

Arvutivõrgud



Arvutivõrkude osa kava

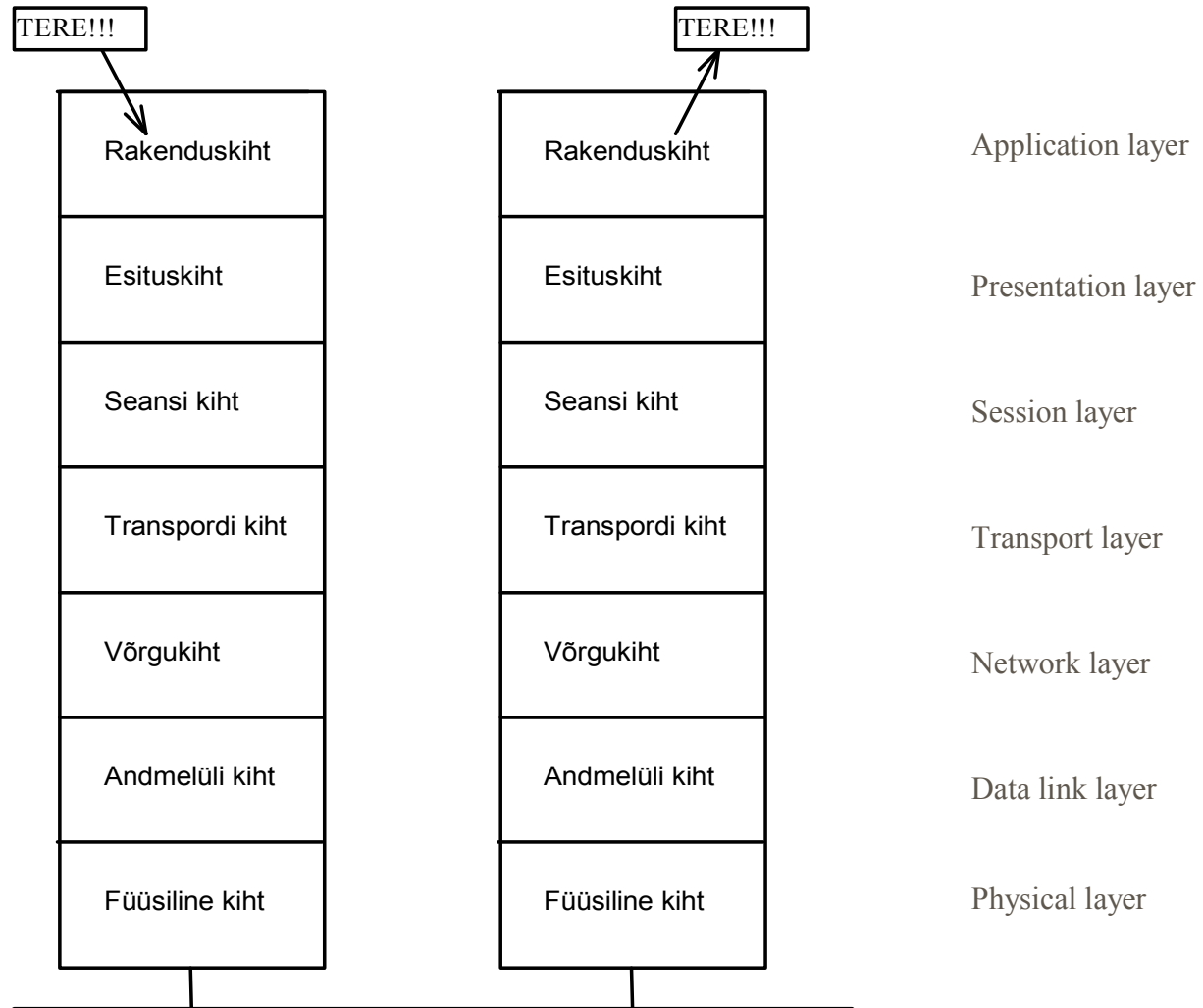


- ISO-OSI võrguprotokollide mudel, mõisted
- TCP/IP protokollipere
 - ARP, RARP
 - IP, ICMP
 - TCP, UDP
- Vigade leidmise meetodid ja vahendid

Infot arvutivõrkudest võib leida

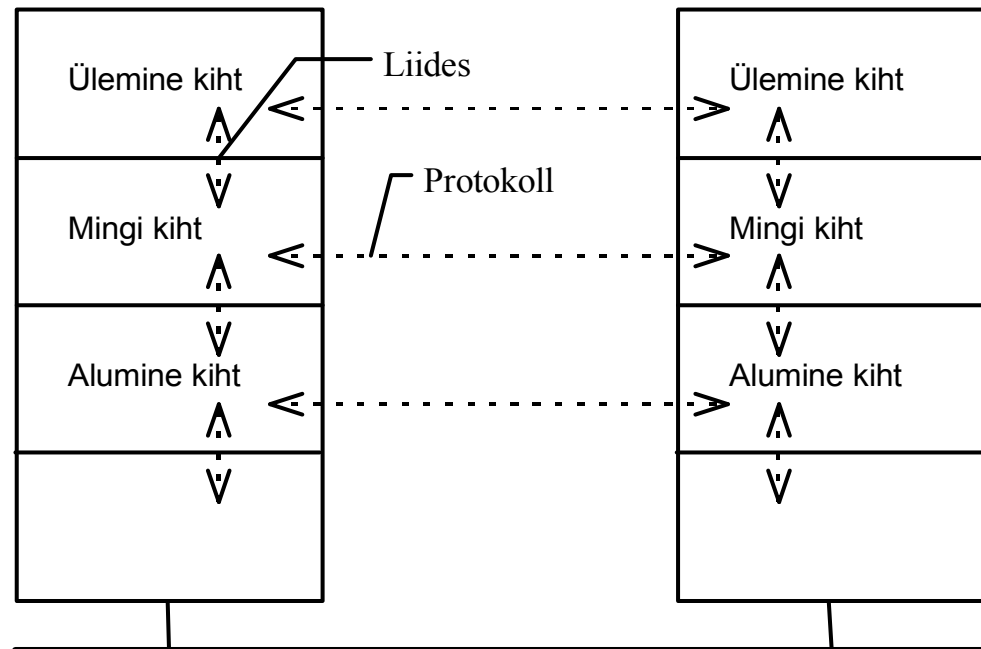
- <http://networking.ittoolbox.com/>
- <http://kuutorvaja.eenet.ee>

ISO - OSI mudel

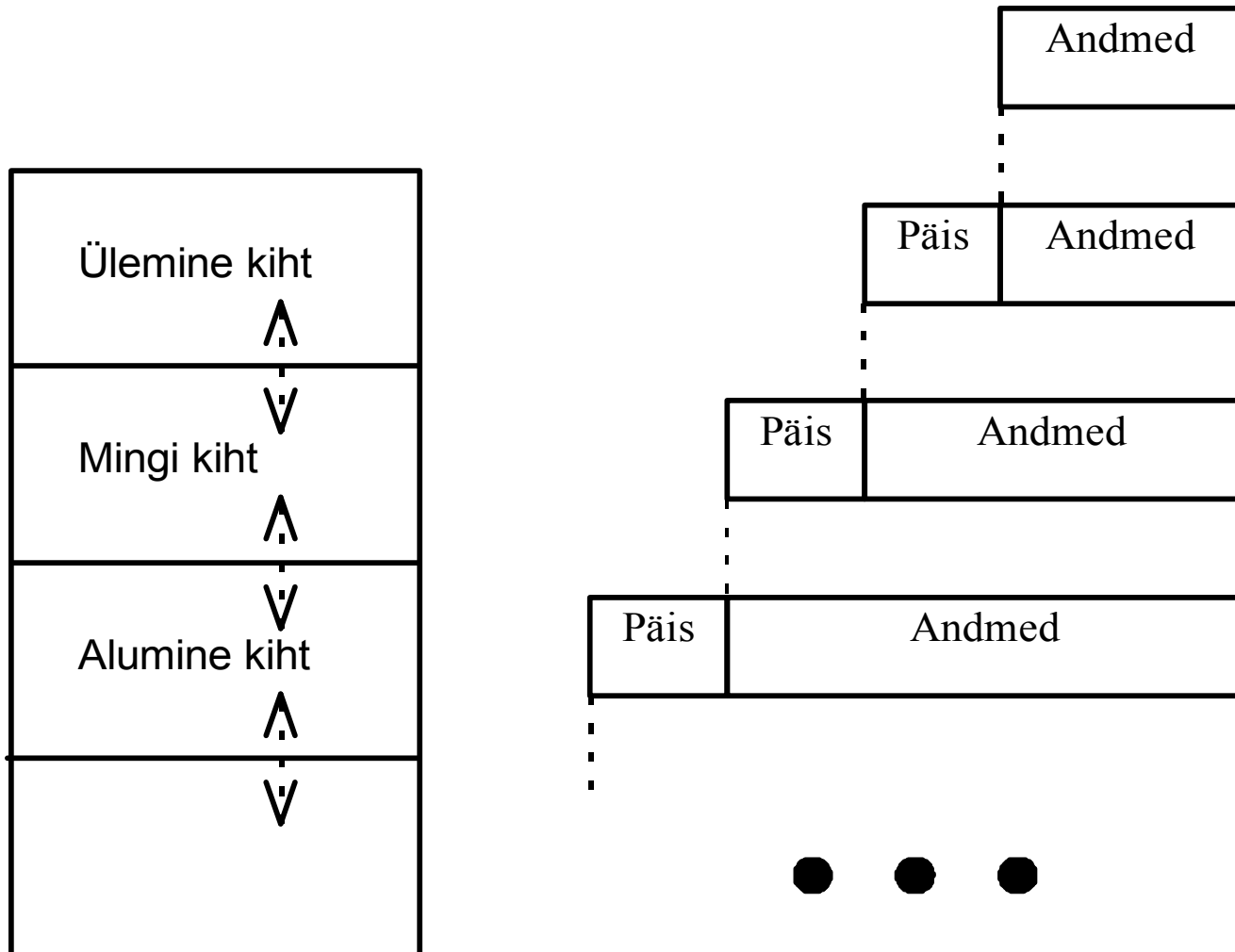


OSI mudeli kihid

- **Protokoll (protocol)**
Eri süsteemide samade kihtide suhtlusviis omavahel
- **Liides (interface)**
Sama süsteemi eri kihtide suhtlusviis omavahel



Kapseldamine (Encapsulation)



Füüsiline kiht (Physical Layer)



Raua ja elektri jms spetsifikatsioon

- Pistikute standardid
- Signaali kuju, sagedus, amplituud
- Traatide arv, tüüp, funktsioon, max pikkus
- Kodeerimismeetod
- Bittide edastamine

Ühenduse kiht (Link Layer)



Kanal segmendi piires

- Võrgu topoloogia
- Seadmete füüsilised aadressid
- Vigade avastamine
- Kaadrite formeerimine, edastamine
- Voo reguleerimine

Võrgu kiht (Network Layer)



Loob võrgu üle mitme segmendi

- Loogiline adresseerimine
- Pakettide marsruutimine, optimeerimine
- Maksustamine (kui kasutatakse)

Transpordi kiht (Transport Layer)



Loob lihtsalt kasutatava (usaldusväärse) kanali (nt klientprogrammist serverprogrammini)

- Varjab kõik tehnilised detailid
- Veakontroll ja -parandus
- Multiplekser
- Ühendusega või ilma ühenduseta kanal

Seansi kiht (Session Layer)



Võimaldab katkenud seansi jätkata

- Sessioonide loomine, haldamine, lõpetamine
- Sünkroonpunktide lisamise võimalus

Esituskiht (Presentation Layer)



Andmete ühtse vormingu kooskõlastamine ja teisendus

- Arvude esitus
- Kooditabelid
- Pildi, heli ühtne vorming
- Krüpteerimine, pakkimine

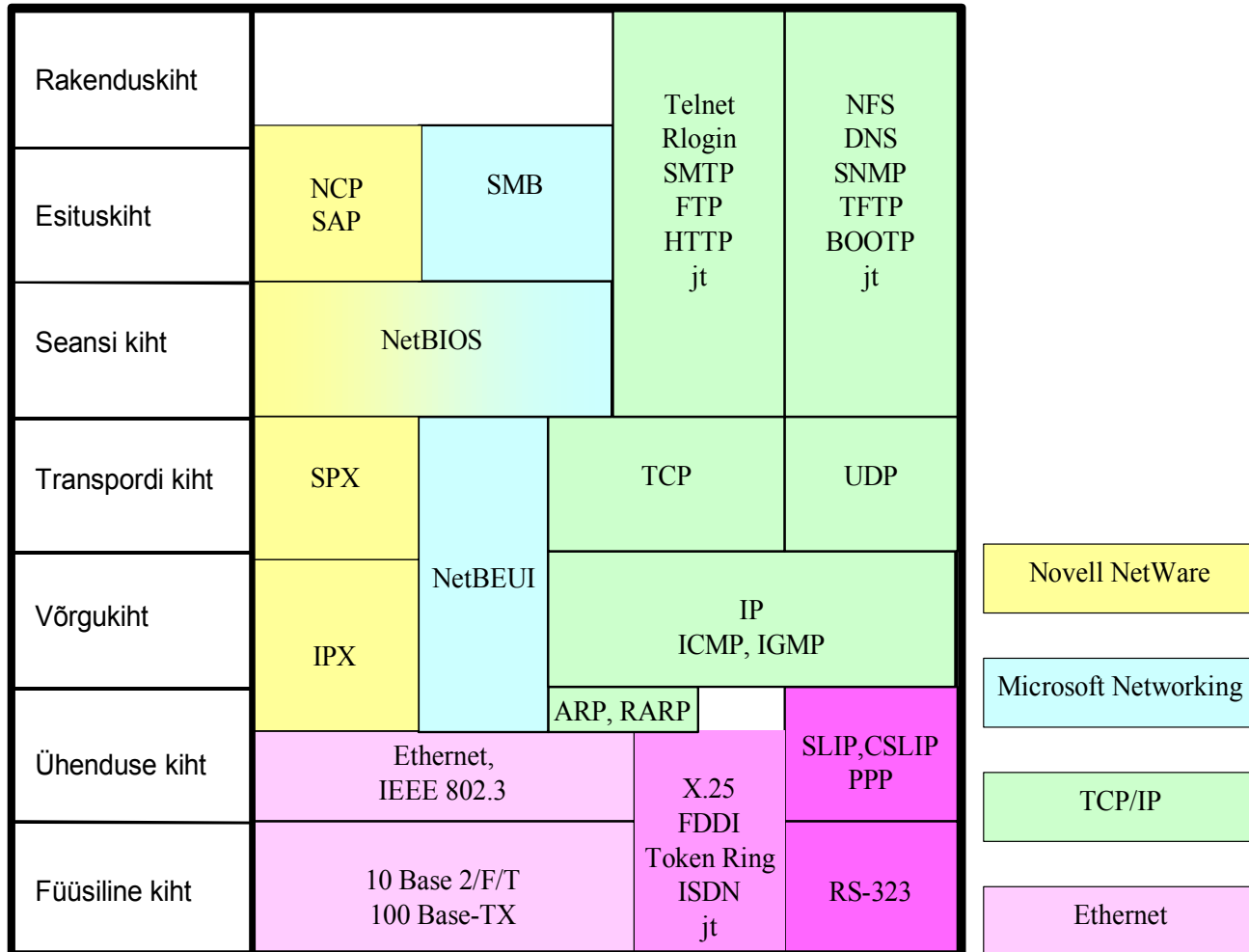
Rakenduskiht (Application Layer)



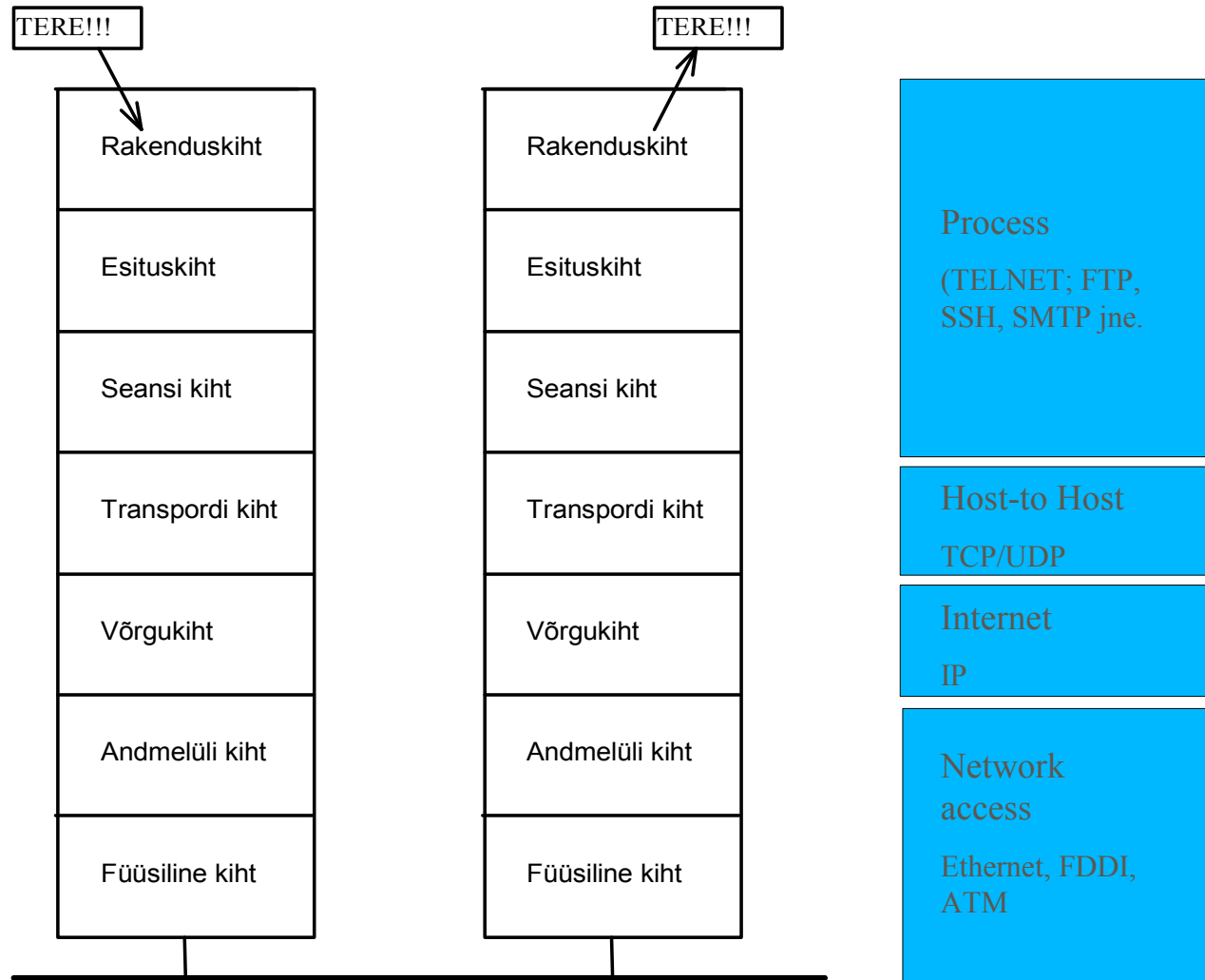
Liides rakendusprogrammidele

- võrguteenused (telnet, ftp, http)
- kaugfailisüsteemid (SMB, CIFS, NFS)

Protokollipered



TCP/IP mudel (DoD mudel)



MTU (Maximal Transmission Unit)



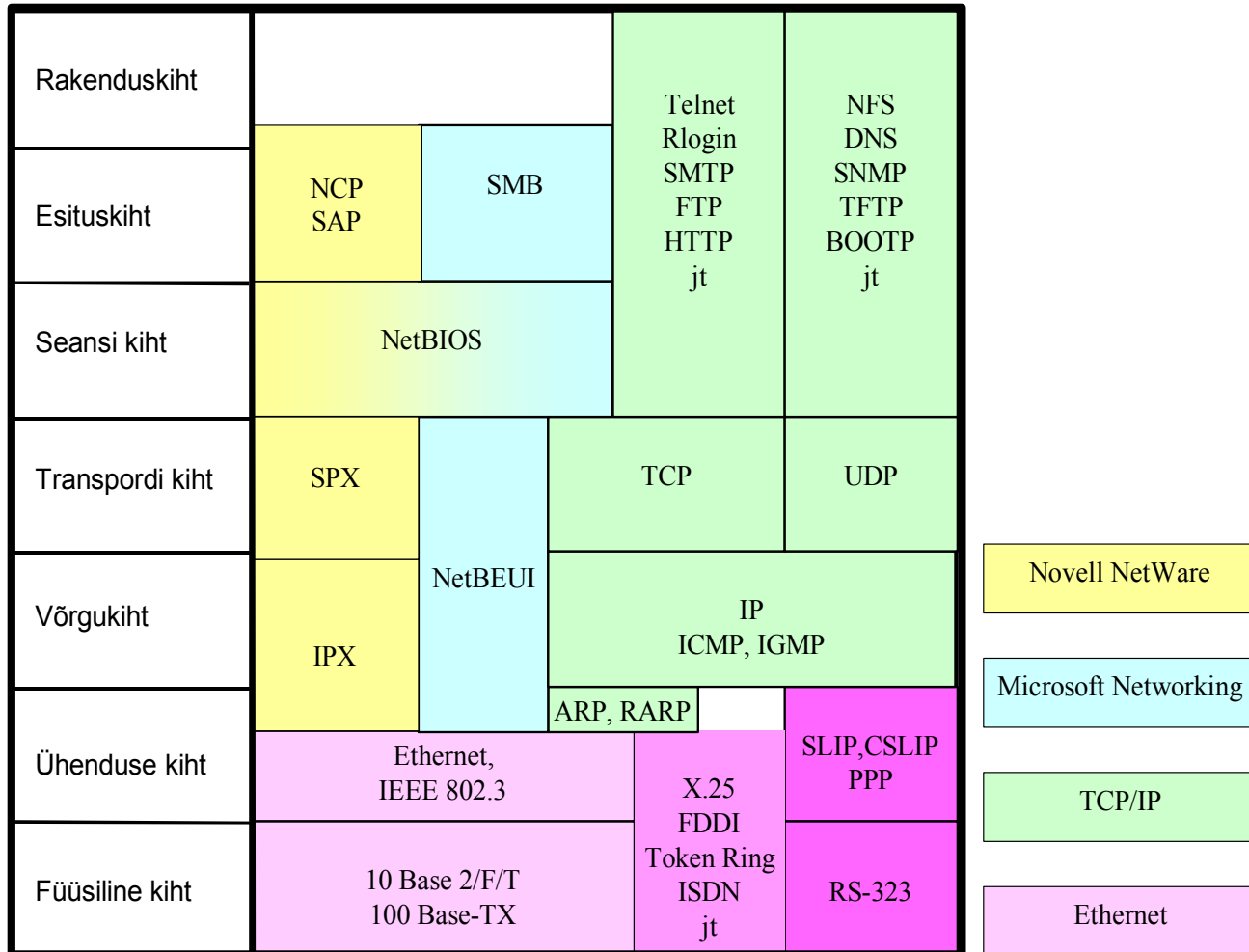
- Kõigil füüsilistel kandjatel on sõnumi pikkuse ülemine piir
 - Ethernet –1500
 - SLIP, PPP – 296
 - Gigabit Ethernet ja kiiremad – 9000 (jumbo frame)
- IP protokoll oskab suuremad paketid fragmenteerida

Võrgu kiht (Network Layer)



- Loob „kanali“ üle mitme segmendi, st võimaldab andmeid saata segmentide vahel
- Virtuaalne adresseerimine
- Pakettide marsruutimine, vajadusel fragmenteerimine, optimeerimine
- Maksustamine (kui kasutatakse)

TCP/IP protokollipere

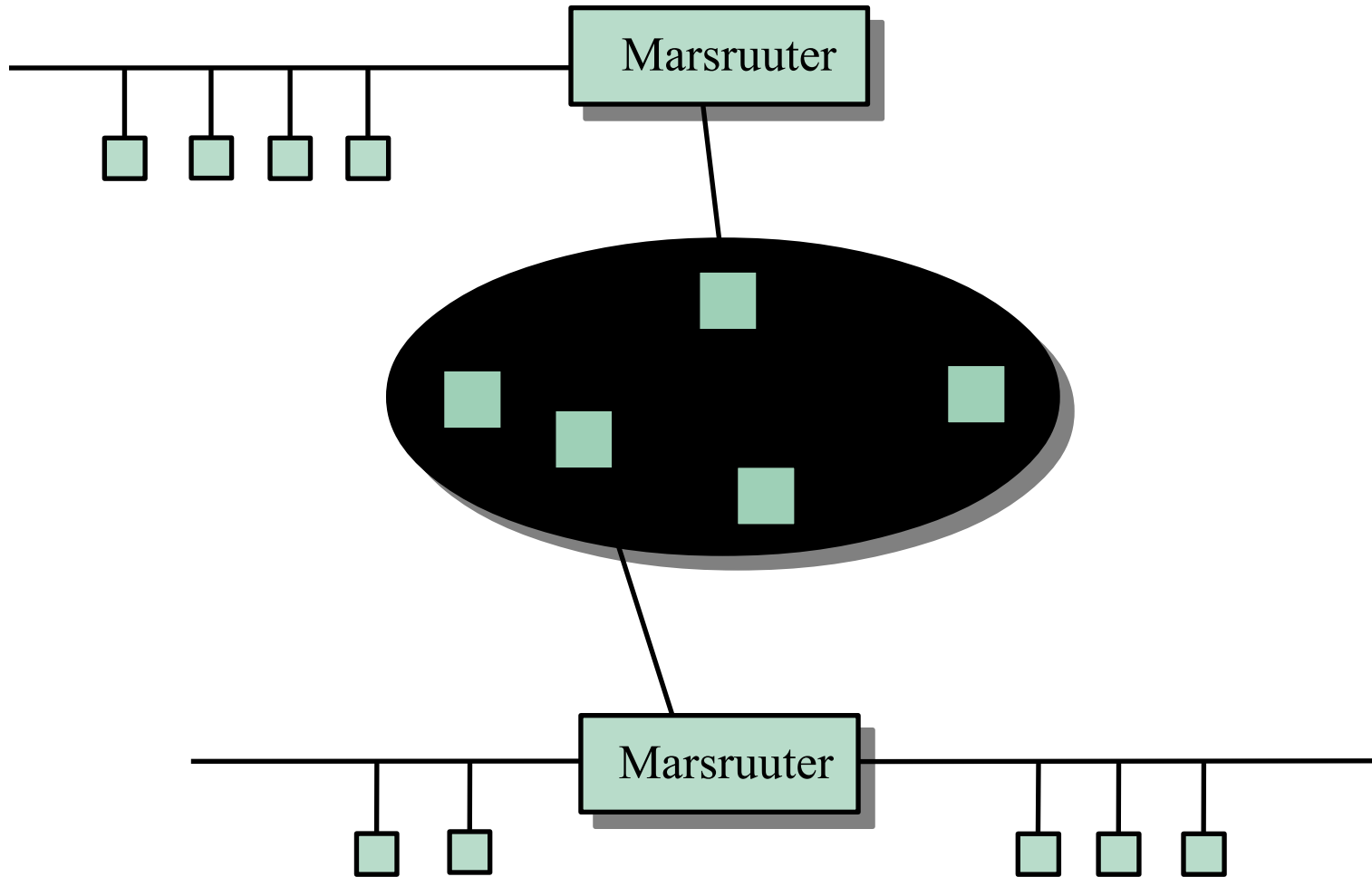


TCP/IP



- TCP/IP - Transmission Control protocol / Internet Protocol
- Sai alguse 60te lõpus akadeemilisest uurimisprojektist
- Internet - ülemaailmne võrk
- internet - eri võrkude ühendus
- Protokollipere
 - Standardid algselt RFC kujul (Request for Comment)
 - Igale protokollile antakse standardsuse ja soovitatavuse hinnang

Internet



IP (Internet Protocol)



- TCP/IP pere "tööhobune"
- RFC 791
- Garanteerib marsruutimise, st pakettide minemise õiges suunas
- Mitteusaldusväärne - ei taga kohalejõudmist
 - Kui seadme sisendpuhver on täis, siis ignoreerib
- Ei loo kanalit
 - iga paketti (datagrammi) käsitletakse sõltumatult

IP datagramm



- Päis kokku 20 baiti, võib olla kuni 60
 - TOS (Type of Service)/Differential services
 - min hilistumine | max läbilaskvus | max usaldatavus | min kulu
 - datagrammi pikkus 20- 65535 (2 baiti)
 - identifikaator (2 baiti)
 - TTL (Time to Live) - max läbitavate marsruuterite arv
 - protokoll (RFC 1060)
 - päise kontrollsumma (2 baiti)
 - lähte ja sihtkoha aadress (8 baiti)
 - lisavõimalused

Interneti aadressid

- Unikaalne igal võrguliidesel
 - Aadress on 32 bitti = 4 baiti (C1.28.EF.1B)
 - Kirjutatakse 4 kümnendarvuna (193.40.239.27)
 - Aadress jaguneb võrgu- ja hosti aadressiks
 - Võrguaadresside klassid
- | | võrke hoste | |
|---------------------------------------|-------------|---------|
| ■ A: 1.0.0.0 kuni 127.0.0.0 | 128 | 1,6milj |
| ■ B: 128.0.0.0 kuni 191.255.0.0 | 16320 | 65024 |
| ■ C: 192.0.0.0 kuni 223.255.255.0 | 2 milj | 254 |
| ■ D, E ja F: 224.0.0.0 kuni 254.0.0.0 | | |

Spetsiaalsed aadressid

- 0.0.0.0 - lähteaddress kui saatja ei tea oma aadressi sihtaadressina iseenda esimene liides
- 0.0.x.x - lähteaddress kus hosti osa on määratud
- 127.x.x.x- tagasiviite (loopback) aadress
- 255.255.255.255 - kohaliku segmendi üldlevi aadress
- aaa.bbb.255.255 - kohaliku alamvõrgu üldlevi aadress
- Sisevõrkudes kasutatavad aadressid
 - 10.0.0.0/8 (kuni 10.255.255.255)
 - 172.16.0.0/12 (kuni 172.31.255.255)
 - 192.168.0.0/16 (kuni 192.168.255.255)

Alamvõrgud



- Saab teha paraja suurusega võrgud
- Jagamine on nähtamatu välistele marsruuteritele
- Alamvõrgu esimene ja viimane aadress on eritähendusega, need ei kuulu ühelegi hostile:
 - esimene tähistab alamvõrku marsruutimistabelites
 - viimane tähistab alamvõrgu üldaadressi
- Alamvõrgu suurus määratakse alamvõrgu maskiga
- Alamvõrkude kalkulaator <http://jodies.de/ipcalc>

Alamvõrgu mask (subnet mask)

- 32 bitine arv nagu aadress
- 1-d alamvõrgu osa jaoks, 0-d hosti osa jaoks
- alamvõrgu suurus on mingi 2 aste
- Reegel: 255.255.255.x, x=256-alamvõrgu suurus
Näide: alamvõrk 193.40.127.64, mask 255.255.255.224,
ehk 193.40.127.64/27

mask	255.255.255.224	11111111.11111111.11111111.111 00000
host	193.40.127.70	11000001.00101000.01111111.010 00110
võrk	193.40.127.64	11000001.00101000.01111111.010 00000
üldlevi	193.40.127.95	11000001.00101000.01111111.010 11111

- Võrgumaski tähistatakse ka 1-bittide arvuga võrgumaskis
193.40.127.64/255.255.255.224 = 193.40.127.64/27

IP marsruutimine



■ Marsruutimistabel

- Hosti või võrgu sihtaadress (aadress+võrgumask)
- Järgmine marsruuter või vahetult ühendatud võrk
- Lipud
- Kasutatav võrguliides

■ Marsruutimisalgoritm

- Otsi tabelist marsruutingut otsitavale siht-hostile
- Otsi tabelist marsruutingut otsitava siht-hosti võrgule
- Kasuta vaikimisi (default) marsruutingut

Võrgu utiliidid linuxis



■ Pakett net-tools

- „old-school”
- ifconfig – võrguliidest seadistamine
- route – marsruutimistabeli seadistamine
- ifup / ifdown – võrguliides käima/seisma

■ Pakett iproute

- ip - „all-in-one” võrguliidest, ruutingu jms-ga
- ss – „netstat” (socket status)
- bridge – silla seadistamise utiliit

Võrgu seadistused



■ Skriptipõhised

- Igal distributsioonil suuremal-vähemal määral isemoodi...

- RHEL/CentOS/Rocky kasutab SYSCONFIG raamistikku

- Seadistused asuvad teksti(konfi)failides

- /etc/sysconfig/network
- /etc/sysconfig/network-scripts/ifcfg-<interface-name>

- Debian-i põhised distributsioonid kasutavad

- /etc/network/interfaces

Võrgu seadistused

■ Network Manager

- Daemon, graafiline utiliit, käsurea utiliit
- Järjekordne „standardne” „kõik ühes” võrgu seadistamise süsteem
- Töötab koos udev ja systemd-ga
- Sobib hästi võrgu osas pidevalt muutuvasse keskkonda – nt laptopid. Serveri puhul „overkill”
- Suudab hallata ka mobiilivõrgu, VPN jms ühendusi
- Käsurea utiliit `nmcli` „imelik”
- Kasuta parem `nmtui` utiliiti

Marsruutimine

- Marsruutimistabeli vaatamine -
 - Windows - *route print*
 - UNIX – *route*
 - Linuxis ka – *ip route*
- Marsruutimistabeli muutmine - *route*
 - route add -net A.B.C.D mask 255.255.255.X if Y*
 - route delete A.B.C.D*
 - route add default marsruuteri_IP*
- Marsruutimistabeli muutmine – *ip route*
 - ip route add A.B.C.D/E via F.G.H.I dev Y*
 - ip route delete A.B.C.D*
 - ip route add default via marsruuteri_IP dev Y*

Võrgu testimise vahendid

- *ping* - hosti kättesaadavuse kontrolliks

```
ping hostinimi
```

```
ping ip-aadress
```

- *tracert* - marsruutimistee analüüsiks

```
tracert hostinimi
```

```
(Windowsis tracert)
```

- Tihti on probleem nimeserveri puudumises või nimeserveri suutmatuses nimesid lahendada
-n võtme abiga ei üritata aadresse nimedeks lahendada

Kohtvõrgu testimine (*tcpdump*)

- Võimaldab jälgida pakette ühenduse kihi (etherneti) tasandil
- Võimaldab filtreerida välja huvitavad paketid (Linuxis)

```
tcpdump -i eth0 host mail.tlu.ee and port smtp
```

- teiste masinate omavahelise liikluse jälgimiseks võib olla vaja sisse lülitada liidese "promiscuous" režiim

```
ifconfig eth0 promisc
```

Kohtvõrgu testimine



- `iptraf` (`iptraf-ng`) - Linuxil konsoolil töötav vahend võrguliikluse jälgimiseks (vana)
- `wireshark` (`tshark`) – võrguliikluse analüsaator
`tshark -i eth0`
- `nmap` - võrguskänner
`nmap 192.168.1.98-127`

ICMP (Internet Control Message Protocol)



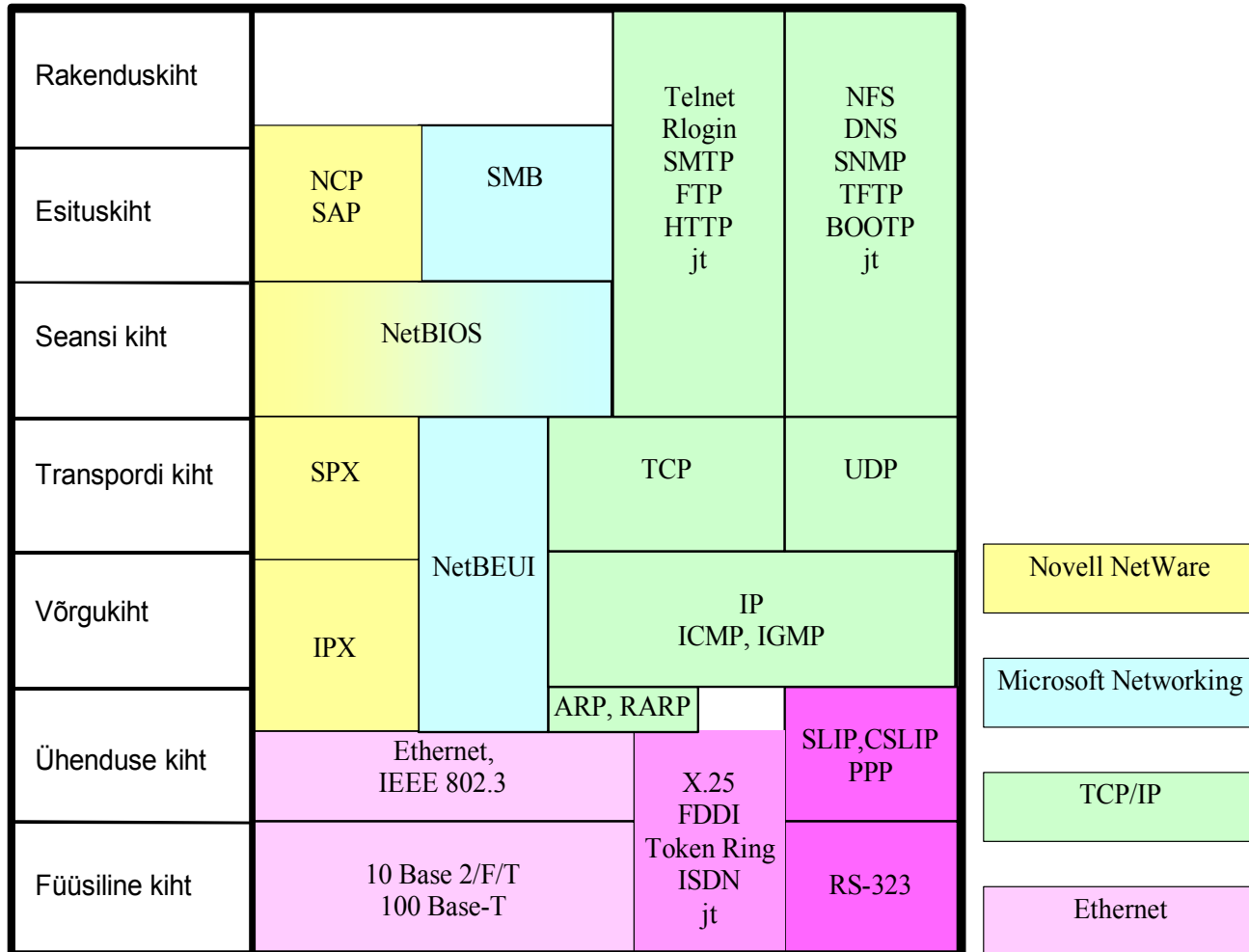
- Veateated ja päringud
 - veateade sisaldab põhjustanud IP datagrammid identifikaatori
 - network/host/protocol/port not reachable jt
- Programm *ping* kasutab ICMP päringut
- Programm *traceroute* kasutab ICMP teadet
 - “Time exceeded”
- Ümbermarsruutimise teade

Dünaamiline marsruutimine



- On vaja kui:
 - võrk on suur
 - mitu ühenduspunkti muu maailmaga
 - tagavaramarsruuterid
 - võrgu konfiguratsioon muutub tihti
- Muudab marsruutimistabelit dünaamiliselt
- Marsruuterid vahetavad omavahel infot
 - autonoomse süsteemi sees: RIP, OSPF
 - autonoomsete süsteemide vahel: EGP, BGP
- Programmid *routed*(RIP), *gated*(RIP,OSPF,BGP), zebra, Quagga, FRR

ARP, RARP



ARP, RARP



- ARP - Address Resolution Protocol
- IP -> ARP -> Ethernet MAC-aadress
- Ethernet -> RARP -> IP (host küsib võrgust endale IP)
- Kuidas ARP töötab
 - IP (protokolli kiht) küsib mis etherneti aadressil asub aaa.bbb.ccc.ddd
 - Kui vastus on vahemälus, siis vastab
 - Kui ei ole, siis saadab etherneti üldaadressil küsimuse "Kes on aaa.bbb.ccc.ddd".
 - aaa.bbb.ccc.ddd saadab oma etherneti aadressi
 - ARP peab selle vahemälus meeles ja saadab IP-le
- ARP ei vaja konfigureerimist (RARP vajab, ei kasutata)

Nimede lahendamine



- Resolver – OS alamsüsteem, mis lahendab nimesid

- Nimede lahendamise järjekord

tavaliselt

hosts

DNS

- Kohalik lahendamine

/etc/hosts, /etc/networks (UNIX/Linux)

C:\WINDOWS\System32\drivers\etc\hosts (Win7, Win10)

- Nimeserveri (DNS) kasutamine

/etc/resolv.conf

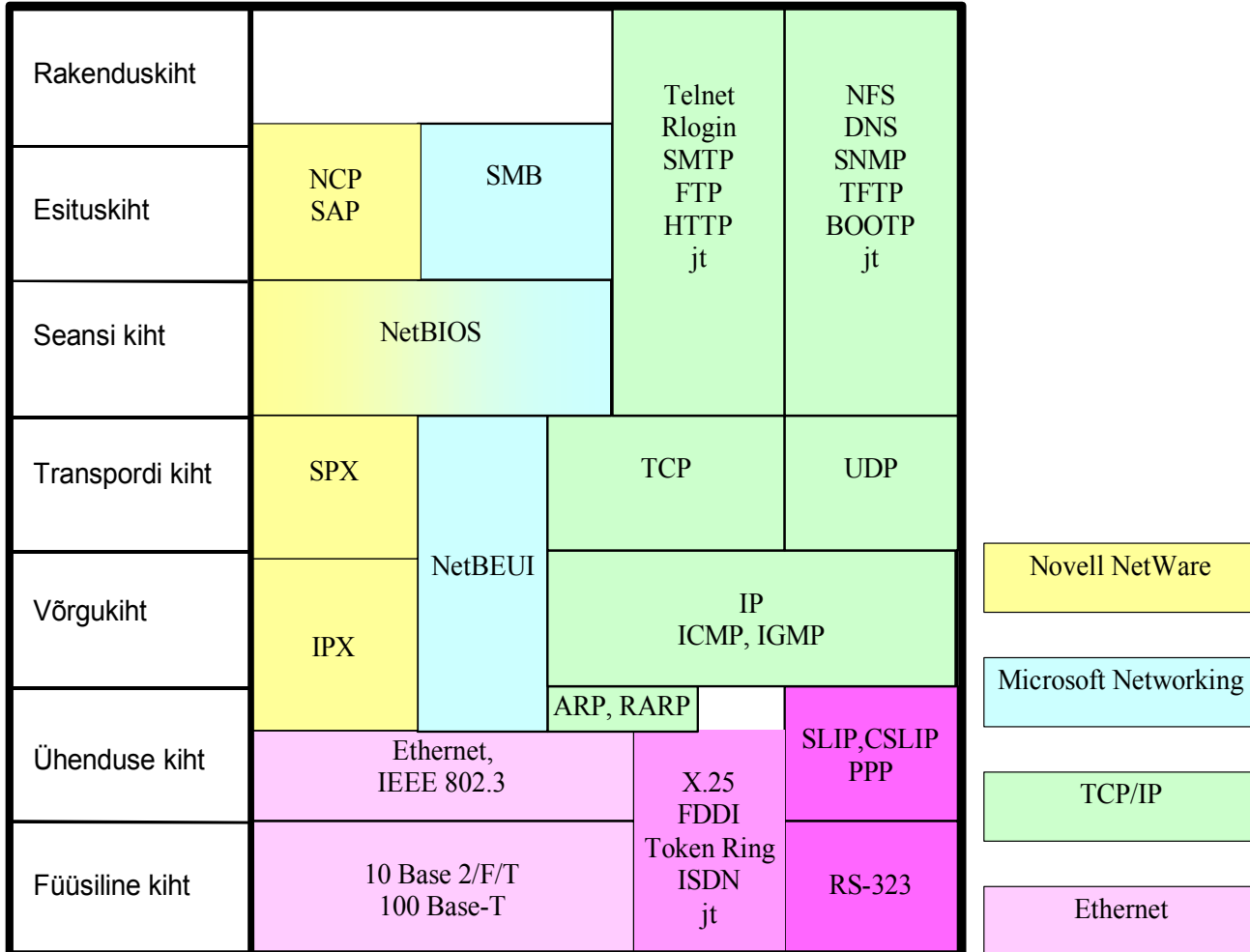
nameserver

kasutatavad nimeserverid

search

domeeninimed, mida lisatakse otsimisel nimele,
mis ei sisalda punkti

Transpordi kiht



Pordid



- Programmidele (ühendustele) antakse kasutamiseks nummerdatud TCP või UDP port
- Ühenduse määravad IP aadressid, pordid, protokoll
- On üldtuntud ja dünaamiliselt jagatavad pordid
 - 0 - 1023 üldtuntud pordid
 - FTP - TCP 21, telnet - TCP 23, TFTP - UDP 69
 - >1023 klientprogrammid, muud serverid
 - >61000 maskeeritud ühendused
- Pordi numbrite ja teenuse nimede vastavus
/etc/services

Klient - server mudel



- Üldine algoritm (ühenduse loomine)
 - server ootab mingil üldteada pordil ühenduskutseid
 - klient reserveerib dünaamilise pordi (tavaliselt >1023)
 - klient saadab serverile ühenduskutse (koos oma pordinumbriga)
 - server vastab kliendile tema pordinumbril
 - ...

<http://www.eventhelix.com/RealtimeMantra/Networking/>
- Itereeriv server
 - Ei võta vastu uut kutset enne eelneva töötlemist
- Paralleelne server
 - Käivitab iga kutse jaoks eraldi serveri

TCP (Transmission Control Protocol)



- Ühendusorienteeritud
- Usaldatav
- Voo tüüpi
 - Jagab voo segmentideks
 - Saates käivitab taimeri ja ootab kinnitust
 - Kinnitab saadud segmendid
 - Kontrollsumma päisest ja andmetest
 - Korrastab segmentide järjestuse
 - Unustab dublikaadid
 - Kontrollib voo mahtu

UDP (User Datagram Protocol)



- Iga rakenduse väljund tekitab uue datagrammi
- Ei taga usaldatavust
- Datagrammi ehitus:
 - lähte- ja sihtport
 - datagrammi pikkus
 - andmeosa
 - kontrollsumma (pole kohustuslik)
- Kontrollsumma vea puhul unustatakse datagramm
- Rakendused: DNS, NFS, TFTP

TCP ja UDP jälgimine (*netstat*)

Linuxis on *netstat* käsul järgmised võtmed:

- t , -u TCP ja UDP ühendused
- a kõik ühendused
- l ootel (kuulavad) pordid
- p koos protsessi nime PID numbriga
- e koos kasutajanimega
- n numbrilisel kujul (nimedeks tõlkimata)

- i liideste statistika
- M maskeeritud ühendused

TCP ja UDP jälgimine (*ss*)



Linuxis on *ss* käsul järgmised võtmed:

- t , -u TCP ja UDP ühendused
- a kõik pistikud (*socket*)
- l ootel (kuulavad) pordid
- p koos protsessi nime PID-ga
- e koos kasutaja UID-ga
- n pordid numbrilisel kujul (teenuse nimeks tõlkimata)
- r IP-d ja pordinumbrid tõlgitakse nimedeks
- s liideste statistika

Kogu protsess HTTP näitel (klient)

■ HTTP

■ Veebiteenus

■ Server asub TCP pordil 80

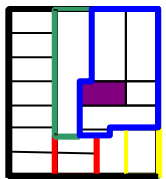
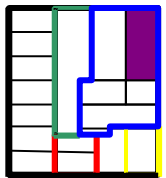
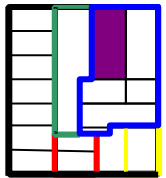
```
$ telnet lin2.tlu.ee 80
```

■ küsitakse nimeserverilt lin2.tlu.ee IP aadress

- nimeserverile saadetakse rekursiivne päring
- nimeserver teeb DNS protokolliga otsingu
- annab tulemuse 193.40.239.27

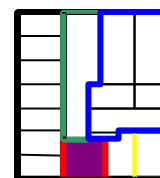
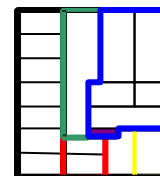
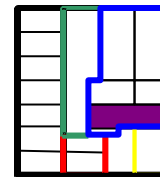
■ telnet loob TCP ühenduse

- reserveeritakse kohalik TCP port (nt 1234)
- saadetakse serverile TCP ühenduse avamise kutse (porti 80)



Kogu protsess HTTP näitel (võrk)

- | telnet saadab päringu (`telnet lin2.tlu.ee 25`)
 - | saadetakse TCP segmenti sisaldav IP datagramm 193.40.239.27-le
 - marsruutimistabelist selgub, et tuleb kasutada vaikimisi marsruutimisreeglit (N: 193.40.232.254)
 - ARP abil tehakse kindlaks selle Etherneti aadress
 - saadetakse üldlevi aadressil küsimus 193.40.232.254
 - saadakse vastus 00:50:DA:C6:1E:E2
 - saadetakse Etherneti kaader aadressile 00:50:DA:C6:1E:E2
 - oodatakse kuni Etherneti võrk on vaba
 - saadetakse kaader
 - 193.40.232.254-s ja teistes marsruuterites korratakse marsruutimisprotseduuri



Kogu protsess HTTP näitel (server)



- lin2 IP kiht annab datagrammi andmeosa edasi TCP kihile
- | lin2 TCP kiht annab pordi numbri järgi andmeosa edasi http serverile
- http server töötleb päringut
- http server saadab vastuse ja lõpetab TCP ühenduse
 - | kordub protseduur läbi TCP, IP ja Etherneti

Võrguseadmed

Rakenduskiht			Telnet Rlogin SMTP FTP HTTP jt	NFS DNS SNMP TFTP BOOTP jt
Esituskiht	NCP SAP	SMB		
Seansi kiht	NetBIOS			
Transpordi kiht	SPX		TCP	UDP
Võrgukiht	IPX	NetBEUI	IP ICMP, IGMP	
Ühenduse kiht	Ethernet, IEEE 802.3		ARP, RARP	SLIP, CSLIP PPP
Füüsiline kiht	10 Base 2/F/T 100 Base-T		X.25 FDDI Token Ring ISDN jt	RS-323

