Pasi Kukkola

VERKKOLIIKENNEANALYSAATTORI LINUX-YMPÄRISTÖSSÄ

Opinnäytetyö
KESKI-POHJANMAAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Toukokuu 2010

KESKI-POHJANMAAN AMMATTIKORKEAKOULU
MELLERSTA ÖSTERBOTTENS YRKESHÖGSKOLA

TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Yksikkö **Ylivieska**	**Aika** Toukokuu 2010	**Tekijä** PASI KUKKOLA
Koulutusohjelma **TIETOTEKNIIKKA**		
Työn nimi **VERKKOLIIKENNEANALYSAATTORI LINUX-YMPÄRISTÖSSÄ**		
Työn ohjaaja HANNU PUOMIO		**Sivumäärä** 45 + 16
Työelämäohjaaja MIKKO NIEMELÄ		

Tämä opinnäytetyö tehtiin Oulun Yliopiston projektiin. Työ annettiin tehtäväksi insinööri Mikko Niemelän toimesta. Insinööri Mikko Niemelä toimii Oulun Yliopistossa projekti-insinöörinä. Opinnäytetyön tarkoituksena oli rakentaa ympäristö, joka kerää tietoa verkkoliikenteestä, ja esittää sen aikajaksoisessa kuvaajassa.

Tehtävänä oli liittää kaksi tietokonetta toisiinsa bridge-ohjelmiston avulla kolmannen tietokoneen kautta. Kun kaksi tietokonetta saatiin ottamaan yhteyttä toisiinsa kolmannen tietokoneen kautta, asennettiin silloittavaan tietokoneeseen verkkoliikenneanalysaattori-ohjelmisto nimeltään Wireshark verkkoliikenteen tutkimista varten. Tiedostojen jakoa varten asennettiin SAMBA-palvelin tietoja lähettävälle tietokoneelle. Tiedonsiirtoa varten asennettiin FTP-palvelin tietoja lähettävälle tietokoneelle. UDP-suoratoistoa varten asennettiin VLC-mediasoitin lähettävälle ja vastaanottavalle tietokoneelle. Verkkoliikenteen seuraamista varten asennettiin ohjelmisto nimeltään Ntop silloittavaan tietokoneeseen.

Verkkoliikenteessä seurattavien tiedostojen osalta ei ollut merkitystä, mitä ne sisälsivät. Ennen kuin tietoja pystyi siirtelemään tietokoneelta toiselle, täytyi tehdä jokaiselle tietokoneelle asianmukaiset asetukset verkkoliikennettä varten.

Lähiverkosta oli tarkoitus saada irti verkkoliikennettä UDP-protokollalla.
Tavoitteena oli myös saada Ntop ohjelma tuottamaan graafeja muutenkin kuin yleisellä tasolla.

Asiasanat
Linux, Verkkoliikenneanalysaattori, Samba, Ntop, Wireshark, Ubuntu, Bridge, Verkkoasetukset

CENTRAL OSTROBOTHNIA
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

CENTRAL OSTROBOTHNIA UNIVERSITY OF APPLIED SCIENCES YLIVIESKA	**Date** May 2010	**Author** PASI KUKKOLA
Degree programme **Information Technology**		
Name of thesis **NETWORK ANALYZER IN LINUX SYSTEMS**		
Instructor HANNU PUOMIO		**Pages** 45 + 16
Supervisor MIKKO NIEMELÄ		

This thesis was done for a project of the University of Oulu. It was commissioned by Engineer Mikko Niemelä. Engineer Mikko Niemelä is A project engineer in the University of Oulu. The purpose was to build an environment that collects data about network traffic and shows it with time sequence graphics.

Two computers had to be connected to the same network. Computers were connected with a bridge program of A third computer. When the computers were connected, a program called Wireshark was installed to examine network traffic. So that files could be shared, a Samba server was installed. For the file transfer an FTP server was installed. A VLC media player had to be installed, because it can be A video server and with it it is possible to watch videos with UDP-protocol. When Ntop program was installed, it was possible to examine network traffic graphically.

It was not important what kinds of files were followed. Before data could be transferred from one computer to another, one had to adjust the network settings of each computer.

The purpose was that there would be network traffic using UDP-protocol, in addition, the aim was to make the NTOP program produce graphs also in other levels, not only in the general level.

Asiasanat
Linux, Network analyzer, Samba, Ntop, Wireshark, Ubuntu, Bridge, Network settings

LYHENTEET

ARP	Address Resolution Protocol
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
PING	Packet Internet Groper
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

ESIPUHE

Opinnäytetyön aihe, saatiin opettajien lehtori Ritva Saviluodon ja lehtori Hannu Puomion kautta. Lehtori Ritva Saviluoto kertoi lehtori Hannu Puomiolle, että olen vailla opinnäytetyön aihetta. Insinööri Mikko Niemelä oli ilmoittanut lehtori Hannu Puomiolle aiheesta verkkoliikenneanalysaattori Linux-ympäristössä. Sain minua kiinnostavan aiheen. Uskon Linuxin osaamisesta olevan hyvin paljon hyötyä työmarkkinoilla. Verkkoliikenneanalysaattori ohjelmiston osaamisesta voi olla hyötyä verkon virheiden tutkimista vaativissa töissä.

Haluan kiittää insinööri Mikko Niemelää ja lehtori Hannu Puomiota kaikesta avusta ja opastuksesta. Haluan kiittää insinööri Linus Torvaldsia ja muita vapaitten ohjelmistojen kehittäjiä mahdollisuudesta toteuttaa opinnäytetyö ilman minkäänlaisia lisenssimaksuja.

1 JOHDANTO

Tämä opinnäytetyö tehtiin Oulun yliopistolle ja Oulun Eteläisen Instituutille vuonna 2010 tammikuun ja toukokuun välisenä aikana. Käytännön työ tehtiin Keski-Pohjanmaan ammattikorkeakoulun, Ylivieskan yksikön tietokoneluokassa. Käytännön osuus aloitettiin varsinaisesti tammikuun lopussa, ja saatiin valmiiksi huhtikuun aikana.

Tämä opinnäytetyö soveltuu luettavaksi niille, joita kiinnostaa verkkoliikenneanalysaattorin käyttöönotto Linux-ympäristössä. Opinnäytetyö soveltuu myös kaikille niille, jotka haluavat luoda lähiverkon Linux-käyttöjärjestelmien välillä.
Suosittelen käyttämään opinnäytetyötäni lähteenä opinnäytetöihin, joissa täytyy yhdistää tietokoneita toisiinsa Linux-käyttöjärjestelmän avulla.

Opinnäytetyön tarkoituksena oli rakentaa ympäristö, joka kerää tietoa verkkoliikenteestä, ja esittää sen aikajaksoisessa kuvaajassa. Aikajaksoiseen kuvaajaan oli tarkoitus saada tiedot näkymään jokaista porttia kohden omana kuvaajana.

Verkkoliikenneanalysaattori on verkkoliikenteen seuraamiseen tarkoitettu laite tai ohjelmisto. Verkkoliikenneanalysaattorilla voidaan selvitellä verkossa tapahtuvia vikatilanteita tai muita verkkoliikenteeseen liittyviä asioita. Ohjelmallisella verkkoliikenneanalysaattorilla voidaan selvittää verkkoliikennettä protokollatasolla. Wireshark-niminen ohjelma on sopiva tähän tarkoitukseen. Wireshark on ilmainen ja vapaasti muokattava ohjelma. Verkkoliikenteen graafista esittämistä varten sopiva ohjelma on Ntop-niminen vapaasti muokattava ja ilmainen ohjelma. Opinnäytetyössä oli tarkoitus käyttää mahdollisimman paljon hyödyksi Linuxin ilmaisia vapaita ohjelmistoja.

Linux on suomalaisen Linus Torvaldsin alulle laittama vapaan lähdekoodin käyttöjärjestelmä UNIX-käyttöjärjestelmästä. Linuxin ytimen tekijänoikeudet omistaa Linus Torvalds. Linuxia saa muokata ja käyttää ilmaiseksi. Linuxia saa myös vapaasti myydä eteenpäin. Linux on ladattavissa useina erilaisina jakeluversioina Internetistä ilmaiseksi. Linuxin jakeluversion Ubuntu, voi ladata Ubuntu Suomi-nimisen yhteisön verkkosivujen kautta.

Alukssa tarjottiin mahdollisuutta käyttää serverinä Windows-käyttöjärjestelmää. Valittiin kolmeen tietokoneeseen Linuxin jakeluversio, koska Windows antoi käyttää vain yhden

kuukauden käyttöjärjestelmää ilman aktivointia. Opinnäytetyöhön valittua Linuxin jakeluversiota kutsutaan nimellä Ubuntu.

Alussa meni paljon aikaa rikkinäisten tietokoneitten kanssa. Lopulta löydettiin ne tietokoneet, joilla työ oli mahdollista saattaa loppuun asti. Suurin osa asioista selvitettiin tutkimalla, tietoa hakemalla ja kokeilemalla. Aineistoa opinnäytetyöhön löydettiin monista eri kirjoista, Linux-ohjelmien ohjeista sekä Internetistä. Pohjatietojen hakemisen jälkeen oli mahdollista aloittaa varsinainen opinnäytetyön työstäminen.

Miettimistä pidemmän aikaa aiheuttivat verkkoasetusten oikeanlaiset asetukset. Verkkoasetuksille löydettiin hyvin tietoa, ja tietokoneet saatiin yhdistettyä toisiinsa. Aluksi tietokoneet yhdistettiin toisiinsa hubin avulla tavallisella verkkokaapelilla. Hubin kautta yhdistettynä verkkokorttien IP-osoitteiden täytyi kuulua saman lähiverkon alaisuuteen. Koska tarkoitus oli saada varmasti kaksi tietokonetta keskustelemaan kolmannen tietokoneen verkkokorttien kautta, vaihdettiin tavallinen verkkokaapeli ristikytkettyyn verkkokaapeliin. Lähiverkko yritettiin saada toimimaan ristikytketyllä verkkokaapelilla kytkemällä suoraan ristikytketty verkkokaapeli verkkokortista toiseen. Suora yhdistäminen kolmen tietokoneen välillä ei ollut kuitenkaan aivan näin yksinkertaista.

Kolmannen tietokoneen kautta kulkeva verkkoliikenne saatiin toimimaan tekemällä kolmanteen tietokoneeseen silta kahden verkkokortin välille. Verkkokorttien silloittamiseen käytettiin bridge ohjelmistoa. Bridge ohjelmisto täytyi erikseen asentaa terminaalin käskyllä Internetiä apuna käyttäen.

Verkkoliikenteen tuottaminen UDP-protokollalla oli aluksi haasteellista. Wireshark ohjelman avulla saatiin tarkkailtua verkkoliikenteessä liikkuvien protokollien tietoja. Opinnäytetyön lopussa perehdytään lyhyesti Wireshark-ohjelman tuloksiin. Wireshark- ohjelmalla tuotettu tieto tuntui aluksi oudolta tutkittavalta. Tietojen tutkiminen selventyi kirjastosta lainatun kirjallisuuden kautta.

Opinnäytetyössä käytetään *kursivointia*, esittämään tietokoneen komentoja, tietokoneessa kirjoitettua tekstiä, sekä tietokoneessa tulostettua tekstiä. Kun kirjoitetaan komentoja Linuxin komentokehotteessa, eli terminaalissa, niin käytetään käskyn edellä terminaalissa näkyvää tunnistetta. Tunniste käskyn edellä on esimerkiksi tietokoneessa jope seuraavanlai-

nen: *jope@jope:~$*

Edellä näkyvä tunniste *jope@jope:~$*, ilmaisee, että käytetään tietokonetta, jonka isäntänimeksi on annettu jope.

Opinnäytetyön tekeminen Linuxia apuna käyttäen kiinnosti minua Linuxin avoimen lähdekoodin osalta. Kun käytin Linuxia, niin huomasin monia asioita joita saa valmiiksi toteutettuna ilmaiseksi. Opinnäytetyöhön valitsemani aihe motivoi minua ottamaan selvää enemmän Linuxin tietoturvaan liittyvistä ominaisuuksista. Opinnäytetyö Linux-ympäristössä tukee ja kehittää minun ammatillista osaamista Linux-asiantuntijana.

Kun puhutaan tietotekniikasta, niin tietotekniikka ulottuu muihinkin laitteisiin kuin pelkästään PC-tietokoneisiin. Monissa uusissa laitteissa tullaan tulevaisuudessa tarvitsemaan Linuxin osaamista sekä tietoturvan osaamista. Linuxin osaaminen ja tietoturvan osaaminen luovat vahvan perustan mahdollisuuksille menestyä työelämässä.

2 LAITTEISTO

2.1 Yleistä käytettävistä laitteista

Laitteiston kanssa oli moneen kertaan ongelmia. Tietokoneita jouduttiin vaihtamaan useaan kertaan toimimattoman tietokoneen takia. Joissakin tietokoneissa tietokone ei lähtenyt ollenkaan päälle. Ongelma, jossa tietokone ei lähtenyt ollenkaan päälle, saatiin ratkaistua seuraavalla tavalla:

1. Laitettiin tietokoneen virtakytkin nollaan.
2. Otettiin tietokoneen virtajohto irti seinäpistokkeesta.
3. Kun virrat olivat täysin pois päältä, painettiin virtakytkintä useaan kertaan.
4. Kun virtakytkimen useasti painamisen jälkeen laitettiin virrat päälle ja painettiin virtakytkintä, lähti tietokone päälle.

Tietokoneessa YKAY-TIETOL-2, kovalevyn paikalleen laittaminen ja käyttöjärjestelmän käynnistäminen aiheutti käyttöjärjestelmän sekoamisen. Kovalevyn muisti vaikutti aivan yhtäkkiä tulleen niin täyteen, ettei tietokoneeseen ollut mahdollista kirjautua ollenkaan sisään graafisen käyttöliittymän kautta. Tietokoneesta saatiin talteen tarpeelliset tiedostot, kun kirjauduttiin käyttöjärjestelmään sisälle tekstipohjaisen käyttöliittymän kautta.

Tietokoneessa YKAY-TIETOL-3, johon olisi haluttu laittaa 40 Gt:n kovalevy, tietokone teki virtanapin painamisen jälkeen seuraavalla tavalla:

1. Virrat kävivät päällä.
2. Tietokone sammui.

Edellä esitetyt vaiheet 1 ja 2 toistuivat taukoamatta. Ei voitu käyttää tietokoneessa YKAY-TIETOL-3 40 Gt kovalevyä. Kun laitettiin 20 Gt kovalevy tietokoneeseen YKAY-TIETOL-3, niin tietokone alkoi toimia.

Tietokoneet YKAY-TIETOL-12, YKAY-TIETOL-3 ja YKAY-TIETOL-11 nimettiin Ubuntun asennuksen yhteydessä nimillä Jope, Repe ja Topi.

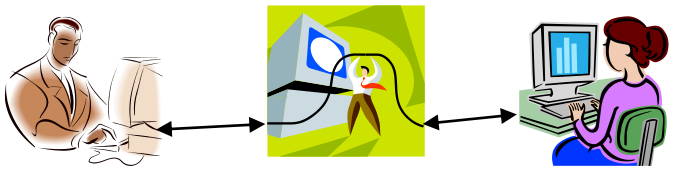
Antamalla terminaalissa käskyn *hostname*, saatiin tietokoneissa Jope, Repe ja Topi selvitettyä jokaisessa erikseen oma isäntänimi.

KUVIO 1

KUVIO 2

Kuviosta 1 selviää, millä tavalla tietokoneet Jope, Repe ja Topi liitettiin kiinni toisiinsa. Kuviossa 1 näkyy tietokoneen repe verkkokortit. Tietokoneiden Jope, Repe ja Topi yhteen liittämisessä käytettiin ristikytkettyä verkkokaapelia. Ylempi ristikytketty verkkokaapeli lähti tietokoneen Repe verkkokortista tietokoneen Jope verkkokorttiin. Alempi ristikytketty verkkokaapeli lähti tietokoneen Repe verkkokortista tietokoneen Topi verkkokorttiin.

Kuviossa 2, näkyy käytössä olevien tietokoneiden vaihtokelkka. Opinnäytetyön tekemistä jatkettaessa otettiin yleisesti käytössä oleva vaihtokelkka irti tietokoneesta. Opinnäytetyötä varten varattu vaihtokelkka vaihdettiin työtä aloitettaessa paikalleen. Vaihtokelkka täytyi työntää kunnolla paikalleen. Lopuksi vaihtokelkan lukitsevalla avaimella lukittiin vaihtokelkan avaimenreiästä lukitus kiinni asentoon. Opinnäytetyötä varten oli käytössä 3 vaihtokelkkaa, jotka kaikki sisälsivät oman kovalevyn.



topi repe jope

KUVIO 3

Kuviosta 3, selviää opinnäytetyössä käytetty toimintatapa tietokoneiden jope, repe ja topi välillä. Kaikki verkkoliikenne tietokoneen topi ja tietokoneen jope välillä kulkee tietokoneen repe kautta. Tietokone repe tutkii verkkoliikennettä.

2.2 Tietokoneen Jope kokoonpano

Tietokonetta Jope varten käytettiin tietokonetta nimeltä YKAY-TIETOL-12.

Tietokoneen Jope kokoonpanoon kuuluivat:

Verkkokortti, ADMtek Comet
Näytönohjain, RADEON X600/X550 Series
Suoritin, Intel® Pentium® 4 CPU 3.40GHz
DVD-asema, HL-DT-ST DVD-RW GWA-4160B
Muistia, 2 x SAMSUNG, 512MB DDR PC3200 CL3
Kovalevy, SAMSUNG, SV2042H, 20.4GB

Tietokoneen Jope tehtävänä oli vastaanottaa tiedostoja. Tietokoneeseen Jope laitettiin videokoodekit kuntoon yleisimmin tarvittavia videotiedostoja varten. Tietokoneeseen Jope asennettiin VLC mediasoitin videoiden toistamista varten ja FileZilla FTP-ohjelma tiedostojen siirtämistä varten.

2.3 Tietokoneen Repe kokoonpano

Tietokonetta Repe varten käytettiin tietokonetta nimeltä YKAY-TIETOL-3.
Tietokoneen Repe kokoonpanoon kuuluivat:

2 verkkokorttia, ADMtek Comet
Näytönohjain, RADEON X600/X550 Series
Suoritin, Intel® Pentium® 4 CPU 3.40GHz
DVD-asema, HL-DT-ST DVD-RW GWA-4160B
Muistia, 2 x SAMSUNG, 512MB DDR PC3200 CL3
Kovalevy, SAMSUNG, SV2042H, 20.4GB

Tietokoneen Repe tehtävänä oli kaapata kaikki mahdollinen verkkoliikenne mikä on kaapattavissa sekä välittää tietoja tietokoneen Jope ja tietokoneen Topi välillä. Tietokone Repen tehtävä oli myös toteuttaa graafiset kuvaajat verkkoliikenteestä. Tietokoneeseen Repe asennettiin Wireshark verkkoliikenneanalysaattori ohjelmisto ja Ntop verkon analysointi ohjelma. Tietokoneeseen Repe asennettiin silloitusohjelmisto, jonka avulla tietokone Jope ja tietokone Topi pystyivät ”keskustelemaan” tietokoneen Repe välityksellä. Kaikki lähetetty ja vastaanotettu tieto tietokoneen Topi ja tietokoneen Jope välillä kulki tietokoneen Repe verkkokortin kautta.

2.4 Tietokoneen Topi kokoonpano

Tietokonetta Topi varten käytettiin tietokonetta nimeltä YKAY-TIETOL-11.

Tietokoneen topi kokoonpanoon kuuluivat:

Verkkokortti, ADMtek Comet
Näytönohjain, RADEON X600/X550 Series
Suoritin, Intel® Pentium® 4 CPU 3.40GHz
DVD-asema, HL-DT-ST DVD-RW GWA-4160B
Muisti, 2 x SAMSUNG, 512MB DDR PC3200 CL3
Kovalevy, Seagate, ST340016A, 40GB

Tietokoneen Topi tehtävänä oli toimia tietojen lähettäjänä. Tietokoneeseen Jope asennettiin Samba-palvelin tiedostojen jakamista varten, FTP-palvelin ohjelma nimeltään PureFtp tiedonsiirron varastoksi, sekä VLC mediasoitin videoserveriksi.

3 LINUX

Linuxia voidaan käyttää moneen tarkoitukseen. Monet tekniset laitteet sisältävät käyttöjärjestelmänään Linux-käyttöjärjestelmän. Linux on mukana monessa yrityksessä palvelinkäytössä. Koska Linux on hyvin vakaa käyttöjärjestelmä, niin Linux voi olla tietokoneessa päällä jopa kymmeniä vuosia, eikä Linuxia tarvitse välillä sammuttaa tai uudelleen käynnistää käyttöjärjestelmän jumiutumisen takia. Linuxin pääasiallinen käyttötarkoitus on olla vapaasti muokattavissa oleva ilmainen käyttöjärjestelmä tietokoneeseen.

Linuxista on olemassa useita jakeluversioita. Tässä opinnäytetyössä käytetty jakeluversio on nimeltään Ubuntu. Kaikki Linuxin jakeluversiot koostuvat ohjelmista, jotka on rakennettu Linux-ytimen ympärille. Linux-ydintä kehittää Linus Torvalds. Linux-ydin mahdollistaa Linux-käyttöjärjestelmän toiminnan tietokoneessa. Linux-ydin on vakaa ja turvallinen usean ohjelman ja käyttäjän yhtä aikaa vakaasti toiminnassa mahdollistava perustus graafiselle X-ikkunointi ympäristölle. Graafinen X-ikkunointi ympäristö mahdollistaa graafiseksi ohjelmoitujen ohjelmien käyttämisen tietokoneessa.

3.1 Ubuntu

Ubuntu on laajalle levinnyt Linuxin jakeluversio. Zulukielinen nimi "Ubuntu" tulee yleisestä afrikkalaisesta yhteisöllisyyden ideologiasta ja se käännetään usein lyhyesti "inhimillisyydeksi toisia kohtaan". Ubuntun kehitystä rahoittaa eteläafrikkalaisen yrittäjän Mark Shuttleworthin perustama Canonical Ltd. Vuonna 2005 Mark Shuttleworth perusti Ubuntu-säätiön ja sijoitti siihen 10 miljoonaa dollaria. Säätiön tarkoituksena on tukea Ubuntun kehitystä. (Ubuntu, About Ubuntu name & Ubuntu Foundation, 2010.)

Ubuntun käyttötarkoitus on kehittäjien mukaan olla helppokäyttöinen Linux-käyttöjärjestelmä. Helppokäyttöisyys on Ubuntussa todellista. Ubuntuun voi hakea ilmaisia ohjelmia Ubuntun hakutoiminnon kautta Internet-yhteyden hinnalla. Tiedonsiirtomaksut ovat tietysti pakollisia. Itse Ubuntun asentaminen ei kuitenkaan vaadi minkäänlaisia maksuja, koska Ubuntun asennuslevyn voi tilata ilmaiseksi Ubuntun verkkokaupasta.

Koska kaikki videokoodekit eivät ole ilmaisia, täytyi käyttää Medibuntun epävirallisia koodikirjastoja apuna. Suljetut video-koodekit saatiin Ubuntussa toimimaan seuraavalla tavalla:

jope@jope:~$ sudo wget --output-document=/etc/apt/sources.list.d/medibuntu.list http://www.medibuntu.org/sources.list.d/$(lsb_release -cs).list && sudo apt-get --quiet update && sudo apt-get --yes --quiet --allow-unauthenticated install medibuntu-keyring && sudo apt-get --quiet update (Mbnet, 2010.)

jope@jope:~$ sudo apt-get install libdvdcss2
jope@jope:~$ sudo apt-get install non-free-codecs
(Mbnet, 2010.)

3.2 Verkkoasetukset

Verkkoasetusten käyttötarkoitus on saada kaikki mahdolliset verkossa olevat tietokoneet keskustelemaan keskenään halutulla tavalla. Pieni kirjoitusvirhe verkkoasetuksissa voi tarkoittaa sitä, että tietokone ei voi saada yhteyttä toiseen verkossa olevaan tietokoneeseen.

Linuxissa hosts tekstitiedosto löytyi polusta /etc/hosts.

Terminaaliin kirjoitettiin käsky:

jope@jope:~$ sudo nano /etc/hosts

Käskyn antamisen jälkeen terminaalissa kysyttiin käyttöjärjestelmän salasanaa. Kun käyttöjärjestelmän salasana annettiin oikein, avautui tekstitiedosto *hosts* muokattavaksi nano tekstieditorilla.

Hosts tekstitiedostossa määritettiin kaikki ne tietokoneet, jotka tunnistettiin saman verkon isänniksi. Kun kaikki tarpeelliset tiedot oli muokattu tekstitiedostoon *hosts*, tallennettiin tekstitiedosto *hosts* näppäinyhdistelmällä Ctrl+o. Nano tekstieditorista pääsi takaisin terminaalin käskytilaan näppäinyhdistelmällä Ctrl+x.

Interfaces tekstitiedostoon asetettiin kaikki verkkokortin tarvitsemat määritykset. Verkkokortin määritykset olivat pakollisia lähiverkkoa rakennettaessa. Verkkokortin määritysten kautta toiset lähiverkossa olevat tietokoneet voivat tunnistaa lähiverkossa olevien tietoko-

neiden verkkokortit lähiverkossa. Lähiverkossa oleva tietokone tunnistetaan lähiverkossa verkkokortin IP-osoitteen perusteella. Kun verkkokortti yksilöidään lähiverkossa, niin tunnistaminen tapahtuu MAC-osoitteen avulla. Oman verkkokortin MAC-osoitteen voi selvittää Linuxissa käskyllä *ifconfig* . *Ifconfig* näyttää verkkokortin juuri sillä hetkellä toiminnassa olevat asetukset. MAC-osoite löytyy ifconfig-tulosteesta nimellä *HWaddr*.

Kun esimerkiksi halutaan tietää tietokoneen Jope verkkokortin MAC-osoite, annetaan tietokoneen jope terminaalissa käsky *ifconfig*. *Ifconfig*-käskyn tulostamassa tiedossa näkyy tekstirivi:

HWaddr 00:30:05:85:03:21 (LIITE 2.)

Tulostetusta rivistä tiedetään, että Jopen verkkokortin MAC-osoite on *00:30:05:85:03:21*. Verkkokortille valittava IP-osoite olisi voinut olla opinnäytetyössä aivan mikä tahansa, koska tarkoitus ei ollut käyttää lähiverkkoa Internettiin liitetyssä lähiverkossa. Lähiverkkoa varten on kuitenkin olemassa aivan omat IP-osoitteet. Käytettiin lähiverkkoa varten olevia IP-osoitteita. Verkkoasetukset tietokoneille Jope, Repe ja Topi, löytyy liitteistä LIITE 1, LIITE 2 ja LIITE 3.

TAULUKKO 1, lähiverkon IP-osoitteet. (mukaillen Hakala & Vainio 2002, 158.)

Erikoisosoite	Käyttötarkoitus
0.0.0.0	Varattu, ei käytössä nykyisin. Aiemmin käytetty broadcast-viesteihin
10.0.0.0 – 10.255.255.255 192.168.0.0 – 192.168.255.255 172.16.0.0 – 172.31.255.255	intranet
127.0.0.0 – 127.255.255.255	loop back –osoitteet (kone viittaa itseensä osoitteella 127.0.0.1 = ns. localhost)
224.0.0.0	Varattu, ei käytössä
224.0.0.1	Kaikki IP-koneet käsittävä pysyvä (permanent) multicast-ryhmä

Taulukosta 1, selviää lähiverkossa käytettävät IP-osoitteet ja lähiverkossa käytettävien IP-osoitteiden käyttötarkoitus. Opinnäytetyötä varten valittiin IP-osoite osoiteavaruudesta 192.168.0.0 - 192.168.255.255. Lähiverkkoa varten tarvittiin kolme IP-osoitetta osoiteavaruudesta 192.168.0.0 - 192.168.255.255. Valitut IP-osoitteet olivat 192.168.1.8, 192,168.1.9 ja 192.168.1.10. IP-osoitteen toiseksi viimeinen numero merkitsee käytettävää lähiverkkoa. IP-osoitteen viimeinen numero tarkoittaa lähiverkossa olevan tietokoneen numeroa.

Esimerkiksi IP-osoite 192.168.1.8 kuuluu lähiverkkoon 1 ja sen tietokoneen verkkokortille yksilöity numero on 8. IP-osoite 192.168.2.8 kuuluu eri lähiverkkoon kuin IP-osoite 192.168.1.8, ja ne eivät tunne suoraan toisiaan, koska ne eivät ole samassa lähiverkossa. IP-osoite 192.168.1.8 ja IP-osoite 192.168.1.9 kuuluvat samaan lähiverkkoon, ja näin ollen

ne tuntevat toisensa lähiverkossa.

Tietokoneiden sekoaminen kesken opinnäytetyön aiheutti monenlaista häiriötä. Verkkokortin numerointi Ubuntussa aiheutti hämmennystä. Ubuntun asentamisen jälkeen verkkokortin numerointi toimi moitteettomasti. Ensimmäinen verkkokortti oli eth0, ja toinen verkkokortti eth1. Kun tuli tilanne, että asennukseen käytetty tietokone ei ollut enää käyttökelpoinen, tuli esiin verkkokortin numerointiin liittyvä ongelma. Asetettiin toimivampaan tietokoneeseen kaksi verkkokorttia. Tietokoneen vaihtamisen yhteydessä verkkokortin numerointi jatkui aivan kuin tietokoneeseen olisi liitetty kaksi uutta verkkokorttia. Selvitettiin Internetin lähteiden avulla verkkokortin MAC-osoitteen sijainti. Ubuntu kirjasi MAC-osoitteen perusteella verkkokortin numeroinnin tekstitiedostossa 70-persistent-net.rules. Tekstitiedostoa 70-persistent-net.rules, päästiin muokkaamaan nano-editorilla, antamalla käskyn:

sudo nano /etc/udev/rules.d/70-persistent-net.rules (Dell, 2010.)

Tekstitiedosto 70-persistent-net.rules, sisälsi useita alla kuvatunlaisia tekstirivejä:

 # PCI device 0x1317:0x0985 (tulip)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?",*
ATTR{address}=="00:30:05:68:06:0c", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth", NAME="eth0*

Kohtaan *ATTR{address}=="00:30:05:68:06:0c"*, vaihdettiin senhetkisessä tietokoneessa oleva verkkokortin MAC-osoite.

Silta (bridge) on lähiverkon aktiivisena oleva komponentti, joka suodattaa ja asettaa lähitseen kulkevan liikenteen puskuriin (Jaakonhuhta 2005, 360). Silta (bridge) liittää yhteen kaksi samanlaista verkkoa tai verkonosaa (Jaakonhuhta 2005, 65).

Sillat välittävät kehyksiä perustuen MAC-osoitteisiin. Sillat toimivat **varastoi ja välitä**-periaatteella. Silta ottaa koko kehyksen itselleen ennen välittämistä ja laskee tarkistussumman kehyksen eheyden varmistamiseksi. (Allen 2002, 142.)

Siltaa käytettiin tietokoneen Repe verkkokorttien yhdistämiseen. Silta yhdisti tietokoneen Repe verkkokortit yhtenäiseksi verkkokortiksi. Tietokoneen Jope verkkokortista johti ristikytketty verkkokaapeli tietokoneen Repe ylempään verkkokorttiin. Tietokoneen Topi verkkokortista johti ristikytketty verkkokaapeli tietokoneen Repe alempaan verkkokorttiin. Kun tietokoneen Jope verkkokortti otti yhteyttä tietokoneen Topi verkkokorttiin, lähetti tietokone Jope tiedot tietokoneen Repe ylemmälle verkkokortille. Tietokoneen Repe verkkoasetuksissa oli määritetty, että tietokoneen Repe ylemmälle verkkokortille lähetetyt tiedot välitetään suoraan tietokoneen Repe alemmalle verkkokortille. Samoin toimi myös tietokoneen Repe alempi verkkokortti. Tietokoneen Repe alempi verkkokortti lähetti tietokoneen Topi lähettämät tiedot tietokoneen Repe ylemmälle verkkokortille. Tällä tavalla tietokone Repe toimi tietokoneen Jope ja tietokoneen Topi välikätenä. Tietokone Repe välitti verkkokorteille saapuneet tiedot eteenpäin verkkokorteissa kiinni oleville tietokoneille. Kun tietokone Repe toimi välikätenä, niin välikätenä oleminen mahdollisti välitettävien tietojen tutkimisen verkkoliikenneanalysaattorin avulla.

4 SAMBA

Sambaa voi käyttää tulostimien ja tiedostojen jakamiseen lähiverkossa ja tarvittaessa myös tiedostojen jakamiseen Internetissä. Samballa voi jakaa myös tietokoneen CD-ROM aseman toisen lähiverkossa olevan tietokoneen käyttöön.

Samban asentaminen aloitettiin terminaalissa käskyllä:
*topi@topi:~$ sudo apt-get install samba (*Youtube. 2010*).*

Kun Samba asentui, siirryttiin Linuxin juureen käskyllä:
*topi@topi:~$ cd / (*Youtube. 2010*).*

Luotiin uusi kansio nimeltään jako, käskyllä:
*topi@topi:~$ sudo mkdir jako (*Youtube. 2010*).*

Vaihdettiin kansion nimeltään jako, ryhmää ja pääkäyttäjää käskyllä:
*topi@topi:~$ sudo chmod topi:topi jako (*Youtube. 2010*).*

Luotiin käyttäjälle topi Samba-salasana käskyllä:
*topi@topi:~$ sudo smbpasswd -a topi (*Youtube. 2010*).*

Salasana pyydettiin antamaan kahteen kertaan, jotta käyttäjä varmistui antamastaan salasanasta. Salasanan asettamisen jälkeen oli vuorossa Samban asetusten säätäminen.

4.1 Samban asetukset

Ennen kuin alettiin tehdä Samban asetuksiin muutoksia, otettiin alkuperäisestä tekstitiedostosta *smb.conf* varmuuskopio. Varmuuskopio tekstitiedostosta *smb.conf* saatiin käskyllä:

topi@topi:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.backup
(Ubuntu Suomi, 2010.)

Mikäli Samban asetuksissa olisi tullut joku huomaamaton virhe, olisi voitu palata alkuperäiseen tekstitiedostoon *smb.conf*, antamalla komennon:

topi@topi:~$ sudo cp /etc/samba/smb.conf.backup /etc/samba/smb.conf

Tekstitiedoston *smb.conf* varmuuskopioinnin jälkeen, siirryttiin muokkaamaan tekstitiedostoa *smb.conf*. Käytettiin tekstitiedoston *smb.conf* muokkaamisessa nano tekstieditoria. Tekstitiedoston *smb.conf* muokkaamista varten annettiin käsky:

topi@topi:~$ sudo nano /etc/samba/smb.conf

Kun tekstitiedostoon *smb.conf* tehtiin kaikki tarpeelliset muutokset, tekstitiedosto *smb.conf* sisälsi tekstin: (LIITE 5)

Tekstitiedostoon *smb.conf* tehtiin seuraavanlaisia muutoksia:

1. Poistettiin *security = user* edestä puolipiste.
2. Vaihdettiin *interfaces* kohtaan verkkokortille annettu IP-osoite 192.168.1.9.
Tehdyn muutoksen jälkeen *interfaces* kohta näytti seuraavalta:

interfaces = 192.168.1.9/24 eth0

3. Haluttiin saada CD-ROM asema käyttöön toisessa tietokoneessa, niin otettiin valmiiksi asetetusta cdrom jaosta puolipiste pois asetusten edestä ja asetettiin käyttäjäksi topi.
CD-ROM asetukset näyttivät seuraavilta:

[cdrom]
comment = Samba server's CD-ROM
read only = yes
locking = no
path = /cdrom
guest ok = yes
valid users = topi

4. Lopuksi tehtiin levytilan jakamista varten asetukset tekstitiedoston *smb.conf* loppuun ja kirjoitetut tekstit näyttivät seuraavalta:

[Kulmakatu]
comment = Kulmakatu - jako
path = /jako
browseable = yes
guest ok = yes
read only = no
writeable = yes

Tekstitiedosto *smb.conf* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan.

Samban asetukset tekstitiedostosta *smb.*conf tulivat voimaan, kun Samba käynnistettiin uudelleen käskyllä:

topi@topi:~$ sudo /etc/init.d/samba restart (Ubuntu Suomi, 2010.)

4.2 Samban käyttöönotto

Kun Samba on käynnissä jossakin lähiverkossa olevalla tietokoneella, voi toinen lähiverkossa oleva tietokone ottaa yhteyttä Samban tarjoamiin jakoihin. Ubuntussa yhteyden ottaminen Samban jakoihin tapahtui seuraavalla tavalla:

Valittiin tietokoneessa jope, Ubuntun Sijainnit-valikko. Ubuntun Sijainnit-valikon alta löytyi ”Yhdistä palvelimeen…”-valikko.

Palvelutyypiksi valittiin ”Windows-jako”-valinta. Palvelin tietokoneen topi IP-osoite oli opinnäytetyössä 192.168.1.9, joten laitettiin IP-osoite 192.168.1.9 ”Palvelin” kohtaan. Kun haluttiin ottaa yhteyttä jaettuun levytilaan, kirjoitettiin ”jako” kohtaan Samban asetustiedostossa *smb.conf* jaolle annettu nimi Kulmakatu.

Jos olisi haluttu ottaa CD-ROM asemaan yhteyttä, **jako**-kohtaan olisi pitänyt kirjoittaa **cdrom**.

Käyttäjätunnus kohtaan laitettiin käyttäjänimi Topi. Valintojen jälkeen painettiin ”Yhdistä”-nappia. Kun painettiin ”Yhdistä”-nappia, niin täytyi antaa käyttäjän Topi Samba sala-

sana. Pyydettiin antamaan toimialue, joka tarkoitti työryhmää WORKGROUP. Työryhmällä on merkitystä vain Linux-käyttöjärjestelmän ja Windows-käyttöjärjestelmän välillä. Opinnäytetyössä käytettiin vain Linux-käyttöjärjestelmää. Toimialue kohdassa luki valmiiksi WORKGROUP, joten muutoksia ei tarvinut tehdä.

Salasanan antamisen jälkeen painettiin ”Yhdistä”-nappia, jonka seurauksena päästiin käsiksi tietokoneessa topi oleviin Kulmakatu jaolla jaettuihin tiedostoihin. Tietokoneelta jope pystyttiin tallentamaan, lisäämään, poistamaan ja muokkaamaan tietokoneella topi jaettuja tiedostoja Kulmakatu-jaossa määritellyssä kansiossa.

5 VERKKOLIIKENNEANALYSAATTORI

Verkkoliikenneanalysaattori on verkkoliikenteen seuraamiseen tarkoitettu ohjelmisto. Verkkoliikenneanalysaattori voi olla myös teknisesti rakennettu laite, jolla tutkitaan verkkoliikennettä. Tähän opinnäytetyöhön valittiin Wireshark-niminen verkkoliikenneanalysaattoriohjelmisto verkkoliikenteen kaappaamista varten. Koska verkkoliikenteestä haluttiin saada tietoon näkymä verkkoliikenteestä graafisena, valittiin verkkoliikennettä analysoivaksi ohjelmaksi graafista kuvaajaa verkkoliikenteestä tuottava Ntop niminen verkkoliikenteen seurantaohjelmisto.

Wireshark verkkoliikenneanalysaattoriohjelmistolla voidaan tutkia myös verkossa ilmeneviä mahdollisia virheitä protokollien kautta.

5.1 Wireshark

Wireshark on verkkoliikenneanalysaattori, jonka avulla voi tutkia verkkoliikenteessä olevia protokollia. Wireshark on avuksi verkkoliikenteen vikatilanteiden selvittämisessä.

Linuxissa Wiresharkia käytetään sillä tavalla, että verkkoliikenne kaapataan ensin dumpcap ohjelmalla, jonka jälkeen avataan dumpcapin synnyttämä kaappaustiedosto Wiresharkilla. Wireshark analysoi tiedoston sisältämän kopion verkkoliikenteestä. Verkkoliikenteen kaappaaminen täytyy Linuxin turvallisuuskäytännön takia tehdä aina root-käyttäjänä, jonka takia dumpcap tulee suorittaa root-oikeuksilla. Wiresharkin käyttämistä root-oikeuksilla ei suositella, koska kaapatun liikenteen mahdollisesti hyökkäystarkoituksessa laadittu verkkoliikenne voi Wiresharkin haavoittuvuuden kautta päästää hyökkääjän järjestelmään. Dumpcap on Wiresharkia pienempi ohjelma ja tämän takia turvallisempi. (Linux, 2010.)

Wiresharkin asentaminen onnistui helpoiten Ubuntun ”ohjelmien haku”-toiminnon kautta. Kirjoitettiin hakukenttään Wireshark, ja valittiin Wireshark asennettavaksi. Wireshark haettiin Internetistä Wiresharkin omista Internet-lähteistä, ja lopuksi Wireshark asentui Ubuntuun.

Wireshark käynnistyi ohjelmana aivan ongelmitta, mutta saatiin huomata, että ei voitu kaapata mitään verkkoliikennettä. Aluksi käynnistettiin Wireshark root-oikeuksilla, jolloin

saatiin näkymään verkkoliikenteen kaappaamisessa tarvittavia rajapintoja. Wiresharkin käyttöohjeen tutkimisen jälkeen, vaihdettiin ohjelman suorittaminen turvallisempaan vaihtoehtoon.

Wiresharkin turvallisempaa käyttöä varten asennettiin libcap2-bin, jonka kautta rajapinnat asetettiin kaappaamaan liikennettä aivan kuten root, mutta turvallisemmin.

Libcap2-bin saatiin asennettua terminaalin kautta, käskyllä:

repe@repe:~$ sudo apt-get install libcap2-bin (Wireshark. 2010. Capture Privileged.)

Kun libcap2-bin saatiin asennettua, niin täytyi asettaa dumpcap toimintaan käskyllä:

repe@repe:~$ sudo setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/bin/dumpcap (Wireshark. 2010. Capture Privileged.)

Dumpcapin toimintaan asettamisen jälkeen, Wiresharkia pystyi käyttämään samalla tavalla, kuin Wireshark olisi käynnistetty root-oikeuksilla.

Wireshark kaatui käytön yhteydessä sen takia, koska tietokoneissa, jotka olivat käytössä, oli vanhat kovalevyt, joiden nopeus ei pysynyt kaapattavien tietojen mukana.

FLV mediasoittimen suoratoiston yhteydessä Wiresharkilla kaapattu tieto ei aiheuttanut Wiresharkin kaatumista. FTP:llä tiedoston lähettämisen yhteydessä verkkoliikenteen kaappaaminen sujui myös ongelmitta.

Wireshark kaatui sellaisessa tilanteessa, kun pitkään kaapattiin jotakin suurta tiedostoa, kuten esimerkiksi Samban avulla toisen tietokoneen CD-ROM asemasta videon toistaminen.

Wiresharkin kehittäjille ei tehty sen kaatumisesta raporttia, koska kaatuminen johtui aivan luonnollisista syistä.

Jos olisi haluttu tehdä raportti Wiresharkin kehittäjille, niin se olisi tapahtunut seuraavalla tavalla. Aluksi olisi annettu terminaalissa käsky:

repe@repe:~$ gdb 'whereis wireshark | cut -f2 -d: | cut -d' ' -f2' core >& bt.txt backtrace
(Wireshark, 2010, ChIntroHelp.)

Käsky tuottaa gdb debuggerilla bt.txt tekstitiedosto, joka lähetetään raportin mukana Wiresharkin kehittäjien postituslistalle wireshark-dev@wireshark.org.
(Wireshark, 2010, ChIntroHelp.)

Ennen raportin lähettämistä, kuuluu Wireshark päivittää uusimpaan versioon. Wiresharkilla kaapattu tieto ei saa sisältää henkilökohtaisia tietoja, kuten salasanoja, mikäli on tarpeen lähettää kaapattua tietoa raportin mukana. Mihinkään postituslistalle ei saa lähettää yli 100 kB tiedostoja, koska lähettäminen kuormittaa turhaan verkkoliikennettä.
(Wireshark, 2010, ChIntroHelp.)

Kun raportoi ongelmasta wiresharkille, auttaa ongelman selvittämisessä seuraavat tiedot:

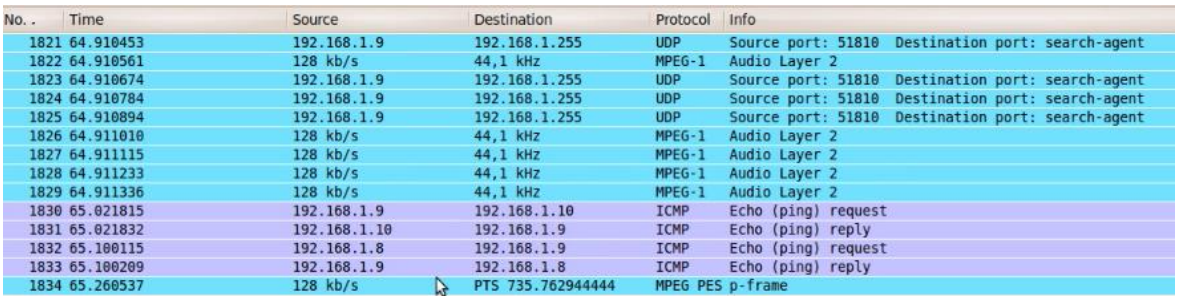
1. Wiresharkin versionumero:

repe@repe:~$ wireshark -v (Wireshark, 2010, ChIntroHelp.)

2. Käyttöjärjestelmän tiedot:

repe@repe:~$ cat /proc/version (Wireshark, 2010, ChIntroHelp.)

Wiresharkin käynnistymisen jälkeen on aika alkaa käyttämään Wiresharkia. Wiresharkin valikoista löytyy ”Interfaces…”-valinta. ”Interfaces…”-valinnan avulla valitaan rajapinta, jota halutaan tarkkailla verkkoliikenteestä. Sopivan rajapinnan löydyttyä, aloitetaan verkkoliikenteen kaappaaminen ”Start”-painikkeen kautta.



No. .	Time	Source	Destination	Protocol	Info
1821	64.910453	192.168.1.9	192.168.1.255	UDP	Source port: 51810 Destination port: search-agent
1822	64.910561	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
1823	64.910674	192.168.1.9	192.168.1.255	UDP	Source port: 51810 Destination port: search-agent
1824	64.910784	192.168.1.9	192.168.1.255	UDP	Source port: 51810 Destination port: search-agent
1825	64.910894	192.168.1.9	192.168.1.255	UDP	Source port: 51810 Destination port: search-agent
1826	64.911010	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
1827	64.911115	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
1828	64.911233	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
1829	64.911336	128 kb/s	44,1 kHz	MPEG-1	Audio Layer 2
1830	65.021815	192.168.1.9	192.168.1.10	ICMP	Echo (ping) request
1831	65.021832	192.168.1.10	192.168.1.9	ICMP	Echo (ping) reply
1832	65.100115	192.168.1.8	192.168.1.9	ICMP	Echo (ping) request
1833	65.100209	192.168.1.9	192.168.1.8	ICMP	Echo (ping) reply
1834	65.260537	128 kb/s	PTS 735.762944444	MPEG PES	p-frame

KUVIO 4

Kuviossa 4, on Wiresharkilla kaapattua verkkoliikennettä. Verkkoliikennettä voi verkkoliikenteen kaappauksen jälkeen tarpeen mukaan analysoida.

5.2 Ntop

Ntop on verkkoliikenteen seuraamiseen tarkoitettu ohjelma. Ntop kerää päällä ollessaan automaattisesti tietoa verkkoliikenteestä. Ntop luo verkkoliikenteestä graafisia kuvaajia. Opinnäytetyössä yritettiin saada Ntop tulostamaan Wiresharkin kaappaamat tiedot graafisena kuvaajana. Onnistuttiin saamaan Wiresharkin kaappaamista tiedoista piirakka graafeja. Päädyttiin tulokseen, että ainakin tämän opinnäytetyön puitteissa tyydytään ottamaan tiedot verkkoliikenteestä talteen Wiresharkilla ja Ntopilla muodostetaan verkkoliikenteestä juuri sillä hetkellä muodostuvat graafiset kuvaajat.

Ntopin asentamisen aloitettiin antamalla terminaalissa käskyn:

repe@repe:~$ sudo apt-get install ntop -y (Ubuntu, Ntop, 2010.)

Ntopin asennuksen aikana tuli kysymys, että halutaanko käyttää levytilaa ohjelman asentamiseen. Kysymykseen vastattiin myöntävästi valitsemalla y-kirjaimen ja painamalla enter-näppäintä.

Kun Ntop saatiin asennettua, niin Ntopille täytyi asettaa salasana. Salasanan asettaminen Ntopille tapahtui terminaalissa käskyllä:

repe@repe:~$ sudo ntop --set-admin-password (Ntop, 2010.)

Ntopin salasanan asettamisen jälkeen oli mahdollista tarkastella ohjelmaa toiminnassa. Käytettiin Firefox-selainta Ntop ohjelman tutkimiseen.

Firefox-selaimen osoitinriville kirjoitettiin:

192.168.1.10:3000

Jos Ntop pyysi jossakin tilanteessa käyttäjätunnusta ja salasanaa, niin käyttäjätunnus oli root ja salasana oli asennuksen jälkeen annettu salasana Ntopille.

Oletuksena Ntop tarjosi tarkkailtavaksi verkkoliikenteen rajapinnaksi eth0 verkkosovitinta. Haluttiin, että voitaisiin tarkkailla eth0 ja eth1verkkosovittimien verkkoliikennettä. Jäi laittamatta muistiin, minkä virheilmoituksen kautta löydettiin ratkaisu verkkoliikenteen rajapinnan vaihtamiseen Ntopissa. Virheilmoituksen kautta selvitettiin, että täytyisi vaihtaa tekstitiedoston init.cfg tietoja paikassa /var/lib/ntop/init.cfg. Tekstitiedostossa init.cfg oli oletuksena seurattavaa liikennettä varten verkkosovitin eth0. Verkkosovittimen eth0 tilalle täytyi kirjoittaa tietokoneelle repe luodun sillan nimi. Tietokoneelle repe luodulle sillalle oli annettu nimeksi silta.

Teksti tiedoston init.cfg muokkaaminen onnistui, kun annettiin terminaalissa käsky:

repe@repe:~$ sudo nano /var/lib/ntop/init.cfg

Tekstitiedosto init.cfg sisälsi aluksi tekstin:

USER=”ntop”
INTERFACES=”eth0”

Tekstitiedostoa init.cfg muokattiin, vaihtamalla nimi silta, nimen eth0 paikalle. Painettiin Ctrl+o tekstitiedoston init.cfg tallentamista varten. Tekstitiedoston init.cfg tallentamisen jälkeen painettiin Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaaliin. Tekstitiedoston init.cfg muokkauksen jälkeen tekstitiedosto init.cfg sisältö oli seuraavanlainen:

USER=”ntop”
INTERFACES=”silta”

Uudet asetukset astuivat voimaan kun Ntop uudelleen käynnistettiin käskyllä:

repe@repe:~$ sudo /etc/init.d/ntop restart

Firefox-selaimen osoiteriville annettiin tietokoneen repe IP-osoite 192.168.1.10:3000, jonka seurauksena Ntop ohjelma käynnistyi selaimessa näkyväksi ohjelmaksi.

Aluksi tehtiin Ntop ohjelman kanssa virheitä, jonka seurauksena Ntop ei näyttänyt toimivan ollenkaan. Ntop ohjelman asennuksen purkaminen onnistui käskyllä:

repe@repe:~$ sudo apt-get purge ntop.

Kun Ntop ohjelman init.cfg tekstitiedostoa oli muokattu, Ntop käynnistettiin oletuksena käskyllä:

repe@repe:~$ /usr/sbin/ntop -d -L -u ntop -P /var/lib/ntop -access-log-file -i silta -p /etc/ntop/protocol.list -O /var/log/ntop (Ntop, 2010.)

Haluttiin saada Wireshark ohjelmalla kaapattu verkkoliikenne tulostumaan Ntopissa. Tutkittiin Ntop man-sivuja. Ntopin man-sivut saatiin näkymään terminaalissa käskyllä:

repe@repe:~$man ntop

Man-sivujen tutkimisen yhteydessä selvisi uusi terminaalissa käytettävä käsky, jonka tarkoitus oli saada muulla kuin Ntopilla otettu tieto tulostumaan Ntopin graafeissa. Annettiin man-sivuilta selvitetty käsky terminaalissa:

sudo ntop -u root -m 192.168.1.0/24 -f /home/repe/Asiakirjat/udp_videostream_vlc
(Ntop, 2010.)

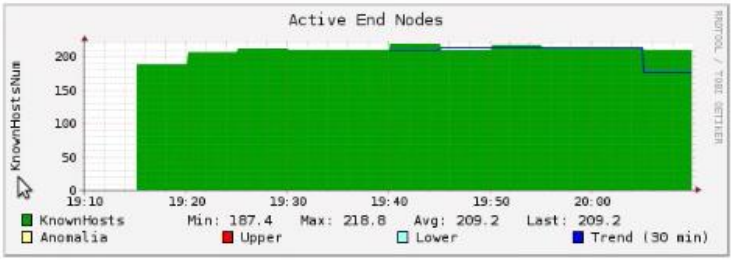
Ntopin man-sivuista selvitetyllä käskyllä onnistuttiin saamaan Wiresharkilla kaapattu tiedosto toimimaan Ntopin graafeissa piirakka mallina. Wiresharkilla kaapattua tiedostoa ei saatu tulostumaan Ntopissa edellä mainitulla käskyllä täydellisesti. Wiresharkilla kaapatusta tiedoista ei saatu verkkoliikennettä tulostumaan Ntopin aikajaksollisissa graafeissa ollenkaan.

Yritettiin käyttää Ntopin oletuksena käynnistyksessä käyttämän käskyn ja Ntop man-sivuilta löydetyn käskyn yhdistelmä käskyä:

repe@repe:~$ sudo /usr/sbin/ntop -a -d -L –u ntop –m 192.168.1.10/24 -P /var/lib/ntop -i silta –f /home/repe/Asiakirjat/udp_videostream_vlc -p /etc/ntop/protocol.list -O /var/log/ntop (Ntop, 2010.)

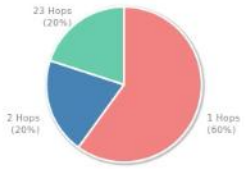
Yhdistelmä käsky ei antanut yhtään parempaa tulosta kuin Ntopin man-sivuilta löydetty käsky.

Ntopin graafisten kuvaajien kautta on helpompaa tutustua verkkoliikenteessä tapahtuvaan liikehdintään. Ntopin graafisissa kuvaajissa on käytetty apuna prosentuaalisia tuloksia ja aikajaksollisia tuloksia. Prosentuaalinen tulos ilmaistaan yleensä piirakka graafina tai pylväs graafina. Aikajaksollinen tulos esitetään viivasuorana esityksenä. Viivasuoraa esitystä aikajaksollisessa tuloksessa korostetaan joissakin tapauksissa käyttämällä viivan sisälle jäävässä alueessa tuloksen esityksessä käytetyn viivan väriä. Ntop ottaa talteen verkkoliikenteessä käytetyt portit. Verkkoliikenteestä kirjattujen porttien kautta saa selvitettyä, mitä portteja kukakin verkossa oleva tietokone on käyttänyt ollessaan yhteydessä Ntopilla varustettuun tietokoneeseen. Portit, joita Ntopilla varustettu tietokone on käyttänyt kommunikoidessaan ulkomaailmaan, löytyvät myös Ntopin tiedoista.



KUVIO 5

Kuviossa 5, näkyy verkkoliikenteessä olevien tunnettujen isäntien eli hosts määrää kullakin ajanjaksolla.

Remote Hosts Distance			
Network Load	**Actual**	749.3 bit/s	1.1 Pkt/s
	Last Minute	1.1 Kbit/s	1.7 Pkt/s
	Last 5 Minutes	1.8 Kbit/s	2.1 Pkt/s
	Peak	4.0 Mbit/s	567.3 Pkt/s
	Average	1.9 Mbit/s	277.8 Pkt/s
Historical Data	[ ]		

KUVIO 6

Kuviossa 6, on malli piirakkakaaviona esitetystä verkkoliikenteen tuloksesta.

TCP/UDP Traffic Port Distribution:
Last Minute View

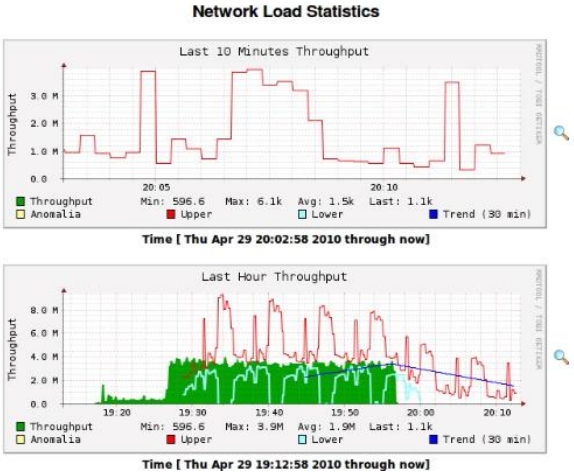
TCP/UDP Port		Total	Sent	Rcvd
netbios-dgm	138	486	243	243
8546	8546	320	0	320
8545	8545	320	320	0
1346	1346	222	222	0
1345	1345	222	0	222
1039	1039	121	121	0
snmp	161	121	0	121
1947	1947	82	0	82
1038	1038	82	82	0

Notes:

- sum(total traffic per port) = 2*(total IP traffic)
  because the traffic per port is counted twice (sent and received)
- This report includes broadcast packets

KUVIO 7

Kuviossa 7, esiintyy verkkoliikenteessä käytettyjen porttien numerot. Portin numerosta johtaa hyperlinkki tietoon, josta selviää porttia käyttäneen tietokoneen nimi tai tietokoneen IP-osoite.



KUVIO 8

Kuviossa 8, Ntop on mitannut verkkoliikenteen tiedostojen lataamiseen liittyviä tietoja, ja ilmaissut tiedot aikajaksollisessa graafissa.

6 VERKKOLIIKENTEESSÄ ILMENNEET PROTOKOLLAT

6.1 FTP

FTP on tarkoitettu tiedostojen siirtämiseen kahden tietokoneen välillä. FTP käyttää TCP-protokollaa. FTP on hieman erilainen muihin protokolliin verrattuna, koska se käyttää kahta porttia yhteyden muodostamiseen. TCP-porttia 21, käytetään yhteyden muodostamiseen. TCP-porttia 20 tai jotakin muuta suurempaa satunnaista porttia käytetään datan siirtämisen yhteydessä. (Reunamo, 2010.)

Wiresharkilla kaapattu tieto ftp:stä lyhyellä selityksellä:

No. Time Source Destination Protocol Info
1 0.000000 FujitsuS_85:03:21 Broadcast ARP Who has 192.168.1.9? Tell 192.168.1.8

Frame 1 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: FujitsuS_85:03:21 (00:30:05:85:03:21), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

Frame 1: Kun otetaan yhteyttä FTP-palvelimeen IP-osoitteeseen 192.168.1.9, lähetetään aluksi ARP-protokollalla tunnistautumis kysely sille yleislähetys osoitteella.

No. Time Source Destination Protocol Info
2 0.000087 FujitsuS_85:01:c6 FujitsuS_85:03:21 ARP 192.168.1.9 is at 00:30:05:85:01:c6

Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Address Resolution Protocol (reply)

Frame 2: Kyselyn tuloksena saadaan selville verkkokortin MAC-osoite, jonka kanssa ollaan yhteydessä. Tässä kohdin verkkokortin MAC-osoitteet keskustelevat keskenään.

No. Time Source Destination Protocol Info
3 0.000144 192.168.1.8 192.168.1.9 TCP 57506 > ftp [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=2016956 TSER=0 WS=6

Frame 3 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: FujitsuS_85:03:21 (00:30:05:85:03:21), Dst: FujitsuS_85:01:c6 (00:30:05:85:01:c6)
Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 192.168.1.9 (192.168.1.9)
Transmission Control Protocol, Src Port: 57506 (57506), Dst Port: ftp (21), Seq: 0, Len: 0

Frame 3: Otetaan portin 57506 kautta yhteyttä ftp porttiin 21.

No. Time Source Destination Protocol Info
4 0.000218 192.168.1.9 192.168.1.8 TCP ftp > 57506 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2521662 TSER=2016956 WS=6

Frame 4 (74 bytes on wire, 74 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 57506 (57506), Seq: 0, Ack: 1, Len: 0

Frame 4: Ilmoitetaan portin 21 olevan valmis vastaanottamista varten.

Tietokoneet lähettävät keskenään paketteja aina frame 12:een asti.

No. Time Source Destination Protocol Info
12 0.149083 192.168.1.9 192.168.1.8 FTP Response: 331 User topi OK. Password required

Frame 12 (103 bytes on wire, 103 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: 57506 (57506), Seq: 321, Ack: 12, Len: 37
File Transfer Protocol (FTP)

Frame 12: Pyydetään antamaan käyttäjälle topi määritettyä salasanaa.

No. Time Source Destination Protocol Info
13 0.151871 192.168.1.8 192.168.1.9 FTP Request: PASS 1234567890

Frame 13 (83 bytes on wire, 83 bytes captured)
Ethernet II, Src: FujitsuS_85:03:21 (00:30:05:85:03:21), Dst: FujitsuS_85:01:c6 (00:30:05:85:01:c6)
Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 192.168.1.9 (192.168.1.9)
Transmission Control Protocol, Src Port: 57506 (57506), Dst Port: ftp (21), Seq: 12, Ack: 358, Len: 17
File Transfer Protocol (FTP)

Frame 13: Kun salasana annetaan, niin se voidaan nähdä selväkielisenä. Annettu salasana on 1234567890.

6.2 ICMP

ICMP-protokolla on käytössä verkon laitteiden hallintaviestien välityksessä. ICMP-protokollan tuottamien aikaleimojen avulla pystytään tutkimaan esimerkiksi pakettien kulkuaikoja verkossa, mutta yleisin käyttötarkoitus sille mahtaa olla pakettien takaisinkaiutus verkkoa testattaessa. (Hakala & Vainio 2002, 249.)

Kun haluttiin varmistaa lähiverkossa olevien tietokoneiden paikallaolo, annettiin terminaalissa käsky *ping*. *Ping*-käsky lähti hakemaan pyydetyn verkkokortin IP-osoitetta tulostaen seuraavaa:

jope@jope:~$ ping 192.168.1.8
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.
64 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=0.031 ms
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from 192.168.1.8: icmp_seq=4 ttl=64 time=0.027 ms
^C
--- 192.168.1.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.025/0.027/0.031/0.002 ms
jope@jope:~$ ping 192.168.1.9
PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.
64 bytes from 192.168.1.9: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 192.168.1.9: icmp_seq=2 ttl=64 time=0.169 ms
64 bytes from 192.168.1.9: icmp_seq=3 ttl=64 time=0.181 ms
64 bytes from 192.168.1.9: icmp_seq=4 ttl=64 time=0.179 ms
^C
--- 192.168.1.9 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.169/0.177/0.181/0.004 ms
jope@jope:~$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=1 ttl=64 time=2.68 ms
64 bytes from 192.168.1.10: icmp_seq=2 ttl=64 time=0.109 ms
64 bytes from 192.168.1.10: icmp_seq=3 ttl=64 time=0.105 ms
64 bytes from 192.168.1.10: icmp_seq=4 ttl=64 time=0.111 ms
^C
--- 192.168.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.105/0.753/2.687/1.116 ms
jope@jope:~$

Ping-käskyn antaman tulosteen perusteella tiedetään lähiverkon verkkokorttien toimivan verkkokorttien IP-osoitteiden 192.168.1.8, 192.168.1.9 ja 192.168.1.10 välillä. Merkintä *^C* tarkoittaa ping-käskyn keskeytystä Ctrl+c näppäinyhdistelmän tuloksena.

Ping-ohjelmaa voidaan kutsua TCP/IP-verkkojen vikaselvityksen yleistyökaluksi. Sen avulla tehdään ensimmäisenä alustava vianhaku (Hakala & Vainio 2002, 279).

Ping-käsky tuottaa verkkoliikennettä ICMP-protokollalla ja ARP-protokollalla. Kun esimerkiksi tietokone jope haluaa lähettää ping-kyselyn tietokoneelle topi, näkyy terminaalissa seuraavaa:

jope@jope:~$ ping 192.168.1.9
PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.
64 bytes from 192.168.1.9: icmp_seq=1 ttl=64 time=0.179 ms

Edellä olevasta selviää, että tietokone jope saa tietokoneelta topi, vastauksen 0.179 millisekunnissa.

Verkkoliikenneanalysaattorilla katsottuna saatiin irti alla olevaa tietoa samaisesta tapahtumasta:

No. Time Source Destination Protocol Info
1 0.000000 FujitsuS_68:06:0c Broadcast ARP Who has 192.168.1.8? Tell 192.168.1.10

Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: FujitsuS_68:06:0c (00:30:05:68:06:0c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No. Time Source Destination Protocol Info
2 0.000090 FujitsuS_85:03:21 FujitsuS_68:06:0c ARP 192.168.1.8 is at 00:30:05:85:03:21

Frame 1: Lähetetään ARP-kysely, jossa halutaan selvittää lähiverkossa IP-osoitteella 192.168.1.8 olevan verkkokortin MAC-osoite. ARP-kyselyn lähettäjä on IP-osoite 192.168.1.10. IP-osoitteen 192.168.1.10 oma MAC-osoite on 00:30:05:68:06:0c. ARP-kyselyn avulla selvitetään, että IP-osoitteen 192.168.1.8 MAC-osoite on 00:30:05:85:03.

Frame 2 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: FujitsuS_85:03:21 (00:30:05:85:03:21), Dst: FujitsuS_68:06:0c (00:30:05:68:06:0c)
Address Resolution Protocol (reply)

No. Time Source Destination Protocol Info
3 0.000112 192.168.1.10 192.168.1.8 ICMP Echo (ping) request

Frame 2: Kun IP-osoite 192.168.1.10 on tutustunut IP-osoitteen 192.168.1.8 MAC-osoitteeseen, voivat ne alkaa kommunikoimaan keskenään. IP-osoite 192.168.1.10 kyselee IP-osoitteelta 192.168.1.8, onko IP-osoite 192.168.1.8 ”hereillä”.

Frame 3 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: FujitsuS_68:06:0c (00:30:05:68:06:0c), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.1.8 (192.168.1.8)
Internet Control Message Protocol

No. Time Source Destination Protocol Info
4 0.000184 192.168.1.8 192.168.1.10 ICMP Echo (ping) reply

Frame 3: IP-osoite 192.168.1.8 vastaa IP-osoitteelle 192.168.1.10 olevansa hereillä.

6.3 UDP

Sovellukset, jotka eivät vaadi luotettavuutta, voivat käyttää protokollana kuljetustason UDP-protokollaa. UDP-protokollaa käytetään sovelluksissa, jotka lähettävät jatkuvasti mutta epäsäännöllisin välein lyhyitä viestejä verkkoon. (Hakala & Vainio 2002, 259.)

UDP on yhteydetön protokolla, ja se ei sisällä yhteyden käsitettä ”perustettu” (established-tila, yhteys päällä). Tämän takia ei ole mitään täysin turvallista tapaa sallia UDP ”paluu”-paketteja normaalin pakettien suodatuksen kautta – paketteja ei voida varmasti yhdistämään lähteneeseen pakettiin. UDP:n vähemmästä turvallisesta huolimatta useat tärkeät palvelut ovat riippuvaisia UDP-paketeista. Toimialueen nimipalvelun (UDP portti 53) täytyy olla käytössä, koska sisäverkon isäntäkoneiden pitää toimia oikein. (Allen 2002, 84.)

0	15	31 bitti
Lähdeportti (source port)	Kohdeportti (destination port)	
UDP-viestin pituus kokonaisuudessaan (otsake + data)	Varmistussumma	
DATA		

TAULUKKO 2, UDP-datagrammin toiminta. (mukaillen Hakala & Vainio 2002, 259.)

Taulukossa 2, esitellään UDP-datagrammin rakenne. UDP:tä tarvitaan monesti yksistään vain socketin muodostuksessa, jossa se lisää IP:n välittämiin tietoihin porttinumeron. Joissakin tapauksissa lähde- tai kohdeporttia ei määritellä ollenkaan. Varmistussumma voidaan myös jättää laskematta, jonka seurauksena kenttä täytetään nollilla. Databittien määrä on oltava joko 16 tai 32:lla jaollinen täytemerkkien lisäyksen jälkeen. (Hakala & Vainio 2002, 259.)

0	15	31 bitti
Lähdeportti (source port)		
Kohdeportti (destination port)		
nolla	Protokollakoodi	UDP-datagrammin pituus

TAULUKKO 3, IP-datagrammin UDP-pseudo-otsakkeen toiminta. (mukaillen Hakala & Vainio 2002, 259.)

Taulukossa 3, esitellään IP-datagrammin UDP-pseudo-otsake. UDP:tä käytettäessä IP-datagrammiin lisätään myös Pseudo-otsake (IP Pseudo header), joka ilmaisee, että sovellus on lähettänyt viestinsä käyttämällä UDP-protokollaa. Protokollakoodin arvo 17 tarkoittaa UDP:tä. (Hakala & Vainio 2002, 260.)

Wirtesharkilla kaapattua UDP-liikennettä lyhyellä selityksellä:

No. Time Source Destination Protocol Info
1 0.000000 192.168.1.9 192.168.1.255 BROWSER Local Master Announcement TOPI, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Master Browser, DFS server

Frame 1 (270 bytes on wire, 270 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol

Frame 1: Tietokone topi aloittaa yleislähetysosoitteen 192.168.1.255 kautta suoratoiston lähettämisen. Tunnistetaan MAC-osoite.

No. Time Source Destination Protocol Info
2 0.000031 192.168.1.9 192.168.1.255 BROWSER Domain/Workgroup Announcement WORKGROUP, NT Workstation, Domain Enum

Frame 2 (247 bytes on wire, 247 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)

NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB MailSlot Protocol
Microsoft Windows Browser Protocol

Frame 2: MAC-osoitteen tunnistamisen jälkeen yleislähetysosoite ja IP-osoite 192.168.1.9 tunnistavat toisensa.

No. Time Source Destination Protocol Info
3 81.075475 192.168.1.10 224.0.0.251 MDNS Standard query PTR _pgpkey-hkp._tcp.local, "QM" question

Frame 3 (82 bytes on wire, 82 bytes captured)
Ethernet II, Src: FujitsuS_68:06:0c (00:30:05:68:06:0c), Dst: IPv4mcast_00:00:fb (01:00:5e:00:00:fb)
Internet Protocol, Src: 192.168.1.10 (192.168.1.10), Dst: 224.0.0.251 (224.0.0.251)
User Datagram Protocol, Src Port: mdns (5353), Dst Port: mdns (5353)
Domain Name System (query)

Frame 3: Silloittava IP-osoite tutustuu IP-osoitteeseen 224.0.0.251.

No. Time Source Destination Protocol Info
4 193.952123 DTS 1867.381244444 PTS 1867.381244444 MPEG PES video-stream

Frame 4 (1358 bytes on wire, 1358 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: 40844 (40844), Dst Port: search-agent (1234)
ISO/IEC 13818-1 PID=0x0 CC=0
ISO/IEC 13818-1 PID=0x42 CC=0
ISO/IEC 13818-1 PID=0x44 CC=0
ISO/IEC 13818-1 PID=0x44 CC=1
ISO/IEC 13818-1 PID=0x44 CC=2
ISO/IEC 13818-1 PID=0x44 CC=3
ISO/IEC 13818-1 PID=0x44 CC=4

Frame 4: Suoratoisto IP-osoitteesta 192.168.1.9, lähetetään portin 1234 avulla lähiverkon toisille tietokoneille. Nyt kun joku lähiverkossa oleva tietokone ottaa yhteyttä, pääsee se näkemään suoraa lähetystä tietokoneesta topi.

6.4 TCP

TCP tarjoaa kohtalaisen yksinkertaiset menetelmät luotettavan yhteyden muodostamiseksi järjestelmien välille. Protokollalla on kolme päätehtävää: yhteyden muodostuksesta sopiminen, lähetettyjen pakettien kuittaaminen ja vuonohjaus. (Hakala & Vainio 2002, 253.)

Vuonohjauksen periaate on, että lähettäjälle ilmoitetaan verkkoliikenteen ruuhkatilanteissa: ”odota, niin käsittelen aiemmin lähetetyt paketit”. Vuonohjausta voidaan verrata autoliikenteessä oleviin liikennevaloihin sillä erotuksella, että vuonohjauksessa vuoro tulee heti kun reitti vapautuu. Vuonohjauksella voidaan säädellä siirrettävien pakettien määrää. (Koivisto 2010.)

Yleisesti WWW-palvelin hyväksyy TCP-yhteydet porttiin 80/tcp (http), joka on oletusporttina. Yleensä ei ole mitään syytä sallia mistään julkisesta verkosta WWW-palvelimelle tulevia yhteyksiä. Jos WWW-palvelin tukee SSL-suojattuja yhteyksiä, täytyy sallia porttiin 443/tcp (https) tapahtuva liikenne. (Allen 2002, 84.)

Käytössä olevat porttinumerot voi tarkistaa Ubuntun terminaalissa käskyllä *netstat* (Hakala & Vainio 2002, 255).

Käytössä olevista porttinumeroista selviää, mitä portteja Ubuntussa on juuri sillä hetkellä käytössä.

0	15	31 bitti
Lähdeportti (source port)	Kohdeportti (destination port)	
Sekvenssinumero (sequence number)		
Kuittausnumero (acknowledgement number)		
Otsakkeen pituus ja liput (header information)	Ikkunakoko (window size)	
TCP-otsakkeen varmistussumma (TCP checksum)	Kiireellisyysosoitin (urgent pointer)	
Optiot (mahdollisesti, ei pakollisia) (options)		
DATA		

TAULUKKO 4, TCP-segmentin toimintakaavio. (mukaillen Hakala & Vainio 2002, 258.)

Kuviossa 12, esitellään TCP-segmentin keskeisimmät tiedot. Nämä tiedot auttavat, kun täytyy selvittää virheiden mahdollisia syitä verkkoliikenneanalysaattorilla.

Verkkoliikennettä TCP-protokollalla oli helppo tuottaa. Samban kautta lähiverkosta avattu video alkoi tuottaa verkkoliikennettä TCP-protokollalla. Wiresharkilla kaapattu verkkoliikenne TCP-protokollasta lyhyellä selityksellä:

No. Time Source Destination Protocol Info
7 0.000546 192.168.1.9 192.168.1.8 TCP http > 49910 [ACK] Seq=1 Ack=174 Win=5824 Len=0 TSV=508524 TSER=4321

Frame 7 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49910 (49910), Seq: 1, Ack: 174, Len: 0

Frame 7: IP-osoite 192.168.1.8 käyttää videon yhteydenottoon http-prorokollaa. IP-osoite 192.168.1.9 lähettää vastauksen porttia 49910 apuna käyttäen. IP-osoite 192.168.1.8 vas-

taanottaa vastauksen portin 80 kautta. 192.168.1.8 kertoo voivansa ottaa vastaan 173 tavun suuruisia segmenttejä. 192.168.1.8 ensimmäinen segvenssinumero on 1.

No. Time Source Destination Protocol Info
8 0.027933 192.168.1.9 192.168.1.8 TCP [TCP segment of a reassembled PDU]

Frame 8 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49910 (49910), Seq: 1, Ack: 174, Len: 1448

Frame 8: IP-osoite 192.168.1.9 lähettää 174 tavun segmentin IP-osoitteelle 192.168.1.8.

No. Time Source Destination Protocol Info
9 0.028056 192.168.1.9 192.168.1.8 TCP [TCP segment of a reassembled PDU]

Frame 9 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49910 (49910), Seq: 1449, Ack: 174, Len: 1448

Frame 9: IP-osoite 192.168.1.9 lähettää uudestaan 174 tavun segmentin IP-osoitteelle 192.168.1.8. 192.168.1.9 ilmoittaa uudeksi ikkunan kooksi 1449 tavua.

No. Time Source Destination Protocol Info
10 0.028129 192.168.1.8 192.168.1.9 TCP 49910 > http [ACK] Seq=174 Ack=1449 Win=8768 Len=0 TSV=4328 TSER=508531

Frame 10 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: FujitsuS_85:03:21 (00:30:05:85:03:21), Dst: FujitsuS_85:01:c6 (00:30:05:85:01:c6)
Internet Protocol, Src: 192.168.1.8 (192.168.1.8), Dst: 192.168.1.9 (192.168.1.9)
Transmission Control Protocol, Src Port: 49910 (49910), Dst Port: http (80), Seq: 174, Ack: 1449, Len: 0

Frame 10: IP-osoite 192.168.1.8 hyväksyy uuden ikkunan koon 1449 tavua. Aloittavaksi segvenssinumeroksi tulee edellisen aloittavan segvenssinumeron loppu 174 tavua.

No. Time Source Destination Protocol Info
11 0.028179 192.168.1.9 192.168.1.8 TCP [TCP segment of a reassembled PDU]

Frame 11 (1514 bytes on wire, 1514 bytes captured)
Ethernet II, Src: FujitsuS_85:01:c6 (00:30:05:85:01:c6), Dst: FujitsuS_85:03:21 (00:30:05:85:03:21)
Internet Protocol, Src: 192.168.1.9 (192.168.1.9), Dst: 192.168.1.8 (192.168.1.8)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49910 (49910), Seq: 2897, Ack: 174, Len: 1448

Frame 11: IP-odoite 192.168.1.9 lähettää lisää data IP-osoitteelle 192.168.1.8.

7 VLC-MEDIASOITIN

VLC mediasoitin toimii parhaiten Linuxissa. VLC mediasoitinta käytetään mm. äänen ja kuvan toistamiseen tietokoneella. Opinnäytetyössä, VLC mediasoittimen käyttötarkoitus oli toimia videoserverinä sekä ottaa vastaan videoserveriltä lähetettyä videota.

7.1 VLC-mediasoittimen asentaminen

VLC-mediasoittimen asentaminen tapahtui, antamalla terminaalissa käskyn:

topi@topi:~$ sudo apt-get install vlc

VLC-mediasoittimen asentamisen jälkeen, VLC-mediasoitin löytyi Linuxin valikosta:

Sovellukset > Ääni & video > VLC media player

7.2 VLC-mediasoitin videoserverinä

Tarkoitus oli saada VLC-mediasoitin tuottamaan verkkoliikennettä UDP-protokollaa käyttäen. Verkkoliikenteen tuottaminen UDP-protokollalla onnistui, kun VLC mediasoitin asetettiin toimimaan videoserverinä. VLC mediasoitin asetettiin käyttämään UDP-protokollaa video-lähetyksessään. videoserverinä käytettiin tietokonetta topi.

Käynnistettiin VLC-mediasoitin Linuxin valikosta:

Sovellukset > Ääni & video > VLC media player.

Valittiin VLC mediasoittimen valikosta:

Media > Suoratoisto…

VLC mediasoittimeen asetettiin tiedosto, jota toistettiin suoratoistona. Valittiin:

Lisää… > home > topi > Asiakirjat > VTS_01_1.VOB

Painettiin alhaalla olevaa ”Suoratoisto”-painiketta.

”Suoratoisto”-valinnan jälkeen tuli ikkuna, jossa valittiin ”Seuraava”-painike.

”Kohteet”-välilehdessä valittiin ”Uusi kohde”-valikosta UDP. UDP valinnan jälkeen painettiin ”Lisää”-painiketta.

”Osoite”-kenttään annettiin yleislähetysosoite 192.168.1.255. Porttina annettiin olla 1234. Profiiliksi valittiin valikosta ”Video - MPGA (TS)”-valinta, jonka jälkeen painettiin ”Suoratoista”-painiketta.

Kun edellä mainitut toimenpiteet oli saatu suoritettua, saatiin VLC mediasoitin lähettämään videota UDP-protokollalla yleislähetysosoitteessa 192.168.1.255.

7.3 Suoratoiston katsominen VLC-mediasoittimella

Video lähetettiin suoratoistona tietokoneelta topi, tietokoneelle jope, tietokoneen repe kautta. Tietokoneisiin topi ja jope asennettiin molempiin VLC-mediasoitin. Kun tietokoneella topi, suoratoisto oli laitettu toistumaan UDP-lähetyksenä, haluttiin nähdä videolähetys tietokoneen jope VLC-mediasoittimessa.

Käynnistettiin VLC-mediasoitin Linux-valikosta:

Sovellukset > Ääni & video > VLC media player.

Valittiin VLC-mediasoittimen valikosta:

Media > Avaa suoratoisto verkosta…

Lähetyksen protokollaksi valittiin UDP. Osoitekenttään annettiin yleislähetysosoite 192.168.1.255 ja porttina annettiin olla 1234.

Kun tämän jälkeen painettiin ”Toista”-painiketta, lähti video toistumaan UDP-lähetyksenä

tietokoneelta topi. UDP-protokollalla videon toistaminen on laadultaan huonompaa kuin TCP-protokollalla toistettu video. UDP-protokollalla suoritettu videon toistaminen oli pätkivää, verrattuna TCP-protokollalla suoritettuun videon toistoon.

8 TULOKSET JA POHDINTA

Opinnäytetyössä oli haasteellista suuri määrä tietoa vieraalla kielellä.Linuxin käyttämistä varten luin paljon englanninkielistä ja suomenkielistä tekstiä kirjoista ja Internetistä. Näin sain hyvät pohjatiedot tulevaisuutta varten Linuxin parissa.

Verkkoliikenteen tuottaminen UDP-protokollalla oli helppoa, kun huomattiin käyttää vain oikeaa ohjelmaa. VLC mediasoitin oli oivallinen apu UDP-protokollan tuottamiseen verkkoliikenteessä.

UDP-protokollalla videon toistaminen oli tietokoneelle vaikeampaa kuin TCP-protokollalla videon toistaminen. Huomattava ero löytyi videon laadussa. UDP-protokollaa käytettäessä video tahtoi olla osittain hieman epätarkkaa. TCP-protokollaa käytettäessä video toistui ongelmitta.

Ntop ohjelma oli hyvä apuväline verkkoliikenteen graafisessa tuottamisessa. Aika loppui hieman kesken kaikkien mahdollisten asioitten selvittämisen suhteen. Ntop saatiin tuottamaan verkkoliikenteestä graafisia tuloksia, mutta tiedon talteen ottaminen Ntop ohjelman avulla ei tämän opinnäytetyön puitteissa onnistunut. Ntop ohjelmassa oli mahdollista saada tiedot talteen MySql tietokantaan. Wiresharkilla kaapatun tiedon lataaminen Ntop ohjelman graafeihin onnistui osittain. Wiresharkilla kaapatusta tiedosta saatiin muodostettua Ntop ohjelman avulla piirakka graafeja, mutta aikajaksollisten graafien tuottaminen ei onnistunut. Tyydyttiin ottamaan tiedot talteen Wiresharkilla ja graafinen tulostus tapahtui samanaikaisesti Ntop ohjelmalla.

Monia kertoja yritettiin saada Ntop tuottamaan muunlaista graafeja kuin pelkästään yleisellä tasolla olevia graafisia kuvaajia. Ohjelmalla ei onnistuttu tuottamaan porttikohtaisia graafisia kuvaajia. Mikäli Ntop ohjelman lähdekoodia muokkaisi tähän tarkoitukseen, suostuisi se varmasti paremmin yhteistyöhön porttikohtaiselta tasolta. Ntopin käynnistäminen oikeanlaisella käskyllä voisi mahdollistaa myös porttikohtaisen graafin tuottamisen.

Kokeilemisen arvoinen ohjelma olisi vielä ollut Mrtg ohjelma. Mrtg on graafien tuottamiseen tarkoitettu ohjelma. Seuraavana tutkimisen aiheena olisi ollut Mrtg, mutta aika loppui kesken.

Kaikista vaikein tehtävä opinnäytetyön tekemisessä on ollut dokumentointi. Tiivistelmän logon kohdistaminen onnistui kokeilemalla. Sivujen numeroinnin kanssa oli ongelmia, mutta ratkaisu siihenkin löytyi. LIITE 6 sisältää CD-ROM levyn, josta löytyy opinnäytetyössä käytetyty asetukset ja Wiresharkilla kaapatut tiedostot.

LÄHTEET

Allen, J. 2002. CERT Verkkotietoturvan hallinta. Helsinki: IT Press.

Dell. 2010. Linux. Www-dokumentti. Saatavissa:
http://linux.dell.com/whitepapers/nic-enum-whitepaper-v4.pdf
Luettu 31.03.2010.

Hakala, M. & Vainio, M. 2002. Tietoverkon rakentaminen. Porvoo: Docendo.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. Painos 4. Helsinki: IT Press.

Linux. 2010. Wireshark. Www-dokumentti. Saatavissa:
http://www.linux.fi/wiki/Wireshark.
Luettu 18.02.2010.

Mbnet. 2010. Linuxista mediakone. Www-dokumentti. Saatavissa:
http://www.mbnet.fi/nettijatkot/2010/03/linuxista_mediakone_3.
Luettu 31.03.2010.

Ntop. 2010. Ntop man-page. Www-dokumentti. Saatavissa:
http://www.ntop.org/ntop-man.html.
Luettu 02.02.2010.

Reunamo. 2010. Lyhyesti FTP:stä. Www-dokumentti. Saatavissa:
http://www.reunamo.com/arto/havainnot/ftp_lyhyesti.htm
Luettu 31.03.2010.

Ubuntu. 2010. About Ubuntu name. Www-dokumentti. Saatavissa:
https://help.ubuntu.com/9.04/about-ubuntu/C/about-ubuntu-name.html
Luettu 31.03.2010.

Ubuntu. 2010. Network Connection Bridge. Www-dokumentti. Saatavissa:
http://help.ubuntu.com/community/NetworkConnectionBridge.
Luettu 02.04.2010.

Ubuntu. 2010. Ntop. Www-dokumentti. Saatavissa:
https://help.ubuntu.com/community/Ntop
Luettu 31.03.2010.

Ubuntu. 2010. Ntop. Www-dokumentti. Saatavissa:
https://help.ubuntu.com/community/Ntop
Luettu 31.03.2010.

Ubuntu. 2010.Ubuntu Foundation. Www-dokumentti. Saatavissa:
http://www.ubuntu.com/news/UbuntuFoundation
Luettu 15.01.2010.

Youtube. 2010. Technoblogical. Www-dokumentti. Saatavissa:
http://www.youtube.com/watch?v=p2r0kIB_ItE.
Luettu 18.02.2010.

Wireshark. 2010. Capture Privileged. Www-dokumentti. Saatavissa:
http://wiki.wireshark.org/CaptureSetup/CapturePrivileged.
Luettu 16.01.2010.

Wireshark. 2010. ChIntroHelp. Www-dokumentti. Saatavissa:
http://www.wireshark.org/wsug_html_chunked/ChIntroHelp.html
Luettu 04.04.2010.

Verkkoasetukset ja proxy

Kun haluttiin käyttää Internettiä, niin täytyi muuttaa proxy-asetukset Internet-yhteyden sallivaksi. Proxy-asetuksien muuttaminen tapahtui Ubuntun valikosta:

Järjestelmä > Asetukset > Välipalvelin

Valittiin ”Välipalvelimen asetus käsin”-valinta ja ”Käytä samaa välipalvelinta kaikille protokollille”-valinta. Valintojen jälkeen painettiin ”Toteuta järjestelmänlaajuisesti”-nappia, jonka jälkeen annettiin käyttöjärjestelmän hallitsijan salasana kaksi kertaa.

Ennen Internettiin yhdistämistä täytyi muuttaa *interfaces* tekstitiedostoa ja käynnistää verkkoasetukset uudestaan. Laitettiin verkkokortin lähiverkkoa varten tehtyjen määritysten eteen yksi kommenttimerkki: #

Intefaces tekstitiedosto näytti muutosten jälkeen tietokoneessa jope seuraavalta:

auto lo
iface lo inet loopback

#auto eth0
#iface eth0 inet static
#address 192.168.1.8
#netmask 255.255.255.0
#broadcast 192.168.1.255

auto eth0
iface eth0 inet dhcp

Lopuksi käynnistettiin verkkoasetukset uudestaan käskyllä:

sudo /etc/init.d/networking restart

Kun haluttiin käyttää taas lähiverkkoa, niin täytyi muuttaa proxy-asetukset lähiverkon sallivaksi.

Proxy-asetuksien muuttaminen tapahtui Ubuntun valikosta:

Järjestelmä > Asetukset > Välipalvelin

Käytettiin ”Suora internet-yhteys”-valintaa. Lopuksi painettiin ”Toteuta järjestelmänlaajuisesti”-nappia, jonka jälkeen annettiin käyttöjärjestelmän hallitsijan salasana kaksi kertaa. Ennen lähiverkkoon yhdistämistä täytyi muuttaa *interfaces* tekstitiedostoa ja käynnistää verkko uudestaan. Laitettiin Internetin määritysten eteen yksi kommenttimerkki: #

Intefaces tekstitiedosto näytti muutosten jälkeen tietokoneessa jope seuraavalta:

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.8
netmask 255.255.255.0
broadcast 192.168.1.255

#auto eth0
#iface eth0 inet dhcp

Lopuksi käynnistettiin verkkoasetukset uudestaan käskyllä:

sudo /etc/init.d/networking restart

Verkkoasetukset tietokoneelle jope

Tekstitiedoston *hosts* muokkaamista varten annettiin terminaalissa käsky:

jope@jope:~$ sudo nano /etc/hosts

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *hosts* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *hosts* sisältö näytti seuraavalta:

127.0.0.1 localhost
127.0.1.1 jope

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

Tekstitiedostoa *hosts* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *hosts* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *hosts* täydentämisen jälkeen tekstitiedosto *hosts* sisälsi seuraavaa:

127.0.0.1 localhost
127.0.1.1 jope
192.168.1.10 repe
192.168.1.8 jope

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouter
ff02::3 ip6-allhosts

Tekstitiedoston *interfaces* muokkaamista varten annettiin terminaalissa käsky:

jope@jope:~$ sudo nano /etc/network/interfaces

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *interfaces* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *interfaces* sisältö näytti seuraavalta:

auto lo
iface lo inet loopback

Tekstitiedostoa *interfaces* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *interfaces* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *interfaces* täydentämisen jälkeen tekstitiedosto *interfaces* sisälsi seuraavaa:

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.8
netmask 255.255.255.0
broadcast 192.168.1.255

Verkkoasetukset täytyi ottaa käyttöön tietokoneen jope verkkokortille, käskyllä:

jope@jope:~$ *sudo /etc/init.d/networking restart*

Kun nyt kirjoitettiin terminaalissa käsky *ifconfig*, niin käsky tulosti tekstin:

```
jope@jope:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr  00:30:05:85:03:21
          inet addr:192.168.1.8  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::230:5ff:fe85:321/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5548  (5.5 KB)  TX bytes:5171  (5.1 KB)
          Interrupt:23 Base address:0x5000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP  LOOPBACK RUNNING MTU:16436 Metric:1
          RX  packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX  packets:18 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX  bytes:1416  (1.4 KB)  TX bytes:1416  (1.4 KB)
jope@jope:~$
```

Verkkoasetukset tietokoneelle topi

Tekstitiedoston *hosts* muokkaamista varten annettiin terminaalissa käsky:

topi@topi:~$ sudo nano /etc/hosts

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *hosts* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *hosts* sisältö näytti seuraavalta:

127.0.0.1 localhost
127.0.1.1 topi

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

Tekstitiedostoa *hosts* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *hosts* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *hosts* täydentämisen jälkeen tekstitiedosto *hosts* sisälsi seuraavaa:

127.0.0.1 localhost
127.0.1.1 topi
192.168.1.10 repe
192.168.1.9 topi

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

Tekstitiedoston *interfaces* muokkaamista varten annettiin terminaalissa käsky:

jope@jope:~$ sudo nano /etc/network/interfaces

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *interfaces* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *interfaces* sisältö näytti seuraavalta:

auto lo
iface lo inet loopback

Tekstitiedostoa *interfaces* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *interfaces* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *interfaces* täydentämisen jälkeen tekstitiedosto *interfaces* sisälsi seuraavaa:

auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.1.9
netmask 255.255.255.0
broadcast 192.168.1.255

Verkkoasetukset täytyi ottaa käyttöön tietokoneen topi verkkokortille, käskyllä:

topi@topi:~$ sudo /etc/init.d/networking restart

Kun nyt kirjoitettiin terminaalissa käsky *ifconfig*, niin käsky tulosti tekstin:

```
topi@topi:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr  00:30:05:85:01:c6
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::230:5ff:fe85:1c6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:51 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:21 dropped:0 overruns:0 carrier:42
          collisions:0 txqueuelen:1000
          RX bytes:7142  (7.1 KB)  TX bytes:5171  (6.2 KB)
          Interrupt:23 Base address:0x5000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP  LOOPBACK RUNNING MTU:16436 Metric:1
          RX  packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX  packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX  bytes:720  (720.0 B)  TX bytes:1416  (720.0 B)
topi@topi:~$
```

Verkkoasetukset tietokoneelle repe

Tekstitiedoston *hosts* muokkaamista varten annettiin terminaalissa käsky:

repe@repe:~$ sudo nano /etc/hosts

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *hosts* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *hosts* sisältö näytti seuraavalta:

127.0.0.1 localhost
127.0.1.1 repe

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

Tekstitiedostoa *hosts* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *hosts* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *hosts* täydentämisen jälkeen tekstitiedosto *hosts* sisälsi seuraavaa:

127.0.0.1 localhost
127.0.1.1 repe
192.168.1.10 repe
192.168.1.9 topi
192.168.1.8 jope

 # The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

Ennen silloittavan tietokoneen repe *interfaces* tekstitiedoston muokkaamista kirjoitettiin terminaalissa:

repe@repe:~$ sudo apt-get update (Ubuntu, Network Connection Bridge, 2010.)
repe@repe:~$ sudo apt-get install bridge-utils (Ubuntu, Network Connection Bridge ,2010.)

ifconfig eth0 0.0.0.0
ifconfig eth1 0.0.0.0
brctl addbr silta
brctl addif silta eth0
brctl addif silta eth1
ifconfig silta up (Ubuntu, Network Connection Bridge ,2010.)

Tekstitiedoston *interfaces* muokkaamista varten annettiin terminaalissa käsky:

jope@jope:~$ sudo nano /etc/network/interfaces

Terminaalin komentorivi pyysi antamaan käyttöjärjestelmän hallitsijan salasanan. Käyttöjärjestelmän hallitsijan salasanan antamisen jälkeen päästiin muokkaamaan tekstitiedoston *interfaces* sisältöä nano tekstieditorilla. Aluksi tekstitiedoston *interfaces* sisältö näytti seuraavalta:

auto lo
iface lo inet loopback

Tekstitiedostoa *interfaces* täydennettiin halutun toiminnan mahdollistavalla tekstillä. Tekstitiedosto *interfaces* tallennettiin näppäinyhdistelmällä Ctrl+o. Lopuksi painettiin näppäinyhdistelmää Ctrl+x, jonka seurauksena nano tekstieditori sulkeutui palaten terminaalin komentorivi tilaan. Tekstitiedoston *interfaces* täydentämisen jälkeen tekstitiedosto *interfaces* sisälsi tekstin:

auto lo
iface lo inet loopback

auto silta
iface silta inet static
address 192.168.1.10
netmask 255.255.255.0
network 192.168.1.0
gateway 192.168.1.1
dns-nameservers 192.168.1.5
dns-search example.com

pre-up ifconfig eth0 down
pre-up ifconfig eth1 down
pre-up brctl addbr silta
pre-up brctl addif silta eth0
pre-up brctl addif silta eth1
pre-up ifconfig eth0 0.0.0.0
pre-up ifconfig eth1 0.0.0.0
post-down ifconfig eth0 down
post-down ifconfig eth1 down
post-down ifconfig silta down
post-down brctl delif silta eth0
post-down brctl delif silta eth1
post-down brctl delbr silta
(Ubuntu, Network Connection Bridge, 2010.)

Verkkoasetukset täytyi ottaa käyttöön tietokoneen repe verkkokorteille, käskyllä:

repe@repe:~$ sudo /etc/init.d/networking restart

Kun nyt kirjoitettiin terminaalissa käsky *ifconfig*, niin käsky tulosti tekstin:

```
repe@repe:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr  00:30:05:68:06:0c
          inet6 addr: fe80::230:5ff:fe68:60c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5537  (5.3 KB)  TX bytes:9196  (9.1 KB)
          Interrupt:23 Base address:0x5000

eth1      Link encap:Ethernet  HWaddr  00:50:bf:b2:c9:3e
          inet6 addr: fe80::250:bfff:feb2:c93e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6839  (6.8 KB)  TX bytes:8268  (8.2 KB)
          Interrupt:19 Base address:0x5000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP  LOOPBACK RUNNING MTU:16436 Metric:1
          RX  packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX  packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX  bytes:240  (240.0 B)  TX bytes:240  (240.0 B)

silta     Link encap:Ethernet  HWaddr  00:30:05:68:06:0c
          inet addr:192.168.1.10  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::230:5ff:fe68:60c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:81 errors:0 dropped:0 overruns:0 frame:0
          TX packets:52 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:11030  (11.0 KB)  TX bytes:5975  (5.9 KB)
repe@repe:~$
```

```
[global]

workgroup = WORKGROUP
server string = %h server (Samba, Ubuntu)
;               wins server = w.x.y.z
dns proxy = no
interfaces = 192.168.1.9/24 eth0
;               bind interfaces only = yes
log file = /var/log/samba/log.%m
max log size = 1000
syslog = 0
panic action = /usr/share/samba/panic-action %d

security = user
encrypt passwords = true
passdb backend = tdmsam
obey pam restrictions = yes
unix password sync = yes
passwd program = /usr/bin/passwd %u
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n
*password\supdated\ssuccessfully*
pam password change = yes
map to guest = bad user
;               domain logons = yes
;               logon path = \\%N\profiles\%U
;               logon drive = H:
;               logon script = logon.cmd
;               add user script = /usr/sbin/adduser --quiet --disabled-password --gecos "" %u
;               add machine script = /usr/sbin/useradd -g machines -c "&u machine account" -d /var/lib/samba -s /bin/false %u
;               add group script = /usr/sbin/addgroup --force-badname %g

;               printing = bsd
;               printcap name = /etc/printcap
;               printing = cups
;               printingcap name = cups

;               include = /home/samba/etc/smb.conf.%m
;               message command = /bin/sh/ -c '/usr/bin/linpopup "%f" "%m" %s' &
;               idmap uid = 10000-20000
;               idmap gid = 10000-20000
;               template shell = /bin/bash
;               winbind enum groups = yes
;               winbind enum users = yes
;               usershare max shares = 100
usershare allow guests = yes

;[homes]
;               comment = Home Directories
```

```
;               browseable = no
;               readonly = yes
;               create mask = 0700
;               directory mask = 0700
;               valid users = %S

;[netlogon]
;               comment = Network Logon Service
;               path = /home/samba/netlogon
;               guest ok = yes
;               read only = yes
;               share modes = no

;[profiles]
;               comment = Users profiles
;               path = /home/samba/profiles
;               guest ok = no
;               browseable = no
;               create mask = 0600
;               directory mask = 0700

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
;               write list = root, @lpadmin

[cdrom]
comment = Samba server's CD-ROM
read only = yes
locking = no
path = /cdrom
guest ok = yes
valid users = topi
;               preexec = /bin/mount /cdrom
;               postexec = /bin/umount /cdrom

[Kulmakatu]
comment = Kulmakatu – jako
```

path = /jako
browsable = yes
guest ok = yes
read only = no
writeable = yes

Opinnäytetyössä käytetyt asetustiedostot ja kaapatut tiedostot: