LIIKENNEANALYSAATTORIT RUNKOVERKOSSA

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2007
Mika Laaksonen

Lahden ammattikorkeakoulu
Tietoliikennetekniikan koulutusohjelma

LAAKSONEN, MIKA: Liikenneanalysaattorit runkoverkossa

Tietoliikennetekniikan opinnäytetyö, 47 sivua

Kevät 2007

TIIVISTELMÄ

Tämä opinnäytetyö käsittelee verkonhallintaa sekä valvontaa. Verkonhallinta jaetaan usein valvontaan ja hallintaan. Valvonta tarkoittaa sitä, että verkkoon ei tehdä mitään muutoksia, vaan sitä ainoastaan tarkkaillaan. Verkonhallinta käsittää sekä tarkkailun että muutoksien teon. Verkonhallinta jakautuu viiteen ITU-T-standardin mukaiseen osa-alueeseen: vikojen hallinta, käytön hallinta, kokoonpanon hallinta, suorituskyvyn hallinta ja turvallisuuden hallinta.

Pääaiheena oli NetFlow-verkonvalvontaprotokolla. NetFlow on Ciscon reitittimissä ja kytkimissä toimiva protokolla, joka tarkkailee IP-flow:ta. NetFlow-laite kerää flow-tiedot NetFlow cacheen ja lähettää niitä 30 - 50 nipuissa UDP-pakettina keräimelle. Keräinpalvelin ottaa raakatiedot vastaan ja tallentaa ne tietokantaan helpommin ymmärrettävässä muodossa. Tämän jälkeen tietokannasta voidaan luoda erilaisia raportteja ja kuvaajia raportointityökalujen avulla.

Toinen tämän opinnäytetyön pääkohdista on SNMP-protokolla, jota käytetään verkonhallintaan tai usein myös pelkkään valvontaan. SNMP on toteutettu siten, että se toimii mahdollisimman yksinkertaisesti ja vähällä komentojen määrällä. SNMP hakee tietoja MIB-tietokannasta. Tämä tietokanta pitää sisällään agentin eli SNMP-laitteen muuttujat. Näitä muuttujia voidaan myös muuttaa, jos on määritelty kirjoitusoikeus. Verkonvalvoja voi esimerkiksi määritellä työpisteeltään jonkin reitittimen käynnistymään uudestaan, menemättä itse paikanpäälle.

Työn NetFlow-osuudessa vertailtiin kahta ohjelmaa, jotka toimivat NetFlow-tiedon analysoijina. Ensimmäinen näistä oli kaupallinen Ciscon kehittämä tietoturvatyökalu CS-Mars. CS-Mars toimitetaan omana koneenaan, jossa ohjelma toimii. Ohjelma on erittäin helppo ottaa käyttöön. Toinen ohjelma oli avoimeen lähdekoodiin perustuva Linuxilla toimiva ilmaisohjelma Stager, joka oli erittäin laadukas, ottaen huomioon että se oli ilmainen. Haittapuolena oli dokumentoinnin vähäinen määrä.

Työn tavoitteena oli parantaa verkon ylläpitäjän näkemystä verkosta. Tulevaisuudessa verkkojen koko vain kasvaa ja hyökkäykset voivat olla aina vain hienostuneempia. NetFlow otettiin käyttöön, jotta saataisiin paremmin selville, miten tieto kulkee verkossa ja ketkä käyttävät verkon resursseja eniten.

Asiasanat: verkonhallinta, verkonvalvonta, SNMP, NetFlow

Lahti University of Applied Sciences
Faculty of Technology

LAAKSONEN, MIKA: Traffic analyzers for core networks

Bachelor's Thesis in Telecommunications Technology, 47 pages

Spring 2007

ABSTRACT

The aim of this thesis was to examine what network management and monitoring is. Network management can be divided to five different categories according to ITU-T standard: management of faults, accounting, configuration, performance and security. Network monitoring only monitors network performance and does not do any changes in it.

The main topic of the thesis is the NetFlow protocol, which is considered to be a network monitoring tool. NetFlow works in routers and switches of Cisco Systems and it monitors IP flows. It records these flows and sends them to a NetFlow collector server. This server then analyses the raw NetFlow data and stores it to a database. Then some report tool can be used to make reports and graphs of net usage.

The thesis also investigates how the SNMP protocol works. SNMP is probably the most widely used network management and monitoring protocol. SNMP queries the data from MIB database, which includes variables of the objects. These Variables can also be configured, if write-permission has been set.

In the NetFlow section of the thesis, two applications used to analyse NetFlow data were examined in theory. One was a commercial product from Cisco Systems that comes with its own hardware and is easy to implement to network. The other was an open source application which was really good considering that it was completely free to use. The problem which comes with the free product is that the documentation is not very good.

In the future it is very important that companies will start to devote more resources to network management. This is because so many new services will move to a network and any shortages in the network may lead to financial losses. New network attacks will be more sophisticated than before. NetFlow-protocol will help to find out how data flows in the network and who uses the data. Most of the network problems can be prevented by good network management.

Key words: network management, network monitoring, SNMP, NetFlow

SISÄLLYS

LYHENNELUETTELO

ACS	Access Control Server. Pääsynhallintapalvelin, joka valvoo, kenellä on pääsy verkkoon ja minkälaiset oikeudet verkon sisällä on.
ASN.1	Abstract Syntax Notation 1. OSI:n standardoima kieli abstraktien kielioppien määrittelemiseksi.
CEF	Cisco Express Forwarding. Ciscon 3. tason skaalautuva IP-verkon kytkentätekniikka.
DoS	Denial of Service. Palvelunestohyökkäys, jossa jonkin palvelun toiminta halutaan lamauttaa esimerkiksi kuluttamalla sen kaista kokonaan.
FTP	File Transfer Protocol. TCP-protokollan tiedonsiirtomenetelmä, joka toimii asiakas-palvelin periaatteella.
ICMP	Internet Control Message Protocol. TCP/IP-pinon kontrolliprotokolla, jolla voidaan kokeilla verkon toimivuutta helposti.
IETF	Internet Engineering Task Force. Internet-protokollien standardoinnista vastaava organisaatio.
IOS	Internetwork Operating System. Ciscon reitittimien käyttöjärjestelmä.
IP	Internet Protocol. TCP/IP-protokollan ydin, joka huolehtii IP-pakettien siirrosta perille pakettikytkentäisessä verkossa.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö, joka tuottaa kansainvälisiä ja kaupallisia standardeja.
ITU	International Telecommunication Union. Kansainvälinen televiestintäliitto, joka koordinoi televiestintäverkkoja ja niiden palveluja.
ITU-T	ITU Telecommunication. ITU telestandardointisektori, joka laatii suosituksia, joilla on käytännössä maailmanlaajuisten standardien asema.
MIB	Management Information Base. SNMP:n käyttämä tietokanta, joka sisältää muuttujat verkonhallintaa varten. SNMP-hakee MIB-tietokannasta laitteiden tiedot.

MPLS	MultiProtocol Label Switching. Yhdistää 2. tason kytkennän ja 3. tason reitityksen IP-verkoiksi
SNMP	Simple Network Management Protocol. Yleisimmin käytetty verkonhallintaprotokolla, joka on pyritty pitämään erittäin yksinkertaisena. Toimii siten, että hallittava laite on agentti ja sitä hallinnoi hallinta-asema.
TCP/IP	Transmission Control Protocol / Internet Protocol. Tietoliikenneprotokollien yhdistelmä. IP vastaa pakettien siirrosta, TCP vastaa päätelaitteiden välisestä yhteydestä, pakettien järjestelystä ja hukkuneiden pakettien uudelleenlähetyksestä.
PDU	Protocol Data Unit. Käytettävä protokolla määrää, mitä PDU sisältää tietyllä OSI-tasolla. Sisältää protokollan ohjaustietoa sekä mahdollisesti käyttäjän tietoja.
QoS	Quality of Service. Palvelunlaatu, joka tarkoittaa tietoliikenteen luokittelua ja suodatusta siten, että tietyt palvelut, kuten VoIP, saavat suuremman prioriteetin kuin toiset.
RFC	Request For Comments. IETF-organisaation julkaisemia Internetiä koskevia suosituksia sisältäviä dokumentteja.
SMI	Structure of Management Information. Säännöt, jotka koskevat MIB-olioiden määritystä.
SQL	Structured Query Language. standardoitu relaatiotietokannan kyselykieli, jossa tietokantaan voidaan tehdä hakuja, muutoksia sekä lisäyksiä.
ToS	Type of Service. IP-paketin palveluluokkakenttä, joka ilmoittaa halutun palveluluokan.
UDP	User Datagram Protocol. TCP/IP-yhteyskäytäntö, joka on yhteydetön, ja näin ollen ei voida varmistaa pakettien perillemenoa tai lähettää hukkuneita pakettaja uudestaan.
UTC	Universal Time Code. Koordinoitu yleisaika, joka seuraa atomikellonaikaa ja tarvittaessa siirtyy sekunnilla korkeintaan kerran vuodessa.

VLAN	Virtual Local Area Network. Virtuaalinen lähiverkko, jossa fyysinen verkko on jaettu loogisiin osiin. Eri osastoja voidaan kytkeä omiksi verkoiksi huolimatta siitä, millainen fyysisen verkon rakenne on.
VoIP	Voice over IP. Tekniikka, jossa ääntä ja videokuvaa siirretään reaaliaikaisesti Internetin välityksellä.
WAN	Wide Area Network. Laajaverkko, joka peittää laajoja maantieteellisiä alueita. Voi yhdistää pienempiä verkkoja yhdeksi isoksi verkoksi.

1 JOHDANTO

Tietoliikenneverkkojen suuri kasvu ja palveluiden siirtyminen verkkoon on johtanut siihen, että verkonhallinta on yhä tärkeämmässä osassa tietotekniikan alalla. Verkonhallinnalla tarkoitetaan tietoverkon eri osa-alueiden valvontaa ja hallintaa. Monet ohjelmistot ovat kuitenkin tulleet ylläpitäjän elintärkeiksi apuvälineiksi. Näiden ohjelmistojen avulla moni verkonhallinnan työvaihe saadaan automatisoitua ja näin ollen ylläpitäjälle jää enemmän aikaa analysoida verkosta saatua informaatiota.

Päijät-Hämeen koulutuskonsernilla on jo käytössään verkonhallintatyökaluja, mutta tarkoitus oli selvittää, millaisia vaihtoehtoja niille löytyisi. Tämä johtui siitä, että kuten muuallakin, niin myös tässä konsernissa verkon koko kasvaa jatkuvasti ja tietoturva on aina vain tärkeämpää. Tässä työssä käydään läpi verkonhallintaa ja analysointia. Työssä vertaillaan kahta eri verkonhallintaprotokollaa, joista toinen valittiin toteutettavaksi. Ensimmäinen näistä SNMP (Simple Network Management Protocol) on jo käytössä Päijät-Hämeen koulutuskonsernissa. Tässä työssä keskitytään tutkimaan NetFlow-protokollaa, joka päätettiin myös ottaa kokeiluun muiden verkonhallintaprotokollien rinnalle.

Työn tavoitteena oli perehtyä tietoliikenneverkon analysointiin runkoverkkotasolla. Työssä oli tarkoitus vertailla erilaisia verkonhallintatekniikoita ja niistä saadun tiedon analysointia. Yhtenä tärkeänä kohtana oli vertailla SNMP- ja NetFlow-protokollien toimintaa. Työn tarkoitus oli parantaa tietoturvaa ja helpottaa verkon ylläpitäjän toimintaa Päijät-Hämeen koulutuskonsernissa. Tavoitteena oli, että verkon ylläpitäjä voisi helpommin seurata verkon käyttöä ja sitä, missä verkon resursseja käytetään eniten.

2 VERKONHALLINTA

2.1 Verkonhallinan perusteet

Tietoverkkojen koko kasvaa jatkuvasti ja verkoista tulee entistä monimutkaisempia ja vaikeammin hallittavia. Verkon laajeneminen ja uudet palvelut, kuten VoIP (Voice Over IP), vaativat aina vain enemmän kaistaa verkolta ja asettavat verkon saatavuudelle tiettyjä vaatimuksia. Palvelut ovat siirtyneet niin suurelta osin verkkoon, että kun verkossa on ongelmia, yritys voi olla täysin halvaantunut ja kärsiä suuristakin ansionmenetyksistä. Tämän vuoksi verkonhallinta ja -valvonta muodostavat hyvin vaikean tehtävän ylläpitäjälle. Ylläpitäjän tulisi aina tietää, mitä verkossa tapahtuu, eikä ongelmia saisi syntyä. Tämä voi olla erityisen hankalaa, koska verkko voi olla niin suuri, että sen tarkkailu ilman oikeita työvälineitä olisi lähes mahdotonta tai se vaatisi useita henkilöitä sitä hoitamaan. Tähän ongelmaan on kehitetty monia erilaisia työkaluja, jotka sekä automatisoivat että helpottavat tietoverkon ylläpitäjän tehtäviä. Esimerkkinä voidaan ottaa tilanne, jossa verkkoon kohdistuu palvelunestohyökkäys ja verkon ylläpitäjän on mahdollista tutkia tulevia paketteja ja selvittää, mikä vika verkossa on. On olemassa useita erityyppisiä protokollia ja palveluita, jotka auttavat ylläpitäjiä virheiden etsinnässä ja verkon hallinnassa. (Hautaniemi 1994; Allen 2002, 1.)

Tietoverkkojen kehittyessä voidaan huomata erityisesti kaksi asiaa, jotka voivat muodostaa suuria ongelmia. Verkkojen monimutkaisuus kasvaa jatkuvasti, ja verkkoon voi tulla monen eri valmistajan laitteita: Tämä vaikeuttaa niiden ylläpitoa, ja koska laitteita on monelta eri valmistajalta, on myös otettava huomioon erilaiset yhteensopivuusongelmat. Verkon ylläpitäjän on osattava konfiguroida erimerkkisiä laitteita, joiden konfiguraatiot voivat erota hyvin paljon toisistaan. Toinen ongelma voi muodostua siitä, että verkko ja sen eri palvelut voivat olla elintärkeitä yritykselle, jolloin verkon tulisi olla aina saatavilla, jotta työ voisi jatkua. Yritys on voinut siirtyä käytännössä kokonaan verkkopohjaisiin puheluihin, jolloin verkon katkos rampauttaa yrityksen puhelinjärjestelmän. Tällöin verkosta on löydettävä ongelmakohdat hyvinkin nopeasti. (Hautaniemi 1994.)

Verkonvalvonta koostuu siis verkonvalvontaan liittyvien tietojen vaihdosta. Tietojen vaihdosta vastaa erillinen valvontaohjelmisto, joka jatkuvasti kerää uutta tietoa verkon tilasta ja sen tapahtumista. Tämä ohjelmisto voi sitten tehdä erilaisia kuvaajia verkon tilasta ja antaa hälytyksiä, kun ongelmia syntyy. Valvontaohjelmiston avulla ylläpitäjä voi myös tarkkailla yksittäisten laitteiden tai jopa niiden porttien toimintaa. (Hautaniemi 1994.)

2.2 Verkonhallinan eri osa-alueet

Verkonhallinta koostuu eri osa-alueista, ja sille voidaan asettaa paljon erilaisia vaatimuksia halutun lopputuloksen mukaan. Käyttäjillä on yleensä aivan erilaiset näkemykset kuin ylläpidolla. ITU-T (International Telecommunication Union) suositus x.700 jakaa verkonhallinnan ja sen vaatimukset viiteen alakategoriaan:

- vikojen hallinta
- käytön hallinta
- kokoonpanon hallinta
- suorituskyvyn hallinta ja
- turvallisuuden hallinta.

Vikojen hallinta auttaa ylläpitäjää paikallistamaan tarkasti ja nopeasti, missä ja minkälainen vika on kyseessä. Tämän jälkeen tulisi myös tietää, miten vika vaikuttaa verkkoon, ja verkkoa tulisi pikaisesti muuttaa tavalla, joka aiheuttaa mahdollisimman vähän häiriöitä. Viallinen laite tulisi eristää muusta verkosta siten, että muu verkko toimii normaalisti viallisesta laitteesta huolimatta. Aina tämä ei kuitenkaan ole mahdollista, mutta sellaiseen topologiaan tulisi pyrkiä, jossa tämä onnistuu. Sitten vian aiheuttanut laite tulisi vaihtaa toimivaan siten, ettei siitä aiheudu liikaa ongelmia muulle verkolle. Tämän jälkeen verkkoon tulisi palauttaa alkuperäiset konfiguraatiot ja verkon pitäisi toimia kuten ennenkin. Verkkoa on kuitenkin vielä tarkkailtava, jotta voidaan todeta, että vika saatiin korjattua ja verkko palautui ennalleen. (Hautaniemi 1994.)

Toinen tärkeä asia verkon ylläpitäjälle on valvoa käyttäjiä ja käyttäjäryhmiä. Käyttäjien tietoja tarvitaan esimerkiksi laskutukseen. Joissakin yrityksissä voi olla tapana laskuttaa eri käyttäjäryhmiä verkon palveluiden käytön mukaan. Myös verkon suorituskyvyn tarkkailu ja tulevaisuuden parannukset tarvitsevat tietoa käyttäjistä. Ylläpitäjän on vain osattava määrittää, mikä on sellaista tietoa, jota kannattaa kerätä. On myös osattava arvioida, kuinka usein tätä koottua tietoa nidotaan yhteen ja analysoidaan. Laskutusvälin tulisi myös olla sopiva, eikä tavallisella käyttäjällä tulisi olla pääsyä laskutustietoihin. Ylläpitäjä voi näin ollen määrätä eri käyttäjäryhmille tietyt kiintiöt, joiden sisällä tulisi pysyä. Jos kiintiö ylitetään, mietitään sopiva toimenpide, jota sovelletaan. Yleisesti ottaen ei ylitystilanteessa kannata katkaista verkkoa suoraan, vaan pyytää ylityksestä raportti, jossa näkyvät syyt ylitykselle. Tämän lisäksi kiintiön ylittämisestä voidaan laskuttaa ylimääräistä kyseiseltä käyttäjäryhmältä. Käytön valvonta antaa työkalun seurata verkon todellista käyttöä ja ylläpitäjä voi helposti nähdä, ovatko resurssit riittävät vai tarvitaanko jossakin uusia laitteita. Verkkoa uusittaessa on myös varmistettava, että kaikki verkkoa kuormittavat palvelut ovat todellisuudessa tarpeellisia. (Hautaniemi 1994.)

Kokoonpanon hallinta koostuu laitteiden konfiguroinnista ja verkon hallitusta muuttamisesta. Ylläpitäjän täytyy tietää, miten konfiguraatioita on muutettava jonkin laitteen vikaantuessa, esimerkiksi kuinka tehdä reititysmuunnokset, jos yksi laite hajoaa. Tämä tarkoittaa sitä, että loogiseen verkkoon tehdään muutoksia, kun fyysisessä verkossa jotakin hajoaa. Laitteet tulee myös osata palauttaa takaisin aikaisempiin asetuksiin, kun vika on saatu korjattua. Ylläpitäjän on jatkuvasti seurattava verkon muutoksia ja sen mukaan muutettava verkkoa, jos se on tarpeellista. Suuremmissa verkoissa tulisi olla täysi ymmärrys käytössä olevista laitteista ja tieto siitä, mitkä ohjelmistoversiot niissä on, jottei synny ylimääräisiä yllätyksiä vian sattuessa. Ylläpitäjän tulisi myös pitää verkko sellaisena, että sen nopeus vastaa käyttäjien tarpeita eikä tukoksia pääsisi syntymään. Yksi kokoonpanon hallinnan tehtävistä on käynnistää ja sammuttaa laitteita hallitusti ja usein automatisoidusti. Tällaiset toimenpiteet olisi hyvä ajoittaa sellaiseen aikaan, kun verkon käyttö on pienimmillään. Verkon laitteisto pitäisi raportoida hyvin, koska joskus käyttäjät voivat pyytää tietoa verkon laitteista, jolloin hyvän raportin pohjalta on

helppoa myös käyttäjille informoida verkon niin uusista kuin vanhoistakin laitteista. (Hautaniemi 1994.)

Suorituskyvyn hallinta kuvaa verkon toimivuutta osittain samalla tavoin kuin käytön hallinta. Nähdään, onko verkon välityskyky tarpeeksi hyvällä tasolla, mitkä ovat palveluiden vasteajat tai onko verkossa jossain kohdassa ”pullonkaula”. Näitä tietoja päästään analysoimaan ja sen lisäksi tulisi olla työkalut verkon hienosäätöön. Vasteajat ja välityskyky ovat tärkeitä tietoja, kun suunnitellaan verkon laajentamista tai parantamista, varsinkin jos kyseessä on suuri verkko. Niiden avulla voidaan myös löytää ja ennaltaehkäistä ”pullonkauloja” verkossa. Tällaisia ongelmia varten on yleensä ratkaisuna muuttaa joitakin reititystietoja, jolloin liikenne jakautuu eri reiteille. Suorituskyvyn valvonta keskittyy lähinnä verkon valvontaan, ei sen palveluiden. Se myös tarjoaa paljon tietoa verkon resurssien käytöstä. (Hautaniemi 1994.)

Turvallisuuden hallinnalla tarkoitetaan sitä, kenellä on pääsy verkosta kerättyihin tietoihin, tai kenellä on pääsy verkossa oleviin laitteisiin. Kyse on siis lokien tallentamisesta turvalliseen paikkaan ja niiden analysoinnista. Turvallisuuden hallinnalla ei puolestaan tarkoiteta käyttäjien tai käyttäjäryhmien oikeuksien määrittelyä. Käytännössä tarkoitus on turvata verkon resurssit ja tarjota työkalut käyttäjien tietojen turvaamiseksi. Käyttäjille on myös kerrottava, että verkko on turvallinen ja itse ylläpito on myös hyvin turvattu. Jos joku kuitenkin yrittää kiertää ennalta määriteltyjä sääntöjä, on tästä tultava ylläpidolle tieto välittömästi. Turvallisuuden hallinnalla turvataan tietojärjestelmiä ja tuetaan verkon sisäisiä tarkistuksia. Jos yrityksellä on olemassa hyvin tiedotettu turvallisuuden hallinta, jo pelkästään tämä tieto vähentää murtautumisyrityksiä huomattavasti. On myös hyvä, että ylläpito pääsee nopeasti pysäyttämään murtautumisyritykset, koska tänä päivänä myös monet kriittiset palvelut toimivat verkossa, kuten palkanmaksujärjestelmät. (Hautaniemi 1994.)

3 SNMP

3.1 SNMP-protokolla

Verkko tarjoaa monia palveluita ja protokollia. Kaikki laitteet eivät kuitenkaan aina liikennöi verkon tarjoamien protokollien mukaisesti. Tämän lisäksi ylläpitäjän tulisi olla selvillä verkon tapahtumista, muuttaa reititystietoja sekä selvittää jo syntyneitä ongelmia. On mahdollista, että ylläpitäjän on hallittava myös laitteita, jotka eivät ole fyysisesti samassa verkossa, mutta tämä onnistuu sen vuoksi, että SNMP-protokolla toimii kuljetuskerroksen yläpuolella. Tällöin ei haittaa, vaikka samassa verkossa olisi useita erilaisia laitteita ja näin ollen liikennöinti voi tapahtua monia eri protokollia käyttäen. Käytössä on tällöin vain yksi hallinnointiprotokolla, ja se helpottaa ylläpitäjän työtä. Koska hallintaprotokolla toimii sovellustasolla, voi kuitenkin syntyä helposti erinäisiä ongelmia. Käyttöjärjestelmä, IP-ohjelmisto tai kuljetusprotokollat voivat aiheuttaa siinä määrin ongelmia, ettei ylläpitäjä välttämättä saa yhteyttä vialliseen reitittimeen. Ongelmia voi syntyä esimerkiksi siitä, että reitittimen reititystaulu vaurioituu. Tällöin ei välttämättä saada enää etäyhteyttä reitittimeen, jotta voitaisiin korjata reititystaulu tai käynnistää laite uudestaan. Tällainen tuotantoverkon käyttäminen verkonhallintaan on nimeltään inbound-hallintaa. Inbound-hallintaa käytettäessä verkon vikaantuminen voi johtaa siihen, että menetetään myös hallintayhteys verkon laitteisiin. Out-of-bound-hallinta ei ole riippuvainen verkon toimivuudesta, vaan laitteisiin ollaan yhteydessä erillisen verkon kautta. Esimerkkinä reitittimen yhteys käyttäen konsolikaapelia, jolloin nähdään myös kaikki käynnistyksen tekstit, toisin kuin inbound-hallinnassa. (Comer 2002, 553.)

Ongelmia on toki ollut olemassa, mutta ne ovat olleet pieniä verrattuna hyötyyn, joka on saatu käytettäessä sovellustason TCP/IP-hallintaohjelmia. Tämä hallintaohjelma sijaitsee tavallisesti ylläpitäjän työasemassa, ja tätä ohjelmaa kutsutaan asiakasohjelmaksi (MC, Management Client). Hallittavat laitteet puolestaan ovat niin sanottuja agentteja (MA, Management Agent), joissa pyörii palvelinohjelma. Yhteys toteutuu siten, että ylläpitäjä määrittää asiakasohjelmaan agentin, johon haluaa olla yhteydessä. Kun yhteys on saatu muodostettua, voi ylläpitäjä pyytää

agentilta erinäisiä tietoja tai muuttaa laitteen asetuksia lähettämällä sille komentoviestejä. Jos verkko on todella laaja, tarvitaan useampia ylläpitäjiä, koska laitteita voi olla liikaa yhden henkilön hallittavaksi. Yleisesti ylläpitäjä hallitsee vain oman toimipaikkansa laitteita ja muilla toimipaikoilla on omat ylläpitäjänsä. Hallintaohjelma sisältää käyttöoikeuksien hallinnan ja näin ollen voidaan varmistaa, että laitteita voivat hallinnoida vain ne käyttäjät, jotka ovat siihen oikeutettuja. Asetukset voidaan esimerkiksi määritellä siten, että useammalla ylläpitäjällä on oikeus lukea ja tarkastella laitteiden asetuksia, mutta vain osalla on oikeus muokata niitä. (Comer 2002, 554; Kaario 2002, 273.)

SNMP on standardi verkonhallintaprotokolla, kun käytössä on TCP/IP-verkko. Protokollasta on julkaistu kolme eri versiota, jotka eivät kuitenkaan suuresti poikkea toisistaan. Jokaisessa versiossa käytetään samanlaista kehystä ja siten myös monet ominaisuudet ovat taaksepäin yhteensopivia. Protokolla itsessään määrittelee kuljetusprotokollan käytön, sanomien rakenteen ja toiminnot, joilla se hakee ja vie tietoja. Toiminnot voidaan suorittaa helposti käyttämällä vain muutamia komentoja. Eniten versiot eroavat toisistaan tietoturvamielessä. (Comer 2002, 554.)

3.2 MIB-tietokanta

Laitteissa on olemassa tiettyjä tietoja, joita ylläpitäjä voi tarkastella ja muuttaa. Esimerkiksi kytkimessä on oltava tiedot liityntöjen tiloista ja liikenteen määrästä. Ylläpitäjä voi sitten tarkastella näitä tietoja ja analysoida niitä. SNMP-standardi itsessään ei määrittele, mitä tietoja laitteesta tulisi saada ulos, vaan tätä varten on olemassa erillinen standardi. Käytetään standardia nimeltä MIB (Management Information Base), joka määrittelee tiedot, jotka laitteen tulisi sisältää, miten näitä tietoja voidaan käyttää ja mikä merkitys kyseisillä tiedoilla on. Esimerkkinä voidaan mainita IP:n MIB, jonka määritys on, että kaikki tietyn liitynnän kautta saapuneet oktetit tulisi laskea ja verkonhallintaohjelmalla on tähän laskuriin pelkästään lukuoikeus. (Comer 2002, 556; Reynders & Wright 2003, 151.)

Hallittavat tiedot jakautuvat MIB-tietokannassa useisiin eri luokkiin. MIB-tietokantaa voidaan ajatella puumaisena. Eri luokat voivat sisältää useita oksia ja

kaikki on lähtöisin yhdestä juurikohdasta (katso KUVIO 1). MIB-määräykset on pidetty tarkoituksella erillään verkonhallintaprotokollasta. Tämä on hyödyllistä niin valmistajan kuin käyttäjänkin näkökulmasta. Valmistajan ei tarvitse huolehtia kuin laitteen SNMP-agentista, vaikka uusia MIB-tietoja tulisikin myöhemmin käyttöön. Käyttäjä voi tehdä MIB-kyselyitä kaikkiin verkon laitteisiin, vaikka ne käyttäisivätkin eri versiota MIB:stä. Jos joitakin MIB-tietoja ei kuitenkaan kyseisestä laitteesta ole saatavilla, osaa laite itse palauttaa virhesanoman, että kyseisiä tietoja ei löydy. (Comer 2002, 557.)

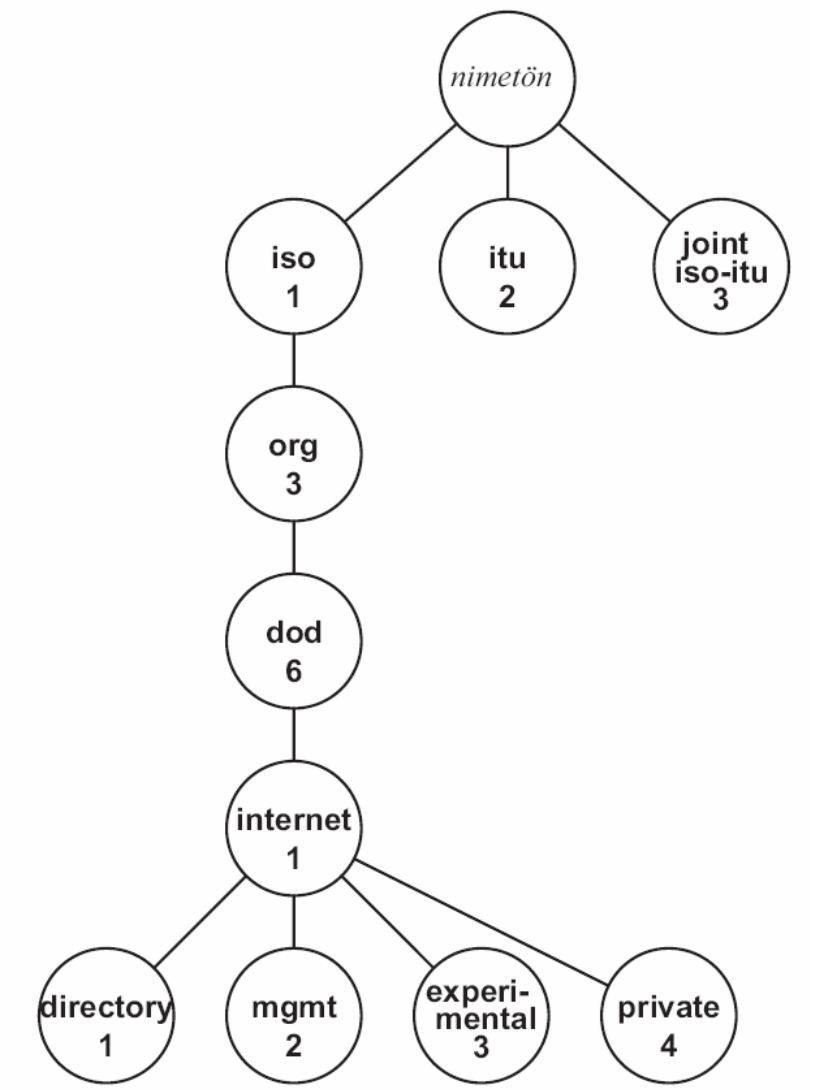
SNMP:n kahdessa ensimmäisessä versiossa kaikki muuttujat kerättiin yhteen laajaan MIB-tietokantaan. Nämä kaikki muuttujat määriteltiin sitten yhdessä RFC-dokumentissa (Request For Comments). Seuraavaksi otettiin käyttöön MIB-II-tietokanta, jossa valittiin täysin toisenlainen strategia. IETF (Internet Engineering Task Force) päätti, että jokaisen laitetyypin muuttujat tulisivat omaan MIB-tietokantaansa. Standardointiprosessi on sittemmin synnyttänyt toistasataa MIB-dokumenttia ja yli 10 000 muuttujaa. (Comer 2002, 557.)

Useimmat MIB-tietokannassa olevat arvot ovat numeerisia muuttujia. Kukin näistä arvoista voidaan ilmoittaa jonakin kokonaislukuna. On kuitenkin olemassa monimutkaisempiakin tietokantarakenteita, jotka MIB määrittelee. Yhtenä esimerkkinä näistä voidaan ottaa ipRoutingTable-muuttuja, joka nimensä mukaisesti sisältää kyseisen laitteen koko reititystaulun. Tiettyjen muuttujien avulla voidaan sitten katsoa tiettyjä kenttiä reititystaulusta, kuten verkko-osoite. Reititin itsessään voi sisältää tiedot erilaisessa muodossa, kuin MIB-määritys sanelee. Agentin tehtävänä on tällöin muuttaa tiedot oikeaan muotoon kyselyn tullessa. (Comer 2002, 558.)

On olemassa tietyt säännöt, jotka määrittävät MIB-muuttujien tunnistamisen ja määrittämisen. Tämä standardi on nimeltään SMI (Structure of Management Information). SMI määrittää kuitenkin vain muutaman muuttujatyypin ja säännöt, jotka koskevat niiden nimeämistä, jottei verkonhallintaprotokollista tulisi aivan liian monimutkaisia. Määritys sisältää säännöt esimerkiksi IP-osoitteelle (IpAddress, 4 oktettia sisältävä merkkijono) ja määrittää, mitä termejä käytetään MIB-

muuttujien määrittelyssä. SMI sisältää myös tiedot siitä, miten MIB-tietokannan tulee viitata taulukon arvoihin, esimerkiksi viitatessa reititystauluun. (Comer 2002, 558.)

MIB-tietokanta on siis hieman puun mallinen, hierarkinen järjestelmä. Juurella ei ole nimeä, mutta sen alla sijaitsevat kolme haaraa ISO (International Organization for Standardization), ITU ja ISO sekä ITU yhdessä. Jokainen näistä haaroista sisältää tietyn kokonaisluvun ja haaran nimeä kuvaavan merkkijonon. Ohjelmat käyttävät pelkästään kokonaislukua, joista ne voivat sitten muodostaa nimen. ISO-haara, numero 1, on haara, jota käytetään kun haetaan joitakin tietoja agentista. Kukin tieto saadaan haettua tietyn numerosarjan takaa, esimerkkinä Internet Management, lyhyemmin mgmt, löytyy numerosarjan 1.3.6.1.2 takaa. Tämä haara sisältää numerolla 1 mib-haaran, jonka alta löytyvät esimerkiksi liityntöjen tiedot. Kyseinen numerosarja voidaan myös kirjoittaa merkkijonoilla, jolloin se on muotoa iso.org.dod.internet.mgmt.mib. (Comer 2002, 559.)



KUVIO 1. MIB-tietokannan rakenne (Comer 2002, 560)

Verkonhallintaprotokolla määrittelee, kuinka agentin ja asiakasohjelman välinen kommunikointi tapahtuu. Tämän lisäksi on määrittely sille, mikä sanomien rakenne on ja mikä merkitys niillä on. Lisäksi on määritelty hallittavien laitteiden hallinnolliset suhteet, mikä mahdollistaa sen, että ylläpitäjä voi määritellä käyttöoikeuksia kyseisiin laitteisiin. Voidaan ajatella, että verkonhallintaprotokolla voisi sisältää erittäin suuren määrän komentoja, kuten uudelleenkäynnistyksen tai reittien lisäyksen sekä poiston, mutta tämä tekisi protokollasta vain monimutkaisemman. Tällöin joka toiminto vaatisi oman komennon ja protokollaa jouduttaisiin muuttamaan, jos otettaisiin käyttöön uusia tietoja. SNMP:tä on kuitenkin lähdetty toteuttamaan yksinkertaisemmalla mallilla. Käytännössä ylläpitäjällä on käytös-

sään ainoastaan kaksi komentoa, joiden avulla voidaan hakea jonkin muuttujan arvo tai tallentaa tilalle uusi arvo. Kaikki muut komennot pohjautuvat näihin kahteen komentoon. Ei ole mahdollista käyttää komentoa, joka käynnistäisi laitteen uudestaan, vaan on määriteltävä laitteeseen uusi arvo kenttään, joka sisältää tiedon monenko sekunnin kuluttua laite on käynnistettävä uudelleen. Laittamalla nolla tähän kenttään laite luonnollisesti käynnistyy uudelleen heti. Koska käytössä on vain kaksi komentoa, voidaan ajatella, että järjestelmä toimii vakaasti sekä on hyvin joustava ja yksinkertainen. Vakaus tulee siitä, että vaikkakin MIB-tietokantaan lisättäisiin uusia muuttujia, ei SNMP:n määrityksiä tarvitse muuttaa millään tavalla. Uusille muuttujille voidaan myös helposti määritellä uusia lisätoimintoja. SNMP:n toiminta on suhteellisen yksinkertaista, joten se on helppo ymmärtää. Näin ollen vikojen selvittäminen on helppoa ja yksinkertaista. Ylläpitäjälle SNMP on vain näkymätön työkalu, jota voidaan käyttää tavalliseen verkon hallintaan. Useimmat hallintaohjelmat sisältävät kuitenkin graafisen liittymän, josta voidaan tarkastella esimerkiksi verkon topologiaa kuvana, josta sitten voi hiiren klikkauksella vaikkapa sammuttaa jonkin reitittimen. (Comer 2002, 564.)

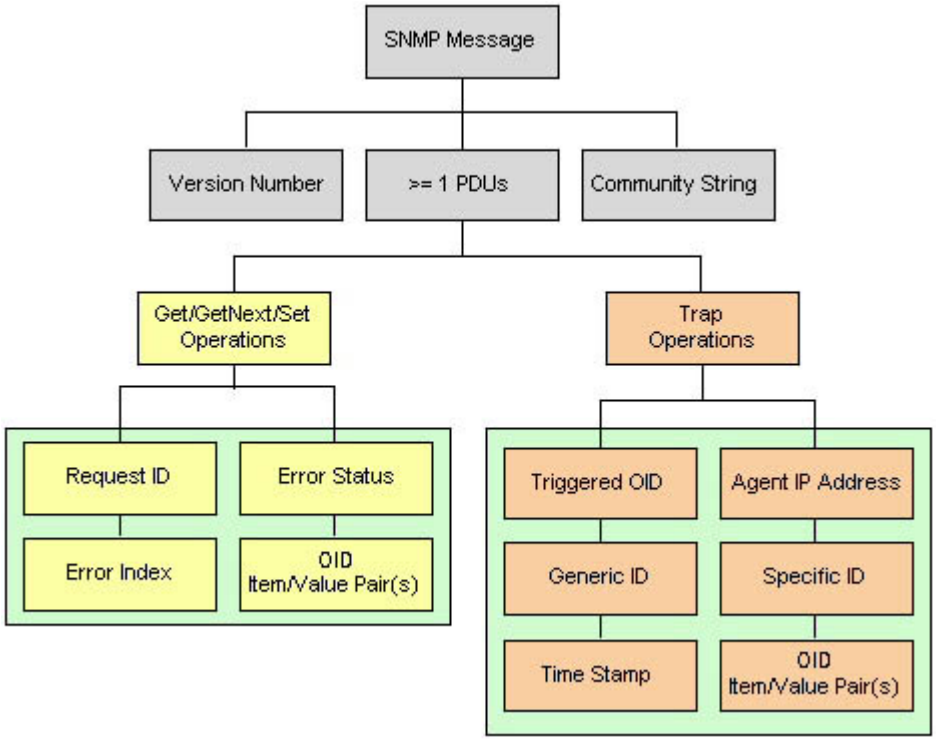
3.3 SNMP:n komennot

Itse komennot, jotka ovat SNMP-protokollan pääosassa, ovat get-request, jolla haetaan tietoa, ja set-request, jolla voidaan asettaa jokin arvo. Vastausta varten on olemassa response-toiminto. Toiminnot on toteutettu siten, että jos jokin pyyntö kohdistuu useampaan muuttujaan kerralla ja jokin näistä on virheellinen, ei mitään arvoja palauteta tai muuteta. Ylläpitäjä voi asettaa agenttiin niin sanotun trap-toiminnon, jolloin tietyn tapahtuman sattuessa agentti lähettää trap-viestin. Yksinkertainen esimerkki trap-toiminnosta on verkkoliitynnän tila, jos se muuttuu, lähetetään trap-viesti. Joskus asiakasohjelma ei välttämättä tiedä taulukon kaikkien muuttujien numerotunnistetta. Tällöin voidaan turvautua apukomentoon get-next-request, jolloin tiedetään kohta, josta on viimeksi haettu arvo ja nyt haetaan seuraavan kentän arvoa. (Comer 2002, 565.)

3.4 SNMP-viestin rakenne

SNMP-viesti poikkeaa muista TCP/IP-protokollan viesteistä huomattavasti siten, ettei se sisällä ollenkaan kiinteitä kenttiä. Tämä ei ole ongelma ohjelmille, mutta ihmiselle voi olla vaikea hahmottaa ja ymmärtää tällaista viestiä. Viesti pohjautuu ASN.1-kielioppiin (Abstract Syntax Notation). ASN.1 on eräänlainen ISO:n kehittämä kuvauskieli. Kieli sisältää kaksi tapaa esittää asiat, ensimmäinen on ihmisten luettavaksi tarkoitettu ja toinen on koneita varten kehitetty. (Comer 2002, 566.)

SNMP-viesti sisältää neljä peruselementtiä, joista ensimmäisenä on kokonaisluku, joka ilmoittaa versionumeron (katso KUVIO 2). Seuraavaksi tulee otsikon lisätietoja, joukko erilaisia suojausparametrejä sekä datakenttä, jossa itse tieto sijaitsee. Datakenttä on sitten jaettu pienempiin osiin, joita kutsutaan nimellä PDU (Protocol Data Unit). Näistä kukin sisältää joko pyynnön tai vastauksen. Käytettäessä SNMP:n versio 3:sta, tämä kenttä voi sisältää salattua tekstiä. (Comer 2002, 567.)



KUVIO 2. SNMP-viestin rakenne (Garcia 2002)

3.5 SNMP:n tietoturva ja eri versiot

Peruspiirteiltään eri SNMP-versiot ovat melko samanlaisia. Ensimmäinen versio eli SNMPv1 määriteltiin vuonna 1990, ja se on luultavimmin yhä eniten käytetty versio. Kolme vuotta myöhemmin määriteltiin SNMPv2, joka sisälsi kaksi uutta viestiä. Nämä olivat get-bulk, jolla voidaan pyytää useita tietoja tekemättä pitkää get-next-putkea, sekä inform, jolla voidaan viestittää tapahtumista muille hallinta-asemille. SNMPv2 toi muutoksia myös MIB-tietokannan määritelmiin. Kaksi ensimmäistä versiota eivät ole täysin yhteensopivia keskenään. Tämän vuoksi on yritetty monia erilaisia ratkaisuja, jotta ne saataisiin keskenään yhteensopiviksi. SNMPv2:ssa yritettiin parantaa myös tietoturvaa lisäämällä tiedon eheystarkistusta ja käyttäjän todentamista. Tämä kuitenkin lisäsi myös protokollan monimutkaisuutta. SNMPv2:ta ei otettu kovinkaan yleisesti käyttöön, koska yleinen käsitys oli, että sen määritelmä on puutteellinen. (Hautaniemi 1994.)

Uusin SNMPv3 on suunniteltu siten, että mukana olisi tietoturvan lisäksi skaalautuvuutta. Tietoturvaa suunniteltaessa on pyritty siihen, että suojauskäytännöt olisivat yleisiä ja joustavia. Samalla niiden on kuitenkin oltava sellaisia, että niitä on helppo hallita. Versio 3 sisältää esimerkiksi sanomien todennuksen, yksityisyyttä, valtuuksien tarkistusta, asetusten etämäärityksen sekä tiedon salauksen. Näiden muutosten ansiosta kolmas versio on huomattavasti parempi tietoturvaltaan kuin aiemmat versiot. Versio 3 on myös tehty yksinkertaisemmaksi kuin versio 2. (Comer 2002, 572.)

Tietoturvaa tarvitaan sen takia, ettei kuka tahansa pääse vaihtamaan verkon laitteiden asetuksia. Joku voisi esimerkiksi vaihtaa joitakin asetuksia siten, ettei verkko toimi tai vaikkapa käynnistää laitteen uudelleen. SNMPv1:ssä käyttäjän varmennukseen käytetään salasanana yhteisötunnusta (Community name) ja IP-osoitteen tarkistusta. Salasanaa ei kuitenkaan ole suojattu verkossa mitenkään ja IP-osoitekin on melko helppo väärentää. Tämän vuoksi versiota 1 käytettäessä ei tulisi käyttää set-viestejä, vaan ainoastaan get-viestejä, joilla voi suorittaa verkonvalvontaa. SNMPv2:ssa yritettiin toteuttaa tietoturvaa huonolla menestyksellä. SNMPv3 puolestaan kiinnittää enemmän huomiota turvallisuuteen, ja tällä kertaa ratkaisun pitäisi olla melko hyvin toimiva, vaikkakin jotain turva-aukkoja on jo

löytynyt. SNMPv3 ei ole täysin erillään toimiva, vaan se tuo tietoturvaa, mutta käyttää kuitenkin version 1 tai 2 PDU:ta. (Hautaniemi 1994.)

4 NETFLOW

4.1 NetFlow-verkonvalvontaprotokolla

NetFlow on Cisco Systemsin kehittämä työkalu, joka auttaa verkon ylläpitäjää kuvaamaan ja ymmärtämään verkon toimintaa. Ylläpitäjän tulisikin tietää, mitä verkossa tapahtuu seuraavilla osa-alueilla:

- ohjelmistojen verkon käyttö
- verkon tuottavuus ja resurssien käyttö
- muutoksien vaikutus
- verkossa tapahtuvat poikkeavuudet ja tietoturva-aukot sekä
- mukautumisongelmat pitkällä tähtäimellä.

Cisco IOS (Internetwork Operating System) NetFlow auttaa selvittämään näitä edellä mainittuja asioita. Se auttaa luomaan ympäristön, jossa verkonhoitajan on helppo selvittää, kuka, mikä, milloin, missä ja miten verkko toimii. Kun ymmärretään täysin, miten verkko toimii, voidaan paremmin tarkastella sen käyttöä. Lisääntynyt tieto auttaa haavoittuvuuksien etsinnässä, kun tutkitaan verkon tehokasta käyttöä. NetFlow on käytössä lähinnä Ciscon laitteissa, mutta myös Juniperin laitteet tukevat NetFlow:n versioita 5 ja 8. Juniperin laitteissa käytetään nimitystä cflowd. (Introduction to Cisco IOS NetFlow - A Technical Overview; Gredler & Semeria 2001, 9.)

Perinteisesti yrityksillä on käytössä ainoastaan SNMP, kun tarkkaillaan verkkoa. SNMP kylläkin auttaa verkon kapasiteetin suunnittelussa, mutta se ei anna minkäänlaista kuvaa siitä, miten esimerkiksi jokin ohjelma käyttää verkkoa. Ohjelmien verkon käyttö olisi kuitenkin syytä ottaa huomioon kun suunnitellaan verkon parannuksia. Tämän päivän IP-verkoissa pakettilaskurit ovat käytännöllisiä, mutta tieto siitä, mistä ja mihin liikenne kulkee, on korvaamatonta. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Verkon toiminnan, saatavuuden ja vianetsinnän kannalta on kriittistä, että ylläpitäjällä on kyky ymmärtää IP-liikennettä ja sen reittejä. Ymmärrys helpottaa ver-

kon suunnittelua ja takaa sen, että verkkoa käytetään siten, kuin on alun perin suunniteltu. NetFlow auttaa päättämään koska tulisi käyttää QoS:ää (Quality of Service), miten verkon käyttöä voitaisiin optimoida ja sillä on suuri rooli tietoturvassa, koska se voi huomata DoS-hyökkäykset (Denial of Service), verkkoa tukkivat madot ja muut ei-toivotut verkon tapahtumat. NetFlow auttaa ratkaisemaan monia ongelmia:

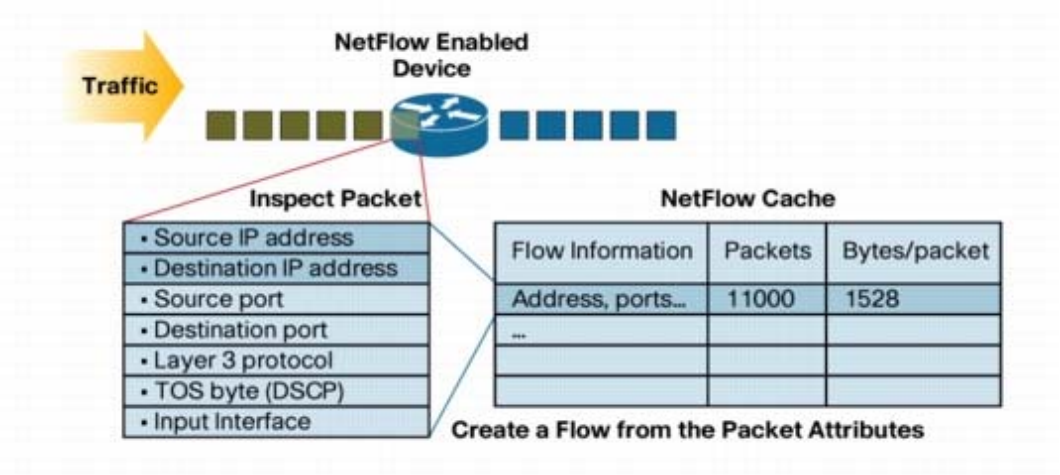
- analysoimalla, miten uudet ohjelmat kuormittavat verkkoa
- tutkimalla WAN-liikennettä (Wide Area Network)
- vianetsinnässä ja ”pullonkaulojen” poistossa
- poikkeavuuksien havaitsemisessa ja turvallisuuden parantamisessa ja
- QoS-parametrien tarkastelussa ja niiden toiminnassa.

(Introduction to Cisco IOS NetFlow - A Technical Overview.)

4.2 Flow:n koostumus

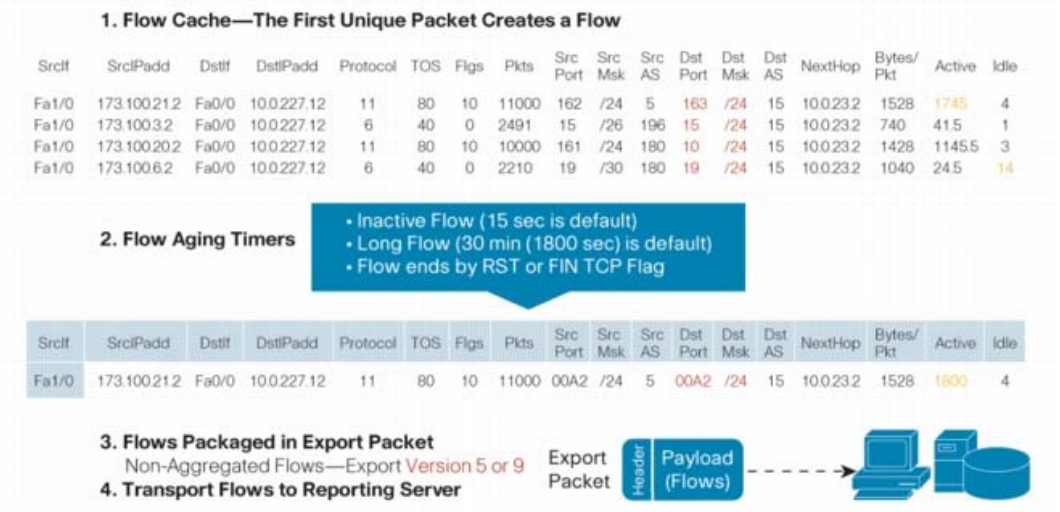
Flow:ta käytettäessä jokainen paketti, joka kulkee reitittimen tai kytkimen läpi, tutkitaan ja näiden ominaisuuksien perusteella nähdään, onko paketti ainutlaatuinen vaiko samanlainen kuin edelliset paketit (katso KUVIO 3). Näitä ominaisuuksia ovat

- IP lähde- ja kohdeosoite
- lähde- ja kohdeportti
- 3. tason protokollatyyppi
- Class of Service sekä
- reitittimen tai kytkimen liityntä.



KUVIO 3. Flow:n koostumus (Introduction to Cisco IOS NetFlow - A Technical Overview)

Kaikki paketit, joissa yhdistyvät samat tiedot, tyypillisesti viisi seitsemästä kentästä, yhdistetään yhdeksi flow:ksi ja tämän flow:n paketit ja tavut lasketaan. Tästä syystä NetFlow skaalautuu hyvin, koska suuri määrä verkon tietoja saadaan näin tiivistettyä NetFlow-tietokantaan, jota kutsutaan nimellä NetFlow Cache (katso KUVIO 4). NetFlow Cache sisältää flow-tiedot kaikista avoinna olevista yhteyksistä. (Introduction to Cisco IOS NetFlow - A Technical Overview.)



KUVIO 4. Flow Cache (Introduction to Cisco IOS NetFlow - A Technical Overview)

Tätä flow-tietoa voidaan sitten käyttää hyväksi, kun tutkitaan, miten verkko käyttäytyy. Lähdeosoite tarjoaa käsityksen siitä, mistä liikenne on lähtöisin. Kohde-

osoitteesta nähdään, mihin liikenne on matkalla. Porttinumeroista voidaan päätellä, mitkä ohjelmat käyttävät verkkoa. Class of Service tutkii verkon käytön prioriteetteja. Laitteen liityntä kuvastaa sitä, kuinka hyvin kyseistä laitetta käytetään hyväksi ja lasketut paketit ja tavut kuvastavat liikenteen määrää. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Flow tekee myös aikamerkintöjä, jotka auttavat ymmärtämään sen ”elämää”. Aikamerkintöjen avulla saadaan myös laskettua pakettien ja tavujen nopeus sekuntia kohden. Flow kertoo myös seuraavan hypyn osoitteen, joten tiedetään mitä reittiä se kulkee. Lisäksi se sisältää aliverkon peitteet lähde- ja kohdeosoitteille, joten voidaan laskea prefiksejä. Mukana ovat myös TCP lippu -tiedot, joista voidaan tutkia TCP:n kättelyä. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

4.3 NetFlow-tietojen tutkiminen

NetFlow:n tuottamaa tietoa voidaan tutkia kahdella eri tavalla. Ensimmäinen tapa on käyttää laitteen komentokehotteessa show-komentoja, toinen tapa on käyttää jotakin raportointiohjelmistoa. Ensimmäinen keino on hyvä, jos halutaan nopeasti tietää mitä verkossa on juuri meneillään, tai kun suoritetaan vianetsintää. Toinen vaihtoehto on käyttää erillistä palvelinta, joka kerää NetFlow-tietoa ja tekee siitä helposti luettavia raportteja. Tällöin on kyseessä NetFlow-keräin, joka kokoaa ja yhdistää flow:t. Tämän jälkeen se luo niistä juuri sellaisia raportteja, kuin käyttäjä haluaa ja tarvitsee, tutkiakseen verkon toimintaa ja turvallisuutta. SNMP:stä poiketen NetFlow-laite lähettää tietoa palvelimelle aina kun sitä on. Käytännössä reitittimen tai kytkimen NetFlow Cache kerää taukoamatta uusia flow:ta ja NetFlow samalla etsii sellaisia flow-tietoja, jotka olisivat jo päättyneet, jotta se voisi lähettää ne NetFlow-keräimeen. NetFlow Cache sisältää hienostuneita algoritmeja, jotka osaavat lajitella paketit oikeisiin flow-tietoihin. Flow katsotaan terminoituneeksi silloin, kun kommunikaatio on loppunut, eli esimerkiksi kun paketti sisältää TCP FIN -lipun. Reitittävä laite tarkistaa NetFlow Cachen kerran sekunnissa etsiäkseen lähetettävää tietoa. Tavallisesti noin 30–50 flow:ta yhdistetään yh-

deksi paketiksi ja tämä sitten lähetetään UDP:n (User Datagram Packet) yli keräimeen. Keräimen ohjelmisto voi sitten luoda yksityiskohtaisia raportteja tapahtumista lähes reaaliaikaisesti. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Flow on valmis, kun se on tietyn ajan toimeton (esimerkiksi ei uusia paketteja tiettyyn aikaan) tai kun se on ollut pitkään aktiivisena ja kestää kauemmin kuin aktiivisuusajastin (esimerkkinä pitkä FTP, eli File Transfer Protocol -siirto). Ajastimet osoittavat, milloin flow on päättynyt tai ollut liian pitkään aktiivinen. Vakiona toimettomuusaika on 15 sekuntia ja pitkän aktiivisuuden aika on 30 minuuttia. Nämä arvot on mahdollista muuttaa haluamakseen, mutta normaaliajat ovat suositeltavia. Keräin osaa yhdistää pitkään kestäneet flow:t yhteen, jolloin pitkä FTP-siirtokin näkyy lopulta yhtenä yhteytenä. Toinen tapa, josta nähdään, että flow on valmis, ovat TCP:n liput. Joissakin tapauksissa flow-tiedot voidaan joutua siirtämään eteenpäin ennen kuin ne ovat valmiit. Tähän voi olla syynä se, että NetFlow-laitteesta loppuu muisti kesken, tai se, että laskurit menevät ympäri. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Tyypillinen sijoituspaikka NetFlow:lle on keskusreititin, koska kaikki liikenne kulkee sen kautta ja NetFlow saa näin ollen kerättyä tiedot kaikesta liikenteestä. Sijoituspaikka voi kuitenkin vaihdella käyttötarkoituksen ja verkon topologian vuoksi. Jos keräinpalvelin sijoitetaan keskeiseen paikkaan, olisi hyvä myös NetFlow ottaa käyttöön sen lähelle. NetFlow voidaan toki sijoittaa kauemmaksi keräävästä palvelimesta, mutta tällöin on muistettava, että se käyttää jonkin verran kaistaa lähettäessään flow-paketteja: tavallisesti kyseessä on noin 1,5 % kaikesta liikenteestä. Lähes kaikki Cisco IOS 11.1 jälkeen tulleet Ciscon reitittimet ja kytkimet tukevat NetFlow:ta. Tarjolla on myös hajautettuja palvelinratkaisuja, joissa monet palvelimet toimivat keräiminä ja lähettävät tiedot edelleen yhdelle keskuspalvelimelle, joka sitten yhdistää tiedot ja tekee niistä raportit. Sijoitusta mietittäessä on myös muistettava, että NetFlow käyttää liikennöintiin UDP-protokollaa, joka on yhteydetön eikä osaa huomata verkon tukkeita. Tällöin vaarana on pakettien menettäminen. Tämä ongelma voidaan kiertää käyttämällä omaa linjaa reitit-

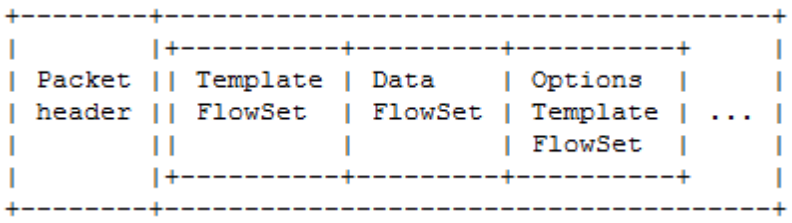
timen ja keräimen välillä. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Keräinpalvelinohjelmia on saatavilla suuri määrä, mukaan lukien Ciscon omat ohjelmat, freeware-ohjelmat sekä kolmannen osapuolen kaupalliset ohjelmat. Ohjelmaa valitessa tulisi kiinnittää huomiota moniin eri asioihin: Ensimmäiseksi on mietittävä mikä tulee olemaan pääkäyttökohde; Halutaanko keskittyä turvallisuuden tutkintaan, kapasiteetin suunnitteluun vai liikenteen analysointiin ja ohjelmien verkon käytön monitorointiin. Seuraavaksi on päätettävä, halutaanko raportit reaaliaikaisena vai historiaraportteina. On myös muistettava tarkistaa, että ohjelma on oikealle käyttöjärjestelmälle. Yksi vaikuttava tekijä on myös verkon koko ja se, tarvitseeko ohjelman olla kuinka hyvin skaalautuva. Sitten on myös ajateltava kustannuksia ja sitä, että olisiko yrityksellä jo käytössä jokin ohjelma, joka tukee myös NetFlow:ta. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

4.4 NetFlow-versiot ja paketin rakenne

NetFlow-laitteesta ulostuleva tieto riippuu käytettävästä versiosta. Ensimmäinen versio oli 1 ja se sisälsi NetFlow-toiminnot, tätä versiota ei juurikaan enää käytetä. Versio 5 otti mukaan flow-sekvenssinumerot. Versio 7 lisäsi Cisco Catalyst -kytkimiin NetFlow-tuen. Uusin versio, jolla tietoa saadaan ulos, on versio 9. Väliin jäävät versionumerot ovat sellaisia, joita ei koskaan julkistettu, tai niille ei ole olemassa tukea. Versio 9:ssä ulostulevalle tiedolle on tehty tietynlainen malli, jonka ansiosta tiedot ovat helpommin tulkittavissa. Lähes kaikkea tietoa voidaan saada ulos reitittimestä, kuten OSI-mallin 2-7 tason tietoja, reititystietoja, Ipv6, Ipv4, multicast ja MPLS-tietoja (MultiProtocol Label Switching). Tämän ansiosta uudet ohjelmat voivat kuvata entistä paremmin verkon toimintaa. Uusi versio myös helpottaa ohjelmien tekijöitä, koska voidaan käyttää erillisiä tiedostoja, jotka sisältävät tiedot versioista. Myös uusia NetFlow-toimintoja voidaan lisätä helposti, tekemättä kuitenkaan aivan uutta versiota. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

Jokaisen version datagrammi koostuu otsakkeesta ja yhdestä tai useammasta flowsetistä (katso KUVIO5). Otsakkeen ensimmäinen kenttä sisältää versionumeron. Jos ohjelma tukee kaikkia versionumeroita, se varaa tilaa suurimmalle mahdolliselle paketille ja sitten lukee otsakkeesta versionumeron ennen paketin käsittelyä. Seuraava kenttä kertoo kuinka monta flowsettiä paketti sisältää ja samalla toimii indeksinä tietoja varten. Versiot 5, 7, 8 ja 9 sisältävät myös kentän, jossa sijaitsee sekvenssinumero, josta nähdään onko matkan varrella hävinnyt paketteja. Versio 9 sallii flowsettien lähetyksen muillakin protokollilla kuin UDP:llä. Tämän ansiosta voidaan käyttää jotakin sellaista siirtoprotokolla, joka osaa tunnistaa verkon tukokset ja kiertää ne. Näin ollen on vähemmän todennäköistä, että menetetään flowsettejä siirtovaiheessa. (Introduction to Cisco IOS NetFlow - A Technical Overview.)

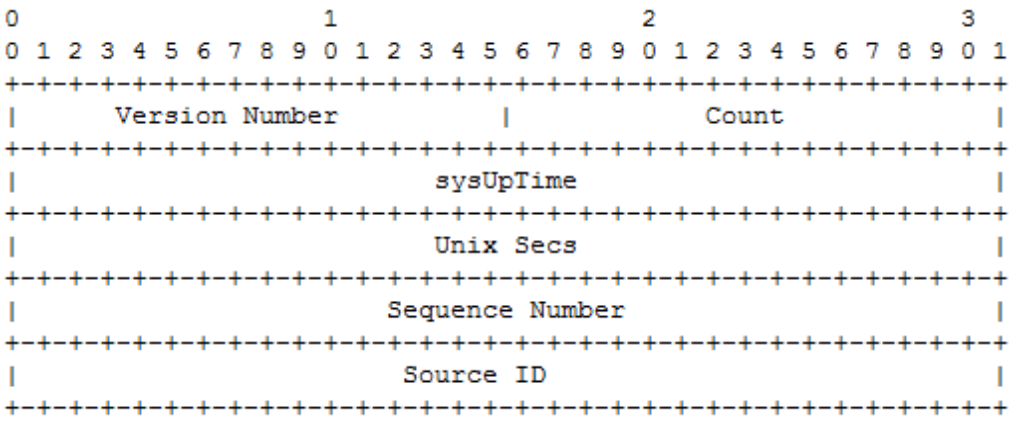


KUVIO 5. Flow-paketin perusidea (Claise 2004)

NetFlow-paketti koostuu otsakkeesta, jota seuraa yksi tai useampi flowset. On olemassa kolme eri flowsettyyppiä: tavallinen, tieto ja asetukset. Nämä flowsetit tunnistetaan omalla ID-numerolla. Tavallinen kulkee numerolla 0 ja asetukset numerolla 1, muut alle 256 numeroiset on myös varattu erikoistarkoituksiin. Tiedot voivat kulkea numeroilla, jotka ovat isompia kuin 256. Ulostulevat paketit voivat sisältää pelkästään yhtä flowsettiä tai täysin sekaisin kaikkia. (Claise 2004.)

Flow-paketin otsake koostuu kuudesta eri kentästä ja on pituudeltaan 140 bittiä (katso KUVIO 6). Versiokenttä sisältää käytettävien flow-tietojen ulostuontiversion. Uusin versio tällä hetkellä on 9. Count-kenttä sisältää summan kaikista paketissa olevista flowseteistä. Seuraava kenttä on sysUpTime, joka kertoo millisekunteina, koska laite on viimeksi käynnistetty uudelleen. UNIX Secs -kenttä puolestaan kertoo kuinka monta sekuntia on kulunut siitä, kun aika oli 0000 UTC (Uni-

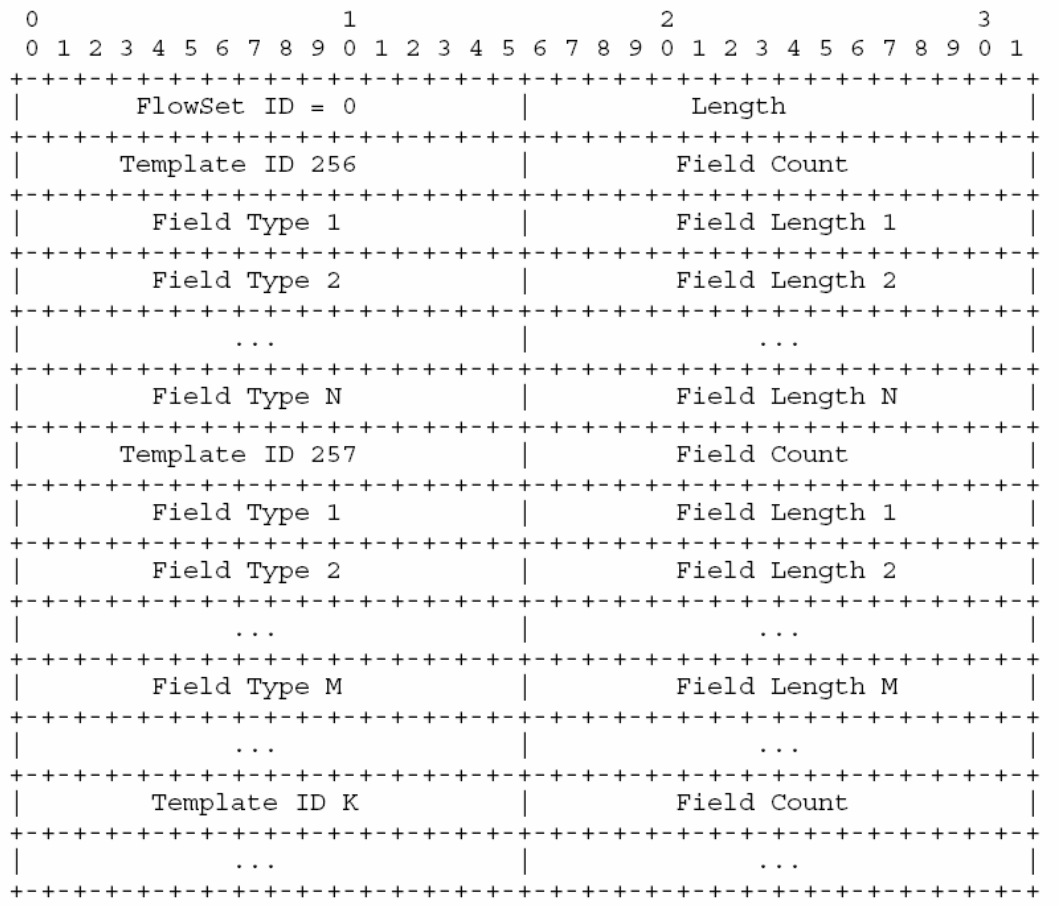
versal Time Code) 1970. Sekvenssinumerokenttä on inkrementaalinen laskuri, josta nähdään jokaisen paketin järjestysnumero. Tästä kentästä keräin voi tarkistaa tulevatko paketit oikeassa järjestyksessä vai onko menetetty jokin paketti. Viimeinen kenttä sisältää arvon, joka yhdistettynä IP-osoitteeseen kertoo tarkasti, mistä tarkastelupisteestä paketti saapuu. (Claise 2004.)



KUVIO 6. Flow-paketin otsake (Claise 2004)

4.5 Erilaiset flowsetit

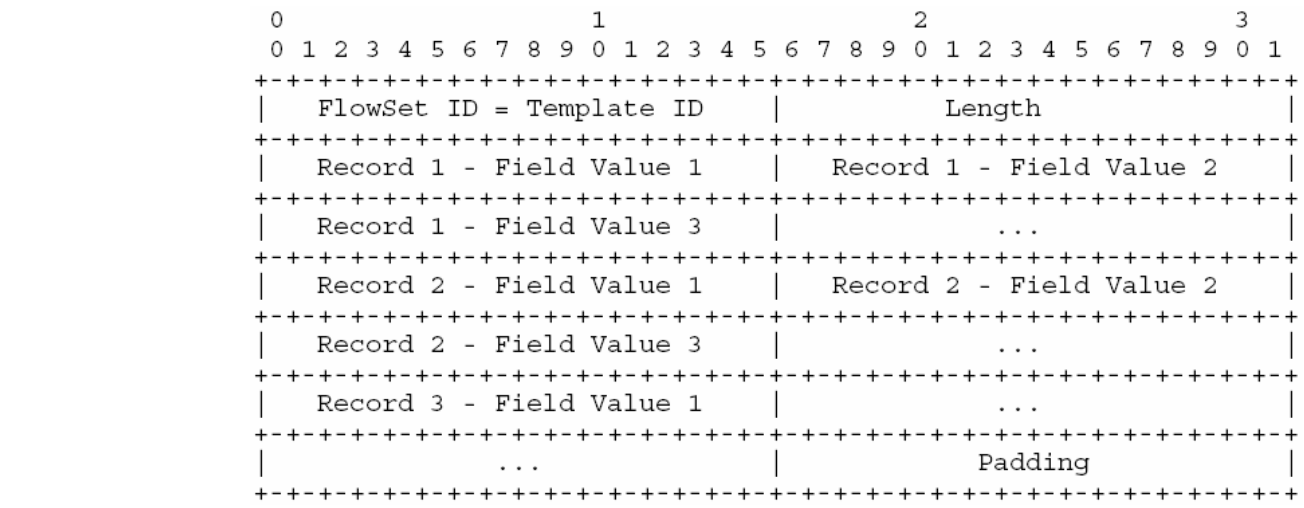
Nämä ovat yksi tärkeä osa NetFlow-protokollaa. Valmiiden pohjien ansiosta flowsetin tallennusformaatti on erittäin hyvin mukautuva, koska keräin voi käsitellä tietoja, vaikka se ei tunnistaisi kaikkia tietokenttiä tai ei välttämättä osaisi tulkita niitä. Ensimmäinen flowset tyyppi on tavallinen flowset (katso KUVIO 7). (Claise 2004.)



KUVIO 7. Tavallinen flowset (Claise 2004)

Tavallisen flowsetin ensimmäinen kenttä sisältää flowset ID-numeron, joka tässä tapauksessa on aina 0. Pituuskenttä määrittää kyseisen flowsetin kokonaispituuden. Arvoa on käytettävä, koska yksi flow-paketti voi sisältää useamman tavallisen flowsetin, ja muutoin ei tiedettäisi, koska vaihtuu toiseen flowsettiin, joka voi olla mitä tahansa tyyppiä. Pituus koostuu kaikista paketin sisältävien kenttien summasta. Seuraava kenttä sisältää ID-numeron, joka on ainutlaatuinen. Jokaiselle uudelle luodulle pohjalle luodaan tällainen numero. Numerot 0 - 255 on varattu tavallisille flowseteille, asetuksille ja muille mahdollisesti uusille malleille. Tietoa sisältävät pohjat numeroidaan väliltä 256 - 65535. Field Count -kenttä sisältää laskurin, joka kertoo, kuinka monta kenttää kyseisessä paketissa on. Yleisesti paketti sisältää useita flowsettejä, joten tästä kentästä keräin tietää, koska jokin tietue loppuu ja koska seuraava alkaa. Field type puolestaan kertoo mitä tyyppiä on käytetty. Ja lopuksi on vielä kentän pituus, joka vastaa käytetyn kentän tyyppiä. (Claise 2004.)

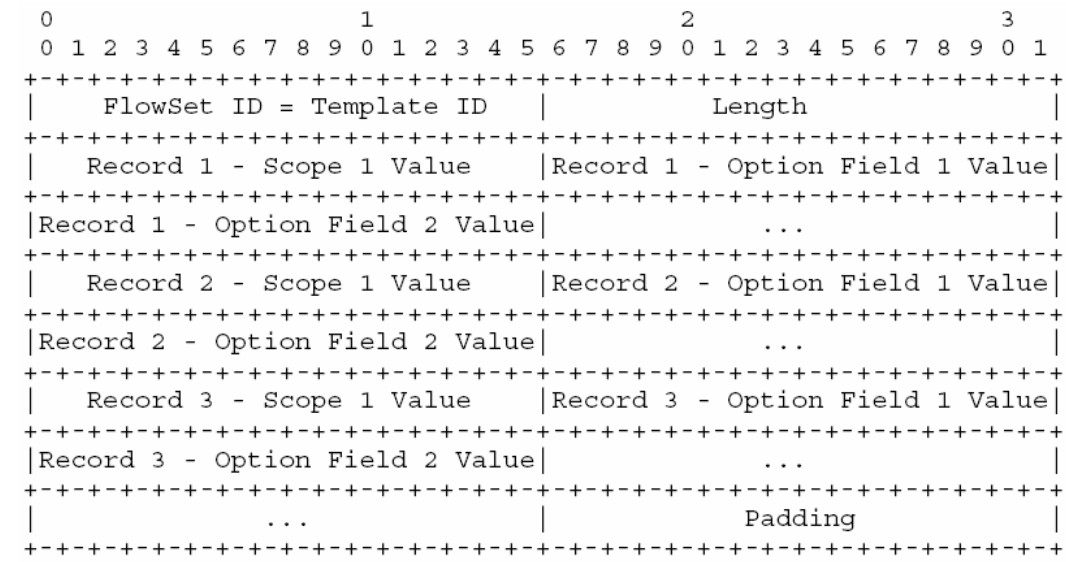
Tietoa sisältävä flowset, eli dataflowset, koostuu vähemmistä tiedoista kuin tavallinen (katso KUVIO 8). Jokainen dataflowset sisältää flowset ID-numeron, joka on sama kuin aiemmin luotu pohjan ID-numero. Keräimen on tällöin löydettävä oikea tavallinen flowset, joka sisältää saman numeron, jotta tiedot voidaan yhdistää. Seuraava kenttä kertoo kokonaispituuden. Seuraavaksi ovat tietoa sisältävät tietuekentät, jotka sisältävät joitakin arvoja. Näiden tyyppi ja pituus on ennalta määritelty tavallisen flowsetin tiedoissa, johon kyseisen data flowsetin ID-numero viittaa. Lopuksi flowset sisältää täytebittejä, jotka ovat nollia. Näitä käytetään sen vuoksi, että jokainen flowset alkaisi aina 4 - bitin rajakohdasta. Dataflowsetin tietoja voidaan tulkita ainoastaan siinä tapauksessa, että keräimestä löytyy jo ennalta sitä vastaava tavallinen flowset. (Claise 2004.)



KUVIO 8. Dataflowset (Claise 2004)

Asetuksia lähetetään tasaisin väliajoin dataflowsettien mukana, mutta ei kuitenkaan joka kerta (katso KUVIO 9). Käyttäjä voi täysin määritellä, kuinka usein tämä tapahtuu. Myös asetusflowsetissä ensimmäinen kenttä koostuu flowset ID-numerosta, joka vastaa aiemmin luodun tavallisen flowsetin ID-numeroa. Keräimestä on löydyttävä molemmat flowsetit, jotta asetuksia voidaan tarkastella, koska keräimen on tiedettävä flowset ID-numeron perusteella oikea tyyppi ja pituus kentille, jotka tulevat seuraavaksi. Seuraava kenttä kertoo flowsetin kokonaispituuden. Sitten tulevat itse asetustiedot, joista jokainen sisältää tietyn määrän arvoja. Dataflowsetin tavoin myös asetusflowset sisältää tarvittaessa täytettä, jotta

saadaan seuraava flowset alkamaan oikeasta kohdasta. Tämä täyte koostuu peräkkäisistä nollista. Keräimestä on löydyttävä tavallista flowsettiä vastaava asetus-flowset, jotta tietoja sisältävää flowsettiä voidaan tulkita. (Claise 2004.)



KUVIO 9. Asetuksia sisältävä flowset (Claise 2004)

4.6 NetFlow-pohjien hallinta

Koska jokainen paketti ei välttämättä sisällä kaikkia tarvittavia flowset-tyyppejä, on keräimen huolehdittava siitä, että se pitää eri tyyppejä tallessa riittävän kauan. Yksi paketti voi sisältää esimerkiksi tavallisen flowsetin, muttei dataflowsettiä, jolloin keräimen on odotettava seuraavia paketteja, joissa sitten tämä dataflowset voinee saapua. Vasta sitten keräin voi tulkita näitä flowsettejä. Jos NetFlow-keräin kerää tietoja useammasta tarkkailupisteestä, on sen otettava huomioon, että flowsettien ID-numeron ainutlaatuisuutta ei tällöin voida taata. (Claise 2004.)

ID-numeroiden tulisi pysyä samanlaisina koko elämänkaaren ajan. Tätä ei kuitenkaan voida taata, jos jostakin syystä keräin tai paketteja lähettävä laite käynnistyy uudelleen. Tällöin numerointi voi alkaa väärästä kohdasta, kun laite on taas toiminnassa. Jos muutetaan joitakin pohja-ID-numeron arvoja, ei sitä voida käyttää

uudestaan, ennen kuin järjestelmä on käynnistetty uudelleen. Mutta jos tämä muutetun arvon sisältävä tallenne tuhotaan, voidaan luoda uusi täysin samat asetukset sisältävä tallenne samalla ID-numerolla. (Claise 2004.)

NetFlow-laite lähettää tavallisen flowsetin sekä asetuksia sisältävän flowsetin seuraavissa tilanteissa:

- Jos NetFlow-järjestelmä käynnistetään uudelleen, on tavallisen flowsetin mukana lähetettävä asetukset. Tämän tulee tapahtua ennen kuin voidaan data flowsettejä lähettää. Tietoa ei voida kuitenkaan lähettää kuin vasta seuraavassa paketissa asetusten jälkeen, ei ennen sitä eikä samaan aikaan asetusten kanssa. Tavallinen flowset ja asetukset on hyvä lähettää molemmat ennalta, jotta voidaan varmistaa, että keräin osaa käsitellä tulevia tietoja.
- Jos järjestelmän asetuksiin tehdään jotakin muutoksia, tulisi uudet määritelmät lähettää mahdollisimman nopeasti. Tällaisessa tapauksessa voidaan lähettää asetustiedot etukäteen, jolloin voidaan olla varmoja, että keräin osaa käsitellä seuraavaksi tulevia dataflowsettejä.
- NetFlow-laite lähettää asetuksia määritellyin aikavälein virkistääkseen keräintä. Tämä johtuu siitä, että tavallisilla ID-numeroilla on tietty rajallinen elinikä ja niitä on uusittava tietyin väliajoin. Käyttäjän on mahdollista määritellä kuinka usein tämä tapahtuu ja kuinka monelle paketille. Kun jompikumpi ehdoista täyttyy, on lähetettävä asetukset uudelleen.
- Viimeinen tilanne on se, että NetFlow-laitteen kellon asetukset muuttuvat, jolloin on uudet asetukset lähetettävä taas mahdollisimman pian.

(Claise 2004.)

4.7 Keräimen puolen toiminta

Tavallisesti keräin saa aluksi pohjatiedot tulevista asetus- ja dataflowseteistä, ennen kuin itse asetuksia tai tietoa tulee keräimeen. Tämä sen vuoksi, että kun pohja on saatu, voidaan tulevien flowsettien koodaus purkaa auki ja tallentaa ne paikallisesti. Jos kuitenkaan pohjaa ei ole saatu ennen muita tietoja, tulisi keräimen tallentaa muut tiedot talteen ja purkaa niiden koodaus sen jälkeen kun pohja on saatu. Keräimen ei tulisi olettaa, että pohja sekä muut tiedot tulevat samassa paketissa. Ei myöskään tule olettaa, että tulossa olisi ainoastaan yksi pohja samassa paketissa. (Claise 2004.)

Pohjan elämä rajoittuu tiettyyn ennalta määriteltyyn aikaan. Jos tämän ajan sisällä ei pohjaa päivitetä, katsotaan sen olevan erääntynyt. Keräin ei tämän jälkeen saa käyttää kyseistä pohjaa koodauksen purkuun. Jos NetFlow-laitteen kellon konfiguraatio muuttuu, tulee keräimen hylätä kaikki siihen laitteeseen liittyvät tallenteet, jotta se voisi sitten oppia uuden konfiguraation mukaiset tietokentät. Kun keräin vastaanottaa uuden pohjan, esimerkiksi NetFlow-laitteen uudelleenkäynnistyksen jälkeen, on sen välittömästi tallennettava se vanhan pohjan päälle. (Claise 2004.)

4.8 Turvallisuus

NetFlow-protokollan versio 9 on suunniteltu siten, että NetFlow-laite ja keräin sijaitsisivat samassa yksityisessä verkossa. On kuitenkin mahdollista käyttää tätä protokollaa siten, että NetFlow-tiedot liikkuvat yleisessä verkossa Internetin yli. Tästä syntyy monia erilaisia tietoturvariskejä. Hyökkääjä voi esimerkiksi kaapata, muokata ja lisätä NetFlow-laitteesta tulevia paketteja. Tämä johtaa siihen, että NetFlow-tietoja voidaan kaapata ja väärentää. Näiden tietojen ansiosta hyökkääjä voi myös kohdistaa hyökkäyksensä juuri NetFlow-keräimeen. (Claise 2004.)

Protokollan suunnittelijat eivät ole lisänneet protokollaan minkäänlaista eheyttä, luottamuksellisuutta tai käyttäjän varmentamista, koska nämä olisivat vähentäneet

protokollan suorituskykyä. Ja pohjalla oli myös ajatus, että protokolla tulee käyttöön lähes ainoastaan yksityisiin verkkoihin, jolloin tietoturva ei ole aivan niin tärkeä, kuin liikennöitäessä yleisissä verkoissa. Ideana oli myös se, että keräin ja NetFlow-laite sijaitsevat verkossa hyvin lähellä toisiaan ja jos mahdollista, keskustelevat keskenään täysin oman linjan välityksellä. (Claise 2004.)

Yksi riskitekijä on myös siinä, että NetFlow-paketteja ei ole salattu millään tavalla. Hyökkääjä voi kaapata NetFlow-paketteja ja saada niiden sisällöstä käyttöönsä sellaista tietoa, joka helpottaa hyökkäystä verkkoon. Hyökkääjä voi melko helposti saada selville aktiivisia yhteyksiä, verkon päätepisteet ja mallin, miten liikenne verkossa kulkee. Tätä tietoa hyökkääjä voi sitten käyttää joko vakoillakseen verkon liikennettä tai tulevan hyökkäyksen suunnitteluun. Tieto, jota hyökkääjä saa kaapatuista flow-paketeista käyttöönsä, riippuu täysin millaisia asetuksia käytetään. Jos käytössä on tarkka liikenteen seuranta, voi hyökkääjä saada paketista ulos tiedot esimerkiksi lähde- ja kohde-IP-osoitteesta, kun taas hieman laajempaa tarkastelua käytettäessä hyökkääjä näkee ainoastaan verkko-osoitteet. (Claise 2004.)

Jos flow-tietoja käytetään laskutukseen tai hyökkäyksien havainnointiin, voi tämä kannustaa hyökkääjää väärentämään flow-paketetteja. Hyökkääjä voi esimerkiksi haluta väärentää tietoja pienemmän laskutuksen toivossa, tai muokata tietoja, jotta hyökkäys jäisi huomaamatta. Tämä onnistuu joko muokkaamalla flow-tietoja, ennen kuin ne menevät keräimeen, tai lähettämällä uusia väärennettyjä tietoja suoraan keräimeen. Hyökkääjä voi myös yrittää väärentää flow-pohjia, jonka jälkeen keräin ei osaa enää purkaa uusien flow-tietojen koodausta. (Claise 2004.)

Keräimeen voidaan myös kohdistaa DoS-hyökkäys. Tämä voi kuluttaa niin paljon keräimen resursseja, ettei se voi enää ottaa vastaan uusia paketteja tai purkaa niiden koodausta. Tällaiseen hyökkäykseen ei ole juuri puututtu mietittäessä NetFlow-protokollaa, mutta normaalit palvelunestohyökkäyksen torjumistoimenpiteet lieventävät tilannetta. (Claise 2004.)

4.9 Reitittimen konfigurointi

Jotta NetFlow-protokollaa voidaan käyttää, on käytössä oltava sitä tukeva reititin tai kytkin ja tämän lisäksi keräinpalvelin, johon tieto kulkeutuu. Reititin on helppo saada toimintaan vain muutamalla lisärivillä, jotka on konfiguraatioon lisättävä. NetFlow-protokolla konfiguroidaan erikseen jokaiselle liitynnälle. Seuraavassa on esimerkki, kuinka NetFlow konfiguroidaan liityntään eth0.

Router(config)# ip cef
Router(config)# interface eth0
Router(config-if)# ip flow ingress

Tai

Router(config-if)# ip route-cache flow

Jälkimmäinen komento riippuu käytetystä IOS-versiosta. IP Cef -komento käynnistää Cisco Express Forwarding -toiminnon, joka vähentää prosessorin käyttöä suorittamalla hieman toisenlaista pakettien reititystä. CEF on 3. tason IP kytkentätekniikka, joka optimoi verkon toimintaa ja skaalautuu hyvin suurissakin verkoissa. (Cisco IOS NetFlow Command Reference, Release 12.4; Greene & Smith 2002, 66 .)

Seuraavaksi tulee konfiguroida mihin käytettävä laite lähettää Netflow-tietoja. Samalla valitaan, mitä NetFlow-protokollan versiota käytetään.

Router(config)# ip flow-export version 9
Router(config)# ip flow-export destination 192.168.1.1 9997

Ensimmäinen rivi määrittelee käytetyn version. Jälkimmäinen rivi kertoo missä IP-osoitteessa keräinserveri sijaitsee, ja lukema 9997 on käytettävä UDP-portti. (Cisco IOS NetFlow Command Reference, Release 12.4.)

4.10 Vaikutus reitittimen suorituskykyyn

NetFlow:n käyttö vaikuttaa tietenkin myös laitteeseen, joka NetFlow-tietoa kerää. Ennen NetFlow:n käyttöönottoa onkin hyvä selvittää oman reitittimen prosessorin käyttöaste ja miettiä, miten NetFlow tulee siihen vaikuttamaan. Kun NetFlow otetaan käyttöön, on monia seikkoja, jotka vaikuttavat prosessorin käyttöön. Tärkeimmät näistä ovat liikenteen määrä eli se, kuinka monta flow:ta kulkee sekunnin aikana, ja käytettävä NetFlow:n versio. Cisco Systems on tehnyt omat kokeilunsa NetFlow:n vaikutuksesta prosessorikuormaan. Näissä testeissä reitittimestä mitattiin prosessorin käyttöastetta erilaisilla konfiguraatioilla. Mittaustulokset otettiin ulos reitittimestä vasta mittausten päätyttyä, jotta tämä ei vaikuttanut lopputulokseen. (NetFlow Performance Analysis.)

Testien tulokset näyttävät myötäilevän melko hyvin reitittimen käyttötarkoituksen mukaan. Pienempi reititinmalli ei jaksa oikein pyörittää NetFlow:ta, jos flow-tietojen määrä, eli liikenne kasvaa liian suureksi. Suuremmissa reitittimissä prosessorin käyttöaste ei nouse kovinkaan korkealle, vaikkakin nousua voi olla huomattavasti peruskäyttöasteeseen verrattuna. Yleisesti ottaen prosessorikuorman nousu on noin 10-20 prosentin luokkaa, joka ei sinällään ole paha asia. Asia kuitenkin muuttuu, jos reitittimessä on jo käynnissä muita prosessoritehoa vaatia prosesseja. Tällöin prosessorin käyttöaste voi nousta hyvinkin korkealle. (NetFlow Performance Analysis.)

4.11 NetFlow-ohjelmat

4.11.1 Cisco CS-Mars

CS-Mars tulee sanoista Cisco security monitoring, analysis and response system. Ohjelma keskittyy verkon tietoturvaan ja lupaa vähentää vääriä hälytyksiä luomalla verkosta todella tarkan kuvan. Se osaa myös kertoa, jos verkossa on jotakin haitallista, mikä pitäisi poistaa. CS-Mars lupaa tarjota ratkaisut esimerkiksi seuraaviin ongelmiin:

- turvallisuus ja tiedon liiallinen määrä verkossa
- hyökkäykset ja vikojen tunnistaminen, priorisointi ja vastaaminen
- hyökkäysten lisääntynyt monimutkaisuus, nopeus ja korjauskustannukset sekä
- henkilöstön vähyys tietoturvan puolella.

CS-Mars lupaa ratkaista nämä ongelmat seuraavanlaisesti:

- Sopeuttaa verkon älykkyyden uudistamalla yhdenmukaisten verkon poikkeavuudet ja hälytykset.
- Visualisoi vahvistetut tapahtumat ja automatisoi tutkinnan.
- Lieventää hyökkäyksiä käyttäen hyväksi olemassa olevaa verkkoa ja sen topologisia muutoksia.
- Monitoroi järjestelmiä, verkkoa ja turvallisuustoimenpiteitä.
- Skaalautuu verkon mukaan.
- Tarjoaa helpon käyttöönoton.

Cisco CS-Mars lupaa siirtää verkon raakamuodossa olevat tarkkailu- ja turvallisuustiedot järkevään muotoon ja näin ollen auttaa turvallisuusvälikohtauksien ratkaisussa ja ylläpidossa. Ohjelma auttaa ylläpitäjää keskittämään valvonnan, löytämään verkon uhkia ja raportoimaan laitteiston tilaa. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Verkon turvallisuus ei ole enää pelkästään sitä, että tarkkaillaan työaseman ja Internetin rajapintaan. Nykyään on käytössä syvälliset turvallisuusmallit, joissa useita hyökkäyksen vastakeinoja on ripoteltu ympäri verkon rakennetta. Tämä on tarpeellista, koska uudet hyökkäykset ovat aina vain monimutkaisempia ja tapahtuvat nopeasti. Verkossa olevia laitteita voidaan etänä tutkia useita tuhansia kertoja joka päivä, kun etsitään tietoturva-aukkoja. Useimmat hyökkäykset koostuvat useiden eri aukkojen hyväksikäytöstä, jolloin voidaan mahdollisesti saada sallimaton yhteys verkkoon ja pahimmassa tapauksessa voidaan päästä liikkumaan vapaasti kyseisessä verkossa. Virusten, matojen, nollapäivähyökkäysten, troijalaisten, spywaren ja hyökkäystyökalujen määrän räjähdysmäinen kasvu asettaa haasteita huolimatta tietoturvan tasosta. Hyökkäykset aiheuttavat myös huomattavaa haittaa verkolle, koska ne voivat hidastaa tai jopa katkaista sen ja korjauksesta syntyy aina kustannuksia. Verkossa voi myös olla suuri määrä laitteita, jotka kaikki luovat omia hälytyksiä ja lokitiedostaja. Näiden läpikäyminen voi kuitenkin viedä erittäin paljon aikaa, joten tilalle tarvitaan jokin toinen ratkaisu. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Monet tuotteet tarjoavat tietoa turvallisuudesta ja auttavat hallitsemaan erilaisia tapahtumia. Nämä toimet auttavat lieventämään erilaisia ongelmia ja mittaamaan järjestelmän tasoa, jotta sitä voisi parantaa. Näiden tuotteiden ansiosta ylläpitäjä voi keskittää toimintansa yhteen paikkaan, jossa eri raportteja voidaan yhdistää siten, että vain tietynlaiset tapahtumat tulevat lopulta ylläpitäjän tutkittavaksi. Monet näistä ohjelmista kuitenkin pitävät sisällään liian vähän tietoa verkon rakenteesta ja muista parametreista. Tällöin tarkkailu ei ole aivan niin perinpohjaista ja joitakin välikohtauksia voi jäädä huomaamatta. Yksi syy tähän voi olla myös ohjelman tehottomuus, jolloin se ei pysy mukana jos liikenteen määrä nousee liian suureksi. Cisco CS-Mars on kuitenkin hyvin skaalautuva järjestelmä, jota on helppo käyttää ja joka tutkii verkkoa järkevällä tavalla. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Cisco CS-Mars osaa tarkkailla verkkoa viisaasti. Aluksi se luo verkosta topologiakartan ja tutkii kaikkien laitteiden konfiguraatiot, sekä käytössä olevat turvallisuusmenettelytavat. Se myös tarkkailee liikennettä, jota verkossa kulkee. Tämän

jälkeen ohjelma osaa tarkastella huomattavasti paremmin pakettien kulkeutumista verkossa. Koska ohjelma käyttää mahdollisimman vähän muita ohjelmia hyödykseen, se ei juuri vaikuta verkon tai järjestelmän suorituskykyyn. Tämä ohjelmaratkaisu yhdistelee erilaisten järjestelmien lokitietoja ja kokoaa niistä järkevän paketin. Näitä järjestelmiä ovat esimerkiksi reitittimet ja kytkimet, palomuurit, tunkeutumisenestojärjestelmät, haavoittuvuuksien havainnointityökalut, virusskannerit ja verkon liikenne NetFlow-muodossa. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Aina kun tapahtumista saapuu tietoa, se normalisoidaan käyttäen apuna laitteiden konfiguraatioita, saman lähteen ja kohteen ohjelmia ja samankaltaisia hyökkäystyyppejä. Samantyyppiset tapahtumat ryhmitellään tietyiksi istunnoiksi reaaliajassa. Käyttäen erilaisia sääntöjä, saadaan näistä istunnoista suodatettua tapahtumat. Järjestelmä itsessään pitää sisällään suuren määrän valmiita sääntöjä ja uusia sääntöjä voidaan luoda yksinkertaisesti käyttämällä graafista käyttöliittymää. Tämä tulosten toisiinsa vertailu vähentää huomattavasti liikutettavan tiedon määrää. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Tämä ohjelma osaa tarkkailla tuhansia tapahtumia ja se myös lajittelee ne tehokkaasti ja tiivistää niistä pieneen tilaan menevän paketin, jonka se arkistoi. Koska tapahtumia voi olla erittäin runsaasti, on käytössä oltava turvallinen ja vakaa alusta, joka kirjaa tiedot ylös. Cisco tarjoaa eritasoisia laitteita tähän tarkoitukseen, joista parhaimmat on optimoitu käsittelemään erittäin suurta määrää tietoja, jopa yli 10 000 tapahtumaa sekunnissa tai yli 300 000 NetFlow-tapahtumaa sekunnissa. Tämä onnistuu, koska käytössä on yhdenmukainen käsittelylogiikka ja sisäänrakennettu Oracle-järjestelmä. Käyttäjän ei tarvitse välittää mitä tietokannassa tapahtuu, vaan kaikki tapahtuu automaattisesti. Kaikki tieto voidaan tallentaa laitteen lisäksi myös verkkoon, jolloin saadaan varmuuskopiot kaikesta järjestelmän keräämästä tiedosta. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Cisco Security Mars helpottaa ja nopeuttaa uhkien tunnistamista, tutkimista ja pienentämistä. Useimmat uhkat, joita ylläpito kohtaa, vaativat usein paljon aikaa

vievää analysointi, jotta tilanne saadaan ratkaistua ja korjattua. Tämän ohjelma käyttäjillä on käytössään tehokas ja interaktiivinen käyttöliittymä, jolla turvallisuusuhkia voidaan tutkia ja torjua. Ylläpitäjälle on tarjolla täysin graafinen järjestelmä, jossa on näkyvissä verkon topologiakuvio. Tässä kuviossa nähdään reaaliaikaisesti kaikki uhkatekijät ja esimerkiksi jonkin hyökkäyksen lähtökohta ja etenemissuunta. Tästä kuviosta ylläpitäjä voi sitten varmentaa uhat ja hyökkäykset, joihin kannattaa kiinnittää huomiota. Ohjelma osaa tutkia hyökkäysten oikeellisuutta arvioimalla koko hyökkäyspolkua aina alkupisteen MAC-tasolle asti. Tämän toiminnon ohjelma suorittaa analysoimalla verkon muitten laitteiden lokitiedostoja ja sitä kautta se voi suodattaa väärät hälytykset pois. Käyttäjät voivat myös säätää näitä asetuksia, jolloin mahdollisesti väärien hälytysten määrä vähenee entisestään. Tarkoituksena on pitää järjestelmä verkossa ja toiminnassa, kuitenkaan tinkimättä turvallisuudesta. (Cisco Security Monitoring, Analysis and Response System 4.2.)

Cisco Security Mars tarjoaa monia valmiita raporttipohjia, jotka auttavat ylläpitäjää verkonhallinnassa ja tietoturvan tarkkailussa. Ohjelma osaa myös tutkia ja raportoida todennustapahtumia, jotka tapahtuvat joko 2. tason kytkimissä tai Cisco Secure ACS:ssä (Access Control Server), joka todentaa käyttäjän tiettyjen parametrien mukaisesti (Kizza 2005, 218). Samoin se voi tarkkailla 3. tason EAP-protokollan (Extensible Authentication Protocol) tapahtumia. Käyttöliittymänä toimii web-selain. (Cisco Security Monitoring, Analysis and Response System 4.2.)

4.11.2 Stager

Stager on raportointityökalu NetFlow:lle, kuten myös SNMP:lle. Stager on julkaistu open sourcena, eli lähdekoodi on kaikille avoin. Lisenssinä kyseisessä ohjelmassa on Free Software Foundationin GNU General Public License Version 2. Tämä lisenssi on käytännössä sellainen, että käyttäjä saa melko vapaasti kopioida ja muokata ohjelmaa sekä levittää sitä edelleen. Tästä on ainakin se hyöty, että kuka tahansa voi helposti kehittää ohjelmaa ja tehdä siihen uusia ominaisuuksia,

koska lähdekoodi on vapaasti kaikkien saatavissa ja muokattavissa. (Solberg 2005b.)

Toimiakseen Stager vaatii Flow-tools nimisen apuohjelman, joka toimii tällöin keräinohjelmana. Tämän lisäksi palvelimella on oltava PostgreSQL ja Perl sekä joitakin moduleita Perliin, jotka useimmat asentuvat vakiona, kun Perl asennetaan. Stagerin asennusskripti osaa tarvittaessa kertoa, jos jokin tarvittava asia puuttuu. Palvelinkoneelle ei juurikaan anneta muita vaatimuksia, kuin että se on sellainen, joka jaksaa pyörittää PostgreSQL-tietokantaa. Toinen vaikuttava tekijä on liikenteen määrä eli se, kuinka paljon flow-tietoja ohjelman pitää analysoida. (Solberg 2005b.)

Ohjelma pyörii palvelimella, ja sitä käytetään Internet-selaimen kautta. Se osaa näyttää useimpia verkkoon liittyviä tilastotietoja. Ohjelma voi kerätä tietoa yhdestä tai useammasta paikasta ja tallentaa tiedot SQL-tietokantaan (Structured Query Language). Ohjelma osaa havaita verkon tukokset ja osaa myös lisätä pois jääneet tiedot myöhemmin tietokantaan. Raportit ovat käyttäjän muokattavissa, ja samaan raporttiin voidaan luoda monia eri näkökulmia. (Solberg 2005b.)

Luotujen raporttien ulkonäkö riippuu sitä, mitä on valittu nähtäväksi. Esimerkiksi raportti IP-protokollasta näyttää liikenteen jakautumisen eri IP-protokollien kanssa, kuten TCP, UDP ja ICMP (Internet Control Message Protocol). Raportteihin voidaan valita erilaisia tapoja ilmoittaa kyseiset arvot, kuten prosentteina tai tavujen määrä sekuntia kohden. Seuraavat raportit löytyvät perusasennuksesta valmiina:

- kohteen liityntä
- IP-protokolla
- IP-palvelutyyppi
- IP-lähdeosoite
- IP-kohdeosoite
- IP-kohdeosoite – lähdeosoite
- lähde-AS (Autonomous System, Itsenäinen järjestelmä)
- kohde-AS

- kohde-AS – lähde-AS
- kuljetuskerroksen lähdeportti
- kuljetuskerroksen kohdeportti sekä
- yhteenveto.

Kohteen liityntä -raportti kuvaa liikennettä yhdestä pisteestä muihin saman laitteen liityntöihin. IP-protokolla sisältää tiedot liikenteen jakautumisesta eri IP-protokollien kesken. IP-palvelutyyppi tutkii pakettien ToS-arvoja (Type of Service). IP-lähdeosoite mittaa liikennettä tietystä kohdasta ja ilmoittaa eniten liikennöivät IP-osoitteet. IP-kohdeosoite toimii kuten edellinen, mutta näyttää eniten liikennöivät kohdeosoitteet. IP-kohdeosoite – lähdeosoite -raportissa nähdään eniten liikennöivät laiteparit ja kerralla voidaan saada näkyviin liikenteen määrä oktetteina, paketteina tai flow-määrinä. AS-raportit toimivat kuten edelliset, eli näkyvissä on aina eniten liikennöivät lähteet, kohteet tai parit. Porttiraportit kertovat, miten paljon liikennettä missäkin porttinumerossa on, kohdeportin mukaan voi päätellä kunkin ohjelman liikennemäärän. Yhteenvetoraportti puolestaan voi näyttää esimerkiksi kokonaisliikennemäärän paketteina. (Solberg 2005b.)

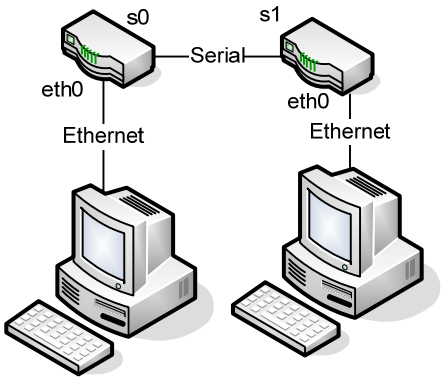
4.11.3 Ohjelmien vertailu

Vertailtavaksi ohjelmiksi valittiin Ciscon CS-Mars sekä ilmaisohjelma Stager. Muitakin ohjelmia olisi toki ollut, mutta nämä tuntuivat olevan molemmat hyviä omalla sarallaan. Kaupallisia ohjelmia oli huomattavasti enemmän kuin ilmaisia, ja useimmat ilmaisohjelmista olivat jääneet kehityksessä jälkeen ja niiden tuki oli lopetettu. CS-Mars ja Stager eroavat huomattavasti toisistaan, koska CS-Mars on tarkoitettu paljon muuhunkin, kuin NetFlow-tietojen analysointiin. Raporttien osalta ohjelmat tekevät melko samankaltaisia raportteja, mutta verkon topologian kannalta CS-Mars on huomattavasti parempi kuin Stager. CS-Mars jouduttiin hyllyttämään testauksesta, koska se on hyvin kallis ohjelma ja työtä tehtiin nollabudjetilla. Stager sen sijaan otettiin käyttöön. Vertailu jää kuitenkin lyhyeksi, koska toista ohjelmaa ei päästy kokeilemaan käytännössä.

5 KÄYTÄNNÖN TESTAUS

5.1 Pilotointi

Ensimmäiseksi haluttiin testata netflow:n toimintaa pilottiympäristössä. Tämä sen vuoksi, että jos jokin menee pieleen, siitä ei synny suurtakaan haittaa. Sijoitusympäristö tulee kuitenkin olemaan suuren verkon runkolaitteisto, joten huonoimmassa tapauksessa koko verkko voisi rampautua. Pilottiympäristöstä tehtiin mahdollisimman yksinkertainen, se sisälsi kaksi työasemaa ja kaksi Ciscon 2500-mallin reititintä (katso KUVIO 10). NetFlow asetettiin toimimaan näiden reitittimien välillä olevaan sarjalinkkiin. Liikennettä luotiin ICMP-protokollan avulla.



KUVIO 10. Pilotointiympäristön verkkokuva

Laitteistona pilotointivaiheessa toimi työasema, jossa ajettiin VirtualPC 2004 -ohjelmaa, sekä reititin, joka konfiguroidaan toimimaan NetFlow-laitteena. Ensimmäiseksi oli asennettava virtuaalikoneeseen Fedora Core Linux -jakelun uusin versio, joka tällä hetkellä on numero 6 ja kulkee nimellä Zod. Tähän Linuxiin sitten asennettiin NetFlow-keräin ja analysointiohjelmisto kokeilua varten. Aluksi oli kuitenkin luotava VirtualPC:hen uusi tietokone, johon asennus tapahtuu. Tämän jälkeen käynnistettiin virtuaalitietokone ja asetettiin se avaamaan Fedoran ensimmäisen asennus-CD:n levykuva. Asennus kysyi ensimmäisenä toteutetaanko asennus graafisena vai tekstipohjaisena, valittiin tekstipohjainen. Asennuskielenä käytettiin englantia ja näppäimistöksi valittiin suomalainen näppäimistö. Seuraavaksi tuli luoda osiot levylle. Asennusohjelma sai hoitaa tämän, koska yleisesti

osiot tulevat helposti kuntoon valitsemalla default layout. Asia tarkistettiin vielä valitsemalla osioinnin esikatselu. Asennuksen edetessä ohjelma kysyi halutaanko ottaa käyttöön käyttöjärjestelmän valintaohjelma koneen käynnistyessä ja halutaanko siinä käyttää salasanaa. Seuraavaksi oli mahdollista määritellä mitkä käyttöjärjestelmät ovat näkyvissä koneen käynnistyessä. Koska käytössä oli vain yksi käyttöjärjestelmä, ei näihin kohtiin tarvinnut tehdä mitään muutoksia. Verkkoasetuksista määriteltiin, että kone saa IP-osoitteen DHCP:ltä. Aiemmin oli asetuksiin määritelty verkkokortin kohdalle, että kone on NAT:in takana. Aikavyöhykkeeksi valittiin Europe/Helsinki. Seuraavassa kohdassa asetettiin järjestelmänvalvojan salasana. Asennettavia paketteja muokattiin siten, että asennus ei vakiona asentanut mitään ylimääräistä, koska se olisi vain turhaan viemässä tilaa ja kaikki ylimääräinen on hyvä jättää pois, jolloin on mahdollisesti pienempi määrä tietoturvariskejä. Tässä vaiheessa asennus oli valmis alkamaan. Asennusohjelma ilmoitti vielä, että asennukseen tarvitaan kaksi ensimmäistä asennuslevyä ja ne tulisi olla valmiina, muutoin asennus tulisi lopettaa tässä kohdassa. Jatkettiin asennusta valitsemalla Continue. Lopuksi kun asennus oli valmis, kirjauduttiin sisään järjestelmänvalvojana ja asennettiin uusimmat päivitykset virtuaalikoneeseen.

Seuraavaksi asennettiin flow-tools, joka toimii NetFlow-keräinohjelmana. Asennus sujui automaattisesti Fedoran omaa paketinhallintatyökalua käyttäen ajamalla komento yum –y install flow-tools. Sitten asennusvuoroon tuli Stager, joka valittiin kokeiltavaksi, koska siinä on monia hyviä ominaisuuksia ja sen lisäksi se on täysin ilmainen. Ohjelman Internet-sivuilta löytyi asennusohjeet, joiden mukaan asennus yritettiin suorittaa. Ongelmia syntyi muutamissa kohdissa, mutta ne saattoivat kuitenkin johtua itse käyttäjän tottumattomuudesta kyseiseen Linux-jakeluun ja sen toimintoihin. Itse ohjelman asennus on kaksivaiheinen. Ensin on asennettava taustalla pyörivät työkalut ja asetettava ne toimimaan tietokannan kanssa. Toinen vaihe on asentaa ohjelman osa, joka oikeasti näkyy käyttäjälle, eli web-selain käyttöliittymä, joka osaa hakea tiedot tietokannasta. (Solberg 2005a.)

Stager-asennuksen ensimmäinen osa alkoi asennusskriptin ajolla, joka kertoi, että kaksi Perl-moduulia on asentamatta. Skripti ajettiin kirjoittamalla asennuskansiossa ./stager-install.pl --type=backend –backends=netflow –prefix=/var/netflow.

Moduulit asennettiin käyttämällä Perlin CPAN-asennusohjelmaa ja asennusskripti ajoi nyt itsensä loppuun asti ilman ongelmia. Seuraava vaihe oli luoda PostgreSQL-tietokantaan käyttäjä, jolla on oikeudet luoda uusia tietokantoja. Tämä tapahtui komennoilla pgsql template1, joka avasi tietokannan, ja create user with password '<password>' createdb;, joka loi käyttäjän, jolla on oikeuksia luoda uusia tietokantoja.

Sitten tämän käyttäjän tiedot lisättiin Stagerin netflow-konfiguraatiotiedostoon (netflow.cfg) ja ajettiin toinen skripti (db-install.pl –backends=netflow), joka loi uuden tietokannan ohjelmaa varten. Tämän jälkeen oli asennettava ohjelman osa, joka on käyttäjän kannalta tärkein, eli web-käyttöliittymä. Tämäkin asennuskohta sujui helposti valmiin asennusskriptin ansiosta kirjoittamalla ./stager-install.pl --type=frontend --backends=netflow --prefix=/var/www/html. Lopuksi skripti kertoi mitä oli seuraavaksi tehtävä. Jotta web-käyttöliittymä toimisi tietokannan kanssa, oli sen asetuksiin määriteltävä tietokantaa koskevat asiat tiedostoon nimeltä user.config.php. (Solberg 2005a.)

Asennus oli nyt näiltä osin valmis. Reitittimeen lisättiin sellainen konfiguraatio, jolla NetFlow-saatiin käyttöön. Seuraava vaihe oli flow-capturen käynnistys. Flow-capture toimi tässä kokoonpanossa netflow-keräimenä. Stagerin mukana tulleet skriptit huolehtivat netflow-tietojen siirrosta PostgreSQL-tietokantaan. Kun uusia netflow-tietoja oli kerätty hetki, piti ajaa skripti, joka huolehtii reitittimen tietojen siirrosta tietokantaan. Tämä skripti ajettiin komennolla ./getRouterInfo.sh –v --timestamp='2007-01-01'. Aikaleiman täytyy olla aikaisempi, kuin mikään flow-tieto, joten valittiin päivämääräksi vuoden ensimmäinen päivä. (Solberg 2005a.)

5.2 Käytännön kokeilu

Kun ohjelma oli esitelty Päijät-Hämeen koulutuskonsernille, se päätettiin myös ottaa käyttöön. Asennus tapahtui tällä kertaa oikeaan tietokoneeseen, toisin kuin pilotointivaiheessa, jossa asennus tapahtui virtuaalikoneeseen. Linuxin asennus ei kuitenkaan poikennut virtuaalikoneen asennuksesta muutoin kuin siten, että nyt oli käytettävä fyysisiä asennuslevykkeitä levykuvien sijaan. Myös sekä Flow-tools että Stager asentuivat samaan tapaan kuin pilotointivaiheessa. Käytössä ollut NetFlow-laite oli Ciscon 6500-sarjan reititin, tarkemmin 6509, ja se toimii verkon runkoreitittimenä sekä yhdyskäytävänä ulkoverkkoon. Reitittimessä oli useita VLAN-verkkoja ja yhteen näistä otettiin NetFlow käyttöön.

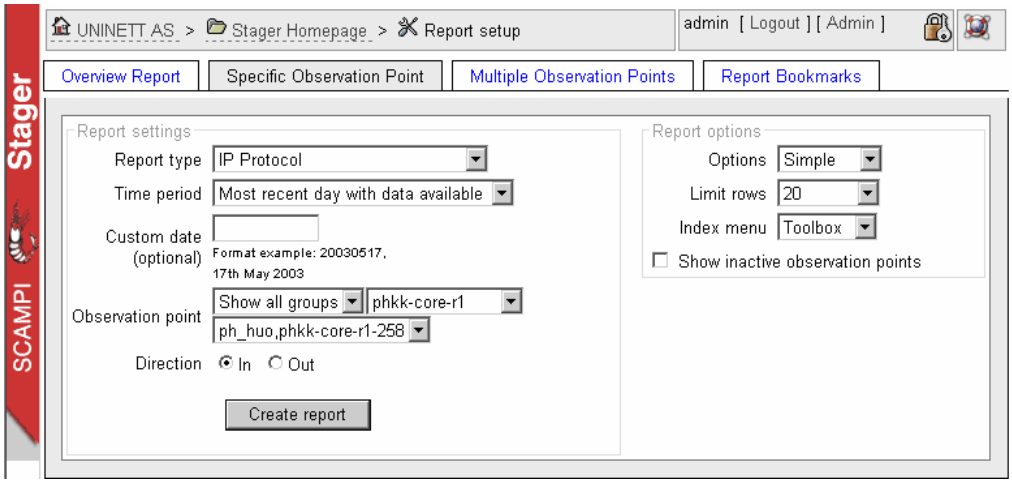
Tässä vaiheessa tehtiin konfiguraatiomuutokset reitittimeen, joka toimi NetFlow-laitteena. Koska kyseessä oli vain kokeilu, tehtiin konfiguraation vain vähäisiä muutoksia. Asetettiin yksi VLAN (Virtual Local Area Network) toimimaan NetFlow-liityntänä, joka kerää NetFlow-tietoa NetFlow-cacheen. Tämän jälkeen määriteltiin käytettävä NetFlow-versio sekä liityntä, josta NetFlow-tiedot tulevat ulos, kun ne lähtevät kohti NetFlow-keräintä. Koska Stager käytti NetFlow-tietojen analysointiin flow-tools-apuohjelmaa ja tämä ei tukenut NetFlow-versiota 9, jouduttiin käyttämään versiota 5. Konfiguraatiomuutokset olivat seuraavanlaiset (IP-osoite ja vlan-numero ovat kuvitteellisia).

```
Router(vlan)# ip flow ingress
Router(config)# ip flow-export version 5
Router(config)# ip flow-export source vlan 100
Router(config)# ip flow-export destination 192.168.1.1  9997
```

Kun asennukset oli tehty, siirryttiin vaiheeseen, jossa NetFlow-laitteen tiedot piti lisätä tietokantaan. Tämä tehtiin käyttämällä ohjelma mukana tullutta skriptiä, joka luki raakaflow-tiedoista IP-osoitteen, josta tiedot tulevat, ja ifIndex-lukeman, jota tarvitaan määrittelelyissä, sekä liitynnät, joista NetFlow-tietoa kerätään. Kun skripti oli saanut IP-osoitteen, se haki siihen liittyvän nimen host-komennolla. Tämän jälkeen skripti kirjasi tiedot tekstitiedostoon sekä lisäsi ne itse tietokantaan.

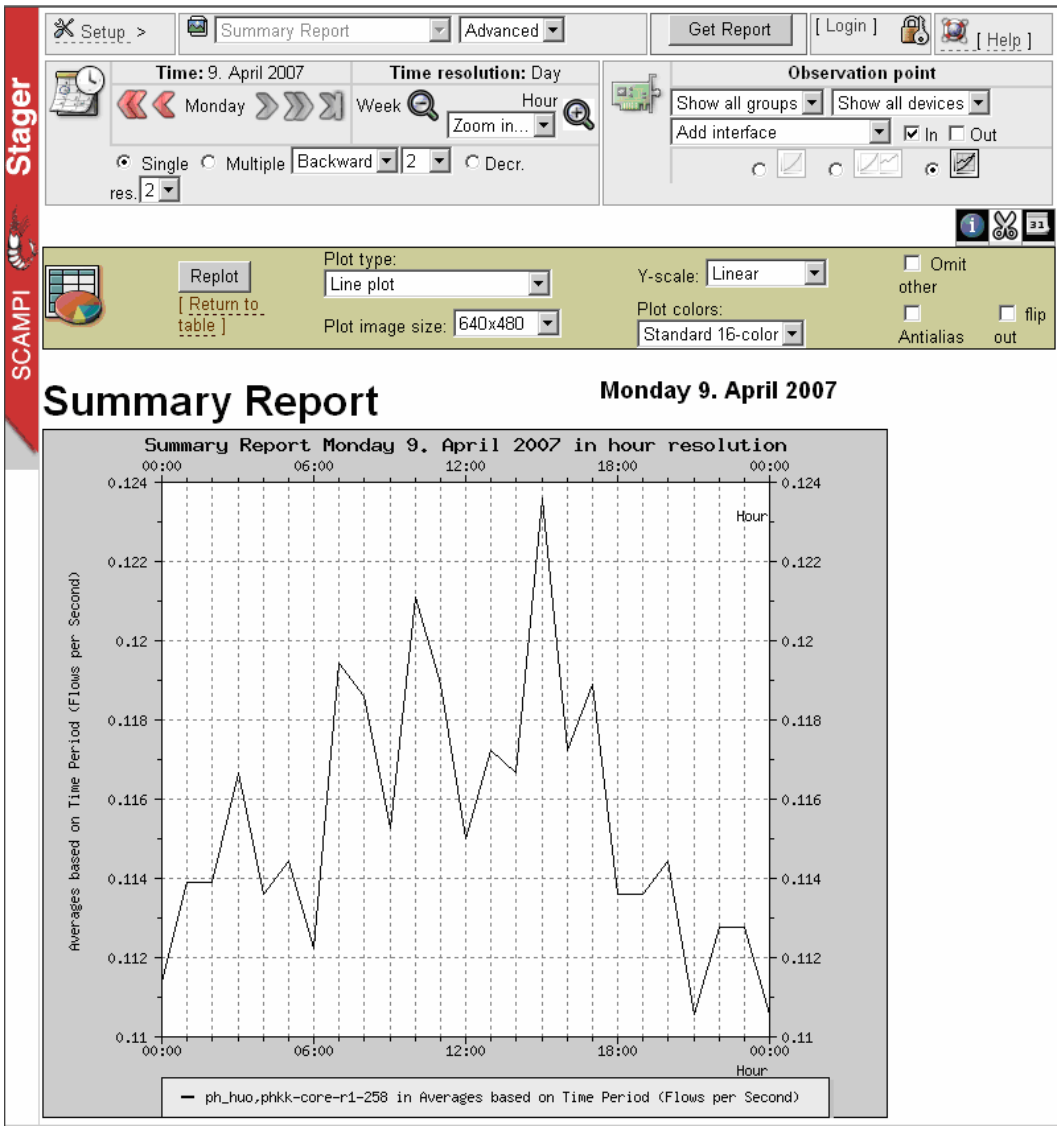
Seuraavaksi oli vielä lisättävä käyttäjien tiedot tietokantaan, jotta voidaan käyttää web-käyttöliittymää. Oletuksena vierailevalla käyttäjällä on mahdollisuus nähdä osa raporteista, mutta tässä tapauksessa se estettiin ja vain käyttäjätunnuksen omistavalla käyttäjällä on mahdollisuus tarkastella raportteja ja laitetietoja. Nyt ohjelma oli valmis käytettäväksi.

Stagerin web-käyttöliittymä on hyvin selkeä ja sen käytön omaksui nopeasti (katso KUVIO 11). Vaikka ohjelmaa käyttäisi ensimmäistä kertaa, onnistuu erilaisten raporttien teko melko vaivattomasti. Aluksi valittiin haluttu tarkkailupiste, seuraavaksi aikaväli, jolta halutaan raportit, ja lopuksi vielä se, minkä tyyppisen raportin haluaa nähdä. Tämän lisäksi käyttäjä voi määritellä raportin ulkoasuun liittyviä asioita, kuten kuinka monta riviä näytetään ruudulla.

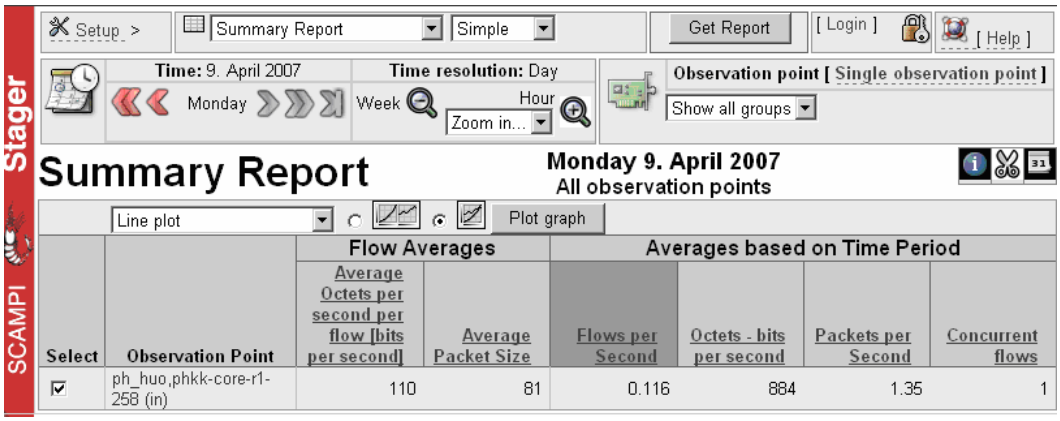


KUVIO 11. Stagerin käyttöliittymä

Stagerilla voidaan tutkia erilaisia verkon liikennöintiin liittyviä asioita. Eniten liikennöivät IP-osoitteet ja IP-protokollien käyttöprosentit lienevät käytännöllisimmät näistä raporteista. Raporteista voidaan luoda erilaisia kuvaajia, kuten piirakkamalli, viivamallia tai aluemalli. Kuvioissa 12 ja 13 näkyvillä erilaisia näkymiä käyttöliittymästä. Verkko, jossa NetFlow oli käytössä, oli melko vähäliikenteinen ja liikenne koostui pelkästä UDP-liikenteestä. Tämän vuoksi yleisraportin tiedot näyttävät niin pientä liikennemäärää.



KUVIO 12. Viivamallinen raportti



KUVIO 13. Yleisraportti taulukkomuodossa

6 YHTEENVETO

Tämän opinnäytetyön päätarkoituksena oli perehtyä NetFlow-verkonvalvonta-protokollaan. Aluksi tutustuttiin hieman verkonhallintaan yleisellä tasolla. Työssä käytiin teoriatasolla läpi SNMP- ja NetFlow-protokollat. Jälkimmäisestä kirjoitettiin hieman syvällisemmin, koska se oli työn pääaiheena. Työkaluina vertailtiin Cisco Systemsin maksullista CS Mars -järjestelmää sekä vapaan lähdekoodin ilmaista Stageria. Stagerin asennus käydään myös läpi.

Itse opinnäytetyössä otettiin testikäyttöön Stager-ohjelmisto ja sen avulla tutkittiin NetFlow:n käyttäytymistä. Stager valittiin sen vuoksi, että se oli ilmainen ja sitä pääsi alustavasti kokeilemaan tekijän Internet-sivuilla. Ohjelma käytti hyödykseen monia muita apuohjelmia sekä PostgreSQL-tietokantaa. Ongelmaksi muodostui hieman puutteellinen dokumentointi ja eri apuohjelmien yhteensopivuus keskenään.

Stageriin olisi myös mahdollista ottaa käyttöön SNMP, mutta koska se oli jo käytössä toisilla ohjelmilla, jätettiin se asentamatta. Itse NetFlow-puoli vaikutti todella hyvältä suhteutettuna siihen, että kyseessä oli ilmainen ohjelma. Koska asennuksessa oli melko paljon ongelmia, tuli ohjelman taustalla pyörivien prosessien toimintaan tutustuttua melko huolella jo asennusvaiheessa. Itse ohjelman käyttö ei vaatinut paljoakaan tutkimista, vaan sitä oli todella helppo hallita.

Opinnäytetyö antoi hyvän kuvan siitä, millaista verkonhallinta ja valvonta todellisuudessa on, sekä auttoi ymmärtämään, miten tärkeitä nämä verkonvalvojien käyttämät apuohjelmat ovat. Työssä oli tarkoituksena oppia NetFlow-protokollan toiminta, joka ei pelkästään rajoittunut flow-tietojen keräämiseen ja niiden analysointiin. Tiedot kulkivat monen eri ohjelman läpi, ennen kuin niitä voitiin tarkastella web-selaimen kautta hienoina kuvaajina. Näiltä osin opinnäytetyö onnistui hyvin, vaikka aikataulu oli hieman tiukka. Tulevaisuudessa NetFlow otetaan mahdollisesti käyttöön koko verkkoon ja keräinpalvelin vaihdetaan tehokkaampaan.

Yrityksille verkonhallinta alkaa nykyään olla jo arkipäivää. Tietoverkot kehittyvät aina vain monimutkaisemmiksi ja niistä löytyy yhä enemmän palveluita. Tämä asettaa myös tiettyjä vaatimuksia verkon toiminnalla ja saatavuudelle. Perusteellinen verkonvalvonta edellyttää, että käytössä on useampia ohjelmistoja, joiden tietoja sitten vertaillaan ja niistä tiedoista tehdään erilaisia päätelmiä. Verkonvalvoja on siis tulevaisuudessa melko tärkeässä asemassa, koska pienetkin katkokset verkossa voivat tietää yrityksellä tulojen menetyksiä.

LÄHTEET

Allen, J. 2002. CERT Verkkotietoturvan hallinta. Helsinki: Edita Prima Oy.

Cisco IOS NetFlow Command Reference, Release 12.4 [verkkojulkaisu]. Cisco Systems, Inc [viitattu 1.3.2007]. Saatavissa http://www.cisco.com/en/US/products/ps6350/products_command_reference_chapter09186a0080443cb7.html

Cisco Security Monitoring, Analysis and Response System 4.2 [verkkojulkaisu]. Cisco Systems, Inc [viitattu 1.3.2007]. Saatavissa http://www.cisco.com/en/US/products/ps6241/products_data_sheet0900aecd80272e64.html

Claise, B. 2004. Cisco Systems NetFlow Services Export Version 9 [verkkojulkaisu]. Internet Society [viitattu 1.3.2007]. Saatavissa ftp://ftp.rfc-editor.org/in-notes/rfc3954.txt

Comer, D. 2002. TCP/IP. Jyväskylä: Gummerus.

Garcia, B. 2002. Creating an SNMP Component [verkkojulkaisu]. 15 Seconds [viitattu 2.4.2007]. Saatavissa http://www.15seconds.com/issue/020723.htm

Gredler, H. & Semeria, C. 2001. Juniper Networks Solutions for Network Accounting [verkkojulkaisu]. Juniper Networks [viitattu 12.4.2007]. Saatavissa: http://www.juniper.net/solutions/literature/white_papers/200010.pdf

Greene, B. & Smith, P. 2002. Cisco ISP Essentials. Indianapolis: Cisco Press.

Hautaniemi, M. 1994. TKK/ATK-keskuksen TCP/IP-verkon valvonta ja hallinta [verkkojulkaisu]. Helsinki: Teknillinen korkeakoulu [viitattu 1.3.2007]. Saatavissa http://users.tkk.fi/%7Ehau/thesis/verkonhallinta.html

Introduction to Cisco IOS NetFlow - A Technical Overview [verkkojulkaisu]. Cisco Systems, Inc [viitattu 1.3.2007]. Saatavissa http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo Finland Oy.

Kizza, J. 2005. Computer network security. New York: Spinger Science+Business.

NetFlow Performance Analysis [verkkojulkaisu]. Cisco Systems, Inc [viitattu 1.3.2007]. Saatavissa http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd802a0eb9.shtml

Reynders, D. & Wright, E. 2003. TCP/IP and Ethernet Networking. Burlington: Newnes.

Solberg, A. 2005a. Installing and running the Stager application [verkkojulkaisu]. UNINETT AS [viitattu 1.3.2007]. Saatavissa http://software.uninett.no/stager/doc/install.html

Solberg, A. 2005b. Stager User Documentation [verkkojulkaisu]. UNINETT AS [viitattu 1.3.2007]. Saatavissa http://software.uninett.no/stager/doc/userdoc.html