# S−38.191 Televerkot yrityksissä

Luento 2: Network Address Translation



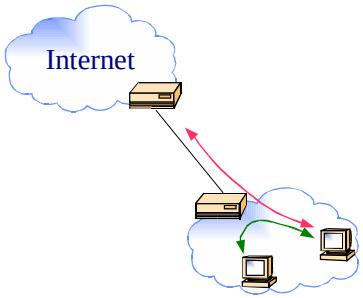
# Miksi ?

- **Ongelma:**
  - A,B ja C −luokkiin perustuva osoitejako johti osoiteavaruuden fragmentoitumiseen ja huonoon hyötysuhteeseen. Jaettavien osoitelohkojen loppuminen uhkasi jo lyhyelläkin aikavälillä.
- **Ratkaisuja:**
  - Pitkällä tähtäimellä
    - Uusi Internet Protokolla, joka mahdollistaisi suuremman määrän osoitteita
  - Lyhyellä tähtäimellä
    - Osoitteiden luokattomuus. Liitetään osoitteeseen peite, jonka perusteella määrätään verkon koko kahden potensseina.
    - ***Hyödynnetään samoja osoitteita useammassa kohdassa verkkoa, mikäli kyseisten verkon osien ei tarvitse (ainakaan täydessä laajuudessa) kommunikoida muualle verkkoon.***



# Miten ?

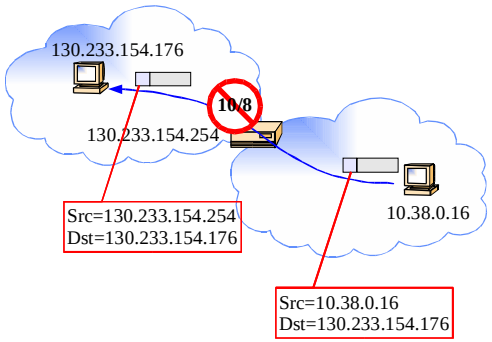
- Hyödyntää yleistä havaintoa, että vain pieni osa yksittäisen nysä/tynkä alueen ***(stub network)*** laitteista kommunikoi alueen ulkopuolelle
  - Saman aikaisesti (dynaamisuus)
  - Yleensäkään (staattisuus)
- Tynkäalue voi olla mikä tahansa internet, joka on muun verkon kannalta yhdestä pisteestä liitetty ja jonka sisällä on yhtenäinen osoitteistus.






# Miten ?

- NATin tehtävä on muuntaa IP−pakettien osoitekenttien sisältöä niiden kulkiessa kahden verkon välillä, joihin NAT on yhteydessä.
- Periaate on siis varsin yksinkertainen.
- Teknisesti tähän liittyy kuitenkin useita vaiheita ja ongelmia, joita käsittelemme tällä luennolla



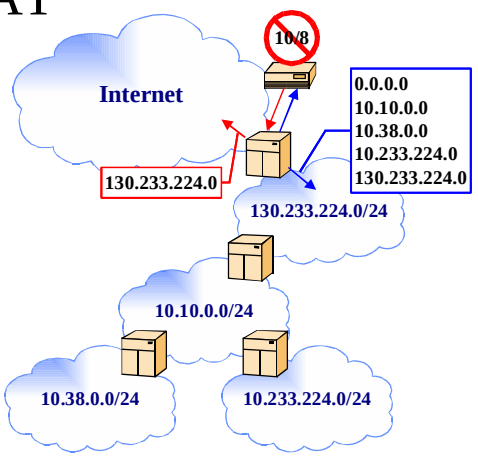
# NATin käyttö tarpeita

- Kahden IP−verkon välillä, jos toisessa verkossa käytetään lokaaleja IP−osoitteita (osoitteita, joita **ei** voida käyttää globaaliin kommunikaatioon):
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Sama osoiteavaruus on käytössä molemmissa verkoissa:
  - Lokaaleja osoitteita (kaksi riippumatonta organisaatiota voi käyttää sisäisesti samoja osoitteita)
  - Globaaleja osoitteita (toinen organisaatioista on saattanut kuulua jonkun muun operaattorin verkkoon ja kuitenkin halunnut säilyttää ko verkon osoitteet)



# NAT

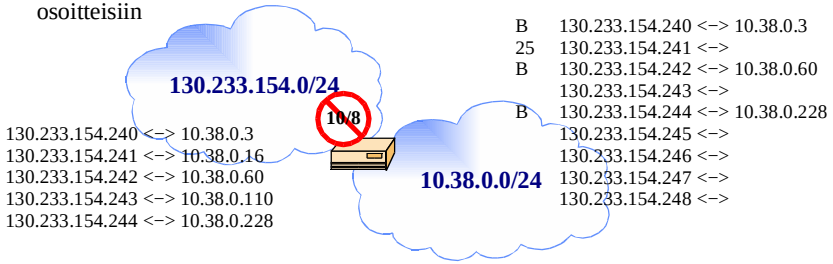
- NAT tarjoaa välityspalvelua kahden osoitereaalisaation välillä
  - NAT **ei** ole reititin
  - Välityspalvelulla tarkoitetaan osoitteen muunnosta muotoon, joka mahdollistaa normaalin välittämisen toisessa osoitereaalisaatiossa
  - ***NAT voi kuitenkin olla integroituna reitittimen ohjelmistoon***
- NAT **voi** puuttua reititysilmoituksiin tarkastamalla, että tynkäalueen muunnettavia osoitteita (verkkoja) ei mainosteta muualle Internettiin.






# Vaihtoehdot

- Staattinen NAT
  - Niille päätelaitteille, joiden on tarve kommunikoida muun maailman kanssa tehdään staattinen varaus tiettyihin osoitteisiin

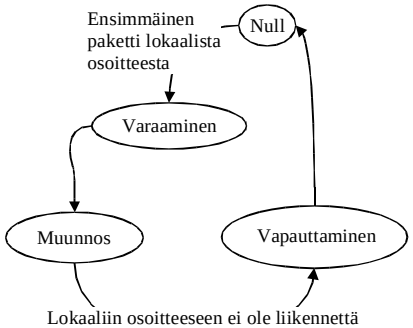



- Dynaaminen NAT
  - Mikäli ei ole tietoa tarpeista tai ne ovat satunnaisia, varataan joukko osoitteita, joita NAT hyödyntää dynaamisesti

B 130.233.154.240 <−> 10.38.0.3
25 130.233.154.241 <−>
B 130.233.154.242 <−> 10.38.0.60
130.233.154.243 <−>
B 130.233.154.244 <−> 10.38.0.228
130.233.154.245 <−>
130.233.154.246 <−>
130.233.154.247 <−>
130.233.154.248 <−>



# Dynaaminen NAT




- Tilakoneella on kolme tilaa
  - **Osoitteen varaaminen**
    - Lokaalin verkon päätelaite aloittaa kommunikaation NATin kautta tai ulkoapäin halutaan kommunikoida lokaalin verkon päätelaitteelle.
    - Globaali osoite liitetään lokaaliin osoitteeseen, jonka jälkeen kaikki ’yhteydet’ kyseisestä lokaalista osoitteesta saavat NATissa kyseisen globaalin osoitteen.

# Dynaaminen NAT

- **Osoitteen haku ja muunnos**
  - Kyseiseltä lokaalin verkon päätelaitteelta on tullut paketteja jo aiemmin ja sille on tehty jo osoitteen liittäminen
  - Suoritetaan tarvittavat muunnokset ja aktivoidaan mahdollisesti tarvittavat sovellusriippuvat osat (ALG)
- **Osoitteen vapauttaminen**
  - Lokaalin päätelaitteen kommunikaatio globaaliin verkkoon on päättynyt eikä globaalia osoitetta enää tarvitse varata sen käyttöön.
    - Viimeisellä TCP−yhteydellä on tullut FIN ja siihen liittyvä kuittaus
    - Paketteja ei ole liikkunut 5 minuuttiin
    - Avoimella TCP−yhteydellä ei ole toimintaa 24 tuntiin



# NATin vaikutuksia

- **Seuraus 1**
  - IP−otsikon sisältö muuttuu (binäärinen)
- **Vaikutus**
  - IP−otsikon tarkistussumma täytyy laskea uudestaan
    - Tarkistussumma on yhden komplementti −> tarvitsee laskea erotus muuttuneelle osoittekentälle ja lisätä se tarkistussummaan
  - TCP:n tarkistussumman täytyy laskea uudelleen (TCPn pseudo−otsikko sisältää IP−osoitteet).
    - Sama yhden komplementti laskenta kuin IP:lle



# NATin vaikutuksia

- **Seuraus 2**
  - Sovellusprotokollan sisältämä osoitetieto muuttuu
- **Vaikutus**
  - Mikäli osoite on koodattu numeroina voi paketin pituus muuttua
    - 10.38.0.16 <−> 130.233.154.242
  - Muuttunut pituus aiheuttaa TCPn tarkistussumma vaatii muutoksen
  - TCPn järjestysnumero (sequence number)ja kuittausnumero (acknowledge number) vaativat muutokset.
    - Tarvitaan erillinen tilakone huolehtimaan lähtevien pakettien ja vastaanotettujen kuittausten välisestä sovellusriippuvasta muunnoksesta.

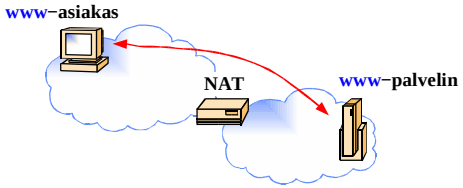


# Application Level Gateway

- ALG on
  - NATin spesifinen toteutus tietylle sovellusprotokollalle
  - Sidottu tiettyyn protokollaporttiin tuleviin paketteihin
  - Suorittaa yksittäisen protokollan vaatimat muutokset paketin rakenteeseen
  - Ylläpitää tilakonetta yskittäisille datavoille, jotta tarvittavat muutokset voidaan suorittaa.
- Tyypillisiä ALG−protokollia
  - FTP
  - HTTP
  - ICMP
  - Telnet
  - H.323

# Julkisesta verkosta lokaaliin verkkoon ?

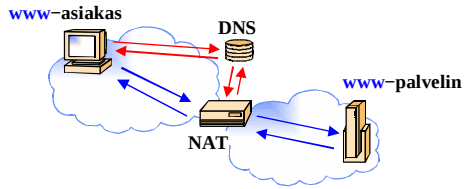
- **Kysymys:**
  - Miten Internettiin kytketty päätelaite voi ottaa yhteyden NATin takana olevaan toiseen päätelaitteeseen ?
- **Ongelma:**
  - www−palvelin käyttää lokaalia osoitetta (esim 10/8 −verkosta), koska sen pääasiallinen käyttö on sisäinen www−palvelu
  - 10−verkon osoitteet eivät ole tiedossa julkisenverkon puolella






# Julkisesta verkosta lokaaliin verkkoon ?

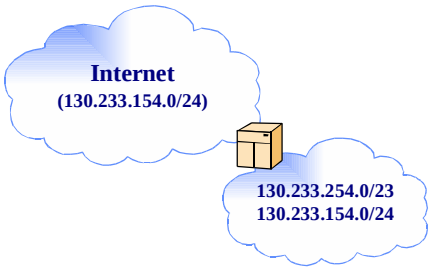
- **Ratkaisu:**
  - Käytetään **nimipalvelua** hyväksi
  - Operoidaan täydellisillä piirinimillä
    - Nimeen liitetään julkisenverkon NAT−osoite (staattinen tai dynaaminen)
    - Käytetään DNS−ALGtä luomaan tarvittavat tilakoneet






# Kaksinkertainen NAT

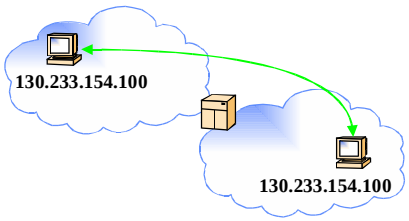
- **Esimerkki:**
  - Organisaatiolla
    - Oli aiemmin 256−osoitteen lohko (130.233.154.0)
    - Vaihtoivat 512−osoitteeseen (130.233.254.0/23)
    - Sisäisesti säilytettiin vanha osoiteavaruus.
  - Operaattori
    - Jakoi luovutetun 256−osoitteen lohkon uudelle käyttäjälle





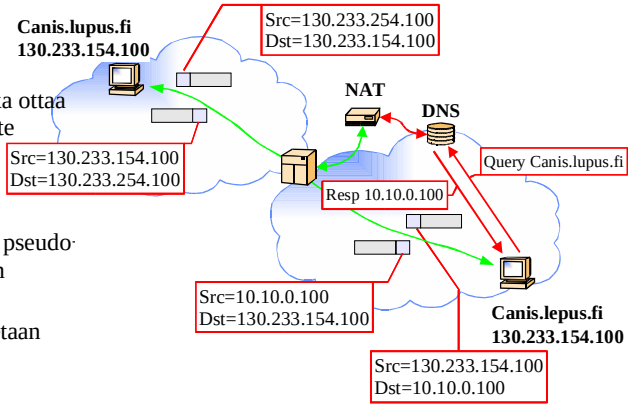

# Kaksinkertainen NAT

- **Ongelma:**
  - Kuinka kaksi konetta voivat kommunikoida keskenään, kun niillä on konfliktoivat osoitteet (tarkoituksella)



# Kaksinkertainen NAT

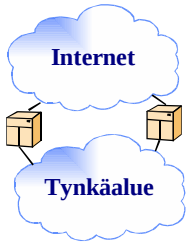
- **Ratkaisu:**
  - Operoidaan piirinimillä
  - Tarvitaan DNS−ALG, joka ottaa huomioon onko haettu laite julkisessa vai lokaalissa versiossa osoiteavaruutta
    - Mikäli ulkoisessa avaruudessa annetaan pseudo-osoite, joka muutetaan NAT:ssa todelliseksi
    - Mikäli sisäisessä annetaan sisäinen osoite






# Monikotisuus

- Periaatteessa NAT on tarkoitettu tynkäalueisiin, eli on vain yksi liityntä ulkomaailmaan
  - Vikaantumisriski on suuri
- Monikotisuudella saavutetaan varmuutta mutta toisaalta tarvittava logiikka kasvaa
  - Kuinka taata, että kaikki yhteyden paketit kulkevat yksittäisen NATin kautta
    - TCPn tilakone sekoaa, jos paketteja puuttuu runsaasti
  - Kuinka NATien välinen konfiguraatio pysyy hallinnassa
    - Samoja osoitteita ei jaeta useammassa paikassa kerrallaan

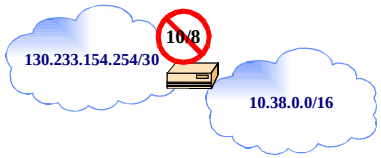





# Porttitason NAT

- Porttitason NATissa useat päätelaitteet jakavat saman globaalin IP−osoitteen
- Hyödynnetään porttinumeroita asiakkaiden erottelussa
- Vaarana **ylivuoto**
- **Esimerkki:**
  - Julkisia osoitteita on 255 kpl
  - Lokaaleja osoitteita on 1000 kpl
  - Liikenteestä 50 % suuntautuu ulos

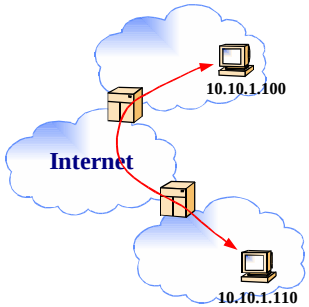
```
B    130.233.154.250:8080 <−> 10.38.0.3:80
25   130.233.154.250:4434 <−> 10.38.100.1:143
B    130.233.154.251:5000 <−> 10.38.0.60:123
B    130.233.154.252:4400 <−> 10.38.8.60:600
5    130.233.154.253:2500 <−> 10.38.11.60:20
B    130.233.154.254:8000 <−> 10.38.0.100:22
```





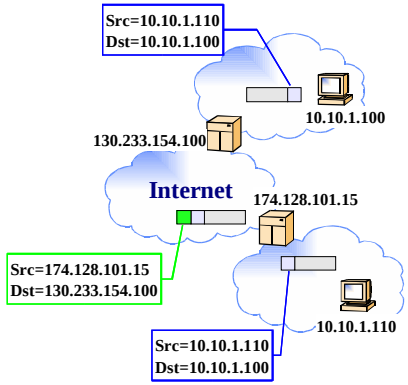

# Jaettu tynkäalue

- Tynkäalue voi olla myös paloiteltu useampaan osaan eri puolille operaattorin verkkoa
- Näiden yhdistämiseen tarvitaan
  - Vuokrajohtoa (ei eleganttia)
  - VPN (usein turhaan)
  - Kaksinkertainen NAT (turhan hankalaa)
  - **Tunnelointia**



# Tunnelointi

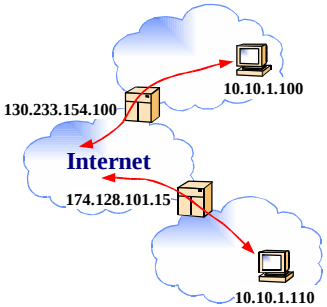
- Tunneloinnissa IP−paketti välitetään toisen paketin hyötykuormana
- Tunnelilla on määrätyt päätepisteet
  - Alku, jossa kehystetään
  - Loppu, jossa puretaan
- Kehystyksessä
  - Voidaan kopioida alkuperäisen paketin välitystietoja, jos halutaan vaikuttaa paketin välitykseen julkisessa verkossa (ToS −kenttä)






# Entäpä tästä Internettiin

- Kommunikointi Internettiin
  - Kaksi erillistä NATtia
    - Kaksi erillistä julkista osoiteavaruutta
  - Yksi NAT
    - Yksi julkinen osoiteavaruus
    - Yksi asiakasosoite (tunnelin toinen pää)






# Ongelmia

- Edellyttää harvaa liikennematriisia
  - Vain pieni osajoukko päätelaitteista kommunikoi tynkäalueen ulkopuolle tai ulkopuolelta kommunikoidaan pieneen osaan tynkäalueen päätelaitteista
  - Muuten hyöty pienenee
    - Osoitteiden uudelleen käytettävyydessä
    - Prosessoinnin raskaudessa
- Lisää riskiä globaalisti vääriin osoitekonfiguraatioihin
- Pienentää tiettyjen sovellusten kapasiteettia (ftp, http jne)
- Piilottaa loppukäyttäjän identiteetin
- Monimutkaistaa nimipalvelua
- Ei sovi IPSecin kanssa
  - IPSecissä hyödynnetään osoitteita, joten osoitemuutos johtaa salausavaimen korruptoitumiseen