TALLINNA POLÜTEHNIKUM

IT ja telekommunikatsiooni erialaosakond

Tõnn Toomsalu

Arvutivõrkude alused

KURUSE KONSPEKT

**TARKVARAARENDUS**

KTA-19E

Juhendaja: Toivo Pärnpuu

TALLINN 2019

**Sisukord**

[HTTP-st PING-ni 3](#_Toc26199804)

[Pordid 5](#_Toc26199805)

[Kokkuvõte 7](#_Toc26199806)

[Nimed ja Aadressid 8](#_Toc26199807)

[DNS 8](#_Toc26199808)

[The resolver 8](#_Toc26199809)

[Protokolli Kihid (Protocol Layers) 14](#_Toc26199810)

[TCP flags 16](#_Toc26199811)

[Big Networks 19](#_Toc26199812)

[Middleboxes: Tulemüürid ja Filtrid 20](#_Toc26199813)

[Middleboxes: Proxies and NAT 21](#_Toc26199814)

# HTTP-st PING-ni

**Ping** on [arvutivõrgu](https://et.wikipedia.org/wiki/Arvutiv%C3%B5rk" \o "Arvutivõrk) võrguühenduse diagnostikaprogramm, mille abil [IP](https://et.wikipedia.org/wiki/IP)-võrgus hinnatakse [hosti](https://et.wikipedia.org/wiki/Host" \o "Host) (serveri või muu võrguseadme) ligipääsetavust programmi käivitanud arvutist, samuti pakettide edastamiseks kuluvat aega.

Käsk: **ping -c3 8.8.8.8** - Test kas ilma aadressita saab saata 3 testsõnumit googlesse

ping vs http - Server ise reageerib pingidele otse. HTTP on erinev protokoll, mida haldab lisarakendus, veebiserver, mis peab serveris töötama (ping on opsüsteemi sisseehitatud).

**Netcat** ehk **nc** – Aitab infot saata ja lugeda otse TCP või UDC kaudu.Prinf saadab vormindatud teksti netcatile ja netcat saadab teksti läbi neti otse veebiserverile. Veebiserverilejääb mulje, et tegu on HTTP päringuga.

## Pordid

Porti kuulamine - Kuulamisport on võrguport, mida rakendus või protsess kuulab ja toimib side lõpp-punktina. Iga kuulamisporti saab tulemüüri abil avada või sulgeda (filtreerida). Üldiselt on avatud port võrguport, mis võtab vastu kaugetest asukohtadest saabuvaid pakette.

Sisestades nc -l 3456 ühte terminali ja nc localhost teise terminali, on võimalik TCP serveriteritel omavahel võimalik ühendust saada. (ctrl + D lõpetab signaali).

Portide numbrid – portide numbrid on vahemikus 1 – 65535. 1 <= 1023 on resreveeritud superkasutajale ehk administraatorile. Allpool on toodud näited

|  |  |
| --- | --- |
| **Port** | **Assignment** |
| 20 | [File Transfer Protocol](https://en.wikipedia.org/wiki/File_Transfer_Protocol) (FTP) Data Transfer |
| 21 | [File Transfer Protocol](https://en.wikipedia.org/wiki/File_Transfer_Protocol) (FTP) Command Control |
| 22 | [Secure Shell](https://en.wikipedia.org/wiki/Secure_Shell) (SSH) Secure Login |
| 23 | [Telnet](https://en.wikipedia.org/wiki/Telnet) remote login service, unencrypted text messages |
| 25 | [Simple Mail Transfer Protocol](https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) (SMTP) E-mail routing |
| 53 | [Domain Name System](https://en.wikipedia.org/wiki/Domain_Name_System) (DNS) service |
| 80 | [Hypertext Transfer Protocol](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol) (HTTP) used in the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web) |
| 110 | [Post Office Protocol](https://en.wikipedia.org/wiki/Post_Office_Protocol) (POP3) |
| 119 | [Network News Transfer Protocol](https://en.wikipedia.org/wiki/Network_News_Transfer_Protocol) (NNTP) |
| 123 | [Network Time Protocol](https://en.wikipedia.org/wiki/Network_Time_Protocol) (NTP) |
| 143 | [Internet Message Access Protocol](https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol) (IMAP) Management of digital mail |
| 161 | [Simple Network Management Protocol](https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol) (SNMP) |
| 194 | [Internet Relay Chat](https://en.wikipedia.org/wiki/Internet_Relay_Chat) (IRC) |
| 443 | [HTTP Secure](https://en.wikipedia.org/wiki/HTTP_Secure) (HTTPS) HTTP over TLS/SSL |

Kui kasutada kahes arvutis korraga sama porti, siis nc annab järgneva veateate: “Address already in use”.

printf 'HTTP/1.1 302 Moved\r\nLocation: https://www.eff.org/' | nc -l 2345 – Kui minna browserisse ja sisestada enda ip aadress :2345, siis browser saadab sind EFF-I kodulehele.

## Kokkuvõte

Netcat on palju lihtsam, kui tavaline brauser. Brauserid ja veebriserverid ei tegele ainult 1 päringuga korraga. Nad töötavad mitme päringuga korraga. Kui brauser laeb alla interneti lehe serverilt, siis peab ta alla laadima mitmeid faile kora nagu html, css ja javascript, pildid jne. Mida kiiremini saab seda paralleelselt teha, seda kiiremini saab lehe ekraanil kuvada. Selleks on olemas erinevaid protokolle ja mooduseid.

# Nimed ja Aadressid

**IP-aadress** ehk **internetiaadress** ([inglise keeles](https://et.wikipedia.org/wiki/Inglise_keel" \o "Inglise keel) *Internet protocol address*) on [arvutivõrgus](https://et.wikipedia.org/wiki/Arvutiv%C3%B5rk" \o "Arvutivõrk) asuva seadme ([arvuti](https://et.wikipedia.org/wiki/Arvuti" \o "Arvuti) või [nutiseadme](https://et.wikipedia.org/wiki/Nutiseade" \o "Nutiseade)) identifikaator ehk seadmele määratud alaline või ajutine tunnusnumber, mille abil võrku ühendatud seadmed üksteist leiavad.

Host(võõrustaja) – masin, mis majutab teenuseid.

Endpoints – 2 masinat või programmi, mis kommunikeeruvad läbi ühenduse.

Iga sõnum, mis reisib läbi internet, on jaotatud pakettideks. Igas paketis on kirjas arvuti, kust see sõnum tuleb ning asukoht, kuhu see sõnum läheb.

DNS - lühend nimest [Domain Name System](https://et.wikipedia.org/wiki/Domain_Name_System) (domeeninimede süsteem) – internetiteenus, mis tõlgib domeeninimed [IP-aadressideks](https://et.wikipedia.org/wiki/IP-aadress). Kui DNS ei tööta, siis ei saa enamus arvutid enam leheküljele ligi.

The resolver **–** Igasse OP-süsteemi ehitatud kood, mis aitab vabalt programmidel nagi NC või brauser DNS-I tuvastada.

Käsk: host - DNS-otsinguutiliit, mis otsib IP-aadressi

domeeninimega. Samuti teostab see pöördotsinguid, leides IP-aadressiga seostatud domeeninime.

DNS on kümneid erinevaid kirjetüüpe, millest toon välja tähtsamad.

Käsk: **Cname** – kirjed on domeeninime pseudonüümid.

Ns – DNS nimeserver.

Aaaa - IPv6 aadress.

Caching server(vahemäulserver) - Vahemäluserver on spetsiaalne võrguserver või teenus, mis töötab serverina ja salvestab kohapeal veebilehti või muud Interneti-sisu. Asetades eelnevalt taotletud teabe ajutisse salvestusse või vahemällu, kiirendab vahemäluserver juurdepääsu andmetele ja nõuab ettevõtte ribalaiust.

**SSL** - Tähistab "turvaliste pistikupesade kihti". SSL on turvaline protokoll, mis on välja töötatud teabe turvaliseks saatmiseks Interneti kaudu. ... Andmeid tunneb ära ainult kasutaja arvuti ja turvaline server. SSL hoiab teie nime, aadressi ja krediitkaarditeavet teie ja kaupmehe vahel, kellele te seda pakute.

Seach Domain (otsingudomeen) -Otsingudomeen on domeen, mida kasutatakse domeeni otsinguloendi osana. Domeeni otsinguloendit ja kohalikku domeeninime kasutab lahendaja täielikult kvalifitseeritud domeeninime (FQDN) loomiseks suhtelisest nimest.

**IPv4 -** on [IP aadressi](https://et.wikipedia.org/wiki/IP_aadress) esitamise protokolli viis, mis koosneb neljast 8-[bitisest](https://et.wikipedia.org/wiki/Bit) (256 erinevat väärtust) osast, mis kirjutatakse nelja omavahel punktidega eraldatud arvuna (näiteks 255.255.255.255). Iga arv on [täisarv](https://et.wikipedia.org/wiki/T%C3%A4isarv" \o "Täisarv) vahemikus 0...255 ja ta vastab 8 kohale aadressi kahendüleskirjutuses.

Ip aadress on tegelikult arvvaäärtus. Punktidega eraldatud ip aadress on tehtud lihtsalt inimesele lihtsamini loetavaks. Päris aadresside jaoks ei kasutata aga kõiki võimalikke 32-bitiseid väärtusi. Mõnda neist kasutatakse erirakenduste jaoks, mis kasutavad aadresse erinevalt. Mõned neist on reserveeritud sisemistele privaatvõrkudele. Mõned neist on testimiseks või dokumenteerimiseks. Ipv4 aadresse on vähem on kokku umbes 4 miljardit, mis teeb ka **IPv4** aadresside kasutamise probleemseks arvestades, et maailmas on üle 7 mkljardi inimese ja suurfirmad kasutavad väga paljusid aadresse.

Pordi numbrid on esitatud 16-bitiste väärtustena.

**Subnetwork**(alamvõrk) - on IP-võrgu loogiline alajaotus. 1,16 Võrgu jagamist kaheks või enamaks võrguks nimetatakse alamvõrguks.

**Subnet** **mask** ehk **netmask-** IPv4 puhul võib võrku iseloomustada ka selle alamvõrgumask või netmask, mis on bitmask, mis bitwise AND operatsiooni rakendamisel suvalisele võrgu IP-aadressile annab marsruudi eesliite. Alamvõrgu maskid on väljendatud ka punkti-kümnendarvuna nagu aadress. Näiteks 255,255.255.0 on eesliite alamvõrgu 198,51.100.0/24. /14 network maskis on üle 250 000 aadressi.

Käsk: **ip addr show** – kasutatakse võrguliideste (nt IP-aadress, MAC-aadress) sügavusteabe saamiseks.

**Kohtvõrk** ehk **lokaalvõrk** ehk **LAN** (ingl. *Local Area Network*) on [arvutivõrk](https://et.wikipedia.org/wiki/Arvutiv%C3%B5rk" \o "Arvutivõrk), mis ühendab piiratud [maa-alal](https://et.wikipedia.org/wiki/Maaala" \o "Maaala), [hoones](https://et.wikipedia.org/wiki/Hoone" \o "Hoone) jne asuvaid arvuteid ja võrguseadmeid. Kohtvõrgud võivad olla näiteks kodus, kontoris ja koolis. Kohtvõrku eristab [laivõrgust](https://et.wikipedia.org/wiki/Laiv%C3%B5rk" \o "Laivõrk) üldjuhul suurem andmeedastuskiirus, väiksem geograafiline ulatus ning tasuliste andmesideliinide mittevajalikkus. Samuti saavad samasse kohtvõrku ühendatud arvutid omavahel näiteks printereid ja faile jagada. Kohtvõrku eraldab üldvõrgust ([internetist](https://et.wikipedia.org/wiki/Internet" \o "Internet)) tavaliselt [tulemüür](https://et.wikipedia.org/wiki/Tulem%C3%BC%C3%BCr_(informaatika)" \o "Tulemüür (informaatika)). Kohtvõrke eristatakse võrgu topoloogia, pöördumisviisi ja töökiiruse järgi.

**Laivõrk** (inglise keeles *wide area network* ehk *WAN*) on [telekommunikatsiooni](https://et.wikipedia.org/wiki/Telekommunikatsioon" \o "Telekommunikatsioon) võrk või [arvutivõrk](https://et.wikipedia.org/wiki/Arvutiv%C3%B5rk" \o "Arvutivõrk), mille kokkuleppeline ulatus on üle 1 km. Laivõrgud kasutavad [järjestikliine](https://et.wikipedia.org/w/index.php?title=J%C3%A4rjestikliin&action=edit&redlink=1" \o "Järjestikliin (pole veel kirjutatud)) (inglise keeles *serial line*), mis on kaht järjestikporti ühendavad juhtmed, mida mööda liiguvad järjestikustest bittidest koosnevad järjestikandmed (levinuim jadaliini standard on RS-423).[[1]](https://et.wikipedia.org/wiki/Laiv%C3%B5rk#cite_note-1) Laivõrk koosneb mitmetest [kohtvõrkudest](https://et.wikipedia.org/wiki/Kohtv%C3%B5rk" \o "Kohtvõrk) (inglise keeles *local area network* või *LAN*), mis on omavahel enamasti ühenduses renditud telekommunikatsiooniliinide (näiteks telefoniliin), optilise kaabli või satelliitühenduse läbi. Laivõrgule on tavaliselt iseloomulik aeglasem andmevahetuskiirus kui kohtvõrgus. Maailma suurimaks laivõrguks võib pidada [Internetti](https://et.wikipedia.org/wiki/Internet" \o "Internet).

**Ethernet** on juhtmetega [kohtvõrgu](https://et.wikipedia.org/wiki/Kohtv%C3%B5rk" \o "Kohtvõrk) tehnoloogia, mis vastab [Elektri- ja Elektroonikainseneride Instituudi](https://et.wikipedia.org/wiki/Elektri-_ja_Elektroonikainseneride_Instituut" \o ") standardile [IEEE 802.3](https://et.wikipedia.org/w/index.php?title=IEEE_802.3&action=edit&redlink=1) ja kasutab juhuslikku pöördumisviisi [CSMA/CD](https://et.wikipedia.org/wiki/CSMA/CD) (multipöördus süsteem põrketuvastusega). Ethernet on alates 1990ndatest põhiline kohtvõrgu tehnoloogia ja selliste võrkude kaudu on ühendatud enamik ühenduses olevatest arvutitest ja tööjaamadest maailmas. Kõik ülejäänud kohtvõrgustandardid on ta välja tõrjunud või muutnud nišitoodeteks.

**Marsruuter** ehk **ruuter** on elektrooniline seade, mis ühendab omavahel kaht või enamat [arvutivõrku](https://et.wikipedia.org/wiki/Arvutiv%C3%B5rk" \o "Arvutivõrk), ning võimaldab nendevahelise [andmeside](https://et.wikipedia.org/w/index.php?title=Andmesid&action=edit&redlink=1" \o "Andmesid (pole veel kirjutatud)).

**Ruuteri tööpõhimõte** - Andmeside kahe arvutivõrgu vahel toimib pakettidena. Iga pakett sisaldab informatsiooni selle kohta, millisest võrgust see tuleb ja millisesse võrku see minema peab. Nende aadresside järgi saab ruuter otsustada, kas paketi saatja ja vastuvõtja on ühes võrgus või on vastuvõtja saatjast erinevas võrgus. Kui alamvõrgust (nt koduarvutist) on soov saavutada ühendus ülemvõrguga (nt internet), siis ruuter otsib oma marsruutimistabelist (ruuterisisene tabel, kus on kirjas ruuteriga ühendatud arvutite ja võrkude aadressid), kas ülemvõrgu aadress on tabelis olemas. Juhul, kui aadressi seal ei ole, siis saadab ruuter paketi [modemi](https://et.wikipedia.org/wiki/Modem" \o "Modem) aadressile, mis omakorda loob ühenduse soovitud [internetiserveriga](https://et.wikipedia.org/wiki/Server" \o "Server), ning saadab saadud paketi tagasi ruuterile. Ruuter saadab omakorda paketi tagasi päringu teinud seadmele. Juhul, kui alamvõrgu seade soovib ühendust saada teise alamvõrgu seadmega, siis leiab ruuter soovitud seadme aadressi marsruutimistabelist ja edastab paketi otse õigele seadmele, ilma modemit läbimata.

**A default gateway** - Interneti-protokollikomplekti kasutav arvutivõrgu sõlm, mis toimib edasisuunamise hostina (ruuterina) teistele võrkudele, kui ükski teine ​​marsruudi spetsifikatsioon ei vasta paketi IP-aadressile.

Käsk: **ip route show default** - leiab default gateway.

**NAT ehk Võrguaadresside teisendus** (ka **võrguaadresside tõlkimine**, **võrguaadresside transleerimine**; inglise *Network Address Translation*) on võrguliikluses ja [ruuterites](http://vikipeedia.ee/Ruuter" \o "Ruuter) kasutatav tehnika, mis seisneb [IP](http://vikipeedia.ee/Internetiprotokoll)-pakettide päiste muutmises, nii et paistaks, nagu võrguliiklus tuleneks NAT-ruuterist, kuigi ühenduse looja oli mingi seade NAT-ruuteri "taga". Selle abil saab terveid arvutivõrke ühe ruuteri taha peita ja kogu liiklus paistab tulevat ruuteri väliselt IP-aadressilt. Enda IP aadessi saab teada näiteks Google-sse sisse kirjutades my IP address.

**ISP Internetiteenuse pakkuja** (inglise keeles *internet service provider*) on [organisatsioon](http://vikipeedia.ee/Organisatsioon" \o "Organisatsioon), mis pakub [Internetile](http://vikipeedia.ee/Internet" \o "Internet) ligipääsu ja kasutamise teenuseid.

**IPv6** (Internetiprotokolli versioon 6) ehk "uue põlvkonna" Internetiprotokoll ([inglise keeles](https://et.wikipedia.org/wiki/Inglise_keel" \o "Inglise keel) **IPng**, *Internet Protocol Next Generation*) on andmesideprotokoll, mis on loodud praegusel ajal üldkasutatava [Internetiprotokolli](https://et.wikipedia.org/wiki/Internetiprotokoll" \o "Internetiprotokoll) [IPv4](https://et.wikipedia.org/wiki/IPv4) asendamiseks.

Põhjuseks uue internetiprotokolli väljatöötamiseks oli vajaduses suurema arvu [IP-aadresside](https://et.wikipedia.org/wiki/IP-aadress) järele. Esialgu jagati aadresse pillavalt. IPv4-aadress on kaheastmeline (võrgu aadress ja [hosti](https://et.wikipedia.org/wiki/Host" \o "Host) aadress) ning IPv4 32-bitine aadressiruum on hakanud ammenduma. 232 tähendab küll üle 4 miljardi aadressi, kuid nende ebatõhus kasutamine on viinud IP-aadresside lõppemisele. Mõeldi küll välja ajutisi lahendusi, millest levinuim on olnud [NAT](https://et.wikipedia.org/wiki/NAT) (Network Address Translation), kuid see toob kaasa teisi puudusi, millest suurim on võimaluse puudumine otse avalikust võrgust ühendus luua.

IPv6 on nendest puudustest vaba. Selle aadressid on pikemad ja nende vorming on teine. Kasutatav 128-bitine aadress lubab teoreetiliselt anda aadresse 2128-le seadmele, mis on võrreldamatult rohkem kui näiteks isegi liivateri maailmas on (üle saja miljoni miljardi aadressi maakera iga ruutmillimeetri kohta). Nii suur hulk võib tunduda pillamisena, kuid nii näis see ka mitukümmend aastat tagasi 32-bitise aadressiga. Samuti lihtsustab uus protokoll mitmeid marsruutimise probleeme. Üks lihtsustumise põhjus on fikseeritud pikkusega IP-paketi [päise](https://et.wikipedia.org/wiki/P%C3%A4is" \o "Päis) kasutuselevõtt, mis kiirendab pakettide töötlemist ja parandab marsruuterite jõudlust.

Arendades internetiaplikatsioone tänapäeval, peab kindlasti arvestama sellega, et **IPv6** aadresse tuleb pidevalt ning aplikatsioon peab neid mõistma!

# Protokolli Kihid (Protocol Layers)

**TCP(Edastusohje protokoll**. [ingl](http://vikipeedia.ee/Inglise_keel) *Transmission Control Protocol* ) on levinuim [transpordikihi](http://vikipeedia.ee/Transpordikiht" \o "Transpordikiht) [võrguprotokoll](http://vikipeedia.ee/V%C3%B5rguprotokoll" \o "Võrguprotokoll), mida kasutatakse [TCP/IP](http://vikipeedia.ee/TCP/IP) võrkudes. Kuna TCP-protokoll on peaaegu alati kasutuses koos IP-protokolliga ([Internet Protocol](http://vikipeedia.ee/Internetiprotokollistik)), siis tavaliselt kasutatakse nime *TCP/IP*.

TCP-protokolliga saadetavaid pakette toimetab edasi võrgukihi protokoll, milleks on üldjuhul [internetiprotokoll](http://vikipeedia.ee/Internetiprotokoll" \o "Internetiprotokoll) (IP). TCP/IP mudeli järgi on loodud enamik arvutivõrke.

TCP-ühendus toimib ainult otspunktide vahel (näiteks kliendi ja serveri vahel). Vahepealsed seadmed, nagu [marsruuterid](http://vikipeedia.ee/Marsruuter" \o "Marsruuter), seda osa pakettidest ei muuda.

TCP tegeleb voo- ja koormusjuhtimisega. Voojuhtimine (*flow control*) tähendab, et TCP jälgib pidevalt otspunktide andmevooge ning teeb andmeedastuse kiiruses ja mahus selle järgi parandusi. Koormusjuhtimine (*congestion control*) tähendab, et TCP jälgib otspunktidevahelise võrgu koormust ning muudab ka selle järgi pakettide parameetreid.

TCP sobib rakendustele, mis vajavat töökindlat andmeedastust, kus kiirus ei ole kriitiline.

**UDP(Kasutajadatagrammi protokoll**. ingl *User Datagram Protocol*) on [transpordikihi](http://vikipeedia.ee/Transpordikiht" \o "Transpordikiht) [andmesideprotokoll](http://vikipeedia.ee/Protokoll_(andmeside)" \o "Protokoll (andmeside)), mis on defineeritud [IP-ga](http://vikipeedia.ee/Internetiprotokoll) sõnumite saatmiseks.

UDP võimaldab IP-aadressiga kirjeldatud otspunktide vahele luua olekuta ühendusi ehk UDPl ei ole erinevalt [TCPst](http://vikipeedia.ee/TCP" \o "TCP) selgelt eristatavaid olekuid "suletud", "ühendamisel", "ühendatud". Kuna ühenduse olekut ei kontrollita, peab UDP kasutama *best-effort* põhimõtet ehk paketi väljasaatmise järel loodetakse, et see jõuab kohale. Kui pakett mingil põhjusel kohale ei jõua, ei ole saatjal võimalik seda protokolli tasemel tuvastada ja seetõttu ei toimu ka automaatset paketi uuestisaatmist.

UDP ei kontrolli paketi kohalejõudmist. Samuti ei nummerda UDP saadetud pakette, mis tähendab, et paketid võivad sihtpunkti jõuda suvalises järjekorras ja neid ei ole võimalik hiljem protokolli tasemel järjestada. Samuti ei ole võimalik tuvastada, kas mingist paketist jõuab sihtpunkti mitu koopiat. UDP ei tuvasta ka ummikuid ega piira sellest tulenevalt saadetavate andmete mahtu (erinevalt [TCPst](http://vikipeedia.ee/TCP" \o "TCP)).

UDP ei paku saadetud andmetele konfidentsiaalsust ega terviklikkust. UDP-protokoll ei [krüpteeri](http://vikipeedia.ee/Kr%C3%BCpteerimine" \o "Krüpteerimine) andmeid ehk paketi sisu on andmeside pealtkuulajale kergelt loetav. UDP ei taga, et algpunkti ja sihtpunkti vahel andmeid sihiteadlikult ei muudeta ([vahendajarünne](http://vikipeedia.ee/Vahendajar%C3%BCnne" \o "Vahendajarünne)). Küll aga sisaldab UDP [kontrollsumma](http://vikipeedia.ee/Kontrollsumma" \o "Kontrollsumma) arvutamist võimalike ülekandevigade tuvastamiseks.

UDP-ühenduse loomine on lihtne ja võtab vähe ressursse. Ühenduse loomiseks on vaja teada ainult sihtpunkti IP-aadressi ja pordi numbrit. UDPl põhinev andmeside on ebakindel, aga kiire, sest sihtpunkt ei pea pakettide kättesaamise kohta kinnitusi saatma. UDP lihtsuse tõttu on ka paketi päis lihtne ja väikese mahuga (8 baiti). Ühte UDP-paketti mahub maksimaalselt natuke alla 64 KiB andmeid (65 507 baiti [IPv4ga](http://vikipeedia.ee/IPv4) ja 65 527 baiti [IPv6ga](http://vikipeedia.ee/IPv6)).

UDP levinumad kasutusalad on sellised, kus kõigi pakettide kohalejõudmine ei ole oluline, andmeside madal latents (sihtpunkti jõudmise aeg) on tähtis või transpordikihist kõrgemal olev protokoll implementeerib ise pakettide uuestisaatmise ja järjestamise.

Käsk: **tcpdump** - on tavaline pakettanalüsaator, mis töötab käsurea all. See võimaldab kasutajal kuvada TCP/IP ja muid pakette, mis edastatakse või võetakse vastu võrgu kaudu, millega arvuti on ühendatud.

Käsk**: sudo tcpdump -i eth0 -n src host <IP address> -v** - Paljusõnalise liiklusteabe vaatamiseks konkreetses võrguliideses konkreetsest hostist.

Käsk: sudo tcpdump -i eth0 -n “src host <IP address> dst port 80 or dst port 443” -vvv - Väga paljusõnalise liiklusteabe vaatamiseks konkreetses võrguliideses konkreetsest hostist portide 80 (HTTP) 443 (HTTPS) suunas:

**Sequence Numbers (Tcp järjenumbrid)** - Järjekorranumber on saadetud TCP-paketis (nimetatakse ka TCP-segmentiks) olevate andmete esimese baidinumber. Kinnitusnumber on järgmise baidi järjekorranumber, mida vastuvõtja eeldatavasti vastu võtab.

## TCP flags

Madalatasemelistes arvutikeeltes on flag kahendväärtus – tõene või väär väärtus –, mis salvestatakse mällu ühe bitina. Kui lipubitt on 1, siis ütleme, et flag on seatud. Kui lipubitt on 0, siis lipp kustutatakse (või tühistatakse). Tavaliselt tulevad flagid gruppidesse, millest igaüht saab sättida või tühjendada.

6 põhilist TCP flagi:

* SYN (sync) [S] – see pakett avab uue TCP seansi ja sisaldab uut algset järjekorranumbrit
* FIN (finish) [F] – seda paketti kasutatakse TCP seansi normaalseks sulgemiseks
* PSH (push) [P] – see pakett on rakenduseandmete kogumi (nt HTTP-päringu) lõpp.
* RST (reset) [R] – see pakett on TCP veateade; saatjal on probleem ja ta soovib seansi lähtestada (hüljata).
* ACK (acknowledge) [.] (Kinnita) – see pakett kinnitab, et saatja on teisest lõpp-punktist andmeid saanud. Peaaegu igal pakil peale esimese SYN on ACK lipp seatud
* URG (pakiline) [U] – Pakett sisaldab andmeid, mis tuleb edastada rakendusele tellimusväliselt. Ei kasutata HTTP-s ega enamikus muudes praegustes rakendustes.

*three-way handshake* - ühendus on töökindel, sest toimub kolmepoolne kinnitus ehk *three-way handshake*. Klient saadab serverile ühenduse loomise soovi, server vastab ning saadab samuti ühenduse loomise soovi, mille klient kadudeta andmevahetuse korral vastusega kinnitab.

Four-way teardown - Kui kumbki lõpp-punkt on ühendusse andmete saatmisega tehtud, võib ta saata FIN-paketi, mis näitab, et see on lõpule viidud. Teine näitaja saadab ACK-i, et näidata, et ta on FIN saanud. HTTP-andmete näites saadab klient kõigepealt oma FIN-i, niipea kui see on HTTP-päringu saatmise lõpetatud. See on esimene pakett, mis sisaldab lippe [F.]. Lõpuks tehakse ka teine ​​tulemusnäitaja saatmine ja see saadab oma FIN-i. Siis saadab esimene lõpp-punkt ACK-i.

In between (vahepeal) - Pikaajalises ühenduses on palju pakette, mida vahetatakse edasi-tagasi. Mõned neist sisaldavad rakenduse andmeid, teised võivad olla ainult ilma andmeteta kinnitused (pikkus 0). Kõik ühenduse TCP paketid, välja arvatud algne SYN, sisaldavad siiski kinnitust kõigi andmete kohta, mida saatja on seni saanud. Seetõttu on neil kõigil ACK lipp seatud. (just seetõttu kujutab tcpdump ACK lippu vaid täpiga: see on tõesti tavaline.)

**Packet loss** - Pakettkaotus toimub siis, kui üks või mitu andmepaketti reisivad arvutivõrgu faili kaudu sihtkohta jõudmiseks. Pakettide kaotuse põhjustavad kas vead andmeedastuses, tavaliselt traadita võrkude kaudu, või võrgu ummikud. Pakettide kadu mõõdetakse kaotatud pakettide protsendina saadetud pakettide suhtes.

Näited, mis põhjustavad TCP time-outi:

* Teise otsa host lülitub ootamatult välja
* Torm puhub lahti teie ja teie ISP vahelise kaabli
* Sa proovid ühendada end serveriga, mis ei eksisteeri

# 

# Big Networks

**Traceroute** - on käsuribal põhinev tööriist, mida kasutatakse paketi sihtmärgi saavutamiseks kasutatava tee tuvastamiseks. See tööriist kasutab ka ICMP-teateid, kuid erinevalt pingist tuvastab see iga ruuteri paketi kulgeval teel. Traceroute on kasulik võrguprobleemide tõrkeotsingul, kuna see aitab tuvastada, kus probleem täpselt on. Saate aru saada, millist ruuterit teel kättesaamatu sihtmärgini tuleks lähemalt uurida kui võrgu rikke tõenäolist põhjust.

Käsk: traceroute <aadress või ip> - Näitab teekonna ja vahesammud, et aadressini jõuda. Aadresside asukoha saab tihtipeale aru lennujaamade lühendite järgi, mis traceroute esile toob. Ping time ehk round trip näitab aega pakettki väjasaatmisest kuni vastuse saamiseni.

**Network bandwidth** (Võrgu ribalaius) - määratlus võib olla segane, kuid põhimõtteliselt määratletakse võrgu ribalaius võrgu maksimaalse edastusvõimsusena. See mõõdab, kui palju andmeid saab korraga saata ja vastu võtta. Ribalaiust mõõdetakse bittides, megabittides või gigabittides sekundis.

**Bandwidth-delay product** - andmemaht, mida saab ühenduse kaudu edastada

Näide : Kuult maale on 384 000km, ühendus: 1Gbit/s, valguskiirus 300 000 km/s = 1,28Gbit/s.

## Middleboxes: Tulemüürid ja Filtrid

Tulemüürid(**firewall**) on seadmed, mida võrguoperaatorid saavad kasutada nende võrku siseneva või sealt väljuva liikluse filtreerimiseks. Tulemüür on üks näide võrguseadmete klassist, mida nimetatakse keskkastideks (**middleboxes**)- seadmed, mis kontrollivad, muudavad või filtreerivad võrguliiklust. Muud vahebokside näited hõlmavad sissetungimise tuvastamise süsteeme ja koormuse tasakaalustajaid. Tehniliselt on see vaid keskmist kasti, kui see on kliendist või serverist eraldi seade - serveripoolsed tulemüürid, nagu Linuxi iptables, ei ole keskmised kastid.

Tulemüür võib olla organisatsiooni võrguturbe tõeline õnnistus. Tulemüüri kõige tavalisem konfiguratsioon on kogu sissetuleva liikluse ärajätmine, välja arvatud liiklus paaridesse (host, port), mis väidetavalt saavad Interneti-ühendust. See võimaldab võrguadministraatoril olla kindel, et teised võrgus olevad masinad - näiteks taustandmebaasid või haldussüsteemid - ei saa otseseid rünnakuid väljastpoolt.

Kuid tulemüürid võivad rakenduste arendajatele probleeme tekitada. Kui proovite võrgurakendust testida või juurutada ning teie serveri ja kasutaja vahel on tulemüür, võib see tulemüür teie rakendust häirida või selle täielikult blokeerida. Rakenduse installimiseks konkreetsesse serverisse ja porti aitab see teada saada, milline tulemüür võib teie ja teie kasutaja vahel olla. Üks põhjus, miks paljud veebivälised rakendused kasutavad HTTP-d transpordina, on see, et HTTP blokeeritakse tulemüürides sageli ka siis, kui muud pordid on blokeeritud.

Lisaks otse liikluse blokeerimisele võivad keskmised kastid muuta ka liiklust, näiteks asendada veebilehed veateadetega. Seda tehakse sageli sotsiaalsetel või poliitilistel eesmärkidel. Näiteks USA-s kasutavad paljud koolid mitmesuguseid liiklusfiltreid, et takistada õpilastel pääseda laste jaoks sobimatutele veebisaitidele. Kuid see, mida saitideks peetakse sobimatuks, võib kajastada filtri kirjutanud või konfigureerinud inimeste eelarvamusi või arvamusi.

Mõned kasutajad kurdavad, et ei saa enam sinu leheküljele ligi. Sa tahad teada kas probleem on filtris või tulemüüris. Probleemisle lahenduse leidmiseks oleks mõistlik uurida järgnevaid punkte:

* Kas kasutaja saab teie saiti pingida?
* Kas kasutaja saab ligi teisele domeenile samas serveris?
* Kas kasutaja saab järgi vaadata server nime host või dig käske?
* Kas kõik kasutajad, kellel on probleeme samast riigist?

## Middleboxes: Proxies and NAT

Varem sel kursusel õppisite IPv4 aadressi puudusest; ning selle vältimiseks võrguaadresside tõlkimise ehk NAT-i kasutuselevõttu. NAT-i abil saavad mitmed seadmed Interneti-ressurssidele juurde pääseda ühe avaliku IP-aadressi kaudu, samas kui NAT-seade kasutab pordi numbreid, et sobitada ühendusi seest ja väljast.

Lõppkasutajate jaoks kattuvad NAT-seadmed tulemüüridega. Tüüpilised koduruuterid võivad toimida nii NAT-i kui ka lihtsa tulemüürina, omades sageli võimalust blokeerida või filtreerida väga põhitasemel. Laiemas plaanis on Interneti-teenuse pakkujad ja muud organisatsioonid juurutanud NAT-seadmed kogu oma kliendivõrgu jaoks, mida nimetatakse operaatoriklassi NAT-ideks. See on väga levinud mobiilsidevõrkude ja ka arengumaade Interneti-teenuse pakkujate puhul, kus kunagi polnud kuskil läheduses kasutajate arvu jaoks piisavalt aadresse.

Tavaliselt kujutleme lõppkasutaja arvutit sellisena, et seda kasutab korraga ainult üks inimene. Lõppude lõpuks on seal ainult üks hiir ja klaviatuur. Kaks klaviatuuri samal ajal kirjutavat inimest ei juhtu tavaliselt väljaspool halvasti läbimõeldud telesaateid. Kuid NAT-i korral näeb teie veebisait sama IP-aadressi päringuid, mis pärinevad tegelikult erinevatelt arvutitelt erinevatelt kasutajatelt.

Teine viis, mis juhtuda võib, on veebipõhiste puhverserverite(**web proxies**) kasutamine. Kui NAT töötab IP-tasemel, kirjutades ümber pakette, siis veebipuhverserver(web proxy) töötab HTTP-tasemel, võttes brauseritest päringuid ja saates need veebiserveritele. Paljud organisatsioonid kasutavad vahemällu salvestamiseks veebipõhiseid puhverservereid, sealhulgas mõned Interneti-teenuse pakkujad. Veebiarendaja või saidipidaja seisukohalt näeb hõivatud puhverserveri liiklus välja samamoodi nagu hõivatud NAT-i liiklus: paljude kasutaja päringud koondatakse paljudes tegelikes arvutites ühe avaliku IP-aadressi kaudu.

Järgnev on nimekiri, kuidas tuvastada sama avaliku ip aadressi taga olevad isikud:

* Kasutaja on sisse logitud, mille kaudu saab kasutaja identiteedi teada
* Seansiküpsised