Tommi Nordlund

TILAPÄISEN VERKON TOTEUTTAMINEN YLLÄPITO JA DOKUMENTOINTI

Tietojenkäsittelyn koulutusohjelma

Järjestelmäpalvelujen suuntautumisvaihtoehto

2008

Satakunnan ammattikorkeakoulu

TILAPÄISEN VERKON TOTEUTTAMINEN, YLLÄPITO JA DOKUMENTOINTI CASE: INSOMNIA

Nordlund Tommi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Tammikuu 2009
Grönholm, Jukka
UDK: 004.7
Sivumäärä: 37

Asiasanat: lähiverkot, ethernet, dokumentointi, rakenteettomat verkot

---

Tilapäisen verkon toteuttaminen, ylläpito ja dokumentointi Case Insomnia – työssä toteutettiin selvitys Insomnia – tapahtuman verkon toteuttamisesta ja ylläpidosta. Tämä työ toimii myös verkon dokumenttina. Tapahtuman verkon toteuttamisesta ja ylläpidosta ei ollut ennen tällaista selvitystyötä tehty. Tapahtuman verkon kehittämisen takia lähdettiin toteuttamaan tätä opinnäytetyötä olemassa olevasta verkosta.

Tulevaisuutta varten vuosittainen Insomnia – tapahtuma saa tästä opinnäytetyöstä kehitystyökalun, jonka avulla tapahtuman verkkoa voidaan jatkossa kehittää entistä paremmaksi.

Opinnäytetyöni teoriaosuudessa käsiteltiin verkon perusprotokollia ja peruspalveluita. Tämän jälkeen perehdyttiin verkon reititykseen ja palomuuritoimintoihin, sekä verkon liikenteen kuormantasaukseen ja sen hallintaan. Myös Spanning Tree Protocol – algoritmi käydään lävitse, koska se oli tapahtuman aikana käytössä pöytäkytkimissä. Tämä lisäksi virtuaaliset lähiverkot ja langattomat lähiverkot sekä niihin liittyvät asiat selvitetään. Lopuksi pohditaan tilapäisen verkon käsitettä ja sen eroavaisuuksia pysyvään verkkoon.

Käytännön osuudessa toteutettiin tapahtuman verkko ja hoidettiin tapahtuman verkon ylläpito tapahtuman aikana. Tapahtuman verkosta, reitityksestä ja autentikoinnista tehtiin verkkokuvat, joiden tarkoitus on selventää näitä asioita. Työn käytännönosuus toteutettiin 22.10.2008 – 26.10.2008 ja tapahtuma pidettiin 24.10.2008 – 26.10.2008. Tapahtuman aikana ei enää verkkoa toteutettu, vaan hoidettiin pelkästään ylläpidollisia asioita. Toteuttaminen tapahtui 22.10.2008 – 24.10.2008 välisenä aikana, jolloin verkko saatiin toimintakuntoon käyttäjiä varten 24.10.2008.

THE TEMPORARY NETWORK IMPLEMENTATION, MAINTENANCE AND DOCUMENTATION CASE INSOMNIA

Nordlund Tommi
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme of Information Technology
January 2009
Grönholm Jukka
UDK: 004.7
Number of Pages: 37

Key words: local area networks, ethernet, documentation, ad hoc - Networks

---

The temporary network implementation, maintenance and documentation Case Insomnia - work was carried out at the Insomnia – event and its network implementation and maintenance. This thesis works as network's documentation. This report from the network implemention and maintenance had not been done before. In order to develop the events network system this thesis was done from the current network system.

For the future the annual Insomnia – event will get a development tool from this work which can used to develop the events network even better.

In the theory part was dealt with network's basic protocols and services. After this were taken a look at how network's routing works and firewall features and also load balancing the network traffic and controlling it. Also Spanning Tree Protocol – algorithm was dealt with because it was used in the event's switches. In addition to this virtual local area networks and wireless local area networks and things related to them was examined. In the end the concept of a temporary network was examined and its differences to permanent network.

In the practical part the event's network was implemented and the network was maintenanced during the event. From the event's network, its routing system and its authentication system was made network pictures which were made for clear these things. The practical part of this work was done 22.10.2008 – 26.10.2008 and the event was held 24.10.2008 – 26.10.2008. During the event there was no implementation done, only maintenance duties were done. The implementation was done between 22.10.2008 and 24.10.2008 and the network was functional for the users 24.10.2008.

SISÄLLYS

1 JOHDANTO

Opinnäytetyöni käsittelee tilapäisen verkon toteutusta, ylläpitoa ja dokumentointia. Opinnäytetyön tavoitteena on tehdä suunnitelma tapahtuman verkosta sen toteuttamisesta, sekä eri osien toiminnasta. Tarkoituksena on myös perehtyä tapahtuman ylläpitoon. Opinnäytetyöni on tehty verkkopeliyhdistys Insomnia ry:n verkkopelitapahtuma Insomniaan. Tapahtuma järjestettiin 24.10.2008 – 26.10.2008, Porissa. Tapahtuma keräsi noin 400 osallistujaa eri puolilta Suomea. Tilapäisen verkon toteuttaminen, ylläpito ja dokumentointi - aiheena on mielenkiintoinen ja osin haastavakin. Vaaditaan asiantuntemusta ja kokemusta monelta eri alalta, jotta pystytään toteuttamaan tällainen projekti eli Insomnia – tapahtuma ja sen verkon toteuttaminen. Insomnia – tapahtuma järjestetään jo kymmenennen kerran, joten tapahtuman järjestäjillä on jo vankka kokemus asiasta.

Tapahtuman järjestäjien kokemuksesta huolimatta, verkon toteuttamisesta ja ylläpidosta ei ole tämän laajuista selvitystyötä tehty. Verkon toteuttamiseen ja ylläpitoon liittyvät suunnitelmat ovat tietysti olleet olemassa, mutta selvitystä verkon toiminnasta, sen komponenteista, käyttäjän autentikoinnista ja ylläpidosta ei ole tehty. Myöskään aiemmin ei ole ollut saatavilla verkkokuvia, jotka tämän työn yhteydessä tullaan tekemään. Niiden avulla pystytään jatkossa suunnittelemaan ja kehittämään tapahtuman verkkoa. Tällä aihevalinnallani pyrin helpottamaan tulevien Insomnia – tapahtumien suunnittelua, toteuttamista, ylläpitoa ja kehittämistä entistä parempaan ja tehokkaampaan suuntaan.

2 TEORIAOSUUS

Opinnäytetyöni teoriaosuudessa käsittelen, ensiksi verkon perusprotokollia ja peruspalveluita, joita verkon toimimiseen tarvitaan. Sen jälkeen perehdytään verkon reititykseen ja palomuuritoimintoihin, sekä verkon liikenteen kuormantasaukseen ja hallintaan. Myös tapahtumassa pöytäkytkimissä käytössä ollut, Spanning Tree Protocol – algoritmi ja sen toiminta selvitetään. Lisäksi vielä käydään virtuaaliset lähiverkot sekä langattomat lähiverkot ja niiden ominaisuudet lävitse. Lopuksi pohditaan tilapäisen verkon käsitettä ja sen eroavaisuuksia pysyvään verkkoon. Nämä kaikki asiat, jotka teoriaosuudessa käsitellään liittyvät tapahtuman verkon toteuttamiseen tai ylläpitoon ja sillä tavoin ovat oleellisia läpikäytäviä asioita.

Nykypäivänä lähes kaikki verkot perustuvat tavalla tai toisella TCP / IP - protokollalle, joka jaetaan kahteen osaan, TCP - protokollaan ja IP - protokollaan. TCP eli Transmission Control Protocol on kuljetuskerroksen protokollista toinen ja UDP eli User Datagram Protocol on toinen. TCP – protokolla on monipuolisempi ja siitä syystä myös paljon yleisemmin käytettävä protokolla. Tärkeämpi osa TCP / IP – protokollaa on IP eli Internet Protocol, joka sijaitsee verkkokerroksella. Se muodostaa TCP / IP – protokollan rungon kuljettamalla TCP - ja UDP - protokollat. Tärkein ominaisuus IP - protokollalle on kuitenkin loogiset IP – osoitteet, näiden avulla protokollan toteutukset osaavat lähettää datapaketit oikeisiin paikkoihin, joko samaan tai eri verkkoon. IP – protokollasta on olemassa kaksi eri versiota, nykyisin internetin muodostava IPv4 ja tulevaisuutta edustava IPv6. (Anttila, 2001, 113 – 114)

IP – protokollan perustehtävä on välittää paketteja yhteen kytkettyjen verkkojen osasta toiseen. IP - protokolla on yhteydetön sekä reitittävä protokolla, joka tarkoittaa sitä, ettei se pidä verkkokerroksen tasolla kirjaa olemassa olevista yhteyksistä. Reitittävyys tarkoittaa sitä, että IP – protokolla liikkuu eri verkkojen lävitse reitityssääntöjen mukaisesti välittäessään paketteja. Tämä tehtävä jätetään ylemmän kuljetuskerroksen protokollien hoidettavaksi, eli

TCP – protokollan tai UDP – protokollan hoidettavaksi. (Anttila, 2001, 113 – 114)

TCP on yhteydellinen protokolla eli se tarkistaa, että lähetetyt tiedot ovat menneet verkon läpi virheettömästi ja ovat vastaanotettaessa samassa järjestyksessä kuin lähetettäessä. Toisin sanoen yhteydellinen protokolla luo ja ylläpitää yhteyttä kommunikoivien tietokoneiden välillä sekä valvoo yhteyttä kommunikoitaessa. TCP luottaa siihen, että käytössä on monikerroksinen protokollapino ja että kuljetuskerroksen alapuolella verkkokerroksessa toimivat protokollat kykenevät tarjoamaan palvelua paketin välittämiseksi verkossa. UDP – protokolla on yhteydetön protokolla, eli siihen ei sisälly toimintoa, millä tarkistettaisiin, että tiedot ovat menneet oikein perille. (Anttila, 2001, 133 – 135 & Casad & Willsey, 1999, 86 - 87)

TCP:tä käytettäessä kaikki datansiirto tapahtuu lähettävän ja vastaanottavan koneen välillä. TCP:n päätehtävät on tarjota kahden laitteen välillä luotettava yhteydellinen tiedonsiirtotie, jossa käytetään hyväksi epäluotettavaa IP:n (Internet Protocol) välityspalvelua. Luotettavuus varmistetaan siten, että TCP lähettää tiedot uudelleen ja uudelleen niin kauan, että saa vastaanottajalta vastauksen tietojen saapumisesta perille. (Anttila, 2001, 133 – 135 & Casad & Willsey, 1999, 86)

Olennainen osa TCP / IP – liikennöintiä on myös ICMP – protokolla eli Internet Control and Message Protocol. Se sijaitsee OSI – mallin internet – kerroksessa ja pääasiallisesti sitä tarvitaan reitittimissä. Kun tietokoneiden välillä lähetetään ja vastaanotetaan tietoja, kulkevat ne yhden tai useamman reitittimen kautta. Nämä reitittimet saattavat kohdata erilaisia ongelmia yrittäessään saada sanoman oikeaan päämäärään. Näistä ongelmista ICMP – sanomat kertovat tietoja lähettävälle IP – protokollaohjelmalle. ICMP – protokollan tärkeimmät toiminnot ovat; vuonohjaus, ilmoitus tuntemattomasta kohteesta, uudelleenreititys sekä etäasemien tarkkailu. ICMP käyttää IP – tietosähkeiden jakelutoimintoja omien viestien lähettämiseen. Käytännössä siis ICMP – protokolla kontrolloi TCP / IP – liikennettä. (Casad & Willsey, 1999, 63 - 64)

Kaikki IP – protokollat on numeroitu, näistä numeroista vastaanottaja tietää mitä kulloinkin IP – paketin mukana tulee. Yleisimpiä protokollia ja niitä vastaavia numeroita on, ICMP eli internet control message protocol, joka siis kontrolloi TCP / IP – liikennettä, sen tunnistenumero on 17. TCP - protokollan numerona toimii 60 ja UDP - protokollan numero on 170. Hyvä on myös tietää IPv6 – järjestelmän numero joka on 101. Näiden edellä mainittujen protokollien lisäksi muun muassa GRE -, ESP-, AH- ja OSPF – protokollat ovat melko yleisiä.

2.1 DNS – Domain Name System ja Reverse – DNS

DNS eli domain name system tarkoittaa nimipalvelinjärjestelmää, joka muuntaa IP - osoitteen selväkieliseksi osoitteeksi. Tämä toimenpide helpottaa käyttäjän toimintaa, sillä selväkielinen osoite, kuten www.samk.fi, on helpompi muistaa, kuin kyseistä osoitetta vastaava looginen IP – osoite 193.166.40.9. Nimipalvelu on käsitteenä yksi hajautettu ja varmennettu hierarkinen eli puumainen tietokanta. Puun ylimpänä on juuri, jonka alapuolella on päätaso eli maataso ja sen alapuolella 2 – taso eli organisaatiotaso. Tämänkin alapuolella voi olla vielä tasoja, esim. 3-taso eli aliorganisaatiotaso, mutta nämä eivät enää ole nimipalvelun kannalta välttämättömiä. Nimipalvelinjärjestelmä koostuu seuraavista komponenteista; resolveri, resolvoiva nimipalvelin, juurinimipalvelin, autoratiivinen nimipalvelin ja primäärinimipalvelin. Sekundääripalvelin, master – palvelin, caching – only palvelin, forwarderi ja slave ovat komponentteja, jotka eivät ole nimipalvelujärjestelmän toiminnan kannalta välttämättömiä.(Casad & Willsey, 1999, 203 & 210 - 214)

Kun työaseman käyttäjä tekee nimipalvelupyynnön, eli menee selaimellaan esimerkiksi osoitteeseen www.samk.fi, hänen työasemansa resolveri välittää kyselyn koneen TCP / IP – asetuksissa määritellylle nimipalvelimelle eli resolvoivalle nimipalvelimelle. Jos kyseessä on iso yritys, tämä palvelin on yleensä paikallinen palvelin, mutta esimerkiksi kotikäyttäjillä ei ole mahdollisuuksia omaan DNS – palvelimeen. Selvitettyään vastauksen kyselyyn, resolvoiva ni-

mipalvelin tallentaa sen välimuistiinsa (cache) ja seuraavalla kerralla hakee sen sieltä. Välimuistiin tallentaminen nopeuttaa nimikyselyihin vastaamista, koska resolvoivan palvelimen ei tällöin tarvitse hakea joka kertaa vastauksia maailmalta monen eri palvelimen kautta. Jos resolvoivan nimipalvelimen välimuistista ei löydy vastausta, se lähtee hakemaan sitä ensimmäisenä juurinimipalvelimelta. Tämä jälkeen juurinimipalvelin ohjaa kyselyn maatason tunnuksista vastaavalle nimipalvelimelle eli autoratiiviselle nimipalvelimelle. Tämä palvelin taas tietää mistä löytyy samk.fi – tunnuksen autoratiivinen nimipalvelin. Tämä nimipalvelin osaa lopulta kertoa haettua tunnusta vastaavan IP – osoitteen. (Casad & Willsey, 1999, 210 - 214)

Normaalin nimipalvelujärjestelmän sijaan, voidaan käyttää myös DDNS – palvelua, eli dynaamista nimipalvelua. Tämä palvelu antaa mahdollisuuden huomata reaaliajassa osoitteenmuutokset ja näin ollen ne pystytään myös talletamaan nimipalveluun. Dynaamisen nimipalvelun tapauksessa ratkaistaan muuttuvan IP – osoitteen ongelma. Muuttuvalle osoitteelle saadaan kuvaava ja helpommin muistettava nimi. Dynaaminen nimipalvelu mahdollistaa www - palvelimen pitämisen kotikoneella, jonka IP – osoite vaihtelee aika ajoin. Dynaamisen nimipalvelun avulla voi osoittaa nimen tiettyyn koneeseen tai laitteeseen, jossa on dynaaminen IP – osoite.

Nimipalvelujärjestelmän toiminta on korostunut nykypäivänä ja korostuu entisestään, kun siirrytään vähitellen IPv4 – käytännöstä IPv6 – käytäntöihin eli pitkiin IP – osoitteisiin. Tämä käytäntö tuo lisää IP – osoitteita, joten ne eivät tule loppumaan kesken. Näin voisi tapahtua, jollei IPv6 – käytäntöä olisi kehitetty. IPv6 on siis kehitetty korjaamaan IPv4 – käytännön ongelmakohdat, joista suurin on laitekohtaisten loogisten IP – osoitteiden loppuminen. Vaikka osoitemuunnokset ja osoitteiden uudelleenkäyttö helpottavat ongelmaa, eivät ne sitä ratkaise.

Reverse – DNS eli käänteisnimipalvelu toimii kuten normaali DNS, mutta käänteisesti, tämän palvelun avulla voidaan etsiä jonkin koneen nimi IP – osoitteen avulla. Käänteisnimipalvelu on normaalin nimipalvelun ohella myös puurakenteinen ja hierarkinen. Käänteisnimipalvelun juuripalvelin on in-addr-

arpa. Tämän juuripalvelimen alapuolella on kolme domain – tasoa, jotka edustavat IP – osoitteessa olevia kolmea ensimmäistä numeroa eli tavua. Esimerkiksi IP – osoitteessa 193.166.40.9 nämä kolme ensimmäistä tavua ja domain – tasoa ovat 193, 166 ja 40. Jos resolverilla siis onkin IP – osoite jota vastaavan nimen se haluaa tietää, lähtee se etsimään vastausta käänteisnimipalvelun juuripalvelimelta ja sen jälkeen vastauksen saatuaan, etsii alemmilta tasoilta. (Casad & Willsey, 1999, 216)

Nimipalvelu ja käänteinen nimipalvelu ovat verkon peruspalveluita, jotka pitää löytyä joko sisäverkon puolelta tai operaattorin tarjoamana ulkoverkon puolelta. Ilman näitä palveluja ei verkosta toimivaa saada. Viime aikoina nimipalvelinjärjestelmien turvallisuutta on koeteltu niihin kohdistuneiden hyökkäysten takia, mutta ainakin toistaiseksi isompaa haittaa ei ole onnistuttu tekemään.

2.3 DHCP – Dynamic Host Configuration Protocol

DHCP eli dynamic host configuration protocol on verkkoprotokolla, jota käytetään IP – osoitteen konfigurointiin. DHCP – protokollan tärkein tehtävä on antaa looginen IP – osoite verkkoon kytkeytyvälle tietokoneelle. DHCP – protokolla voi välittää käyttäjälle myös muita tietoja, kuten aliverkon maskin, oletusyhdyskäytävän osoitteen ja nimipalvelimen tai – palvelimien osoitteet. DHCP – protokollalla on kolme erilaista määrittelytapaa, jotka ovat automaattinen määrittely, dynaaminen määrittely sekä käsin määrittely. Automaattinen määrittely tarkoittaa sitä, että koneelle joka DHCP – palvelulta pyytää IP - osoitetta, saa osoitteen automaattisesti, ilman käyttäjän toimia. Dynaaminen määrittely tarkoittaa, IP - osoitteen antamista vain tietyksi ajaksi. Dynaaminenkaan määrittely, ei edellytä käyttäjän toimia. (Anttila, 2001, 202 – 203)

Käsin määrittely tarkoittaa sitä, että verkon ylläpitäjä määrittää manuaalisesti pysyvät osoitteet palvelimelle, käytettäväksi tietyn tietokoneen kanssa. Ylläpitäjä voi yhdistää käyttäjän koneen tai muun verkon laitteen verkkokortin MAC

- osoitteen ja tietyn IP – osoitteen toisiinsa. Tämä toiminto mahdollistaa pysyvästi määritellyn IP – osoitteen käytön kyseisessä koneessa tai laitteessa. Yleisin DHCP - protokollan määrittelytapa on dynaaminen määrittely. Käsin määrittelyä käytetään vain tietyissä erikoistapauksissa. Käytännössähän dynaaminen ja automaattinen määrittelytapa ovat samanlaisia, mutta dynaamisessa määrittelyssä koneelle, voidaan antaa muuttuvia parametreja, kuten oletusyhdyskäytävä tai nimipalvelin. Myös käytettäessä käsin määrittelyä, voidaan tietokoneella antaa muita parametreja kuten yllä mainitut nimipalvelimen tai – palvelinten osoitteet sekä oletusyhdyskäytävän osoite. (Anttila, 2001, 202 – 203)

DHCP – palvelu on nimipalvelujärjestelmän ohella pakollinen osa niin tilapäisen kuin pysyvänkin verkon palveluita. DHCP – protokollan avulla tietokoneet saavat siis loogiset IP – osoitteet, joilla laitteet tunnistavat toisensa ja kommunikoivat toistensa kanssa verkossa. Tämä protokolla voi myös jakaa muitakin tietoja kuten aliverkon peitteen, jonka DHCP myös yleensä jakaa IP – osoitteen jakamisen ohella.

2.4 Reititys

Reititys tarkoittaa TCP / IP – maailmassa sanomien ohjausta oikeisiin paikkoihin. Tämän hoitavat tehtävään erikoistuneet laitteet, reitittimet. Reitityksen yleensä hoitaa palomuuri, kytkin tai ADSL – modeemi, riippuen minkälainen ja kokoinen verkko on kyseessä. Yleensä reitittimillä on kaksi liityntää, yksi sisäverkon puolelle ja toinen ulkoverkon puolelle. Reititin reitittää IP – liikennettä IP – paketissa olevan vastaanottajan osoitteeseen. On olemassa kahdenlaisia verkkoprotokollia joiden avulla paketit internet – maailmassa liikkuvat, reititettäviä ja reitittämättömiä. Tunnetuin ja käytetyin reitittävä protokolla on TCP / IP protokolla, kun taas yleisin reitittämätön protokolla on NetBEUI, tosin sitä ei enää käytetä yksinään, vaan se kuljetetaan TCP / IP – protokollan päällä. Tässä opinnäytetyössä toteuttavassa verkossa käytetään TCP – IP – protokollaa. (Anttila, 2001, 263 – 266)

Reitittävä ja reitittämätön protokolla eroaa toisistaan siinä, miten verkkoja rakennetaan ja kuinka suuria ne voivat olla. Reitittämättömän verkon suurimmaksi ongelmaksi muodostuu yleensä levitysviestien eli broadcast - liikenteen hallitsematon tulva, joka tarpeeksi suuressa verkossa haittaa verkkoon kytkettyjen koneiden suorituskykyä. Myös reitittämättömien protokollien kohdalla käytettävä verkkotekniikka asettaa rajoituksia sekä verkkoon liittyvien koneiden määrään että verkon fyysiseen kokoon. Reitittävässä protokollassa ei edellä mainittuja ongelmia ole, koska reititin poistaa koko- ja levitysviestiongelmat. Tämä johtuu siitä, että yleensä levitysviestit ovat paikallisia, eikä reititin välitä niitä muihin verkkoihin. Yleensä IP – osoitepyyntöjä ei välitetä eri verkkojen välillä, jos kuitenkin näin täytyy toimia, tulee käyttää DHCP – relay ominaisuutta. Tämän ominaisuuden avulla DHCP – pyynnöt saadaan kuljetettua eri verkkojen välillä.(Anttila, 2001, 263 – 266)

Reititin toimii OSI – mallin verkkokerroksella ja ohjaa eri protokollien paketit verkkoprotokollan osoitteen mukaan kohti tiedossa olevaa kohdetta. Reititin on riippuvainen verkkoprotokollista ja sen tehtävänä on muun muassa kuunnella verkon liikennettä ja käsitellä sen osoitteella lähetetyt protokollapaketit. Reitittimen tehtäviin kuuluu myös levittää tietoa muille reitittimille tuntemistaan aliverkoista käytetyn reititysprotokollan mukaisesti. Osa protokollista lähettää tiedot kaikille verkon reitittimille, osa vain lähimmille reitittimille eli naapurireitittimille. Reitittimen tulee määrittelyjensä ja muilta reitittimiltä saamiensa tietojen perusteella laskea optimaalisin reitti kohdeverkkoihin. Jokaisen eri reitin valintaperusteet riippuvat aina käytettävästä reititysprotokollasta. Reititin myös muuttaa reititettävien pakettien kohdeosoitteiksi aina seuraavan reitittimen osoitteen sekä vähentää reititetyn paketin elinaikalaskuria eli Time To Live – arvoa. Tämä arvo kertoo kuinka kauan paketti on vielä elossa. Jokainen reititin vähentää TTL – arvoa yhdellä. (Anttila, 2001, 205 - 207)

Reitittimellä on myös muita tehtäviä kuten saantilistan (Access Table) tarkistus, kohteen mahdollisen siirtoyhteyskerroksen osoitteen selvittäminen sekä protokollapinon mukaisen hallinta- ja virhesanomien vastaanottaminen. Myös lähettäminen sekä hallintapäätteeltä ja – asemalta tulevien viestien vastaanot-

taminen ja toimiminen niiden mukaan kuuluu reitittimen tehtäviin. Reitittimen tulee mahdollisesti myös toteuttaa lisäpalvelut, joista yleisimpiä ovat siltaus, protokollatunnelointi, yhdyskäytävätoiminnot ja pakettien sovellustason suodatus. (Anttila, 2001, 206 - 207)

2.5 Palomuuri & Osoitteenmuunnos

Palomuurin tarkoituksena on olla järjestelmä, joka on suojattavan sisäverkon ja vaarallisen ulkoverkon välissä. Palomuurin tehtävänä on tutkia ja valvoa kaikkea saapuvaa ja lähtevää liikennettä. Se soveltaa verkon liikenteelle sille asetettuja sääntöjä, joiden perusteella se joko sallii yhteyden sisäverkkoon tai estää yhteyden. Palomuurit osaavat suodattaa liikennettä IP – lähde- ja kohdeosoitteiden, protokollan ja yhteyden perusteella, eli palomuuri voi toimia pääsylistoilla. Pääsylistat voivat olla standardeja pääsylistoja tai laajennettuja pääsylistoja. Standardi IP – pääsylista tarkistaa reititettävien pakettien lähdeosoitteen ja tästä saadut tulokset sallivat tai kieltävät ulosmenon koko IP – protokollaperheeltä, verkko-, aliverkko-, tai isäntäosoitteen perusteella. Laajennettu pääsylista tarkistaa sekä lähde- että kohdeosoitteen. Laajennetut listat voivat myös etsiä tiettyjä protokollia, porttinumeroita sekä muita parametreja. Paketin ulostulo voidaan joko sallia tai kieltää sen lähtöpisteen tai kohteen perusteella. (Thomas, 2005, 157 – 158 & 161 – 162, Chappel, 1999, 309)

Palomuuri voi myös suodattaa liikenteen pakettisuodatuksena. Oletuksena palomuurit sallivat kaikki luotetusta lähteestä, eli sisäverkon puolelta tulevan liikenteen, joka menee ulkomaailmaan. Palomuurit osaavat kirjata lokeihin tiettyjä sääntöjenmukaisuuksia yhteysyrityksistä, jotka aiheuttavat hälytyksiä. Palomuureilla on myös yleisesti käytössä oleva ominaisuus, NAT eli network address translation eli osoitteenmuunnos. Kyseinen ominaisuus muuntaa sisäverkon osoitteet julkisiksi osoitteiksi. Tällä tavalla säästetään IP – osoitteita ja annetaan mahdollisuus useille tietokoneille päästä samanaikaisesti ulkoverkkoon vain yhdellä julkisella IP - osoitteella palomuurin takaa. NAT – ominai-

suus myös piilottaa sisäverkon osoitteet ulkoverkolta, lisäten verkon tietoturvaa.. (Thomas, 2005, 161 - 162)

NAT – ominaisuudessa on siis kyse osoitteenmuunnoksesta. Se voidaan hoitaa kolmella eri tavalla, staattisella NAT – toiminnolla, dynaamisella NAT – toiminnolla tai Porttimuunnoksella eli PAT – toiminnolla toiselta nimeltään NAT – overloading - muunnoksella. Staattinen osoitteenmuunnos suorittaa yksityisen IP - osoitteen muunnoksen julkiseksi IP – osoitteeksi yksi osoite kerrallaan. Tämä on erittäin hyödyllinen ratkaisu silloin, kun verkon ulkopuolelta tulee olla pääsy laitteeseen, joka on verkon sisäpuolella. Eli reitittimelle on konfiguroitu tietty määrä julkisia IP – osoitteita, jotka vastaavat sisäverkossa käytettäviä osoitteita. Julkisten IP – osoitteilla ja sisäverkon IP - osoitteilla on reitittimessä selkeä yhteys, jonka avulla reititin osaa ohjata liikenteen oikeaan IP - osoitteeseen. (Thomas, 2005, 101 - 103)

Dynaaminen osoitteenmuunnos suorittaa yksityisen sisäverkon IP – osoitteen muunnoksen julkiseksi osoitteeksi tietystä rekisteröityjen IP – osoitteiden ryhmästä. Tämä ryhmä on valmiiksi määritelty tätä muunnostapaa varten. PAT - muunnos kehitettiin dynaamisen NAT – muunnoksen ongelmien takia. Ongelma syntyy, kun käyttäjän koneen sisäverkon IP – osoitteelle on tehty osoitteenmuunnos ja käyttäjä on päässyt ulkoverkkoon. Kun toinen käyttäjä tällöin yrittää päästä ulkoverkkoon ja saada sisäverkon osoitteelleen osoitteenmuunnosta, se ei onnistu ellei palomuurille ole määritelty useampia julkisia IP – osoitteita. Näin vain yksi käyttäjä kerrallaan pääsee ulkoverkkoon, joka ei ole hyvä ratkaisu verkon toimivuuden kannalta. PAT – muunnos suorittaa osoitteenmuunnoksen siten, että se muuntaa useita yksityisiä IP – osoitteita, yhdeksi julkiseksi osoitteeksi. Tämä tapahtuu useita TCP – portteja käyttämällä. PAT – muunnos on erittäin hyvä tapa hoitaa osoitteenmuunnos, koska yhdellä IP – osoitteella voi olla käytettävissä yli 64 000 porttia ja näin ollen saadaan monelle käyttäjälle sallittua yhteys yhden julkisen IP – osoitteen takaa yhtäaikaisesti. Tämä osoitteenmuunnoksen tyyppi on yleisimmin maailmalla käytetty, koska se palvelee suuria käyttäjämääriä kerralla. (Thomas, 2005, 101 - 103)

NAT – ominaisuuden ollessa päällä, verkosta ei näy ulos kuin yksi IP – osoite. Kun on olemassa yksi julkinen IP – osoite ja NAT – ominaisuus on käytössä, toimii ulkoverkkoon pääsy seuraavasti, ulkomaailmaan haluava laite lähettää sanoman reitittimelle, joka useimmissa tapauksissa on sama kuin palomuuri. Vastaanottaessaan pyynnön, reititin vaihtaa alkuperäisen sisäverkosta tulleen IP – osoitteen tilalle ulkoverkossa käytetyn julkisen IP - osoitteen. Sisäverkkoon päin reititys tapahtuu tällä ulkoverkossa hyväksytyllä osoitteella, jonka reititin osaa kääntää ennalta asetettujen asetusten mukaisesti sisäverkon osoitteeksi ja osoittaa oikealle laitteelle. (Anttila, 2001, 86)

2.6 Kaistanhallinta

Tällä tarkoitetaan verkkoa hidastavan liikenteen hallitsemista niin, että kaikilla käyttäjillä olisi tasapuolisesti ulkopuolelta tulevaa kaistaa käytössään. Kaistanhallinta toteutetaan yleensä erillisellä laitteella, kuormantasaajalla. Tämä laite voi tasata verkon liikenteen muun muassa yhteyskohtaisesti tai pakettikohtaisesti. Pakettikohtainen liikenteenhallinta on tarkempaa kuin yhteyskohtainen. Tämä johtuu siitä, että yhteyskohtaista hallintaa käytettäessä jokaisesta TCP – yhteydestä otetaan tuhansien pakettien joukosta vain muutama näyte, joiden perusteella päätetään, miten kyseistä yhteyttä käsitellään. Tästä johtuu, että yhteyskohtaisen liikenteenhallinnan säädön tarkkuus on vain murto – osa pakettikohtaisen hallinnan vastaavasta.

Kaistanhallintaa kannattaa käyttää, sillä jos tätä ominaisuutta ei ole verkossa käytössä ja tällöin käyttäjä lataa P2P – sovellusta käyttäen tiedostoa monta rinnakkaista TCP – yhteyttä käyttäen, muille käyttäjien verkon käyttö hidastuu huomattavasti. Se johtuu siitä, että TCP – yhteyksiä voi P2P – sovelluksia käytettäessä ottaa kymmeniä tuhansia yhtä aikaa. Jos tässä tapauksessa käytetään yhteyskohtaista liikenteenhallintaa eli laitetaan jokaiselle TCP – yhteydelle kiinteä kaistarajoitus, tilanne muuttuu paljon huonommaksi. Pakettikohtaisessa hallinnassa kyseistä ongelmaa ei tule, koska se on dynaamista, jonka ansiosta pystytään hyödyntämään koko käytettävissä oleva kaista kaiken ai-

kaa. Tällöin jos ei koko kaista ole käytössä, voidaan sitä jakaa muille käyttäjille ja sovelluksille, kuten juuri P2P – sovelluksille.

Tietyissä liikenteenhallintaan tarkoitetuissa laitteissa on ominaisuutena reilu kaistanjako – toiminto toiselta nimeltään diplomat – toiminto. Tämä ominaisuus päällä ollessaan jakaa kaistaa automaattisesti tarpeen mukaan. Etusijalla on normaalisti vähän kaistaa käyttävät käyttäjät. Kaiken aikaa jokaisella käyttäjällä on kaistaa käytössään heidän tarvitsemansa määrä. Ruuhka – aikana ei välttämättä näin ole, sillä silloin kaistaa otetaan pois käyttäjiltä joilla on eniten kaistaa käytössään. Tästä huomataan, että liikenteenhallinta - laitteet, kutsutaan niitä kuormantasaajiksi tai kaistanhallitsijoiksi toimivat eri tavalla ruuhka – aikana ja aikana jolloin verkossa on vähän liikennettä.

Liikenteenhallinnalla voidaan estää verkon ylikuormittaminen vertaisverkko – eli niin sanottujen P2P – sovellusten liikenteeltä. Voidaan myös järjestää oma kaista esimerkiksi tietokantasovelluksille, jotka tarvitsevat paljon kaistaa. Myös voip – ja videokonferenssiyhteyksille sekä valvontajärjestelmille voidaan järjestää oma kaista. Tällaisella laitteistolla voidaan hallita liikennettä niin sisään, kuin ulospäin. Tämänlainen liikenteenhallinta molempiin suuntiin voidaan toteuttaa lähde – tai kohdeosotteiden tai ip – osoiteryhmien mukaan sekä protokollien kuten ICMP, TCP ja UDP mukaan. Myös porttien perusteella voidaan kaistaa jakaa käyttäjille. (Lehto, 2004)

2.7 STP - Spanning Tree Protocol

STP eli Spanning Tree Protocol on protokolla, joka estää silmukoiden syntymistä verkkoon. Tämä tapahtuu STP – protokollassa toimivalla spanning tree – algoritmilla. Se estää silmukat laskemalla vikasietoiselle verkolle pysyvän spanning tree – topologian eli se muokkaa verkon loogisesti väylämäiseksi. Vikasietoisia verkkoja toteutettaessa tulee kaikkien verkossa olevien ethernet – solmujen välillä olla silmukoista vapaa polku. Edellä mainittu spanning tree

– algoritmi laskee kyseisen silmukkavapaan polun verkkoon. Spanning Tree Protocollan käyttöönotossa ja käytössä pitää huomioida viive, joka syntyy algoritmin laskiessa silmukkavapaan polun verkkoon. Välitysviive eli forward delay – parametri tarkoittaa aikaa, joka menee verkon palauttamiseksi toimintakuntoon topologiamuutoksen jälkeen. Tälle parametrille voidaan määritellä käsin aika, jonka halutaan menevän verkon palauttamiseen. Hello time eli mainosviestien lähetysväli kertoo ajan kuinka usein spanning tree protocol – protokollaa käyttävät laitteet viestittävät olemassaolostaan toisilleen. (Cisco, 2002, 57, Jaakohuhta, 2000, 183 – 184)

Laittaessaan osan yhteyksistä odotustilaan, STP havaitsee silmukan ja samalla se myös poistaa silmukan. Kun kytkimissä on käytössä Ethernet tai Fast Ethernet – pohjainen VLAN, on käytössä myös STP – protokolla. Jokaisessa konfiguroidussa VLAN:ssa on käytössä oma STP – protokollansa. Tällä varmistetaan, että kaikki verkon ethernet – topologiat noudattavat standardia. (Cisco, 2002, 57)

STP:n etuna voidaan pitää sitä, että se voidaan asettaa koskemaan myös koko verkkoa. STP on yhteensopiva eri laitevalmistajien laitteiden kesken ja se myös tunnistaa verkossa tapahtuvat topologia – eli rakennemuutokset, kun se on käytössä verkon osassa, jossa muutos tapahtuu. STP:tä kannattaa käyttää vain sellaisessa verkon osassa tai sellaisessa verkossa, jota halutaan hallita STP:n avulla. Sellaisissa verkoissa, joissa on laitteita, jotka eivät tue uusia ja kehittyneitä vianhallintaominaisuuksia, STP on yleensä ainoa mahdollisuus hallita näitä verkkoja. Lähiverkon tulee olla vikasietoinen, jotta siihen kytketyt laitteet voidaan saada toimimaan toistensa kanssa ja ettei verkossa tai sen laitteiden yhteensopivuuksissa esiintyisi muita ongelmia. Spanning tree protocol – protokollan ongelmana voidaan pitää sen varsin hidasta kytkeytymisaikaa eli niin sanottua failover – aikaa, joka on 30 – 90 sekuntia. (Jaakohuhta, 2000, 183)

Käytössä olleessaan STP – hallinta-aluetta hallitsee joko juurisilta tai juurikytkin. Näistä laitteista lähtien, STP alkaa rakentaa verkkoon puumaista hierarkiaa. Tämä menettely huolehtii siitä, että verkossa on vain yksi toimiva yhteys

eri laitteiden välillä. Spanning Tree protokollasta on olemassa erilaisia evoluutioita ja lisäosia. Näitä ovat muun muassa RSTP eli Rapid Spanning Tree Protocol, joka on käytössä Insomnia - tapahtumassa. Muita evoluutioita tai lisäosia ovat Per – VLAN Spanning Tree, Multiple Spanning Tree Protocol sekä Rapid Per – VLAN Spanning Tree. (Jaakohuhta, 2000, 183)

2.8 VLAN - Virtual Local Area Network

”VLAN eli virtuaalinen lähiverkko on looginen joukko verkkolaitteita tai käyttäjiä, joita ei ole rajattu tiettyyn fyysiseen kytkinsegmenttiin” (Cisco, 2002, 56). Virtuaalisessa lähiverkossa olevat laitteet tai käyttäjät voidaan ryhmitellä muun muassa toiminnon, osaston tai sovelluksen perusteella riippumatta siitä missä ne fyysisesti sijaitsevat. Normaalisti kytkin jakaa lähiverkon fyysisesti erillisiin törmäysalueisiin, kaikkien alueiden ollessa samaa yleislähetysaluetta. VLAN – ominaisuuden ollessa toiminnassa se muodostaa yhden yleislähetysalueen, jota käsitellään yhtenä aliverkkona. Kyseinen muodostettu yleislähetysalue, ei jakaudu fyysisiin osiin. (Cisco, 2002, 56)

Virtuaalinen lähiverkko voidaan toteuttaa porttikeskeisesti, dynaamisesti tai staattisesti. Porttikeskeisessä vaihtoehdossa kaikki saman virtuaalisen lähiverkon portteihin kuuluvat solmut, saavat saman VLAN ID – tunnisteen. Tämä helpottaa verkon valvontaa ja tehostaa verkkoa, koska käyttäjät on porttikohtaisesti määritelty. Tällöin virtuaalisten lähiverkkojen hallinta on helppoa ja eri virtuaalisten lähiverkkojen välille muodostuu tietosuoja, joten VLAN parantaa tietoturvaa, eikä verkossa liikkuvat paketit ”vuoda” muille VLAN – alueille. Staattiset virtuaaliset lähiverkot ovat kytkimen yksittäisiä portteja, jotka määritellään pysyvästi tiettyyn virtuaaliseen lähiverkkoon. Portit säilyttävät VLAN – asetuksensa, kunnes niitä muutetaan. Staattiset virtuaaliset lähiverkot vaativat verkonvalvojan toimia, mutta ne ovat turvallisia ja helppoja konfiguroida, mutta myös selkeästi hallittavissa. (Cisco, 2002, 71 - 72)

Dynaamiset virtuaaliset lähiverkot ovat kytkimen portteja, jotka osaavat itse automaattisesti päätellä mihin virtuaaliseen lähiverkkoon ne kuuluvat. Tämän tyyppisen virtuaalisen lähiverkon toiminnat perustuvat MAC – osoitteisiin, loogisiin osoitteisiin tai protokollatyyppeihin. Virtuaalisten lähiverkkojen käytöstä saadaan erilaisia hyötyjä. Muun muassa hallinnolliset kustannukset, jotka aiheutuvat erilaisista siirroista, lisäyksistä tai muutoksista syntyvissä ongelmista, pienenevät. VLAN – ominaisuus tarjoaa mahdollisuuden yleislähetyksen hallintaan, sekä työryhmille että koko verkolle tietoturvallisuutta. (Cisco, 2002, 72 - 73)

Virtuaalisen lähiverkon toteutustavat määrittelee IEEE standardi 802.1Q. Virtuaaliverkot jakautuvat 1 tason, 2 tason, 3 tason ja korkeamman tason verkkoihin. Tason yksi - virtuaaliverkot ovat porttikohtaisia virtuaaliverkkoja, eli laitteen jäsenyys virtuaaliverkoissa perustuu porttinumeroon, johon laite on kytketty. Tällöin virtuaaliverkko pitää määritellä uudelleen kun käyttäjä siirtää laitteensa toiseen kytkimeen. Tason kaksi - verkot voivat perustua laitteiden MAC – osoitteisiin. Eri virtuaaliverkkoihin kuuluvista osoitteista pitää kirjaa kytkin. Käyttäjäkin voi vaihtaa laitteensa toiseen kytkimeen, mutta silti virtuaaliverkko pysyy samana. Kolmostason virtuaaliverkot perustuvat verkkokerroksen aliverkkoihin. Kolmostasolla virtuaaliverkkojen jäsenyys määräytyy IP – osoitteen aliverkko – osan perusteella. IEEE 802.1Q – standardin nykyversiossa ei ole määritelty kolmostason tai korkeamman tason virtuaaliverkkoja. Korkeamman tason virtuaaliverkkojen jäsenyys määräytyy dynaamisesti sovelluksen tai palvelun perusteella. Esimerkiksi siis HTTP – liikenne tai SMTP – liikenne voidaan ohjata omiin virtuaaliverkkoihinsa. (Puska, 2000, 104 - 106)

Virtuaalisen lähiverkon ollessa käytössä kytkimissä voidaan levitysviestit eli broadcast – liikenne sekä multimediasovellusten tuottama multicast - liikenne rajoittaa vain samaan virtuaalisen lähiverkkoon kuuluviin portteihin. Tällä tavalla saadaan levitysviestien kokoa pienennettyä ja levitysviestien aiheuttamaa verkon hidastumista lievitettyä. Lisäksi kun virtuaalinen lähiverkko on käytössä sen liikenne pitää reitittää, joten reitittimen suodatuslistoilla pystytään lisäämään verkon turvallisuutta.

Virtuaaliseen lähiverkkoon pohjautuvassa verkossa pystytään vähentämään reitittimen konfigurointia, sillä reititin osaa reitittää monesta virtuaalisesta verkosta peräisin olevan datan joko samasta tai eri liitännästä eri virtuaaliseen verkkoon. Tällöin vain kytkimen konfigurointia pitää muuttaa. Kytkin toimii yleensä virtuaalisen lähiverkon tapauksissa myös reitittimenä. Tällöin siitä käytetään nimeä reitittävä kytkin. Se siis muun muassa reitittää broadcast – ja multicast – liikenteen tietyn lähiverkon haluttuihin portteihin. Myös normaalissa käytössä oleva kytkin voidaan konfiguroida reitittäväksi kytkimeksi.

2.9 WLAN – Wireless Local Area Network

Langaton verkko on tarkoitettu myös datan siirtämiseen, kuten tavallinen verkko, mutta kun käytössä on WLAN, siirrettävä data siirtyy langattomasti paikasta toiseen ilman johtoja. Saadaksesi yhteyden langattomaan verkkoon, käytössäsi pitää olla kannettava tietokone sisäisen verkkokortin kanssa. Toinen vaihtoehto on pöytäkone, jossa on verkkokortti ja siihen liitetty langaton vastaanotin. Uusissa kannettavissa tietokoneissa on valmiina sisäinen verkkokortti jo valmiina mukana, mutta vanhempiin malleihin voi joutua ostamaan ulkoisen vastaanottimen, esimerkiksi USB – porttiin. Langattomasta lähiverkosta, joka on tarkoitettu yleisissä tiloissa kaikkien ihmisten käytettäväksi, käytetään kaupallista nimitystä Wi-Fi.

Langaton verkko voidaan toteuttaa kahdella eri tavalla. Ensimmäinen tapa on käytössä yleisesti kotitalouksissa. Tällä tavalla toteutetussa verkossa on ADSL – modeemi, jossa on valmiina langattoman verkon tukiasema. ADSL – modeemissa voi myös olla erikseen kiinnitetty WLAN – tukiasema. Kuten edellä mainittiin, pöytätietokoneet tarvitsevat tällaisessa tapauksessa vastaanottimen verkkokorttiinsa kiinni, jotta pääsevät langattoman tukiaseman kautta verkkoon. Pienemmät yritykset voivat käyttää myös WLAN – tukiasemia toteuttaessaan langattoman lähiverkon. Tukiasemia voi olla useampia samassa verkossa ja yleensä paremman kuuluvuuden saadakseen on käytettävä useita tuki-

asemia. Yleensä yhtä avointa tilaa kohden, riittää yksi tukiasema. Toinen tapa toteuttaa langaton lähiverkko on kontrolleriin perustuva ratkaisu. Tällä tavalla toteutetussa verkossa on langattoman verkon laite, niin kutsuttu kontrolleri. Se ohjaa tukiasemia ja niiden toimintaa verkossa. Tässä tapauksessa tukiasemilla ei ole itsellään tietoa verkon toiminnasta, vaan kontrollerilla asetetaan niihin asetukset ja hallitaan verkkoa. Tämä toteutustapa soveltuu paremmin isoihin verkkoratkaisuihin.

Yleisiä WLAN – standardeja on tällä hetkellä kolme, IEEE802.11a, IEEE802.11b sekä IEEE802.11g. Nämä standardit ovat virallisia, mutta on myös olemassa muitakin standardeja. Ensimmäinen standardi eli 802.11a on käytössä 5 gigahertsin taajuusalueella toimiville laitteille. Toinen standardi eli 802.11b on käytössä 2.4 gigahertsin taajuusalueella ja 11 megabittiä sekunnissa toimiville laitteille. IEEE802.11g - standardi on käytössä 2.4 gigahertsin taajuusalueella ja 54 megabittiä sekunnissa toimiville laitteille. Suurimmassa osassa nykyään myytävissä langattoman verkon laitteissa on käytössä IEEE802.11g – standardi. (Puska, 2000, 118 - 119)

WLAN – verkkoihin löytyy kaksi standardoitua salausmenetelmää, WEP - ja WPA – menetelmä. WEP – salausmenetelmä on ensimmäinen standardoitu salausmenetelmä. Se toimii hyvin peruskäyttäjiä vastaan, mutta on kuitenkin verrattain helposti murrettavissa, joten se ei ole yleistynyt yrityskäyttöön. WPA – salaus ja siitä kehitetty WPA2 – salausmenetelmä kehitettiin korvaamaan hyökkäyksille alttiiksi huomattu WEP – salaus. Langattoman verkon salaukseen sekä autentikointiin liittyy tiiviisti käsite SSID, joka on langattoman verkon tunniste. Tämän tunnisteen perusteella käyttäjät tunnistavat verkon johon ovat liittymässä.

2.10 Tilapäinen - ja pysyvä verkko

Tilapäinen verkko on kuten normaali lähiverkko, mutta on käytössä ennakkoon tiedossa olevan tietyn ajan. Tilapäisellä verkolla tarkoitetaan verkkoa, jota käytetään esimerkiksi tietyn tapahtuman ajan, jonka jälkeen verkko pure-

taan, eikä se ole enää käyttövalmiudessa. Pysyvä verkko on normaali lähiverkko, joka on toiminnassa jatkuvasti ja sen tulee olla valmiudessa joka päivä. Tilapäinen verkko tarvitsee samoja verkon laitteita kuin pysyväkin verkko. Näitä laitteita ovat kytkimet, reitittimet, palomuurit ja eri tarkoituksiin kuuluvat palvelimet. Tilapäinen verkko tarvitsee toimiakseen myös samat palvelut, kuin pysyväkin verkko.

Näitä palveluja ovat DHCP – protokolla, joka osoittaa laitteille IP – osoitteet. DNS – järjestelmä, joka muuntaa verkkolaitteiden loogiset IP – osoitteet selväkielisiksi nimiksi ja myös päinvastoin. Reititys – palvelu, joka hoitaa pakettien reitityksen verkossa sekä palomuuri – palvelu, joka suodattaa liikennettä sille annettujen asetusten mukaan.. Reititin ja palomuuri voivat toimia samassa laitteessa, mutta reititin voi myös sijaita kytkimessä tai ADSL - modeemissa. Olisi myös käyttäjien ja verkon toimivuuden kannalta hyvä käyttää kaistanhallinta – laitetta. Näin varmistetaan, että jokaisella käyttäjällä on tarpeellinen määrä kaistaa käytössään. Hyvänä esimerkkinä pysyvästä verkosta on yritysten sisäiset verkot. Nämä verkot ovat pysyviä ja käytössä juuri niin kauan, kun yritys muuttaa, lopettaa toimintansa tai muusta syystä päättää lakkauttaa verkkonsa. Hyvinä esimerkkeinä tilapäisistä verkoista ovat erilaisten messujen ja tapahtumien, kuten Cebit – messujen sekä Assembly – verkkopelitapahtuman tilapäiset verkot.

3 KÄYTÄNNÖNOSUUS (CASE INSOMNIA)

Opinnäytetyöni käytännön osuudessa suoritettiin verkon toteuttaminen ja tehtiin siihen liittyvät kuvat. Verkon autentikointi eli miten käyttäjä saa yhteyden internetiin ensimmäisen kerran on läpikäyty ja dokumentoitu. Tapa on ainutlaatuinen ja tällaisenaan ainoastaan Insomnia – tapahtumassa käytössä. Myös verkon ylläpito on dokumentoitu eli on otettu selvää minkälaisilla ohjelmilla

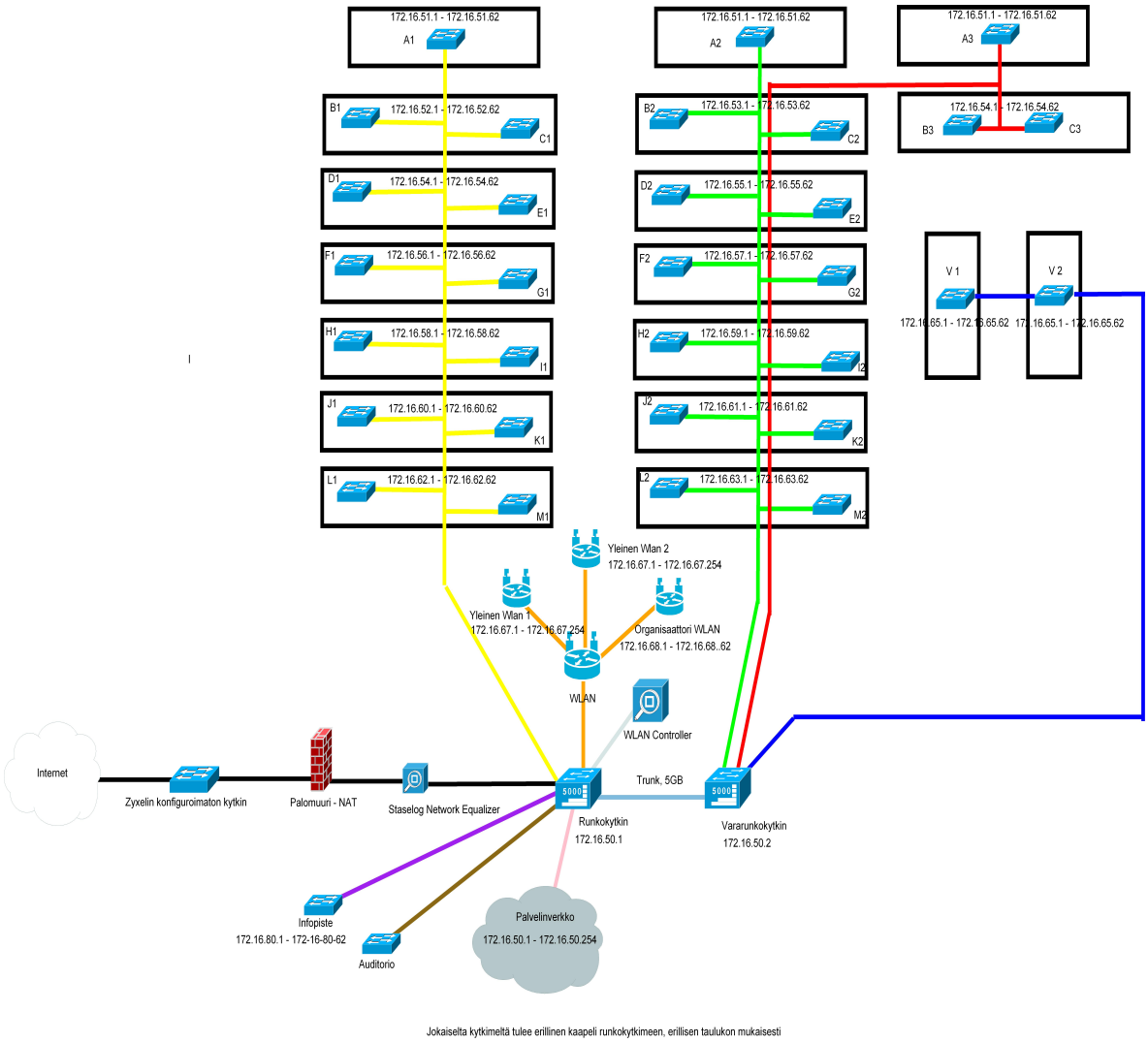
mitäkin osaa verkosta tutkittiin ja seurattiin. Työhön liittyvää verkon dokumentointia on kokonaisuudessaan tämä käytännönosuus.

3.1 Verkon dokumentointi

Tässä työssä tapahtuman verkosta dokumentoitiin sen fyysinen rakenne, reititys sisään ja ulos, tapahtuman ainutlaatuinen tapa autentikoida käyttäjä, langaton verkko sekä ylläpito. Verkosta tehtiin fyysinen kuva, Dia – piirto – ohjelmalla. Myös reitityksen toteuttamisesta ja autentikoinnin etenemisestä tehtiin samalla ohjelmalla verkkokuvat. Langaton verkko on osa verkon fyysistä kuvaa, näin ollen siitä ei tehty erikseen omaa kuvaa. Ylläpidon ohjelmista ja niiden toiminnasta saatiin erikseen kuvankaappauksia. Verkon fyysisessä kuvassa (Liite 1) on kuva koko verkosta. Reitityksessä (Liite 2 ja Liite3) ja käyttäjien autentikoinnissa (Liite 4), otettiin vain pieni osa verkkoa käsiteltäväksi kuvaan asian ymmärtämisen helpottamiseksi. Käytännön osuudessa on edellä mainituista kuvista pienennetyt versiot. Työn liitteenä ovat isommat ja selkeämmät kuvat.

3.2 Verkon kuvaus

Alla on verkon fyysinen kuva, josta käy ilmi verkon fyysinen rakenne ja verkon komponentit. Verkon peruselementteinä toimii runkokytkin ja sen varakytkin, sekä 31 käyttäjille osoitettua pöytäkytkintä. Verkossa on myös olennaisena osana palomuuri sekä kuormantasaaja (Staselog Network Equalizer), joka suoritti verkon liikenteen jakamisen tasaisesti kaikkien käyttäjien kesken. Verkossa oli myös palvelinverkko, jossa toimi muun muassa DHCP - ja DNS - palvelut, virtuaalisessa ympäristössä.



(Liite 1 Fyysinen verkkokuva)

Yllä olevasta kuvasta, käy myös ilmi että tapahtumassa on ollut käytössä langaton verkko. Se perustui kolmeen tukiasemaan ja yhteen langattoman verkon ”kontrolleriin”. Tukiasemat olivat konfiguroimattomia ja kontrollerin avulla tukiasemia ohjattiin ja niihin asetettiin halutut asetukset.

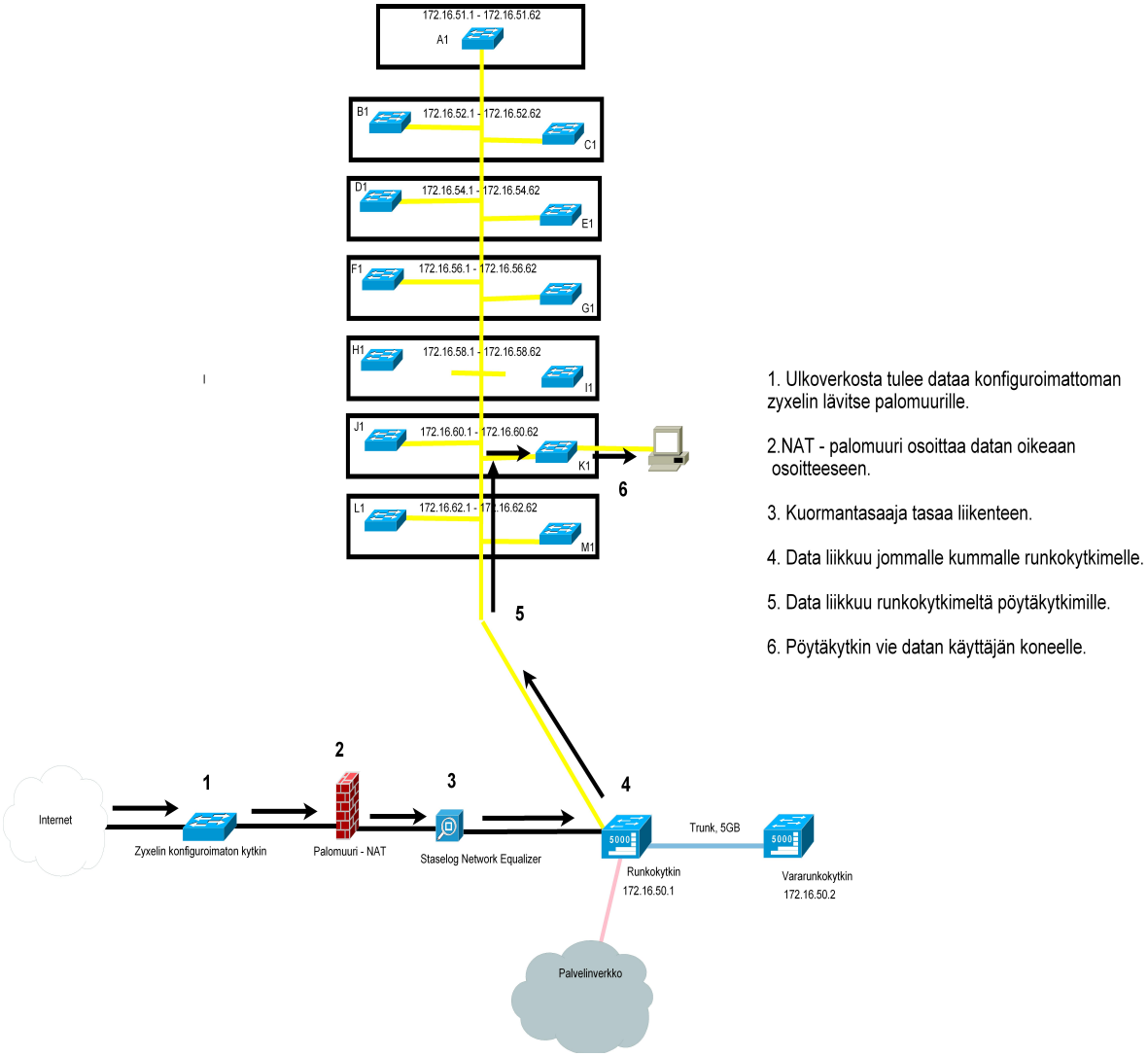
3.3 Verkon toteutus

Tapahtuman tilapäisen verkon toteuttaminen alkoi kaapeloinnilla. Ennen tapahtumaa oli tehty suunnitelma kytkimien sijoittamisista. Tämän suunnitelman perusteella oli etukäteen tehty määrämittaiset kaapelit sen perusteella, mi-

hin tietyt pöytäkytkimet sijoittuvat. Kaapeleiden molemmissa päissä oli merkintä, josta selvisi, mikä kaapeli oli kyseessä. Näin koko ajan tiedettiin, mikä kaapeli kuului mihinkin kohtaan. Tällä pyrittiin helpottamaan kaapelien vetoa paikalleen ja pyrittiin myös välttymään ylimääräiseltä kaapelinkulutukselta. Näin myös helpottui vianetsintä, jos kaapeleihin tulisi vikaa. Kaapelit vedettiin oikeille paikoilleen ja niputettiin toisiinsa kiinni sähköteipillä. Tämän jälkeen käytävien kohdalle jääneiden kaapeleiden päälle laitettiin ”cable cross” – kynnys, johon kaapelit saatiin siististi suojaan käyttäjien tallomiselta ja rikkoontumiselta.

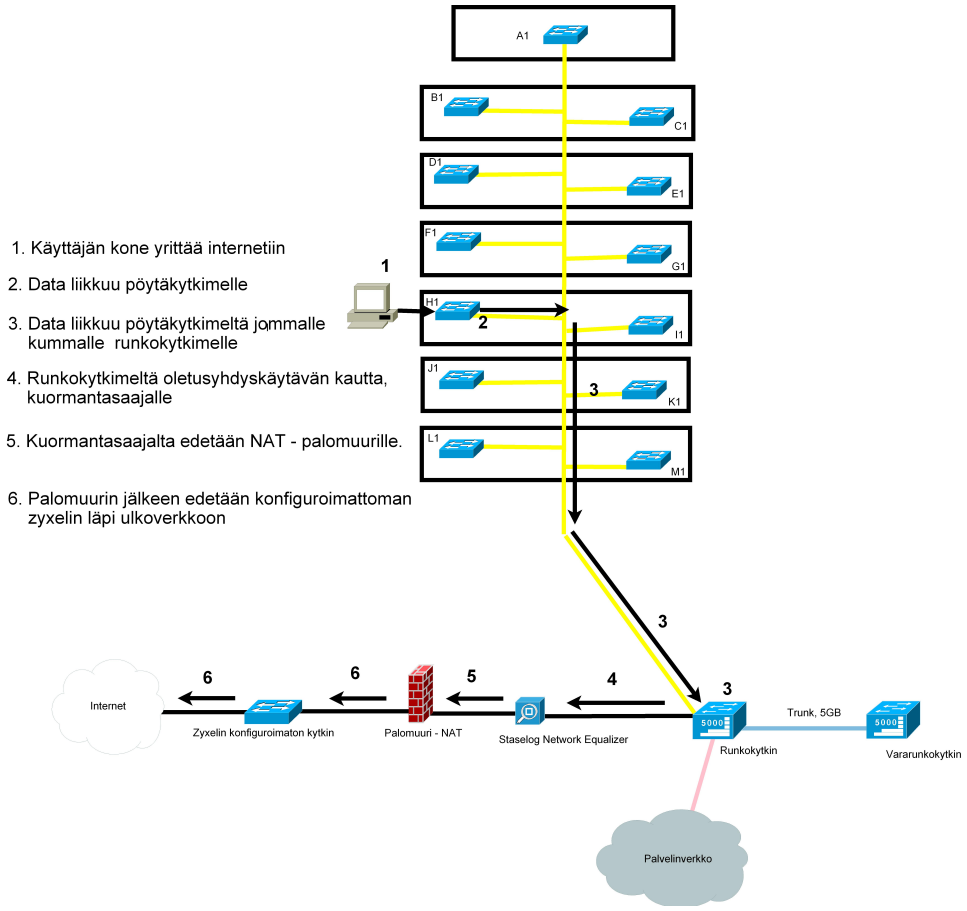
Ennen kuin kytkimet sijoitettiin oikeisiin pöytiinsä, niihin asetettiin niiden hallintaan käytettävä salasana sekä niiden portit määriteltiin niille kuuluviin VLANeihin. Portit jaoteltiin VLANeihin niin, että portit 1 - 23 pöydän VLANiin ja portti numero 24 oli varattu uplink – toiminnolle eli ulospäin menevälle liikenteelle. Jokaisessa kytkimessä oli kaksi VLANia, pöytä – ja hallinta - VLAN. Uplink – portti oli konfiguroituna sekä pöytä - että hallinta - VLANissa. Samalla kytkimiin määriteltiin RSTP eli Rapid – Spanning – Tree – Protocol – protokolla päälle. Tämän protokollan avulla verkon kytkimet ottivat yhden kytkimen juurisillaksi, jonka kautta reitti pöytäkytkimiltä eteenpäin vei. Tämän toimenpiteen avulla estettiin silmukoiden syntyminen verkkoon joka voisi aiheuttaa verkon liikenteen hidastumista tai liikenteen loputtoman kiertämisen verkossa.

Palomuurina toimi iptables – työkalulla konfiguroitu netfilter pakettisuodatin eli palomuuriratkaisu oli Linux – pohjainen. Kyseinen netfilter – suodatin on valmiina ominaisuutena Linuxin ytimessä ja iptables – työkalulla sitä konfiguroimalla saatiin tehokas palomuuri. Tällä tavalla toteutettu palomuuri toimii pakettisuodatuksella eli tietyt paketit pääsevät lävitse ja tietyt ei.



(Liite 2 Reititys sisäänpäin)

Reititys ulkomaailmasta käyttäjän koneelle tapahtui yllä olevan kuvan mukaan eli data liikkui päin vastaisessa järjestyksessä kuin ulkomaailmaan päin liikkuessaan. Konfiguroimattoman kytkimen jälkeen, data saapuu palomuurille, joka tarkastaa, että kyseessä on sallitulle käyttäjälle menevää sallittua liikennettä. Tämän jälkeen kuormantasaaja mahdollisesti tasaa liikennettä ja tutkii liikenteen laatua. Näiden operaatioiden jälkeen data liikkuu toiselle olemassa olevalle runkokytkimelle, joka ohjaa datan kaapeleita pitkin pöytäkytkimelle ja sieltä käyttäjän koneelle.



(Liite 3 Reititys ulospäin)

Reititys kulki käyttäjän koneelta internetiin yllä olevan kuvan mukaisesti. Käyttäjän liitettyä koneensa kytkimeen ja autentikoiduttuaan järjestelmään, hänen koneelta lähtevä data kuljetettiin pöytäkytkimen kautta kaapeleita pitkin runkokytkimelle. Sieltä data kuljetettiin oletusyhdyskäytävän kautta, kuormantasaajalle. Tämän jälkeen palomuurille tarkistaa, että kyseessä on sallitulta käyttäjältä tulevaa sallittua liikennettä. Tämän jälkeen data kuljetetaan konfiguroimattomalle kytkimelle, jonka lävitse data kulkee. Tämän kytkimen jälkeen yhteys on ulkomaailman puolella. Näin siis tapahtuu reititys käyttäjän koneelta ulkomaailmaan. Edellä reititys on kuvattu melko yksinkertaisella tavalla, sillä reitityksen eri vaiheissa eri laitteissa tapahtui lukematon määrä asioita, joiden selvittäminen tässä työssä ei ole olennaista eikä tarpeellista.

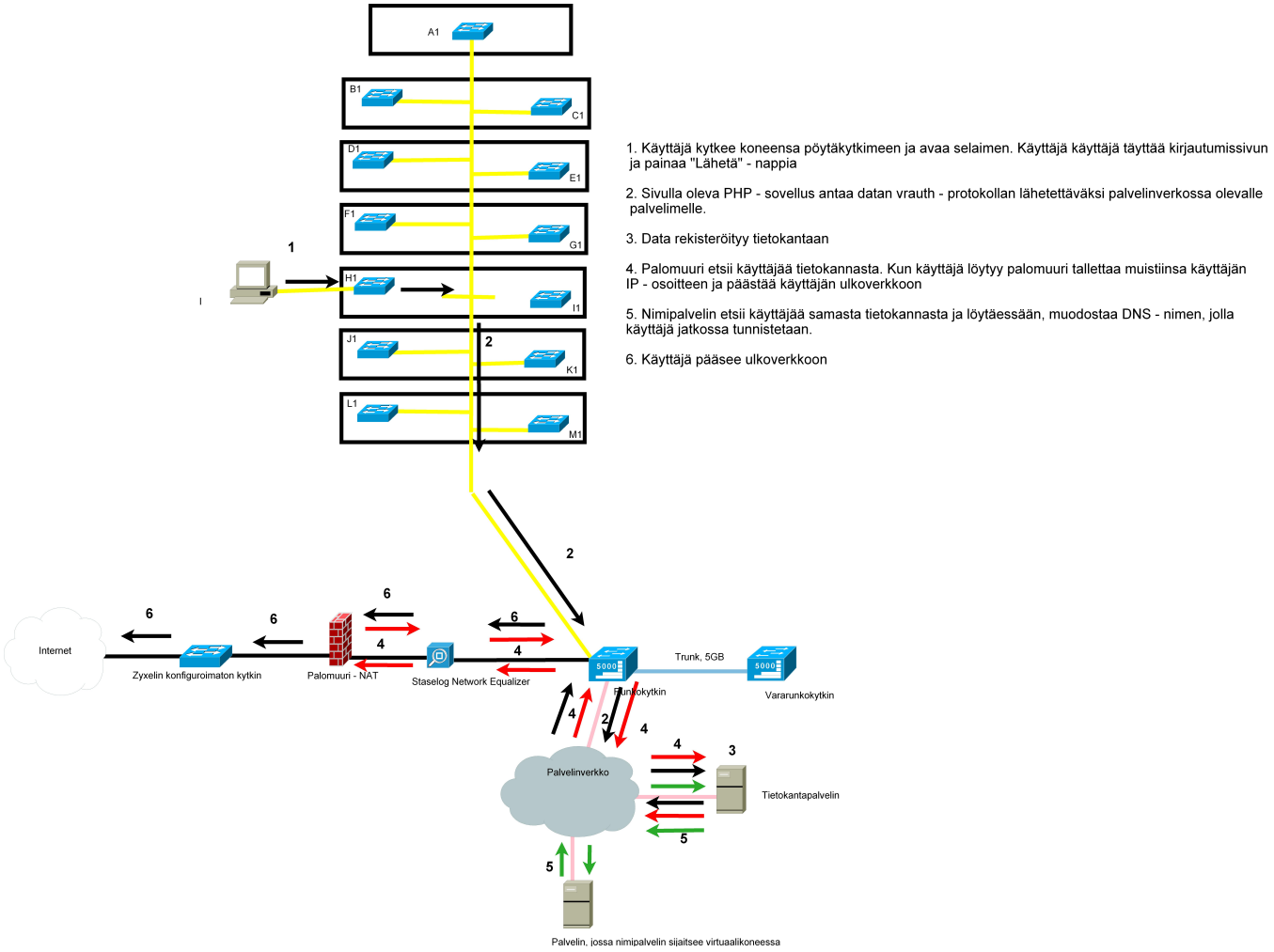
Verkossa käytettiin Staselog Network Equalizer – liikenteenhallintalaitetta, joka oikein asennettuna, jakoi verkon kaistaa tasaisesti kaikille käyttäjille ja sillä voitiin estää esimerkiksi kiellettynä olleen P2P – liikenne, joka aiheuttaa liikaa kuormaa verkolle. Staselog ei jakanut verkon kaistaa datamäärän tai prosenttimäärän mukaan, vaan sitä mukaa missä kaistaa tarvittiin, niin sinne sitä myös jaettiin. Verkon kaistan jakamisessa siis käytettiin Staselogin diplomat – toimintoa, eli reilua kaistanjakoa. Tämä toiminto jakoi kaistaa siten, että isoimmilta kaistarohmuilta saatettiin väliaikaisesti vähentää kaistan määrää ja antaa sitä muille. Kuitenkin niin, että kaikilla oli tarpeeksi kaistaa käytössään.

Langaton verkko toteutettiin tapahtumassa kolmella tukiasemalla ja yhdellä niin sanotulla WLAN – kontrollerilla. Käytössä oli siis kontrolleriin perustuva langaton lähiverkko - ratkaisu, jossa tukiasemissa ei ole asetuksia, vaan kontrolleri määrittää yhteyden asetukset ja hallinnoi tukiasemia. Tapahtuman käyttäjillä oli käytössään kaksi WLAN – tukiasemaa ja tapahtuman järjestäjille oli oma WLAN - tukiasema. Nämä asemat olivat kiinni satunnaisissa kytkimissä eri puolella tapahtumatilaa. Langattomassa verkossa oli SSID - ominaisuus käytössä, jonka avulla käyttäjät tunnistivat langattoman verkon johon liittyä. Verkon autentikointi tapahtui samalla tavalla, kuin normaaliinkin verkkoon liityttäessä, eli vrauth – protokollan avulla autentikoitiin käyttäjä. Autentikointi – tapa käydään lävitse verkon autentikointi – kappaleessa. Langattomassa verkossa ei käytetty salausta, vaan toimittiin ilman salausmetodeja.

Tapahtuman verkon vikasietoisuuden toteuttamiseen kuului varakytkin, johon osa yhteyksistä tuli, mutta ei varakaapelointeja eli rinnakkaisia yhteyksiä. Tämä siitä syystä, että ylläpito oli kokoajan paikalla tapahtuman aikana, ja pystyi nopeasti reagoimaan mahdollisiin muutoksiin ja ongelmiin. Kaapeleihin mahdollisesti osuvat viat olisi saatu paikannettua kaapelitesterillä eli laitteella, joka tutkii kaapelin koko matkalta, löytäen siinä olevan vian ja kohdan missä vika on.

3.4 Verkkoautentikaatio

Tapahtumassa oli käytössä ainutlaatuinen tapa tunnistaa käyttäjä. Tunnistustapahtuma lähtee liikkeelle kun käyttäjä saapuu ulko-ovesta sisälle. Tällöin hän ilmoittautuu informaatiopisteellä ja hänen varaustietonsa otetaan esiin tietokoneella ja käyttäjästä otetaan kuva varaustietoihin liitettäväksi. Tässä yhteydessä käyttäjälle annetaan kortti, josta ilmenee käyttäjän tunnistusnumero ja kortissa on myös verkkoon kirjautumiseen tarvittava koodi.



(Liite 4 Käyttäjän autentikointi tapahtumassa.)

Saatuaan tunnuksensa käyttäjä vie koneensa hänen varaamalleen konepaikalle ja hän kytkee koneensa pöydällä olevaan kytkimeen kiinni. DHCP – palvelu, automaattisesti määrittää hänen koneelleen IP – osoitteen. Avatessaan selaimensa hän saa eteensä kirjautumissivun, johon hän kirjautuu informaatiopis-

teessä saamassa kortissa olevalla koodilla ja konepaikkansa nimellä. Kun hän kirjautuu sisään, käyttäjän tiedot rekisteröityvät tietokantaan.

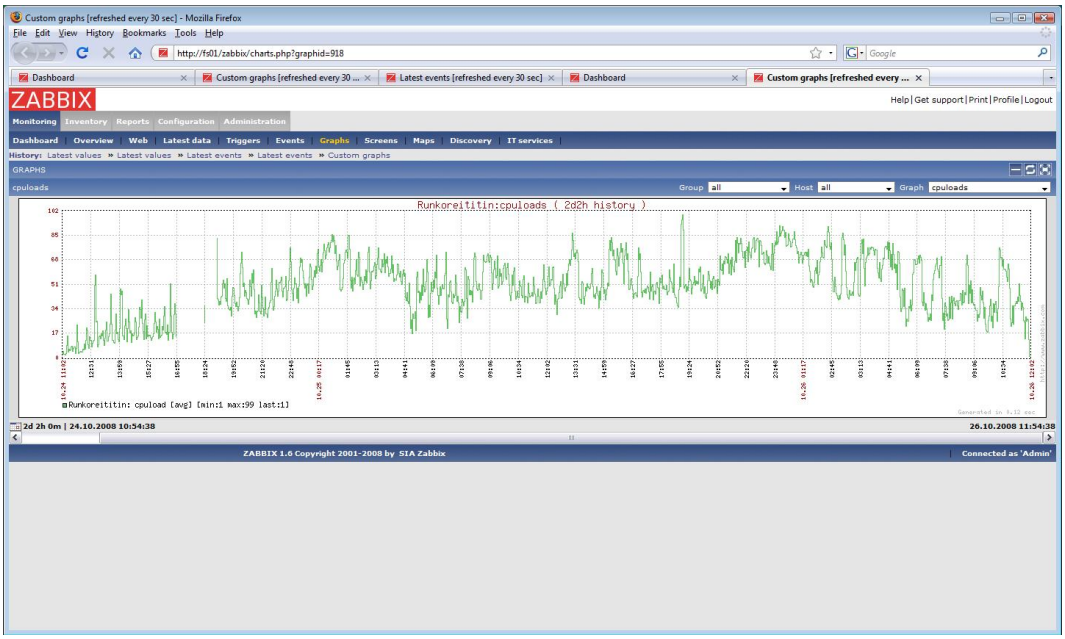
Täältä tietokannasta palomuuri kyselee, että löytyykö käyttäjää. Näin tapahtuessa palomuuri tallettaa muistiinsa, että tuon IP – osoitteen omaava kone päästetään lävitse. Tämän jälkeen nimipalvelin kyselee samasta tietokannasta käyttäjän tietoja ja muodostaa, DNS – nimen, jonka perusteella käyttäjä jatkossa tunnistetaan. DNS – nimi muodostuu konepaikan tunnuksesta ja käyttäjän koneelle annetusta IP – osoitteesta.

Verkkoon autentikoituessa käytettiin vrauth nimistä protokollaa. Vrauth on protokolla, jolle kirjautumissivun PHP - sovellus antaa tiedot, jotka käyttäjä on sivulle syöttänyt. Tämän jälkeen vrauth tutkii tietokannasta, että sieltä löytyvä koodi on yhteensopiva käyttäjän antaman koodin kanssa. Kun yhteensopivuus on tunnistettu, vrauth tekee assosiaation konepaikan ja pelaajan välille ja aukaisee vielä palomuuriin portin, jotta kyseisestä IP - osoitteesta pääsee internetiin. Tämäkään ei silti vielä riitä, vaan pitää olla oikealla IP – osoitteella ja oikealla MAC – osoitteella verkossa, jotta palomuurin ohi pääsee. Tämä käytettävä vrauth – protokolla, on tapahtuman järjestäjien itse tekemä protokolla.

Yhteenvetona autentikointi siis toimi tapahtumassa seuraavasti. Ensimmäisenä HTTP - yhteys otetaan palomuurilta www - palvelimelle jossa sijaitsee vrauth – protokollan PHP – sovellus. Tämän jälkeen käyttäjä syöttää tiedot kirjautumissivulla olevaan lomakkeeseen ja painaa ”kirjaudu” – painiketta. Tämän toimenpiteen jälkeen PHP - sovellus keskustelee vrauth - protokollan kanssa, jonka jälkeen käyttäjä pääsee käyttämään internetiä. Tämän operaation aikana tietokantaan jää tieto käyttäjien konepaikoista ja heidän koneiden MAC - ja IP – osoitteista. Tätä autentikointi - tapaa käytettiin myös langattomaan verkkoon kirjautuessa.

3.5 Verkon ylläpito

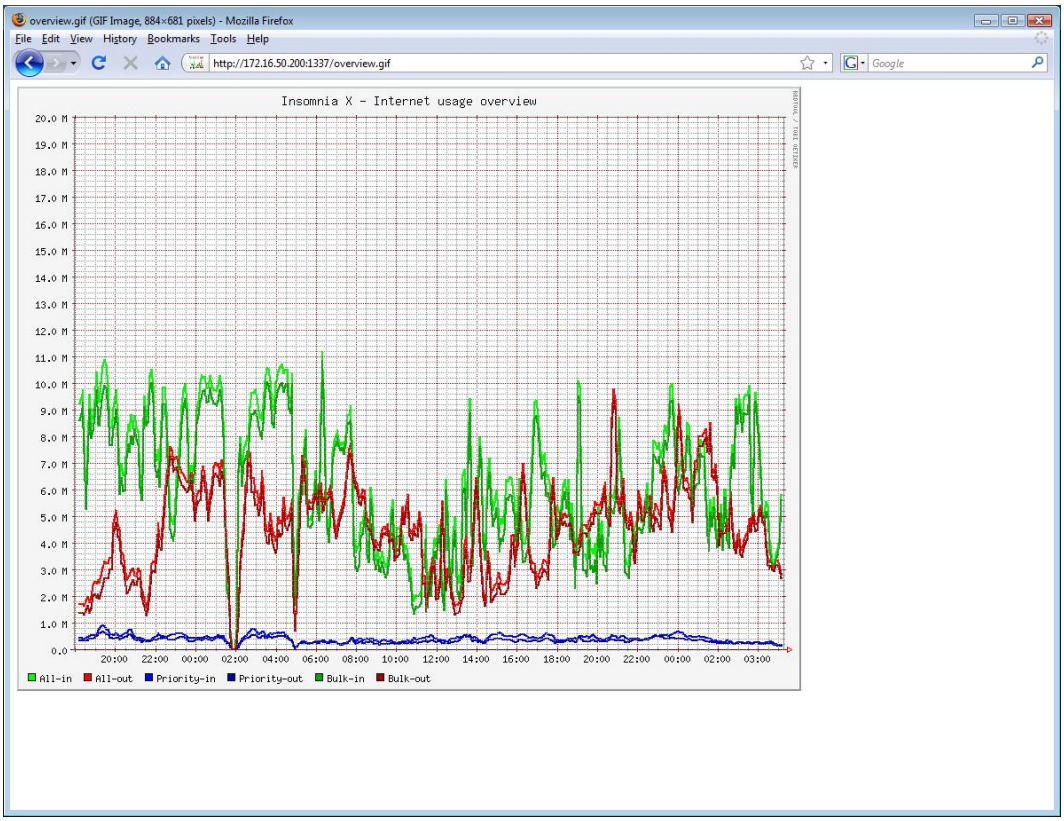
Tapahtuman ylläpito hoidettiin muutamilla eri ohjelmilla ja kahdella eri ping – kyselyllä. Ylläpitoon kuului myös mahdollisten kuormittavien laitteiden poistaminen verkosta, jotta saataisiin verkko uudelleen toimintakuntoon. Ylläpidossa oli koko ajan yksi vastaava henkilö ja kaksi muuta henkilöä valvomassa verkon toimintaa. Yleensä verkkoa valvoi useampia ihmisiä muiden tehtäviensä ohella. Zabbix - ohjelmalla seurattiin oletusyhdyskäytävän käyttäytymistä sekä runkokytkimen ja runkoreitittimen verkon käyttöä. Tällä samalla ohjelmalla seurattiin myös runkokytkimen suorittimen ja muistin käyttöä. Ohjelmalla toisin sanoen monitoroitiin tapahtuman verkon ydinkomponentteja sekä niiden suorittimien ja muistien käyttöä.



(Liite 5 - runkoreitittimen prosessorikuorma)

Yllä olevassa kuvassa (Liite 5) on Zabbix – ohjelmasta otettu kuvankaappaus, josta näkyy verkossa olleen runkoreitittimen suorittimen kuormaa tapahtuman eri ajankohtina. X – akselilla on aika ja Y – akselilla on suorittimen kuorman määrä prosentteina. Kuvasta nähdään, että muutamia piikkejä ja tapahtuman alkupuolella ollutta lyhyttä käyttökatkosta lukuun ottamatta runkoreititin ja

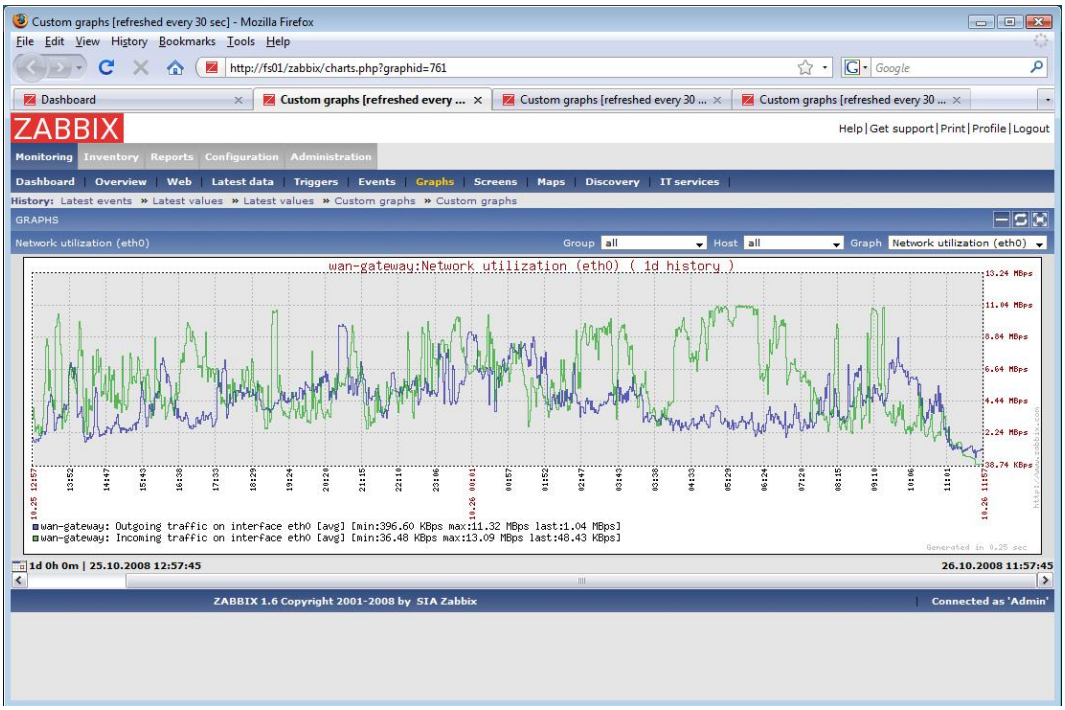
sen suoritin toimi normaalisti ja ilman ongelmia. Zabbix – ohjelmalla tarkkailtiin myös toisen runkokytkimen, pikkuhoopon suorittimen kuormaa (Liite 6). Pikkuhoopo kytkettiin käyttöön vasta tapahtuman aikana, siitä johtuu pikkuhoopon suorittimen käytön alkaminen vasta 25.10. tapahtuman ollessa jo hyvässä vauhdissa.



(Liite 7 – verkon käyttöasteet)

Yllä olevasta kuvasta (Liite 7), käy ilmi verkon käyttöasteet eri aikoina. Kuvassa on eritelty erilainen liikenne eri väreillä. Vaaleanvihreä tarkoittaa kaikkea sisäänpäin menevää liikennettä ja punainen väri kaikkea ulospäin menevää liikennettä. Kahdella eri sinisellä värillä on eroteltu tärkeysluokiteltu liikenne, joka on ollut tärkeää liikennettä, joko ulos - tai sisäänpäin. Tummanvihreällä ja tummanpunaisella on eroteltu niin sanottu bulk – liikenne eli oletusliikenne, jota ei ole luokiteltu mihinkään luokkaan. Tässä tapauksessa kyseessä on verkkoa tarvitsevien pelien aiheuttama liikenne.

Myös tapahtumassa olleen palvelinverkon palvelinten käyttöä seurattiin kyseisellä ohjelmalla. Verkon oletusyhdyskäytävän liikennettä tutkailtiin myös Zabbixilla (Liite 8). Kuvassa on eroteltuna sisäänpäin tuleva liikenne ja ulospäin menevä liikenne. Tässä kuvassa on aikavälinä 25.10 iltapäivän ja 26.10 klo 12.00 välinen aika. Vihreällä värillä on tässä kuvassa eroteltu sisäänpäin tuleva liikenne ja sinisellä on eroteltu ulospäin menevä liikenne.



(Liite 8 – oletusyhdyskäytävän liikenne)

Zabbix - ohjelmalla käytännössä tutkailtiin vain sisäverkon laitteita, ulkoverkon puolta ei tällä ohjelmalla tutkittu. Staselog Network Equalizerilta eli verkon kuormantasaajalta saatiin tietoa tapahtuman verkon käyttöasteesta ja sen jakaantumisesta eri kytkimille ja käyttäjille. Kuormantasaajalta saatiin tarkkaa tietoa sekä sisäänpäin tulevasta, että ulospäin menevästä liikenteestä. Toisin sanoen saatiin tarkasti tietoon kuinka suuria tapahtuman liikennemäärät kulloinkin olivat. Näin pystyttiin nopeasti reagoimaan suuriin liikennemäärien muutoksiin. Bittivahti seurasi tapahtuman ajan verkon liikenteen määriä. Näin pystyttiin näkemään helposti kuinka suurta liikennettä verkossa milläkin het-

kellä oli. Tämän lisäksi suoritettiin ping – kysely oletusyhdyskäytävä - koneelle, jolla seurattiin kuinka nopeasti se vastaa tähän kyselyyn. Sen perusteella tehtiin jatkotoimia, jos kesto oli liian suuri. Ping – kyselyä suoritettiin jatkuvasti, 0,1 sekunnin välein, jotta voitiin heti havaita isommat viiveet ja jolloin niihin voitiin myös nopeasti reagoida ja vaikuttaa oletusyhdyskäytävän toimintaan parantavasti.

Edellä mainitun ping – kyselyn lisäksi toisella ping – kyselyllä testattiin tietyn palvelimen yhtä tiettyä pöytäkytkimen virtuaalista lähiverkkoa kohdetta vaihdellen. Toisin sanoen yksi palvelinverkossa oleva palvelin on virtuaalisesti yhteydessä pöytäkytkinten virtuaalisten lähiverkkojen kanssa. Näitä virtuaaliverkkoja tutkitaan ping - kyselyllä palvelimen yhdestä ”verkkointerfacesta”. Näin nähdään, että kytkimet ovat toiminnassa ja vastaavat kyselyyn. Jos joku virtuaalinen lähiverkko ei vastaa, voidaan kyseisen lähiverkon omaava kytkin paikallistaa nopeasti ja alkaa selvittää ongelmaa.

Tapahtumaa ylläpidettäessä oli valmiudet sulkea liikaa verkkoa kuormittavat laitteet nopeasti verkosta pois. Laite voi olla niin käyttäjän työasema kuin mikä tahansa muukin verkon laite, jos siellä käytetään esimerkiksi P2P – sovelluksia, sillä ne kuormittavat verkkoa. Tämän takia kyseiset P2P – palvelut olivat kiellettyjä käyttää. Tällaiset liikaa verkkoa kuormittavat koneet poistettiin manuaalisesti vetämällä verkkojohto irti kytkimestä. Oli myös mahdollisuus ohjelmalliseen verkkoyhteyden poistamiseen tai kaistan vähentämiseen kyseisiltä koneilta tai laitteilta.

4 JOHTOPÄÄTÖKSET

Tapahtuman verkko saatiin suunnitellussa aikataulussa toimintakuntoon ja se toimi muutamia lieviä häiriöitä lukuun ottamatta koko tapahtuman ajan. Opinnäytetyön tavoitteena ollut selvitystyö verkon toteuttamisesta ja ylläpidosta onnistuttiin tekemään suunnitelman mukaisesti. Verkon ylläpito-osuudessa olevista verkkokuvista käy ilmi, että tapahtuman verkko toimi yhtä käyttökatkosta lukuun ottamatta moitteetta. Voidaan siis todeta, että verkon toteuttaminen onnistui suunnitelman mukaisesti. Tapahtuman verkon ja sen toteuttamisen dokumentointi tehtiin suunnitelman mukaisesti. Voidaan todeta, että edelleen verkkoa kehitettäessä, etenkin havainnollistavat verkkokuvat ovat hyödyllisiä apuvälineitä nyt ja tulevaisuudessa. Ylläpidon puolelta saatiin myös kattavasti tietoa ja kuvia tapahtuman verkkoa seuraavista laitteista. Voidaan todeta, että verkon ylläpito onnistui, koska isoja käyttökatkoksia ja häiriöitä verkkoliikenteeseen ei tullut. Erittäin onnistuneena osana tapahtumaa ja tätä opinnäytetyötä pidän tapahtuman ainutlaatuisen autentikointi – järjestelmän toimintaa ja sen onnistunutta dokumentointia. Myös autentikoinnin apuvälineenä olevat havainnollistavat verkkokuvat onnistuivat hyvin.

Haastavin ja ongelmallisin asia tämän opinnäytetyön tekemisessä ja verkon toteuttamisessa oli ymmärtää tiettyjä asioita, joita verkossa oli käytössä. Spanning Tree Protocol – protokolla ei ollut minulle entuudestaan tuttu, joten tätä työtä varten siihen piti tutustua. Myös virtuaaliset lähiverkot olivat omalta osaltaan itselleni ongelmallisia ymmärtää ja hahmottaa. Tosin tämän työn ansiosta ymmärrän jo melko hyvin, yksinkertaisen virtuaalisen lähiverkon toimintaidean ja funktion. Ennakolta odotin, että autentikointi – järjestelmän toiminnan ymmärtäminen olisi ollut vaikeampaa. Itse asiassa, kuten autentikointi - kappaleesta selviää, ei kyseessä ole kovinkaan monimutkainen asia.

Tapahtuma on nuorisolle turvallinen tapa viettää aikaansa hyvässä seurassa, varjopuolena kuitenkin on liikunnan puute ja liiallinen monitorin tuijottaminen. Yleisesti ottaen tämän kaltaisilla tapahtumilla olisi enemmänkin tilausta,

sillä tapahtuma on melko ainutlaatuinen muun muassa kilpailujen ja päihteettömyytensä ansiosta. Tapahtumassa jaettiin noin 5000 euroa palkintorahoja eri kilpailujen parhaille, kuten esimerkiksi robosodan voittajalle. Tapahtuman toteuttajilla ja käyttäjillä oli hyvä ja kannustava henki, koko tapahtuman ajan. Jokainen tapahtuman toteuttaja teki saman päämäärän eteen töitä, jotta saatiin verkko ja puitteet ajoissa kuntoon. Tämä loi käyttäjille sujuvan ja onnistuneen viikonvaihteen, jolloin ei oltu otsa rypyssä.

LÄHTEET

Anttila, A. 2001. TCP / IP – tekniikka. Juva. WS Bookwell.

Jaakohuhta, Hannu. 2000. Lähiverkot – Ethernet. Jyväskylä. Gummerus Kirjapaino Oy.

Casad J & Willsey B. 1999. TCP – IP Trainer. Jyväskylä. Gummerus Kirjapaino Oy.

Cisco Systems. 2002. Cisco Verkkoakatemia Toinen vuosi. Helsinki. Edita Prima Oy.

Chappel, L. 1999. Cisco Reitittimet. Jyväskylä. Gummerus Kirjapaino Oy.

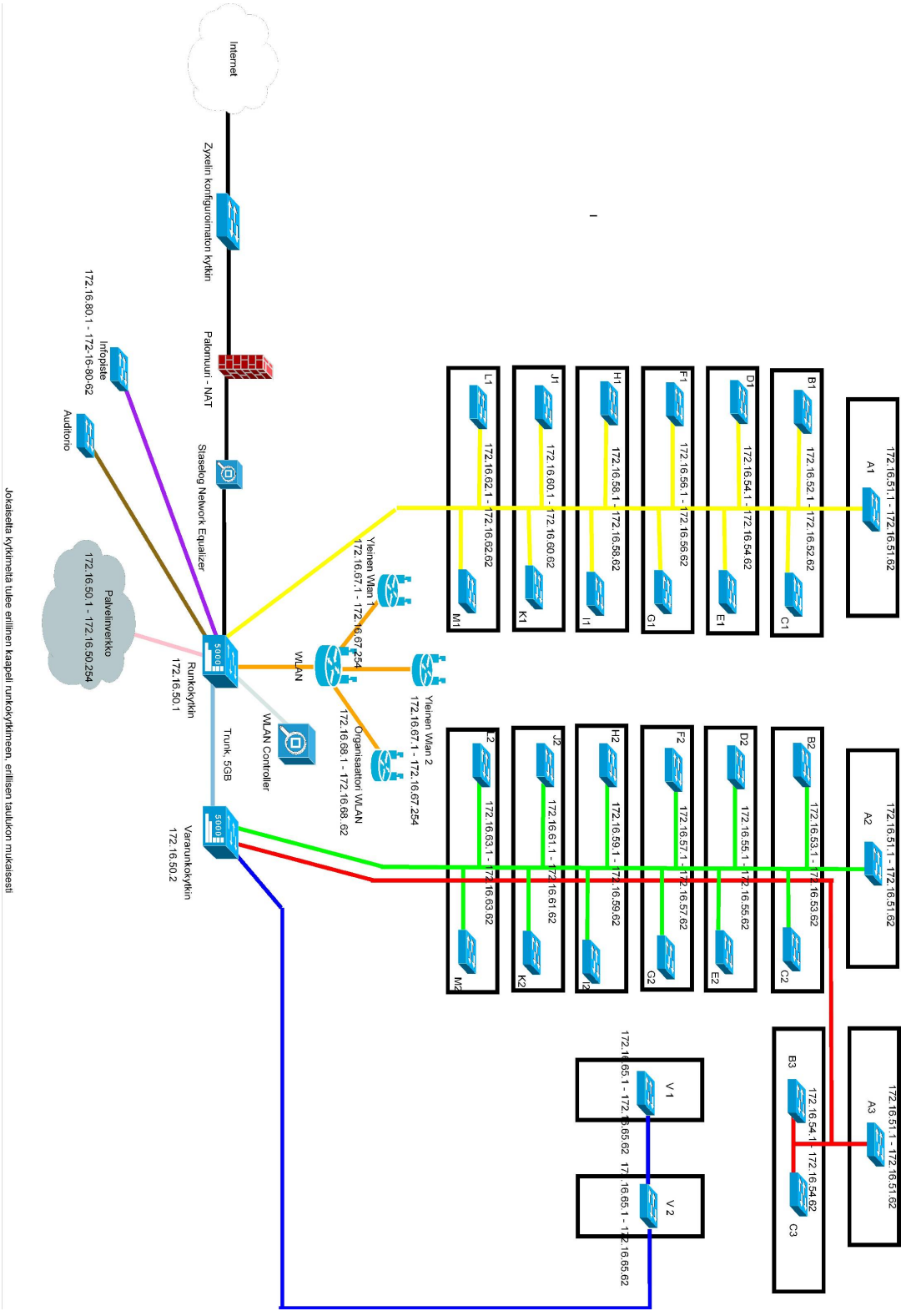
Puska, M. 2000. Lähiverkkotekniikka – Pro Training. Jyväskylä. Gummerus Kirjapaino Oy.

Thomas, T. 2005. Verkkojen tietoturva. Helsinki. Edita Prima Oy.

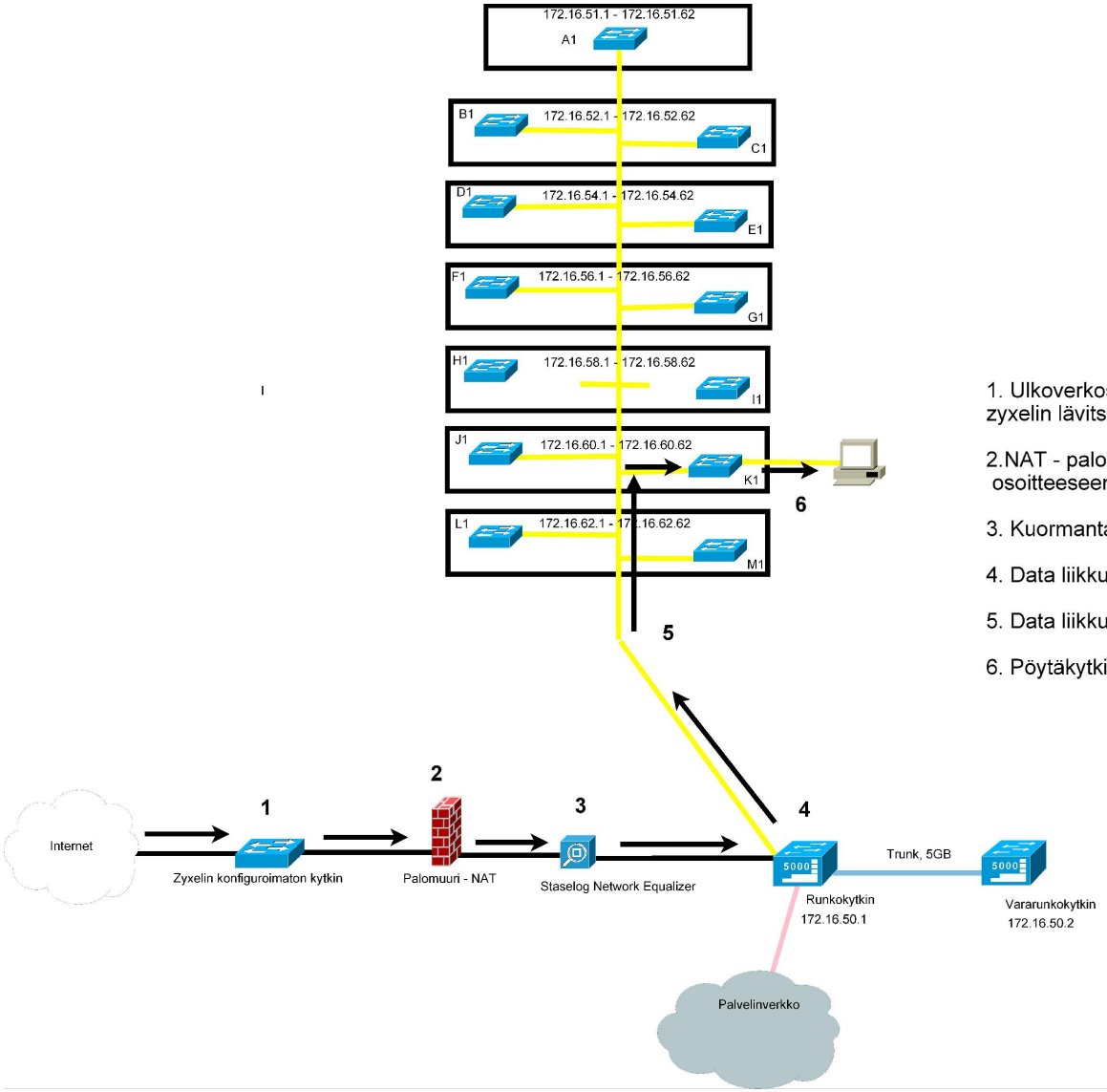
Lehto, T Tietokone 3/2004, Verkkokaistan käyttö hallintaan Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=20799&tyyppi=1.

LIITTEET

LIITE 1 Fyysinen verkkokuva



LIITE 2 Reititys Sisään



1. Ulkoverkosta tulee dataa konfiguroimattoman zyxelin lävitse palomuurille.

2.NAT - palomuuri osoittaa datan oikeaan osoitteeseen.

3. Kuormantasaaja tasaa liikenteen.

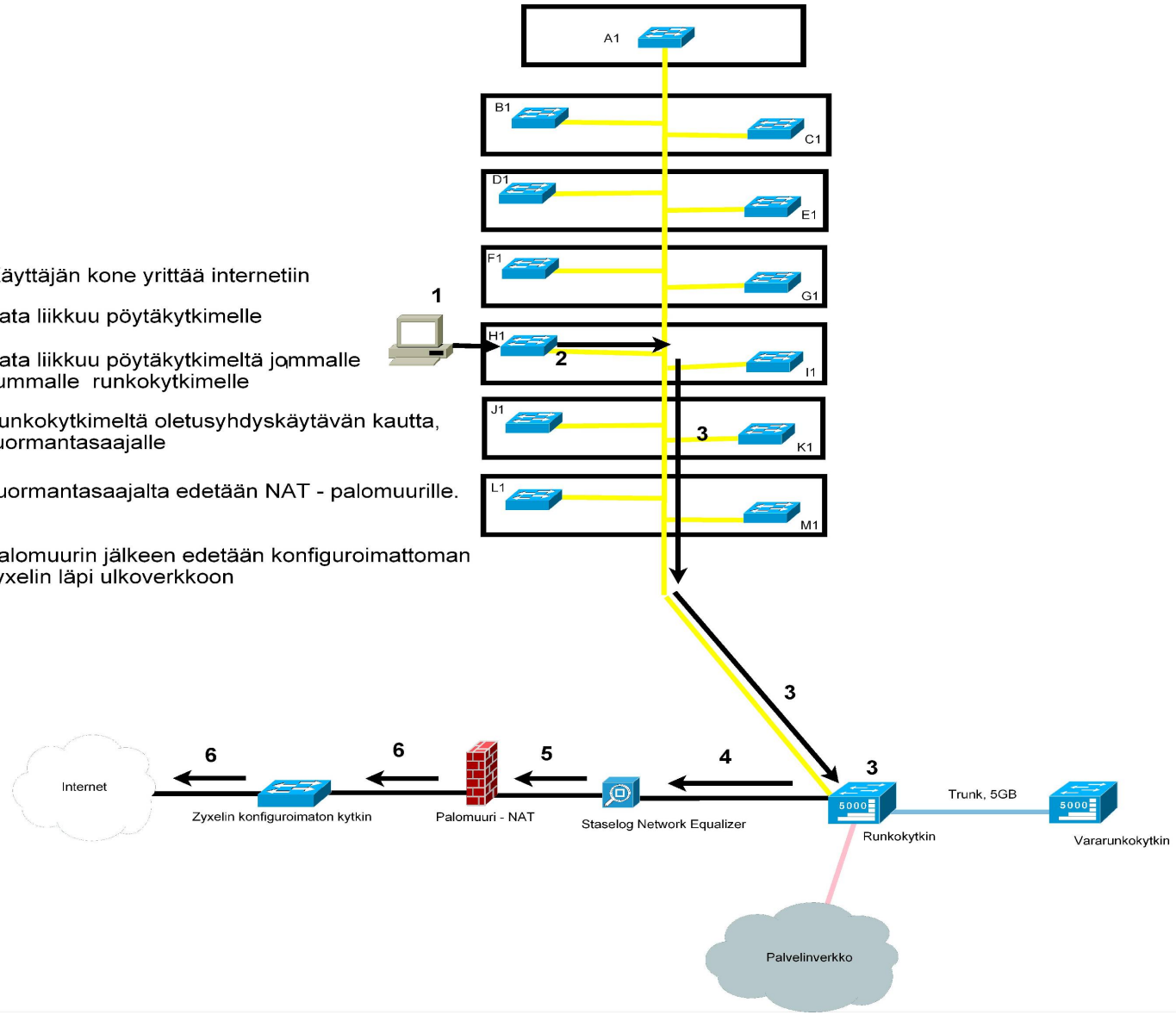
4. Data liikkuu jommalle kummalle runkokytkimelle.

5. Data liikkuu runkokytkimeltä pöytäkytkimille.

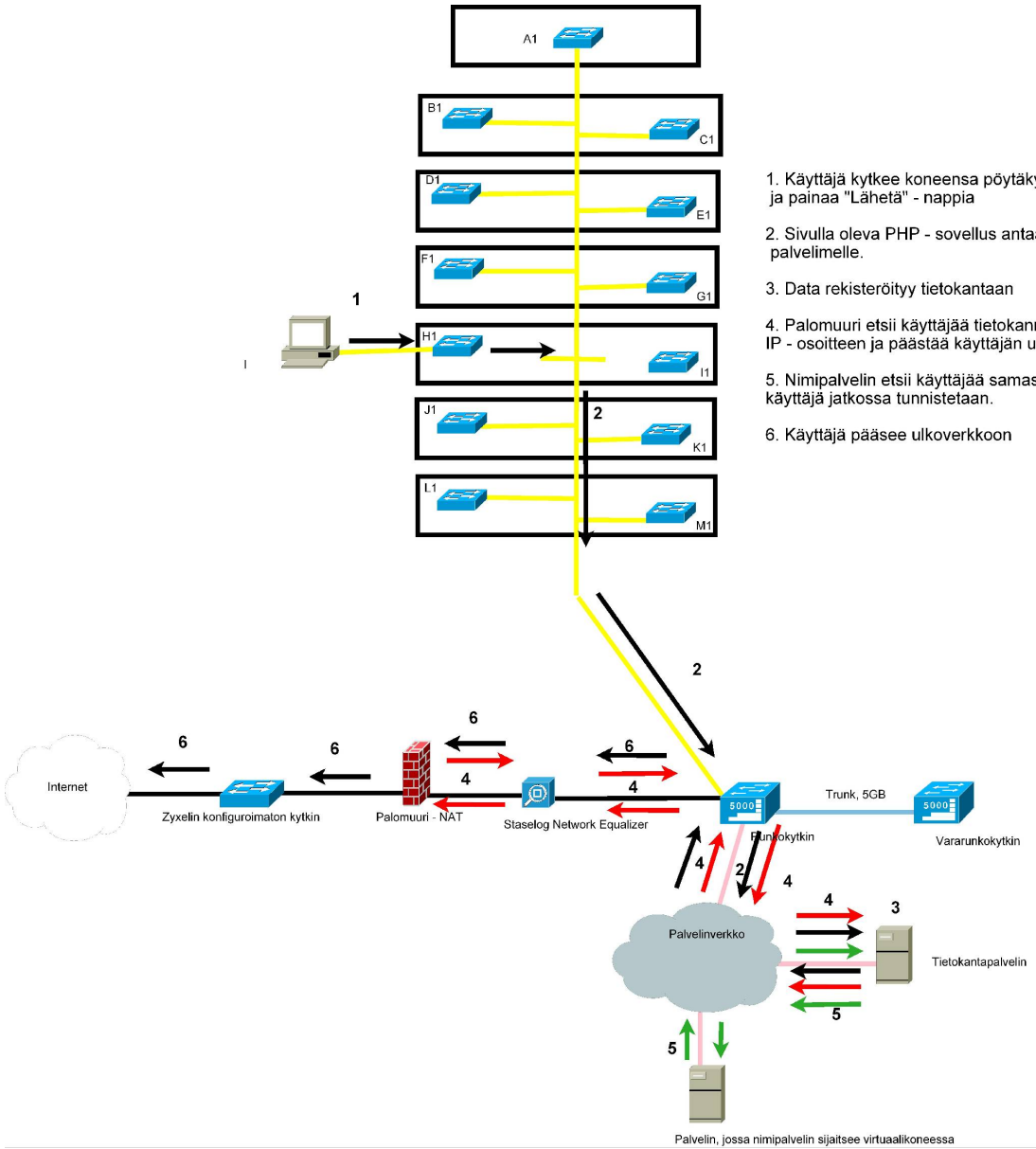
6. Pöytäkytkin vie datan käyttäjän koneelle.

LIITE 3 Reititys Ulos

1. Käyttäjän kone yrittää internetiin
2. Data liikkuu pöytäkytkimelle
3. Data liikkuu pöytäkytkimeltä jommalle kummalle runkokytkimelle
4. Runkokytkimeltä oletusyhdyskäytävän kautta, kuormantasaajalle
5. Kuormantasaajalta edetään NAT - palomuurille.
6. Palomuurin jälkeen edetään konfiguroimattoman zyxelin läpi ulkoverkkoon



LIITE 4 Autentikointi



1. Käyttäjä kytkee koneensa pöytäkytkimeen ja avaa selaimen. Käyttäjä käyttäjä täyttää kirjautumissivur ja painaa "Lähetä" - nappia

2. Sivulla oleva PHP - sovellus antaa datan vrauth - protokollan lähetettäväksi palvelinverkossa olevalle palvelimelle.

3. Data rekisteröityy tietokantaan

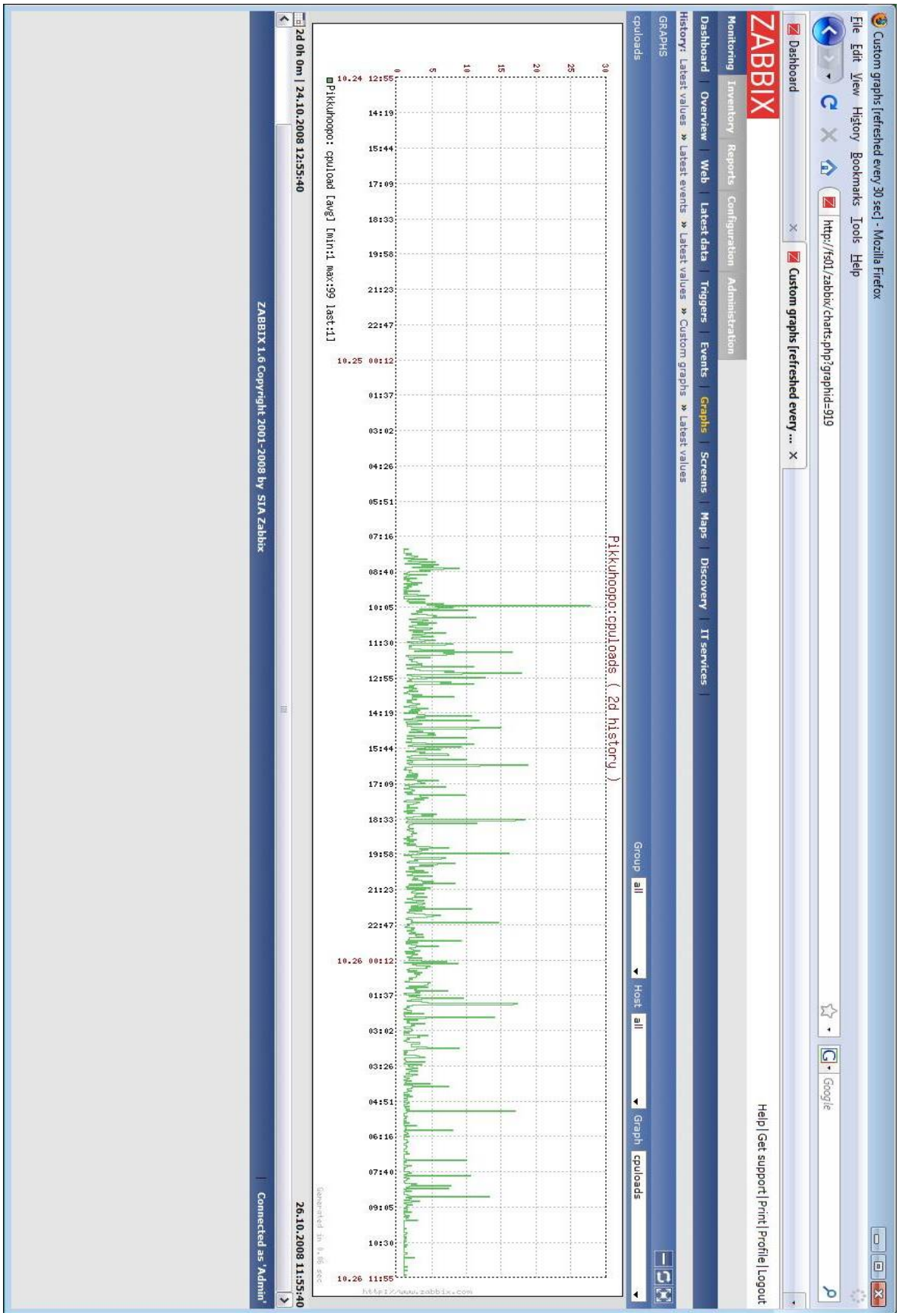
4. Palomuuri etsii käyttäjää tietokannasta. Kun käyttäjä löytyy palomuuri tallettaa muistiinsa käyttäjän IP - osoitteen ja päästää käyttäjän ulkoverkkoon

5. Nimipalvelin etsii käyttäjää samasta tietokannasta ja löytäessään, muodostaa DNS - nimen, jolla käyttäjä jatkossa tunnistetaan.

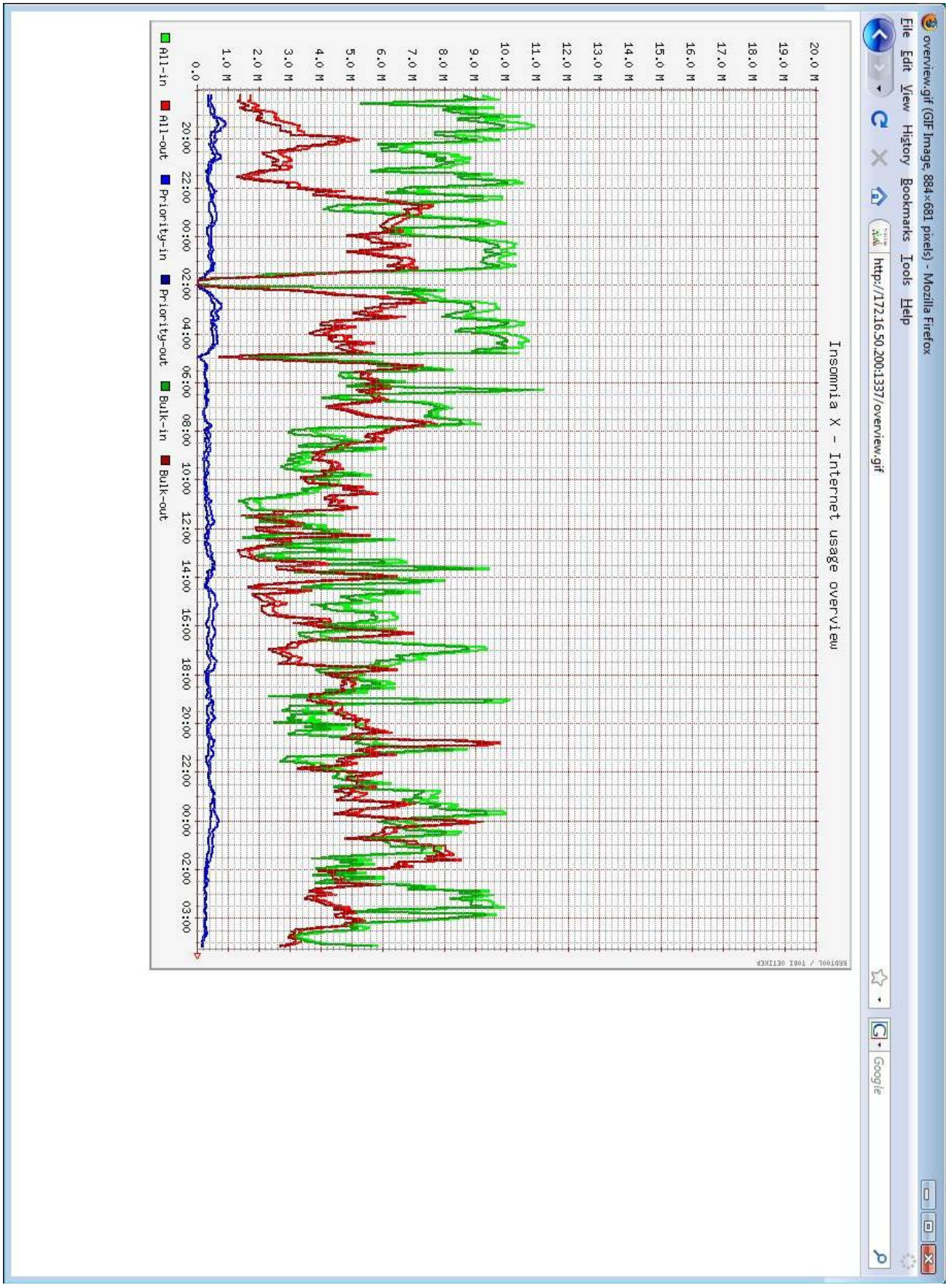
6. Käyttäjä pääsee ulkoverkkoon

LIITE 5 Runkoreitittimen suorittimen käyttö

LIITE 6 Vararunkoreitittimen suorittimen käyttö



LIITE 7 Verkon liikenteen käyttö



LIITE 8 Oletusyhdyskäytävän liikenne