NETFLOW-VERKONVALVONTA

LAHDEN AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Syksy 2011
Mikko Liukkonen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

LIUKKONEN, MIKKO: NetFlow-verkonvalvonta

Tietoliikennetekniikan opinnäytetyö, 59 sivua

Syksy 2011

TIIVISTELMÄ

Verkonvalvonnalla on tärkeä rooli varsinkin suurten verkkojen ylläpidossa. Verkossa voi liikkua paljon erilaista dataa, joten verkonvalvojan on hyödyllistä ymmärtää, millainen verkkoliikenne kuormittaa verkkoa eniten. Perinteinen SNMP:llä toteutettu verkonvalvontajärjestelmä ei tarjoa yksityiskohtaista tietoa verkkoliikenteen sisällöstä. Cisco Systemsin kehittämällä NetFlowlla on mahdollista päästä tarkemmin käsiksi verkossa liikkuvien pakettien tietoihin ja näin ollen saada selville erilaisia tietoja verkkoliikenteestä.

Päijät-Hämeen koulutuskonsernin tietohallinto on suunnitellut NetFlown käyttöönottoa ylläpitämässään koulutuskonsernin verkossa. Tämä opinnäytetyö käsittelee NetFlowta protokollana sekä perehtyy kahteen NetFlow-dataa hyödyntävään sovellukseen, jotka ovat ilmaissovellus NfSen sekä kaupallinen SolarWindsin valmistama Orion NetFlow Traffic Analyzer. Myös komennot, joilla NetFlow konfiguroidaan käyttöön Ciscon laitteissa, käydään läpi. Lisäksi perehdytään hieman SNMP-protokollaan, sillä se on yleinen verkonvalvonnassa käytetty protokolla, mutta työn pääpaino on NetFlowlla. Tarkoituksena on tuoda ilmi NetFlown tarjoamia hyötyjä sekä selvittää sopiva sovellus NetFlown käyttöönottoa varten. Näiden tulosten pohjalta PHKK:n tietohallinto voi sitten tehdä päätöksiä NetFlown käyttöönottoon liittyen.

NetFlow-datan keräämistä varten verkon aktiivilaite konfiguroitiin lähettämään NetFlow-dataa kohti testattavia sovelluksia. Ensimmäisenä testattiin Fedora 13 -käyttöjärjestelmällä pyörivää NfSeniä ja toisena Orion NetFlow Traffic Analyzeria, joka asennettiin Windows Server 2003 -käyttöjärjestelmälle. NfSen osoittautui sopivammaksi vaihtoehdoksi, mikäli suunnitelmissa on pelkästään NetFlown käyttöönotto.

NetFlowsta ilmeni useita hyötyjä verkonvalvontaan liittyen. NetFlow tarjoaa SNMP:n tavoin verkkolaitteiden yleisiä liikennemääriä koskevat tiedot, mutta tämän lisäksi myös yksityiskohtaista tietoa verkossa liikkuvasta datasta. Näitä tietoja voidaan hyödyntää usealla eri tavalla.

Avainsanat: verkonvalvonta, SNMP, NetFlow, NfSen, Orion NetFlow Traffic Analyzer

Lahti University of Applied Sciences
Degree Programme in Information Technology

LIUKKONEN, MIKKO: NetFlow-based network monitoring

Bachelor's Thesis in telecommunications, 59 pages

Autumn 2011

ABSTRACT

Network monitoring has an important role, especially in the administration of large networks. A lot of different kinds of data can move in a network so it is important for the network administrator to understand what kind of network traffic causes the most load on the network. A traditional SNMP-based network monitoring system does not offer detailed information about the content of the network traffic. With NetFlow, developed by Cisco Systems, it is possible to get access to the information of the packets traveling the network and therefore uncover different kinds of information about the network traffic.

The IT administration of the Lahti Region Educational Consortium has planned the deployment of NetFlow in the network they administrate. This thesis deals with NetFlow as a protocol and examines two software products that utilize NetFlow data, which are NfSen and Orion NetFlow Traffic Analyzer, manufactured by SolarWinds. The former is freeware and the latter is a commercial product. The commands that are used for the configuration of NetFlow on Cisco devices are also dealt with. The SNMP protocol is also covered slightly since it is a common protocol used in network monitoring. However, the primary focus is on NetFlow. The purpose is to reveal the benefits provided by NetFlow and to find out which software is more suitable for the deployment of NetFlow. With these results the IT administration of the Lahti Region Educational Consortium can then make decisions about the deployment of NetFlow.

For the collection of NetFlow data, a network device was configured to send NetFlow data towards the test software. NfSen, running on the Fedora 13 operating system, was tested first and after that Orion NetFlow Traffic Analyzer, which was installed on the Windows Server 2003 operating system. NfSen turned out to be a more suitable choice if only NetFlow is going to be deployed.

Many benefits for network monitoring were revealed with NetFlow. Like SNMP, NetFlow offers information about common traffic rates of network devices but in addition to this it also provides detailed information about the data traveling the network. This information can be utilized in many ways.

Key words: network monitoring, SNMP, NetFlow, NfSen, Orion NetFlow Traffic Analyzer

SISÄLLYS

LYHENNELUETTELO

AS	Autonomous System. Joukko reitittimiä yhden toimijan hallinnassa.
BGP	Border Gateway Protocol. Tärkeä runkoreititysprotokolla Internetissä.
CEF	Cisco Express Forwarding. Nopea pakettien välitystekniikka.
DES	Data Encryption Standard. Salausmenetelmä, jota ei enää nykyään pidetä kovin turvallisena. DES on symmetrinen salausmenetelmä eli salaukseen ja purkamiseen käytetään samaa avainta. Kyseessä on myös lohkosalain eli salattava viesti jaetaan lohkoihin ennen salausta.
DoS	Denial of Service. Palvelunestohyökkäys, jolla pyritään kaatamaan jokin verkon resurssi.
dCEF	Distributed Cisco Express Forwarding. dCEF-tilassa reitittimen jokainen kortti toimii CEF-tilassa. Jokainen kortti sisältää näin ollen reititystaulun, joten reititys nopeutuu, koska ei tarvitse tehdä kyselyjä pääreititystauluun reititystietojen selvittämiseksi.
GHz	Gigahertsi. Prosessorin tehokkuutta kuvaava yksikkö. Giga tarkoittaa miljardia, ja hertsi on taajuuden yksikkö.
Gt	Gigatavu. Tallennustilan yksikkö. 1 Gt on 10^9 tavua.
HTTP	Hypertext Transfer Protocol. Sovelluskerroksen protokolla, jota käytetään tiedonsiirtoon www-palvelinten ja käyttäjien selainten välillä.
ICMP	Internet Control Message Protocol. Verkkokerroksen protokolla, jolla voidaan viestiä verkkolaitteiden saatavuudesta.
ID	Identification. Tunniste.

IEC	International Electrotechnical Commission. Kansainvälinen standardointiorganisaatio, johon kuuluu kansallisia järjestöjä. IEC tekee yhteistyötä ISO:n kanssa.
IETF	The Internet Engineering Task Force. Yhteisö, joka keskittyy Internetiä koskevien teknisten dokumenttien julkaisuun.
IGMP	Internet Group Management Protocol. Multicast-tietoja välittävä protokolla.
IIS	Internet Information Services. Windows-palvelinohjelmisto, joka tarjoaa esimerkiksi HTTP- ja FTP-palveluja verkkoon.
IOS	Internetwork Operating System. Ciscon kytkimien ja reitittimien käyttöjärjestelmä.
IP	Internet Protocol. Verkkokerroksen protokolla, jolla paketteja siirretään IP-verkoissa. IP-osoitteiden avulla paketit löytävät verkossa oikeaan osoitteeseen.
LAN	Local Area Network. Lähiverkko on verkko, joka yhdistää laitteita pienellä alueella, kuten esimerkiksi kotona tai toimistossa.
MAC	Media Access Control. MAC-osoitteilla tunnistetaan verkon laitteiden verkkoliitynnät. MAC-osoitteet ovat 48 bittiä pitkiä.
Mbps	MegaBits Per Second. Tiedonsiirtonopeus, joka tarkoittaa miljoona bittiä sekunnissa.
MIB	Management Information Base. Tietokanta, joka sisältää laitekohtaisia tietoja, joita voidaan hyödyntää käyttäen SNMP:tä.
MPLS	Multiprotocol Label Switching. Pakettien välitystekniikka, jonka yhteydessä ei tarvitse tehdä reititystä.
MSFC	Multilayer Switch Feature Card. Esimerkiksi Cisco Catalyst 6500 -laitteissa oleva kortti, joka hoitaa ohjelmistoon liittyvät prosessit.

NMS	Network Management System. Hallinta-asema verkossa, jolla voidaan tarkkailla ja hallita muita verkon laitteita.
NTP	Network Time Protocol. NTP-protokollan avulla verkon laitteiden aikatiedot saadaan synkronoitua.
OID	Object Identifier. Tunniste, joka viittaa MIB-tietokannan tietoon.
P2P	Peer to Peer. Vertaisverkko eli verkko, jossa käyttäjien laitteet muodostavat verkon keskenään. Ei sisällä erillisiä palvelimia.
PDF	Portable Document Format. Tiedostomuoto, jota käytetään tekstin ja kuvien julkaisemisessa.
PDU	Protocol Data Unit. Protokollan datayksikkö. Voi sisältää esimerkiksi käyttäjän dataa tai protokollan kontrolli-informaatiota.
PFC	Policy Feature Card. Esimerkiksi Cisco Catalyst 6500 -laitteissa oleva kortti, joka hoitaa datan ohjauksen rautatasolla.
PHP	PHP: Hypertext Preprocessor. Alustariippumaton ohjelmointikieli, jota käytetään erityisesti dynaamisten web-sivujen tekemiseen. PHP suoritetaan palvelimella, joten selain ei tarvitse erillistä tukea PHP:lle näyttääkseen kyseisiä sivuja.
QoS	Quality of Service. Palvelunlaatu, jonka avulla voidaan priorisoida verkkoliikennettä ja näin taata esimerkiksi tietyn tyyppiselle liikenteelle kaistaa verkosta.
RFC	Request for Comments. IETF:n julkaisemia dokumentteja, jotka käsittelevät Internetin standardeja.
RP	Route Processor. Reitittimessä oleva reititysprosessori, joka hoitaa esimerkiksi reititysprotokolliin liittyvät tehtävät.
SCTP	Stream Control Transmission Protocol. Kuljetuskerroksen protokolla, joka tarjoaa luotettavan kuljetuksen. Muutamia eroja TCP-protokollaan: mahdollisuus osittain luotettavaan kuljetukseen sekä

	olla välittämättä pakettien järjestyksestä, multi-streaming, multihoming.
SNMP	Simple Network Management Protocol. Protokolla, jonka avulla voidaan valvoa ja hallita verkon laitteita.
SQL	Structured Query Language. Kyselykieli, jonka avulla relaatiotietokantoja voidaan hallita.
SSH	Secure Shell. Protokolla, jonka avulla saadaan muodostettua suojattu etähallintayhteys laitteeseen.
TCP	Transmission Control Protocol. Luotettavan tiedonsiirron tarjoava kuljetuskerroksen protokolla.
TOS	Type of Service. IP-paketin sisältämää TOS-tavua voidaan käyttää palvelunlaatua koskevissa asioissa.
UDP	User Datagram Protocol. Kuljetuskerroksen protokolla, joka ei tarjoa luotettavaa tiedonsiirtoa. Käytetään esimerkiksi äänen ja kuvan suoratoistossa.
USM	User-based Security Model. SNMPv3:ssa oleva turvallisuuteen liittyvä USM vastaa viestien autentikoinnin lisäksi myös niiden salauksesta.
UTC	Universal Time, Coordinated. Kansainvälistä atomiaikaa seuraava aika.
VACM	View-based Access Control Model. SNMPv3:n yhteydessä VACM rajoittaa pääsyä MIB-tietoihin.
VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko, joka on osa fyysistä lähiverkkoa. Yksi fyysinen lähiverkko voi sisältää useita VLAN-verkkoja.
WAN	Wide Area Network. Laajan alueen kattava verkko. WAN voi yhdistää esimerkiksi useita LAN-verkkoja toisiinsa.

1 JOHDANTO

1.1 Työn tausta

Tietoverkoilla on tärkeä asema tämän päivän yritysten ja organisaatioiden toiminnassa. Verkot tarjoavat tärkeitä palveluita sekä välittävät tietoa sen käyttäjien välillä. Verkkojen kasvaessa ja laajentuessa myös usein niissä liikkuvan tietoliikenteen määrä kasvaa. Ilman verkonvalvontaa on vaikea hahmottaa, millaista dataa verkossa liikkuu sekä ketkä ja minkä tyyppiset käyttäjät vievät verkosta eniten kaistanleveyttä. Päijät-Hämeen koulutuskonsernin tietohallinto on suunnitellut ratkaisua tähän ongelmaan. Tämä ratkaisu on Cisco Systemsin kehittämä verkonvalvontaan tarkoitettu protokolla nimeltä NetFlow.

Päijät-Hämeen koulutuskonserni on kuntayhtymä, johon kuuluu 13 kuntaa, joissa PHKK järjestää, kehittää sekä ylläpitää koulutusta. Koulutuskonsernin tulosalueita ovat Lahden ammattikorkeakoulu, Koulutuskeskus Salpaus sekä Tuoterengas, joissa tarjotaan ammattikorkeakoulutusta, lukiokoulutusta, ammatillista koulutusta, oppisopimuskoulutusta sekä kuntoutusta ja työhön valmennusta. Vuonna 2010 koulutuskonsernissa oli päätoimisia opiskelijoita 12 639 sekä henkilöstöä yhteensä 1707. (Päijät-Hämeen koulutuskonserni 2011a.)

PHKK:n tietohallintopalvelut koordinoi ja ylläpitää erilaisia palveluita koulutuskonsernissa. Palveluihin kuuluvat asiakaspalvelut, tietojärjestelmäpalvelut, tietotekniikkapalvelut sekä tietohallinnon sisäiset palvelut. Tietohallinto vastaa tietojärjestelmien ylläpidosta ja kehittämisestä sekä IT-tukipalveluista. Sisäisiin palveluihin kuuluvat puhelinliikennepalvelut sekä puhelunvälitys. Tietohallinto ylläpitää tietoverkkoa, joka sisältää yli sata palvelinta, tuhansia työasemia sekä noin tuhat tulostinta. Verkossa on aktiivilaitteita noin 400 ja käyttäjiä verkolla on noin 20 000. (Päijät-Hämeen koulutuskonserni 2011b.)

1.2 Työn tavoitteet

Tässä opinnäytetyössä käsitellään verkonvalvontaa ja siihen liittyviä protokollia SNMP ja NetFlow. Koska SNMP on todella yleinen verkonvalvonnassa sekä

-hallinnassa käytetty protokolla, niin teoriaa siihen liittyen käydään läpi, mutta pääpaino on Cisco Systemsin kehittämällä NetFlowlla. Tavoitteena on perehtyä NetFlown toimintaan sekä ottaa selvää sen mukanaan tuomista mahdollisuuksista ja hyödyistä verkonvalvontaan liittyen.

Teorian tutkimisen lisäksi on tarkoituksena testata NetFlowta käytännössä PHKK:n verkossa. Tavoitteena on tutustua kahteen eri NetFlow-sovellukseen, joista toinen on kaupallinen ja toinen ilmainen. Sovelluksia käyttämällä pyritään selvittämään, millaista liikennettä verkossa liikkuu. NetFlown avulla yritetään päästä käsiksi verkon käyttäjien liikenteeseen ja tavoitteena on saada selville verkon kovimmat käyttäjät eli esimerkiksi top-10-lista tai vastaavia tietoja. Myös verkkoon eniten liikennettä muodostavat sovellukset pyritään selvittämään. Tavoitteena on myös, että NetFlown avulla voitaisiin tarvittaessa löytää verkkoliikenteestä tietyt yksittäiset käyttäjät tai tietyt sovellukset. Tämän opinnäytetyön avulla PHKK:n tietohallinto tulee saamaan tietoa ja kokemuksia NetFlown käyttöönottoa varten.

2 VERKONVALVONTA JA SNMP

2.1 Verkonvalvonnan tavoitteet

Tietoverkot ovat tärkeä osa yrityksiä, joten on olennaista optimoida niiden toimintaa, jolloin voidaan säästää rahaa ja lisätä työntekijöiden tehokkuutta. Yrityksissä ei voida luottaa vain arvailuun verkon toiminnan suhteen, vaan tähän tarvitaan verkonvalvontaa. Verkonvalvonnan avulla verkon tilasta ja suorituskyvystä saadaan tietynlainen lähtö- tai vertailukohta, jolloin negatiiviset muutokset voidaan havaita ja niihin voidaan reagoida. Verkonvalvonnan avulla pyritään ylläpitämään ja parantamaan verkon suorituskykyä, varmistamaan verkon saatavuus sekä havaitsemaan verkkoon negatiivisesti vaikuttavat uhkatekijät. (Nash & Behr 2009; Fluke Corporation 2011.)

Verkonvalvonnan avulla voidaan tarkkailla esimerkiksi verkon suorituskykyä, huomata kyseenalaisia verkon käyttäjiä sekä kaatuneita servereitä sekä havaita muita ongelmia. Erilaisilla sovelluksilla ja laitteilla voidaan valvoa lähes kaikenlaisia verkkoja. Ei ole väliä, onko kyseessä esimerkiksi langallinen vai langaton verkko, LAN, tai palveluntarjoajan WAN-yhteys ja sisältääkö verkko esimerkiksi kytkimiä, reitittimiä tai palvelimia, sillä niitä kaikkia voidaan valvoa. On tärkeää suunnitella, mitä halutaan valvoa. Tätä varten on tärkeää, että verkon topologiakuvat ovat ajan tasalla. (Nash & Behr 2009.)

Ihanteellinen verkonvalvontaratkaisu sisältää laajuutta toimintojen suhteen. Sen tulee olla hyvin skaalautuva ja sen avulla saadaan laajakin verkko valvontaan. On tärkeää, että päästään käsiksi kaikkiin verkon eri kerroksiin. Näin mahdolliset ongelmat saadaan paikallistettua riippumatta siitä, onko vika verkon aktiivilaitteissa, kuten kytkimessä tai reitittimessä, vai onko ongelma tietyssä sovelluksessa tai sovellusta pyörittävässä palvelimessa tai päätelaitteessa. Hyvään verkonvalvontaan kuuluu reaaliaikaisen tarkkailun lisäksi myös mahdollisuus historiatietojen tutkimiseen, joiden avulla ajoittain ilmenevät ongelmat saadaan selvitettyä ja ratkaistua. (Fluke Corporation 2011.)

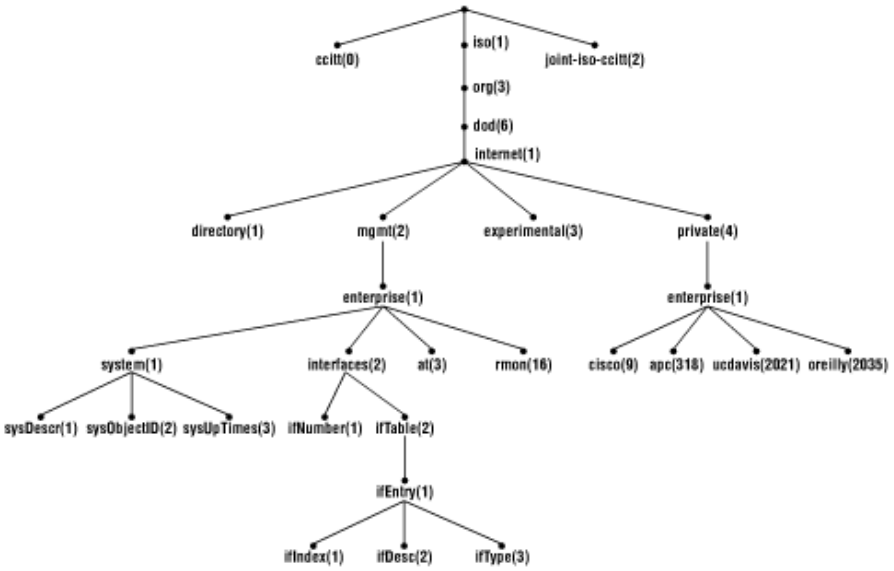
ISO (International Organization for Standardization) yhdessä IEC:n (International Electrotechnical Commission) kanssa on luonut standardin ISO/IEC 7498-4 verkonhallintaan liittyen, mikä sisältää myös verkonvalvontaan liittyviä määrityksiä. Standardissa verkonhallinta on jaoteltu viiteen eri osa-alueeseen, jotka ovat seuraavat:

- Vian hallinta - Viat pyritään havaitsemaan ja korjaamaan.
- Laskutuksen hallinta - Verkon käyttöä valvotaan ja sen mukaan laskutetaan.
- Konfiguraation hallinta - Hallitaan verkon laitteiden toimintaa. Valvotaan niitä keräämällä niistä dataa ja tarvittaessa muutetaan asetuksia.
- Suorituskyvyn hallinta - Valvotaan ja tarkkaillaan verkon laitteita ja liikennettä käyttäen siihen tarkoitettuja protokollia. Näin voidaan tarkkailla tiettyä laitetta, tietyn kerroksen liikennettä tai yksittäisiä yhteyksiä.
- Turvallisuuden hallinta - Ylläpidetään turvallisuuteen liittyviä asioita ja ilmoitetaan käyttäjille turvallisuuteen liittyvistä asioista.
  (ISO/IEC 7498-4 1989.)

2.2 SNMP-protokolla

SNMP-protokolla eli Simple Network Management Protocol on verkonvalvonnassa sekä -hallinnassa käytetty protokolla, jolla kommunikoidaan hallintalaitteen sekä hallittavien ja valvottavien laitteiden välillä. Vuonna 1990 SNMP:stä tuli Internet-standardi ja jo ennen sitä useat eri laitevalmistajat tukivat SNMP:tä eli sillä voitiin hallita eri valmistajien laitteita (Hautaniemi 1994). Protokollan avulla voidaan havaita ja välttää vikatilanteita verkkoyhteyksissä ja laitteissa. Valvottavat laitteet keräävät tietoa itsestään ja tieto siirretään SNMP-protokollan avulla valvovalle asemalle. SNMP:n avulla haluttuja tietoja voidaan kysellä laitteilta tietyin väliajoin tai laitteisiin voidaan etukäteen määritellä millaisen tapahtuman yhteydessä hallinta-asemalle raportoidaan SNMP:n trap-viestillä. Lisäksi SNMP:n avulla on mahdollista muokata valvottavan laitteen tietoja. (Hunt 1998, 356 - 357.)

SNMP:n yhteydessä käytetään MIB-tietokantoja, jotka sisältävät laitteen tietoja. MIB-tietokannat ovat puumaisia rakenteeltaan (kuvio 1), ja niistä löytyy sekä pakollisia tietoja, että valmistajakohtaisia tietoja. MIB-tietokannan yksittäiset tiedot voidaan ilmaista OID-numerosarjalla, joka kuvaa yhden tiedon sijainnin MIB-tietokantapuussa. Näiden OID eli Object Identifier -numeroiden avulla laitteista voidaan kysellä erilaisia tietoja. (Hakala & Vainio 2005, 325.)



KUVIO 1. MIB-tietokannan puumainen rakenne (Sloan 2001, 7)

Tietoa SNMP:n avulla välitetään erilaisilla viesteillä, joita kutsutaan nimellä PDU. PDU tulee sanoista Protocol Data Unit, ja se sisältää tiedon, millaisesta SNMP-viestistä on kyse. Tällaisia viestejä ovat mm. GetRequest-, GetNextRequest-, SetRequest- ja Trap-viestit. GetRequest-viesteillä voidaan kysellä laitteelta jotain tiettyä tietoa ja GetNextRequest-viestillä seuraavaa tietoa. Set-Request-viestit kehottavat laitetta muuttamaan jotain arvoa. Trap-viestit ovat hälytysviestejä, joilla viestitään jostain tietystä tapahtumasta hallinta-asemalle. Näiden viestityyppien lisäksi SNMP:n ensimmäisessä versiossa on vielä vastausviestit GetResponse sekä SetResponse, joilla ilmoitetaan vastaukset kyselyihin ja käskyihin. SNMP:n uudemmissa versioissa on tullut uusia viestejä sekä viestit ovat muuttuneet rakenteeltaan. (Hakala & Vainio 2005, 328 - 329.)

SNMP käyttää tiedonsiirrossa UDP-protokollaa, jonka avulla SNMP-PDU:t välitetään lähettäjältä vastaanottajalle. Porttinumeroita SNMP:ssä on käytössä kaksi kappaletta, joista ensimmäinen on portti numero 161. Tätä porttia käytetään, kun SNMP:llä kysellään tietoa laitteista. Mikäli laitteessa jokin aiheuttaa Trap-viestin lähettämisen, niin se lähetetään porttiin numero 162 eli hallinta-asema ottaa Trap-viestit vastaan UDP-porttiin numero 162. (Hunt 1998, 357.)

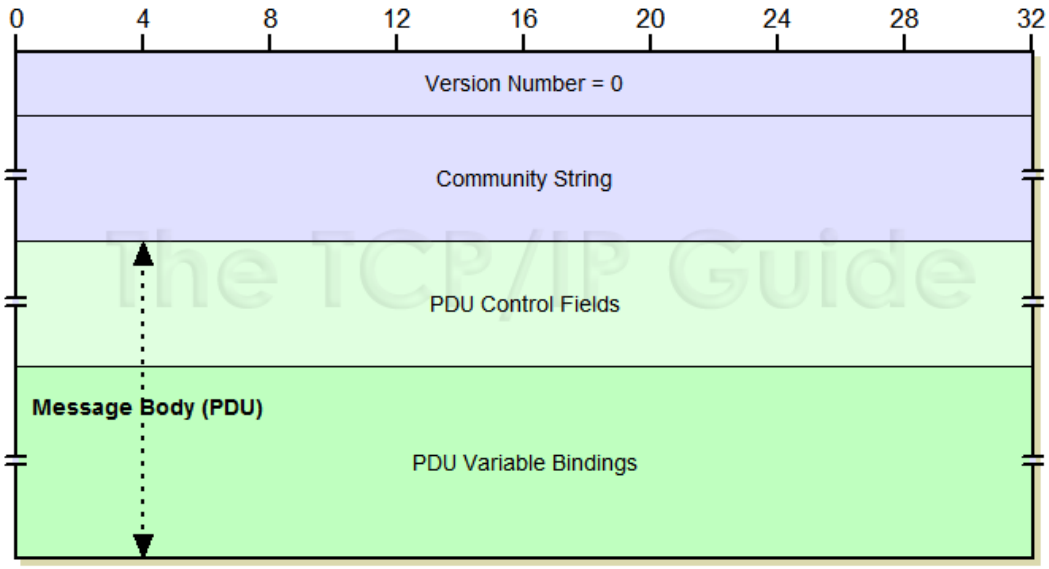
2.3 SNMP-protokollan versiot

SNMP-protokollasta on olemassa eri versioita, joista jokainen tuo edelliseen hiukan lisää toimintoja tai ominaisuuksia. Versiot ovat SNMPv1, SNMPv2 sekä SNMPv3. SNMP:n ensimmäinen versio standardoitiin vuonna 1990, toinen versio vuosina 1993 - 1994 ja SNMPv3 hyväksyttiin Internet-standardiksi vuonna 2002 (Hautaniemi 1994; IBR 2011). Versionumerossa korkeammalle mentäessä SNMP-sanomia tulee lisää sekä turvallisuus kasvaa (Bibbs & Matt 2006, 3).

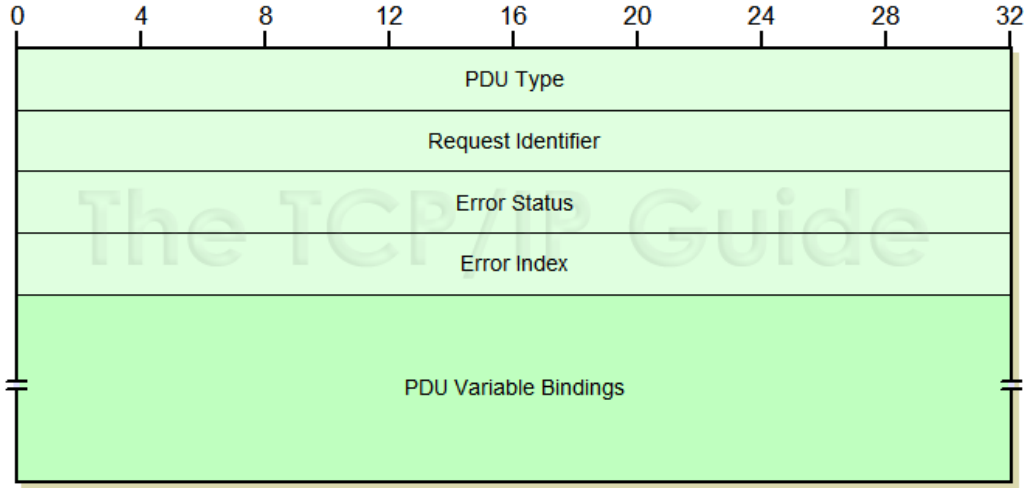
SNMP:n ensimmäisessä versiossa eri viestityyppejä on viisi kappaletta. GetReguest-viestillä hallinta-asema voi kysyä laitteelta jotain yksittäistä MIB-tietokannan tietoa. Seuraavana olevia tietoja voidaan kysyä GetNextRequest-viestillä. SetRequest pyytää laitetta päivittämään MIB-tietokannan yhden muuttujan halutuksi arvoksi. Laitteet vastaavat hallinta-asemalta tuleviin viesteihin GetResponse-nimisellä viestillä. Viides viestityyppi on nimeltään Trap, joka lähtee valvottavasta laitteesta hallinta-asemalle jonkin tapahtuman yhteydessä. Trap-viesteihin ei lähetetä vastausviestiä. (Puska 2000, 311.)

SNMPv1-sanomat ovat melko yksinkertaisia, kuten kuviosta 2 voidaan havaita. Sanoma alkaa versionumerolla, jonka jälkeen on tieto yhteisöstä. Yhteisö toimii salasanana, joten väärän yhteisön sisältävät viestit hylätään (Kozierok 2005d). Sitten alkaa dataosuus, joka sisältää kontrollidataa sekä varsinaisen datan. Tarkemmat PDU:n tiedot nähdään kuviosta 3. PDU Type -kenttä sisältää tiedon viestin tyypistä, eli onko kyseessä esimerkiksi GetRequest-viesti vai SetRequest-viesti. Toisena oleva Request Identifier sisältää arvon, jolla kyselyt ja vastaukset liitetään toisiinsa. Error Status -kenttää käytetään GetResponse- eli vastausviesteissä ilmaisemaan mahdollisen virhetilanteen syy. Error Status on arvoltaan 0,

mikäli virheitä ei ilmennyt. Virheen ilmaantuessa Error Index ilmaisee objektin, josta virhe johtui. PDU:n lopussa oleva Variable Bindings sisältää MIB-objekteihin viittaavat OID-numerot sekä mahdolliset arvot, mikäli kyseessä on esim. SetRequest-viesti. Trap-viestit ovat ainoita SNMPv1-viestejä, joiden muoto on hieman erilainen. (Kozierok 2005a.)



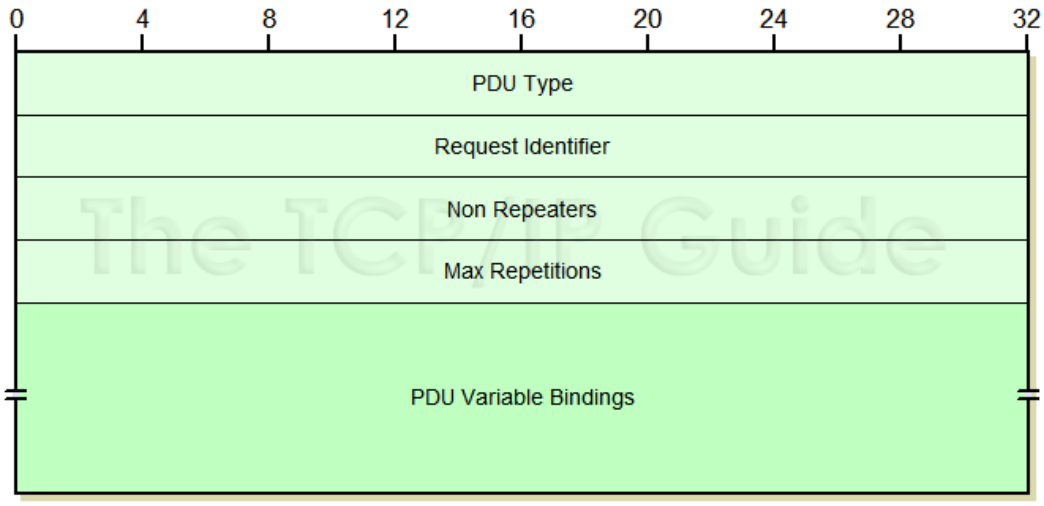
KUVIO 2. SNMPv1-viestin muoto (Kozierok 2005a)



KUVIO 3. SNMPv1 PDU:n muoto (Kozierok 2005a, 2)

SNMP:n toisesta versiosta on itse asiassa neljä eri muotoa, mutta yleisesti on käytössä SNMPv2c. Muita muotoja ovat alkuperäinen SNMPv2, SNMPv2* sekä SNMPv2u. SNMP:n ensimmäinen versio ei ole kovin turvallinen, sillä tietoa ei salata ennen kuin se lähetetään verkkoon. SNMPv2 toi tähän muutoksen tuomalla

mukaan DES-salausalgoritmin. Myös MIB-tietokanta on päivitetty SNMP:n toisen version myötä. PDU on pysynyt samana kuin SNMP:n ensimmäisessä versiossa, mutta Get-Bulk-viestin PDU on hieman erilainen (kuvio 4). Siinä olevat Non Repeaters- ja Max Repetitions -kohdat liittyvät usean tiedon hakemiseen samalla kertaa. Non Repeaters -kenttä ilmoittaa, kuinka monta objektia edetään Variable Bindings -kentässä ilmoitetun OID-numeron alla, ja Max Repetitions kertoo, kuinka monta arvoa näistä tauluista luetaan. (Parker 2005; Kozierok 2005b, 5 - 6.)



KUVIO 4. Get-Bulk-viestin PDU (Kozierok 2005b, 6)

SNMP:n toinen versio kasvattaa myös viestien määrää. Alkuperäiset viisi viestiä ovat edelleen käytössä, mutta niiden lisäksi on tullut kaksi uutta viestiä nimeltään Get-Bulk sekä Inform. Get-Bulk-viestiä käytetään, mikäli halutaan saada suuri määrä tietoa laitteesta ulos kerralla. Inform-viestit taas on tarkoitettu hallinta-asemien väliseen liikenteeseen. Eli jos käytössä on useita hallinta-asemia, niin Inform-viesteillä ne voivat ilmoittaa toisilleen vastaanotetuista Trap-viesteistä. Inform-viesteihin lähetetään myös vastausviesti. (Puska 2000, 311.)

SNMP:n kolmas versio eli SNMPv3 sisältää useita samoja asioita kuin edeltäjänsä. SNMP-viestit ovat samat kuin SNMPv2:ssa sekä PDU on pysynyt sisällöltään samanlaisena. Tärkeä uudistus SNMP:n kolmannessa versiossa on parannukset turvallisuuteen liittyen. SNMPv3-sanomien alussa ennen PDU:ta on joukko salaukseen sekä autentikointiin liittyviä parametreja, joiden avulla turvallisuutta saa-

daan lisättyä. SNMPv3:n yhteydessä puhutaan termeistä USM sekä VACM. USM eli User-Based Security Model liittyy käyttäjiin ja ryhmiin, joiden avulla SNMP-viestit autentikoidaan. Näin saadaan rajattua pääsyä SNMP-tietoihin. VACM puolestaan liittyy MIB-tietokannan tietoihin ja siihen, kenellä niihin on pääsy. Näin voidaan rajata, mitä tietoja eri käyttäjät pääsevät muokkaamaan. (Kozierok 2005c; H3C Technologies 2008, 2.2.3.)

2.4 SNMP-järjestelmän arkkitehtuuri

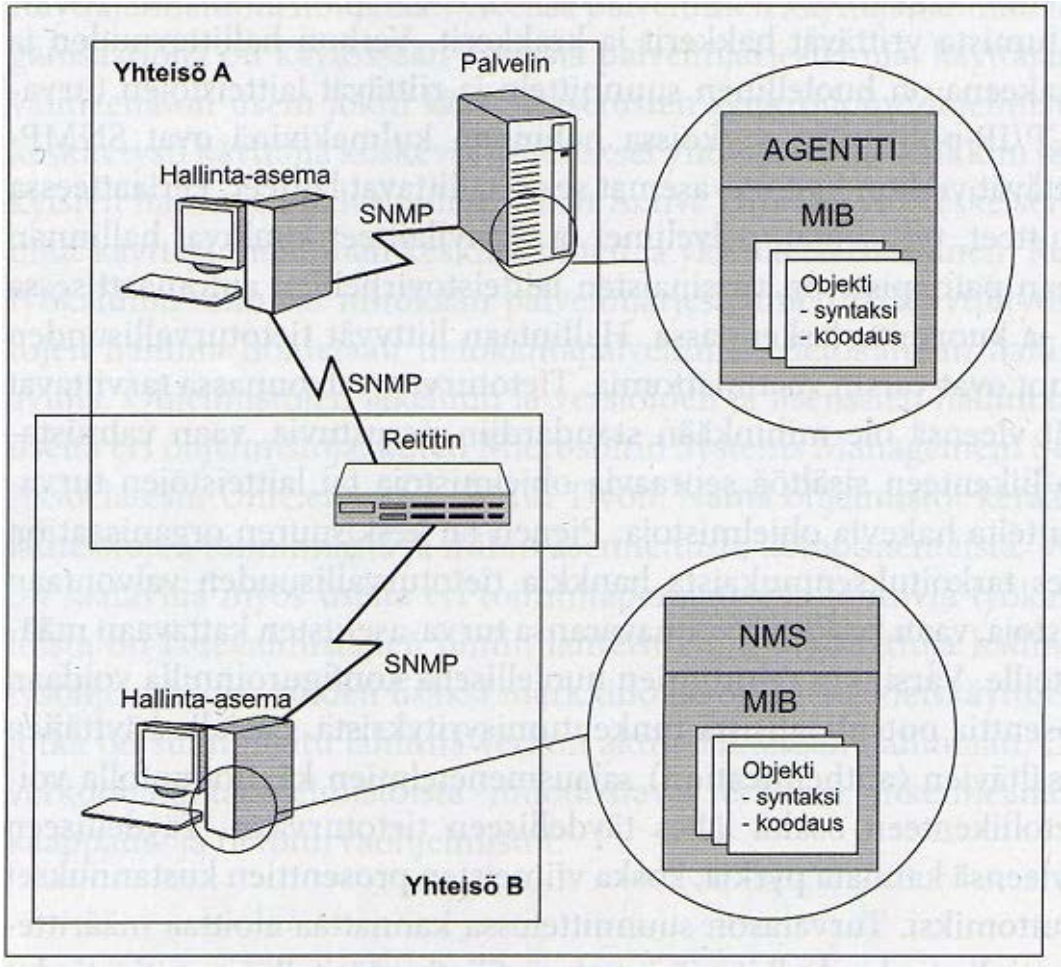
SNMP-järjestelmä koostuu laitteista, jotka pitävät yllä MIB-tietokantaa omista tiedoistaan sekä hallinta-asemasta, jolla SNMP-viestejä analysoidaan. Hallittavat laitteet voivat olla verkon aktiivilaitteita, kuten kytkimiä tai reitittimiä, tai sitten ne voivat olla vaikka palvelimia. Laitteet, joita valvotaan, sisältävät SNMP-agentin, joka pitää yllä MIB-tietokantaa laitteen tiedoista. Valvottavat laitteet sekä hallinta-asemat keskustelevat keskenään SNMP-protokollalla. (Hakala & Vainio 2005, 323.)

SNMP-järjestelmässä hallinta-asema konfiguroidaan niin, että se kyselee haluttuja tietoja laitteiden MIB-tietokannoista. MIB-tietokannassa on pakollisia standardissa määriteltyjä objekteja, joiden lisäksi tietokannasta voi löytyä myös valmistajakohtaisia objekteja järjestelmästä riippuen. Mikäli Trap-viesteille on tarvetta, niin ne tulee määritellä laitekohtaisesti eli agentti asetetaan lähettämään viestejä hallinta-asemalle ilman, että hallinta-asema on niitä erikseen pyytänyt. Hallinta-asemissa on laitteiden MIB-tietokannat, jotta SNMP-agenttien lähettämät Trap-viestit ymmärretään hallinta-asemalla. Laitteen MIB-tietokanta tarvitaan Trap-viestien yhteydessä OID-numeron ymmärtämiseen, jotta tiedetään, mitä asiaa hälytysviesti koskee. (Hakala & Vainio 2005, 323 - 324.)

SNMP-järjestelmän yhteydessä puhutaan yhteisöistä. Laitteet ja hallinta-asemat muodostavat yhteisöjä. Jokainen laite määritellään kuuluvaksi johonkin yhteisöön. Kun hallinta-asema ja laite ovat samassa yhteisössä, niin ne voivat keskustella keskenään SNMP:n avulla. Nämä yhteisöt eli communityt ovat tietoturvaan liittyvä tekijä, jolla rajataan laitteen tietojen leviäminen ulkopuolisille. Oletusyhteisöt uusissa laitteissa ovat nimeltään public ja private, jotka on syytä vaihtaa, ja yhtei-

söjen nimiä ei kannata jakaa julkisesti, sillä yhteisön avulla laitteen tietoja päästään lukemaan ja mahdollisesti muuttamaan. Public-yhteisöllä on oletuksena vain lukuoikeus ja private-yhteisöllä on luku/kirjoitusoikeus. (Hakala & Vainio 2005, 324; CTDP 2011.)

Kuvio 5 näyttää, millainen on SNMP-järjestelmän perusrakenne. Kuviossa nähdään kaksi erillistä yhteisöä, jotka sisältävät laitteita, joissa SNMP on käytössä. Laitteet sisältävät MIB-tietokannan. Myös hallinta-asemia kuviossa on kaksi kappaletta.



KUVIO 5. SNMP-järjestelmän perusrakenne (Hakala & Vainio 2005, 324)

Kuviossa 5 näkyvä NMS tulee sanoista Network Management Station, joka tarkoittaa hallinta-asemaa. Myös hallinta-asemassa nähdään MIB-tietokanta. Kuviossa näkyvät kaksi yhteisöä eivät keskustele keskenään vaan laitteet on jaettu yh-

teisöihin A ja B, eli vain samaan yhteisöön kuuluvat laitteet keskustelevat keskenään SNMP:n avulla. (Hakala & Vainio 2005, 324.)

2.5 SNMP-sovellukset

SNMP-sovelluksia on olemassa muutamaa eri tyyppiä. Tällaisia sovellustyyppejä ovat SNMP-komentoja lähettävä sovellus, SNMP-komentoihin vastaava sovellus, SNMP-ilmoituksia lähettävä sovellus, ilmoituksia vastaanottava sovellus sekä SNMP-viestejä eteenpäin ohjaava sovellus. Näiden sovellusten ei kuitenkaan tarvitse aina olla täysin erillisiä toisistaan, nimittäin esimerkiksi viestejä lähettävä sovellus voi toimia samassa laitteessa viestejä vastaanottavan sovelluksen rinnalla. (RFC 2573 1999, 1.)

Komentoja lähettävä sovellus luo SNMP-pyynnöt ja lähettää niitä. Sovellus voi luoda sekä luku- että kirjoituspyyntöjä tai vain toisia näistä kahdesta. Tällainen SNMP-sovellus myös käsittelee vastausviestit lähettämiinsä pyyntöihin. Näihin pyyntöihin vastaa SNMP-komentoihin vastaava sovellus, joka käsittelee sille osoitetut viestit ja lähettää vastauksen niihin. (RFC 2573 1999, 1.)

Kolmas SNMP-sovellusten tyyppi eli SNMP-ilmoituksia lähettävä sovellus toimii laitteen tarkkailijana. Kun se havaitsee jonkin tietyn tapahtuman laitteessa, niin se luo ja lähettää ilmoitusviestin kohti ennalta määrättyä kohdetta. Sovelluksen täytyy myös tietää, mitä SNMP:n versiota käyttää ilmoitusviestien yhteydessä. Myös viestien yhteydessä käytettävät turvallisuuskäytännöt on oltava sovelluksen tiedossa. Neljäs SNMP-sovellustyyppi on tällaisia ilmoitusviestejä vastaanottava sovellus. Sovellus ottaa vastaan ilmoituksen ja lähettää siihen vastauksen, mikäli kyseessä on viesti, joka vaatii vastauksen. (RFC 2573 1999, 1.)

Viimeinen sovellustyyppi on SNMP-viestejä eteenpäin välittävä sovellus. Tällaisia proxy-sovelluksilla voidaan tarkoittaa kolmenlaisia eri sovelluksia. Tällaisia ovat SNMP-pyyntöjä eteenpäin ohjaava sovellus, SNMP-pyyntöjä muiden protokollien operaatioiksi kääntävä sovellus tai sovellus, joka tarjoaa tuen objekteille, joiden arvo riippuu useasta muusta objektista. (RFC 2573 1999, 1.)

3 NETFLOW

3.1 NetFlow-protokolla

SNMP:n avulla verkosta on mahdollista selvittää datamääriä. SNMP ei kuitenkaan pysty luonnehtimaan, minkä tyyppistä liikennettä verkossa kulkee. NetFlow tarjoaa mahdollisuuden päästä datamäärien mittauksesta tarkempaan liikenteen karakterisointiin, jolloin päästään käsiksi esimerkiksi yksittäisten yhteyksien IP-osoitteisiin. NetFlow on IP-verkkojen liikenteen seurantaan tarkoitettu tekniikka. Sen on kehittänyt Cisco, joka on kyseisen tekniikan johtava yritys. NetFlow on osa Cisco IOS -käyttöjärjestelmää kytkimissä ja reitittimissä. NetFlown avulla verkossa olevissa aktiivilaitteissa voidaan kerätä dataa verkkoliikenteestä. Tätä dataa voidaan analysoida ja hyödyntää eri tavoilla. Kun verkkoliikenne kasvaa koko ajan, niin on hyödyllistä ymmärtää, mistä liikenne koostuu, mistä se on lähtöisin ja minne se on menossa. Kaikkeen tähän NetFlow tarjoaa mahdollisuuden. (Cisco Systems 2007a; Cisco Systems 2011a; Cisco Systems 2004.)

NetFlown avulla on mahdollista saada tietoa verkon käyttäjistä sekä sovelluksista. Näitä tietoja voidaan hyödyntää verkon resurssien jakamisessa eri käyttäjien sekä sovelluksien kesken. Liikenteestä voidaan havaita tietynlaisia toistuvia kuvioita tai esimerkiksi yksittäisiä verkkoliikenteen käytäntöjen rikkomisia. NetFlown avulla voidaan siis monitoroida, mistä lähteestä data on kotoisin, mihin verkkoon se on matkalla ja mitä sovellusta käytetään. (Cisco Systems 2004.)

NetFlown avulla kerättyä dataa voidaan hyödyntää verkon suunnittelussa ja tulevaisuutta arvioitaessa. Dataa voidaan esimerkiksi kerätä pitkältä ajalta, jolloin sen avulla voidaan esimerkiksi arvioida, riittävätkö verkkoyhteyksien kaistanleveydet tulevaisuuden mahdollisen liikennemäärän kasvun yhteydessä. Näin voidaan selvittää, onko tulevaisuudessa mahdollisesti tarvetta verkkolaitteiden uusimiseen, kuten uusien reitittimien hankintaan tai korkeamman kaistanleveyden omaavien liityntöjen käyttöönottoon. (Cisco Systems 2004.)

Verkon turvallisuutta analysoitaessa voidaan käyttää NetFlown tarjoamaa dataa. NetFlow-dataa tutkimalla voidaan selvittää verkkoliikenteen epätavalliset poik-

keamat ja esimerkiksi DoS-hyökkäykset on mahdollista tunnistaa NetFlow-datan avulla. NetFlow voi toimia siis tärkeänä tutkimusvälineenä verkon liikennettä tutkittaessa. (Cisco Systems 2004.)

Yksi NetFlown käyttömahdollisuus on myös verkkoliikenteen laskutukseen liittyvä, sillä NetFlown avulla verkossa liikkuvaa dataa voidaan mitata ja sen mukaan laskuttaa. Lisäksi NetFlown avulla on mahdollista mitata kahden pisteen välistä liikennettä ja näin todeta onko liikennevälit esimerkiksi palveluntarjoajiin sopimuksen mukaisia. (Cisco Systems 2004.)

3.2 NetFlow-protokollan versiot

NetFlowsta on olemassa yhdeksän erillistä versiota. Näistä kaikki versiot eivät ole yleisessä käytössä. Versio 1 on versioista alkuperäinen, jonka jälkeen tulleita versioita 2, 3 ja 4 ei koskaan julkaistu. Versio 5 on laajennus, joka toi mukaan BGP:n (Border Gateway Protocol) AS-numerot sekä flow-numeroinnin. Versio 6 ei ole käytössä uusissa IOS-versioissa ja se on hyvin samantapainen version 7 kanssa. Versio 7 ei ole käytössä reitittimissä. Se mahdollistaa NetFlown käytön Cisco Catalyst 5000 -sarjan kytkimissä, jotka sisältävät NetFlow feature card -kortin. Versio 8 toi mukanaan laajennuksen, joka mahdollistaa NetFlow-datan yhdistelyn reitittimissä ennen sen lähettämistä NetFlow-kerääjälle. Näin NetFlow-datan lähettäminen saatiin viemään vähemmän kaistaa verkosta. (Caligare 2006a.)

Uusin NetFlown versio on versio 9 ja se on pohjana IETF:n standardille. Suurin ero versiossa 9 aikaisempiin versioihin nähden on, että se käyttää mallipohjia. Tämä tarkoittaa sitä, että NetFlown laajennettavuus paranee ja uusia ominaisuuksia on helpompi lisätä. Tämä helpottaa myös NetFlow-sovellusten kehittäjien työtä, sillä uusia ominaisuuksia on näin helpompi ottaa käyttöön. Mallipohjaisuus mahdollistaa myös NetFlow-viestin tulkitsemisen kerääjällä, vaikka jotain yksittäistä uutta tietoa ei ymmärrettäisikään. NetFlow-kerääjälle voidaan myös lähettää vain tietyt halutut tiedot flowsta, jolloin säästetään muistia sekä verkon kaistaa. (Cisco Systems 2011b; RFC 3954 2004, 1.)

3.3 NetFlow-järjestelmän arkkitehtuuri

NetFlow-järjestelmän voidaan katsoa koostuvan kolmesta eri osasta. Jokaisella näillä kolmella osalla on omat tehtävänsä. Ensimmäinen tehtävä on kerätä ja varastoida flow-dataa välimuistiin. Reititin tai kytkin hoitaa tämän asian varastoimalla läpi kulkevan datan flow-tiedot talteen. Tässä vaiheessa NetFlow-data valmistellaan myös lähetettäväksi eteenpäin. (Cisco Systems 2004.)

Toinen osa NetFlow-järjestelmää on flow-kerääjä. Sen tehtävänä on vastaanottaa reitittimien lähettämät NetFlow-datat sekä varastoida ne jatkoa varten. Kun data on kerätty ja lähetetty sen jälkeen kerääjälle, niin vuorossa on datan analysointi. Tämä tapahtuu graafista käyttöliittymää hyväksi käyttäen, joka on NetFlow-järjestelmän kolmas komponentti. (Cisco Systems 2004.)

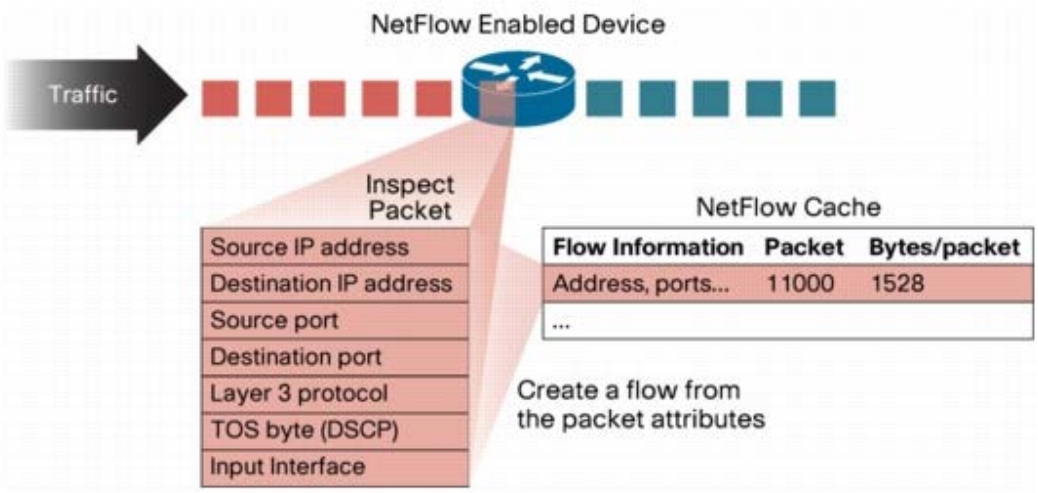
3.4 Flown tiedot

Reitittimen läpi kulkee datapaketteja, jotka sisältävät erilaisia tietoja, kuten esimerkiksi lähde- ja kohdeosoitteet sekä porttinumerot. Tietoja tutkimalla paketit saadaan identifioitua ja niistä saadaan muodostettua yksittäinen flow. Flow tunnistetaan siis pakettien tiedoista ja tunnistuksessa käytetään perinteisesti viidestä seitsemään erilaista tietoa. Samat tiedot sisältävät paketit kerätään yhteen ja flown sisältämät paketit ja tavut lasketaan yhteen. Flow-tietoja säilytetään reitittimen NetFlow-välimuistissa. (Cisco Systems 2007a.)

Flowt tunnistetaan seuraavilla tiedoilla:

- IP-lähdeosoite
- IP-kohdeosoite
- lähdeportti
- kohdeportti
- 3-kerroksen protokollan tyyppi
- palvelun laatu
- laitteen liitäntä.

Näistä flown tiedoista saadaan selville, kuka liikennettä lähettää ja minne sekä mitä sovelluksia käytetään. Lisäksi tietoa saadaan pakettien prioriteetista TOS-tavun avulla sekä tietoa, mihin liitäntään paketit saapuvat reitittimeen tullessaan. Kuvio 6 havainnollistaa vielä, kuinka pakettien saapuessa reitittimeen tiedot tarkastetaan ja ne lisätään välimuistiin. (Cisco Systems 2007a.)



KUVIO 6. Flown muodostuminen välimuistiin (Cisco Systems 2007a)

Jokaista aktiivista flowta varten muodostetaan välimuistiin merkintä, jota voidaan kutsua myös nimellä flow record. Kun flow on vanhentunut, niin flow recordit voidaan lähettää kohti NetFlow-kerääjää. Flow voi vanhentua esimerkiksi olemalla toimettomana tietyn aikaa tai saavuttamalla flowlle säädetyn maksimiajan, joka on oletuksena 30 minuuttia. (Cisco Systems 2011.)

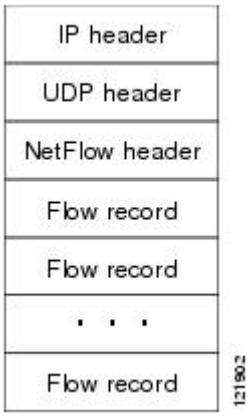
3.5 NetFlow-paketti

3.5.1 Pakettien koostumus

NetFlow-paketilla tarkoitetaan pakettia, joka sisältää flow recordeja. Nämä paketit lähtevät laitteesta, jossa NetFlow on päällä ja ne menevät kohti NetFlow-kerääjää. NetFlow-paketit lähetetään käyttäen UDP-protokollaa. Versiossa 9 on mahdollista UDP:n lisäksi käyttää myös SCTP-protokollaa. Jokaisen NetFlow-version käyttämät paketit koostuvat kahdesta osiosta, joista ensimmäinen on otsikkotiedot ja

toinen joukko flow recordeja. Tosin NetFlow-versio 9 on poikkeus tähän, sillä se käyttää mallipohjia eli Templateja. (RFC 3954 2004; Caligare 2006b.)

Tässä työssä käydään läpi tarkemmin versioiden 5 ja 9 pakettien formaatti. Kuvio 7 näyttää tyypillisen NetFlow-viestin koostumuksen, jossa IP-paketti sisältää UDP-kehyksen, jonka alta löytyy NetFlown otsikkokenttä sekä flow recordit.



KUVIO 7. Tyypillinen NetFlow-viesti (Cisco Systems 2011d)

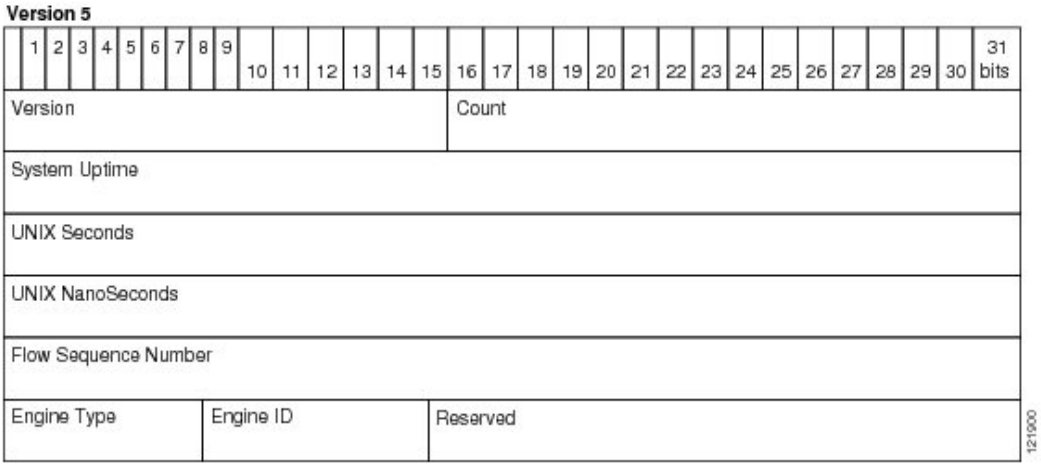
3.5.2 Pakettien otsikkotiedot ja Flow Recordit

NetFlow paketissa ensimmäisenä on otsikkotiedot. Näistä tiedoista selviää paketin sisältöön liittyviä asioita. Tällaisia asioita ovat esimerkiksi käytetyn NetFlow-version numero, flow recordien määrä paketissa sekä paketin numero. (RFC 3954 2004.)

Kuviossa 8 on NetFlow-version 5 otsikon koostumus. Eri kenttien merkitykset ovat seuraavat:

- Version - NetFlow-version numero.
- Count - NetFlow Recordien määrä tässä paketissa.
- System Uptime - Aika millisekunteina reitittimen edellisestä käynnistyksestä.
- UNIX Seconds - Sekuntien määrä ajasta 0000 UTC 1970.
- UNIX NanoSeconds - Jäännösnanosekuntien määrä ajan 0000 UTC 1970 jälkeen.

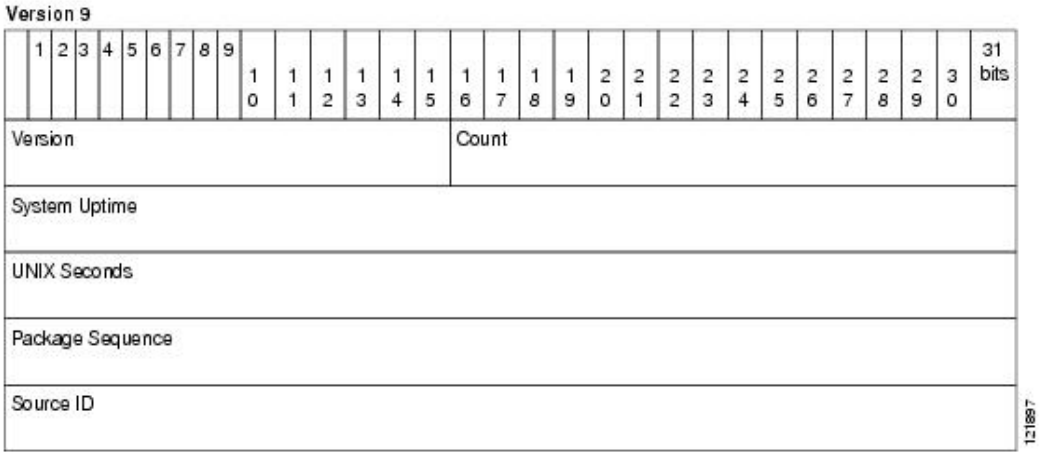
- Flow Sequence Number - Laskuri, joka ilmoittaa lähetetyn flowmäärän.
- Engine Type - Kytkentämoottorin tyyppi.
- Engine ID - NetFlow-moottorin tunniste.
- Reserved - Varattu.
  (Cisco Systems 2011c.)



KUVIO 8. NetFlow-version 5 otsikkotiedot (Cisco Systems 2011c)

Kuviossa 9 on NetFlow-version 9 otsikon koostumus. Kenttien merkitykset ovat seuraavat:

- Version - NetFlow-version numero eli tässä tapauksessa 9.
- Count - Paketin sisältämien FlowSettien Recordien summa.
- System Uptime - Millisekuntien määrä ensimmäisestä laitteen käynnistyksestä.
- UNIX Seconds - Sekuntien määrä ajasta 0000 UTC 1970.
- Package Sequence - Paketin järjestysnumero, joka kertoo kuinka monta pakettia on lähetetty.
- Source ID - Tunniste, jolla tunnistetaan NetFlow-pakettien lähettäjä.
  (Cisco Systems 2011c.)



KUVIO 9. NetFlow-version 9 otsikkotiedot (Cisco Systems 2011c)

Kuvioista 8 ja 9 selviää, että otsikkotiedot ovat hieman muuttuneet versioiden välillä, vaikka samojakin kenttiä otsikoista löytyy. Heti ensimmäinen kenttä eli Version, joka löytyy sekä versiosta 5 että 9, paljastaa tutkittavan paketin NetFlow-version. Seuraavat kentät Count, System Uptime sekä UNIX Seconds ilmaisevat kummassakin versiossa jokseenkin samoja asioita. System Uptimen tarkoitus on vaan muuttunut versiossa 9 tarkoittamaan aikaa ensimmäisestä käynnistyksestä laskettuna edellisen käynnistyksen sijaan. Unix NanoSeconds, Engine Type, Engine ID ja Reserved -kentät ovat poistuneet versiossa 9. Tunnistusta varten version 9 otsikon loppuun on tullut kenttä nimeltä Source ID. Version 5 otsikossa laskurina toimii lähetetty flowmäärä, joka ilmaistaan kentässä nimeltä Flow Sequence Number, kun taas versiossa 9 lasketaan lähetettyjä paketteja kentässä Package Sequence. (Cisco Systems 2011c.)

Kuviosta 10 nähdään NetFlow-version 5 flow recordin sisältämät tiedot. Taulukossa on kolme kenttää: Content, Bytes sekä Descriptions. Content- eli sisältöosuudesta selviää kyseisen kentän sisältämä tieto, jonka vieressä oleva Bytes- eli tavut-kohta ilmaisee, mitkä tavut flow recordissa sisältävät kyseisen tiedon. Viimeinen kohta eli Descriptions sisältää selityksen kyseisen kentän sisällöstä. (Cisco Systems 2011c.)

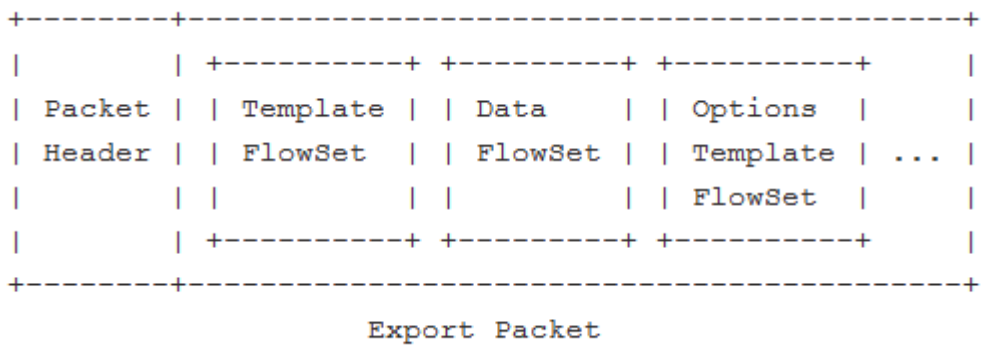
Content	Bytes	Descriptions
srcaddr	0-3	Source IP address
dstaddr	4-7	Destination IP address
nexthop	8-11	Next hop router's IP address
input	12-13	Ingress interface SNMP ifIndex
output	14-15	Egress interface SNMP ifIndex
dPkts	16-19	Packets in the flow
dOctets	20-23	Octets (bytes) in the flow
first	24-27	SysUptime at start of the flow
last	28-31	SysUptime at the time the last packet of the flow was received
srcport	32-33	Layer 4 source port number or equivalent
dstport	34-35	Layer 4 destination port number or equivalent
pad1	36	Unused (zero) byte
tcp_flags	37	Cumulative OR of TCP flags
prot	38	Layer 4 protocol (for example, 6=TCP, 17=UDP)
tos	39	IP type-of-service byte
src_as	40-41	Autonomous system number of the source, either origin or peer
dst_as	42-43	Autonomous system number of the destination, either origin or peer
src_mask	44	Source address prefix mask bits
dst_mask	45	Destination address prefix mask bits
pad2	46-47	Packet Assembler/Disassembler (PAD) 2 is unused (zero) bytes

KUVIO 10. NetFlow-version 5 Flow Recordin sisältö (Cisco Systems 2011c)

Flow record on 47 tavua pitkä, ja se sisältää useita tietoja flowsta. Ensimmäisenä ovat lähde- ja kohde-IP-osoitteet, joita seuraa IP-osoite, johon paketti seuraavaksi ohjataan. Seuraavana tiedoista löytyy sisään- ja ulostuloliitynnät, pakettien ja tavujen määrä kyseisessä flowssa sekä ajat, jolloin flow alkoi ja loppui. Flow recordista löytyy myös kohde- ja lähdeportit sekä TCP-lippujen tiedot, joiden jälkeen selviää kuljetuskerroksen protokolla sekä TOS-tavun sisältö. Flow recordin loppupuolella tavut 40-43 sisältävät lähde- ja kohde-AS-numerot, joiden jälkeen löytyy vielä lähde- ja kohdemaskit. Pad1- ja Pad2-kentät ovat käyttämättömiä eli ne sisältävät vain nollia. (Cisco Systems 2011c.)

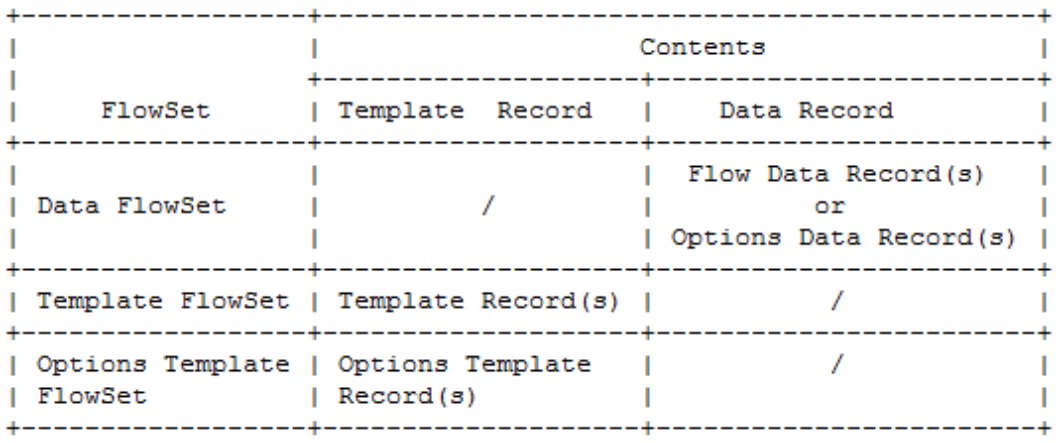
3.5.3 Version 9 FlowSetit

NetFlow-version 9 paketissa ensimmäisenä on otsikkotiedot, joista selviää esimerkiksi NetFlown versio sekä paketin sisältämien recordien eli tietueiden määrä. Otsikkotietojen jälkeen paketissa on FlowSet-osio. FlowSetit kuvaavat flow recordeja, joilla on samanlainen muoto. Erilaisia FlowSettejä on kolmenlaisia, jotka ovat Template FlowSet, Options Template FlowSet sekä Data FlowSet. Erilaiset FlowSetit tunnistetaan niissä olevilla ID-numeroilla. Template FlowSetillä ID-numerona on 0 ja Options Template FlowSetillä ID on 1. Data FlowSeteissä ID:n arvo on suurempi kuin 255. Paketti voi sisältää mitä tahansa FlowSet-tyyppejä. Kuviossa 11 nähdään NetFlow-paketti, joka sisältää kaikkia kolmea FlowSettiä. (RFC 3954 2004.)



KUVIO 11. NetFlow-versio 9 -paketti, joka sisältää erilaisia FlowSettejä (RFC 3954 2004)

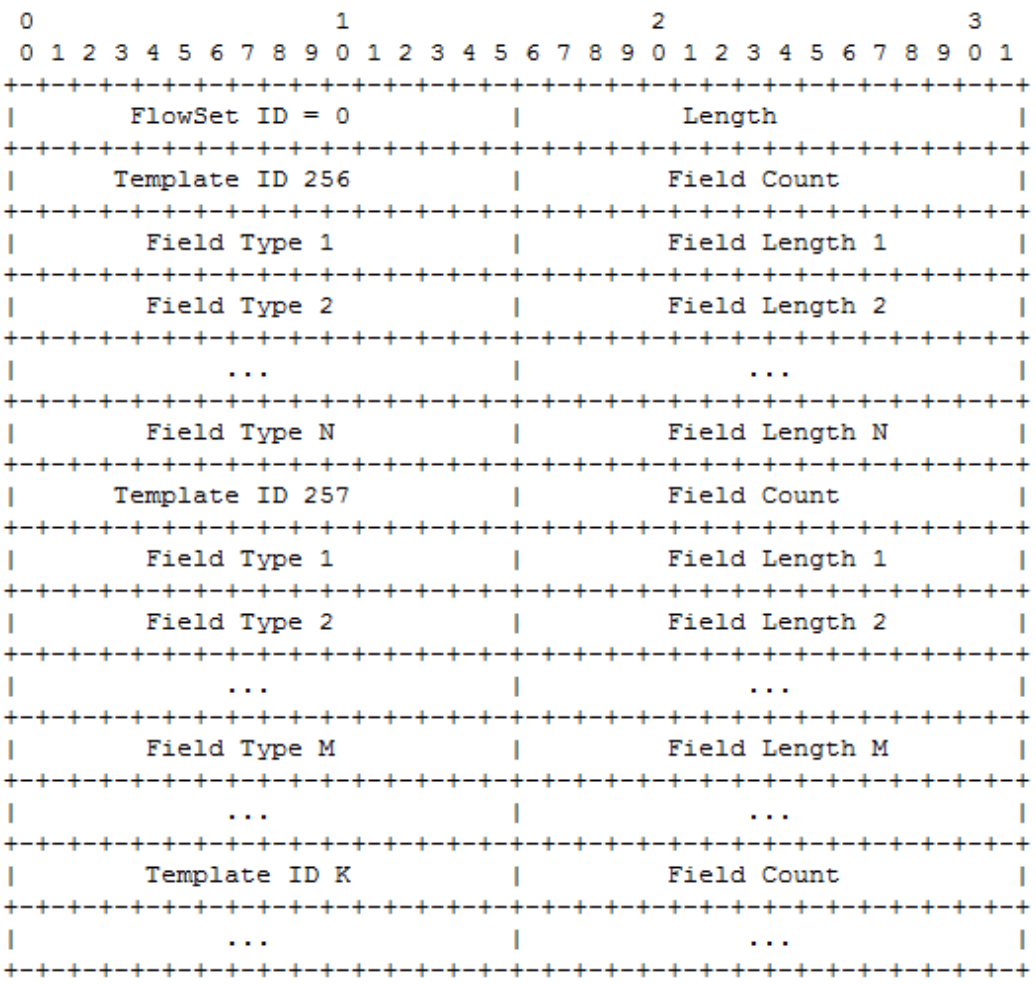
Data FlowSet sisältää recordeja. Se voi sisältää Flow Data Recordeja eli tietoja Flowsta tai Options Data Recordeja, jotka sisältävät arvoja flow-mittaukseen liittyen. Näiden recordien sisällöt määritellään mallipohjissa. Flow Data Recordien sisällöt määritellään Template Recordissa ja Options Data Recordien sisältö määritellään Options Template Recordeissa. Template FlowSetit sisältävät ainoastaan Template Recordeja, joilla määritellään Flow Data Recordien sisältö. Viimeinen FlowSet-tyyppi eli Options Template Flowset sisältää Options Template Recordeja, jotka sisältävät ohjeet Options Data Recordien tulkitsemiseen. Kuvio 12 havainnollistaa eri FlowSettien sisällöt. (RFC 3954 2004.)



KUVIO 12. Erilaisten FlowSettien sisällöt (RFC 3954 2004)

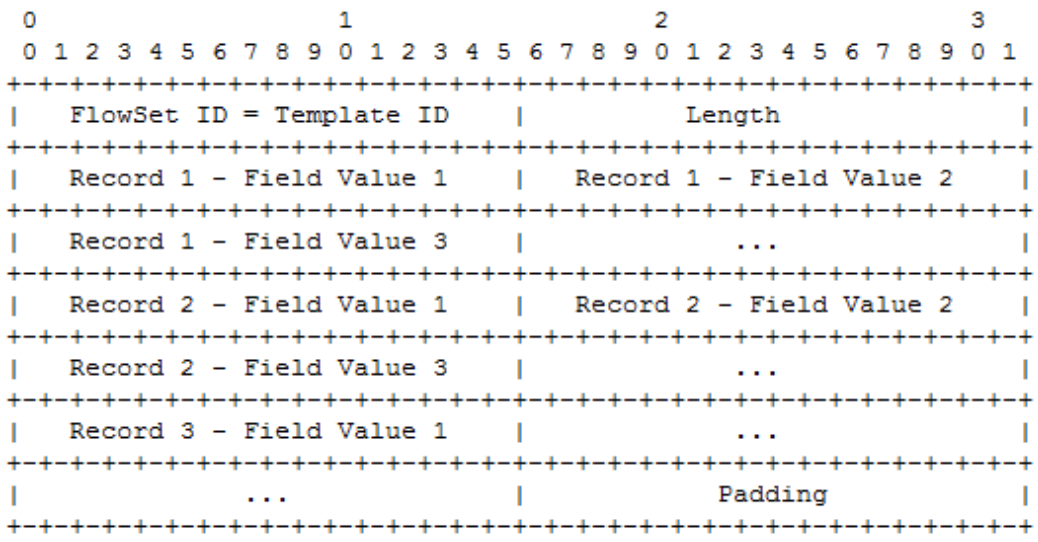
Seuraavaksi käydään läpi erilaisten FlowSettien sisällöt tarkemmin. Ensimmäisenä on vuorossa Template FlowSet. Sen rakenne voidaan nähdä kuviossa 13 ja sen eri kenttien selitykset ovat seuraavat:

- FlowSet ID - FlowSet ID -arvo 0 tarkoittaa Template FlowSettiä.
- Length - Tämän FlowSetin pituus, jolla tunnistetaan, milloin tämä FlowSet päättyy.
- Template ID - Uniikki tunnistenumero, jolla mallipohja tunnistetaan.
- Field Count - Kenttien määrä tässä mallipohjassa. Tällä tunnistetaan, milloin tämä Template Record päättyy ja seuraava alkaa.
- Field Type - Arvo, jolla tunnistetaan tämän kentän tyyppi. Nämä tyypit ja niiden tiedot ovat nähtävissä taulukossa 3.
- Field Lenght - Edellisen Field Typen määrittämän kentän pituus tavuina. (RFC 3954 2004.)



KUVIO 13. Template FlowSet (RFC 3954 2004)

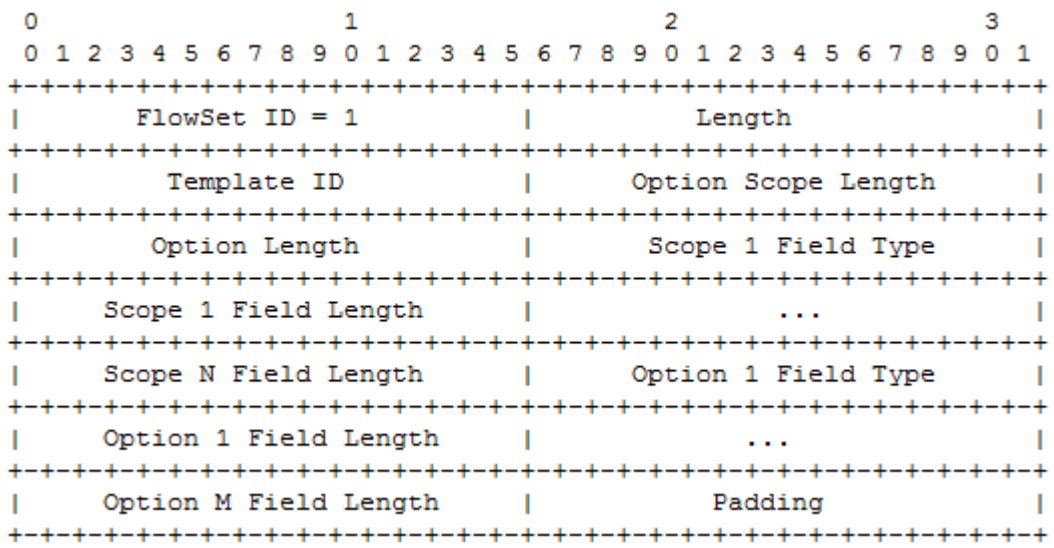
Kuviossa 14 nähdään, miltä näyttää Data FlowSet. Data FlowSetissä on vain neljänlaisia kenttiä, joista ensimmäinen on FlowSet ID, joka tarkoittaa Template ID:tä, jolla tunnistetaan mallipohja, jota käytetään kyseisen paketin flow recordien purkamiseen. Data FlowSettiä voidaan hyödyntää ainoastaan, kun siihen liittyvä mallipohja on jo tiedossa. Toinen kenttä eli Length kertoo tämän FlowSetin pituuden. Seuraavana ovat vuorossa flow recordien arvot. Template Recordissa on aikaisemmin määritelty näiden arvojen tyypit ja pituudet. Viimeisenä on kenttä nimeltä Padding, johon NetFlow-datan lähettäjä voi lisätä nollia ennen seuraavan FlowSetin alkua tasatakseen viestin pituutta. (RFC 3954 2004.)



KUVIO 14. Data FlowSet (RFC 3954 2004)

Options Template FlowSetillä (kuvio 15) ei ilmoiteta tietoja flow-tiedoista vaan sen ilmoittamat tiedot liittyvät NetFlown konfigurointiin verkon aktiivilaitteessa. Tällainen tieto voi olla esimerkiksi NetFlown näytteenottotaajuus. Näytteenotto-taajuudella voidaan säädellä sitä, kuinka usein paketteja tutkitaan, ja luodaan merkinnät NetFlow-välimuistiin (Cisco Systems 2007b). Seuraavaksi käydään läpi Options Template FlowSetin kenttien tiedot:

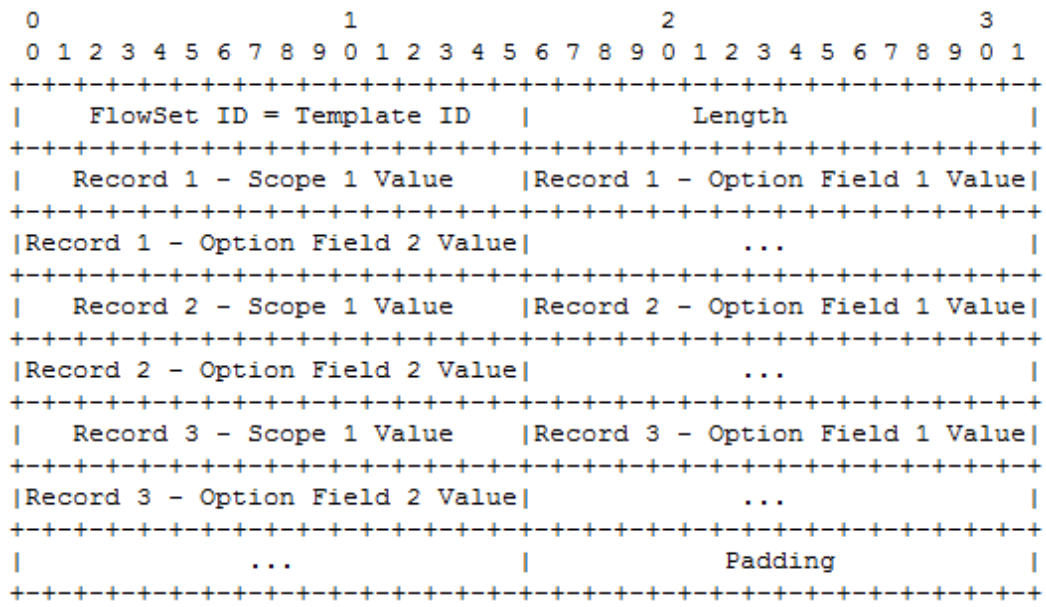
- FlowSet ID - Options Templaten ID on 1.
- Length - FlowSetin kokonaispituus.
- Template ID - Tämän mallipohjan ID-numero.
- Option Scope Lenght - Scope-kenttien pituus Options Template Record-issa.
- Option Length - Option-kenttien pituus Template Recordissa.
- Scope 1 Field Type - Tässä määritellään, mitä Options Template Record koskee. Esimerkkinä arvo 2, joka tarkoittaa liityntää.
- Scope 1 Field Lenght - Scope-kentän pituus Options Data Recordissa.
- Options 1 Field Type - Option-kentän tyyppi. Tyypit nähtävissä taulukossa 3.
- Option 1 Field Lenght - Option-kentän pituus.
- Padding - Tasausbittejä ennen seuraavan FlowSetin alkua.
  (RFC 3954 2004.)



KUVIO 15. Options Template FlowSet (RFC 3954 2004)

Options Data Recordit lähetetään Data FlowSeteissä. Näiden viestien lähetystiheys voidaan konfiguroida. Kuvio 16 näyttää Options Data Recordin formaatin. Eri kenttien selitykset ovat seuraavat:

- FlowSet ID = Template ID - Tällä numerolla yhdistetään nämä recordit oikeaan templateen, jossa eri kentät on selitetty.
- Length - Tämän FlowSetin pituus.
- Record ja Option - Nämä kentät sisältävät varsinaiset lähettävät tiedot, jotka on määritelty aikaisemmin Options Template FlowSetissä.
- Padding - Tasausbittejä.
  (RFC 3954 2004.)



KUVIO 16. Options Data Record (RFC 3954 2004)

Seuraava taulukko (taulukko 1) sisältää tietoja, joita FlowSeteissä pystytään ilmoittamaan flowsta. Kaikki laitteet eivät välttämättä pysty kertomaan kaikkia näitä tietoja. Uusia kenttätyyppejä käyttöönotettaessa paketin formaatti pysyy edelleen samana. Tiedot vain päivitetään NetFlow-lähteelle sekä kerääjälle. Taulukko ilmoittaa kentän, arvon, pituuden tavuina sekä selitteen. (RFC 3954 2004.)

TAULUKKO 1. Kenttien tyyppien määrittelyt (RFC 3954 2004)

Kentän tyyppi	**Arvo**	**Tavumäärä**	**Selitys**
IN_BYTES	1	N	Sisäänpäin tulevien tavujen määrä. N vakiona 4.
IN_PKTS	2	N	Sisäänpäin tulevien pakettien määrä. N vakiona 4.
FLOWS	3	N	Yhteenkerätty flowmäärä.
PROTOCOL	4	1	IP-paketin otsikon protocol-kenttä.
TOS	5	1	TOS-kentän arvo sisääntullessa.
TCP_FLAGS	6	1	TCP-lippujen tiedot.
L4_SRC_PORT	7	2	4-kerroksen lähdeportti.
IPV4_SRC_ADDR	8	4	IPv4-lähdeosoite.
SRC_MASK	9	1	Lähdeosoitteen maski.
INPUT_SNMP	10	N	Sisääntuloliitynnän numero. N vakiona 2.
L4_DST_PORT	11	2	4-kerroksen kohdeportti.
IPV4_DST_ADDR	12	4	IPv4-kohdeosoite.
DST_MASK	13	1	Kohdeosoitteen maski.
OUTPUT_SNMP	14	N	Ulosmenoliitynnän numero. N vakio-

			na 2.
IPV4_NEXT_HOP	15	4	Seuraavan hyppäyksen IP-osoite.
SRC_AS	16	N	Lähde BGP AS-numero. N vakiona 2.
DST_AS	17	N	Kohde BGP AS-numero. N vakiona 2.
BGP_IPV4_NEXT_HOP	18	4	Seuraavan hyppäyksen IPv4-osoite BGP-toimialueella.
MUL_DST_PKTS	19	N	Ulosmenevien multicast-pakettien määrä. N vakiona 4.
MUL_DST_BYTES	20	N	Ulosmenevien multicast-tavujen määrä. N vakiona 4.
LAST_SWITCHED	21	4	Flown viimeisen paketin sysUptime.
FIRST_SWITCHED	22	4	Flown ensimmäisen paketin sysUptime.
OUT_BYTES	23	N	Ulospäin menevien tavujen määrä. N vakiona 4.
OUT_PKTS	24	N	Ulospäin menevien pakettien määrä. N vakiona 4.
IPV6_SRC_ADDR	27	16	IPv6-lähdeosoite.
IPV6_DST_ADDR	28	16	IPv6-kohdeosoite.
IPV6_SRC_MASK	29	1	IPv6-lähdemaski.
IPV6_DST_MASK	30	1	IPv6-kohdemaski.
IPV6_FLOW_LABEL	31	3	IPv6-Flowtunniste.
ICMP_TYPE	32	2	ICMP-paketin tyyppi.
MUL_IGMP_TYPE	33	1	IGMP-paketin tyyppi.
SAMPLING_INTERVAL	34	4	NetFlown näytteenottotaajuus.
SAMPLING_ALGORITHM	35	1	Näytteenottotapa.
FLOW_ACTIVE_TIMEOT	36	2	Aktiivisen flown aikakatkaisun aika sekunteina.
FLOW_INACTIVE_TIMEOUT	37	2	Passiivisen flown aikakatkaisun aika sekunteina.
ENGINE_TYPE	38	1	Flown ohjausmoottorin tyyppi.
ENGINE_ID	39	1	Flown ohjausmoottorin ID-numero.
TOTAL_BYTES_EXP	40	N	NetFlow-laitteen lähettämien tavujen määrä. N vakiona 4.
TOTAL_PKTS_EXP	41	N	NetFlow-laitteen lähettämien pakettien määrä. N vakiona 4.
TOTAL_FLOWS_EXP	42	N	NetFlow-laitteen lähettämä flow-määrä. N vakiona 4.
MPLS_TOP_LABEL_TYPE	46	1	Päällimmäisen MPLS-tunnisteen tyyppi.
MPLS_TOP_LABEL_IP_ADDR	47	4	Päällimmäiseen MPLS-tunnisteeseen liittyvä FEC.
FLOW_SAMPLER_ID	48	1	Flow Sampler tunniste.
FLOW_SAMPLER_MODE	49	1	Algoritmin tyyppi näytteenottoon liittyen.
FLOW_SAMPLER_RANDOM_INTERVAL	50	4	Näytteenottotaajuus.
DST_TOS	55	1	TOS-kentän arvo ulosmentäessä.

SRC_MAC	56	6	Lähde-MAC-osoite.
DST_MAC	57	6	Kohde-MAC-osoite.
SRC_VLAN	58	2	Lähde-VLAN.
DST_VLAN	59	2	Kohde-VLAN.
IP_PROTOCOL_VERSION	60	1	IP-protokollan versio.
DIRECTION	61	1	Flown suunta eli sisään vai ulos (ingress - egress).
IPV6_NEXT_HOP	62	16	Seuraavan hypyn IPv6-osoite.
BGP_IPV6_NEXT_HOP	63	16	Seuraava reititin BGP-toimialueella.
IPV6_OPTION_HEADERS	64	4	IPv6-paketin Option-kentän arvot.
MPLS_LABEL_1	70	3	MPLS-pinon 1. tunniste
MPLS_LABEL_2	71	3	MPLS-pinon 2. tunniste
MPLS_LABEL_3	72	3	MPLS-pinon 3. tunniste
MPLS_LABEL_4	73	3	MPLS-pinon 4. tunniste
MPLS_LABEL_5	74	3	MPLS-pinon 5. tunniste
MPLS_LABEL_6	75	3	MPLS-pinon 6. tunniste
MPLS_LABEL_7	76	3	MPLS-pinon 7. tunniste
MPLS_LABEL_8	77	3	MPLS-pinon 8. tunniste
MPLS_LABEL_9	78	3	MPLS-pinon 9. tunniste
MPLS_LABEL_10	79	3	MPLS-pinon 10. tunniste

3.6 NetFlow-datan analysointi

NetFlow-dataa analysoimalla on mahdollista selvittää useita asioita verkkoliikenteeseen liittyen ja saada vastauksia verkkoon liittyviin ongelmiin. NetFlow-datan avulla voidaan havaita sovelluksia sekä käyttäjiä, jotka vievät eniten kaistaa verkosta. Verkon ruuhkauttajien lisäksi NetFlow-sovelluksien avulla voidaan esimerkiksi havaita poikkeavuuksia verkkoliikenteessä, kuten DoS-hyökkäyksiä. NetFlown avulla on myös mahdollista tarkkailla QoS-parametreja eli palvelunlaatua ja näin ollen varmistua oikeanlaisesta kaistanjaosta. (Cisco Systems 2007a.)

Yksittäisiä flow-tietoja tutkimalla saadaan tietoa yksittäisistä yhteyksistä. Näin nähdään, mistä liikenne on peräisin, kuka on sen vastaanottaja ja mitä sovellusta käytetään. Muita mahdollisia selville saatavia tietoja yksittäisistä yhteyksistä ovat myös esimerkiksi flown kesto ja siirretty datamäärä. (Cisco Systems 2007a.)

NetFlow-dataa päästään analysoimaan kahdella tavalla. Näistä ensimmäinen tapa on lukea NetFlow-dataa suoraan reitittimellä, jossa flow-tietoja kerätään. Tämä tapahtuu show-komennoilla. Komennolla *show ip cache flow* päästään tutkimaan

NetFlow-välimuistissa olevia tietoja. Lisäämällä komentoon sanan verbose eli *show ip cache verbose flow*, nähdään vielä lisätietoja NetFlow-dataan liittyen. Toinen tapa datan analysoimiseen on ottaa käyttöön NetFlow-datan kerääjä, joka kokoaa saamansa datan ja tarjoaa raportteja analysoitavaksi. (Cisco Systems 2007a; Cisco Systems 2011d.)

3.7 Aktiivilaitteiden konfigurointi

Useat Ciscon laitteet tukevat NetFlowta. NetFlown perustoiminnot eivät ole vaikeita konfiguroida laitteeseen. NetFlow konfiguroidaan käyttöön johonkin liityntään. Liitynnän liikenne kerätään NetFlow-välimuistiin, minkä jälkeen tiedot on mahdollista lähettää NetFlow-keräimelle. Kuviosta 17 nähdään Ciscon eri sarjojen laitteita ja niiden NetFlow-tuki. Useat laitteiden sarjat tukevat NetFlowta, joten on todennäköistä, että NetFlow on käytettävissä verkon laitteissa. Poikkeuksena ovat sarjojen 2900, 3500, 3660 sekä 3750 laitteet. (Cisco Systems 2007a.)

Device	Supported
Cisco 800, 1700, 2600	Yes
Cisco 1800, 2800, 3800	Yes
Cisco 4500	Yes
Cisco 6500	Yes
Cisco7200, 7300, 7500	Yes
Cisco 7600	Yes
Cisco 10000, 12000, CRS-1	Yes
Cisco 2900, 3500, 3660, 3750	No

KUVIO 17. NetFlow-tuki Ciscon laitteissa (Cisco Systems 2007a)

Seuraavilla komennoilla saadaan NetFlow käyttöön halutussa liitynnässä ja NetFlow-tiedot lähtemään kohti NetFlow-keräintä. Ensimmäinen komento eli *ip cef* vaaditaan NetFlown käyttöönoton kannalta. Laitteessa tulee olla käytössä joko CEF eli Cisco Express Forwarding, dCEF eli distriputed CEF tai fast switching, jotka kaikki liittyvät pakettien nopeampaan ohjaamiseen portista toiseen. Seuraa-

vat kaksi komentoa liittyvät NetFlown käyttöönottoon eli flow-tietojen kaappaamiseen välimuistiin. Komennolla *interface* mennään halutun liitynnän alle, jossa NetFlow on tarkoitus ottaa käyttöön. Liitynnän alla annetaan komento *ip flow ingress* tai *egress*. Ingress viittaa siihen, että flow-tiedot kaapataan porttiin sisään tulevasta liikenteestä, kun taas egress-komento kaappaa tiedot portista ulos lähtevästä liikenteestä. Joissain IOS-versioissa on käytössä komento *ip route cache flow*, jolla flow-tiedot kaapataan porttiin sisään tulevasta liikenteestä. Viimeiset kaksi komentoa liittyvät NetFlow-tietojen lähettämiseen kohti kerääjää. *Ip flow-export version* -komennolla otetaan käyttöön NetFlow-tietojen lähetys ja samalla komennolla määritetään myös käytettävä NetFlow-versio. Viimeisellä komennolla valitaan vielä, mihin IP-osoitteeseen tiedot lähetetään ja mitä porttia kerääjä kuuntelee. (Cisco Systems 2007a; Cisco Systems 2008.)

Peruskomennot NetFlown käyttöönottamiseksi:

Router(config)# ip cef
Router(config)# interface *liitynnän tyyppi liitynnän numero*
Router(config-if)# ip flow ingress/egress tai route cache flow
Router(config)# ip flow-export version *numero*
Router(config)# ip flow-export destination *IP-osoite porttinumero*
(Cisco Systems 2007a; Cisco Systems 2008).

Cisco Catalyst 6500 -sarjan laitteissa NetFlow voidaan ottaa käyttöön rautapohjaisesti tai ohjelmistopohjaisesti. Ohjelmistopohjainen NetFlow kerää tietoa jokaisesta flowsta, joka ohjataan RP:n eli Route Processorin kautta. Rautapohjainen NetFlow taas kerää flowt, joiden ohjaus tapahtuu ilman RP:tä. Lähes kaikki ohjaus tapahtuu rautapohjaisesti 6500-sarjan laitteissa. MSFC:n (Multilayer Switch Feature Card) sisältämä NetFlow kerää tietoa ohjelmistopohjaisesti ja PFC:n (Policy Feature Card) keräämiä tietoja kutsutaan rautapohjaiseksi NetFlowksi. Ohjelmistopohjaisen NetFlown käyttöönottokomennot ovat samanlaisia, kuin aikaisemmin luetellut komennot. Rautapohjaisen NetFlown komennot ovat mls-alkuisia komentoja, joita on muutamia nähtävissä taulukossa 2. Osa taulukon komennoista ovat vapaavalintaisia eli ne eivät ole pakollisia NetFlown käyttöönoton kannalta. Mls-komennoilla käyttöön otettu NetFlow on käytössä kaikissa liitynnöissä. Ip flow-export -komennolla lähetetään sekä rauta- että ohjelmistopohjaiset

NetFlow-tiedot kerääjälle. (Cisco Systems 2011g; Cisco Systems 2006; Cisco Systems 2007a.)

TAULUKKO 2. Muutamia mls-komentoja (Cisco Systems 2006; Cisco Systems 2011e; Cisco Systems 2011h)

Komento	**Selitys**
mls netflow	NetFlow käyttöön PFC:ssä eli rautapohjainen NetFlow päälle.
mls flow ip *maski*	Valitaan flow-maski eli kuinka tarkasti flowt otetaan talteen. Komennon perään siis annetaan Flow-maskit-taulukosta (taulukko 3) haluttu flow-maski.
mls nde sender version *numero*	Valitaan käytettävä NetFlown versio. Tällä komennolla valitaan, mitä NetFlown versiota käytetään, kun flow recordit lähetetään kerääjälle. Kerääjän täytyy tukea käytettävää versiota.
mls sampling time-based/packet-based *tiheys*	(Vapaavalintainen komento) Ottaa käyttöön näytteistetyn NetFlown. Perusasetuksilla flown jokaisen paketin tiedot otetaan talteen. Tällä komennolla vain osasta flowta otetaan näytteitä. Näytteistys voidaan tehdä ajan mukaan tai pakettien mukaan eli yksi näyte tietyn ajan kuluttua tai yksi näyte tietyn pakettimäärän kuluttua. Käytettävät tiheysarvot: 64, 128, 256, 512, 1024, 2048, 4096, 8192.
mls aging long *arvo*	(Vapaavalintainen komento) Valitaan aika, jolloin pitkäaikaiset flowt poistetaan välimuistista ja lähetetään kerääjälle. Näin flowsta saadaan tietoa kerääjälle vaikka se on vielä aktiivinen. Perusasetuksilla aikana on 32 minuuttia.
mls aging normal *arvo*	(Vapaavalintainen komento) Tällä komennolla määritellään aika, jonka jälkeen ei-aktiivinen flow vanhenee ja se poistetaan välimuistista. Perusasetuksilla aikana on viisi minuuttia.
mls nde flow include/exclude	(Vapaavalintainen komento) Tätä komentoa käyttämällä voidaan tehdä filttereitä, jotka määrittelevät, mitkä flowt lähetetään kerääjälle. Include tai exclude valitaan sen mukaan, halutaanko filtterillä ottaa mukaan vai ohittaa flow. Vain yksi filtteri voi olla käytössä kerrallaan. Komennon loppuun tehdään halutut määritykset lisäämällä dest-port *numero*, src-port *numero*, protocol tcp/udp, destination *ip-osoite maski* tai source *ip-osoite maski*.
mls nde interface	(Vapaavalintainen komento) Lisätään lisätietoja flowsta flow recordiin. Lisätiedot: reitityksessä seuraavana oleva IP-osoite, ulosmenoliitynnän numero ja BGP AS-numero. Ilman tätä komentoa edelle mainitut tiedot eivät välity kerääjälle NetFlow-datan mukana.

6500-sarjassa käytetään myös NetFlown yhteydessä flow-maskeja, joilla voidaan määritellä, miten tarkasti flow-tiedot kerätään välimuistiin. Flow-maskeja on kuusi erilaista, jotka nähdään taulukossa 3. Flow-maski voidaan valita sen mukaan, kuinka tarkasti flow-tiedot halutaan erotella välimuistiin. (Cisco Systems 2006.)

TAULUKKO 3. Flow-maskit (Cisco Systems 2006)

Flow-maski	**Selitys**
source-only	NetFlow-välimuistiin merkitään flowt lähdeosoitteen mukaan. Tämä ja destination-maski ovat epätarkimmat flow-maskit.
destination	NetFlow-välimuistiin merkitään flowt kohdeosoitteen mukaan.
destination-source	Flow-merkintä muodostetaan välimuistiin jokaista lähde-kohdeosoiteparia kohden.
destination-source-interface	Lisää yllä olevaan maskiin tiedon VLAN-liitynnästä.
full	Joka IP-flowlle oma merkintänsä. Flowt erotellaan käyttäen lähde- ja kohdeosoitteita, protokollaa sekä porttinumeroita.
full-interface	Tämä on tarkin flowmaski, joka sisältää samat tiedot kuin full-maski, mutta siihen on lisätty vielä VLAN-tieto.

3.8 NetFlow-sovellukset

Cisco on kehittänyt NetFlown, ja siltä on saatavilla NetFlow-dataa varten sovelluksia, mutta myös muilla valmistajilla on tarjolla NetFlow-sovelluksia. NetFlow-dataa hyödyntäviä sovelluksia on kaupallisia sekä ilmaisia. Sovelluksia on saatavilla eri käyttöjärjestelmille, kuten Linuxille ja Windowsille. Sovelluksien hinnat vaihtelevat melko paljon eri valmistajilla. (Cisco Systems 2007a.)

NetFlow-sovellusta valittaessa on syytä ottaa huomioon muutamia asioita. Hinnan lisäksi ratkaisevia asioita voivat olla esimerkiksi käyttöjärjestelmä tai pääkäyttötarkoitus, joka voi olla esimerkiksi eri sovelluksien ja käyttäjien tarkkailu tai verkon suorituskyvyn mittaaminen ja suunnittelu. On myös hyödyllistä tarkistaa, onko jo käytössä olevia verkonvalvontasovelluksia mahdollista laajentaa käyttämään myös NetFlow-dataa. (Cisco Systems 2007a.)

Kuvio 18 sisältää kaupallisia NetFlow-sovelluksia. Kuten listasta nähdään, niin vaikka NetFlow on Ciscon kehittämä protokolla, niin useat eri valmistajat ovat tuoneet markkinoille NetFlow-dataa hyödyntäviä sovelluksia. Pääkäyttötarkoitus, pääkäyttäjä, käyttöjärjestelmä sekä hinta vaihtelevat sovelluksen mukaan. Sovelluksella voi olla pääkäyttötarkoituksena esimerkiksi verkkoliikenteen analysointi, laskutus tai turvallisuuteen liittyvä tarkkailu. Primary User eli pääkäyttäjällä tarkoitetaan, onko tuote suunnattu erikokoisille yrityksille tai esimerkiksi palveluntarjoajille. Kuviosta 18 selviää myös, että kaupallisia sovelluksia on saatavilla useille eri käyttöjärjestelmille, kuten esimerkiksi Windowsille, Linuxille sekä So-

larikselle. Kaupallisten sovelluksien hinnat vaihtelevat melko paljon, ja ne on kuviossa luokiteltu kolmeen luokkaan, joista ensimmäinen on Low, jossa hinta on alle 7500 dollaria. Medium-hinta on 7500-25000 dollaria ja High-hinta yli 25000 dollaria. (Cisco Systems 2007a.)

Product Name	Primary Use	Primary User	Operating System	Starting Price Range
Cisco NetFlow Collector	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	Medium
Cisco CS-Mars	Security Monitoring	Enterprise, SMB	Linux	Medium
AdventNet	Traffic Analysis	Enterprise, SMB	Windows	Low
Apoapsis	Traffic Analysis	Enterprise	Linux	Medium
Arbor Networks	Traffic/Security Analysis	Enterprise, Service Provider	BSD	High
Caligare	Traffic/Security Analysis	Enterprise, Service Provider	Linux	Medium
Fluke Networks	Traffic Analysis	Enterprise, SMB	Windows	Medium
CA Software[1]	Traffic Analysis	Enterprise, Service Provider	Windows	High
Evident Software[1]	Traffic Analysis, Billing	Enterprise	Linux	High
HP[1]	Traffic Analysis	Enterprise, Service Provider	Linux, Solaris	High
IBM Aurora	Traffic Analysis/Security	Enterprise, Service Provider	Linux	Medium
IdeaData	Traffic Analysis	Enterprise	Windows/Linux	Medium
InfoVista	Traffic Analysis	Enterprise, Service Provider	Windows	High
IsarNet	Traffic Analysis	Enterprise, Service Provider	Linux	Medium
Lancope	Traffic/Security Analysis	Enterprise, Service Provider	Linux	High
Micromuse[1]	Traffic Analysis	Enterprise, Service Provider	Solaris	High
NetQoS	Traffic/Security Analysis	Enterprise	Windows	High
Valencia Systems	Traffic Analysis	Enterprise	Windows	High
Solarwinds	Traffic Analysis	Enterprise, SMB	Windows	Low
Wired City	Traffic Analysis	Enterprise	Windows	High

[1]Uses Cisco NetFlow Collector

KUVIO 18. Kaupallisia NetFlow-sovelluksia (Cisco Systems 2007a)

Kuten jo aikaisemmin mainittiin, kaupallisten NetFlow-sovelluksien lisäksi on saatavilla ilmaisia NetFlow-sovelluksia. Näitä ilmaisia sovelluksia eli freeware-sovelluksia on nähtävillä kuviossa 19. Kuvio kertoo sovelluksen nimen lisäksi pääkäyttötarkoituksen, käyttöjärjestelmän sekä lisätietoja muutamista sovelluksista. (Cisco Systems 2007a.)

Product Name	Primary Use	Comment	Operating System
CFlowd	Traffic Analysis	No longer supported	Unix
Flow-tools	Collector Device	Scalable	Unix
Flowd	Collector Device	Supports V9	BSD, Linux
FlowScan	Reporting for Flow-Tools		Unix
IPFlow	Traffic Analysis	Support V9, IPv4, IPv6,MPLS, SCTP, etc.	Linux, FreeBSD, Solaris
NetFlow Guide	Reporting Tools		BSD, Linux
NetFlow Monitor	Traffic Analysis	Supports V9	Linux
NTOP	Collector Device	Supports V9	Unix
Panoptis	Security Monitoring		Unix
Stager	Reporting for Flow-Tools		Unix

KUVIO 19. Ilmaisia NetFlow-sovelluksia (Cisco Systems 2007a)

Kuvioista 18 ja 19 nähdään, että NetFlow-dataa käyttäviä sovelluksia on saatavilla useita sekä kaupallisina että ilmaisina sovelluksina. Ilmaisia ja kaupallisia on saatavilla eri pääkäyttötarkoitukseen. Ilmaisista sovelluksista osa toimii vain kerääjäsovelluksena, joka nähdään listalla nimellä Collector Device. Näitä sovelluksia varten voidaan asentaa sovellus, joka muodostaa raportteja kerääjän keräämästä datasta. Esimerkiksi Stager ja FlowScan käyttävät Flow-toolsin keräämää dataa. Kuvioiden mukaan yksi suuri ero ilmaisten ja kaupallisten välillä on käyttöjärjestelmässä, sillä ilmaisten listalla ei näy yhtään Windows-käyttöjärjestelmälle olevaa sovellusta. Sen sijaan ilmaisia Unix/Linux-sovelluksia on saatavilla useita. (Cisco Systems 2007a.)

3.9 NetFlow ja SNMP -vertailu

SNMP:tä ja NetFlowta pystytään kumpaakin käyttämään liikennemäärien mittaamiseen. SNMP:n avulla nähdään, kuinka paljon verkkoliittymän kaistaa käytetään, minkä avulla voidaan esimerkiksi päätellä, onko kaistanleveys riittävä. Ongelma tässä tapauksessa ei kuitenkaan välttämättä ole kaistanleveyden riittämättömyys, vaan nykyistä kaistaa saatetaan väärinkäyttää. (Patterson 2010a.)

SNMP ei kerro, kuka tai mikä aiheuttaa verkkoon suuren määrän liikennettä. Tähän tehtävään tarvitaan NetFlowta, jonka avulla saatujen tietojen avulla voidaan

selvittää kaistan käyttäjät. SNMP voi kyllä kertoa tietoja tavumääristä sekä bittinopeuksista eri liitynnöissä, mutta enempää sen avulla ei saada liikenteestä selville, joten tärkeitä kysymyksiä jää ilman vastauksia. NetFlow tarjoaa vastauksia, joiden avulla selviää esimerkiksi liikenteen lähde ja kohde sekä sovellus. (Patterson 2010a; Jacob 2010.)

Yksi ero näiden protokollien välillä on myös niiden yleinen toimintaperiaate. SNMP perustuu siihen, että valvontasovellukset käyvät kyselemässä tietoja eri laitteilta niiden MIB-tauluista, minkä jälkeen laite lähettää vastaukset valvontasovellukselle. NetFlow taas perustuu kyselyiden sijasta siihen, että data kulkee ainoastaan NetFlow-lähteeltä kohti NetFlow-kerääjää. (Jacob 2010.)

SNMP on reaaliaikaisempi kuin NetFlow, sillä SNMP:llä kyselyjä voidaan tehdä vaikka jokainen sekunti. NetFlowssa reaaliaikaisuutta voidaan parantaa säätämällä aktiivisen flown katkaisuaikaa. NetFlowlla lähetetty data sisältää enemmän tietoa kuin SNMP-viestit, joten NetFlowlla kerätyt historiatiedot kuluttavat enemmän kovalevytilaa kuin SNMP-data. SNMP mahdollistaa myös esimerkiksi prosessorin ja muistin käytön mittaamisen. Ainakaan vielä NetFlowlla tämä ei ole mahdollista. (Patterson 2010b.)

Yhdistävä tekijä näiden kahden protokollan välillä on NetFlow MIB. Tämän avulla NetFlow-tietoja voidaan lukea käyttäen SNMP-protokollaa. Tällöin NetFlow konfiguroidaan päälle reitittimessä, mutta sitä ei tarvitse asettaa lähettämään NetFlow-dataa minnekään, vaan NetFlow-välimuistiin päästään käsiksi SNMP:n avulla. Tämä on hyödyllinen tapa tutkia NetFlow-dataa, jos NetFlow-kerääjää ei ole mahdollista käyttää, mutta tällä tapaa tietoa on saatavilla vain rajoitetusti. (Cisco Systems 2011f.)

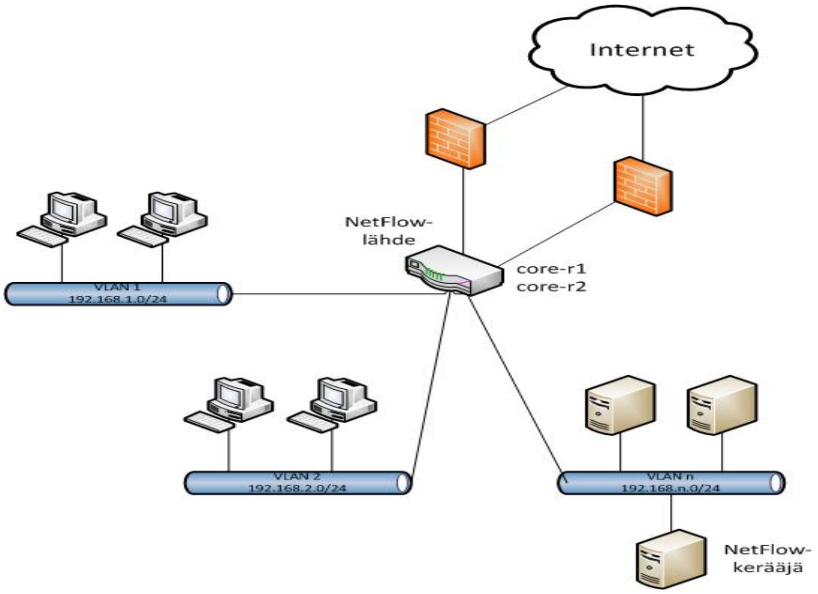
Lähitulevaisuudessa on nähtävissä vielä sekä SNMP:n että NetFlown käyttöä. NetFlown kehittyessä on kuitenkin mahdollista, että se korvaa joitakin SNMP:n toimintoja. (Patterson 2010a.)

4 NETFLOWN KÄYTTÖÖNOTTO PHKK:N VERKOSSA

4.1 Ympäristön kuvaus

Tavoitteena oli testata ja mahdollisesti ottaa käyttöön NetFlowlla toteutettu verkonvalvonta PHKK:n sisäverkossa. PHKK:n sisäverkko sisältää useita erilaisia eri tarkoitukseen asennettuja aktiivilaitteita. Verkosta löytyy mm. kytkimiä, reitittimiä, palomuureja sekä langattomia tukiasemia. Verkko sisältää suuren määrän eri VLAN-verkkoja, joiden liikennettä haluttiin tarkkailla NetFlowlla. Kaikki VLAN-verkkojen liikenne menee keskusreittimen läpi. Keskusreititin on kahdennettu vikasietoisuuden takaamiseksi, mikä tarkoittaa sitä, että mikäli keskusreititin vikaantuu, niin toinen reititin jatkaa toimintaa ja takaa verkon toimivuuden. Keskusreittimien ja ulkoisten verkkojen välillä on ainoastaan Cisco ASA -palomuuri. Keskusreitittimien jälkeen sisäverkossa on suuri määrä toimipistekohtaisia kytkimiä ja tukiasemia.

NetFlow-dataa haluttiin kerätä pisteestä, jonka läpi suuri määrä verkkoliikenteestä kulkee. Niinpä NetFlow päätettiin ottaa käyttöön keskusreitittimissä, joiden läpi kaikki VLAN-verkkojen liikenne kulkee liikuttaessa ulkoverkkoihin sekä VLAN-verkkojen välillä. Kuviosta 20 nähdään PHKK:n verkon looginen kuva, jossa erottuvat eri VLAN-verkot, NetFlow-lähde ja -keräin sekä yhteys ulkoverkkoihin.



KUVIO 20. PHKK:n looginen verkkokuva

4.2 Testisovellukset

NetFlown testaamista varten valittiin kaksi sovellusta. Tarkoituksena oli testata kahta eri käyttöjärjestelmällä toimivaa sovellusta. Lisäksi haluttiin, että ensimmäinen sovelluksista on ilmainen ja toinen on kaupallinen eli maksullinen. Testisovelluksiksi valittiin NfSen ja Orion NetFlow Traffic Analyzer.

NfSen on avoimen lähdekoodin ohjelma, joka toimii Linux/Unix-käyttöjärjestelmissä. NfSen itsessään on ainoastaan graafinen selaimella käytettävä sovellus, joka tarjoaa käyttäjälle nähtäväksi NetFlow-datan, jonka NfDump työkalu on kerännyt. NfSen vaatii toimiakseen Linux/Unix-käyttöjärjestelmän, johon on asennettu PHP ja Perl, sillä NfSen on kirjoitettu näillä ohjelmointikielillä. NfSenissä on mahdollista tehdä eräänlaisia hälytyksiä, jotka vaativat toimiakseen vielä muutaman lisämoduulin Perliin. RRD tool on myös pakollinen NfSeniä varten, sillä sen avulla graafit piirtyvät NfSeniin. (Haag & Jändling 2011; NfSen - Netflow sensor 2011.)

NfDump on myös pakollinen NfSenin kannalta, sillä se kerää ja käsittelee kaiken NetFlow-datan. NfDump tukee NetFlown versioita 5, 7 ja 9. NfSen ja NfDump ovat vapaasti ladattavissa Internetissä. (NFDUMP 2011.)

Toiseksi testattavaksi sovellukseksi valittiin SolarWindsin valmistama Orion NetFlow Traffic Analyzer eli lyhennettynä Orion NTA. Se on NetFlow-datan analysointia varten tehty sovellus, jolla on myös mahdollista käsitellä muiden valmistajien NetFlown tyylisiä protokollia, joista esimerkkinä Juniper J-Flow. NTA tukee NetFlown versioita 5 ja 9. NTA on lisämoduuli Orion Network Performance Monitoriin eli se täytyy hankkia, jotta NTA:ta voidaan käyttää. NPM ja NTA ovat maksullisia, mutta niistä on ladattavissa ilmaiset kokeiluversiot, joilla testaus voitiin suorittaa. NPM ja NTA on lisensoitu valvottavien elementtien mukaan. Halvin on 100 elementin lisenssi, joka mahdollistaa esimerkiksi 100 laitteen valvonnan. NTA:n lisenssin täytyy täsmätä NPM:n lisenssiin eli jos ostetaan 100 elementin NPM lisenssi hintaan 2015€ ja halutaan siihen NetFlow-tuki, niin siihen täytyy ostaa 100 elementin NTA lisenssi, joka maksaa 1465€. (SolarWinds 2011.)

Käyttöjärjestelmävaatimuksena NPM:llä ja NTA:lla on Windows Server 2003 tai 2008, johon on asennettu IIS sekä SQL Server 2005 tai 2008. Lisävaatimuksena ovat 3,0 GHz:n prosessori, 20 Gt kovalevytilaa sekä 3 Gt keskusmuistia. (Solar-Winds 2010.)

4.3 NetFlown asennus ja konfigurointi

4.3.1 NfSen-asennus

NfSeniä varten asennettiin PHKK:n Tietohallinnon tiloissa testikoneelle Fedora 13 -käyttöjärjestelmä oletusasetuksin. Koneen verkkokortille annettiin staattinen IP-osoite ja palomuuriin tehtiin ennakoidusti muutamia muutoksia. Koska NfSeniä käytetään selaimen kautta, niin palomuuriin avattiin TCP-portti 80. NetFlow-dataa varten avattiin UDP-portti 9997 sekä lisäksi SSH-yhteys sallittiin vain tietystä verkosta. UDP-portti 9997 avattiin sisääntulevalle liikenteelle ainoastaan tietystä IP-verkosta, jossa sijaitsivat reitittimet, joista NetFlow-dataa oli tarkoitus kerätä. NTP-palvelu asennettiin, jotta käyttöjärjestelmän aika pysyisi tarkkana. NTP-palvelulle kerrottiin kolme PHKK:n omaa NTP-palvelinta, joita käytetään ajan synkronointiin. Lisäksi tietokoneen oma kello päivitettiin käyttöjärjestelmän kellonaikaan komennolla *hwclock --systohc* ja tämä komento lisättiin suoritettavaksi päivittäin.

Käyttöjärjestelmän asennuksen jälkeen päästiin aloittamaan NfSenin asentaminen. NfSenin asennus suoritettiin SSH-yhteyden yli toiselta koneelta käskyttäen. NfSen ja sen vaatima NfDump haettiin wget-työkalulla Internetistä eli komennolla *wget ”www-osoite”*, minkä jälkeen nämä paketit purettiin tar-työkalulla komennolla *tar -zxf polku*. NfSen vaatii toimiakseen myös PHP:n, Perlin, muutaman Perl-moduulin sekä RRD-toolsin. RRD-tools saatiin asennettua yum-työkalulla komennoilla *yum install rrdtool.i686* ja *yum install rrdtool-devel.i686*. PHP ja Perl olivat joko valmiiksi asennettuina tai ne asentuivat muiden asennuksien yhteydessä. Perliin asennettiin vielä MailTools-moduuli komennolla *yum install perl-MailTools.noarch* . NfDump asennettiin komennoilla *./configure --prefix=/usr/local/nfdump-1.6.2 --enable-nfprofile, make* ja *make install*.

Ennen NfSenin asennusta sen mukana tullutta konfigurointitiedostoa muokattiin omien tarpeiden mukaan. Tätä varten mukana tulleesta konfigurointitiedostosta tehdään kopio komennolla *cp nfsen-dist.conf nfsen.conf*, jota voidaan muokata vaikka nano-työkalulla komennolla *nano nfsen.conf*. Tässä tiedostossa määriteltiin NfSeniin liittyviä asetuksia, kuten asennuskansioiden polut sekä käyttäjiin liittyviä määrityksiä. Lisäksi tähän tiedostoon voitiin määritellä jo ennen asentamista NetFlow-lähteet. Tähän tiedostoon kerrottiin kummankin keskusreitittimen IP-osoitteet sekä porttinumero 9997, johon NetFlow dataa saapuu. Näille NetFlow-lähteille annettiin nimet core-r1 ja core-r2. NfSeniä varten luotiin myös netflow-niminen käyttäjä komennolla *useradd -g apache netflow*, joka myös kerrottiin ennen asentamista konfigurointitiedostossa. Ennen asentamista luotiin vielä kansio, joka aikaisemmin määriteltiin konfigurointitiedostossa. Tämä tehtiin komennolla *mkdir -p /home/data/nfsen*. Tämän jälkeen NfSen voitiin asentaa komennolla *./install.pl etc/nfsen.conf*. Seuraavilla riveillä on nähtävissä konfigurointitiedoston kohdat, joihin kiinnitettiin huomiota ja joita muokattiin:

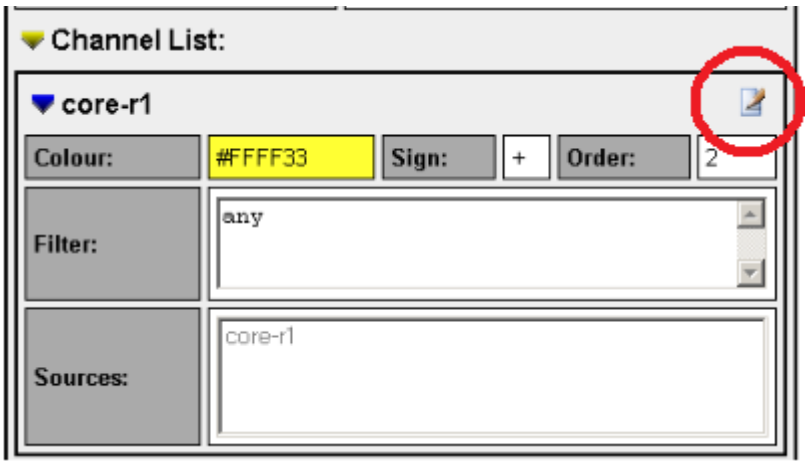
```
$BASEDIR = "/usr/local/nfsen-1.3.5";
$HTMLDIR    = "/home/data/nfsen";
$PREFIX  = '/usr/local/nfdump-1.6.2/bin';
$USER    = "netflow"; (tätä ei muutettu, mutta kyseinen käyttäjä täytyy muistaa
luoda ja liittää se $WWWGROUP ryhmään)
$WWWUSER  = "apache";
$WWWGROUP = "apache";
%sources = (
   'core-r1'       => { 'port' => '9997', 'IP' => 'tähän netflow-lähteen IP' },
   'core-r2'       => { 'port' => '9997', 'IP' => 'tähän netflow-lähteen IP' },
);
$MAIL_FROM   = 'netflow@nfsen.prv.phkk.fi';
```

NfSen yritettiin käynnistää komennolla */usr/local/nfsen-1.3.5/bin/nfsen start*, mutta se ei käynnistynyt, joten virheilmoituksen perusteella muokattiin nfsen-kansiosta /bin/nfsen-tiedoston yksi rivi seuraavaan muotoon: #!/usr/bin/perl -w -I /usr/local/nfsen-1.3.5/libexec. Tämän jälkeen muokattiin tiedostoa /usr/local/nfsen-1.3.5/bin/nfsend, jossa %%PERL%% korvattiin muotoon

/usr/bin/perl eli kerrottiin Perl-polku. Nyt NfSen voitiin käynnistää komennolla */usr/local/nfsen-1.3.5/bin/nfsen start*.

NfSenin asennuksen jälkeen muokattiin Apachen konfigurointitiedostoa, joka löytyy polusta /etc/httpd/conf/httpd.conf. Tiedostoa muutettiin niin, että NfSenin näkymä aukeaa, kun otetaan selaimella yhteys palvelimen osoitteeseen. Tämä tapahtui tekemällä seuraavat muutokset: <Directory "/home/data/nfsen"> ja DirectoryIndex nfsen.php. Kaikki NfSenin selainnäkymässä olevat pienet ikonit eivät näkyneet, joten tutkittiin httpd:n error-logia, josta löytyi virheilmoitus, joka kertoi, että httpd.conf-tiedostossa on ikoneihin liittyvä polku väärin, minkä jälkeen kyseinen polku käytiin korjaamassa. Valitettavasti httpd.conf-tiedostoon tehtyä muutosta ei tullut otettua talteen, joten mikäli ikonit eivät näy selainhallinnassa, niin kannattaa tutkia Apachen error-logia, joka löytyy polusta /var/log/httpd/error_log.

NfSenissä on valmiina profiili nimeltä Live, joka näyttää NetFlow-lähteiden dataa. Datasta piirretään graafeja, mutta näille graafeille ei asennuksen yhteydessä tullut automaattisesti mitään väriä, joten ennen kuin graafit näkyivät, niin selainnäkymän Stats-välilehdeltä täytyi vielä käydä antamassa NetFlow-lähteille värit, joita käytetään graafeissa. Värit päästään määrittelemään Channel List -kohdan alla (kuvio 21).



KUVIO 21. NetFlow-lähteen värin muuttaminen graafeja varten

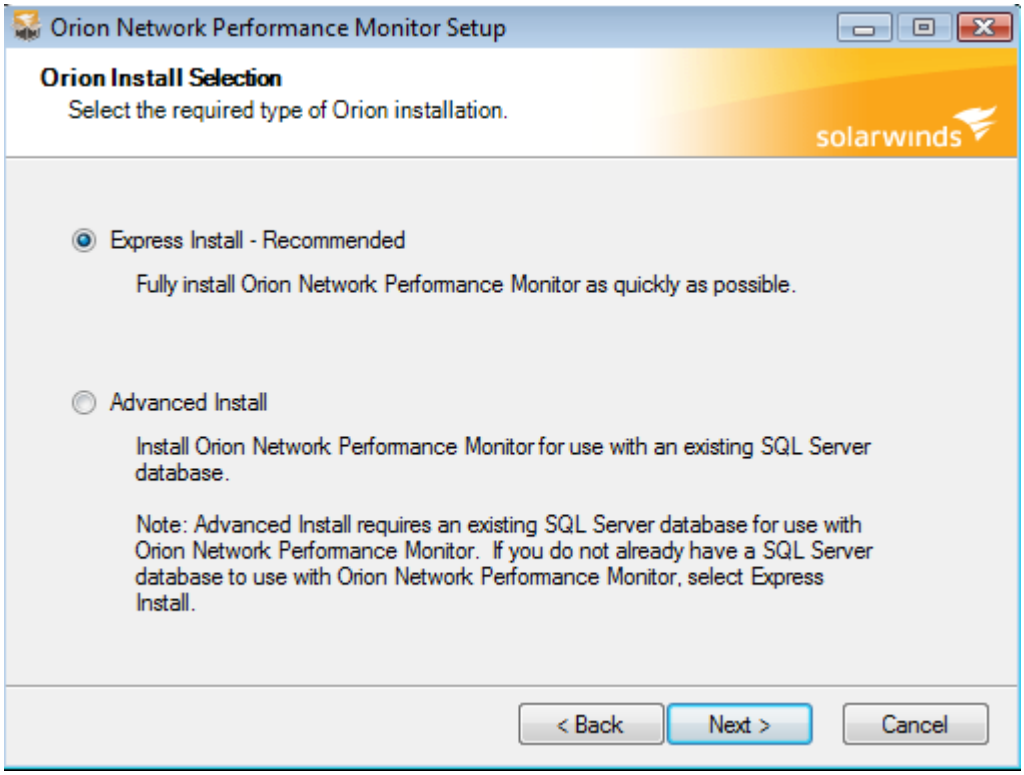
Mikäli NetFlow-lähteitä on useita, niin niille kannattaa määritellä selvästi erisävyiset värit, jotta ne erottuvat graafeissa selkeästi. Värin muuttamisen jälkeen

asennukset ja muutokset oli tehty ja NfSen oli valmiina NetFlow-datan analysointia varten.

4.3.2 Orion NetFlow Traffic Analyzer -asennus

Orion NetFlow Traffic Analyzer on Windows-käyttöjärjestelmällä toimiva sovellus, joka päätettiin asentaa Windows Server 2003 -käyttöjärjestelmälle. Ensimmäiseksi asennettiin käyttöjärjestelmä testikoneelle. Kun koneen käyttöjärjestelmä ja verkkoasetukset oli laitettu kuntoon, niin lisättiin vielä Windowsin palomuuriin aukko etätyöpöydälle eli Remote Desktop -yhteydelle, joka käyttää TCP-porttia 3389, ja tämä yhteys sallittiin vain tietystä IP-verkosta. Orion NTA toimii Orion Network Performance Monitorin päällä, mikä vaatii, että käyttöjärjestelmään on asennettu IIS, joka on web-palvelinohjelmisto. Tämä saatiin asennettua Windows Server 2003 -levyltä. Loput asennukset suoritettiin etätyöpöytäyhteyden kautta.

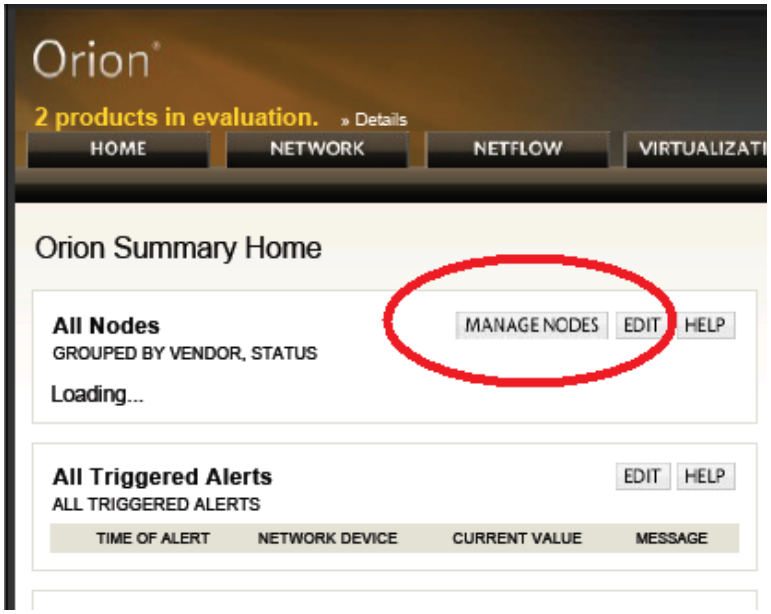
SolarWindsin sivuilta ladattiin Orion NetFlow Traffic Analyzer, joka vaatii toimiakseen myös Orion Network Performance Monitorin. Nämä saatiin ladattua samalla latauksella zip-tiedostona, joka purettiin ja asennus voitiin aloittaa. Ensin asennettiin NPM, joka asennettiin oletusasetuksilla, ja asennuksessa ei ilmennyt mitään ongelmia. Jos IIS on asennettu, niin ainoat asiat, joita asennuksessa kysytään, ovat asennuspolku sekä asennuksen tyyppi, joita ovat Express Install ja Advanced Install (kuvio 22). Oletusasetus on Express Install, ja Advanced Install valitaan vain, mikäli halutaan käyttää NPM:n kanssa jo olemassa olevaa SQL-tietokantaa.



KUVIO 22. NPM:n asennustyypin valinta

Tämän jälkeen asennettiin NTA osaksi NPM:ää. NTA:n asennus on yksinkertainen, eikä siinä kysellä mitään erikoista eli asennus tapahtuu vain etenemällä muutaman kerran Next-nappia painamalla. Windowsin palomuuriin ilmestyi asennuksen yhteydessä automaattisesti aukot sekä saapuvalle NetFlow-datalle että selainhallinnalle.

Seuraavaksi otettiin selaimella yhteys NPM:n selainhallintaan, jonka kautta oli tarkoitus lisätä PHKK:n verkon keskusreititin NetFlow-lähteeksi. Ensimmäiseksi reititin lisättiin IP-osoitteella NPM:n puolelle valvottavaksi laitteeksi, mikä päästiin tekemään painamalla aloitusnäkymän Manage Nodes -kohdasta (kuvio 23), minkä jälkeen valittiin Add Node. Valvottavan solmun lisäyksen aikana oli pakko käyttää SNMP:tä reitittimen liityntöjen löytämiseen eli SNMP community string täytyi antaa, jotta reitittimeltä saatiin luettua tiedot (kuvio 24). Tämän jälkeen reitittimen liitynnät ilmestyivät näkyviin, minkä jälkeen valikoitiin niistä se liityntä, josta NetFlow-data konfiguroidaan reitittimeltä lähtemään.

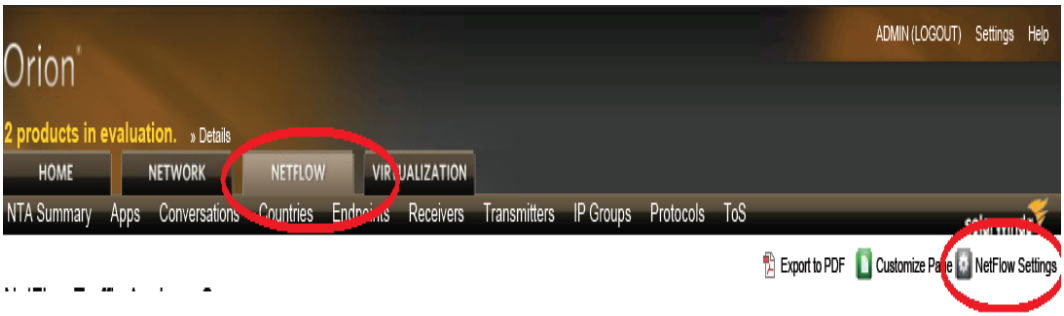


KUVIO 23. Uusi laite päästään lisäämään Manage Nodes -kohdasta

KUVIO 24 Uuden laitteen lisääminen (IP-osoite ja community string peitetty)

Nyt laite oli lisätty NPM:n puolelle ja laitteen alla nähtiin yksi valvottava liityntä. Nyt saatiin valittua tämä laite ja liityntä NetFlow-lähteeksi NTA:n puolella.

NTA:n puolelle päästään painamalla selainnäkymän yläosasta kohtaa NETFLOW, jonka alta löytyy kohta NetFlow Settings (kuvio 25). NetFlow Settings -kohdan alta löytyy NetFlow Sources, jota painamalla löytyy lista NPM:n puolelle lisätyistä laitteista. Tästä listasta valittiin keskusreititin NetFlow-laitteeksi laittamalla ruksi sen vieressä olevaan NetFlow-kohtaan.



KUVIO 25. NTA-osio löytyy NETFLOW-kohdan alta

Lopuksi muutettiin portti, jota NTA käyttää NetFlow-datan keräämiseen. Tämän portin täytyi tietysti olla sama, johon reititin konfiguroidaan dataa lähettämään. Porttinumero muutettiin NETFLOW-välilehden alta painamalla NetFlow Settings, josta löytyi kohta nimeltä NetFlow Collector Services. Kuunneltavaksi portiksi laitettiin 9997. Nyt Orion NetFlow Traffic Analyzer oli asennettu ja valmiina vastaanottamaan NetFlow-dataa.

4.3.3 Reitittimien konfigurointi

PHKK:n verkossa toimivat keskusreitittiminä Cisco Catalyst 6500 sarjan laitteet. NetFlown käyttöönottoa varten konfiguroidut komennot näkyvät kuviossa 26.

```
core-r1(config)#mls netflow
core-r1(config)#mls flow ip full
core-r1(config)#mls nde sender version 9
core-r1(config)#ip flow-export source vlan 10
core-r1(config)#ip flow-export destination 192.168.xxx.xxx 9997
```

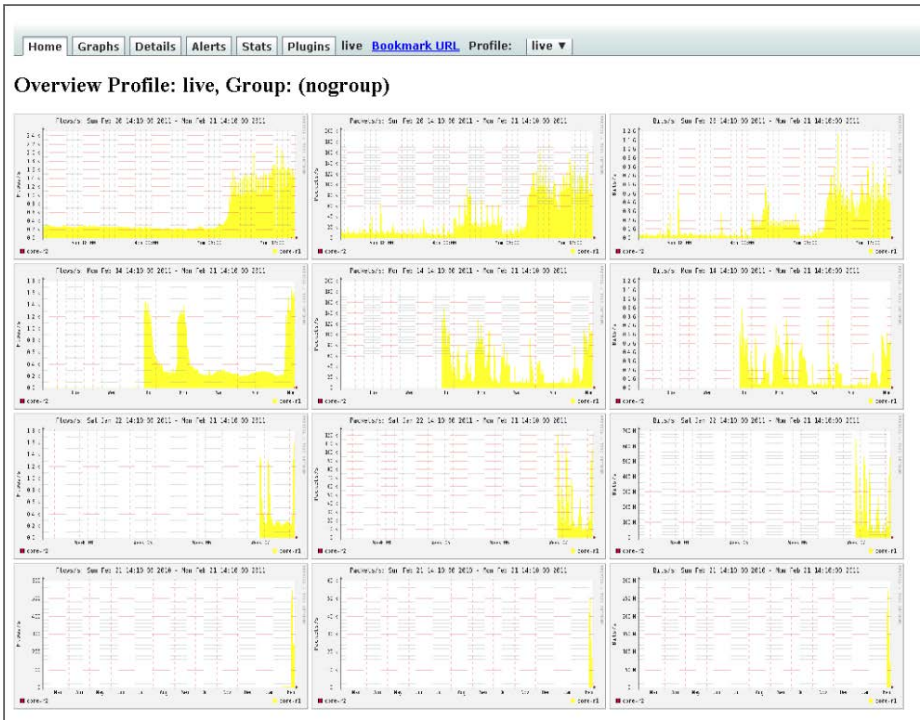
KUVIO 26. NetFlown konfigurointi

Komennolla *mls netflow* NetFlow otettiin käyttöön, jonka jälkeen valittiin flow-maski komennolla *mls flow ip full*. Seuraavaksi valittiin NetFlown versioksi 9,

joka tehtiin komennolla *mls nde sender version 9*. NetFlow-datalle valittiin komennolla *ip flow-export source* IP-osoite, josta data lähtee kohti NetFlow-kerääjää eli tässä tapauksessa vlan 10 -liitynnän IP-osoite. Lopuksi komennolla *ip flow-export destination ip-osoite portti* saatiin valittua minne NetFlow-data lähetetään ja mihin porttiin.

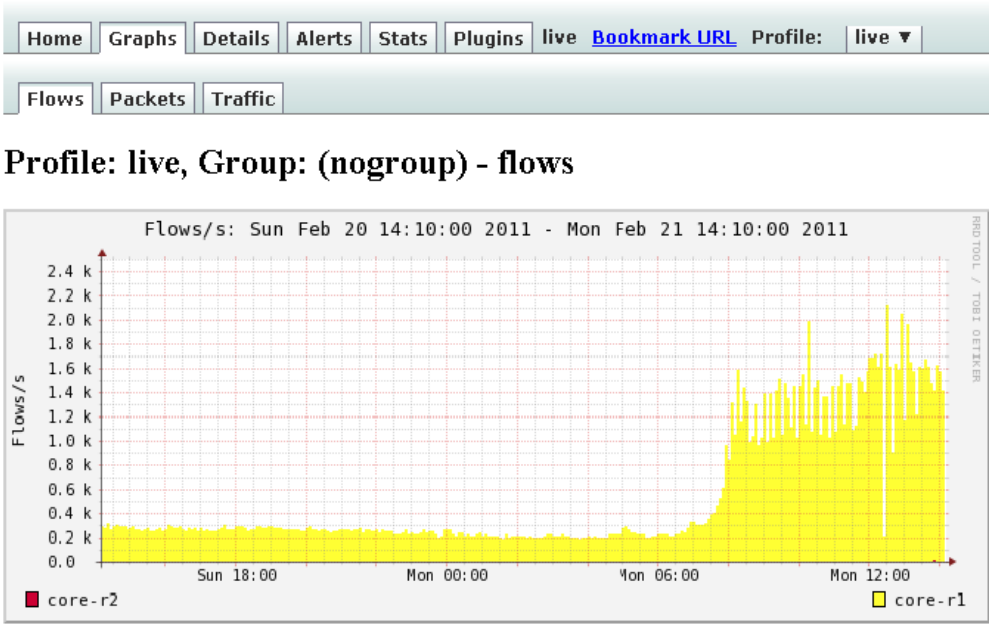
4.4 NfSen

Ohjelmistojen asennuksien ja reitittimien konfigurointien jälkeen voitiin testata asennettuja NetFlow-datan analysoimiseen tarkoitettuja sovelluksia eli NfSeniä sekä Orion NetFlow Traffic Analyzeria. Ensimmäisenä vuorossa oli NfSen. NfSenin tutkiminen aloitettiin ottamalla selainyhteys ohjelman selainhallintaan, jonka kautta NetFlow-dataa oli mahdollista tutkia. Heti selainhallinnan aloitusnäkymästä pystyi havainnoimaan, oliko NfSen saanut reitittimeltä dataa. Tältä sivulta nähtiin erilaisia graafeja verkkoliikenteeseen liittyen. Kuvio 27 näyttää, miltä NfSenin aloitusnäkymä näyttää. Graafeista voidaan havainnoida, että NfSen on kerännyt dataa.



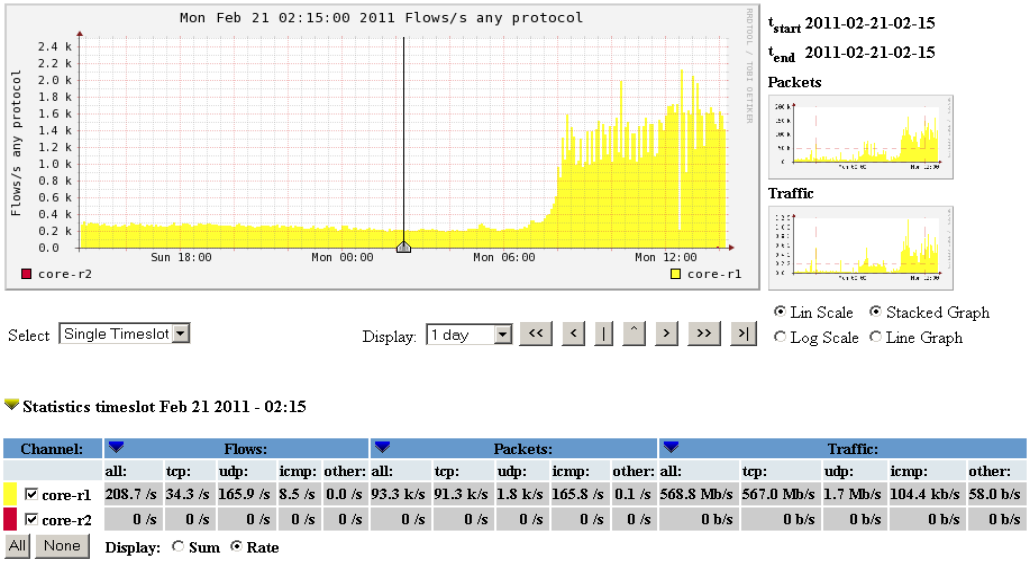
KUVIO 27. NfSenin selainhallinnan aloitusnäkymä

NfSenissä navigoidaan eri näkymiin sivun yläreunassa olevista välilehtipainikkeista, joita ovat Home, Graphs, Details, Alerts, Stats sekä Plugins. Home-sivulla nähdään vierekkäin graafeja, jotka kertovat flowmäärät, pakettien määrät sekä bittien määrät. Lisäksi näitä rivejä on neljä kappaletta, jotka kuvaavat edellä mainittuja määriä eri aikoina. Ensimmäinen rivi kertoo päivän tapahtumat, toinen rivi viikon tapahtumat, kolmas kuukauden ja neljäs vuoden tilastot. Näitä graafeja pääsee katsomaan isompina Graphs-välilehdeltä. Kuviossa 28 nähdään Graphs-välilehdeltä otettu graafi, joka kertoo flowmäärät päivän ajalta.



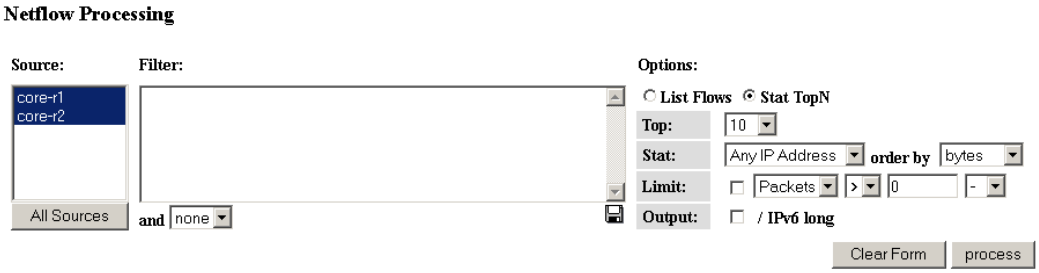
KUVIO 28. Päivän flowmäärät

Details-välilehdellä päästään tutkimaan NetFlow-dataa tarkemmin. Tältä sivulta nähdään graafeja TCP-, UDP- ja ICMP-liikenteestä sekä muusta liikenteestä. Lisäksi on mahdollista katsoa graafeja kokonaisliikenteestä. Tällä sivulla voidaan myös graafeista valita jokin ajankohta, jonka liikennemääriä voidaan tutkia. Voidaan valita yksittäinen ajan hetki tai sitten jokin aika-alue. Aika valitaan liikuttamalla graafissa olevaa osoitinta. Sen jälkeen graafin alla nähdään tarkemmat tiedot liikenteestä. Esimerkiksi kuviossa 29 nähdään helmikuun 21. päivän liikenne kello 02.15.



KUVIO 29. Liikennemäärät tiettynä ajan hetkenä

Alempana Details-näkymässä päästään tutkimaan NetFlow-dataa yksityiskohtaisesti. NetFlow-datasta saadaan suodatettua näkyviin vain haluttua tietoa. Esimerkiksi syöttämällä Filter-kohtaan *port 80* saataisiin suodatettua näkyviin vain HTTP-liikennettä. Filtteri tottelee NfDumpin komentoja, ja nämä nähdään NfDumpin manuaalista. Filtterin tekemisen lisäksi voidaan valita kahdesta eri vaihtoehdosta joko List Flows tai Stat TopN. List Flows listaa löydetyt flowt ja lisäksi voidaan määritellä, mitä tietoja niistä näytetään, kuten esimerkiksi lähdeosoite ja lähde-portti. Stat TopN vaihtoehdolla voidaan hakea esimerkiksi top-10 IP-osoitetta järjestettynä siirretyn datamäärän mukaan. Painamalla process-nappia NfSen sitten listaa löytämänsä tiedot sivun alaosaan. Ideana siis on, että filtterillä saadaan suodatettua näkyviin haluttua liikennettä ja sen jälkeen ne voidaan järjestää näkyville halutulla tavalla. Kuviosta 30 nähdään Details-välilehden osio nimeltä Netflow Processing, jossa näitä edellä mainittuja asioita voidaan tehdä.



KUVIO 30. NetFlow-datan prosessointi

Filter-toimintoa testattiin tekemällä P2P-niminen filtteri, johon listattiin tunnettujen P2P-ohjelmien käyttämiä portteja. Filtteri saatiin tallennettua ja sitä voitiin jatkossa käyttää valitsemalla se Filter-kohdan alla olevasta valikosta.

Lisäksi NfSenissä on vielä Alerts-, Stats- ja Plugins-välilehdet. Alerts-välilehdeltä oltaisiin saatu tehtyä hälytyksiä verkkoliikenteeseen liittyen, mutta emme niitä testanneet. Selainhallinnan yläreunassa Profile-kohdasta voitiin vaihtaa profiilia. NfSeniin pystyttiin luomaan profiileja, joille voitiin valikoida näkymään vain tiettyjä NetFlow-lähteitä. Stats-välilehdeltä voitiin tarkistaa profiilin tiedot. NfSeniin on mahdollista asentaa myös lisäosia, joita voidaan käyttää Plugins-välilehdeltä.

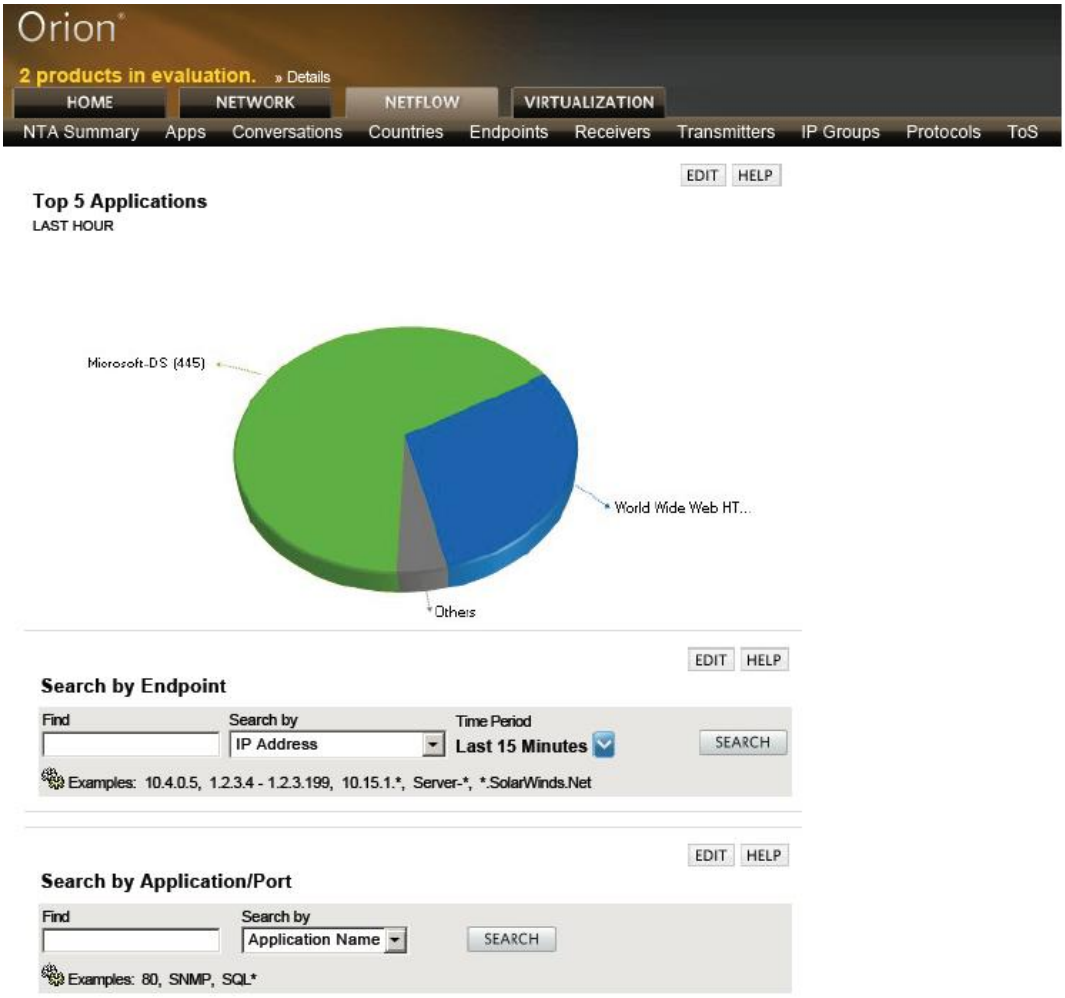
NfSen tuntui toimivalta NetFlow-datan analysoimiseen tarkoitetulta sovellukselta. Ennen NfSenin käyttöä on syytä muistaa tutustua NfDumpiin, joka hoitaa kaiken NetFlow-datan prosessoinnin ennen kuin dataa voidaan katsella NfSenillä. Graafit olivat selkeitä ja erilaisia graafeja oli tarjolla sopiva määrä. NetFlow-datan prosessointi Details-välilehdellä oli toimiva ja sillä saatiin etsittyä ja listattua halutunlainen verkkoliikenne. NfSen on ilmaiseksi sovellukseksi hyvä ja toimiva. Miinuksena voidaan nähdä raporttien tallentamisen puuttuminen. NetFlow-datasta olisi hyvä saada tallennettua raportteja esimerkiksi PDF-muodossa.

Mikäli halutaan ottaa käyttöön pelkästään NetFlow-dataa varten tehty sovellus, niin NfSen on toimiva vaihtoehto, mutta jos tarkoituksena on ottaa käyttöön laajempi verkonvalvontaan tarkoitettu sovellus, jossa on samassa paketissa esimerkiksi NetFlow- sekä SNMP-tuki, niin on syytä tutustua esimerkiksi SolarWindsin Orion Network Performance Monitoriin ja siihen saatavaan NetFlow Traffic Analyzeriin.

4.5 Orion NetFlow Traffic Analyzer

SolarWindsin Orion Network Performance Monitorin selainhallinnassa olevan NETFLOW-välilehden alta päästiin Orion NetFlow Traffic Analyzerin puolelle, jossa NetFlow-dataa voitiin analysoida. Tällä sivulla nähtiin yhteenveto NetFlow-datasta. Sivulla nähtiin useita graafeja, jotka kertoivat eri asioita. Tällaisia graafeja

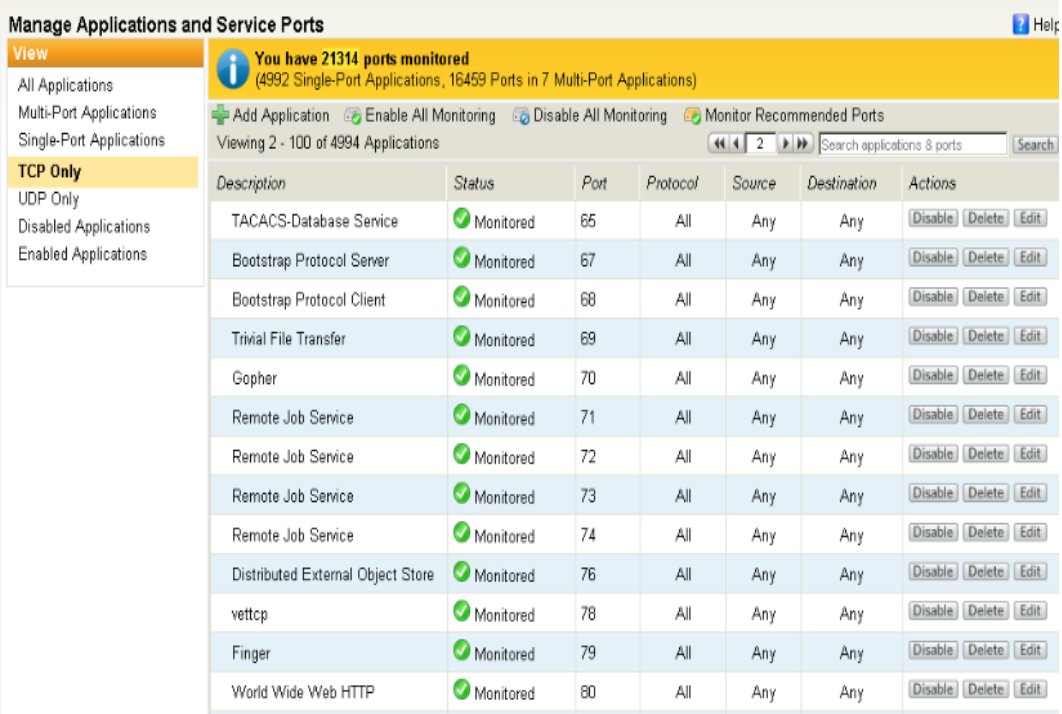
olivat mm. top 5 sovellusta, top 5 IP-osoitetta sekä top 5 yhteyttä. Lisäksi tällä yhteenvetosivulla nähtiin listattuna käytössä olevat NetFlow-lähteet sekä NetFlow Traffic Analyzeriin liittyviä ilmoituksia, kuten esimerkiksi, että NTA kuuntelee porttia 9997. Sivulla oli myös hakutoiminto, josta voitiin etsiä IP-osoitteen tai porttinumeron perusteella liikennettä. Kuvioon 31 on yhdistetty muutamia kohtia NTA:n yhteenvetosivulta.



KUVIO 31. NTA:n yhteenvetosivulta otettuja kohtia

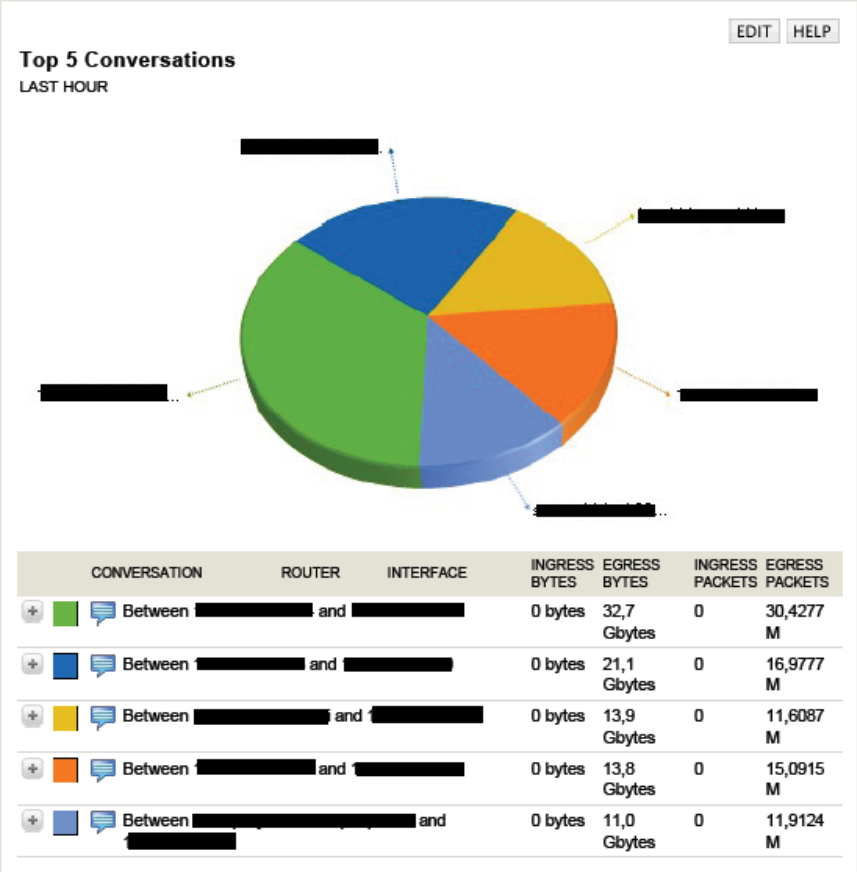
NETFLOW-välilehden alta löytyi Apps-niminen kohta, josta painamalla avautui näkymä, jossa voitiin tarkastella eri ohjelmien liikennettä. Ohjelmat tunnistetaan porttinumeroiden perusteella ja NTA:ssa on valmiina listattu portit ja niille nimet. NTA:n asetuksista päästiin tarkastelemaan näitä portteja ja niitä oli mahdollista muokata. Esimerkiksi TCP-portin 80 kohdalla luki World Wide Web HTTP. Koska NTA:ssa on valmiina nimettynä portit, niin tämä helpottaa esimerkiksi graafien

lukua, joissa porttinumeroiden lisäksi lukee myös portin nimi. Tällöin sovellusten porttinumeroita ei tarvitse muistaa ulkoa. Kuviossa 32 nähdään NTA:n asetuksista otettu kuva, jossa on listattuna portteja ja niiden nimiä.



KUVIO 32. Sovelluksien käyttämiä portteja

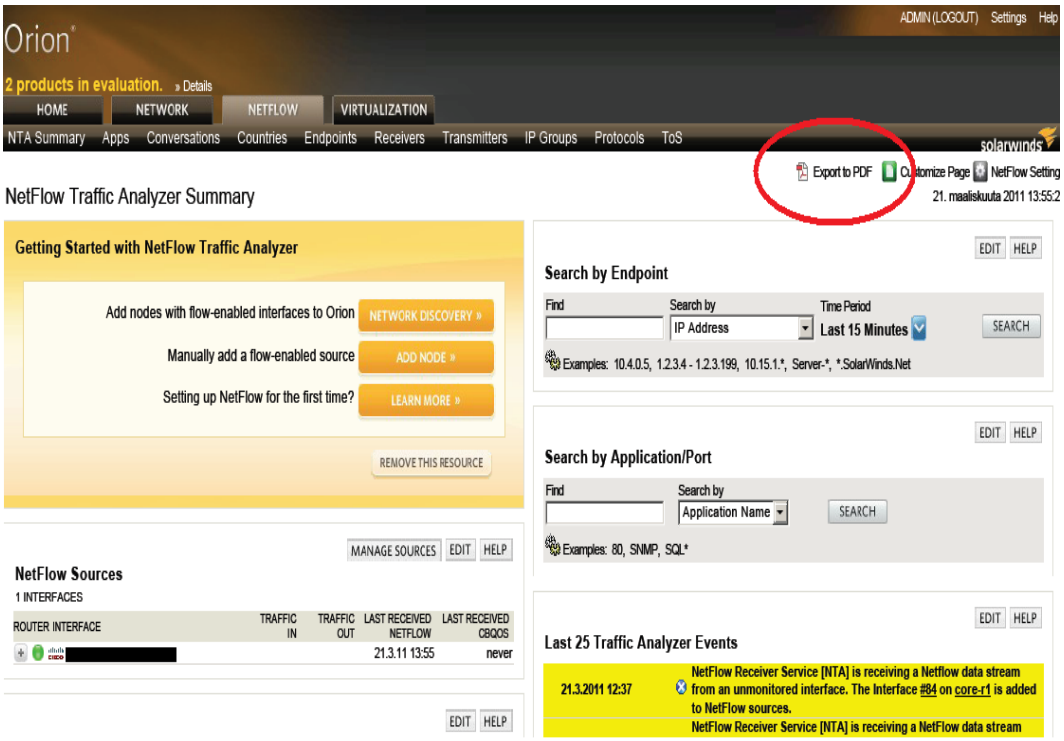
Conversations-kohdasta painamalla päästiin tutkimaan mitkä osoitteet ovat liikennöineet eniten keskenään (kuvio 33) ja Countries-osiosta nähtiin maakohtaiset liikenteet. Endpoints-kohdasta nähtiin, mitkä osoitteet ovat olleet aktiivisimpia verkossa. Sitten olivat vuorossa Receivers ja Transmitters. Receivers-kohdasta päästiin katsomaan, mitkä osoitteet ovat vastaanottaneet eniten dataa ja Transmitters kertoi osoitteet, jotka ovat lähettäneet eniten dataa.



KUVIO 33. Osoitteet, jotka ovat liikennöineet eniten (IP-osoitteet peitetty)

Kolme viimeistä linkkiä NETFLOW-välilehden alla olivat IP Groups, Protocols ja ToS. NTA:n asetuksissa voitiin tehdä IP-ryhmiä, joiden liikenne sitten näkyi IP Groups -kohdassa, eli olisi esimerkiksi voitu luoda eri VLAN-verkoille omat ryhmät, jolloin IP Groupsista olisi päästy tarkkailemaan, mitkä VLAN-verkot liikennöivät eniten. Protocols-näkymässä nähtiin TCP-, UDP- sekä muun liikenteen määrät. ToS-kohta liittyi IPv4-kehyksien Type of Service -kohdan tietoihin, mutta tähän näkymään ei testauksessa tutustuttu.

NTA:n jokaisessa näkymässä on oikeassa yläkulmassa Export to PDF -painike (kuvio 34), jonka avulla NTA:sta on mahdollista tuoda NetFlow-tietoja PDF-muodossa. Tämä on hyvä toiminto, mikäli halutaan saada talteen raportteja verkkoliikenteeseen liittyen. Graafit ohjelmassa ovat selkeitä ja niitä on tarjolla useita. On hyvä asia, että ohjelmassa on porttinumerot nimettynä valmiina. Huonona puolena NetFlow-lähteen lisäämisen kannalta on se, että laitteessa täytyy olla SNMP päällä.



KUVIO 34. PDF-painike

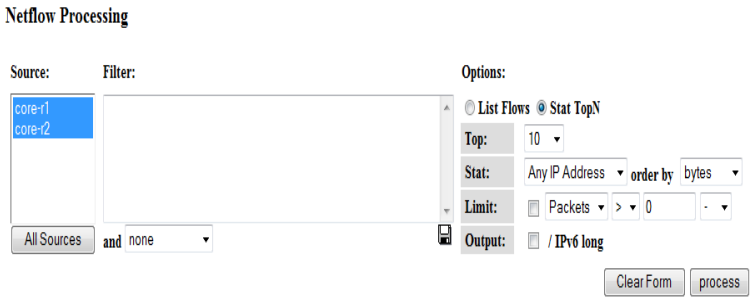
Kokonaisuutena SolarWindsin Orion NetFlow Traffic Analyzer on monipuolinen NetFlow-datan analysointiin tarkoitettu sovellus. Ohjelman avulla NetFlow-datasta saadaan selville useita asioita liikennemääristä sekä tarkempia tietoja yksittäisistä yhteyksistä. Koska NTA vaatii toimiakseen NPM:n, niin pelkästään NetFlown takia tätä tuotetta ei ole kannattavaa ottaa käyttöön, sillä lisenssi täytyy ostaa kumpaankin tuotteeseen. NTA olisi hyvä vaihtoehto NetFlow-datan analysoimiseen, mikäli olisi tarvetta myös laajemmalle verkonvalvontasovellukselle eli NPM:lle tai mikäli NPM olisi jo käytössä.

4.6 Raporttien analysointi

NfSen ja SolarWindsin Orion NetFlow Traffic Analyzer kummatkin tarjoavat yleiset sekä halutessa tarkemmat tiedot verkkoliikenteestä. Seuraavaksi tutkitaan hieman kerättyä NetFlow-dataa. Otetaan muutamia esimerkkejä kummastakin sovelluksesta ja katsotaan millaisia tietoja ohjelmien avulla saadaan selville.

NfSenin Netflow Processing -osiosta saadaan selville, mitkä IP-osoitteet ovat lähettäneet/vastaanottaneet eniten dataa tavuina verkossa. Tällaisia hakuja voidaan

tehdä halutulle aika-alueelle eli jos esimerkiksi havaitaan, että verkon liikenne on kasvanut huomattavasti jonain tiettynä hetkenä, niin tältä ajalta voidaan etsiä verkon aktiivisimmat käyttäjät ja listata ne halutulla tavalla. Kuviossa 35 nähdään listattuna top-10 IP-osoitetta ja ne on järjestetty siirretyn tavumäärän mukaan. Aika-alue hakua varten valittiin Netflow Processing -kohdan yllä olevasta graafista. Nähdään, että listalla ensimmäisenä on IP-osoite, joka on siirtänyt 107,1 Gt dataa ja tiedonsiirtonopeus on ollut keskimäärin 92,8 Mbps. Tiedoista nähdään myös mm. flow- sekä pakettimäärät.



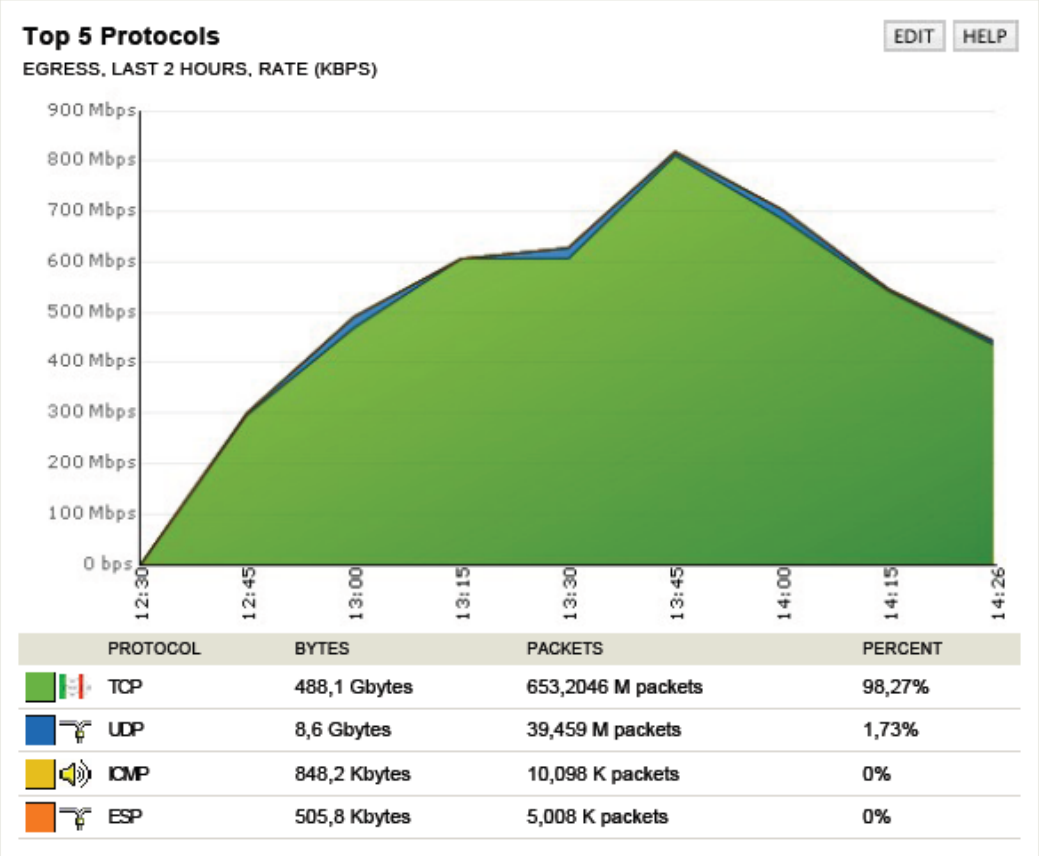

```
** nfdump -M /usr/local/nfsen-1.3.5/profiles-data/live/core-r1:core-r2  -T  -R 2011/03/03/nfcapd.201103031215:2011/03/03/nfcapd.201103031440 -n 10 -s ip/bytes
nfdump filter:
any
Top 10 IP Addr ordered by bytes:
Date first seen          Duration Proto          IP Addr    Flows(%)      Packets(%)       Bytes(%)        pps      bps   bpp
2011-03-03 12:10:45.882  9240.980 any       [redacted]    77086( 1.6)  112.4 M(22.2)  107.1 G(30.1)    12166   92.8 M   952
2011-03-03 12:12:10.202  8913.968 any       [redacted]      235( 0.0)   35.1 M( 6.9)   33.5 G( 9.4)     3933   30.1 M   955
2011-03-03 12:11:13.559  9170.310 any       [redacted]      480( 0.0)   33.1 M( 6.5)   31.8 G( 8.9)     3608   27.7 M   960
2011-03-03 11:53:43.146 10261.668 any       [redacted]    12614( 0.3)   29.6 M( 5.8)   27.2 G( 7.6)     2888   21.2 M   917
2011-03-03 12:10:54.953  9095.577 any       [redacted]     4899( 0.1)   25.5 M( 5.0)   23.4 G( 6.6)     2807   20.6 M   915
2011-03-03 12:10:54.283  9228.708 any       [redacted]     2352( 0.0)   23.3 M( 4.6)   22.3 G( 6.3)     2529   19.3 M   954
2011-03-03 11:53:38.090 10267.214 any       [redacted]    16146( 0.3)   30.0 M( 5.9)   21.1 G( 5.9)     2924   16.4 M   701
2011-03-03 12:10:50.619  9229.797 any       [redacted]     3061( 0.1)   15.7 M( 3.1)   15.9 G( 4.5)     1703   13.8 M  1009
2011-03-03 12:10:54.822  9207.076 any       [redacted]     4547( 0.1)   14.8 M( 2.9)   14.8 G( 4.2)     1611   12.9 M   998
2011-03-03 13:13:34.012  5464.785 any       [redacted]     7780( 0.2)   15.3 M( 3.0)   14.3 G( 4.0)     2792   21.0 M   937

Summary: total flows: 4844786, total bytes: 355.7 G, total packets: 507.3 M, avg bps: 260.7 M, avg pps: 46476, avg bpp: 701
Time window: 2011-03-03 11:42:51 - 2011-03-03 14:44:46
Total flows processed: 4844786, Blocks skipped: 0, Bytes read: 232782968
Sys: 2.325s flows/second: 2083200.1   Wall: 2.322s flows/second: 2085886.3
```

KUVIO 35. Top-10-lista NfSenistä (IP-osoitteet peitetty)

Mikäli haluttaisiin tarkempaa tietoa esimerkiksi Top-10-listan ensimmäisestä IP:stä, niin seuraavaksi olisi voitu laittaa Filter-kohtaan *HOST ip-osoite* ja selvittää vaikka kyseisen IP-osoitteen verkkoliikenteen käyttämät porttinumerot. Tällä tapaa saataisiin tarkempaa tietoa kyseisen IP-osoitteen verkkoliikenteestä.

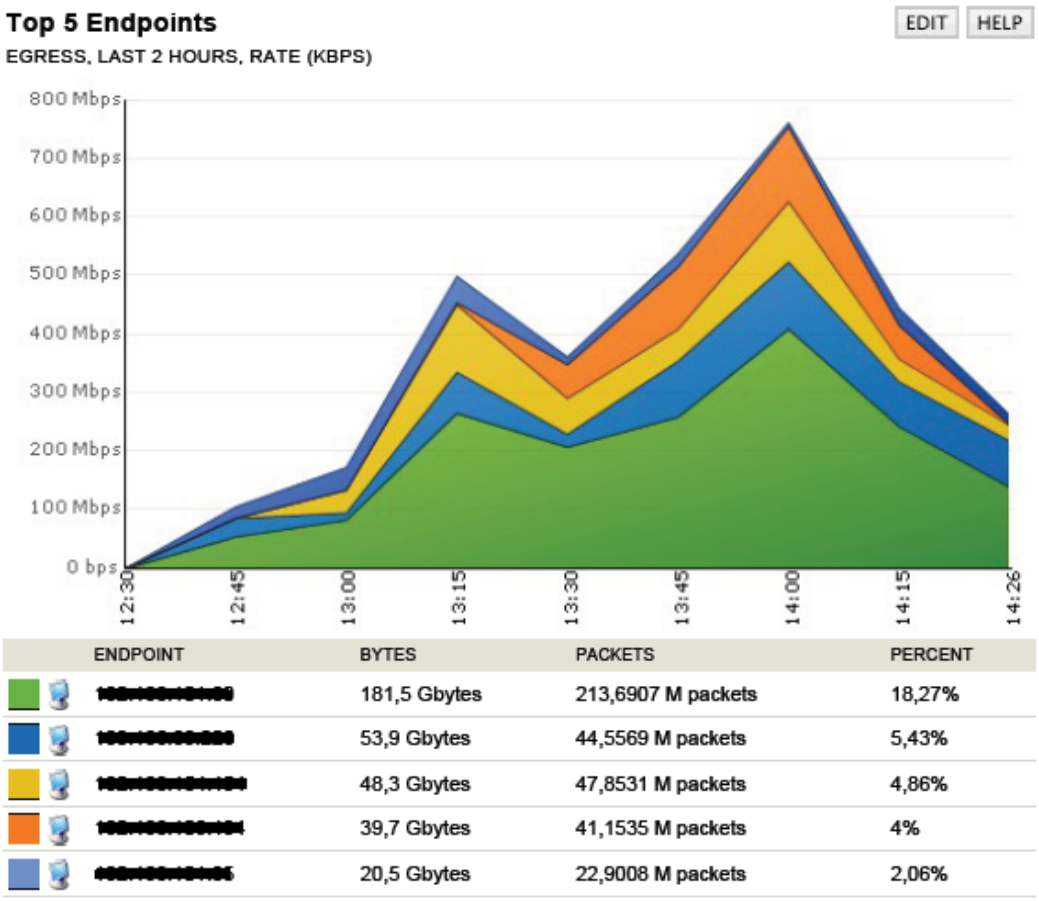
Seuraavaksi katsotaan muutamia Orion NetFlow Traffic Analyzerista otettuja graafeja. Kuviossa 36 nähdään graafi, joka kertoo verkkoliikenteen määrän kahden tunnin ajalta. Tästä graafista ei selviä yksityiskohtaisia tietoja verkkoliiken-

teestä, mutta nähdään yleisesti, kuinka paljon verkossa liikkuu dataa. Kuviosta nähdään, että TCP-liikennettä on selvästi eniten ja se muodostaa 98,27 % koko liikenteestä. Toisena listalla on UDP, jota verkossa on liikkunut 8,6 Gt. Kuvio kertoo myös, että eniten liikennettä on ollut noin kello 13:45.



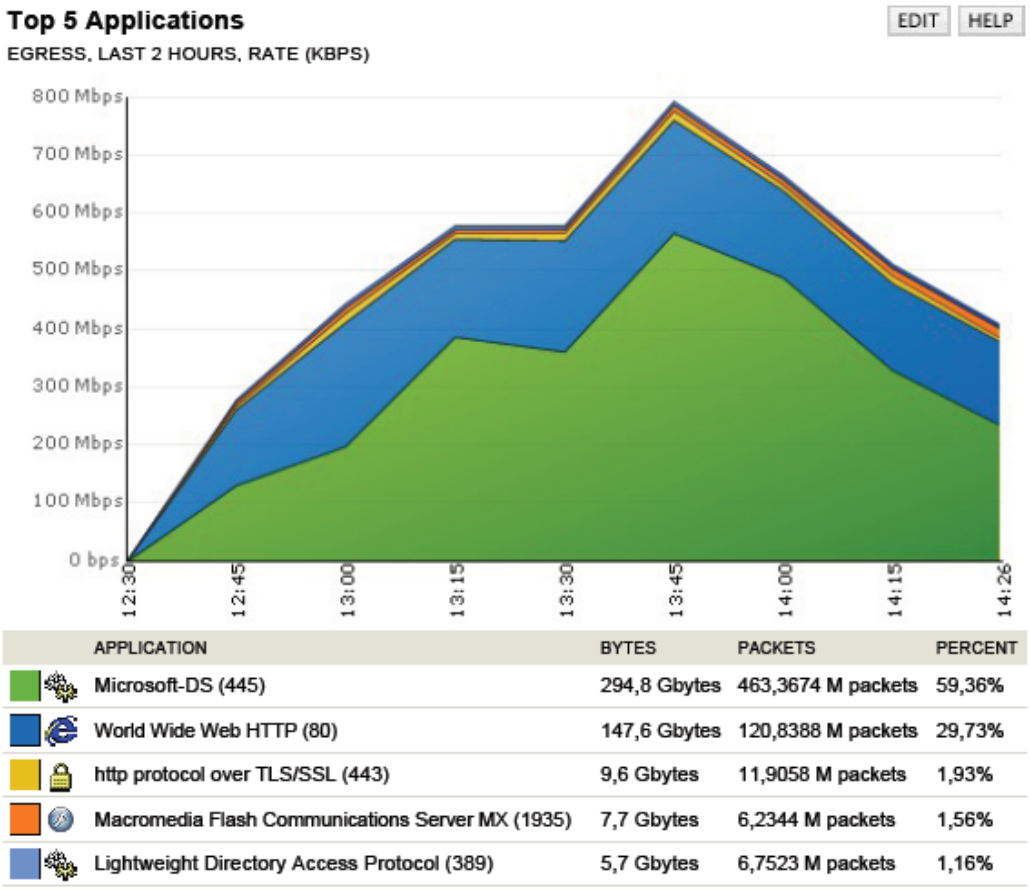
KUVIO 36. Kahden tunnin aikana verkossa on liikkunut eniten TCP-liikennettä

Kuviossa 37 nähdään viisi IP-osoitetta, jotka ovat aiheuttaneet verkkoon eniten liikennettä tiettynä aikana. Kuvio kertoo IP-osoitteiden lisäksi siirretyn datamäärän tavuina, pakettien määrän sekä prosenttiosuuden koko verkkoliikenteestä. Eniten verkkoon liikennettä aiheuttanut IP-osoite on vastuussa 18,27 prosentista koko verkkoliikenteestä. Tavuina tämä IP-osoite on siirtänyt verkossa 181,5 Gt ja paketteja yli 200 miljoonaa.



KUVIO 37. Eniten dataa siirtäneet IP-osoitteet (IP-osoitteet peitetty)

Kuviosta 38 nähdään, että NTA:sta saadaan näkyville myös porttinumeroihin liittyvä top-5-graafi. Tästä graafista saadaan selville eniten käytetyt porttinumerot. Kuvio kertoo, että kahden tunnin aikana eniten käytetty portti verkkoliikenteessä on ollut portti 445, joka on nimeltään Microsoft-DS. Paketit, joissa tätä porttinumeroa on käytetty, muodostavat lähes 300 Gt liikennettä, joka on melkein 60 % koko verkkoliikenteestä. Toisena listalla on portti 80 eli HTTP-portti, joka muodostaa noin 30 % kokonaisliikenteestä kyseisellä ajanjaksolla.



KUVIO 38. Verkkoliikenteessä eniten käytetyt portit

NTA tarjoaa enemmän graafeja kuin NfSen, mutta monet samat tiedot saadaan NfSenissä selville ilman graafeja Netflow processing -osiossa. Graafit kyllä auttavat hahmottamaan eri liikennemäärien suhteita toisiinsa, mutta ne eivät ole aina välttämättömiä. Erona ohjelmissa onkin se, että NTA tarjoaa monet tiedot valmiina graafeina, kun taas NfSenissä tiedot täytyy osata itse hakea käyttäen Netflow processing -osiota, jonka käytön oppii melko nopeasti. NTA:n Countries-osion tarjoamat tiedot eivät ole suoraan saatavilla NfSenissä, mutta filttereitä tekemällä maakohtaiset liikennöinnitkin voitaisiin NfSenissä periaatteessa toteuttaa. Kummallakin ohjelmalla saadaan siis samat tiedot selville NetFlow-datasta. Erona on itse tehtävän työn määrä tietojen saamiseksi sekä tietojen esitystapa.

4.7 NetFlown käyttöönotto

Päijät-Hämeen koulutuskonsernin tietohallinto on suunnitellut NetFlown käyttöönottoa, joten tässä opinnäytetyössä tutustuttiin NetFlow-protokollaan sekä kah-

teen NetFlow-dataan liittyvään sovellukseen, joiden avulla verkkoliikennettä voidaan tarkkailla. NetFlown käyttöönotto ei ole kovin suuri projekti, mikäli NetFlow-sovelluksen asennuksessa ei ilmene ongelmia ja verkko on jo muilta osin toiminnassa. Reitittimen osalta selvitään muutamalla komennolla, jotka voidaan syöttää komentoriville nopeasti. Sovelluksia löytyy useita , joihin kannattaa tutustua NetFlown käyttöönottoa suunniteltaessa.

Mikäli PHKK:n tietohallinnon työntekijät päätyvät ottamaan NetFlown käyttöön, niin NfSen ja Orion NetFlow Traffic Analyzer ovat kumpikin toimivia vaihtoehtoja. NfSenin etuna on Linux-käyttöjärjestelmä, jota PHKK:n tietohallinnon verkonvalvonta suosii. NfSen tarjoaa paljon tietoa NetFlow-datasta, kuten tarjoaa myös Orion NetFlow Traffic Analyzer. Käytettävyydeltään kumpikin sovellus vaikuttaa melko selkeältä ja yksinkertaiselta. NfSenin etuna on myös sen maksuttomuus. NetFlow-dataan liittyvien raporttien osalta NTA on parempi, sillä se tarjoaa PDF-mahdollisuuden jokaisessa näkymässä. Koska NTA vaatii toimiakseen myös Orion Network Performance Monitorin, niin pelkästään NetFlowta varten näitä kahta tuotetta ei ehkä ole järkevää hankkia, mutta mikäli halutaan ottaa käyttöön laajempi verkonvalvontasovellus, jossa on myös mukana esimerkiksi SNMP-mahdollisuudet, niin NPM ja NTA voivat muodostaa halutun kokonaisuuden, kun taas pelkkää NetFlowta varten NfSen on parempi vaihtoehto. NetFlow-sovelluksia on kuitenkin saatavilla melko paljon useilta eri valmistajilta, joten ennen sovelluksen valintaa kannattaa tutustua myös muihin vaihtoehtoihin näiden kahden sovelluksen lisäksi.

5 YHTEENVETO

Tämä opinnäytetyö käsitteli verkonvalvontaa sekä siihen liittyviä protokollia SNMP ja NetFlow. Verkonvalvonta on tärkeää ja hyödyllistä yritysten ja organisaatioiden kannalta, sillä parhaassa tapauksessa sen avulla säästetään rahaa sekä aikaa. Verkonvalvonnan avulla saadaan tietoa verkon tilasta, jolloin vikatilanteet voidaan havaita mahdollisimman nopeasti tai jopa välttää ne kokonaan.

Työssä tavoitteena oli keskittyä pääasiassa NetFlow-protokollaan, mutta koska SNMP on tänä päivänä erittäin paljon käytetty verkonvalvontaprotokolla, niin myös sen perusesittely nähtiin tarpeelliseksi tässä yhteydessä. SNMP ei ole vain valvonnassa käytetty protokolla, vaan se tarjoaa myös hallintaominaisuuksia. Sekä valvonta että hallinta tapahtuu SNMP:ssä käyttäen MIB-tietokantoja, joihin SNMP-viesteissä viitataan. SNMP:n valvontaominaisuudet liittyvät verkon laitteiden verkkoliityntöihin sekä esimerkiksi muistin ja prosessorin käyttöön, mutta kävi ilmi, ettei SNMP:n avulla saada tarkempaa tietoa verkkoliikenteen sisällöstä. Tähän tarkoitukseen Cisco Systemsin kehittämän NetFlown taas huomattiin soveltuvan täydellisesti.

NetFlow osoittautui erittäin mielenkiintoiseksi verkonvalvontaprotokollaksi, jonka avulla verkossa olevan laitteen läpi kulkevaa dataa päästään analysoimaan. NetFlow ei tarjoa mahdollisuutta ainoastaan liikennemäärien tutkimiseen, kuten SNMP, vaan sen avulla saadaan myös yksityiskohtaista tietoa verkkoliikenteestä. Vaikka NetFlow-järjestelmä sisältää yksinkertaisimmillaan yhden flow-tietoja keräävän laitteen sekä NetFlow-kerääjän, niin näin päästään täysin perille siitä, mitä verkossa liikkuu. NetFlown versioista erityisesti versio yhdeksän vaikutti mielenkiintoiselta, sillä siinä käytetyt mallipohjat tuovat mukanaan mahdollisuuksia laajennettavuuteen liittyen, mikä lupaa hyvää tulevaisuutta NetFlowlle.

Käytännön osuudessa tutustuttiin kahteen eri NetFlow-datan analysoimiseen tarkoitettuun sovellukseen, jotka olivat NfSen ja Orion NetFlow Traffic Analyzer. Sovellukset olivat käyttöjärjestelmältään, ulkoasultaan sekä hinnaltaan erilaisia, mutta kummallakin sovelluksella saatiin kerättyä ja tuotua esille samat tiedot verkkoliikenteestä NetFlown avulla. Sovelluksien käyttöliittymät tuntuivat melko

selkeiltä, ja oli hienoa nähdä, kuinka muutamalla painalluksella verkossa liikkuneet flowt avautuivat silmien eteen paljastaen pakettien sisältämät tiedot, joista saatiin selville esimerkiksi datan lähde ja kohde sekä se, minkä tyyppisestä liikenteestä oli kyse.

Sovelluksista NfSen osoittautui paremmaksi vaihtoehdoksi NetFlown käyttöönottoa varten, sillä se on vain NetFlowta varten suunniteltu sovellus kuten on NTA:kin, mutta NTA on lisämoduuli laajemmalle sovellukselle, jolloin sekin täytyisi hankkia ja ottaa käyttöön. Kuitenkin kumpikin sovellus tuntui toimivalta ja kummassakin oli omat vahvuutensa, minkä takia kummallekin sovellukselle varmasti löytyy käyttäjiä. PHKK:n tietohallinnon osalta NfSen on kuitenkin parempi vaihtoehto ainakin käyttöjärjestelmän ja hinnan suhteen sekä mikäli tarvetta ei ole laajemmalle, myös SNMP:tä hyödyntävälle verkonvalvontasovellukselle.

Teorian tutkiminen ja käytännön testaukset osoittivat, että NetFlow tarjoaa jotain, mihin perinteisessä SNMP:llä toteutetussa verkonvalvonnassa ei olla pystytty. Tämä jokin on NetFlown kyky tarjota tietoja verkon aktiivilaitteen läpi kulkevan verkkoliikenteen pakettien sisältämistä otsikkotiedoista. NetFlown avulla verkkoliikenteen sisältö aukenee verkonvalvojalle uudella tavalla mahdollistaen liikenteen analysoinnin, jonka avulla voidaan laatia raportteja verkkoliikenteestä, havaita väärinkäytöksiä, tarkkailla ja parantaa verkon suorituskykyä sekä tutkia yksittäisen flown sisältämiä tietoja.

NetFlow tarjoaa selviä hyötyjä verkonvalvontaan liittyen ja NetFlow-dataa voidaan soveltaa erilaisissa tilanteissa tarpeen mukaan riippuen siitä, mitä verkkoliikenteestä halutaan saada selville. Erityisesti NetFlown kyky havaita liikenteen tyyppi porttinumeroiden avulla on hyödyllistä verkkoliikenteen ymmärtämisen kannalta, jolloin havaitaan, minkä tyyppinen liikenne syö eniten kaistaa verkosta, ja näin voidaan esimerkiksi ottaa käyttöön palvelunlaatua koskevia määrityksiä verkon laitteissa. NetFlown mukanaan tuomat hyödyt vaihtelevat verkkoliikenteen kokonaiskuvasta aina yksittäisen flown tarkkoihin tietoihin. Yksittäisen flown tietoja voidaan käyttää hyväksi esimerkiksi haitallisen liikenteen paikantamisessa verkossa. Laajasti sanottuna NetFlow tarjoaa täydellisen näkymän verkon läpi virtaavan datan sisällöstä jättämättä yhtäkään flowta havaitsematta. Tätä dataa

voidaan käyttää monella tavalla useissa eri tilanteissa eli on siis selvää, että NetFlown mukanaan tuomat hyödyt ovat siis moninaiset.

Työn alussa esitellyt tavoitteet toteutuivat hyvin opinnäytetyön aikana. Verkkoliikenteestä saatiin tietoa niin yleisellä kuin yksityiskohtaisellakin tasolla. NetFlown avulla saatiin erilaisia verkkoliikenteen top-listoja selville, joista verkkoa eniten kuormittavat käyttäjät sekä sovellukset selvisivät. NetFlow osoittautui hyödylliseksi protokollaksi, ja jatkossa kannattaisikin miettiä tarkemmin, kuinka NetFlow-dataa voitaisiin hyödyntää ja millaisissa tilanteissa. Lisäksi vapaavalintaisia NetFlow-komentoja on tarjolla reitittimen päässä, joten niihin kannattaisi jatkossa tutustua. Myös useampien NetFlow-sovelluksien testaaminen olisi suotavaa, joten valintaa ei välttämättä kannata tehdä vain näiden kahden testatun sovelluksen perusteella.

LÄHTEET

Bibbs, E. & Matt, B. 2006. Comparison of SNMP Versions 1, 2 and 3. Infosec Writers [viitattu 27.6.2011]. Saatavissa: http://www.infosecwriters.com/text_resources/pdf/SNMP_BMatt.pdf

Caligare. 2006a. Netflow export format [viitattu 9.7.2011]. Saatavissa: http://netflow.caligare.com/netflow_format.htm

Caligare. 2006b. What is netflow? [viitattu 20.7.2011]. Saatavissa: http://netflow.caligare.com/index.htm

Cisco Systems. 2004. Cisco IOS NetFlow Data Sheet [viitattu 5.7.2011]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/product_data_sheet0900aecd80173f71.html

Cisco Systems. 2006. Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting [viitattu 2.8.2011]. Saatavissa: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a0080721701.shtml

Cisco Systems. 2007a. Introduction to Cisco IOS NetFlow – A Technical Overview [viitattu 16.7.2011]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html

Cisco Systems. 2007b. NetFlow Performance Analysis [viitattu 28.7.2011]. Saatavissa: http://www.cisco.com/en/US/technologies/tk543/tk812/technologies_white_paper0900aecd802a0eb9.html

Cisco Systems. 2008. Cisco IOS NetFlow Configuration Guide [viitattu 1.8.2011]. Saatavissa: http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/12_2sr/nf_12_2sr_book.pdf

Cisco Systems. 2011a. Cisco IOS NetFlow [viitattu 5.7.2011]. Saatavissa: http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

Cisco Systems. 2011b. NetFlow version 9 [viitattu 9.7.2011]. Saatavissa: http://www.cisco.com/en/US/products/ps6645/products_ios_protocol_option_home.html

Cisco Systems. 2011c. Configuring NetFlow and NetFlow Data Export [viitattu 20.7.2011]. Saatavissa: http://www.cisco.com/en/US/docs/ios/ios_xe/netflow/configuration/guide/cfg_nflow_data_expt_xe.html#wp1057290

Cisco Systems. 2011d. NetFlow Services Solutions Guide [viitattu 20.7.2011]. Saatavissa: http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html#wp1030114

Cisco Systems. 2011e. Configuring NDE [viitattu 2.8.2011]. Saatavissa: http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SXF/configuration/guide/nde.pdf

Cisco Systems. 2011f. NetFlow MIB [viitattu 16.8.2011]. Saatavissa: http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/nflowmib.html

Cisco Systems. 2011g. NetFlow [viitattu 23.9.2011]. Saatavissa: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/netflow.html

Cisco Systems. 2011h. Cisco IOS NetFlow Command Reference [viitattu 23.9.2011]. Saatavissa: http://www.cisco.com/en/US/docs/ios/netflow/command/reference/nf_02.html#wp1012543

CTDP. 2011. Simple Network Management Protocol [viitattu 23.9.2011]. Saatavissa: http://www.comptechdoc.org/independent/networking/guide/netsnmp.html

Fluke Corporation. 2011. Network Monitoring [viitattu 9.8.2011]. Saatavissa: http://www.flukenetworks.com/Expertise/Learn-About/Network-Monitoring

H3C Technologies. 2008. SNMP Technology White Paper [viitattu 28.6.2011]. Saatavissa: http://www.h3c.com/portal/Products___Solutions/Technology/System_Management/Technology_White_Paper/200805/606347_57_0.htm#_Toc199046592

Haag, P. & Jändling, T. 2011. nfsen. Sourceforge [viitattu 25.3.2011]. Saatavissa: http://sourceforge.net/projects/nfsen/

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. uudistettu, 2. laitos. Jyväskylä: Dovento Finland Oy.

Hautaniemi, M. 1994. TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. TKK, Tietoverkkolaboratorio [viitattu 22.9.2011]. Saatavissa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/SNMP.html

Hunt, C. 1998. TCP/IP verkonhallinta. Helsinki: Suomen Atk-kustannus Oy.

IBR. 2011. SNMP version 3 (SNMPv3) [viitattu 22.9.2011]. Saatavissa: http://www.ibr.cs.tu-bs.de/projects/snmpv3/

ISO/IEC 7498-4. 1989. Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4 : Management Framework [viitattu 22.9.2011]. Saatavissa: http://standards.iso.org/ittf/PubliclyAvailableStandards/s014258_ISO_IEC_7498-4_1989%28E%29.zip

Jacob, D. 2010. Bandwidth Monitoring - NetFlow or SNMP or maybe both ?. Zoho Corporation [viitattu 16.8.2011]. Saatavissa: https://blogs.manageengine.com/netflowanalyzer/2010/01/19/bandwidth-monitoring-netflow-or-snmp-or-maybe-both

Kozierok, C. 2005a. SNMP Version 1 (SNMPv1) Message Format. Kozierok, C. [viitattu 28.6.2011]. Saatavissa: http://www.tcpipguide.com/free/t_SNMPVersion1SNMPv1MessageFormat.htm

Kozierok, C. 2005b. SNMP Version 2 (SNMPv2) Message Formats. Kozierok, C. [viitattu 28.6.2011]. Saatavissa: http://www.tcpipguide.com/free/t_SNMPVersion2SNMPv2MessageFormats.htm

Kozierok, C. 2005c. SNMP Version 3 (SNMPv3) Message Format. Kozierok, C. [viitattu 28.6.2011]. Saatavissa: http://www.tcpipguide.com/free/t_SNMPVersion3SNMPv3MessageFormat.htm

Kozierok, C. 2005d. SNMP Protocol Security Issues and Methods [viitattu 22.9.2011]. Saatavissa: http://www.tcpipguide.com/free/t_SNMPProtocolSecurityIssuesandMethods-2.htm

Nash, K. & Behr, A. 2009. Network Monitoring Definition and Solutions. CIO [viitattu 9.8.2011]. Saatavissa: http://www.cio.com/article/133700/Network_Monitoring_Definition_and_Solutions#whatis

NfSen - Netflow sensor. 2011. Sourceforge [viitattu 25.3.2011]. Saatavissa: http://nfsen.sourceforge.net/

NFDUMP. 2011. Sourceforge [viitattu 25.3.2011]. Saatavissa: http://nfdump.sourceforge.net/

Parker, D. 2005. Understanding the SNMP Protocol. TechGenix Ltd [viitattu 28.6.2011]. Saatavissa: http://www.windowsnetworking.com/articles_tutorials/Understanding-SNMP-Protocol.html

Patterson, M. 2010a. Bandwidth Monitoring: SNMP Vs. NetFlow. Plixer International [viitattu 16.8.2011]. Saatavissa: http://www.plixer.com/blog/netflow/bandwidth-monitoring-snmp-vs-netflow/

Patterson, M. 2010b. Comparing SNMP to NetFlow. LoveMyTool [viitattu 16.8.2011]. Saatavissa: http://www.lovemytool.com/blog/2010/06/comparing-snmp-to-netflow-by-michael-patterson.html

Puska, M. 2000. Lähiverkkojen tekniikka. 2. uudistettu painos. Jyväskylä: Gummerus.

Päijät-Hämeen koulutuskonserni. 2011a. Esittely [viitattu 10.8.2011]. Saatavissa: http://www.phkk.fi/esittely/

Päijät-Hämeen koulutuskonserni. 2011b. Tietohallintopalvelut [viitattu 10.8.2011]. Saatavissa: http://www.phkk.fi/esittely/

RFC 2573. 1999. SNMP Applications. IETF [viitattu 30.6.2011]. Saatavissa: http://www.ietf.org/rfc/rfc2573.txt

RFC 3954. 2004. Cisco Systems NetFlow Services Export Version 9. IETF [viitattu 9.7.2011]. Saatavissa: http://www.ietf.org/rfc/rfc3954.txt

Sloan, J. 2001. Network Troubleshooting Tools. O'Reilly & Associates [viitattu 26.6.2011]. Saatavissa: http://docstore.mik.ua/orelly/networking_2ndEd/tshoot/index.htm

SolarWinds. 2010. NetFlow Traffic Analyzer [viitattu 25.3.2011]. Saatavissa: http://www.solarwinds.com/resources/datasheets/SolarWinds_NTA_Datasheet.pdf

SolarWinds. 2011. Orion NetFlow Traffic Analyzer [viitattu 25.3.2011]. Saatavissa: http://www.solarwinds.com/products/orion/nta/