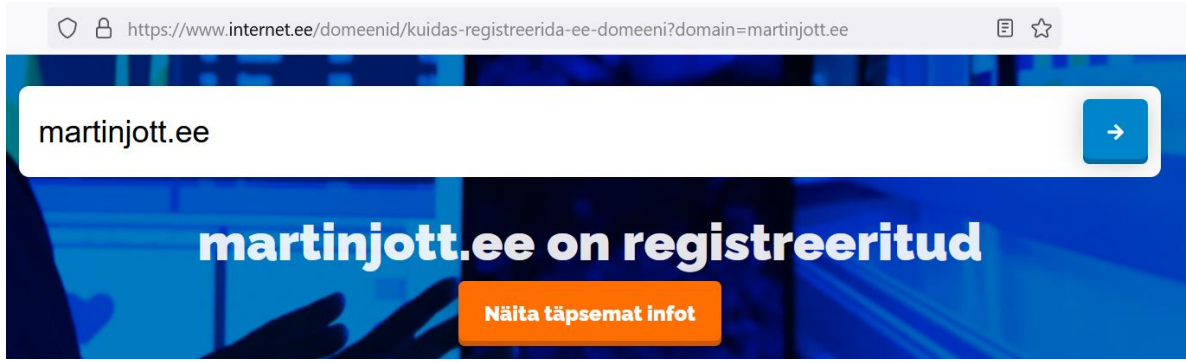
Whois | DNS Records | Diagnostics

DNS Records for isc.ttu.ee

Hostname	Type	TTL	Priority	Content
isc.ttu.ee	SOA	1800		ns.taltech.ee hostmaster@taltech.ee
isc.ttu.ee	A	10800		193.40.240.71

Nimeserver

- Internet.ee , Eesti registripidaja



217.146.69.28

martinjott.ee

Staatus:	**Makstud ja tsoonis**
Registreeritud:	**14.02.2016 16:35**
Muudetud:	**30.09.2023 10:55**
Aegub:	**15.02.2026**
Nimeserverid:	**ns2.zone.ee** **ns3.zonedata.net** **ns.zone.eu**

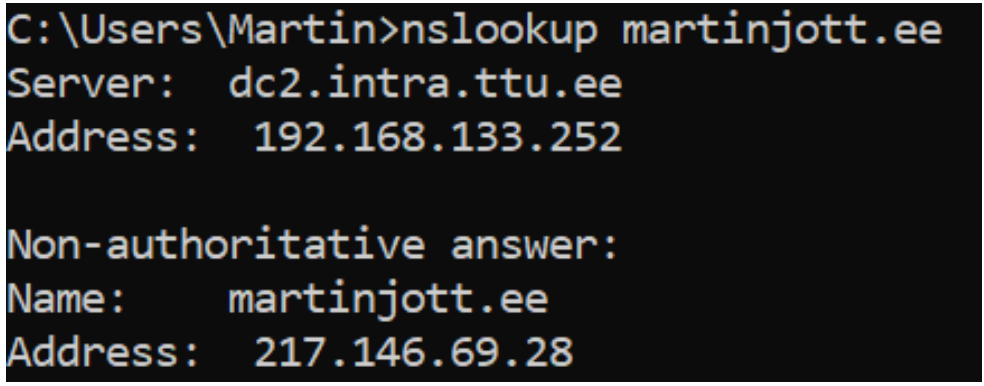
Registreerija:	**Eraisik**
Halduskontakt:	**Avaldamata**
Tehniline kontakt:	**Avaldamata**
Registripidaja:	**Zone Media OÜ** **http://www.zone.ee**

Kontakteeru registreerijaga

Igaüks võib endale domeene registreerida. Tuleb pöörduda registripidaja poole.

Kuidas see kõik koos töötab

- Kirjutame veebilehitsejasse aadressi – nt www.martnjott.ee
- Operatsioonisüsteem küsib nimeserverilt selle sisend IP aadressi 217.146.69.28
- Tehakse võrdlus võrgumaskiga /IP segmendiga Kas on 217.146.69.28 samas alamvõrgus ? EI ?
- Järelikult pöördume lüüsi poole.
- Küsime järgmise võrgusegmendi käest
- Kas on 217.146.69.28 samas alamvõrgus ? EI ?
- Järelikult pöördume lüüsi poole.
- Küsime järgmise võrgusegmendi käest
- Kas on 217.146.69.28 samas alamvõrgus ? EI ?
- Jne….
- Kuni JAH (visualiseerib hästi traceroute)



Traceroute – näitab pakettide teekonda

- Windows keskkonnas käsk TRACERT

Proovime 3 korda PING – ehk koputame uksele (vt järgmine slaid)

```
C:\Users\Martin>tracert www.martinjott.ee

Tracing route to martinjott.ee [217.146.69.28]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.145.254
  2    <1 ms    <1 ms    <1 ms  fg-1800f.taltech.ee [193.40.242.158]
  3     1 ms    <1 ms    <1 ms  soc-1k-core-vsp-2.ttu.ee [193.40.250.253]
  4     1 ms     1 ms     1 ms  ttu-gw.eenet.ee [193.40.244.1]
  5     1 ms    <1 ms    <1 ms  kjj-bb3-xe-1-0-2-3-0.ee.estpak.ee [195.250.170.69]
  6     1 ms     1 ms    <1 ms  noe-bb3-ae-2-0.ee.estpak.ee [194.126.123.41]
  7     1 ms     1 ms     1 ms  38-170-250-195.sta.estpak.ee [195.250.170.38]
  8     1 ms     1 ms     1 ms  CR-200-2.TLL07.ZONEAS.EU [85.234.245.14]
  9     1 ms     1 ms     1 ms  CR-200-1.TLL07.ZONEAS.EU [85.234.245.12]
 10     *        *        *     Request timed out.
 11     1 ms     1 ms     1 ms  LS-251-6.TLL07.ZONEAS.EU [85.234.245.43]
 12     1 ms     1 ms     1 ms  sn-69-28.tll07.zoneas.eu [217.146.69.28]

Trace complete.
```

Midagi läks kohta, kus päikesepaneelid elektrit ei tooda, valime teise tee

PING – koputame uksele

- Nimetus tuleb ultraheliradarist – saadame välja impulsse ja mõõdame peegeldusaega (mõelge robotauto programmi peale)
- https://en.wikipedia.org/wiki/Ping_(networking_utility)
- Mõõdetakse aega, mis kulub paketi jõudmiseni lõpp-seadmeni
- TTL – paketi eluiga ,algab 255 ,igas sõlmes väheneb 0

Küberrünnakute üks tööriistu : **kuna keegi ei keela koputada**,me ei tea iial, kas külaline on hea või halva kavatsusega aga kui koputajaid on palju, ei jõua ohver lihtsalt vastata. DOS - (A Denial-Of-Service attack – kuna PING on lihtne käsk, saab seda teha IGA veebikaamera, nutikell, roheteadlik elektritõukeratas, päikesepargi kontroller vms) – mõelge oma semestri lõpu peale . Teid palju ja õppejõud üks Pöördutakse samaaegselt.

```
C:\Users\Martin>ping martinjott.ee

Pinging martinjott.ee [217.146.69.28] with 32 bytes of data:
Reply from 217.146.69.28: bytes=32 time=1ms TTL=249
Reply from 217.146.69.28: bytes=32 time=1ms TTL=249
Reply from 217.146.69.28: bytes=32 time=1ms TTL=249
Reply from 217.146.69.28: bytes=32 time=1ms TTL=249

Ping statistics for 217.146.69.28:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Martin>
```

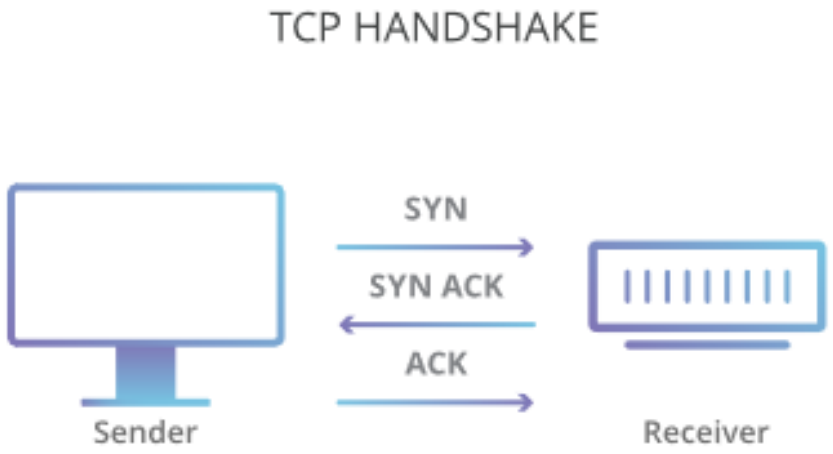
Transpordikihi protokollid

Andmeside protokollid tuleb kokku leppida , sest muidu ei saa vastuvõtja saatjast aru.

Kaks põhilist, millele ehitatakse enamik ülejäänud

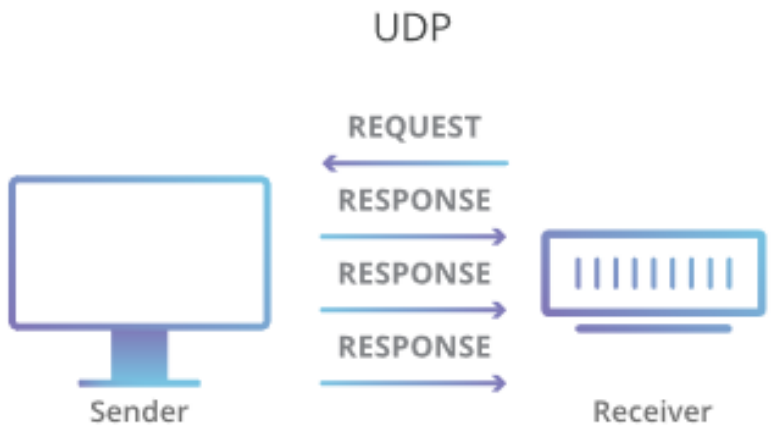
TCP (Transmission Control Protocol)

- kindlustatakse andmete liikumine , nõutakse kinnitust , et andmed jõuaksid õigesti kohale .
- Aeglasem, kindel



UDP (User Datagram Protocol)

- Ei kontrollita, kas andmed jõuavad (ja kui õigesti jõuavad) kohale
- Kiirem kui TCP
- Multimeedia, mängud
- Ei sobi failide jaoks !



Pordid

- Network Socket , tarkvaraline lahendus, mis seob ühenduse kliendi ja server vahel - võib võrrelda “elektripistikuga) . Vajalik on ip aadress ja pordi number
- Näitab ära ühenduse tüübi, tekitab virtuaalse “sidekanali”
- Võimalik on teha ühele IP aadressile virtuaalselt kuni 65535 ühendust
- Porte saab ümber suunata (nt on soov koduvõrgus tööle panna server, millele saab avalikust võrgust ligi). Vajalik laiendatud funktsioonidega ruuter.
- Või mängude tarbeks (nt mäng RuneScape kasutab porti 43594)

- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- Üldjuhul on pordi number seotud konkreetse sideprotokolliga (nt :http on 80)

- Osade portide liiklus võib olla turvakaalutlustel suletud (tavakasutaja internetiühendusel reeglina vaikimisi kõik sisenevad TCP pordid)

Mõned rakenduskihi protokollid

- **HTTP (HTTPS)** Hyper Text Transfer Protocol (S) secure –turvatud – vaikimisi saadetakse veebilehekülјed – Kasutatakse HTML (HyperText Markup Language) kirjelduskeelt, mis on tänapäevaste veebilehekülgede põhiehituskivi. Alates 1993
- SMTP(Simple Mail Transfer Protocol) , IMAP(S) ((Internet Message Access Protocol) - sedasi liiguvad E-kirjad, S - turvatud
- FTP (File transfer protocol) –ka SFTP (turvatud) – liiguvad faild
- TELNET (Terminal Network) kõige vanem protokoll (1969) – liigutatakse toorandmeid kahe punkti vahel . Tänapäeval ebasoovitav - kõik on näha , selle asemel SSH (Secure Shell)
- PPP (Point-to-Point Protocol) Punktist punkti protokoll ehk lõppseadmed suhtlevad omavahel (torrentid, failijagamised), ka vanemad “sissehelistamisteenused”
- Jne….

Mida teeb arvuti võrgus ?

- Käsk NETSTAT

```
C:\Users\Martin>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:50190        EE182P:50191           ESTABLISHED
  TCP    127.0.0.1:50191        EE182P:50190           ESTABLISHED
  TCP    127.0.0.1:50241        EE182P:50242           ESTABLISHED
  TCP    127.0.0.1:50242        EE182P:50241           ESTABLISHED
  TCP    127.0.0.1:50246        EE182P:50247           ESTABLISHED
  TCP    127.0.0.1:50247        EE182P:50246           ESTABLISHED
  TCP    127.0.0.1:56382        EE182P:56383           ESTABLISHED
  TCP    127.0.0.1:56383        EE182P:56382           ESTABLISHED
  TCP    192.168.145.234:3389   LAPTOP-5EAPQS0K:59770  ESTABLISHED
  TCP    192.168.145.234:7680   U02-20504K-old:59229   TIME_WAIT
  TCP    192.168.145.234:49765  20.199.120.85:https    ESTABLISHED
  TCP    192.168.145.234:50346  20.199.120.151:https   ESTABLISHED
  TCP    192.168.145.234:54171  edge-star-shv-01-arn2:https  ESTABLISHED
  TCP    192.168.145.234:54176  edge-star-shv-01-arn2:https  ESTABLISHED
  TCP    192.168.145.234:54183  edge-z-p3-shv-01-arn2:https  ESTABLISHED
  TCP    192.168.145.234:54185  edge-star-shv-01-arn2:https  ESTABLISHED
  TCP    192.168.145.234:55404  52.96.69.66:imaps      ESTABLISHED
  TCP    192.168.145.234:55434  93:https               ESTABLISHED
  TCP    192.168.145.234:55478  52.111.209.16:https    ESTABLISHED
  TCP    192.168.145.234:55486  52.111.209.16:https    ESTABLISHED
```

Turvalisus

- Kõige suurem inimlik turvarisk tänapäeval – ekraani ja seljatoe vahel , ehk kasutaja ise (jagab salasõnu , paigaldab rakendusi jne)
- Tehnilised turvariskid – nt ühenduse pealtkuulamine , segamine , kaaperdamine , juurtasandil andmete vargus, sihilik võrgu ülekoormamine . Tavakasutaja seda vältida ei saa, küll aga võib oma naiivsuses kaasa aidata.

- Võrguliikluse alged pärinevad aastast 1969 ja protokollid on avatud . Ehk liiguvad turvamata ühenduse puhul toorandmed . Kõik on lihtsate vahenditega jälgitav. Sellepärast eelistatakse tänapäeval turvatud ühendusi (nt. https) , kus sidekanal krüpteeritakse.

- Elame tegelikult kübersdade ajastuil, kus lahingumasinatena kasutatakse meie seadmeid, nii, et me seda ei teagi. (vt käsk netstat, eelmine slaid)
- Ei pruugita rünnata alati mitte avalikke teenused, vaid võib olla häkkerite rühmituste omavaheline lahing/arveteklaarimine – kelle arvuti kukub enne kokku

Võrgurünnakute liike

- (d)DOS (Denial of service) . Kõige tavalisem , kõige levinum, kõige lihtsam Pannakse tegema tuhandeid seadmed lihtsat päringut (nt ping) ühte kohta. Me kõik saame teenuse tellida.

Nõuavad üldjuhul otsest sekkumist, saab ka tarvaraliselt, eesmärk varastada andmeid.

- Mürgitamine , ka mees meie keskel . (Poisoning, Man in the middle). Seade pannakse (reeglina) sisevõrku, kus ta üritab mingi võrgusõlme töö endale võtta , häirides otseselt valepakettidega selle tööd. Suunab liikluse läbi enda ja vajalikku kohta. Suunatud ründed konkreetse info ja sisevõrgu vastu, ära luba võõrast seadet sisevõrku !!!! Ka nt veebikaamera võib seda teha !
- Saab mürgitada ka nimeserverit (DNS tunneling) , suunates õige nimega “oma lehele”.
- Õngitsemine, nuusutamine (phishing,sniffing) – kuulatakse sidekanalit pealt ja üritatakse tabada sisselogimisi ja need paketid salvestada. (väidetavalt tegelevad sellega mõne firma ruuterid – nn küberohud, aga ka poliitika)

Kuidas kaitsta (tehnilises mõttes)

Tea, mida sa teed ! Päriselt ka ! Lühidalt:

- **Kasuta tulemüüri** (see välistab ebasobivad päringud). Veel parem kui see on seadistatud su enda (kui oskad) või selle poolt, kes päriselt on IT teadlik ! . Luba võrgusuhtlus ja pordid programmidel, millel on see hädavajalik !
- Ära lase oma personaalse arvuti (ka telefoni !!) taha mitte kedagi teist !
- Ära lase oma kodu (ettevõtte) võrku suvalist seadet , vajadusel tee eraldi kinnine alamvõrk (nt TTÜ avalikus wifi võrgus ei saa peale veebilehitsemise eriti midagi teha)
- Kui Sul on mure ja lased IT pädeva inimese enda arvutile ligi (kas otse või virtuaalselt) – ta näeb kõike (isegi siis kui ta ei taha)
- Viirusetõrjed,ka teenusepakkuja omad (liiklus ja su privaattandmete analüüs läbi nende seadmete) – suhtu kriitiliselt !
- Kuritegeliku koodi saab seadmesse imelihtsalt (nt vahemällu läbi brauseri aadressirea kasvõi) – seda EI SAA tehniliselt keelata. Keerulisem on koodi käivitamine, siin on ülisuur roll enamasti kasutajal. Väga vähe on juhtumeid,kus “ise” midagi juhtub.
- Kui vaja kasutada või testida tundmatut tarkvara – kasuta “liivakasti – sandbox” ehk virtuaalmasinat, teist arvutit jne

Kas saab olla päriselt anonüümne ?

- Lühike vastus – EI . Nii kui hakkad rääkima, on kohe kuulda kes räägib.
- Kogu liikluse jälg (metaandmed) on näha, isegi , kui liiklus ise on turvatud. Võrgusõlmed PEAVAD TEADMA, kuhu paketid saata !
- Ei saa ennast peita, kui soovid päringule vastust (no kellele teisele siis see saata)

Mida tehakse, et anonüümsust suurendada :

- Ruutimisteekond kahe seadme vahel tehakse võimalikult,sh, läbi erinevate riikide, pikaks, lisades juurde ka virtuaalprivaarvõrke (VPN) . Aga ka nende teenusepakkujad näevad mõlemat “otsa” – “sisse ja välja”
- Kui vaja jälgi segada, siis kurjategija “ruuteriks” võib osutada ka Sinu arvuti , turvakaamera ja miks mitte päikesepaneelide kontroller !

Lõeptuseks

- Tundke aegajalt huvi, mida Teie digipädev digiseade võrgus teeb .
- Kui seadet ei kasuta, aga võrguliikus on pidevalt aktiivne, võib põhjust olla muretsemiseks.
- Tunne lihtsamaid tööriistu – võimalik, et suudate ise võrguprobleemid lahendada !