Verkkoliikenteen rajoittaminen

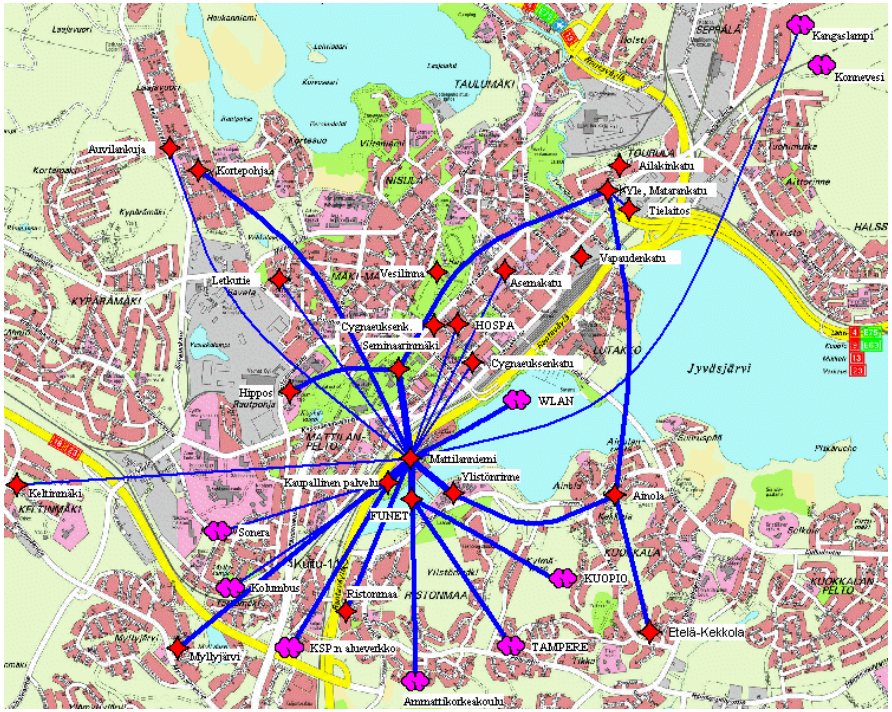
Miska Sulander
Jyväskylän yliopisto
Atk-keskus

Agenda

1. Jyväskylän yliopistoverkko
2. Verkon käytöstä
3. Verkkoliikenteestä
4. Käytön jakautuminen
5. Liikennemäärien hallinta
6. Rajoitusmenetelmät
7. JYU liikennerajoitukset
8. Toteutus
9. Kokemukset
10. Haasteet
11. Tulevaisuuden näkymiä

Jyväskylän yliopistoverkko

- Yliopiston verkko
  - Käyttäjämäärä: n. 30 000 – 40 000 käyttäjää
  - Päätelaitteita: n. 13 000 kpl
- Verkon palvelut
  - Verkkoliittymät ja -palvelut yliopiston tiloissa



  - Etäyhteydet: ADSL, kaapelimodeemi, WLAN, soittosarjat
- Tulevaa
  - v. 2004 aloitetaan siirtyminen QoS-palveluihin ja 802.1x käyttäjätunnistukseen
  - Valmistaudutaan dynaamisiin verkkopalveluihin (käyttäjäkohtaiset profiilit ym.)

Opiskelijaverkot yliopiston verkossa

- JYY (Jyväskylän yliopiston ylioppilaskunta)
  - 2 verkotettua aluekokonaisuutta
  - 1400 liittymää
- KOAS (Keski-suomen opiskelija-asuntosäätiö)
  - 20 kohdetta verkotettuna
  - 2300 liittymää
- 90-luvun alussa nähtävissä työasemien määrän merkittävä kasvutarve yliopistolla. Haluna:
  - Vähentää työasemien tarvetta yliopistolla, sekä samalla saadaan tilasäästöjä.
  - Parantaa opiskelumahdollisuuksia ja nostaa myös asuntojen arvoa. Välimatkojen merkitys vähenee.

Verkon käytöstä

- Verkkoon siirtyvät kaikki nykyiset IT-palvelut. Verkko on tärkein yksittäinen tekijä palveluinfrassa.
- Tärkeää tarjota verkkoinfra ja mahdollistaa eri palveluiden käyttö, ei tehdä valintaa käyttäjän puolesta mikä on tarpeellista ja mikä ei.
- Käyttö lisääntyy ja monipuolistuu jatkuvasti. Siten myös liikennemäärät ja vaatimukset kasvavat.
  - Reaaliaikaiset sovellukset (VoIP, videoneuvottelu,..): QoS
  - Käyttäjäkohtaiset profiilit ja dynaaminen toiminta
  - Tietoturva ja suojaus jo verkon reunalla, käyttäjäkohtaisesti (verkon keskitetty palomuuri ei vastaa vaatimuksiin)
- Toimintatarve jo nyt 24h/7

Verkkoliikenteestä

- Perinteisten sovellusten (www, ftp, news) osuus kokonaisliikenteestä nykyisin olematonta.
- Pääosa liikenteestä uuden sukupolven palveluita, kuten:
  - Virtuaalisesti hajautetut palvelut (levytila, varmuuskopiot,..)
  - Multimedia (video, voice, streaming)
  - P2P-verkot
- Nämä palvelut vaativat verkolta:
  - Nopeutta (>10Mbps), laatua (viive, jitter) ja toimintavarmuutta

Käytön jakautuminen

- Verkon käyttö painottuu yhä enemmän eri viihdepalveluiden käyttöön
  - mp3-musiikki, elokuvat, verkkopelit, live-feed
- Käytön jakautuminen yleisesti:
  - 10-12% käyttäjistä aiheuttaa 58-95% kokonaisliikenteestä
  - 2% käyttäjistä aiheuttaa 22-33% kokonaisliikenteestä
- Suurin osa käyttäjistä (80-90%) käyttää verkkoa vähäisesti.

Liikennemäärien hallinta

- Hallintamenetelmiin liittyviä ongelmia
  - Palvelut käyttävät yhä useammin dynaamisia portteja, ts. palvelu on tunnistettavissa vain tutkimalla liikenteen sisältöä.
  - Liikenne muuttumassa salatuksi -> haittaliikenteen tunnistaminen ja erottaminen muusta liikenteestä mahdotonta.
  - Vaatimukset verkolle lisääntyvät: nopeus, viive, laatu. Menetelmien oltava mahd. tehokkaita ja läpinäkyviä käytölle.
  - Myös IPv6 tuloillaan..
- Liikenne- ja käyttäjämäärät suuria
  - Liikenteen kustannustehokas hallinta on tällä hetkellä haaste
    - Tehokkaat kaupalliset järjestelmät kalliita. Ongelmana myös skaalautuminen tuleviin tarpeisiin, esim. laskutus, seuranta, QoS, multicast, anycast jne.
  - DoS-hyökkäyksistä toipuminen

Rajoitusmenetelmät

I. Palvelurajoitukset
   - Portti- ja palveluestot (verkkokerroksen l4-l7 tasot) ennalta määrätyille sovelluksille

II. Liikenteen luokittelu (QoS-tekniikat)
   - Luokitellaan ja priorisoidaan ennalta määritelty liikenne/sovellukset
   - Voidaan hallita myös yksittäisiä liikennevirtoja (microflow policing)
   - Ei ole oikeudenmukainen

III. Verkkokiintiö
   - Kaikki palvelut käyttäjien käytettävissä

IV. NAT (Network Address Translation)

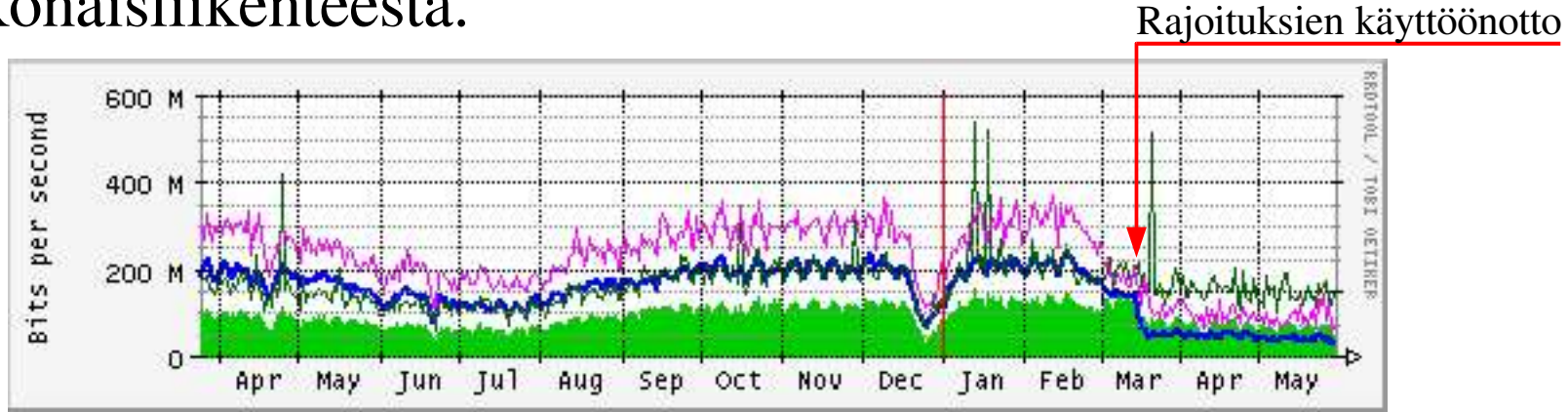
V. Kombinaatio eri menetelmistä

JYU liikennerajoitukset

- Rajoitukset tällä hetkellä:
  - Käyttäjäkohtainen verkkokiintiö: 1 GB/ 24h (in+out)
  - Käyttö täysin vapaata:
    - Opiskelijaverkkojen sisällä,
    - yliopiston verkkoon ja
    - muihin FUNET-verkkoihin
- Kiintiö ei rajoita normaalia verkkokäyttöä millään tavalla.
- Kiintiön ylittäneet käyttäjät joutuvat yhteiselle 5 Mbps kaistalle (in+out) -> merkittävä vaikutus käytettävään nopeuteen.
- Opiskelijaverkkojen sisäistä liikennettä tai liikennettä yliopiston verkkoon ei ole rajoitettu ollenkaan. Liittymänopeus nyt 10 Mbps, tulevaisuudessa 100 Mbps.

Liikennerajoituksien tulokset

- Ennen rajoituksia:
  - n. 12% “hyödyllistä” liikennettä (www,ftp,ssh,irc,..)
  - 88% P2P- ja muuta liikennettä (kazaa, mutella, gnutella,..)
- Rajoituksien jälkeen:
  - n. 25% “hyödyllistä” liikennettä
  - 75% P2P- ja muuta liikennettä
  - Kokonaisliikennemäärä vähentynyt lähes 50%!
- Arviolta 4-5% käyttäjistä käyttänyt lähes 40% kokonaisliikenteestä.

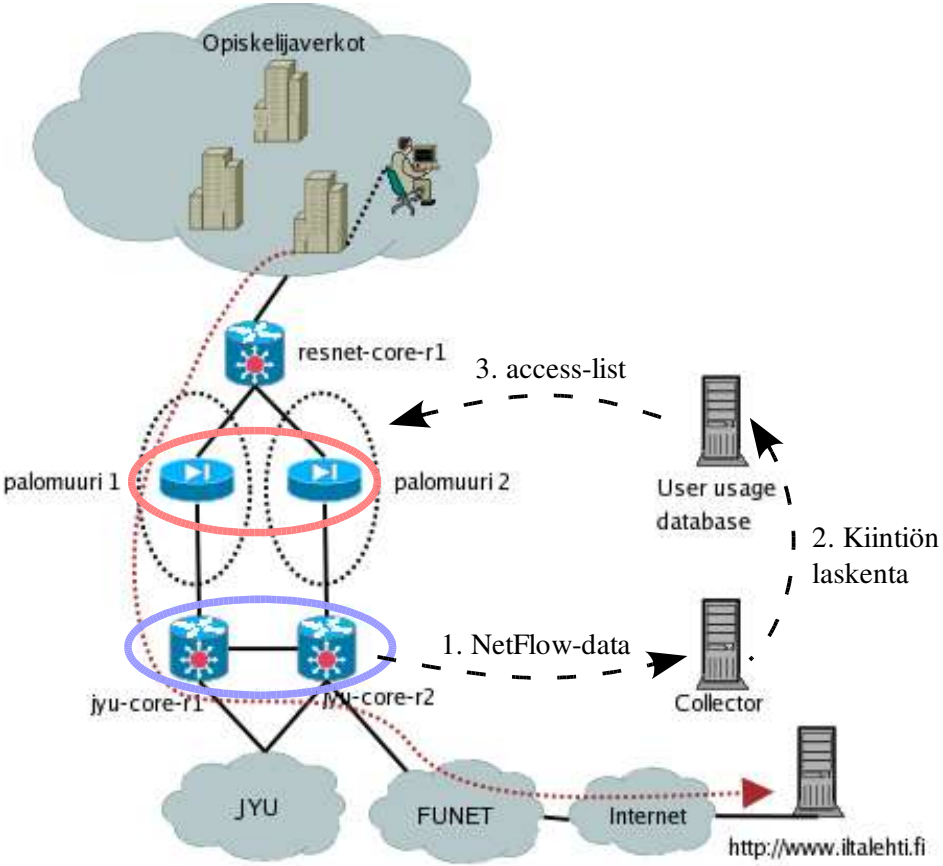


Toteutus 1/2

- Käytetään standardiin perustuvaa NetFlow:ta liikennemäärien seurantaan. Liikennedata saadaan runkolaitteista (L4-tasolla).
- Liikennetilastoista generoidaan käyttäjäkohtaiset tilastot kiintiöitä varten.
- Linux-pohjaisia palomuureja käytetään pakettien merkitsemiseen (DSCP-kenttä), sekä nimipalvelusta generoidulla access-listalla määritellään sallitut käyttäjät.
- Runkoverkon laitteet rajoittavat kiintiönsä ylittäneiden käyttäjien nopeuden yhteiselle 5 Mbps kaistalle.
- Menetelmä käytössä tällä hetkellä vain opiskelijaverkoille, halutessa samalla järjestelmällä voidaan hallita koko yliopiston liikennettä, myös sisäistä.

Toteutus 2/2

1. NetFlow-data saadaan runkoreitittimistä.
2. Käyttäjäkohtaiset (IP-numero) tilastot siirretään tietokantaan ja lasketaan 24h käyttömäärä.
3. Generoidaan access-lista, jossa määritellään sallitut käyttäjät ja kiintiön ylittäneet.
4. Linux-palomuurit merkkaavat (DSCP) ylittäneiden paketit.
5. Runkoreitittimet sääntelevät kiintiön ylittäneiden liikenteen.



Kokemukset

- Palaute käyttöönoton jälkeen:
  - Liikenteen luokitteluun (QoS-tekniikka) pohjautuva
    - Epäoikeudenmukainen käyttäjiä kohtaan
    - Muiden kuin priorisoitujen sovellusten toiminta varsin heikkotasoista
  - Verkkokiintiöön pohjautuva
    - Selvästi suurin osa käyttäjistä tyytyväisiä nykyiseen järjestelyyn. Nykyiset kiintiörajat vaikuttavat sopivilta.
- Käyttäjät voivat seurata omaa kiintiötä lähes reaaliaikaisesti.
- Järjestelmä toiminut moitteettomasti käyttöönoton jälkeen.
- Nykyisellään järjestelmä kykenee 2x 400-500 Mbps liikennemäärän käsittelyyn. Skaalautuu helposti paljon suurempiin liikennemääriin.

Haasteet

- Verkon liikennemäärien hallinta
  - Jatkuvan kasvun kustannukset
    - Liikennemäärän aiheuttamat suorat kulut
    - Uusien verkkolaitteiden investoinnit
    - Käytön hallinta ja valvonta (investointi ja työkulut)
  - Käyttö on saatava hallituksi, rajoittamatta kuitenkaan palveluiden käyttöä
- Rajoituksien kiertoyritykset
  - Toisen käyttäjän IP-numeron käyttäminen / MAC-numeron muuttaminen
- DoS-hyökkäykset
- Käyttäjien sekä verkon tietoturva ja tietosuoja

Tulevaisuuden näkymiä

- Verkon käyttö lisääntyy edelleen merkittävästi. Mobiliteetti (WLAN, GPRS, 3G,..) tekee tuloa.
- Lisäarvopalvelut tekevät tuloa:
  - Video on demand, IP-puhelut (SIP),..
  - Opetus (virtuaaliyliopisto)
- Verkot tulevat älykkäiksi/dynaamisiksi
  - Käyttäjän tunnistus ja käyttöprofiilit
  - IDS,VPN,FW -palvelut verkon reunalla
  - Self protecting, healing, prevention networks

Lopetus

- Kysymyksiä?
- ..ja kiitos!