# S−38.191 Televerkot yrityksissä

Luento 5: AAA



# Ideologia

- Internet palveluista muodostuu yksi suuri kauppapaikka.
- Yksittäinen käyttäjä ’ostaa’ palveluita verkolta standardoiduilla menetelmillä
- Tarkoituksena on mahdollistaa joustava, tarvepohjainen resurssien käyttö (varaus)
- Pyrkimykset
  - Ongelmakohtaiset
    - PPP−linkeillä (PAP, CHAP, EAP)
    - Geneerisesti (RADIUS)
    - Profiilitietojen käsittely (COPS)



# Mikä

- **AAA**
  - **A**AA: **Authentication**
    - Tunnistaminen/varmentaminen
    - Käyttäjän tunnistaminen jollain haastemenetelmällä
  - A**A**A: **Authorization**
    - Valtuuttaminen
    - Määritellään resurssit ja menetelmät, joita käyttäjällä on oikeus/velvollisuus käyttää
  - AA**A**: **Accounting**
    - Laskutus
  - ***Lyhyesti:***
    - ***AAA käsittää kaikki ne menetelmät ja tiedot, joita tarvitaan yksittäisen asiakkaan tunnistamiseen, palvelemiseen ja laskuttamiseen ennaltasovitun palvelusopimuksen puitteissa***



# Vaihe 1: Tunnistus

- Operaattorin kannalta on neljänlaisia tilaajia
  - **Kiinteä yritystilaaja**
    - Kiinteä yhteys, jonka takana on useita IP−osoitteita ja käyttäjiä
    - Oikeutus verkon käyttöön tapahtuu IP−osoitteen perusteella
  - **Valinnainen yritystilaaja**
    - Valinnainen yhteys, jonka takana on yksi tai useampi käyttäjä
    - Oikeutus verkon käyttöön perustuu A−tilaajan numeron tunnistamiseen, IP−osoitteeseen ja/tai salasanaan

# Vaihe 1: Tunnistus

- **Kiinteä kotitilaaja**
  - Kiinteäyhteys, jonka takana on yksi tai muutamia käyttäjiä
  - Oikeutus verkon käyttöön perustuu IP−osoitteeseen ja/tai salasanaan
- **Valinnainen kotitilaaja**
  - Valinnainen yhteys, jonka takana on yksi tai muutamia käyttäjiä
  - Oikeutus verkon käyttöön perustuu salasanaan



# Tunnistus

- IP−osoitteeseen perustuva
  - Kiinteillä tilaajayhteyksillä asiakkaalle on annettu tietty IP−osoitelohko.
  - Mikäli paketeissa on lähettäjänä ko lohkon osoite, välitetään ne eteenpäin
  - Jos lähettäjä on joku muu osoite, poistaa tilaajareititin paketit
  - Tarjoaa staattisen sidoksen tilaajan, tilaajaliittymän ja palveluprofiilin välille
- A−tilaajan tunnistus
  - Valinnaisilla tilaajayhteyksillä, joissa asiakkaana on yritys, jolle on annettu tietty IP−osoitelohko
  - Asiakkaan reititin tekee valinnaisen yhteyden verkkopalvelua tarjoavan operaattorin verkon tilaajapalvelimeen.
  - Tilaajapalvelin tunnistaa käyttäjän puhelinnumeron perusteella



# Tunnistus

- Tunnus/Salasana
  - Yksinkertaisin mekanismi liikkuvien asiakkaiden sekä valinnaisten tilaajayhteyksien yli toimivien asiakkaiden kanssa
  - Verkkotunnus (*n*−merkkiä)
  - Salasana (*m*−merkkiä)
  - Tunnus/salasana −yhdistelmä yksilöi käyttäjän ja mahdollistaa muut tilaajatoiminteet
- Haaste
  - Perustuu asiakkaalle esitettyyn haasteeseen
  - Haaste pohjautuu operaattorin tietoon asiakkaan kyvyistä vastata haasteeseen
    - Vertaa pankkiavaimet
  - Haaste esitetään yleensä primäärisen tunnistamisen jälkeen
    - Vaatii tiedon vastaajan kyvyistä



# Vaihe 2: Valtuutus

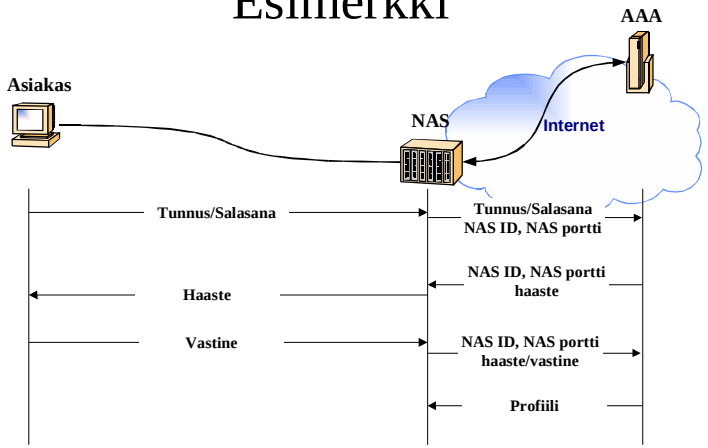
- Valtuutus määrittelee palvelun, joka asiakkaalle tarjotaan
  - Äärimmillään määritelmä voi kieltää kaiken palvelun
- Määritelmä perustuu
  - Tunnistuksen tietoihin
  - Kredentiaaliin
  - Järjestelmän tilaan
  - Hallinnollisiin rajoitteisiin
    - Asiakkaan sijainti
    - Kellon aika
    - Yhtäaikaisten sessioiden määrä (reiluus)
- Palvelun määrittely on käytännössä
  - IP−osoite
  - Oletusreitit
  - NAS suodattimet (IP−osoitteille TCP−porteille)
  - QoS riippuvat asetukset (DiffServ parametrit)
  - Tunnelointitiedot
  - Salaustiedot (IPSec)

# Vaihe 3: Laskutus

- Laskutuksella tarkoitetaan lähinnä laskutuksessa käytettävien resurssitietojen keruuta.
- Tosin näitä tietoja voidaan käyttää myös muihin tarkoituksiin
  - Verkon mitoituksen lähtötietoina
  - Verkon ylläpidon referenssitietoina
- Joskus puhutaan myös seurannasta (auditing), jolla tarkoitetaan käyttäjien aktiviteetin seurantaa (käyttötietojen keruuta)
- Ero laskutukseen on lähinnä katsantokanta
  - Resurssitiedot (kuinka paljon mitäkin verkon resurssia kulutetaan ja kenen toimesta)
  - Käyttötiedot (minne kukin kommunikoi ja millä protokollalla)



# Esimerkki






# Olemassa olevaa

- **R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice
  - Yksinkertainen AAA ratkaisu
  - Alunperin valinnaisten asiakasyhteyksien varmennettuun tunnistamiseen tarkoitettu
  - Ei skaalaudu
    - Nykyisille käyttäjämäärille
    - Nykyisten verkkojen kokoon
- **Diameter**
  - ~RADIUS
    - Poistettu skaalautuvuusongelmat
    - Lisätty laajennukset
      - Liikkuville asiakkaille
        - » Mobile IP
        - » Roaming
      - Monipuolisemmille NAS−optioille



# Yleisemmin

- Mistä puhumme ?
  - Erillaisten verkkopäätelaitteiden kautta kommunikoivien käyttäjien tunnistamisesta sekä heidän palvelusopimustensa täyttämisestä
- IETF
  - AAA
  - Policy Framework
- Internet2
  - Qbone
- DMTF
  - DEN & CIM
- ITU
  - 3G

# Vaatimukset

- Palvelut
  - Asiakkaille myytävät
  - Verkkopalvelut
- Operaattorin ja asiakkaan väliset sopimukset
  - Service Level Agreement (SLA)
- Verkon tila
  - Käyttöaste
  - Palveluiden välinen käyttöaste
- Asiakkaiden tila
  - Lokaali / roaming
- Miten asettuu
  - Tietovarannot
    - Asiakastiedot
    - Laitetiedot
    - Palvelutiedot
    - Liikennetiedot



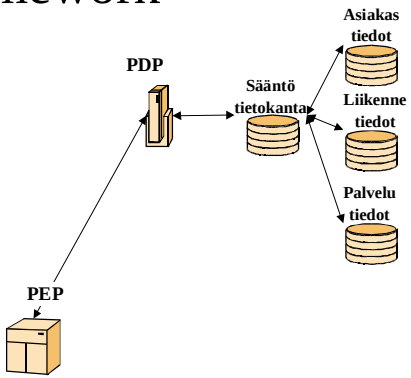
# AAA & Policy Framework

- Kaikenlainen asiakaskohtainen palvelu vaatii aina asiakkaan tunnistamista.
  - Kiinteillä yhteyksillä triviaalia
  - Liikkuvilla vaatii enemmän
    - 3G
    - Kotisoitto
- AAA tarjoaa itsessään mekanismit tunnistamiseen
  - Haaste ja kredentiaalimenetelmät
- Policy Framework
  - Tarjoaa mekanismit hallita kokonaisuudessaan erillaisia tietoelementtejä, jotka vaikuttavat tarjottuun palveluun
  - Tunnitustietojen perusteella muodostetaan valtuutus eli erillaisten sääntöjen ja ohjeiden kokoelma, jotka siirretään asiakkaan sen hetkiseen liitäntäpisteeseen.



# Policy Framework

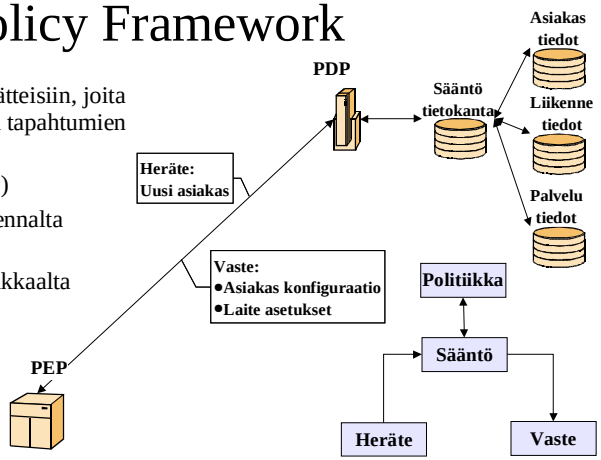
- Ajatuksena
  - Palvelutietojen välitys
    - Päätöspisteestä (PDP)
      - Tarvitaan tietoa
        - » Asiakkaasta
        - » Palvelurakenteesta
        - » Verkon kuormituksesta
    - Suorituspisteeseen (PEP)





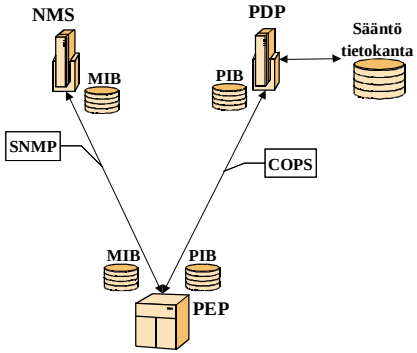

# Policy Framework

- Toiminta perustuu herätteisiin, joita PEP generoi erillaisten tapahtumien pohjalta
  - Uusi asiakas (NAS)
  - Kuormitus ylittää ennalta asetetun rajan
  - RSVP sanoma asiakkaalta



# Policy Framework

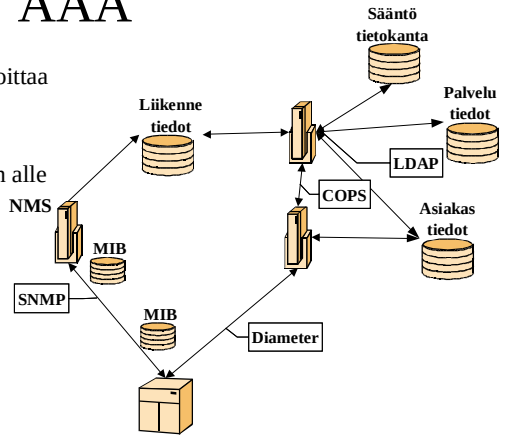
- PDP ja PEP kommunikoivat keskenään käyttäen erillistä protokollaa **C**ommon **O**pen **P**olicy **S**ervice
- COPS hyödyntää PEPn ja PDPn välisessä kommunikaatiossa SNMPn MIBien kaltaista **P**olicy **I**nformation **B**ase tietokantaa.
- PIBin sisältö riippuu **laitteesta**, jonka tarjoamia palveluja konfiguroidaan (aivan kuten MIBin sisältö)





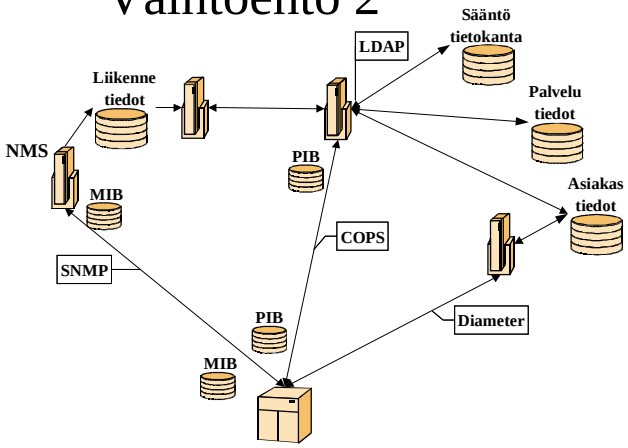

# AAA

- AAAn ja PFn yhteenliitos sekoittaa hieman kuviota
- Kaksi vaihtoehtoa
  - Kaikki integroidaan AAAn alle
  - PF toimii AAAn kautta





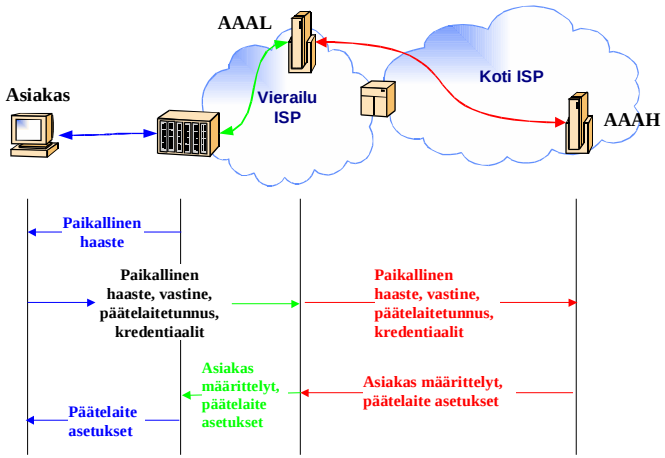

# Vaihtoehto 2





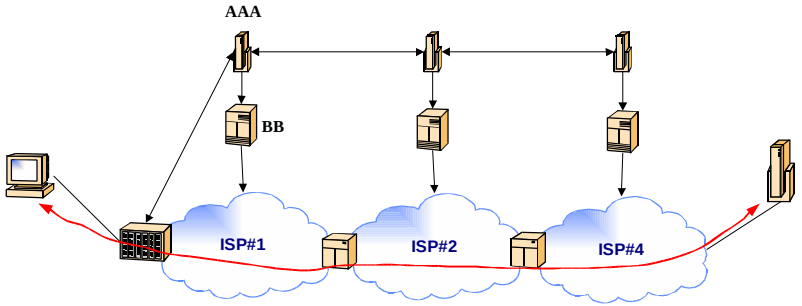

# AAA

- Kaikki toimii hienosti yhden operaattorin alueella
- Miten roaming eli vierailut toisen operaattorin alueelle ?
  - Tarvitaan protokolla, joka kommunikoi useiden AAA palvelimien kesken
    - Diameter ?
- Miten yhteydet, jotka kulkevat usean operaattorin alueen yli mutta tarvitsevat, joitain erityisiä palveluparametreja ?
  - Tarvitaan protokolla, joka siirtää palvelutiedot alueelta toiselle
  - Tarvitaan alueiden sisällä palveluprofiilien manipulointia
    - Resurssien varaus
    - Suodattimet
    - Reititys






# Kauhukuva tulevaisuudesta






# Yhteenveto

- AAA on osa laajaa kokonaisuutta, jolla pyritään mahdollistamaan erillaiset palveluprofiilit per asiakas sekä asiakkaiden liikkuvuus.
- Taustalla on varma tunnistus ja siihen pohjautuva asiakastietojen hyödyntäminen
- Tehtävään liittyy monia rinnakkaisia protokollia sekä rinnakkaisia arkkitehtuureja
- AAA ei ole läheskään valmis. Se toimii yhden alueen sisällä mutta laajempi toiminta on vielä alkutekijöissä.