S−38.192 Verkkopalvelujen tuotanto

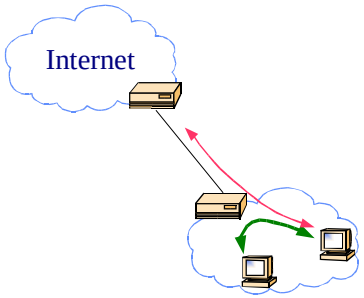
Luento 4: Verkko−osoitteiden manipulaatiopalvelut

Osoitemanipulaation syitä

- **Verkossa käytetään lokaaleja IP−osoitteita.**
  - Osoitteita, jotka on tarkoitettu testi− sekä sisäiseen käyttöön:
    - 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)

Miten ?

- Hyödynnetään 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



Pääosa liikenteestä on paikallista −> pätee suurelta osin yritysten lähiverkkoihin

Vaihtoehtoja

Network Address Translation (NAT)

- Yhdyskäytävä suorittaa jokaiselle IP−paketille IP−otsikon osoitteen muunnoksen
  - IP−otsikon muunnos
  - Siirto−otsikon muunnos
    - TCP−pseudo−otsikko
  - Sovellustason muunnos

Realm Specific IP (RSIP)

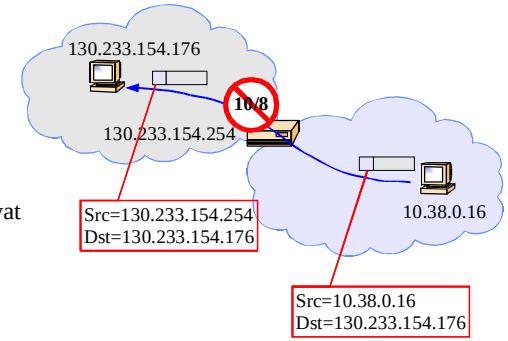
- Yhdyskäytävä luovuttaa päätelaitteelle julkisen osoitteen rajalliseksi ajaksi (vertaa DHCP)
- Informaatio tunneloidaan paikallisessa alueessa yhdyskäytävälle, joka välittää varsinaisen paketin julkiseen verkkoon

Network Address Translation

- NATin toiminta on kuvattu pääpiirteissään seuraavissa RFC:ssä:
  - RFC2663: IP Network Address Translator (NAT) Terminology and Considerations
  - RFC3022: Traditional IP Network Address Translator (Traditional NAT)
  - RFC2766: Network Address Translation − Protocol Translation (NAT−PT)
  - RFC2694: DNS extensions to Network Address Translators (DNS_ALG)
  - RFC2709: Security Model with Tunnel−mode IPsec for NAT Domains
  - RFC2993: Architectural Implications of NAT
  - RFC3235: Network Address Translator (NAT)−Friendly Application Design Guidelines

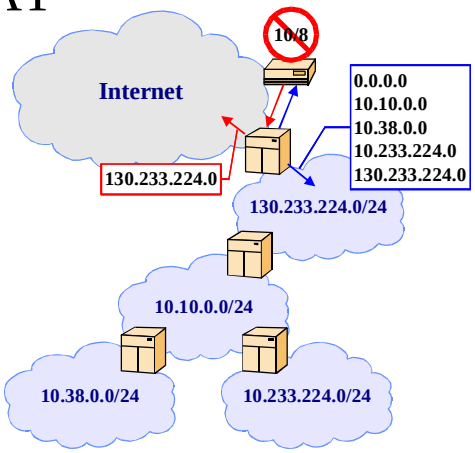
Network Address Translation

- **NATin tehtävä** on muuntaa IP−pakettien osoitekenttien sisältöä niiden kulkiessa kahden osoitereaalisaation välillä, joihin NAT on yhteydessä.
  - Periaatessa: yksinkertainen
  - Teknisesti: toimintaan liittyy useita vaiheita jotka aiheuttavat ongelmia



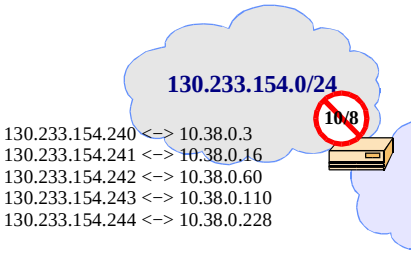
NAT

- NAT tarjoaa yhdyskäytäväpalvelua kahden osoitereaalisaation välillä
  - NAT **ei** ole itsessään 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

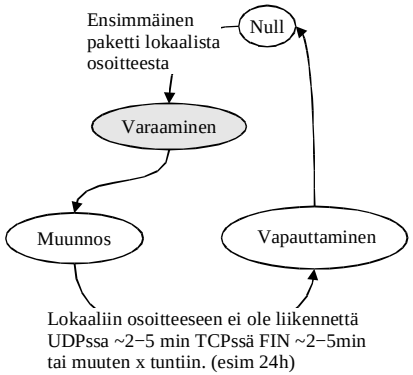
- **Staattinen NAT**
  - Niille päätelaitteille, joilla on 'jatkuva' tarve kommunikoida muun maailman kanssa tehdään staattinen kuvaus



- **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 <−>

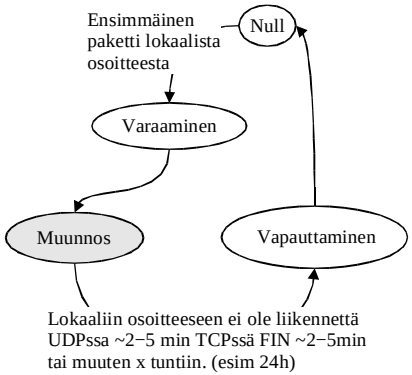
Dynaaminen NAT – toiminta



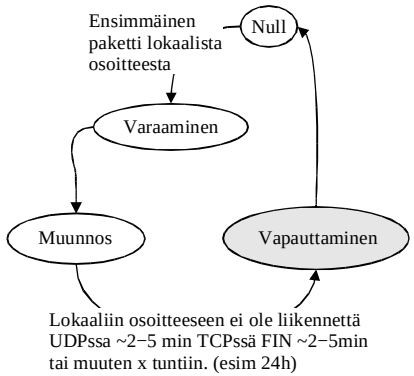
- Tilakoneella on kolme tilaa
  - **Osoitteen varaaminen**
    - Lokaalin verkon päätelaite aloittaa kommunikaation NATin kautta tai ulkoapäin halutaan kommunikoida lokaalin verkon päätelaitteelle.
    - Globaali osoite liitetään lokaaliin osoitteeseen, jonka jälkeen kaikki ’yhteydet’ kyseisestä lokaalista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

Dynaaminen NAT – toiminta

- **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)



Dynaaminen NAT – toiminta

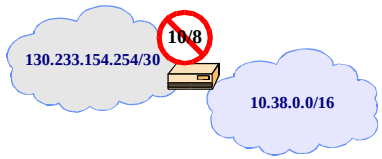


- **Osoitteen vapauttaminen**
  - Lokaalin päätelaitteen kommunikaatio globaaliin verkkoon on päättynyt eikä globaalia osoitetta enää tarvitse varata sen käyttöön.
    - Viimeisellä TCP−yhteydellä on tullut FIN ja siihen liittyvä kuittaus
    - Paketteja ei ole liikkunut 5 minuuttiin
    - Avoimella TCP−yhteydellä ei ole toimintaa *x* tuntiin

Porttitason NAT (NAPT)

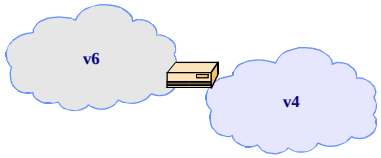
- **NAPT ? NAT−PT**
- NAPTissa useat päätelaitteet jakavat saman globaalin IP−osoitteen
- Hyödynnetään porttinumeroita asiakkaiden erottelussa
- Vaarana **ylivuoto**
- **Esimerkki:**
  - Julkisia osoitteita on 255 kpl
  - Lokaaleja osoitteita on 1000 kpl
  - Liikenteestä 50 % suuntautuu ulos

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



Protokolla NAT (NAT−PT)

- Protokolla NAT vastaa perinteistä NATia mutta suorittaa osoitemuunnoksen protokollatasolla
  - IPv4 <−> IPv6
- Lähtökohtaisesti IPv4 osoitteita on varattu joukko IPv6 verkon käyttöön
- Kaksi varianttia, kuten normaalissa NATissa
  - NAT−PT
  - NAPT−PT
- NAT−PT on viimeinen keino saada yhdysliikenne toimimaan
  - Suositeltava ratkaisu päätelaitteiden kaksoispinot
    - Tunnelointi
    - Protkolla riippuvat VLAN−verkot



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
    - Perinteinen päästä päähän integriteetti katoaa
- **Vaikutus**
  - Mikäli osoite on koodattu numeroina voi paketin pituus muuttua

```
(10.38.0.16 <−> 130.233.154.242)
```

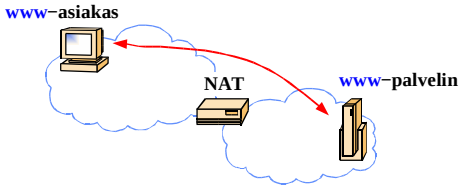
    - TCPn tarkistussumma vaatii muutoksen
- TCPn järjestysnumero (sequence number)ja kuittausnumero (acknowledge number) vaativat muutokset.
- Tarvitaan erillinen tilakone huolehtimaan lähtevien pakettien ja vastaanotettujen kuittausten välisestä sidonnaisuudesta

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

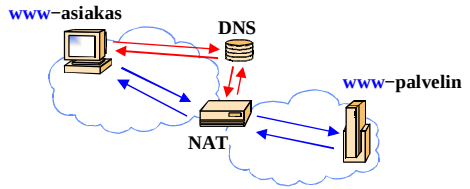
Julkisesta verkosta lokaaliin verkkoon ?

- **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



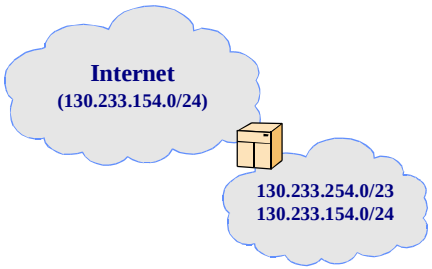
Julkisesta verkosta lokaaliin verkkoon ?

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



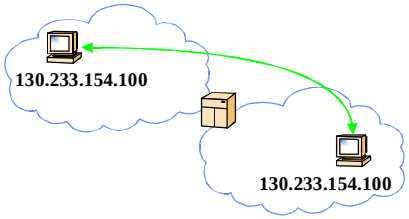
Kaksinkertainen NAT

- **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



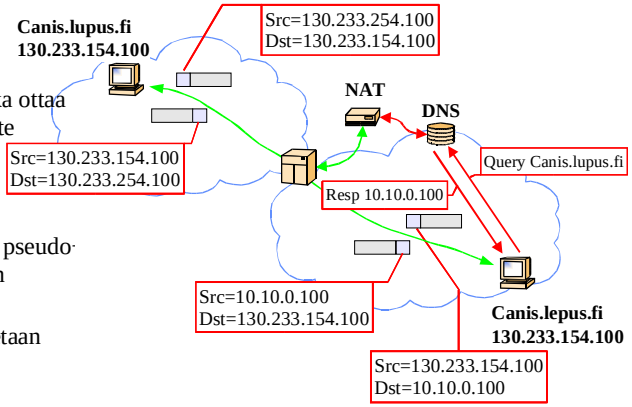
Kaksinkertainen NAT

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



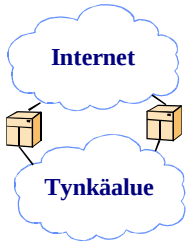
Kaksinkertainen NAT

- **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



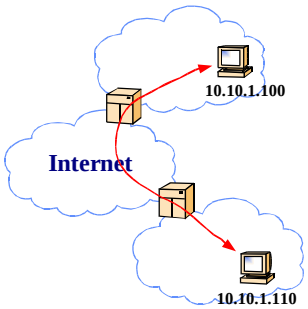
Monikotisuus

- 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



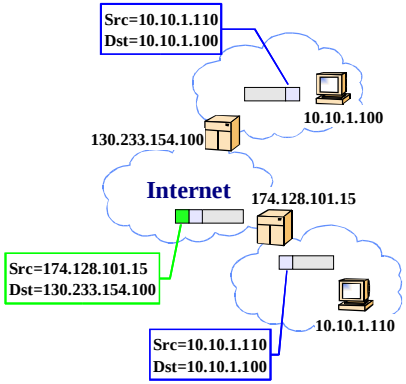
Jaettu tynkäalue

- 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**



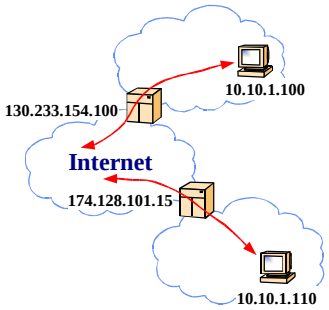
Tunnelointi

- 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)



NATin 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

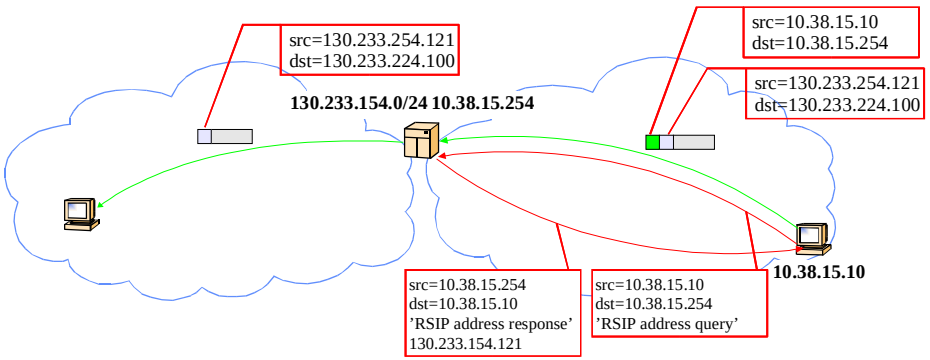
Realm Specific IP

- RSIP on määritelty seuraavissa RFC:ssä:
  - RFC3102: Realm Specific IP: Framework
  - RFC 3103: Realm Specific IP: Protocol Specification
  - RFC3104: RSIP Support for End−to−end IPsec
  - RFC3105: Finding an RSIP Server with SLP

Realm Specific IP

- **RSIP on tarkoitettu** korvaamaan NATin käyttö siellä missä se on mahdollista
- RSIP **ei** riko päästä päähän integriteettiä
- RSIP **vaatii** päätelaitteisiin muutoksia
- Komponentit
  - RSIP palvelin
    - Hallinnoi julkisia osoitteita
  - RSIP yhdyskäytävä
    - Yhdyskäytävä, joka toimii RSIP−tunnelin päätepisteenä
  - RSIP asiakas
    - Tarjoa sovellukselle läpinäkyvän yhteyden julkiseen verkkoon palvelimelta saamalla osoiteella

RSIP – toiminta



RSIP

- Toiminta muistuttaa DHCP:n toimintaa
  - **DHCP**: Haetaan koneelle IP−osoite
  - **RSIP**: Haetaan koneelle IP−osoite, jota käytetään kommunikointiin julkiseen verkkoon
  - IP−osoitteella on *elinaika*, jonka jälkeen varaus täytyy vahvistaa uudelleen
- RSIP voi perustua myös porttitason toimintaan
  - Yhdyskäytävän täytyy pitää kirjaa kenelle (mille lokaalille osoitteelle) tunneloidaan mikäkin paketti samasta julkisesta osoitteesta
- RSIP voi perustua myös muihin kanavointi kriteereihin
  - IPSec !!!

Kommunikointi julkisesta verkosta ?

- RSIP voidaan yhdistää DNS:n kanssa kuten NAT
  - Piirinimen haku liittää julkisen osoitteen käyttöön. Kyseinen liitos informoidaan lokaalin verkon päätelaitteelle
    - Raskas prosessi
    - Haku ei välttämättä johda liikenteeseen
    - Porttitason toiminnassa ???
- RSIP ei ole primäärinen ratkaisu julkisten palveluiden toteuttamiselle

IPv6 <−> IPv4

- RSIP tarjoaa joustavan menetelmän lokaalin verkon siirtymiselle IPv6:n käyttöön
  - Julkiseen verkkoon kulkevat paketit tunneloidaan lokaalissa verkossa
- Päätelaitteelta edellytetään kahta protokollapinoa
  - Oletusarvo nykyisissä TCP/IP ohjelmistoissa

RSIP ongelmia

- Suurin yksittäinen ongelma
  - VAATII TUKEA PÄÄTELAITTEELTA
    - Useita, vastaanottaja riippuvaisia, IP−osoitteita
    - Tunnelointi
- Muita ongelmia
  - Levitys− ja jakeluliikenteen toteuttaminen