NAT

RFC 3022 *(Network Address Translation)*

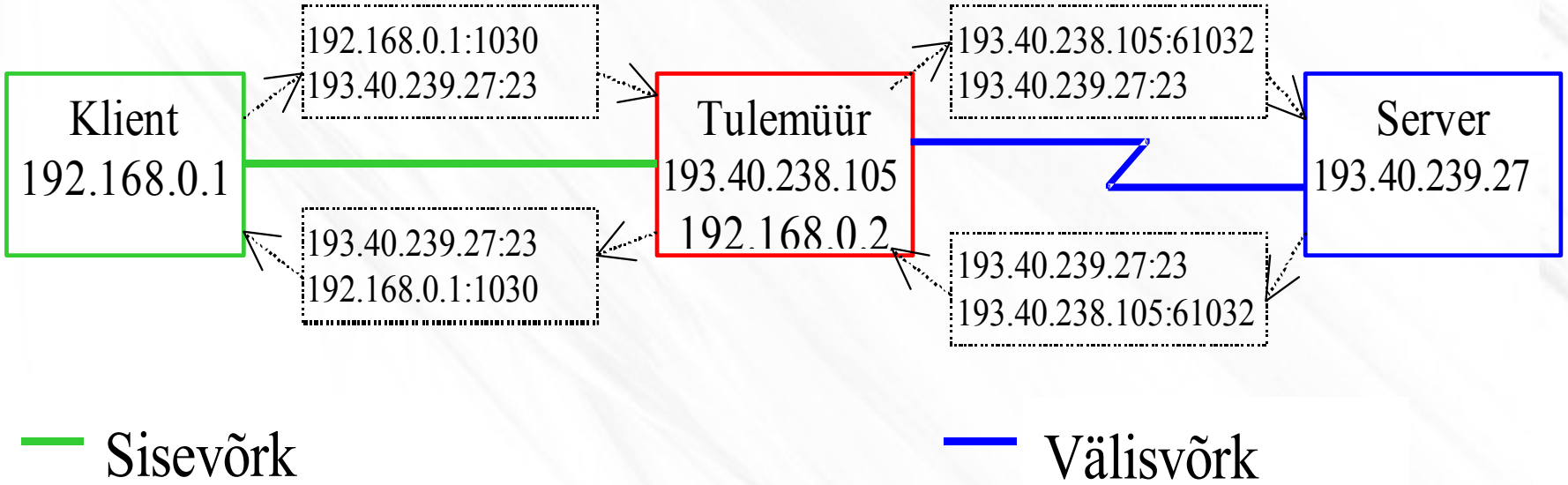
- Tegelikult kaks osa
  - NAT
  - PAT *(Port Address Translation)*
  - Kokku: NAPT *(Network Address and Port Translation)*
  - Tavaliselt realiseeritud (IPv4) marsruuteri lisafunktsionaalsusena

NAT

- Privaatvõrkudeks kasutatavad IP aadressid – 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
- Pordid, nt TCP ja UDP protokolli pordid

NAT *(masquerading)*

- Välisvõrgule on sisevõrk nähtamatu
- Lähte IP aadress ja port asendatakse NAT seadme välisvõrgu IP aadressi ning mingi pordiga



NAT

- SNAT *(Source Network Address Translation)* – kasutatakse nö *masquerade* tegemiseks, et sisevõrgu seadmed saaksid välisvõrguga suhelda
- DNAT *(Destination Network Address Translation)* – kasutatakse SNAT seadmesse nö “aukude” tegemiseks, et sisevõrgus olev server oleks nähtav välisvõrku
  - mõnikord kutsutakse ka “virtuaalseks serveriks” või “pordi edastuseks” *(port forwarding)*

NAT plussid-miinused

+ Hoitakse kokku palju avaliku võrgu IP aadresse

+ Interneti ühenduse pakkuja (ISP) vahetuse korral pole vaja muuta sisevõrgu hostide IP-seadeid

+ Lisab võrguturvalisust – väljapoole ei paista sisemine topoloogia ja aadressid, vaikimisi väljastpoolt sisevõrku ühendusi luua ei saa

- Piirab samaaegsete ühenduste arvu

- Lõhub TCP mudeli, kus ühenduste olekuid peavad teadma vaid otspunktid

- Raskendatud suhtlevate masinate kindlakstegemine

- Osad (mitmed!) programmid ja protokollid ei tööta NAT-ga või vajavad lisatarkvara/-mooduleid

- Suurendab viivitust, kuna marsruuteris tuleb teha lisatööd

DMZ

- Vaikimisi visatakse kõik tundmatud välisvõrgust tulnud ühenduse loomise paketid ära
- Osadel NAT seadmetel on võimalik need paketid edasi saata administraatori poolt määratud sisevõrgumasinale
  - Seda masinat nimetatakse demilitariseeritud tsooniks (d*emilitarized zone*, DMZ), tegelikult on tegu küll “demilitariseeritud” hostiga