KÄYTTÄJÄN TUNNISTUS OPPILASTALO OY:N VERKOSSA
Päijät-Hämeen Puhelin Oyj:n case-toteutus

LAHDEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
03.05.2007
Pasi Riihimäki

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

RIIHIMÄKI, PASI: Käyttäjän tunnistus Oppilastalo Oy:n verkossa
Päijät-Hämeen Puhelin Oyj:n case-toteutus

Tietoliikennetekniikan opinnäytetyö, 51 sivua, 56 liitesivua

Kevät 2007

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena oli toteuttaa lain vaatimukset täyttävä käyttäjän tunnistus alueverkossa, jonka Päijät-Hämeen Puhelin Oyj tarjoaa asiakkaallensa Oppilastalo Oy:lle Lahden kaupunkialueella. Tunnistamisen tarkoituksena on pystyä jälkeenpäin, mahdollisissa verkon väärinkäytöstapauksissa, näyttämään toteen milloin, mistä ja millä päätelaitteella tapahtuma on suoritettu. Tunnistamisen yhteydessä ei rajoiteta käyttäjän pääsyä verkkoon ja sen palveluihin.

Työssä esitellään nykyisissä tietoliikenneverkoissa verkkotekniikkana käytetyn Ethernetin perusteita, nykyisiä verkkototeutuksia, käyttäjäntunnistuksessa käytettäviä tekniikoita sekä vertaillaan näiden ratkaisumalleja ja niiden tehokkuutta. Käsiteltäviä käyttäjätunnistustekniikoita olivat MAC-osoitteiden tunnistus, PPPoE, DHCP ja DHCP option-82.

Eri käyttäjätunnistustekniikoita vertailtaessa havaittiin MAC-osoitteiden tunnistus -tekniikan työläs ylläpito, PPPoE-tekniikan tarvitsema erillinen kirjautumispalvelin ja salasanojen käytön hankaluus sekä perinteisen DHCP-tekniikan hankaluus väärinkäytösten selvityksessä. DHCP option-82 -tekniikka havaittiin toteutuskelpoisimmaksi, koska se tarjoaa helpompaa ylläpitoa ja väärinkäytösten selvitystä eikä tarvitse erillistä kirjautumispalvelinta.

Tunnistuksen mahdollistamiseksi verkkoon tehtiin mittavia laitehankintoja ja verkko muutettiin kokonaan kytkinverkoksi. Samassa yhteydessä verkon palvelun laatua saatiin nostettua merkittävästi. Työn yhteydessä tilaajalle tehtiin myös mahdolliseksi valita liittymänsä nopeusluokka alkuperäisen 512 kbit:n/s lisäksi myös kahdesta uudesta nopeusluokasta 256 kbit/s ja 2 Mbit/s. Nopeusluokkien jako toteutettiin VLAN-tekniikalla. Työssä esitellään Oppilastalo Oy:n verkkototeutus, laitevalinnat, tekninen toteutus ja konfiguraatiot sekä selvitetään, kuinka käyttäjän tunnistus toteutettiin.

Työn tuloksena Oppilastalon verkossa otettiin onnistuneesti käyttöön käyttäjän tunnistus niin sanotulla DHCP option-82 -tekniikalla, erilaiset siirtonopeusluokat sekä uusia tietoturva- ja liikenteenhallintaominaisuuksia. Opinnäytetyön kannalta oleellinen työtehtävä oli myös verkon dokumentoinnin päivitys, joka oli haastava mutta myös antoisa työ. Kokonaisuutena työ vastasi haastavuudeltaan ja tuloksiltaan odotuksia ja sitä voidaan pitää näin ollen onnistuneena.

Asiasanat: DHCP option-82, käyttäjän tunnistus, päätelaitteen tunnistus, teletunniste

Lahti University of Applied Sciences
Faculty of Technology

RIIHIMÄKI, PASI: Subscriber identification in the network of the Oppilastalo Oy
Case implementation by the Päijät-Hämeen Puhelin Oyj

Bachelor's thesis in Telecommunications Technology, 51 pages, 56 appendices

Spring 2007

ABSTRACT

The objective of this thesis was to implement subscriber identification required by law in the metropolitan area network which Päijät-Hämeen Puhelin Oyj is providing to its customer Oppilastalo Oy in the urban area of Lahti. The subscriber identification will be used only afterwards, in the case of possible improper use, to indicate when, where and by which device the improper use has been performed. There will be no restrictions at all to prevent user access to the network or networks services.

The thesis presents the basics of Ethernet technology, as well as today's network implementations, different techniques used for user identification, and solutions offered by these techniques and their efficiency. The techniques covered in this thesis were MAC address identification, PPPoE, DHCP and DHCP option-82.

Comparison of these user identification techniques revealed that the MAC address identification technique is hard to maintain, the PPPoE technique requires a separate login server and has difficult use of passwords, and in the classic DHCP technique it is difficult to solve cases of improper network use. The most applicable of these four techniques was DHCP option-82 because it provides easier maintenance and allows solving of improper use and it does not need a separate login server.

To make subscriber identification possible, a lot of network devices were purchased and the network was changed to switch based. At the same time the quality of the service of the network improved significantly. It also became possible for subscribers to choose the speed of network connection of two new rate classes 256 kbps and 2 Mbps, in addition to the originally 512 kbps.

As a result of the thesis subscriber identification was applied successfully to the network of the Oppilastalo by DHCP option-82 technique. Different rate classes and new security and traffic control properties were also introduced. The documentation of the network was also updated.

Keywords: DHCP option-82, subscriber identification, terminal identification, identification data

SISÄLLYS

LYHENNELUETTELO

802.1p	IEEE-standardi liikenneluokan lähetykseen, oleellisinta on antaa keinot palvelunlaadun (QoS) toteuttamiseksi MAC eli OSI-2 -tasolla.
802.1Q	IEEE-standardi VLAN:n määrittämiseen sekä saman fyysisen linkin jakamiseen useamman sillatun verkon välillä läpinäkyvästi, etteivät tiedot vuoda verkosta toiseen eli esim. trunking.
Access switch	Liityntäkytkin, johon verkon päätelaitteet kytketään.
Alavirta	Ks. Downstream.
ARP	Address Resolution Protocol, TCP/IP-protokolla-perheen osoitteenselvitysprotokolla.
ATM	Asynchronous Transfer Mode, soluvälitteinen ja piirikytkentäinen tiedonsiirtotekniikka.
Backbone switch	Ks. Core switch.
BOOTP	BOOTstrap Protocol, protokolla, jota käyttämällä tietokone pyytää palvelimelta asetustiedot kuten IP-osoitteen.
Bridge	Ks. Silta.
Broadcast	Ethernetissä käytetty kehystyyppi levitysviestille.
Broadcast domain	Levitysviestialue, Ethernetissä.
CAT5	Category 5, Lyhenne, jota käytetään kategorian 5 kierretystä parikaapelista.
CEF	Cisco Express Forwarding, edistyksellinen OSI-3 -tason kytkentätekniikka, jota käytetään pääasiassa yritysten runkoverkoissa.

Circuit ID	DHCP option-82 -tunnistustekniikassa käytetty tunnuskenttä, jolla kuvataan (liityntä)kytkimen porttia, josta DHCP-kysely tuli ja johon asiakastietokone on yleensä suoraan kytketty. Kenttä sisältää esimerkiksi VLAN-tunnuksen, johon kytkinportti on määritetty, kytkimen moduulinumeron sekä porttinumeron.
Collision domain	Törmäysalue, Ethernetissä.
Core switch	Runko- tai keskuskytkin.
CoS	Class of Service, paketin priorisointiin perustuva jonotusmekanismi, joka on määritetty IEEE 802.1p -standardissa.
CSMA/CD	Carrier Sense Multiple Access with Collision Detection, Ethernetissä käytetty kanavallepääsymenetelmä.
DHCP	Dynamic Host Configuration Protocol, TCP/IP-protokollaperheen verkkokerroksen protokolla, jota käytetään, kun päätelaitteille halutaan jakaa IP-osoite ja muita tietoja verkon palveluista.
DHCP option-82	DHCP Relay Agent Information Option, DHCP-protokollakehyksen lisätietokenttä, jota käytetään asiakkaan tunnistamiseksi tarvittavien tietojen kuljetukseen.
DHCP Relay Agent	OSI-mallin kolmannen kerroksen laite DHCP-sanomien välitykseen eri verkossa sijaitsevien DHCP-asiakkaiden ja -palvelimien välillä.
DHCP Snooping	Cisco Systems:n kytkimissä käytetty DHCP-liikennettä seuraava turvallisuus ominaisuus.
DHCP Snooping Bind	DHCP Snooping -ominaisuuden muodostama sidos.

Distribution switch	Jakelu- tai levityskytkin.
Downstream	Alavirta, hierarkkisesti tietoverkon keskuksesta asiakkaalle päin.
DSL	Digital Subscriber Line, digitaalinen tilaajajohto.
DSLAM	Digital Subscriber Line Access Multiplexer, DSL-keskus.
Ethernet	Verkkotekniikka, joka sai alkunsa vuonna 1973 Xerox:n PARC-tutkimuskeskuksessa.
Frame	Kehys, sanomasta käytetty nimitys Ethernetissä.
Full-duplex	Kuvaus tiedonsiirrolle, jossa tietoa voidaan siirtää kumpaankin suuntaan samanaikaisesti kuten puhelintekniikassa.
Gbit/s	Gigabittiä sekunnissa tai gigabittiä per sekunti, tiedonsiirtonopeus, myös lyhenne Gbps (Gigabits per second).
Giaddr	Gateway IP Address, oletusyhdyskäytävän IP-osoite DHCP-protokollassa.
G.SHDSL	Symmetric High-speed Digital Subscriber Line, ITU-T:n vuonna 2001 standardoima symmetrinen DSL-tekniikka.
HomePNA	Home Phone line Network Alliance, yhteenliittymä, joka on kehittänyt samaa nimeä kantavan tekniikan. Tekniikassa käytetään jaettuna siirtotienä rakennuksen valmista puhelinkaapelointia.
Host	Isäntä, tietokone tai muu verkon päätelaite.

Hub	Laite tähtimäisen Ethernet-topologian keskipisteessä, mihin on kytketty useampia isäntiä, tunnetaan myös nimillä keskitin (consentrator) tai moniporttitoistin (multiport repeater).
IEEE	Institute of Electrical and Electronics Engineers, järjestö, joka keskittyy sähköteknillisen tekniikan kehitykseen.
IEEE 802.3	IEEE:n projekti 802:n alikomitea 3 ja myös sen määrittämä standardiperhe, jossa määritetään Ethernet-tekniikka.
IETF	Internet Engineering Task Force, internet standardeja kehittävä ja julkaiseva elin.
IP	Internet Protocol, protokolla tiedonvälitykseen pakettikytkentäisissä verkoissa.
ISO	International Organization for Standardization, 1947 perustettu kansainvälinen teollisia ja kaupallisia standardeja tuottava järjestö, joka koostuu kansallisien standardointijärjestöjen edustajista.
ISO 88023	ISO:n 1989 tuottama kansainvälinen Ethernet-standardi.
ISP	Internet Service Provider, internetpalveluiden tarjoaja tai internetoperaattori.
Isäntä	Ks. host.
Kytkin	Switch, Eräänlainen moniporttisilta. Hub:iin verrattuna kytkimen jokainen portti on oma törmäysalue.
LAN	Local Area Network, lähiverkko.
LED	Light Emitting Diode eli valodiodi.

Mbit/s	Megabittiä sekunnissa tai megabittiä per sekunti, tiedonsiirtonopeus, myös lyhenne Mbps (Megabits per second).
MAC	Media Access Control, osa OSI-viitemallin Data Link Layer -kerrosta (OSI-2). Mahdollistaa liittymisen useisiin erilaisiin fyysisiin verkkotekniikoihin.
MAC-osoite	Media Access Control -osoite eli fyysinen osoite tai laiteosoite on yksilöllinen tunniste, jollainen on muun muassa kaikilla verkkosovittimilla.
MTU	Maximum Transfer Unit, suurin pakettikoko, joka verkon läpi voidaan välittää.
Multicast	Ethernetissä käytetty kehystyyppi yhdeltä monelle lähetettävälle viestille.
OSI	Open Systems Interconnection, ISO:n kehittämä seitsemänkerroksinen viitemalli viestintään ja tietokoneverkkojen protokollasuunnitteluun.
OSI-2	Seitsemän kerroksisen OSI-viitemallin toinen eli siirtoyhteyskerros, jota vastaa myös viisikerroksisen TCP/IP-protokollapinon toinen eli Data Link Layer -kerros.
OSI-3	Seitsemän kerroksisen OSI-viitemallin kolmas eli verkkokerros, jota vastaa myös viisikerroksisen TCP/IP-protokollapinon kolmas eli internet-kerros.
PO	Palvelu Operaattori, telepalveluja tarjoava yritys.
PPP	Point-to-Point Protocol, TCP/IP-protokollaperheen Data Link Layer -kerroksen protokolla.

PPPoE	PPP over Ethernet, muoto, jossa PPP-protokolla on kapseloitu Ethernet-kehykseen.
QoS	Quality of Service, palvelunlaatu.
Remote ID	DHCP option-82 -tunnistustekniikassa käytetty tunnus, jolla kuvataan laitetta, jonka kautta DHCP-kysely tuli verkkoon. Tämä kenttä sisältää esimerkiksi liityntäkytkimen MAC-osoitteen.
RFC	Request For Comments, IETF:n standardijulkaisu.
Session ID	PPPoE-tekniikassa käytetty yksilöllinen istuntotunnus.
Silta	Bridge, OSI-2 -kerroksen laite, jolla voidaan yhdistää kaksi verkon osaa toisiinsa. Silta ei vaikuta levitysviestialueeseen mutta rajoittaa törmäysalueet sillan eri puolille.
SNMP	Simple Network Management Protocol, TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla.
SNMP-trap	SNMP-viesti, jolla raportoidaan muuttuneesta tilasta, esimerkiksi hälytyksistä.
SSL-VPN	Secure Socket Layer-Virtual Private Network, www-pohjainen VPN-tekniikka.
Sub-option	Alioptio, käytössä DHCP Relay Agent Information Option eli DHCP option-82 -kentässä.
Switch	Ks. kytkin.
Syslog	Standardi lokiviestien välitykseen IP-verkoissa.

TCP/IP	Transmission Control Protocol / Internet Protocol, 1970-luvulla kehitetty protokollaperhe erilaisten verkkojen yhdistämiseen.
Terminointi	Tietoliikenneyhteyden tai -linjan päättäminen.
Token	SSL-VPN tekniikassa käytettävä henkilökohtainen avain.
Unicast	Ethernetissä käytetty kehystyyppi kahden osapuolen väliseen liikenteeseen.
Upstream	Ylävirta, hierarkkisesti asiakkaalta tietoverkon keskukseen päin.
UTP	Unshielded Twisted Pair, suojaamaton kierretty pari(kaapeli).
VC	Virtual Channel, virtuaalikanava. ATM-tekniikassa käytetty nimitys esimerkiksi asiakkaan modeemin ja operaattorin keskuslaitteen välisestä yhteydestä.
VLAN	Virtual Local Area Network, virtuaali(lähi)verkko. IEEE standardi 802.1Q vuonna 1998 ja uusi päivitetty versio 2003.
VO	Verkko Operaattori, televerkkoa, esimerkiksi puhelin- tai tiedonsiirtoverkkoa, tarjoava yritys.
VoIP	Voice over Internet Protocol, puheen kuljetustekniikka IP-verkoissa.
VPN	Virtual Private Network, virtuaalinen yksityisverkko.
WLAN	Wireless Local Area Network, langaton lähiverkko.
Ylävirta	Ks. Upstream.

1 JOHDANTO

Työn taustana on Päijät-Hämeen Puhelin Oyj:n, myöhemmin PHP, ja Oppilastalo Oy:n, myöhemmin Oppilastalo, välinen sopimus, jonka perusteella PHP tarjoaa Oppilastalon asukkaille pääsyn internetin palveluihin. Verkon käyttäjät tulee tarvittaessa voida tunnistaa. Päijät-Hämeen Puhelin Oyj on etelä-suomen alueella toimiva tietoliikenne- ja tietotekniikkapalveluita tarjoava yritys. Oppilastalo Oy on lahtelainen opiskelija-asuntokiinteistöjä hallinnoiva ja vuokraava yritys.

Työn tavoitteena oli muuttaa Oppilastalo Oy:n verkko kokonaisuudessaan kytkimillä toteutetuksi lähiverkoksi ja tämän jälkeen toteuttaa lain vaatima käyttäjän tunnistus, jolla mahdolliset väärinkäytökset voidaan jäljittää. Työn tutkimusongelmana oli selvittää, millä tekniikalla ja millä tavalla tunnistus toteutettaisiin. Lisätavoitteena oli päivittää verkon dokumentaatio, parantaa verkon tietoturvatasoa ja ottaa käyttöön useampi nopeusluokka asiakkaiden tarpeiden eroavuudesta johtuvista syistä.

Käyttäjän tunnistus -termillä tarkoitetaan tässä asiakirjassa lain vaatimaa internetyhteyden käyttäjän/päätelaitteen selvittämistä käyttöajankohdan, sijainnin, asiakkaan päätelaitteen fyysisen- ja operaattorilta saadun verkko-osoitteen perusteella. Tietoa näistä säilytetään operaattorin DHCP-palvelimien (Dynamic Host Configuration Protocol) lokitiedostoissa ja niistä otetuissa varmistuksissa laissa määritetyn ajan.

Aikatauluksi käytännön työn toteuttamiseksi asetettiin touko-elokuu vuonna 2005.

2 KÄYTTÄJIEN TUNNISTUS

2.1 Käyttäjien tunnistus yleisesti

Tunnistaminen on menettely, jolla yksilöidään kohde, kuten käyttäjä tai järjestelmä, eikä se edellytä välttämättä kohteelta mitään toimenpiteitä. Todentaminen puolestaan tarkoittaa tunnistetietojen paikkansapitävyyden tarkistamista, ja sitä käytetään yleisesti samaan aikaan tunnistamisen kanssa. Kiistämättömyydellä on tarkoitus näyttää toteen esimerkiksi, kuka on viestin lähettäjä tai vastaanottaja. (Viestintävirasto 2004a.)

Käyttäjän tunnistusta käytetään tänä päivänä kaikilla tekniikoilla toteutetuissa liityntäverkoissa, joilla tarjotaan käyttäjälle pääsy verkon palveluihin. Tunnistukseen käytetyt tekniikat ja niiden tuottamien tunnistustietojen monipuolisuus vaihtelevat eri verkoissa tarpeen mukaan. Joissakin toteutuksissa tunnistus tehdään automaattisesti asiakkaan sitä huomaamatta ja joissakin toisissa tunnistus tapahtuu samalla, kun asiakas kirjautuu verkkoon.

2.2 Käyttäjien tunnistukseen liittyvä problematiikka

Käyttäjien tunnistukseen liittyy aina myös problematiikkaa tunnistuksen käytettävyyden ja turvallisuuden välillä. Tunnistustietoja keräävän ja tallentavan tekniikan tulee olla palveluntarjoajan kannalta sekä helposti että turvallisesti toteutettavissa ja ylläpidettävissä.

Käyttäjän kannalta tekniikan tulee olla yksinkertainen ja helppokäyttöinen, jottei se muodostu esteeksi verkon palveluiden käytölle. Käytettävässä tunnistustekniikassa pitää muun muassa pyrkiä välttämään turhaa moninkertaista kirjautumista.

Tekniikan keräämien tunnistustietojen tulee olla viranomaisten tarpeen mukaan saatavilla, jotta voidaan esimerkiksi todistaa milloin, mistä, millä laitteella ja kenen toimesta mahdollinen väärinkäytös on tapahtunut. Näiden tietojen säilytyksessä palveluntarjoajan tuleekin kiinnittää huomiota turvallisuusnäkökohtiin ja tiedon eheyteen. Palveluntarjoaja voi olla esimerkiksi tele- tai internetoperaattori

yksityisille ja yritysasiakkaille tai yhteisötilaajana yritys, jonka tiedonsiirtojärjestelmän kautta työntekijät tai muut käyttäjät pääsevät verkon palveluihin. Teletunnistustietojen käsittelystä palveluntarjoajalla tai yrityksellä on velvollisuus kirjata muun muassa käsittelyajankohta ja henkilö, joka tietoja käsitteli sekä syy, joihin tietoja tarvittiin.

2.3 Teletunnistetiedot

2.3.1 Teletunnistetietoihin liittyvät viranomaismäärittelyt

Teleyrityksiä on kahdenlaisia, verkkoyrityksiä ja palveluyrityksiä. Verkkoyritykset tarjoavat viestintäverkon, joka voi olla esimerkiksi puhelinverkko tai tiedonsiirtoverkko, palveluyritysten käytettäväksi esimerkiksi viestien siirtoon. Palveluyrityksiä ovat muun muassa kiinteän- ja matkaviestinverkon puhelinpalveluiden tarjoajat ja internetpalveluiden tarjoajat (ISP eli Internet Service Provider). (Viestintävirasto 2004b.)

Sähköisen viestinnän tietosuojalaki sääntelee teleyritysten oikeutta käsitellä viestinnän tunnistamis- ja paikkatietoja. Laissa myös määrätään teleyritys velvolliseksi huolehtimaan palvelujensa turvallisuudesta, ja tämän nojalla on teleyrityksille myös annettu oikeus puuttua asiakasyrityksen välittämään viestintään, mikäli palvelun tietoturvallisuus uhkaa vaarantua, esimerkiksi sulkemalla asiakasyrityksen liittymät tai palvelut. (Viestintävirasto 2004b.)

Vuonna 2004 Viestintävirasto on perustanut lähinnä teleyritysten edustajista koostuvan Telcosec-työryhmän selvittämään tietoturvallisuus- ja tietosuoja-alueiden tulkintakysymyksiä ja vaihtamaan yleistä tietoa viestintämarkkinalain ja sähköisen viestinnän tietosuojalain sekä niiden pohjalta annettavien määräysten osalta. (Viestintävirasto 2004b.) Ohje sähköisen viestinnän tietosuojalain 15 §:n mukaisesta teleyritysten velvollisuudesta tallentaa tunnistamistietojen käsittelytiedot on valmisteltu Telcosec-työryhmässä (Viestintävirasto 2005a).

Teleyrityksellä on velvollisuus kerätä tunnistetietoja, joilla käyttäjät on kyettävä tunnistamaan. Lisäksi teleyrityksellä on oikeuksia näiden tietojen käsittelyyn muun muassa väärinkäytösten selvittämiseksi.

2.3.2 Teletunnistetietojen käsittely

Teleyrityksellä on oikeus viestinnän tunnistamistietojen käsittelyyn palvelun toteuttamiseksi, laskuttamiseksi sekä huolehtiakseen palvelun tietoturvasta. Oikeus käsittelyyn on myös viestinnän teknisen vian havaitsemiseksi sekä palvelun teknistä kehittämistä varten. Tilaajan tai käyttäjän suostumuksella voidaan tunnistetietoja käyttää myös muiden palveluiden markkinoimiseksi. Myös joissain väärinkäytöstilanteissa, joissa esimerkiksi verkkopalvelun yksittäistä maksullista palvelua käytetään maksutta tai oikeudettomasti, voidaan tunnistamistietoja käsitellä asian selvittämiseksi. (Viestintävirasto 2004c.)

Liittymän tai päätelaitteen maantieteellisen sijainnin ilmaisevaa ja muuhun kuin verkkopalvelun tai viestintäpalvelun toteuttamiseen käytettyä tietoa kutsutaan paikkatiedoksi. Kun tätä paikkatietoa käytetään, viestinnän välittämiseen on kyse tunnistamistietojen käsittelystä eikä paikkatietojen käsittelystä. Tällöin tulee soveltaa lain mukaisia säännöksiä tunnistamistietojen käsittelystä. (Viestintävirasto 2004d.)

Tunnistamistietojen käsittelyä rajoitetaan teleyrityksen oikeudella käsitellä tietoja vain sen verran, kun tarkoitus edellyttää. Käsittelyllä ei saa myöskään rajoittaa välttämätöntä enempää luottamuksellisen viestin ja yksityisyyden suojaa. (Viestintävirasto 2004c.)

Teleyritys saa myös luovuttaa tunnistamistietoja ainoastaan niille osapuolille, joilla on oikeus käsitellä tietoja tapauksesta riippuen. Mikäli teleyritys on ulkoistanut osan palveluidensa tuottamisesta, on sillä oikeus luovuttaa tunnistamistietoja niille osapuolille, joilla on oikeus niitä käsitellä. Näidenkin tietojen käsittelyn lainmukaisuudesta vastaa teleyritys. (Viestintävirasto 2004c.)

Teleyritystä ja mahdollisia muita osapuolia koskee aina myös vaitiolovelvollisuus tunnistamistietoja koskien. Viestien tai niiden tunnistamistietojen käsittelyn jälkeen ne on tuhottava tai muutettava muotoon, jossa niitä ei voida yhdistää käyttäjään tai tilaajaan ellei laissa muuta määrätä. (Viestintävirasto 2004c.)

3 KÄYTTÄJIEN TUNNISTUS ETHERNET-VERKOISSA

3.1 Ethernet-tekniikan perusteet

Ethernet on nykyään maailman eniten käytetty (lähi)verkkotekniikka, joka kehitettiin 1970-luvun puolivälissä ja standardoitiin 1983 IEEE 802.3 -standardiksi (Institute of Electrical and Electronics Engineers) sekä vuonna 1989 ISO 88203 -standardiksi (International Organization for Standardization). Ethernet:n kehitystyötä jatketaan edelleen ja aika-ajoin IEEE 802.3 -standardiperheeseen lisätään uusia standardeja.

Ethernet perustuu alun perin jaettuun väylään, johon kaikki verkkolaitteet kytketään. Myöhemmin Ethernet on muuttunut pääosin kytkentäiseksi, jolloin kytkimeltä (switch) on oma väylä jokaiselle päätelaitteelle. Jaettua ja kytkentäistä Ethernetiä voidaan kuitenkin myös yhdistää. MAC (Media Access Control) on protokolla, jossa on menetelmät tiedon välitykseen sekä jaetussa että kytkentäisessä Ethernetissä (Jaakonhuhta 2005, 83).

Sanomia Ethernet-verkossa kutsutaan kehyksiksi (frames). Ethernetissä käytetään päätyypiltään kolmenlaisia kehyksiä, jotka ovat unicast, multicast sekä broadcast. Unicast-kehyksiä käytetään kahden laitteen väliseen liikennöintiin, multicast-kehyksiä yhdeltä laitteelta monelle tapahtuvaan liikenteeseen ja broadcast-kehyksiä yhdeltä laitteelta kaikille tapahtuvaan liikennöintiin. (Jaakonhuhta 2005, 83-84.)

Ethernetissä on käytössä CSMA/CD-tekniikka (Carrier Sense Multiple Access with Collision Detection). Se on jaetulle siirtotielle (Multiple Access) kehitetty kanavallepääsymenetelmä, jossa ensin kuunnellaan, onko siirtotie vapaa (Carrier Sense) ja lähetetään tieto vasta sitten. Menetelmässä on myös törmäyksen tunnistusominaisuus (Collision Detection), jolla havaitaan törmäys, mikäli useampi lähde lähettää tietoa siirtotielle samaan aikaan. Lähettävä laite kuuntelee linjaa ja mikäli se huomaa törmäyksen, se lähettää siirtotielle sotkua törmäyksen merkiksi. Tämän jälkeen lähettäjä odottaa satunnaisen ajan, jonka jälkeen se yrittää

udelleenlähetystä. Uudelleenlähetysyritykset on rajoitettu 16:een. (Anttila 2000, 50-51.)

Törmäysalue (collision domain) käsitteellä kuvataan aluetta eli verkon osaa, jossa kaikki laitteet kuulevat toistensa lähetykset. Tämä alue voi olla yksittäinen kaapelisegmentti tai toistimilla yhdistettyjä kaapeleita. Törmäysalueen kokoa voidaan rajoittaa laitteilla kuten silta, kytkin tai reititin. (Jaakonhuhta 2005, 89; Anttila 2000, 51.)

Ethernet-tekniikassa on myös käsite levitysviestialue (broadcast domain). Tämän alueen sisällä broadcast-kehyksissä kulkevat levitysviestit tavoittavat kaikki alueella olevat päätelaitteet. Tämä pätee myös keskittimien avulla tähtimäiseen topologiaan rakennetuissa verkoissa. Levitysviestit kulkevat myös silta-laitteiden yli ja näin ollen myös, moniporttisillaksi kutsutun, kytkimen kaikkiin portteihin. Levitysviestialueita voidaan rajata joko OSI-viitemallin (Open Systems Interconnection) kolmannen kerroksen, OSI-3, eli verkkokerroksen laitteilla, kuten reitittimillä tai OSI-viitemallin toisen kerroksen, OSI-2, eli siirtoyhteyskerroksen kytkimillä, käyttämällä VLAN-ominaisuutta (Virtual Local Area Network) eli virtuaalilähiverkkoja. (Jaakonhuhta 2005, 90, 24; Anttila 2000, 43-47; Jaakonhuhta 2005, 162-163.)

3.2 Nykyiset Ethernet-verkkototeutukset

3.2.1 Alkuperäisen käyttötarkoituksen laajentuminen

Ethernetin alkuperäinen käyttötarkoitus oli jakaa siirtotie mahdollistaen useamman käyttäjän pääsyn verkon palveluihin. Ethernet-tekniikkaa oli alun perin tarkoitus käyttää vain rajoitetulla alueella, yleensä lähiverkoissa, johtuen tekniikan ominaisuuksista. Nykyisin Ethernet-tekniikan kehityttyä on sitä alettu käyttää aina enenevissä määrin pidemmillä välimatkoilla myös alue- ja runkoverkoissa.

Ethernet on muun muassa korvaamassa ATM-tekniikkaa (Asynchronous Transfer Mode) operaattoreiden runkoverkoissa. ATM-tekniikka on kallista, ja se vaatii enemmän erikoisosaamista. Useimmat laitevalmistajat ovat tuoneet markkinoille

muun muassa DSLAM-laitteita (Digital Subscriber Line Access Multiplexer), joissa on ATM-liitännän asemasta Ethernet-liitäntä. Nämä DSLAM-laitteet liitetään runkoverkoissa usein OSI-3 -tasolla toimivaan eli reitittävään Ethernet-kytkimeen. (Jaakonhuhta 2005, 239-240.)

3.2.2 Runko-, alue-, liityntä- ja kiinteistöverkot

Runkoverkot ovat korkean suorituskyvyn omaavia ja eri alueverkkoja, kuntia ja kaupunkeja yms. yhdistäviä verkkoja. Runkoverkot toteutetaan pääasiassa valokuidulla johtuen pitkistä välimatkoista ja suurista tiedonsiirtonopeuksista.

Alueverkot ovat tietyn maantieteellisen alueen kattavia, esimerkiksi kaupungin tai yliopiston, verkkoja (Jaakonhuhta 2005). Alueverkot sisältävät kiinteistö- ja liityntäverkot.

Liityntäverkot ovat verkkoja, joiden avulla eri kiinteistöverkot liittyvät alueverkoiksi ja runkoverkkoon. Liityntätekniikkana voi toimia esimerkiksi jokin DSL-tekniikka (Digital Subscriber Line) tai Ethernet. Liityntäverkkojen tiedonsiirtonopeudet vaihtelevat usein tarpeesta riippuen sadoista kilobiteistä sekunnissa jopa useisiin gigabitteihin sekunnissa.

3.3 Nykyiset tekniset toteutukset käyttäjän tunnistukseen Ethernet-verkoissa

3.3.1 Taustat ja tarpeet käyttäjän tunnistukseen

Ethernet-tekniikka on yleistynyt nopeasti erilaisissa liityntä- ja asiakasverkoissa johtuen sen edullisuudesta ja laajasta laitetarjonnasta. Lait puolestaan velvoittavat palveluntarjoajaa keräämään tarvittavaa tietoa käyttäjän tunnistamiseksi tarvittaessa. Tämän vuoksi palveluntarjoajalla on velvollisuus ja oikeus tarvittavien tietojen keräämiseen.

Tarvittavan tunnistuksen toteuttamiseen on olemassa useita eri tekniikoita, joita käytetään eri kokoisissa ja tyyppisissä verkoissa. Tunnistustekniikat poikkeavat

toisistaan muun muassa palveluntarjoajan kannalta tekniikan vaatiman ylläpidon suuruudessa ja asiakkaan kannalta tekniikan läpinäkyvyydessä.

3.3.2 MAC-osoitteiden tunnistus

Tämä tunnistustekniikka perustuu päätelaitteiden verkkosovittimen fyysisen eli MAC-osoitteen tietämiseen. Kun verkkosovitin kommunikoi verkon aktiivilaitteen, esimerkiksi kytkimen, kanssa, liikenne sallitaan vain etukäteen hyväksytyille verkkosovittimille MAC-osoitteen perusteella. MAC-osoitteen tunnistaminen, tai MAC-suodatus, tapahtuu yleensä aktiivilaitteen pääsylistojen tai porttikohtaisten määritysten avulla. Mikäli MAC-osoite löytyy pääsylistoilla sallituista osoitteista tai porttikohtaisista määrityksistä, sen liikennöinti voidaan sallia kokonaan tai rajoitetusti pääsylistan mukaisesti. Jos taas MAC-osoite on tuntematon, liikennöinti kielletään useimmiten kokonaan, mutta myös rajoitettu liikennöinti on mahdollista pääsylistan mukaisesti.

MAC-tunnistus sopii yleensä hyvin pieniin verkkoihin, joissa käyttäjämäärä pysyy kohtuullisena eikä aktiivilaitteita ole paljon. Tämä sen vuoksi, että sallittujen MAC-osoitteiden hallinta pääsylistoilla on työlästä suuremmissa ympäristöissä ja varsinkin asiakasverkoissa, joissa käyttäjiä ovat yksityiset henkilöt. Tämän tekniikan käyttö puolustaa kuitenkin tarkoitustaan yksityisissä LAN-verkoissa (Local Area Network) eli ’langallisissa’ lähiverkoissa ja WLAN-verkoissa (Wireless Local Area Network) eli langattomissa lähiverkoissa sekä kaupunkialueilla toimivissa kaupallisissa WLAN-verkoissa, joissa asiakas vuokraa verkkosovittimen palveluntarjoajalta.

MAC-suodatuksen palveluntarjoaja toteuttaa WLAN-verkossa sallimalla liikennöinnin tukiasemiensa kautta verkkoon vain vuokraamiensa verkkosovittimien MAC-osoitteista. ’Langallisissa’ lähiverkossa MAC-osoitteiden suodatus tapahtuu esimerkiksi määrittämällä palveluntarjoajan toimesta ennakkoon kytkimen porttiasetuksiin tai pääsylistoihin asiakkaan verkkosovittimen MAC-osoite sallituksi osoitteeksi ja kieltämällä muiden MAC-osoitteiden pääsy verkkoon. MAC-osoitteiden tunnistus ei kuitenkaan anna sellaisenaan keinoja hyvän tietoturvan saavuttamiseksi.

Väärinkäytösten jäljitys voi olla hankalaa vaikka DHCP-palvelimen lokitiedostoon jää käyttäjän päätelaitteen verkkosovittimen verkko- eli IP-osoite (Internet Protocol) ja fyysinen eli MAC-osoite, mutta tieto siitä mistä DHCP-kysely tuli löytyy vain aktiivilaitteiden MAC-osoitetauluista ja ARP-välimuisteista (Address Resolution Protocol), joita ei normaalisti tallenneta mihinkään.

3.3.3 PPP-over-Ethernet

Point-to-Point Protocol over Ethernet eli PPPoE tai PPP-over-Ethernet on määritelty IETF:n (Internet Engineering Task Force) dokumentissa RFC 2516 (Request For Comments). Se määrittää, kuinka useat isännät (hosts) jaetussa Ethernetissä voivat muodostaa PPP-istunnon (Point-to-Point Protocol) useisiin kohteisiin yhden tai useamman siltaavan modeemin kautta. Tarkoituksena on ollut, että tekniikkaa käytettäisiin laajakaistaisten liityntätekniikoiden kanssa, jotka luovat sillatun Ethernet-topologian, samalla säilyttäen PPP:n istunnon muodostustavan. (IETF 1999.)

PPPoE-tekniikka tarjoaa mahdollisuuden kytkeä usean käyttäjän verkko palveluntarjoajalle yhden yksinkertaisen siltaavan laitteen kautta ja silti yksilöidä muun muassa yhteyksien pääsyn hallinnan ja laskutuksen. Jotta PPP-istunto voidaan muodostaa Ethernet-verkon yli, niin jokaisen PPP-istunnon täytyy tietää vastapään MAC-osoite ja muodostaa yksilöllinen istuntotunnus eli SESSION ID. Tämä tapahtuu PPPoE-tekniikan sisältämällä alustus- eli discovery-protokollalla. (IETF 1999.)

PPPoE-tekniikassa käyttäjän tunnistus perustuu tekniikan osalta fyysisen MAC-osoitteen ja istuntotunnuksen määritykseen ja tallentamiseen lokitiedostoihin. Käyttäjän tietokoneella täytyy olla PPP-client -ohjelmisto, jonka avulla yhteys muodostetaan ja kirjaudutaan verkkoon käyttäjätunnuksella ja salasanalla.

PPPoE-tekniikka on verkon topologiasta riippumaton ja täten erittäin hyvä ja käyttökelpoinen liityntätekniikka uusissa ja myös vanhemmissa verkkoympäris-

töissä. Tekniikkaa on käyttänyt jo pitkän aikaa muun muassa Oulun Puhelin Oyj laajakaistaliittymiensä käyttäjätunnistustekniikkana.

Käytön kannalta PPPoE-tekniikan miinuspuolena on tunnusten käyttö verkkoon kirjauduttaessa. Tämä vaatii palveluntarjoajalta kirjautumispalvelimen, palvelimen ylläpidon sekä käyttäjien opastuksen PPP-client -ohjelmiston käytössä ja mahdollisesti myös ohjelmiston hankinnassa. PPP-client -ohjelmisto sisältyy muun muassa Microsoft Windows XP ja Vista -käyttöjärjestelmiin.

3.3.4 DHCP ja DHCP option-82

DHCP-protokolla on määritetty IETF:n dokumentissa RFC 2131, ja protokolla mahdollistaa lukuisten asetusten, kuten IP-osoitteen välittämisen asiakastietokoneille TCP/IP-verkossa (Transmission Control Protocol / Internet Protocol). Asetusten välittämisen jälkeen asiakastietokoneiden on mahdollista liikennöidä verkossa. (IETF 1997).

Perinteisesti DHCP-protokollalla tapahtuva käyttäjän tunnistus perustuu usein DHCP-palvelimelle määritettyihin sääntöihin, joiden perusteella asiakaslaitteille jaetaan IP-osoitteita ja muita tietoja verkosta. Väärinkäytöstapauksissa käyttäjä tunnistetaan DHCP-palvelimen lokitiedostoon tallennetuista asiakaslaitteiden MAC-osoite – IP-osoite pareista. Näistä tiedoista ei kuitenkaan selviä, mistä kysely on tullut, vaan tämän tiedon saamiseksi joudutaan etsimään tieto dokumentoinnista.

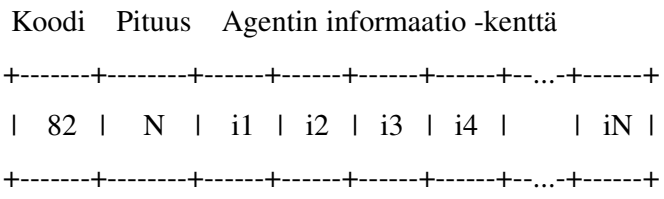
Uutena tekniikkana on DHCP-protokollaan lisätty option-82 -lisätietokenttä eli Relay Agent Information Option, jonka avulla voidaan välittää käyttäjän tunnistamiseen riittävät tiedot DHCP-palvelimelle. DHCP option-82 -lisätietokentän käyttö ja toiminta on määritelty IETF:n dokumentissa RFC 3046 vuonna 2001.

DHCP option-82 -kenttä lisätään, DHCP Relay Agent -laitteen eli DHCP-välitysagentin toimesta, asiakkaalta palvelimelle suuntautuviin DHCP-paketteihin. Palvelimet, jotka tunnistavat option-82 -kentän, voivat käyttää kentän sisältämää tietoa IP-osoitteen tai muiden parametrien osoittamissääntöihin. DHCP-palvelin

kopioi option-82 -kentän vastausviestiinsä täysin samanlaisena, kun palvelin lähettää vastauksen asiakkaalle. (IETF 2001.)

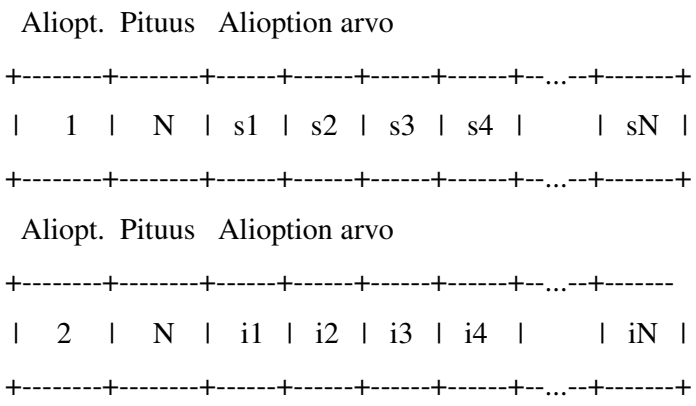
DHCP Relay Agent Information Option -kenttä on järjestäytynyt yhdeksi DHCP-lisätietokentäksi, joka sisältää yhden tai useampia alioptioita (sub-option). Alioptiot kuljettavat DHCP-välitysagentin muodostamaa tietoa asiakkaasta. Esimerkiksi piirin liityntälaitteessa sijaitsevalle DHCP-välitysagentille on määritetty nimetyt alioptiot. Näitä ovat muun muassa Circuit ID -tunnus kuvaamaan liityntää, josta liikennöidään verkkoon ja Remote ID -tunnus asiakastunnuksen kuvaamiseen. (IETF 2001.)

Relay Agent Information Option -kenttä on niin sanottu ’säiliö’ optio tietyille välitysagentin tarjoamille alioptioille (IETF 2001). Kenttä on kuvion 1 mukainen.



KUVIO 1. Relay Agent Information Option -kenttä. (IETF 2001)

Koodi-kentässä on option numero eli tässä tapauksessa 82. Pituus N kertoo Agentin informaatio -kentän pituuden okteteissa. Agentin informaatio -kenttä koostuu sarjasta alioptio/pituus/arvo -tietueita jokaista alioptiota kohti. Alioptiot koodataan kuvion 2 tavalla. (IETF 2001.)



KUVIO 2. Alioptio-tietueet (IETF 2001)

Alioptio-kentässä on alioption tunnusnumero eli koodi, pituus-kentässä alioption pituus okteteissa ja alioption arvo -kentissä itse informaatio. DHCP-välitysagentin alioptiot ovat merkitty eli koodattu taulukon 1 mukaisesti. Kuviossa 3 on puolestaan esimerkki Cisco Systems:n käyttämistä alioptio-kentistä Ethernet-kytkimissä.

TAULUKKO 1. DHCP Relay Agent -alioptiot (IETF 2001)

DHCP-välitysagentin alioption koodi	Alioption kuvaus
1	Agentin Circuit ID -alioptio
2	Agentin Remote ID -alioptio

DHCP option-82 -kentän lisääminen tulisi olla määritettävissä, ja sen pitäisi olla oletuksena poiskytkettynä. Välitysagenteilla tulisi olla erilliset määrittelyt jokaiselle alioptiolle ohjaamaan sitä, lisätäänkö alioptio asiakkaalta palvelimelle meneviin paketteihin. (IETF 2001.)

Välitysagentin lisätessä Relay Agent Information Option -kenttää DHCP-pakettiin pitää kenttä lisätä viimeiseksi optioksi DHCP-optiot -kenttään, mutta kuitenkin ennen End Option -kenttää, jos paketissa sellainen on. Tämä tulee tehdä kaikkiin tunnistettuihin asiakkaalta palvelimelle välitettäviin BOOTP-paketteihin (Bootstrap protocol) tai DHCP-paketteihin. (IETF 2001.)

Välitysagenttien pitää pudottaa epäluotetusta piiristä vastaanotettu DHCP option-82 -kentän sisältävä DHCP-paketti, jossa giaddr-arvo (gateway IP address) on asetettu nollaksi. Nollaksi asetettu giaddr-osoite eli oletusyhdyskäytävän IP-osoite ilmaisee välitysagenttien olevan ensimmäisen hypyn reitittimiä. Edellä mainitun tapauksen sattuessa pitää myös virhelaskuria kasvattaa. (IETF 2001.)

Luotettu piiri voi sisältää luotetun silta- tai kytkinlaitteen, joka sijaitsee alavirrassa (downstream) eli lähempänä asiakasta, asiakkaan ja välitysagentin välillä. Tämä luotettu verkkolaite voi lisätä DHCP option-82 -kentän asettamatta giaddr-osoitetta. Tässä tapauksessa välitysagentti ei lisää ’toista’ DHCP option-82 -kenttää mutta välittää DHCP-paketin muuten normaalin DHCP-välitysagentin toimintojen mukaisesti asettaen giaddr-osoitteen sopivaksi katsomallaan tavalla. (IETF 2001.)

Luotettujen ja epäluotettujen piirien erottamiseen käytetyt mekanismit poikkeavat piirin liityntälaitteen tyypin mukaisesti, ja ne saattavat sisältää paikallista hallintaa. Esimerkiksi kaapelimodeemien terminointijärjestelmä voi usein pitää asiakkaan kaapelimodeemilta tulevia ylävirran (upstream) paketteja epäluotettuina, mutta ATM-kytkin, joka terminoi DSLAM:n läpi kytketyt VC:t (Virtual Channel) eli virtuaalikanavat voi pitää näitä virtuaalikanavia luotettuina ja hyväksyä DSLAM:n lisäämän DHCP option-82 -kentän. (IETF 2001.)

Välitysagenteilla voi olla määritetty maksimikoko DHCP-paketille, joka muodostetaan DHCP option-82 -kentän lisäämisen jälkeen. Paketit, jotka ylittäisivät tämän määritetyn arvon, mikäli DHCP option-82 -kenttä niihin lisättäisiin, välitetään ilman kyseistä kenttää. Virhelaskuria kasvatetaan myös tässä tapauksessa. Jos maksimikokomääritystä ei ole, niin DHCP-paketin maksimikoon raja-arvona, jonka yli välitysagentti ei saa pakettia kasvattaa, toimii paketin kohderajapinnan MTU-arvo (Maximum Transfer Unit). (IETF 2001.)

Välitettäessä vastausviesti palvelimelta takaisin asiakkaalle pitää siitä poistaa DHCP option-82 -kenttä, jonka palvelin kopioi sellaisenaan kyselyviestistä vastaukseen. Poiston suorittaa sama laite, joko välitysagentti tai luotettu alavirran verkkolaite, joka lisäsi kentän kyselyviestiin. (IETF 2001.)

DHCP-välitysagentit, joihin kytkentäinen tai kiinteä piiri on terminoitu eli päätetty voivat lisätä Agentin Circuit ID -alioption DHCP option-82 -kenttään. Agentin Circuit ID -alioptio muodostaa paikallisen tunnisteen DHCP-välitysagentin liitynnälle, josta DHCP-asiakkaan paketti DHCP-palvelimelle vastaanotettiin. Circuit ID -tunnus on tarkoitettu DHCP-välitysagentin käyttöön, kun välitysagentti välittää DHCP-vastaukset takaisin oikeaan liityntään. Agentin Circuit ID -kenttää on mahdollista käyttää esimerkiksi

- reitittimen rajapinnan numerolle tai
- kytkevän keskittimen portin numerolle. (IETF 2001.)

DHCP-palvelimet voivat käyttää Agentin Circuit ID -tunnusta sääntöihin, joiden avulla määritetään IP- sekä muita parametreja. Circuit ID -tunnusta tulisi ajatella läpinäkyvänä arvona ja osoitettujen sääntöjen tulisi perustua vain tarkalleen vastaavaan merkkijonoon. Palvelin ei saisi myöskään jäsennellä Circuit ID -tunnusta sisäisesti. (IETF 2001.)

DHCP-palvelimen tulisi raportoida sen hetkisten osoitevarausten Circuit ID -arvot tilastolliseen raporttiin ja lokeihin. Koska Circuit ID -tunnus on paikallinen vain tietylle DHCP-välitysagentille, tulisi Circuit ID sallia vain yhdessä DHCP-välitysagentin yksilöivän giaddr-osoitteen kanssa. (IETF 2001.)

DHCP-välitysagentit, joihin kytkentäinen tai kiinteä piiri on terminoitu eli päätetty ja joilla on mekanismi tunnistaa etäisäntä piirin toisessa päässä voivat lisätä Agentin Remote ID -alioption DHCP option-82 -kenttään. Remote ID -kenttää voidaan käyttää koodaamaan esimerkiksi

- kaapelimodeemin ID -tunnuksen tai
- point-to-point -linkin etäpään IP-osoitteen. (IETF 2001.)

Remote ID -tunnuksen täytyy olla yleismaailmallisesti yksilöllinen. DHCP-palvelimet voivat käyttää Remote ID -alioptiota valitakseen parametreja tietyille käyttäjille, isännille tai tilaajamodeemeille. Myös Remote ID -tunnusta tulisi ajatella läpinäkyvänä arvona ja osoitettujen sääntöjen tulisi perustua vain tarkalleen vastaavaan merkkijonoon. Palvelin ei saisi myöskään jäsennellä Remote ID -tunnusta sisäisesti. (IETF 2001.)

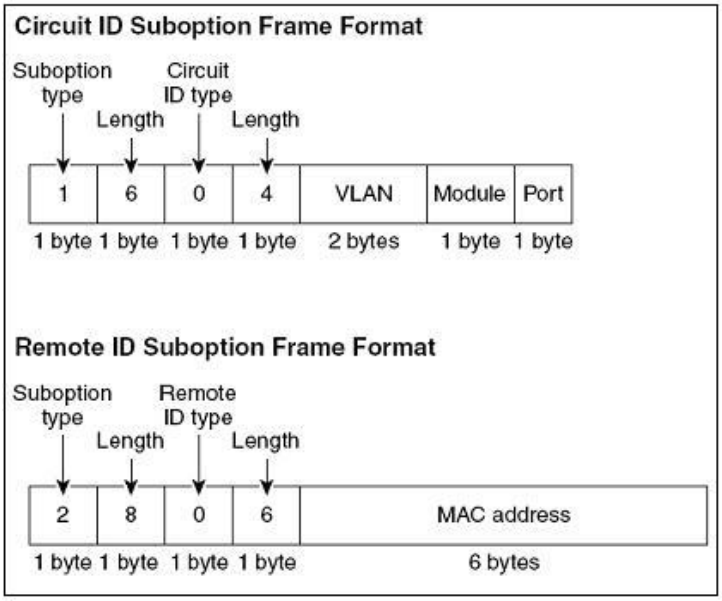
Välitysagentti voi käyttää Remote ID -kenttää Circuit ID -kentän sijaan tai sen lisänä valitakseen piirin, johon DHCP-vastaussanoma välitetään. DHCP-palvelimien tulisi raportoida Remote ID -arvo kaikkiin raportteihin, jotka liittyvät tiettyyn DHCP-asiakkaaseen. (IETF 2001.)

DHCP Relay Agent Information Option ratkaisee useita pulmakysymyksiä ympäristössä, jossa epäluotetut isännät pääsevät internetiin piiripohjaisen julkisen verkon kautta. Tämä ratkaisu olettaa, että kaikki DHCP-protokollaliikenne julkisilta isänniltä kulkee DHCP-välitysagentin kautta ja IP-verkko välitysagentin ja DHCP-palvelimen välillä on vaarantamaton. (IETF 2001.)

Seuraavassa on esitetty DHCP option-82 -tekniikan ominaisuuksia ja käytäntöjä, jotka IETF on määrittänyt RFC 3046 dokumentissaan:

- Normaalisti levitysviestinä lähetetty DHCP-vastaus välitetään piirin liityntälaitteesta vain siihen piiriin, joka Agentin Circuit ID -tunnuksessa on mainittu.
- Yleisesti ottaen DHCP-palvelimen ominaisuuksia voidaan laajentaa säilyttämään tietokannassa asiakkaan IP-osoitteen ja MAC-osoitteen lisäksi myös asiakkaan Remote ID -tunnusta.
- DHCP-palvelimen tulisi toteuttaa säännöt, jotka rajoittavat useamman osoitteen osoittamisen yhdelle Remote ID -tunnukselle.
- DHCP-palvelin voi käyttää Remote ID -tunnusta osoitettavan IP-osoitteen valintaan. DHCP-palvelin voi myös sallia kiinteiden IP-osoitteiden määrittämisen tietyille Remote ID -tunnuksille sekä estää valtuuttamattomien Remote ID -tunnusten osoitepyynnöt.

- Piirin liityntälaite voi liittää toisiinsa, DHCP-palvelimen määrittämän ja DHCP ack -paketissa eteenpäin välittämän, IP-osoitteen sekä piirin, johon paketti välitettiin. Piirin liityntälaite voi myös estää IP-pakettien välityksen sellaisista IP-osoitteista, joita se ei ole liittänyt vastaanottaviin piireihin. Edellä mainittu ehkäisee yksinkertaisia IP-väärennös hyökkäyksiä lähiverkkoa vastaan sekä toisen isännän esittämistä väärennetyllä IP-osoitteella.
- Välitysagentin tarjoamaa Remote ID -tunnusta käyttämällä ei DHCP-palvelimella ole tarvetta käyttää epäluotettua ja vielä standardoimatonta asiakastunniste kenttää.
- Liittämällä asiakkaan MAC-osoitteen Agentin Remote ID -tunnukseen voi DHCP-palvelin ehkäistä IP-osoitteen tarjoamista hyökkääjälle, joka on väärentänyt MAC-osoitteensa vastaamaan toista isäntää mutta IP-osoitepyyntö tulee eri Remote ID -tunnuksella. (IETF 2001.)



KUVIO 3. Cisco Systems:n Ethernet-kytkimissä käyttämät alioptiokentät (Cisco 2004.)

Circuit ID:	Esim. 0004018f0003
1-tavun tyyppikenttä,	00 = Circuit ID tyyppi = 0
1-tavun pituuskenttä,	04 = Circuit ID pituus = 4-tavua
2-tavun VLAN ID-kenttä,	018f = VLAN ID = 399
1-tavun MODuulin numerokenttä ja	00 = MODuuli = 0
1-tavun PORTin numero kenttä.	03 = PORTti = 3 + 1 = 4, koska lasku alkaa nollasta mutta numerointi yhdestä

Remote ID:	Esim. 00060013c46c5600
1-tavun tyyppikenttä,	00 = Remote ID tyyppi = 0
1-tavun pituuskenttä,	06 = Remote ID pituus = 6-tavua
6-tavun mittainen liityntäkytkimen MAC-osoite	0013c4 = MAC- osoitteen kolme ensimmäistä tavua osoittavat laitteen valmistajan = tässä tapauksessa Cisco 6c5600 = liityntäkytkimen MAC-osoitteen kolme viimeistä tavua, yksilöllinen osa laitteen MAC-osoitetta

3.4 Toteutuksiin liittyvän problematiikan kuvaus

MAC-osoitteiden tunnistus ei sovellu suuriin ’langallisiin’ lähiverkkoihin, joissa liityntä verkkoon tapahtuu asiakkaan omalla verkkosovittimella. Tämä johtuen suuritöisestä asiakkaiden verkkosovittimien MAC-osoitteiden määrittämisestä verkon aktiivilaitteisiin sekä dokumentaatioon.

PPPoE-tekniikassa problematiikka on lähinnä siinä, että asiakkaan pitää osata käyttää tekniikkaa, jossa verkkoyhteys avataan kirjautumisella. Asiakkaan kirjautumista vaativat järjestelmät ovat usein hankalia ongelmien esiintyessä, koska niihin liittyy aina inhimillisiä seikkoja esimerkiksi kirjautumistunnusten kirjoitusvirheiden vuoksi. Lisäksi tekniikassa käytettävien erillisten PPP-client -ohjelmistojen tarjoaminen ja näiden käytön opastaminen on työlästä palveluntarjoajalle.

Perinteisessä DHCP-tunnistuksessa ongelmat ovat vastaavia kuin MAC-osoitteiden tunnistuksessa, koska DHCP-palvelimen asetuksien tekemiseen palveluntarjoaja joutuu käyttämään paljon aikaa.

DHCP option-82 -tekniikassa problematiikkaa saattaa tuottaa tekniikan uutuus ja eri valmistajien laitteiden mahdolliset yhteensopivuusongelmat.

3.5 Ratkaisumallit ja niiden tehokkuus

Käyttäjän tunnistus MAC-osoitteiden tunnistuksessa voi toimia joustavasti langattomissa verkoissa silloin, kun palveluntarjoajalla on tiedossa vuokraajan verkkosovittimen tiedot. Verkkoon kirjautumisen ehtona voidaan lisäksi käyttää erilaisia liikenteen salausavaimia, joilla saavutetaan lisätietoturvaa. ’Langallisessa’ lähiverkossa puolestaan käyttäjän tunnistuksen toteuttaminen vaatii erittäin tarkkaa ja työlästä liityntäporttien käyttäjäkohtaista määrittämistä sekä dokumentointia. Esimerkiksi asiakkaan vaihtaessa päätelaitettaan pitäisi uuden laitteen verkkosovittimen MAC-osoite päivittää kytkimen asetustiedostoon ja dokumentointiin. Väärinkäytöstilanteissa sekä WLAN- että LAN-verkoissa DHCP-palvelimen lokitietoja pitää verrata käyttäjän verkkosovittimen MAC-osoitteeseen, joka joudutaan etsimään ylläpidetystä dokumentaatiosta tai aktiivilaitteiden asetustiedostoista.

PPPoE-tekniikassa käyttäjän tunnistukseen käytetään kirjautumispalvelinta, jolla käyttäjien tietoja ja oikeuksia hallitaan yhdessä PPP-client -ohjelmistojen kanssa käytettävien käyttäjätunnus – salasana parien kanssa. Kirjautumispalvelin vaatii myös palveluntarjoajan ylläpitoa, joka täytyy huomioida tunnistustekniikkaa valitessa.

PPPoE-tekniikassa on käytössä myös erilaisia kirjautumistekniikoita, kuten ilman PPP-client -ohjelmistoa käytettävä www-pohjainen SSL-VPN -tekniikka (Secure Socket Layer–Virtual Private Network), jossa kirjautumisavaimena voi toimia esimerkiksi avaimenperässä kulkeva vaihtuvan salasanan tekniikka. Väärinkäytöstilanteissa kirjautumispalvelimelta löytyvät asiakkaan tiedot, joita voidaan verrata väärinkäytöksestä epäillyn IP-osoitetietoihin.

Perinteisen DHCP:n avulla toteutettu käyttäjän tunnistus perustuu aiemmin mainitun mukaisesti palvelimeen määritettyjen sääntöjen perusteella jaettaviin IP-osoitteisiin ja niihin liitettyihin asetuksiin. Väärinkäytöstilanteissa DHCP-palvelimen lisäksi joudutaan käymään läpi myös dokumentointia, jotta saadaan selville kaikki tarvittavat tekijät.

DHCP option-82 -tunnistustekniikka tuo helpotusta perinteiseen DHCP-tunnistustekniikkaan välittämällä DHCP-palvelimelle suoran tiedon asiakaspäätelaitteen sijainnista. Tämä oleellisesti yksinkertaistaa väärinkäytösten selvittämistä.

DHCP option-82 -tunnistustekniikka on kompromissi vahvan PPPoE-tunnistustekniikan ja heikompien MAC- ja perinteisen DHCP-tunnistustekniikoiden välillä. DHCP option-82 -tekniikka on helppokäyttöinen palveluntarjoajalle, koska ei tarvita erillistä kirjautumispalvelinta tai työläitä MAC-osoitemäärityksiä aktiivilaitteisiin ja dokumentaatioon. DHCP option-82 -tekniikka ei myöskään vaadi asiakkaalta mitään toimia, vaan tunnistusprosessi tapahtuu automaattisesti palveluntarjoajan laitteistossa.

4 TAPAUS OPPILASTALO OY:N VERKKOTOTEUTUS

4.1 Yleinen kuvaus

Oppilastalo Oy on perustettu 11.9.1969 lahtelaisten ammatillisten oppilaitosten toimesta. Oppilastalo Oy omistaa tai hallinnoi vuokramiehenä useita kiinteistöjä Lahden keskustassa, Paavolassa, Ankkurissa, Mukkulassa, Kiveriössä, Möysässä sekä asemantaustassa. Oppilastalo Oy tarjoaa asiakkaillensa myös mahdollisuuden internetyhteyteen, joka veloitetaan vuokranmaksun yhteydessä. (Oppilastalo 2006).

Oppilastalo Oy on tehnyt sopimuksen internetpalveluiden tarjoamisesta, kiinteistöjä yhdistävän alueverkon ja kiinteistöjen lähiverkkojen ylläpidosta Päijät-Hämeen Puhelin Oyj:n kanssa. Päijät-Hämeen Puhelin Oyj omistaa pääosan verkkoon kytketyistä aktiivilaitteista sekä vastaa niiden hankinnoista ja ylläpidosta sopimuksen mukaisesti.

Oppilastalo Oy:n asuntojen määrä on kasvanut vuosien aikana kovasti ja jatkaa kasvuaan koko ajan. Tällä hetkellä asuntoja on noin 700. Internetpalveluiden tarjoamiseen ja käyttäjien tunnistamiseen on käytettävä tekniikkaa, joka toimii kaikissa kiinteistöissä.

4.2 Lähtötilanne

Oppilastalo Oy:n verkko koostuu Lahden ympäristössä sijaitsevien oppilas-asuntokiinteistöjen lähiverkoista sekä niitä yhdistävästä Päijät-Hämeen Puhelin Oyj:n Oppilastalo Oy:lle vuokraamasta liityntäverkosta, joka tarjoaa pääsyn runkoverkon palveluihin. Verkon asiakasrajapinta on toteutettu pääosin Ethernet-tekniikalla, yhdessä kohteessa on käytössä HomePNA-tekniikka, mikä johtuu kiinteistön kaapeloinnista. Verkon asiakasrajapinnassa on käytössä vielä n. 100 kpl Ethernet-keskittimiä, jotka tullaan korvaamaan kytkimillä insinöörityön aikana. Liityntäyhteydet lähiverkkoihin on toteutettu pääosin, ITU-T:n G.991.2 standardista poikkeavilla, 4,6 tai 9,2 Mbit/s nopeuksilla toimivilla G.SHDSL-yhteyksillä, yhtä tai kahta kuparikaapeliparia käyttäen, mutta myös 100 Mbit/s valokuituyhteyksiä

on käytetty mikäli kohteeseen on rakennettu valokuitukaapelointi. Verkkokuva lähtötilanteesta löytyy liitteestä (LIITE 1).

4.3 Verkon uudistaminen

4.3.1 Laitevalinnat

Laitetoimittajille lähetettiin tarjouspyynnöt, joissa mainittiin, että laitteiden ominaisuuksiin tuli sisältyä muun muassa pienet fyysiset mitat, monipuoliset etäoperointimahdollisuudet sekä tuki DHCP option-82 -tunnistustekniikalle. Lisäksi laitteiden tuli toimia yhdessä vanhojen laitteiden kanssa, ja niiden tuli mahtua huoneistoissa jo olemassa oleviin pieniin laitekaappeihin. Tarjouspyyntöjä tehdessä huomioitiin myös jo käytössä ja hyödynnettävissä olevat laitteet sekä asennustilat.

Tarjous saatiin vain yhden laitevalmistajan laitteista, koska muilla valmistajilla ei vielä ollut tarjota laitetta, joka tukisi DHCP option-82 -tunnistustekniikkaa. Näin päädyttiin hankkimaan Cisco Systems -merkkisiä laitteita, joita verkossa oli jo ennestään.

Cisco Systems, Inc. on maailmanlaajuinen johtaja internetin verkotuksessa. Yrityksen tuotteet ovat yleisesti ottaen laadukkaita ja monipuolisia, ja niitä käytetään yleisesti operaattoritason laitteina sekä runko- että liityntäverkoissa. Laitteet sisältävät myös kattavat tietoliikenteen analysointi ominaisuudet, joita tarvitaan ongelmatilanteiden selvityksissä ja uusien ominaisuuksien käyttöönottojen yhteydessä. Hankittuihin laitteisiin sisältyi lisäksi DHCP option-82 -tunnistustekniikka ilman lisähintaa.

4.3.2 Tekninen toteutus

Oppilastalon verkon runkokytkimenä palveluntarjoajan tiloissa toimi Cisco Systems Catalyst 3550, joka on reitittävä monipalvelukytkin. Catalyst 3550 -kytkin tarjoaa korkeaa käytettävyyttä, palvelun laatua (QoS, Quality of Service) ja turvallisuutta parantamaan verkon toimintoja. Laajoilla Fast Ethernet ja Gigabit

Ethernet konfigurointi mahdollisuuksilla Catalyst 3550 -kytkin on vahva lisä yritys- ja alueliityntäsovelluksiin.

Catalyst 3550 -kytkin on varustettu 24:llä, 100 Mbit/s -nopeudella toimivalla, Fast Ethernet -kupariportilla sekä kahdella GBIC-liitännällä (GigaBit Interface Converter), joihin saadaan kytkettyä erilaisten GBIC-muuntimien avulla 1 Gbit/s -nopeudella toimivia kupari- tai valokuituyhteyksiä.

KUVIO 4. Cisco Systems Catalyst 3550 -sarjan kytkimet.

Jakelu/liityntäkytkiminä kiinteistöjen talojakamoissa tai pääristikytkentäpisteissä käytettiin Cisco Systems Catalyst 2950-24 -kytkimiä. Catalyst 2950-24 -kytkimet kuuluvat Catalyst 2950 -sarjan kytkimiin, jotka ovat erillisiä, hallittavia 10/100 Mbit/s -kytkimiä käyttäjien kytkentään pienissä ja keskisuurissa verkoissa.

Catalyst 2950-24 -kytkimet on varustettu runkokytkimen tapaan 24:llä, 100 Mbit/s -nopeudella toimivalla, Fast Ethernet -kupariportilla sekä kahdella GBIC-liitännällä, joihin saadaan kytkettyä erilaisten GBIC-muuntimien avulla 1 Gbit/s -nopeudella toimivia kupari- tai valokuituyhteyksiä.

KUVIO 5. Cisco Systems Catalyst 2950-24 -kytkin.

Huoneistojakamoissa käytettiin liityntäkytkiminä Cisco Systems Catalyst 2940-8TT -kytkimiä. Catalyst 2940-8TT -kytkimet ovat pieniä, erillisiä, hallittavia kytkimiä, joissa on 8 kpl, 100 Mbit/s -nopeudella toimivia, Fast Ethernet -kupariportteja sekä yksi 1 Gbit/s -nopeudella toimiva kupariportti kytkentään verkkoon päin.

Catalyst 2940 -sarjan kytkimet on suunniteltu sijoitettavaksi ristikytkentäkaappien ulkopuolelle loppukäyttäjien työpisteisiin, kuten luokkatiloihin tai neuvotteluhuoneisiin. Catalyst 2940 -kytkimissä on kestävä metallikuori, hiljainen käyntiääni, helpot asennusmahdollisuudet sekä ura lukitusta varten.

KUVIO 6. Cisco Systems Catalyst 2940-8TT -kytkin.

Kaikissa verkossa käytetyissä Cisco Systems:n Catalyst -sarjojen kytkimissä on erittäin laajat asetusmahdollisuudet erilaisiin verkkototeutuksiin. Kytkimissä on Cisco IOS -käyttöjärjestelmä (Internetwork Operating System), jota voidaan päivittää tarvittaessa ja näin laitteisiin saadaan tulevaisuudessakin uusia ominaisuuksia. Laitteiden etähallinta onnistuu joko merkkipohjaisesti pääteohjelmalla käyttäen telnet-protokollaa tai Cisco Network Assistant -ohjelmistolla www-selaimella.

Cisco Systems C7200 (7206VXR NPE-400) -reititin on modulaarinen reititin yritysten ja palveluntarjoajien reunasovelluksiin. Cisco 7206VRX -kehikossa on kuusi vaakasuoraa moduulipaikkaa erilaisille moduulikorteille. Reititin tarjoaa jopa 2 Mpps:n (Millions of packets per second) suorituskyvyn reitityksessä.

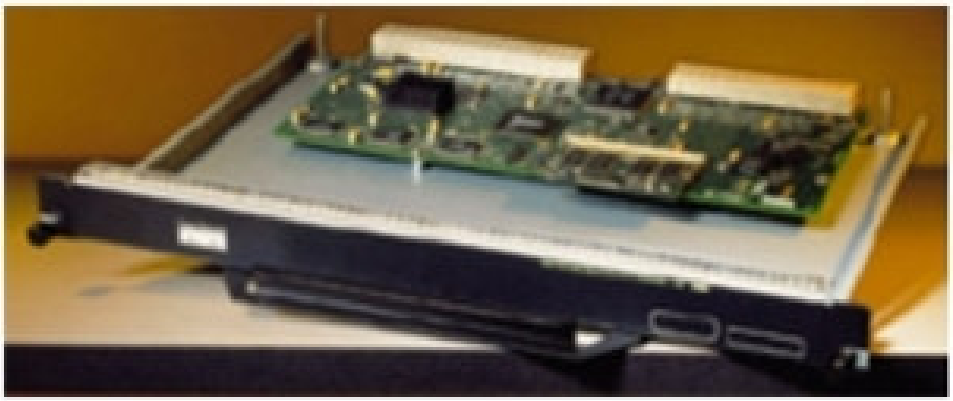
NPE-400 -moduuli sisältää muun muassa seuraavat ominaisuudet:

- suorituskyky jopa 400 kpps (kilo packets per second) CEF-kytkennässä (Cisco Express Forwarding)
- prosessorin modulaarisuus ja päivitettävyys
- 350-MHz (Megahertz) RM7000A RISC -prosessori (Reduced Instruction Set Computer)
- 4 megatavun L3 -välimuisti

- 128 megatavun SDRAM (Synchronous Dynamic Random Access Memory) -vakiomuisti, joka on laajennettavissa 512 megatavuun
- 16 megatavun pakettimuisti 128/256 megatavun SDRAM-muistilla ja 32 MB pakettimuisti 512 megatavun SDRAM-muistilla
- ECC-tuki (Error Code Correction).

Reititin ei ole ainoastaan Oppilastalon verkon käytössä, vaan sitä käytetään myös muiden PHP:n asiakkaiden tarpeisiin sekä PHP:n oman liikenteen reitittämiseen.

KUVIO 7. Cisco Systems 7200 -sarjan reitittimet.



KUVIO 8. Cisco Systems NPE-400 -moduulikortti.

DHCP-palvelin oli tunnistuksen käyttöönottohetkellä ISC DHCP server -versiota 3.0.2, käyttöjärjestelmänä toimi Debian Linux 3.0 ’woody’, ja laitteistona toimi Dell-palvelin. DHCP-palvelin on kahdennettu, jolloin esimerkiksi toisen vikaantuessa toinen jatkaa toimintaa yksin asiakkaan tätä huomaamatta. DHCP-palvelimissa ei ole graafista käyttöliittymää, vaan käyttö on merkkipohjainen. DHCP-palvelimet ovat toimineet erittäin vakaasti ollen vuosia käytössä ilman ongelmia. Lisäksi palvelimien etuna oli kyky ottaa vastaan ja vastata DHCP option-82 -tunnistekentillä varustettuihin DHCP-kyselyihin, joita kaikki palvelimet eivät huomioineet. Nämä palvelimet toimivat myös muun muassa PHP:n laajakaistaliittymien DHCP-palvelimina.

Kaapelointina alueverkon runkoyhteyksillä on käytössä palveluntarjoajan kuparikaapeliverkko sekä joihinkin kiinteistöihin ulottuva valokuitukaapeliverkko. Valokaapeliverkon käyttöä laajennetaan tulevaisuudessa asiakkaan kaistantarpeiden mukaan.

Kiinteistöjen lähiverkoissa puolestaan on kaapelointina käytetty kategoria 5:n (CAT5, Category 5) tasoista suojaamatonta parikaapelia (UTP, Unshielded Twisted Pair) pois lukien yksi kohde, jossa on käytössä ainoastaan puhelinjohtosi-

säverkko. Kategorian 5 UTP-kaapelilla päästään standardien mukaan maksimissaan 100 Mbit/s siirtonopeuksiin. Myös kiinteistöjen talojakamoista huoneistojakamoihin kaapeloidut nousut on kaapeloitu samalla kaapelilla. Opinnäytetyön aikana ei kaapelointeihin tehty muutoksia, ja myös laitevalinnoissa painotettiin laitteiden sovittamista olemassa oleviin kaapelointeihin.

Ristikytkentä- ja työasema/laitekaapeleina käytetään suoraan kytkettyjä CAT5-tasoisia UTP-kaapeleita. Ristikytkentäkaapelit kuuluvat palveluntarjoajan vastuulle ja työasema/laitekaapeli ja sen hankinta puolestaan asiakkaan vastuulle.

4.3.3 Konfiguraatiot

Kytkinten asetusmuutoksia tehtiin useaan kertaan työn edistymisen aikana muun muassa päivittämällä ja muuttamalla laitenimiä ja porttikuvauksia, ottamalla käyttöön lisää virtuaalilähiverkkoja, lisäämällä liityntäportteihin turva- ja liikenteen hallinta ominaisuuksia sekä suurimpana kertamuutoksena DHCP option-82 -käyttäjätunnistuksen käyttöönotto. Runkokytkimen asetuksiin ei lisätty DHCP option-82 -komentoja, koska siihen ei suoraan liitetä asiakkaita. Liitteissä on esimerkit lopullisista konfiguraatioista liityntäkytkimen (LIITE 3), jakelu/liityntäkytkimen (LIITE 4) ja runkokytkimen (LIITE 5) osalta.

Reitittimiä konfiguroitiin ainoastaan muutaman kerran testausvaiheessa ja käyttäjän tunnistuksen käyttöönoton yhteydessä. Tunnistustekniikan testausvaiheessa käytettiin eri reititintä kuin toteutuksen yhteydessä. Liitteessä (LIITE 6) on esimerkki lopullisesta reitittimen/DHCP-välitysagentin konfiguraatiosta.

DHCP-palvelimien muutokset tehtiin Oppilastalon käyttöön määritettyyn DHCP-pooliin käyttäjätunnistuksen käyttöönoton yhteydessä. Testausvaiheessa käytettiin PHP:n laajakaistaliittymien käyttöön määritettyä DHCP-poolia, joka oli jo valmiiksi määritetty vastaanottamaan DHCP option-82 -tunnistekenttä. Liitteessä on esimerkki lopullisesta DHCP-palvelimen konfiguraatiosta (LIITE 7).

DHCP Relay Agent eli DHCP-välitysagentti on OSI-viitemallin kolmannen kerroksen, OSI-3, laite, joka välittää DHCP-paketteja DHCP-asiakkaan ja -palveli-

men välillä, kun ne ovat fyysisesti eri aliverkoissa. Välitysagentin välitystekniikka eroaa normaalista toisen kerroksen, OSI-2, välityksestä, jossa IP-paketit kytketään läpinäkyvästi verkkojen välillä. Välitysagentti vastaanottaa DHCP-sanomat ja luo uudet DHCP-sanomat ulkoverkon rajapinnasta lähetettäväksi.(Cisco 2004.)

DHCP snooping on Cisco Systems:n aktiivilaitteissaan käyttämä turvallisuusominaisuus. DHCP snooping tarjoaa verkkoturvallisuutta suodattamalla epäluotetut DHCP-sanomat ja kasaamalla sekä ylläpitämällä DHCP snooping binding -tietokantaa, jota kutsutaan myös DHCP snooping binding -tauluksi. (Cisco 2004.)

DHCP snooping käyttäytyy palomuurin tavoin epäluotettujen isäntien, eli DHCP-asiakkaiden, ja DHCP-palvelimen välillä. DHCP snooping -ominaisuutta voidaan käyttää myös loppukäyttäjille yhdistettyjen epäluotettujen porttien ja DHCP-palvelimelle tai toiselle kytkimelle yhdistettyjen luotettujen porttien erottamiseen. Kaikki DHCP-palvelimet on yhdistettävä kytkimeen luotettujen porttien kautta, jotta DHCP snooping -ominaisuus toimisi oikein. (Cisco 2004.)

Epäluotettu sanoma on sanoma, joka vastaanotetaan verkon ulkopuolelta tai palomuurilta. Käytettäessä DHCP snooping -ominaisuutta palveluntarjoajan ympäristössä, epäluotettu sanoma on lähetetty laitteelta, joka ei ole palveluntarjoajan verkossa eli esimerkiksi asiakkaan kytkimeltä. Tuntemattomien laitteiden sanomat ovat epäluotettuja, koska ne voivat olla liikennehyökkäysten lähteitä. (Cisco 2004.)

DHCP snooping binding -taulu sisältää MAC-osoitteen, IP-osoitteen, IP-osoitteen voimassaoloajan, sidostyypin, VLAN-tunnuksen ja portin tiedot, jotka vastaavat paikallisiin epäluotettuihin portteihin. Taulussa ei ole tietoa koskien luotettuihin portteihin kytkettyjä isäntiä eli asiakastietokoneita. (Cisco 2004.)

Palveluntarjoajan verkossa luotettu portti on kytketty samassa verkossa olevalle laitteelle. Kytkimen epäluotettu portti on yhdistetty saman verkon toiseen epäluotettuun porttiin tai verkon ulkopuolisen laitteen porttiin. (Cisco 2004.)

Kun kytkin vastaanottaa paketin epäluotetusta portista ja tämä portti kuuluu VLAN:iin, jossa DHCP snooping -ominaisuus on kytketty päälle, kytkin vertaa paketin lähteen MAC-osoitetta DHCP-asiakkaan laiteosoitteeseen. Kytkin välittää paketin vain osoitteiden ollessa samat ja muuten paketti pudotetaan. (Cisco 2004.)

Kytkin pudottaa DHCP-paketin jos jokin seuraavista tilanteista ilmenee:

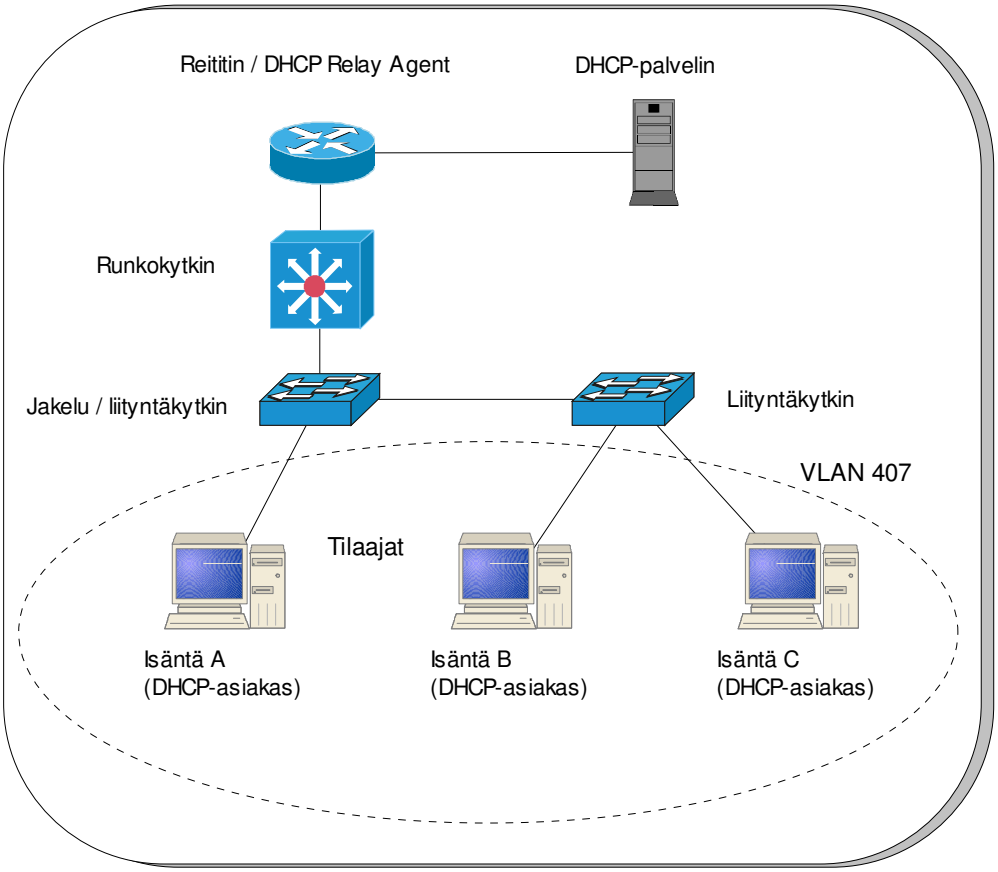
- DHCP-palvelimen paketti, kuten DHCP offer, DHCP ack, DHCP nak tai DHCP leasequery, vastaanotetaan verkon ulkopuolelta tai palomuurilta.
- Lähteen MAC-osoite ja DHCP-asiakkaan laiteosoite ei täsmää, kun paketti vastaanotetaan epäluotetusta portista.
- Kytkin vastaanottaa DHCP release tai DHCP decline -levityssanoman, joka sisältää DHCP snooping binding -taulusta löytyvän MAC-osoitteen, mutta binding-taulun porttitiedot eivät täsmää porttiin, josta sanoma vastaanotettiin.
- DHCP-välitysagentti välittää edelleen DHCP-paketin, joka sisältää välitysagentin IP-osoitteen ja kyseinen IP-osoite on jotain muuta kuin 0.0.0.0 tai välitysagentti välittää edelleen DHCP option-82 -tunnuksen sisältävän paketin epäluotettuun porttiin. (Cisco 2004.)

Kun DHCP option-82 -ominaisuus on otettu käyttöön kytkimessä, tunnistetaan tilaajalaite MAC-osoitteen lisäksi, sen kytkinportin perusteella, johon laite on kytketty. Useampi tilaajalähiverkon isäntä, eli asiakastietokone voi kytkeytyä samaan liityntäkytkimen porttiin, ja kaikki saavat yksilöllisen tunnisteen. (Cisco 2004.)

DHCP option-82 -ominaisuus on tuettu ainoastaan silloin, kun DHCP snooping -ominaisuus on otettu käyttöön kytkimen päätasolla sekä VLAN:eissa, jotka käyttävät tätä ominaisuutta ja joihin tilaajalaitteet on määritetty. (Cisco 2004.)

Kuvio 9 on esimerkki Ethernet-alueverkosta, jossa keskitetty DHCP-palvelin jakaa IP-osoitteet liityntäkytkimeen sekä jakelu/liityntäkytkimeen liitetyille tilaajille. DHCP-asiakkaat ja verkon DHCP-palvelin eivät sijaitse samassa IP-verkossa tai -aliverkossa, joten asiakkaiden ja palvelimen välissä olevaan DHCP-välitysagenttiin on määritetty DHCP-palvelimen osoitteen kertova helper address -

osoite. Helper address -osoite tarvitaan, jotta levitysviestien välitys saataisiin käyttöön ja DHCP-sanomat saataisiin siirtymään DHCP-asiakkaiden ja -palvelimen välillä (Cisco 2004).



KUVIO 9. DHCP Relay Agent Ethernet-alueverkossa.

DHCP option-82 -tunnistuksen käyttöönottamiseksi käytetyt komennot kytkimissä on esitelty taulukossa 2 ja reitittimessä eli DHCP-välitysagentissa käytetyt komennot puolestaan taulukossa 3.

TAULUKKO 2. DHCP option-82 -tunnistuksen käyttöönotossa käytetyt komennot jakelu- sekä liityntäkytkimissä.

Kofigurointitila	Komento	Toiminto
Globaali	ip dhcp snooping	tällä komennolla otetaan käyttöön DHCP snooping -ominaisuus
Globaali	ip dhcp snooping vlan *VLAN ID*	tällä komennolla määritetään missä VLAN:ssa DHCP snooping -ominaisuutta käytetään
Interface	ip dhcp snooping trust	tällä komennolla asetetaan kytkimen portti trusted-tilaan eli luotetuksi lähteeksi

TAULUKKO 3. DHCP option-82 -tunnistuksen käyttöönotossa käytetyt komennot reitittimessä eli DHCP-välitysagentissa.

Kofigurointitila	Komento	Toiminto
Globaali	ip dhcp relay information option	tällä komennolla otetaan käyttöön DHCP option-82 -kentän sisältävien DHCP-pakettien välitys
Globaali	ip dhcp relay information policy keep	tällä komennolla määritetään DHCP-välitysagentti säilyttämään paketin DHCP option-82 -kentän sisältämä tieto ennallaan
Globaali	no ip dhcp relay information check	tällä komennolla määritetään ettei reititin tarkista paketin DHCP option-82 -kentän sisältämää tietoa
Interface	ip dhcp relay information trusted	tällä komennolla asetetaan reitittimen portti/rajapinta trusted-tilaan eli luotetuksi lähteeksi

Kytkimien perusasetuksiin tehtiin työn aikana muutoksia paremman tietoturvan saavuttamiseksi. Lisäykset tehtiin pääasiassa liityntäportteihin, jotka on kytketty kiinteistön lähiverkon kaapelointiin ja sen kautta asiakkaiden päätelaitteisiin. Käyttöön otettiin kytkimien mahdollistamista ominaisuuksista muun muassa port-based traffic control ja sen porttikohtaisen liikenteen ohjauksen ominaisuuksista seuraavat: protected port, port-security ja storm-control. Tämän lisäksi asiakkaiden liityntäporteissa estettiin CDP-protokollan (Cisco Discovery Protocol) käyttö ja korvattiin mahdolliset asiakaslaiteilta tulevat, ja IEEE 802.1p -standardissa määritetyt, CoS liikenteen priorisointi -määritykset (Class of Service). Komennot näiden ominaisuuksien käyttöönottoon on esitetty taulukossa 4.

Protected port -ominaisuutta käytetään, kun jotkin sovellutukset vaativat, ettei liikennettä välitetä saman kytkimen eri porttien välillä niin, että yksi asiakas näkisi naapuriasiakkaan muodostamaa liikennettä. Tällaisessa ympäristössä protected port -ominaisuuden käyttö varmistaa, ettei saman kytkimen porttien välillä vaihdu unicast, multicast tai broadcast -liikennettä. (Cisco 2004.)

Potected port -ominaisuutta käyttävät portit toimivat seuraavasti:

- Potected port -portti ei välitä mitään liikennettä (unicast, multicast tai broadcast) suoraan toiseen protected port -porttiin. Tiedonvälitys ei toimi protected port -porttien välillä OSI-2 -tasolla, vaan kaikki protected port -porttien välinen liikenne kiertää reititettynä OSI-3 -tason laitteen kautta. Ainoastaan ohjausliikenne välitetään suoraan myös protected port -porttien välillä, koska ohjausliikenteen on muodostanut kytkimen CPU (Central Processing Unit) eli suoritin ja välitys tapahtuu ohjelman sisällä.
- Protected port -porttien ja muiden porttien välinen liikennöinti toimii normaalisti.
- Protected port -ominaisuus on tuettu myös 802.1Q trunk eli VLAN-runko-yhteyksillä.

Oletuksena protected port -ominaisuus ei ole päällä. (Cisco 2004.)

Protected port -ominaisuus otettiin käyttöön kaikissa asiakasrajapinnoissa eli liityntäporteissa sekä niissä välityskytkimien porteissa, joihin on liitetty liityntäkytkin. Tällä tavalla estetään, saman liityntäkytkimen sisällä OSI-2 -tasolla tapahtu-

van asiakasrajapintojen välisen liikenteen lisäksi, myös eri liityntäkytkimiin kytkettyjen asiakasrajapintojen välinen OSI-2 -tason liikenne jakelukytkimen kautta. Kyseinen liikenne ohjataan OSI-3-tason laitteelle ja sieltä edelleen mahdollisten pääsylistojen kautta vastaanottajalle toisen liityntäkytkimen asiakasrajapintaan.

Port-security -ominaisuutta voidaan käyttää rajoittamaan rajapinnan käyttöä rajaamalla ja tunnistamalla rajapintaan kytkettäväksi sallittujen päätelaitteiden MAC-osoitteita. Kun MAC-osoitteita osoitetaan rajapintaan, jossa port-security -ominaisuus on aktivoituna, ei rajapinta välitä paketteja muista kuin määritetyistä osoitteista. Rajapintaan pystytään osoittamaan MAC-osoitteita manuaalisesti, tai rajapinta voi oppia MAC-osoitteita dynaamisesti. Yhteen rajapintaan voi olla liitettynä 1 - 132 MAC-osoitetta ja kytkimeen yhteensä 1024 MAC-osoitetta. Osoitteiden maksimilukumäärä voidaan määrittää porttikohtaisesti, ja oletusasetus on yksi MAC-osoite porttia kohti. (Cisco 2004.)

Port-security -ominaisuus rajoittaa rajapinnan käyttöä valvomalla turvallisuusrikkeitä ja reagoimalla niihin halutulla tavalla. Turvallisuusrikkeiksi katsotaan seuraavat tapahtumat:

- Osoitetauluun on lisätty maksimimäärä turvallisia MAC-osoitteita mutta päätelaite, jonka MAC-osoite ei ole osoitetaulussa, yrittää pääsyä rajapintaan.
- Port-security -ominaisuudella varustettuun rajapintaan määritetty tai opittu MAC-osoite havaitaan toisessa Port-security -ominaisuudella varustetussa rajapinnassa samassa VLAN:ssa. (Cisco 2004.)

Rajapintaan voidaan määrittää yksi seuraavista kolmesta rikkomuksen vastaisista tiloista perustuen haluttuun toimintoon rikkeen tapahduttua:

- Protect eli suojaa – kun turvallisten MAC-osoitteiden lukumäärä saavuttaa porttiin sallitun määrän, pudotetaan paketit, joilla on tuntematon lähdeosoite, kunnes riittävä määrä turvallisia MAC-osoitteita poistetaan, tai sallittujen osoitteiden maksimimäärää lisätään. Turvallisuusrikkeestä ei ilmoiteta verkon valvojalle.

- Restrict eli rajoita – tämä tila on muuten vastaava kuin protect, mutta tässä tilassa verkon valvoja saa ilmoituksen turvallisuusrikkeestä. SNMP-trap (Simple Network Management Protocol) lähetetään, syslog-viesti lisätään lokiin ja rikelaskuria kasvatetaan.
- Shutdown eli sammuta – tässä tilassa turvallisuusrike johtaa välittömästi portin siirtymiseen error-disable -tilaan, eli virheen vuoksi suljettuun tilaan sekä portin LED-merkkivalon (Light Emitting Diode) sammumiseen. Myös SNMP-trap lähetetään, syslog-viesti lisätään lokiin ja rikelaskuria kasvatetaan. Shutdown on oletusasetus, kun port-security -ominaisuus otetaan käyttöön. (Cisco 2004.)

Sekä staattisille eli manuaalisesti osoitetuille että dynaamisille eli opituille turvallisille MAC-osoitteille voidaan asettaa ikääntymisaika, jonka jälkeen MAC-osoitteet poistetaan portin osoitetaulusta. Portit tukevat kahdentyyppistä ikääntymistä:

- Absolute – turvalliset osoitteet poistetaan portin osoitetaulusta tietyn ennalta asetetun ikääntymisajan jälkeen.
- Inactivity – turvalliset osoitteet poistetaan portin osoitetaulusta ainoastaan, jos ne eivät ole olleet käytössä ennalta asetetun ikääntymisajan aikana.

Tätä ominaisuutta voidaan käyttää, jos ei haluta manuaalisesti poistaa ja lisätä MAC-osoitteita turvallisiin osoitteisiin, mutta silti halutaan rajoittaa turvallisien MAC-osoitteiden määrää. Staattisesti osoitettujen turvallisten MAC-osoitteiden ikääntyminen voidaan ottaa käyttöön tai poistaa käytöstä porttikohtaisesti. Ikääntymisaika valitaan 0 - 1440 minuutin väliltä, mikäli ajaksi valitaan 0 niin ikääntyminen ei ole käytössä kyseisessä portissa. (Cisco 2004.)

Port-security -ominaisuus otettiin käyttöön kaikissa asiakasrajapinnoissa eli liityntäporteissa. Turvallisten MAC-osoitteiden maksimilukumääräksi porttia kohti asetettiin 10. Rikkomuksen vastaiseksi tilaksi asetettiin lievin mahdollinen, eli protect, koska ei katsottu tarpeelliseksi asettaa porttia error-disable -tilaan tai saada rikkeestä SNMP-trap -viestiä, vaan ainoastaan rajoittaa päätelaitteiden lukumäärää ja MAC-osoite huijauksia. MAC-osoitteiden ikääntymisajaksi asetettiin 10 minuuttia ja ikääntymistyypiksi käyttämättömyys. Täten 10 minuuttia käyttämättä olleen päätelaitteen MAC-osoite poistetaan osoitetaulusta.

Pakettimyrsky esiintyy, kun suuri määrä broadcast-, unicast- tai multicast-paketteja vastaanotetaan portista. Näiden pakettien välittäminen voi aiheuttaa verkon hidastumisen tai aikakatkaisun. Tämän ongelmatilanteen estämiseen tarkoitettu, storm control eli myrskynhallinta -ominaisuus asetetaan päälle koko kytkimeen, mutta se toimii porttikohtaisesti. Oletuksena myrskynhallinta on pois käytöstä. (Cisco 2004.)

Storm control -ominaisuus käyttää nousevaa ja laskevaa raja-arvoa estääkseen ja palauttaakseen broadcast-, multicast- tai unicast-pakettien välityksen. Kytkin voidaan asettaa myös sulkemaan portin, kun nouseva raja-arvo on saavutettu. (Cisco 2004.)

Storm control -ominaisuus käyttää jompaakumpaa seuraavista kahdesta keinosta liikennemäärän mittaamiseen:

- kaistanleveyteen perustuvaa tai
- liikennemäärää, jolla paketteja vastaanotetaan yksikkönä pps (packets per second) eli paketteja sekunnissa.

Raja-arvot voidaan esittää joko broadcast-, multicast- tai unicast-liikenteen käytettävissä olevana prosenttiosuutena kokonaiskaistanleveydestä tai määränä, jonka verran rajapinta vastaanottaa broadcast-, multicast- tai unicast-liikennettä (Cisco 2004.)

Oletuksena, pakettimyrskyn saavuttaessa määritetyn nousevan raja-arvon, suodatetaan liikenne, eikä SNMP-trap -viestiä lähetetä. Vaihtoehtoiseksi tai lisätoimenpiteeksi voidaan valita jompikumpi seuraavista:

- Shutdown eli sammuta – tässä tilassa pakettimyrsky johtaa rajapinnan siirtymiseen error-disable -tilaan ja SNMP-trap -viestin lähettämiseen.
- Trap eli viesti – tämä tila valitaan, jos halutaan muodostaa SNMP-trap -viesti pakettimyrskyn esiintyessä.

Mikäli toimenpiteeksi valitaan shutdown, täytyy portti avata uudelleen manuaalisesti pakettimyrskyn jälkeen. (Cisco 2004.)

Broadcast- eli levitysviestimyrskyn nousevaksi raja-arvoksi määritettiin 10 % asiakasrajapinnan kokonaiskaistanleveydestä 10 Mbit/s, jonka jälkeen toimitaan action-komennolla määritetyn toimenpiteen mukaisesti. Laskevaksi raja-arvoksi määritettiin puolestaan 8 % kokonaiskaistanleveydestä. Multicast- ja unicast-myrskyjen nouseviksi raja-arvoiksi määritettiin 2000 pakettia sekunnissa ja laskeviksi raja-arvoiksi 1000 pakettia sekunnissa. Jatkotoimenpiteet eivät poikkea pakettimyrskyn tapauksesta.

Toimenpiteeksi broadcast-, multicast- tai unicast-myrskyn sattuessa asetettiin trap. Tämä on oletuksena olevan suodatuksen (filtering) lisätoimenpide, joka lähettää SNMP-trap sanoman, jos myrsky ilmenee ja portista vastaanotettava liikenne suodatetaan. Liikennemäärän pudotessa laskevan raja-arvon alle palautetaan liikenteen välitys automaattisesti.

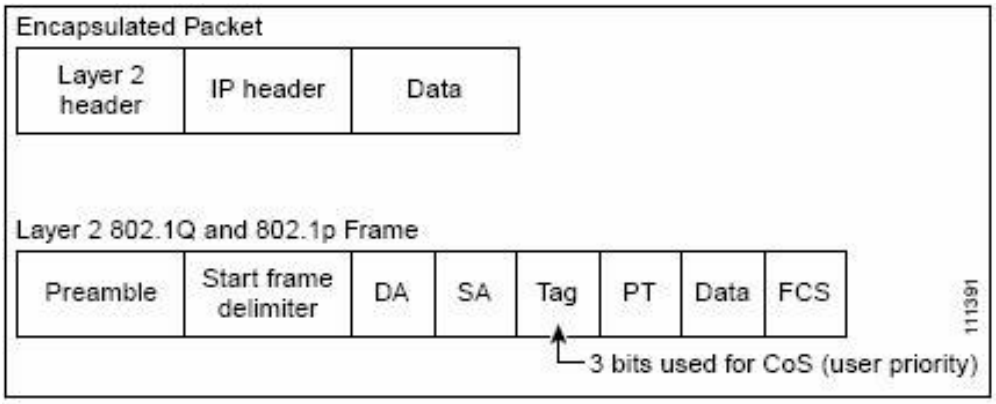
CDP-protokolla on laitteiden havaintiprotokolla, joka toimii OSI-2 -tasolla kaikissa Cisco-merkkisissä laitteissa ja mahdollistaa verkon-hallintaohjelmistojen havaita Cisco-laitteet, jotka on kytketty jo verkossa tunnettuihin Cisco-laitteisiin. Koska CDP toimii ainoastaan OSI-2 -tasolla, voivat mitkä tahansa kaksi järjestelmää oppia toisistaan CDP:n välityksellä. (Cisco 2004.) Oppilastalon verkossa CDP-protokollaa estettiin välittämään tietoa verkon aktiivilaitteista verkon ulkopuolelle poistamalla protokolla käytöstä liityntäporteissa.

Tyypillisesti verkot toimivat parhaan yrityksen toimitusperiaatteella, mikä tarkoittaa, että kaikki liikenne on samanarvoista ja kaikella liikenteellä on samanlainen mahdollisuus tulla toimitetuksi perille ajoissa. Myös ruuhkan esiintyessä on kaikella liikenteellä samansuuruinen mahdollisuus tulla pudotetuksi. (Cisco 2004.)

QoS eli palvelun laatuominaisuuksia voidaan käyttää hallitsemaan ja ehkäisemään verkon ruuhkautumistilanteita ja priorisoimaan tietoliikenteen eri laatuluokkia halutulla tavalla. Kun QoS otetaan käyttöön verkossa, tekee se verkon suorituskyvyn helpommaksi ennustaa ja kaistanleveyden käytöstä tehokkaampaa.(Cisco 2004.)

QoS-toteutus perustuu OSI-2 -tason kehysten priorisointi arvoihin. OSI-2 -tason 802.1Q-kehysotsikoissa on kahden tavun mittainen Tag Control Information -

kenttä, joka kuljettaa laatuluokka (CoS) arvoa kolmessa eniten merkitsevässä bitissä, joita kutsutaan User Priority eli käyttäjä prioriteetti biteiksi. Rajapinnoissa, jotka on määritetty OSI-2 -tason 802.1Q trunk -rajapinnoiksi, kaikki liikenne tapahtuu 802.1Q-kehyksillä paitsi liikenne hallinta VLAN:ssa. Muut kuin 802.1Q-kehystyypit eivät voi kuljettaa OSI-2 -tason CoS-arvoja. OSI-2-tason CoS-arvot ovat 0 - 7, jossa 0:lla on pienin ja 7:llä suurin prioriteetti. (Cisco 2004.)



KUVIO 10. QoS-luokitustasot paketeissa ja kehyksissä (Cisco 2004.)

QoS asettaa ennalta määritetyn CoS-arvon leimaamattomiin kehyksiin, jotka vastaanotetaan luotetuista ja epäluotetuista porteista. CoS-arvoksi voidaan määrittää arvo 0 ja 7 väliltä, ja mikäli arvoa ei määritetä, käytetään oletusarvoa 0. Käytettäessä komennossa avainsanaa override, saadaan mahdollinen aikaisempi CoS-arvo korvattua ennalta määritetyllä tai oletusarvolla. Oletuksena CoS override -ominaisuus ei ole käytössä. (Cisco 2004.)

Verkon käyttö ei olisi tasavertaista, mikäli osa verkon asiakkaista määrittäisi päätelaitteensa lisäämään paketteihin korkean prioriteetin CoS-arvon saavuttaakseen muita paremman palveluluokan. Tämän vuoksi liityntäporttien asetuksilla otettiin käyttöön CoS-override -ominaisuus, joka korvaa liityntäporteista tulevissa paketeissa mahdollisesti olevat CoS-arvot ennalta määritetyllä tai oletusarvolla. Oletusarvoa ei katsottu tarpeelliseksi muuttaa, vaan se säilytettiin arvossa 0.

TAULUKKO 4. Liityntäporttien turva- ja liikenteenohjausominaisuuksien käyttöönotossa käytetyt komennot.

Kofigurointitila	Komento	Toiminto
Interface	switchport protected	Otettiin käyttöön protected port -ominaisuus
Interface	switchport port-security	Otettiin käyttöön port-security -ominaisuus
Interface	switchport port-security maximum 10	Määritettiin turvallisten MAC-osoitteiden maksimilukumääräksi 10
Interface	switchport port-security aging time 10	Määritettiin turvallisten MAC-osoitteiden ikääntymisajaksi 10 minuuttia.
Interface	switchport port-security aging type inactivity	Määritettiin turvallisten MAC-osoitteiden ikääntymistavaksi käyttämättömyys.
Interface	switchport port-security violation protect	Määritettiin turvallisuusrikettä seuraavaksi tilaksi protect
Interface	storm-control broadcast level 10.00 8.00	Broadcast-myrskyn nousevaksi raja-arvoksi määritettiin 10 % ja laskevaksi raja-arvoksi 8 % kokonaiskaistanleveydestä .
Interface	storm-control multicast level pps 2000 1000	Multicast-myrskyn nousevaksi raja-arvoksi määritettiin 2000 pakettia sekunnissa ja laskevaksi raja-arvoksi 1000 pakettia sekunnissa.
Interface	storm-control unicast level pps 2000 1000	Unicast-myrskyn nousevaksi raja-arvoksi määritettiin 2000 pakettia sekunnissa ja laskevaksi raja-arvoksi 1000 pakettia sekunnissa.
Interface	storm-control action trap	Toiminnaksi broadcast-, multicast- tai unicast-myrskyn tapahtuessa asetettiin trap.
Interface	no cdp enable	Estetään CDP-protokollaa välittämästä tietoa aktiivilaitteista verkon ulkopuolelle
Interface	mls qos cos override	Korvataan liityntäportista vastaanotettujen pakettien mahdollinen palveluluokka (CoS) arvo oletusarvolla.

4.3.4 Käyttäjien tunnistuksen toteutus

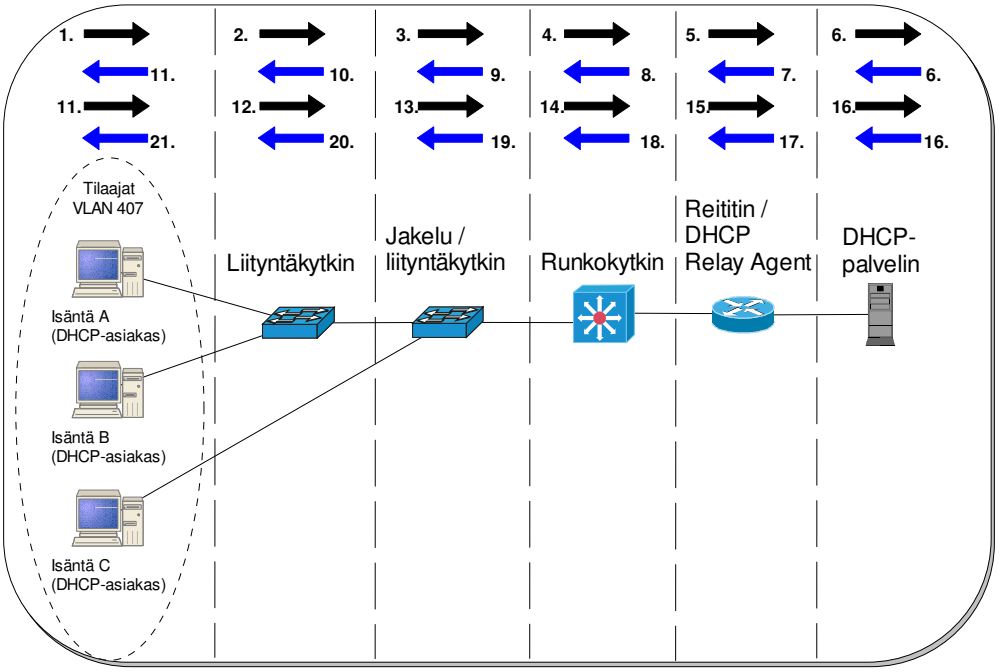
Käyttäjien tunnistuksen toteutus aloitettiin päivittämällä verkon kytkimien IOS-käyttöjärjestelmät versioihin, joissa tunnistustekniikka oli saatavilla. Tämän jälkeen suoritettiin noin sadan vanhan hub:n korvaaminen uusilla kytkimillä.

Kun asennukset oli saatu päätökseen, jatkettiin työtä tutkimalla DHCP option-82 -tunnistustekniikan toimivuutta PHP:n toimitiloihin rakennetussa testiympäristössä, johon kuului kaksi työasemaa, kaksi Cisco Catalyst 2940-8TT-kytkintä ja yksi Catalyst 2950-24 -kytkin. Testiympäristön Catalyst 2950 -kytkin liitettiin laitetilassa sijaitsevaan Oppilastalon verkon Catalyst 3550 -runkokytkimeen yleiskaapeloinnin välityksellä.

Testiympäristön kytkimiin luotiin VLAN-tunnus, joka oli käytössä PHP:n laajakaistaverkossa ja jossa käytettiin jo DHCP option-82 -tekniikkaa. Ensimmäinen testitavoite oli tutkia miten tunnistustiedot kulkisivat Ethernet-kytkimistä DHCP-välitysagenttina toimivalle reitittimelle ja edelleen DHCP-palvelimelle. Tutkimuksessa käytettiin kytkimien ja reitittimen liikenteen analysointi- ja vianetsintäominaisuuksia sekä työasemaan asennettua Ethereal-pakettianalysaattoriohjelmistoa.

Testiympäristössä käytiin tutkimuksen aikana läpi erilaisia asetusvaihtoehtoja, jotta löydettäisiin Oppilastalon verkkoon soveltuva ratkaisu asiakkaan tunnistetietojen välitykseen DHCP-välitysagentin avulla DHCP-palvelimelle. Liitteissä on kuvattu näitä tutkimuksia kuvien ja lokiviestien avulla (LIITE 8 - 14).

Kun oikeat asetukset olivat löydetty, oli aika alkaa suunnitella tunnistuksen käyttöönottoa. Käyttöönotetut asetukset selviävät taulukoista 2 ja 3.



KUVIO 11. DHCP-kysely, jossa option-82 -kenttä kuljettaa tunnistustietoa.

Seuraavassa on esitetty vaiheittain DHCP-kysely, jossa välitetään DHCP option-82 -kentän avulla asiakkaan tunnistustiedot DHCP-palvelimelle kuvion 11 mukaisesti:

1. Asiakkaan päätelaite tarvitsee IP-osoitteen ja lähettää DHCP discover -sanoman levitysviestinä verkkoon lähdeosoitteella 0.0.0.0 ja kohdeosoitteella 255.255.255.255.

2. Sanoma tulee liityntäkytkimelle portista, johon asiakkaan päätelaite on kytketty. Portti on määritetty VLAN:iin 407 ja DHCP snooping -ominaisuus on määritetty käyttöön tässä VLAN:ssa. Päätelaitteille tarkoitetut liityntäportit eivät ole luotettuja (trusted) portteja. DHCP snooping -ominaisuus keskeyttää levitysviestin ja lisää DHCP discover -sanomaan DHCP option-82 -kentän ja välittää sanoman eteenpäin. DHCP option-82 -kenttä sisältää Remote ID -tunnuksen, joka on liityntäkytkimen MAC-osoite sekä Circuit ID -tunnuksen, joka kuvaa liityntäporttia vlan-port-mod -muodossa. Sano-

man ollessa levitysviesti, se lähetettäisiin oletuksena koko verkkoon tai mikäli verkko on jaettu virtuaalilähiverkoilla, niin sanoma lähetettäisiin koko VLAN:iin, johon portti on liitetty. DHCP snooping -ominaisuus ohjaa sanoman ulos vain kaikkiin trusted-portteihin, jotka eivät ole protected-portteja.

3. Jakelu/liityntäkytkin vastaanottaa DHCP discover -sanoman liityntäkytkimeltä portista, joka on määritetty luotetuksi (trusted) portiksi. Koska sanoma tulee luotetusta portista ja se on levitysviesti, se lähetetään oletuksena koko verkkoon tai VLAN:iin, sanoman VLAN-tunnuksen mukaisesti. DHCP snooping -ominaisuus ohjaa paketin ulos kaikkiin luotettuihin portteihin, paitsi siihen, josta sanoma vastaanotettiin tai niihin, jotka ovat protected-portteja.

4. Runkokytkin, johon ei ole määritelty DHCP snooping -asetuksia, vastaanottaa DHCP discover -sanoman jakelu/liityntäkytkimeltä ja välittää sen koko VLAN:iin, ja täten myös ulos reitittimelle menevästä IEEE 802.1Q VLAN-trunk -portista.

5. Reitittimessä on otettu käyttöön DHCP Relay Information Option -ominaisuus, määritetty porttiasetuksissa runkokytkimelle kytketty portti luotetuksi portiksi ja se, ettei DHCP-välitysagentti korvaa DHCP option-82 -kenttää, vaan jättää sen ennalleen. DHCP-välitysagentti lisää tiedon sanomasta Relay Binding -tauluunsa. DHCP-välitysagentti asettaa myös sanoman giaddr-osoitteeksi sen rajapinnan IP-osoitteen, josta sanoma vastaanotettiin ja kohdeosoitteeksi DHCP-palvelimen IP-osoitteen, joka on määritetty IP helper address -komennolla sanoman vastaanottorajapinnan asetuksissa. Tämän jälkeen se välittää sanoman DHCP-palvelimelle unicast-viestinä.

6. DHCP-palvelin vastaanottaa ja käsittelee DHCP discover -sanoman, tallentaa asiakkaan tiedot osoitetauluunsa, joka varmistetaan lokitiedostoihin. Tämän jälkeen DHCP-palvelin palauttaa DHCP offer -sanoman takaisin DHCP-välitysagentille. DHCP-palvelin kopioi DHCP option-82 -kentän sellaisenaan DHCP discover -sanomasta DHCP offer -sanomaan. DHCP offer -sanoma lähetetään unicast-viestinä.

7. Kun DHCP offer -sanoma tulee DHCP-välitysagentille, DHCP-välitysagentti tarkistaa omasta DHCP relay binding -taulustaan DHCP offer -sanoman vastaavuuden DHCP discover -kyselyihin. Jos DHCP relay binding -taulussa ei ole vastaavuutta, pudotetaan paketti, mutta jos vastaavuus löytyy, välitetään DHCP offer -sanoma siihen rajapintaan, josta DHCP discover -sanoma tuli.

8. Runkokytkin vastaanottaa DHCP offer -sanoman välitysagentilta ja välittää sen levitysviestinä oikeaan VLAN:iin, sanoman VLAN-kentän mukaisesti.

9. Jakelu/liityntäkytkin vastaanottaa DHCP offer -sanoman runkokytkimeltä. DHCP snooping -ominaisuus keskeyttää levitysviestin ja avaa DHCP offer -sanoman DHCP option-82 -kentän tarkistaakseen, onko sanoma tarkoitettu kyseiselle jakelu/liityntäkytkimelle. DHCP snooping havaitsee, ettei sanoma ole tarkoitettu kyseiselle kytkimelle, koska DHCP option-82 -kentän Remote ID -tunnus ei täsmää jakelu/liityntäkytkimen MAC-osoitteeseen. DHCP snooping jättää DHCP option-82 -kentän DHCP offer -sanomaan ja välittää sanoman levitysviestinä eteenpäin kaikkiin muihin luotettuihin portteihin paitsi siihen, mistä sanoma vastaanotettiin.

10. Liityntäkytkin vastaanottaa jakelu/liityntäkytkimen välittämän DHCP offer -sanoman. Myös tässä tapauksessa DHCP-snooping -ominaisuus keskeyttää levitysviestin ja avaa DHCP option-82 -kentän tarkistaakseen, onko sanoma tarkoitettu kyseiselle liityntäkytkimelle. DHCP snooping tulkitsee sanoman paikalliseksi, koska DHCP option-82 -kentän Remote ID -tunnus on kyseisen liityntäkytkimen MAC-osoite. Tämän jälkeen DHCP snooping poistaa DHCP option-82 -kentän ja välittää sanoman tulkitsemansa Circuit ID -tunnuksen mukaiseen porttiin.

11. DHCP-asiakas vastaanottaa DHCP offer -sanoman. Seuraavaksi DHCP-asiakas muodostaa DHCP request -sanoman lähettää sen levitysviestinä verkkoon.

12. DHCP request -sanoma tulee DHCP-asiakkaalta liityntäkytkimelle. DHCP snooping -ominaisuus keskeyttää levitysviestin ja lisää DHCP request -sanomaan DHCP option-82 -kentän sekä välittää sanoman eteenpäin ohjaamalla sanoman vain kaikkiin trusted-portteihin, jotka eivät ole protected-portteja.

13. Jakelu/liityntäkytkin vastaanottaa DHCP request -levitysviestisanoman liityntäkytkimeltä. DHCP snooping -ominaisuus keskeyttää levitysviestin ja ohjaa sanoman vain kaikkiin luotettuihin portteihin, jotka eivät ole protected-portteja.

14. Runkokytkin vastaanottaa DHCP request -sanoman jakelu/liityntäkytkimeltä ja välittää sen koko VLAN:iin, ja täten myös ulos reitittimelle menevästä IEEE 802.1Q VLAN-trunk -portista.

15. DHCP-välitysagentti vastaanottaa DHCP request -sanoman ja jättää DHCP option-82 -kentän ennalleen. Tämän jälkeen se välittää sanoman DHCP-palvelimelle unicast-viestinä.

16. DHCP-palvelin vastaanottaa ja käsittelee DHCP request -sanoman ja lähettää DHCP ack -sanoman takaisin DHCP-välitysagentille unicast-viestinä. DHCP-palvelin kopioi DHCP option-82 -kentän sellaisenaan DHCP request -sanomasta DHCP ack -sanomaan.

17. DHCP ack -sanoman tullessa DHCP-palvelimelta DHCP-välitysagentille, DHCP-välitysagentti tarkistaa löytyykö sen omasta Relay Binding -taulusta tietoja välityksestä. Vastaavuus löytyy, ja DHCP-välitysagentti välittää DHCP ack -sanoman siihen rajapintaan, josta DHCP request -sanoma tuli. Tämän jälkeen DHCP-välitysagentti poistaa Relay Binding -taulustansa merkinnän välityksestä.

18. Runkokytkin vastaanottaa DHCP ack -sanoman DHCP-välitysagentilta ja välittää sen edelleen levitysviestinä oikeaan VLAN:iin, sanoman VLAN-kentän mukaisesti.

19. Jakelu/liityntäkytkin vastaanottaa DHCP ack -sanoman runkokytkimeltä, jolloin DHCP snooping -ominaisuus keskeyttää levitysviestin ja avaa option-82 -kentän tarkistaakseen, onko sanoma tarkoitettu jakelu/liityntäkytkimelle. DHCP option-82 -kentän Remote ID -tunnus ei täsmää jakelu/liityntäkytkimen omaan MAC-osoitteeseen, joten DHCP snooping välittää sanoman levitysviestinä eteenpäin kaikkiin muihin luotettuihin portteihin paitsi siihen, mistä sanoma vastaanotettiin.

20. Liityntäkytkin vastaanottaa DHCP ack -sanoman jakelu/liityntäkytkimeltä, jolloin DHCP-snooping -ominaisuus keskeyttää levitysviestin ja avaa DHCP option-82 -kentän tarkistaakseen, onko sanoma tarkoitettu liityntäkytkimelle. DHCP option-82 -kentän Remote ID -tunnus on liityntäkytkimen oma MAC-osoite, joten DHCP snooping tulkitsee sanoman paikalliseksi, poistaa DHCP option-82 -kentän ja välittää sanoman Circuit ID -tunnuksen mukaiseen liityntäporttiin.

21. DHCP-asiakas vastaanottaa DHCP ack -sanoman ja voi aloittaa liikennöinnin verkkoon.

Käyttöönotettu käyttäjien tunnistus onnistui teknisesti hyvin, ja se täyttää viranomaismääräysten vaatimukset. Edellä esitetyn sanomanvaihdon tapaan tiedot asiakkaan verkkosovittimesta, ja asiakkaan sijainnista välitetään DHCP-palvelimelle, jonka lokitiedostoihin tiedot tallentuvat. DHCP-palvelimen lokitiedostoja varmistetaan ja säilytetään laissa määrätyn ajan.

4.4 Valmis verkko

4.4.1 Dokumentointi

Verkon dokumentaatio päivitettiin työn aikana. Tähän dokumentointiin kuuluvat verkkokuvat, IP-osoitteiden rekisteri ja aktiivilaitteiden konfguraatiotiedostot.

Verkkokuvat on tehty erikseen joka kohteesta (LIITE 2), ja niistä löytyy muun muassa aktiivilaitteiden kuvaukset ja IP-osoitteet sekä liityntäyhteyksien tyypit ja

nopeudet. IP-osoiterekisterissä on aktiivilaitteiden hallintaan tarvittavat IP-osoitteet. Aktiivilaitteiden konfguraatiotiedostoista ilmenevät muun muassa, mihin huoneeseen mikäkin liityntäkytkimen porteista on kytketty. Verkon dokumentteja säilytetään palveluntarjoajan tietojärjestelmässä ja siitä otetuissa varmistuksissa.

4.4.2 Käyttäjien kokemukset

Tunnistustekniikkaa koskien verkon käyttäjiltä saatu palaute on jäänyt vähäiseksi, koska tunnistustekniikka ei näy suoraan käyttäjille vaan heidän yhteytensä verkkoon toimivat kuten ennenkin. Välittömästi käyttöönoton jälkeen joillakin käyttäjillä ilmeni ongelmia verkkoyhteyden kanssa, mutta niistä selvittiin tietokoneen uudelleen käynnistyksellä. Nämä ongelmat aiheutuivat siitä, ettei tiedotettamme muutoksen suorittamisesta tiettynä ajankohtana oltu huomioitu, vaan tietokoneet olivat päällä muutoksen aikana.

Sen sijaan positiivista palautetta käyttäjiltä on saatu mahdollisuudesta valita nopeusluokka muutamasta vaihtoehdosta. Tämä on ollut näkyvin muutos käyttäjille ja se innostikin useita käyttäjiä vaihtamaan nopeusluokan omiin tarpeisiin perustuen.

5 TULOKSET JA JOHTOPÄÄTÖKSET

Suunnitelmana työssä oli ensin luoda tekninen valmius tietoverkon käyttäjien / päätelaitteiden tunnistamistietojen keräämiseen ja välittämiseen eteenpäin internetpalveluntarjoajalle, tunnistamistietojen lainmukaista arkistointia varten. Käyttäjätunnistustekniikkaa valittaessa vertailtiin muun muassa eri tekniikoiden ominaisuuksia, arvioitiin niiden käytössä tarvittavaa ylläpidon määrää sekä tunnistuksen helppoutta asiakkaille. Vertailluiksi tekniikoiksi valittiin MAC-osoitteiden tunnistus, PPPoE, perinteinen DHCP sekä DHCP option-82. Tämän jälkeen tehtävänä oli edellä mainitun vertailun perusteella valitun tunnistustekniikan käyttöönotto. Lisäksi suunnitelmiin kuului päivittää verkon dokumentointi, suorittaa verkon parannustöitä muun muassa ottamalla käyttöön verkon tietoturvatasoa parantavia aktiivilaitteiden ominaisuuksia sekä luoda verkon käyttäjille vaihtoehtoisia liittymänopeusluokkia. Tavoitteena oli suunnitelman asteittainen toteuttaminen onnistuneesti touko - elokuun 2005 aikana.

Käyttäjätunnistustekniikoiden vertailussa havaittiin että toimintaperiaatteeltaan MAC-osoitteiden tunnistus on yksinkertainen, mutta yksinkertaisuudestaan johtuen tunnistustekniikkaa on myös helppo huijata. MAC-osoitteiden tunnistuksen käyttö vaatii palveluntarjoajalta myös jatkuvaa laiteasetusten ja dokumentoinnin ylläpitotyötä. PPPoE-tunnistustekniikka puolestaan on tekniikoista monipuolisin ja sillä saadaan liitettyä käyttäjätunnistukseen myös muunlaisia käyttäjäoikeussovelluksia. PPPoE-tekniikan miinuspuolina on erillisen kirjautumispalvelimen tarve ja ylläpito sekä tekniikan kanssa usein käytettävien client-ohjelmistojen tarjoaminen sekä opastaminen asiakkaille. PPPoE-tekniikassa ongelmia voivat lisäksi aiheuttaa verkkoon kirjautumiseen tarvittavien käyttäjätunnusten ja salasanojen muutokset ja unohdukset. Perinteisen DHCP-tunnistustekniikan positiivisiin puoliin kuului tekniikan yksinkertaisuus, koska tällä tekniikalla voidaan tunnistus toteuttaa helposti verkossa, jossa on jo DHCP-palvelin. Perinteisen DHCP-tunnistustekniikan miinuspuoliksi havaittiin muun muassa väärinkäytöksien selvityksen hankaluus. DHCP option-82 -käyttäjätunnistustekniikan havaittiin vertailussa toimivan hyvänä kompromissina muihin tekniikoihin verrattuna. DHCP option-82 -tunnistus ei vaadi jatkuvaa ylläpitoa, ja se toimii asiakkaan kannalta läpinäkyvästi, eli tunnistus ei vaadi asiakkaan toi-

menpiteitä. DHCP option-82 -tekniikan miinuspuolena on sen uutuus ja mahdolliset yhteensopivuusongelmat käytettäessä eri laitevalmistajien verkkolaitteita.

Vertailun jälkeen päädyttiin valitsemaan suunnitelman mukaisen tunnistuksen toteutustekniikaksi DHCP option-82 -tekniikka, josta yrityksellä oli jo aiempia kokemuksia laajakaistatekniikan saralta. Tämän tekniikan käyttöönotto vaati Oppilastalon verkkoon määrällisesti mittavia laitehankintoja, koska verkossa oli yhä noin 100 kpl Ethernet-keskittimiä, joista puuttui etähallintaominaisuus. Korvaavien laitteiden hankinnassa oli huomioitava muun muassa tekniset ominaisuudet käyttäjätunnistuksen toteuttamiseen, etähallintaan, tietoturvaan ja yhteensopivuuteen nykyisten jakelu- ja runkolaitteiden kanssa sekä myös fyysiset ulkomitat, koska olemassa olevat laitekaapit haluttiin säilyttää ennallaan. Laitteista tehtiin tarjouspyynnöt usealle toimittajalle, mutta johtuen vain yhdestä tarjouksesta, päädyttiin hankkimaan lisää saman valmistajan tekniikkaa kuin osassa verkkoa oli jo ennestään.

Laitehankintojen jälkeen rakennettiin testiympäristö, jossa tunnistustekniikan käyttöönottoa ja toimintaa tutkittiin, kunnes päästiin tavoiteltuihin tuloksiin. Kaikkien tarvittavien ominaisuuksien saamiseksi käyttöön, tehtiin sekä uusiin että jo käytössä oleviin kytkimiin ohjelmistopäivitykset. Kun kytkinten ohjelmistopäivitykset oli tehty, päästiin tekemään halutut perusasetukset ja vanhat laitteet korvattiin uusilla. Laiteasennukset tehtiin kiinteistö kerrallaan. Kaikista verkkoon kohdistuneista huolto ynnä muista töistä ilmoitettiin asiakkaille etukäteen Oppilastalo Oy:n sääntöjen mukaisesti, yleensä kiinteistöjen ilmoitustauluilla.

Kun kaikki laitteet oli vaihdettu, otettiin verkossa käyttöön käyttäjätunnistus, DHCP option-82 -tekniikalla, tekemällä yhden illan aikana n. 150:een verkon aktiivilaitteeseen sekä internetpalvelun tarjoajan DHCP-palvelimiin tarvittavat lisämääritykset. Kaikki verkon aktiivilaitteisiin tehdyt asetukset tehtiin telnet- tai konsoliyhteydellä.

Käyttöönotto sujui pääosin ongelmitta, ja tunnistamistiedot alkoivat välittyä internetpalvelun tarjoajalle. Joillakin käyttäjillä oli ongelmia verkkoyhteyden muodostamisessa välittömästi käyttäjän tunnistuksen käyttöönoton jälkeen. Nämä tapauk-

set tutkittiin, ja kaikki osoittautuivat tapauksiksi, joissa asiakas ei ollut huomioinut tiedotetta verkon muutostöistä ja tietokoneen uudelleenkäynnistys korjasi ongelman.

Työn tulokset vastasivat asetettuja tavoitteita, ja siitä saatiin hyvää kokemusta tulevaisuutta varten muihin vastaaviin toteutuksiin. Päätavoite oli tunnistustekniikan käyttöönotto, joka sujui verkon kokoon ja käyttäjien määrään suhteutettuna erinomaisesti. Aktiivilaitteiden tietoturvaominaisuuksilla parannettiin merkittävästi mahdollisuuksia torjua verkkoon kohdistuvia hyökkäyksiä ja minimoida viallisten laitteiden aiheuttamaa haittaa. Myös verkon asiakkaat saivat vaihtoehtoja liittymänopeuden suhteen, mikä on osoittautunut tarpeelliseksi ja kiitellyksi ominaisuudeksi.

6 TULEVAISUUS

Oppilastalo Oy:n verkkoympäristö on nyt pääpiirteittäin hyvällä tasolla, ja tekniikkana toimii nykyisissä tietoliikenneverkoissa eniten käytetty Ethernet. Yleisten ennusteiden mukaan verkkoliikenne tulee kasvamaan merkittävästi tulevaisuudessa uusien sovellutusten, kuten VoIP-tekniikan (Voice over Internet Protocol), verkossa välitettävien TV-lähetysten ynnä muun multimedian vaikutuksesta. Tätä silmälläpitäen seuraavana parannustoimenpiteenä voisi olla G.SHDSL-tekniikalla toteutettujen runkoyhteyksien muutos nopeampaan liityntätekniikkaan tai useamman yhteyden yhtäaikainen käyttö tarpeiden näin vaatiessa. Asiakasrajapinnan liittymänopeus on kuitenkin helppo kasvattaa nykyisillä laitteilla 100 Mbit/s ja laitepäivityksillä Ethernet-standardien mukaisesti jopa 10 Gbit/s.

Näin suurien tiedonsiirtonopeuksien tarve voi kuitenkin johtaa siihen, että kiinteistöjen sisäverkkoja voidaan joutua kaapeloimaan vielä uudelleen, mikäli halutaan ottaa käyttöön yli 100 Mbit/s tiedonsiirtonopeuksia.

Oppilastalon verkon liittymien hinnoittelussa tulee kiinnittää huomiota siihen, että hinta pysyy asiakkaille houkuttelevana verrattuna esimerkiksi tavallisiin ADSL- ja kaapelimodeemitekniikalla toteutettuihin laajakaistaliittymiin, koska verkon asiakkailla on mahdollisuus tilata laajakaistaliittymä myös yleisiltä markkinoilta. Hinnoittelua voidaan muuttaa tulevaisuudessa esimerkiksi ottamalla käyttöön edullisempia tekniikoita niiden tullessa saataville.

Käyttöönotetulla tekniikalla liittymien hinnoittelu pystytään kuitenkin pitämään tavallisia laajakaistatekniikoita edullisempana, johtuen verkon yksinkertaisesta rakenteesta, helposta muunneltavuudesta ja Oppilastalon kiinteistöjen suurista asiakasmääristä.

Tavallisiin laajakaistaliittymiin verrattuna Oppilastalon verkon eduksi on laskettava myös parempi palvelutaso. Verkon etävalvonta on helppoa ja asennus tehdään Ethernet-rajapintaan, jolloin käyttöönotto on asiakkaalle helppo. Erillisiä päätelaitteita ei tarvita, vaan asiakkaan tarvitsee ainoastaan hankkia CAT5-tasoinen työasemakaapeli kytkeäkseen tietokoneensa seinärasiaan.

Päijät-Hämeen Puhelimen tulee myös tulevaisuudessa huolehtia siitä, että asiakaspalvelutilanteet, kuten liittymien avaus, sulku ja viankorjauksen vasteaika, toimivat Oppilastalon verkossa tehokkaammin kuin yleisiltä markkinoilta hankittavissa laajakaistaliittymissä.

Verkossa käytetyn DHCP option-82 -tunnistustekniikan käyttö yleistyy koko ajan operaattori- ja asiakasverkoissa, jotka ovat muuttuneet pääasiassa Ethernet-pohjaisiksi. DHCP option-82 -tunnistustekniikkaa voivat käyttää palveluntarjoajien lisäksi myös suuremmat yritykset, ja käyttö tulee kasvamaan edelleen, kun tämän tunnistustekniikan tuki tulee kaikkiin verkon aktiivilaitteisiin. DHCP option-82 -tunnistustekniikka voidaan ottaa käyttöön myös asteittain niissä laitteissa, jotka tekniikkaa tukevat.

Yksi tällaisen verkon suurimmista hallintatöistä on pitää yllä kytkimien porttikohtaista dokumentointia, jolla kohdistetaan tietty kytkinportti tiettyyn asuntoon, soluun, huoneeseen tai asukkaaseen. Tätä dokumentointia pitää aina päivittää asukasmuutosten mukaisesti.

Tässä opinnäytetyössä kuvatun ja toteutetun käyttäjätunnistustekniikan avulla IP-osoitteiden käyttäjätiedot ja aikaleimat tallentuvat DHCP-palvelimen lokiin, jota käsiteltäessä on syytä tiedostaa näiden laissa teletunnistetiedoiksi luokiteltujen tietojen luottamuksellisuus ja siitä johtuva tarve erityiseen huolellisuuteen.

LÄHTEET

Anttila, A. 2000. TCP/IP-tekniikka. Helsinki Media, Juva.

Cisco 2004. Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide, Cisco IOS Release 12.1(22)EA2 [verkkodokumentti]. Cisco Systems, Inc, 2004 [viitattu 20.07.2005]. Saatavissa: http://www.cisco.com/application/pdf/en/us/guest/products/ps628/c2001/ccmigration_09186a00802c3143.pdf

IETF 1997. RFC 2131 - Dynamic Host Configuration Protocol [verkkodokumentti]. IETF, lokakuu 1997 [viitattu 30.07.2005]. Saatavissa: http://www.ietf.org/rfc/rfc2131.txt

IETF 1999. RFC 2516 - A Method for Transmitting PPP Over Ethernet (PPPoE) [verkkodokumentti]. IETF, helmikuu 1999 [viitattu 30.07.2005]. Saatavissa: http://www.ietf.org/rfc/rfc2516.txt

IETF 2001. RFC 3046 - DHCP Relay Agent Information Option [verkkodokumentti]. IETF, tammikuu 2001 [viitattu 04.02.2007]. Saatavissa: http://www.ietf.org/rfc/rfc3046.txt

Jaakonhuhta, H. 2005. Lähiverkot – Ethernet. 4. uudistettu painos. Edita Publishing Oy, IT Press, Helsinki.

Oppilastalo 2005. Oppilastalo Oy:n internet-sivut [verkkodokumentti]. Oppilastalo Oy, 2005 [viitattu 02.08.2005]. Saatavissa: http://www.oppilastalo.fi

Viestintävirasto 2004a. Tietoturva: Tietoturvallisuuden perusteet, Peruskäsitteitä [verkkodokumentti]. Viestintävirasto, 01.09.2004 [viitattu 10.08.2005]. Saatavissa: http://www.ficora.fi/suomi/tietoturva/ttkasitteet.htm

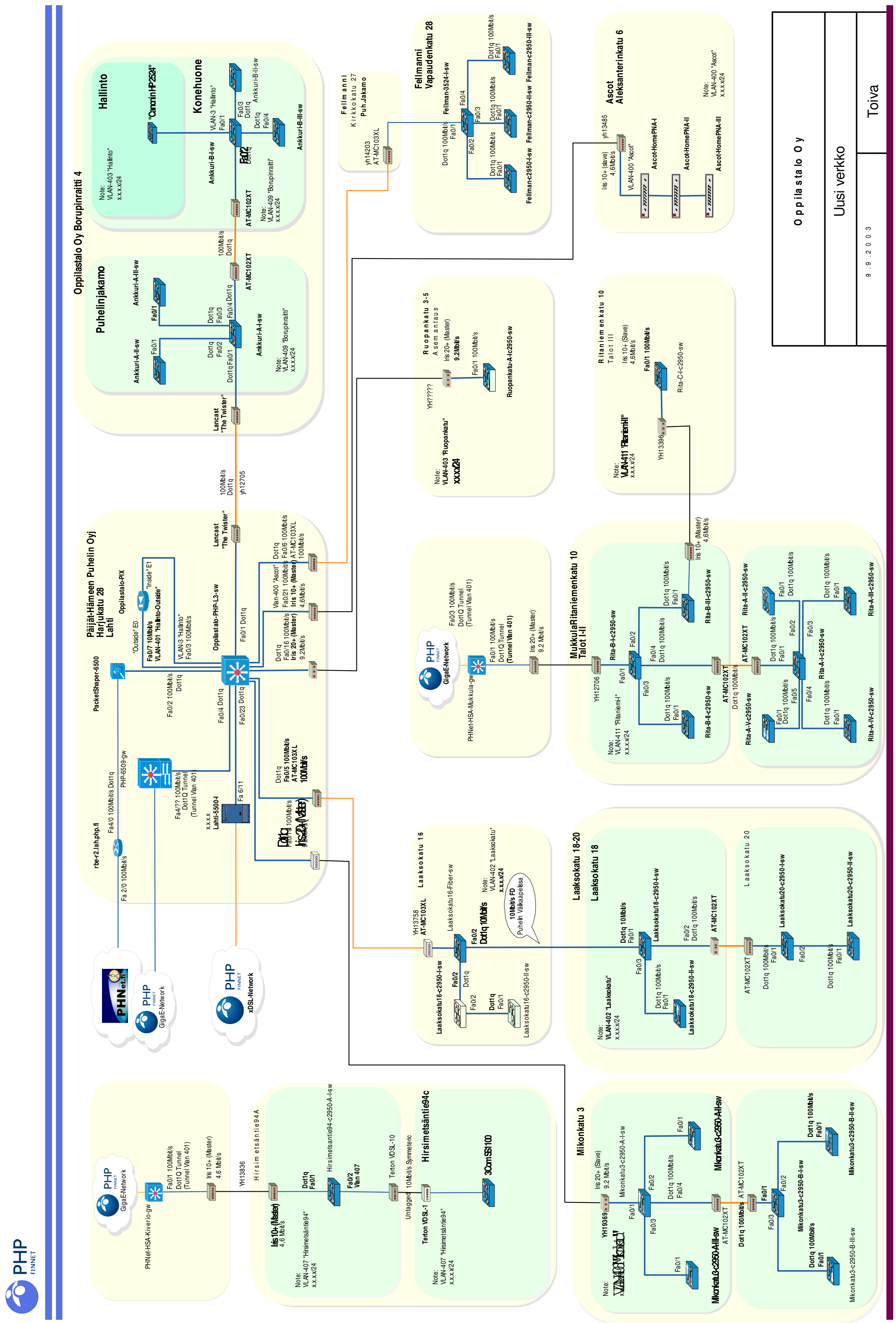
Viestintävirasto 2004b. Tietoturva: Sähköisen viestinnän tietosuoja, Teleyritykset [verkkodokumentti]. Viestintävirasto, 28.09.2004 [viitattu 10.08.2005]. Saatavissa: http://www.ficora.fi/suomi/tietoturva/svttele.htm

Viestintävirasto 2004c. Tietoturva: Sähköisen viestinnän tietosuoja, Tunnistamistietojen käsittely [verkkodokumentti]. Viestintävirasto, 02.12.2004 [viitattu 10.08.2005]. Saatavissa: http://www.ficora.fi/suomi/tietoturva/svtteletunnistaminen.htm

Viestintävirasto 2004d. Tietoturva: Sähköisen viestinnän tietosuoja, Paikkatietojen käsittely [verkkodokumentti]. Viestintävirasto, 28.09.2004 [viitattu 10.08.2005]. Saatavissa: http://www.ficora.fi/suomi/tietoturva/svttelepaikka.htm

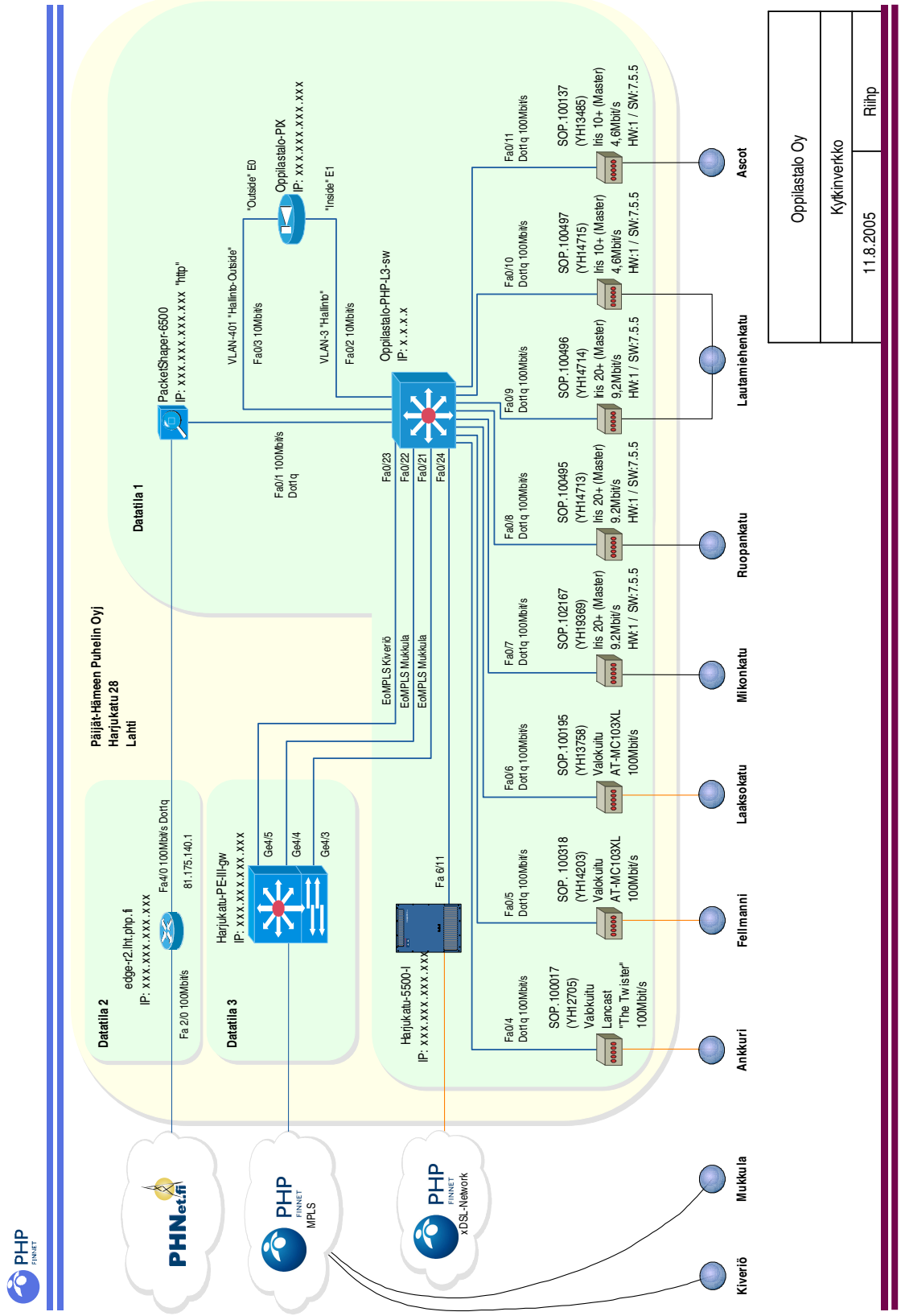
Viestintävirasto 2005a. Tietoturva: Sähköisen viestinnän tietosuoja, Telcosec [verkkodokumentti]. Viestintävirasto, 17.05.2005 [viitattu 10.08.2005]. Saatavissa: http://www.ficora.fi/suomi/tietoturva/svtteletelcosec.htm

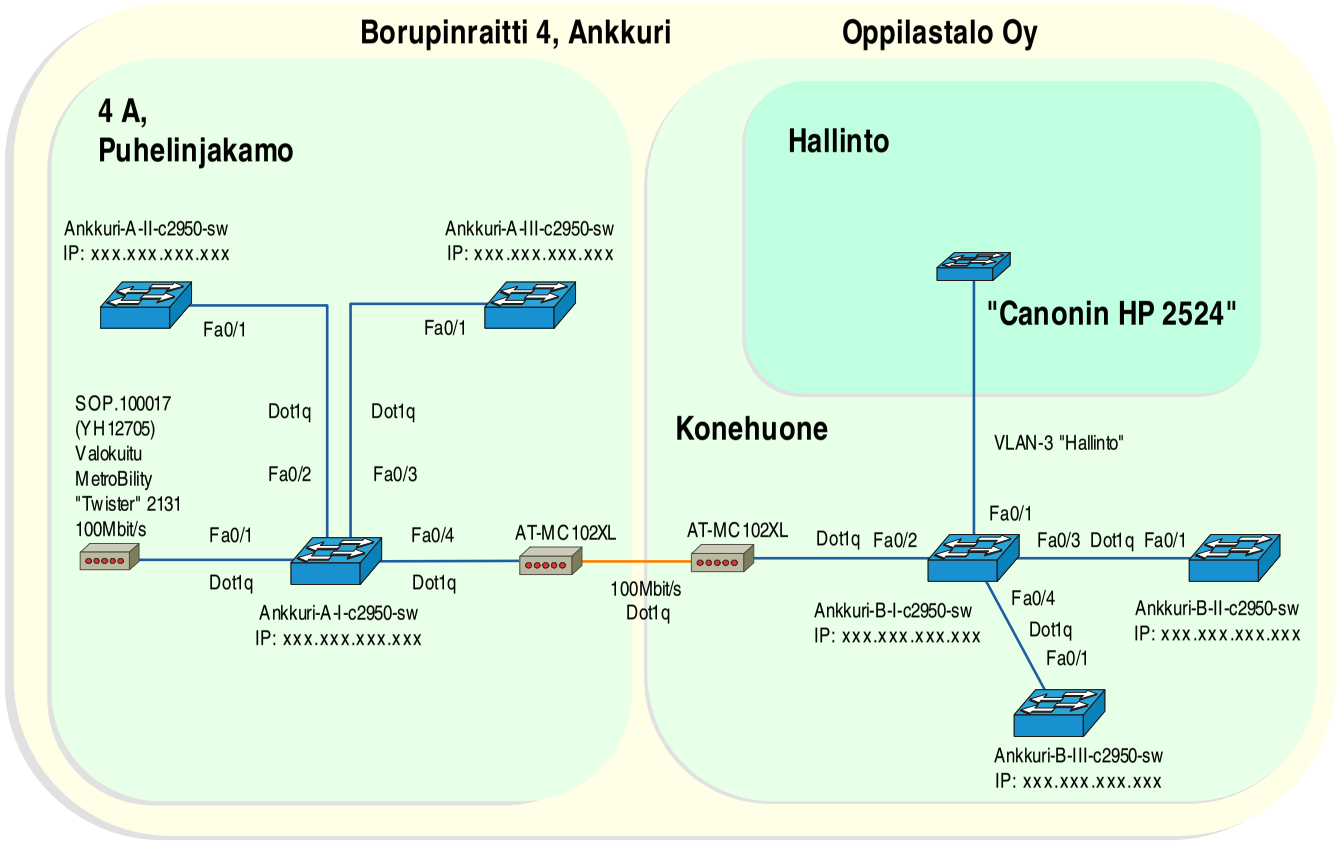
LIITE 1



Oppilastalo Oy
Uusi verkko
Toiva
9.9.2003
Oppilastalo Oy Borupinraitti 4
Päijät-Hämeen Puhelin Oyj Harjukatu 28 Lahti
Puhelinjakamo
Konehuone
Hallinto
Fellmanni Vapaudenkatu 28
Ascot Aleksanterinkatu 6
MukkulaRitaniemenkatu 10 Talot I-II
Laaksokatu 18-20
Laaksokatu 18
Mikonkatu 3
Hirsimetsäntie94c

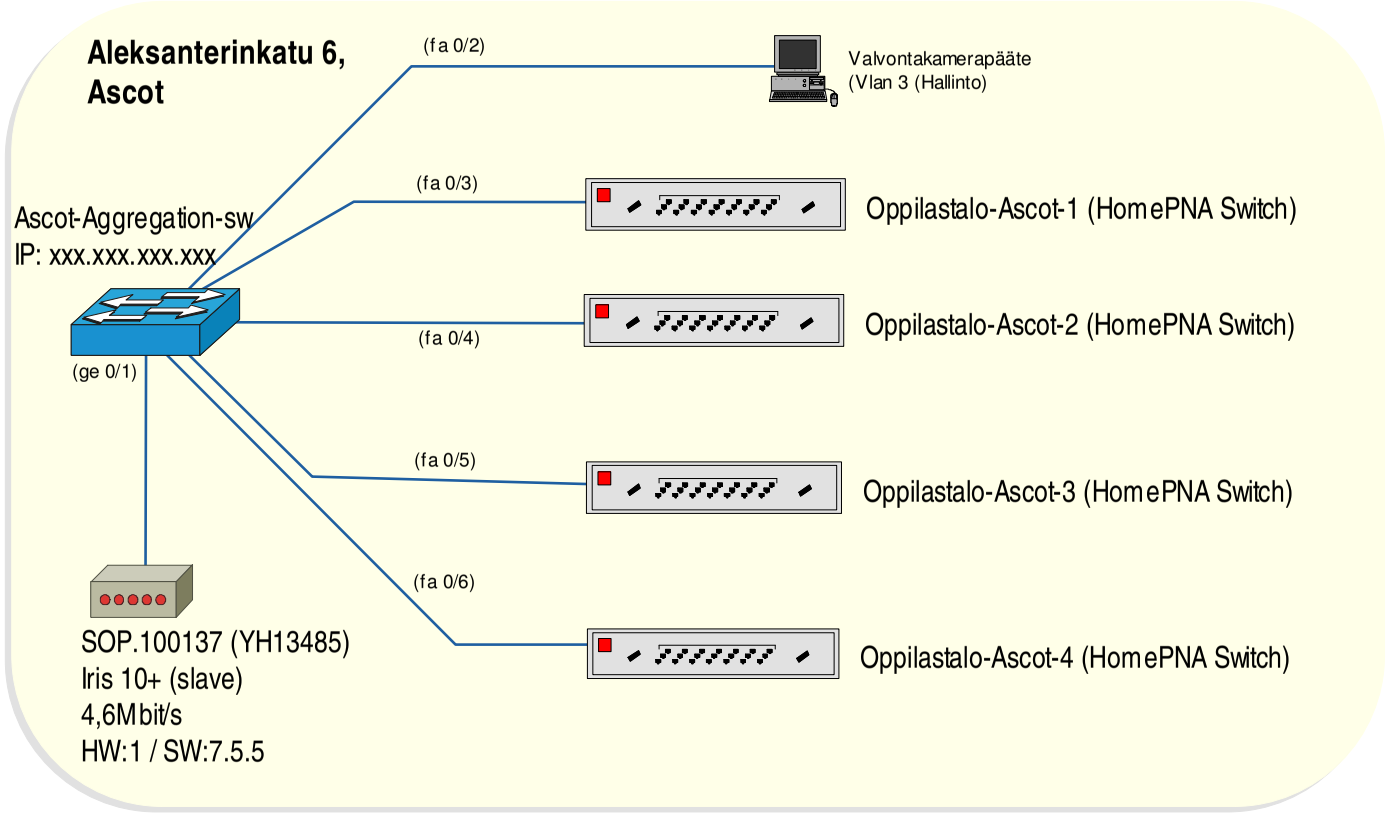
LIITE 2


Oppilastalo Oy
Kytkinverkko
11.8.2005
Riihp
Päijät-Hämeen Puhelin Oyj
Harjukatu 28
Lahti
Datatila 1
Datatila 2
Datatila 3
edge-r2.lht.php.fi
IP: xxx.xxx.xxx.xxx
Fa4/0 100Mbit/s DotIq
Fa 2/0 100Mbit/s
81.175.140.1
Harjukatu-PE-III-gw
IP: xxx.xxx.x.xxx.xxx
Ge4/5
Ge4/4
Ge4/3
Harjukatu-5500-I
IP: xxx.xxx.xxx.xxx
Fa 6/11
PacketShaper-6500
IP: xxx.xxx.xxx.xxx "http"
VLAN-401 "Hallinto-Outside"
Fa0/3 10Mbit/s
"Outside" E0
Oppilastalo-PIX
IP: xxx.xxx.xxx.xxx
VLAN-3 "Hallinto"
Fa0/2 10Mbit/s
"Inside" E1
Fa0/1 100Mbit/s
DotIq
Oppilastalo-PHP-L3-sw
IP: x.x.x.x
Fa0/23
Fa0/22
Fa0/21
Fa0/24
EoMPLS Kivenlö
EoMPLS Mukkula
EoMPLS Mukkula
Fa0/4
DotIq 100Mbit/s
SOP.100017
(YH12705)
Valokuitu
Lancast
"The Twister"
100Mbit/s
Fa0/5
DotIq 100Mbit/s
SOP. 100318
(YH14203)
Valokuitu
AT-MC103XL
100Mbit/s
Fa0/6
DotIq 100Mbit/s
SOP.100195
(YH13758)
Valokuitu
AT-MC103XL
100Mbit/s
Fa0/7
DotIq 100Mbit/s
SOP.102167
(YH19369)
Iris 20+ (Master)
9.2Mbit/s
HW:1 / SW:7.5.5
Fa0/8
DotIq 100Mbit/s
SOP.100495
(YH14713)
Iris 20+ (Master)
9.2Mbit/s
HW:1 / SW:7.5.5
Fa0/9
DotIq 100Mbit/s
SOP.100496
(YH14714)
Iris 20+ (Master)
9.2Mbit/s
HW:1 / SW:7.5.5
Fa0/10
DotIq 100Mbit/s
SOP.100497
(YH14715)
Iris 10+ (Master)
4.6Mbit/s
HW:1 / SW:7.5.5
Fa0/11
DotIq 100Mbit/s
SOP.100137
(YH13485)
Iris 10+ (Master)
4.6Mbit/s
HW:1 / SW:7.5.5
Ankkuri
Fellmanni
Laaksokatu
Mikonkatu
Ruopankatu
Lautamiehenkatu
Ascot
Kiverlö
Mukkula
PHNet.fi
PHP FINNET MPLS
PHP FINNET xDSL-Network



Note:
VLAN-409 "Borupinraitti"
xxx.xxx.xxx.xxx/24

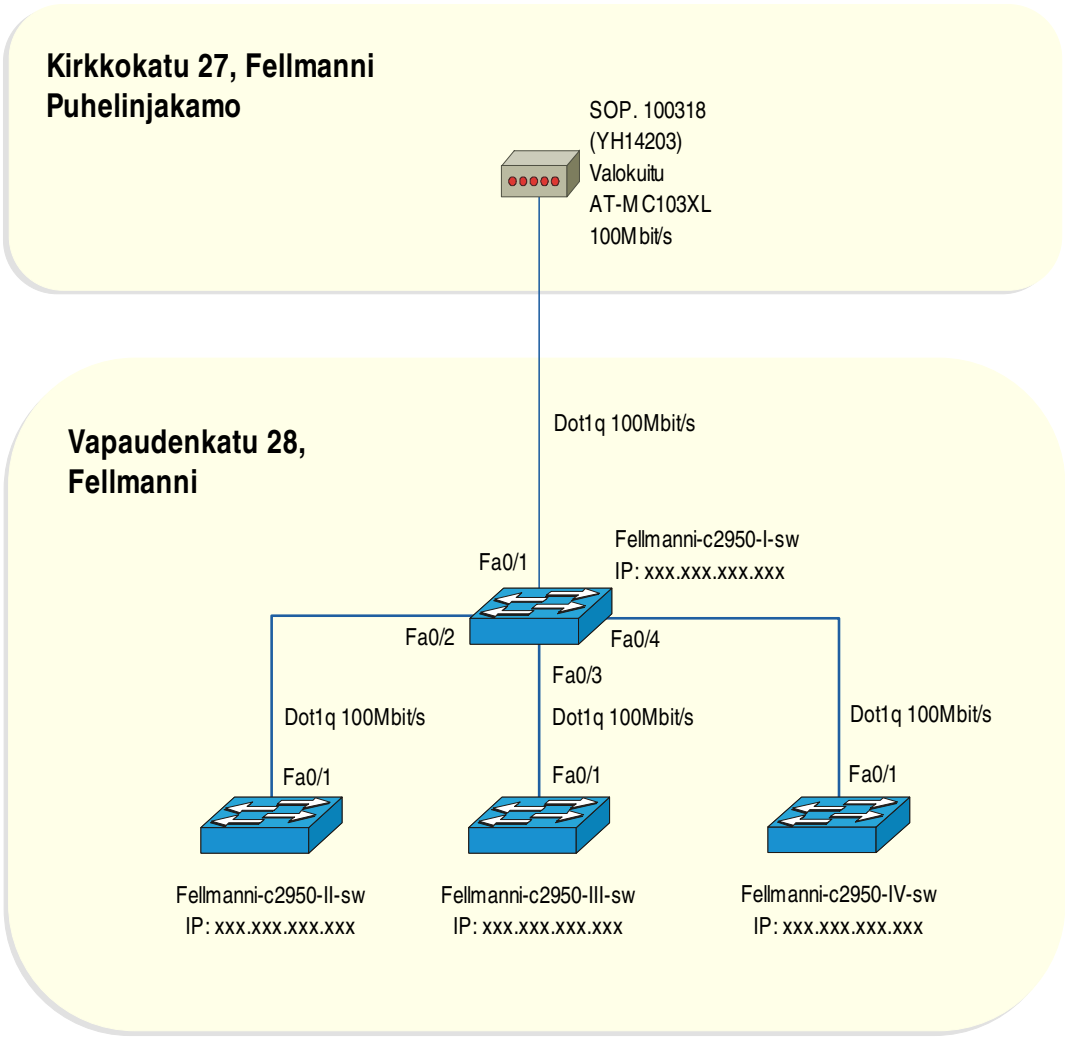
Oppilastalo Oy	
Ankkuri Sub-diagram	
10.8.2005	Riihp



Note:
VLAN-400, 405, 408 "Ascot"
IP: xxx.xxx.xxx.xxx/24

Oppilastalo Oy	
Ascot Sub-diagram	
10.8.2005	MykkH

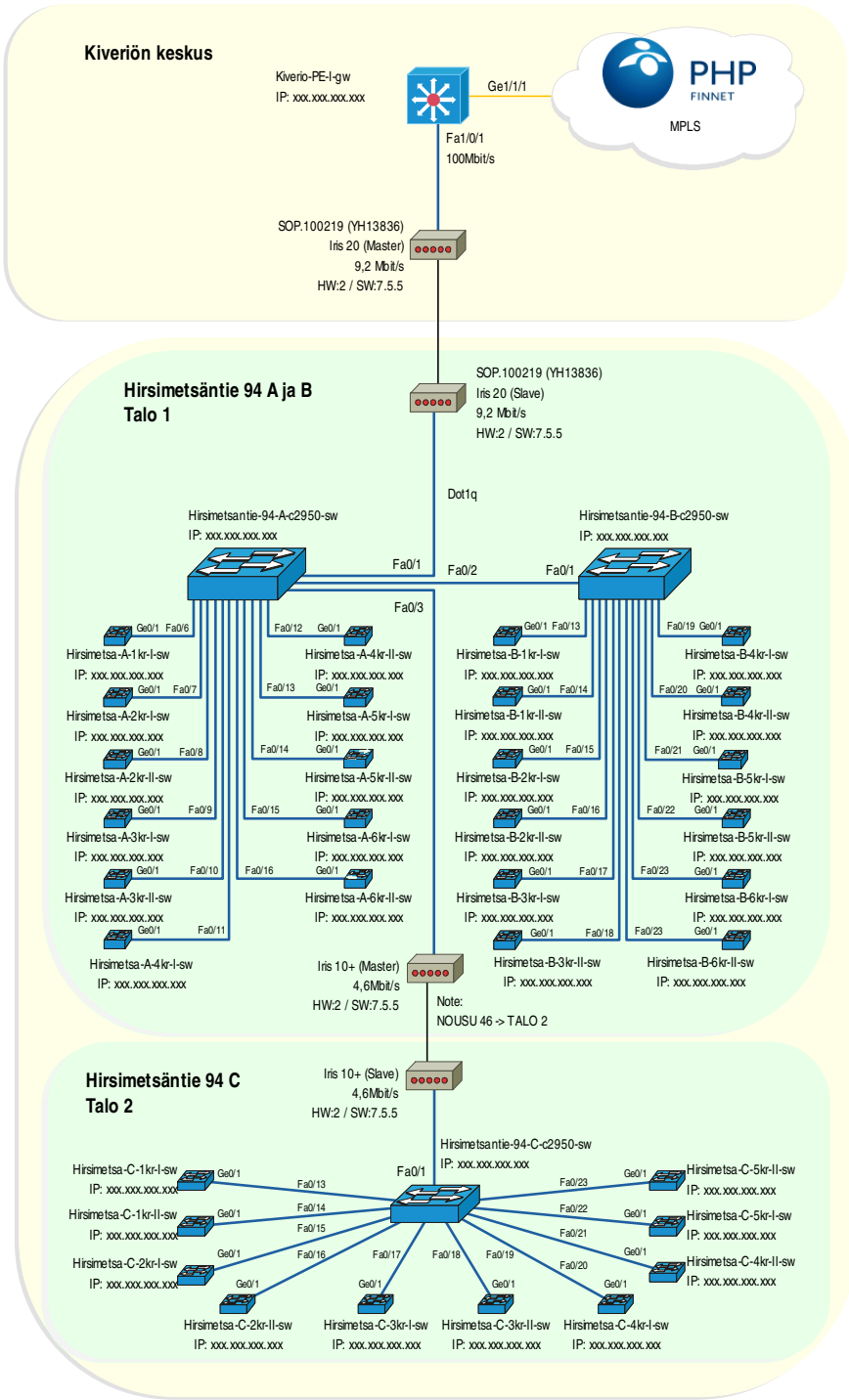
LIITE 2



Note:
VLAN-410 "Fellmanni"
IP: xxx.xxx.xxx.xxx/24

Oppilastalo Oy	
Fellmanni Sub-diagram	
9.8.2005	Riihp

LIITE 2

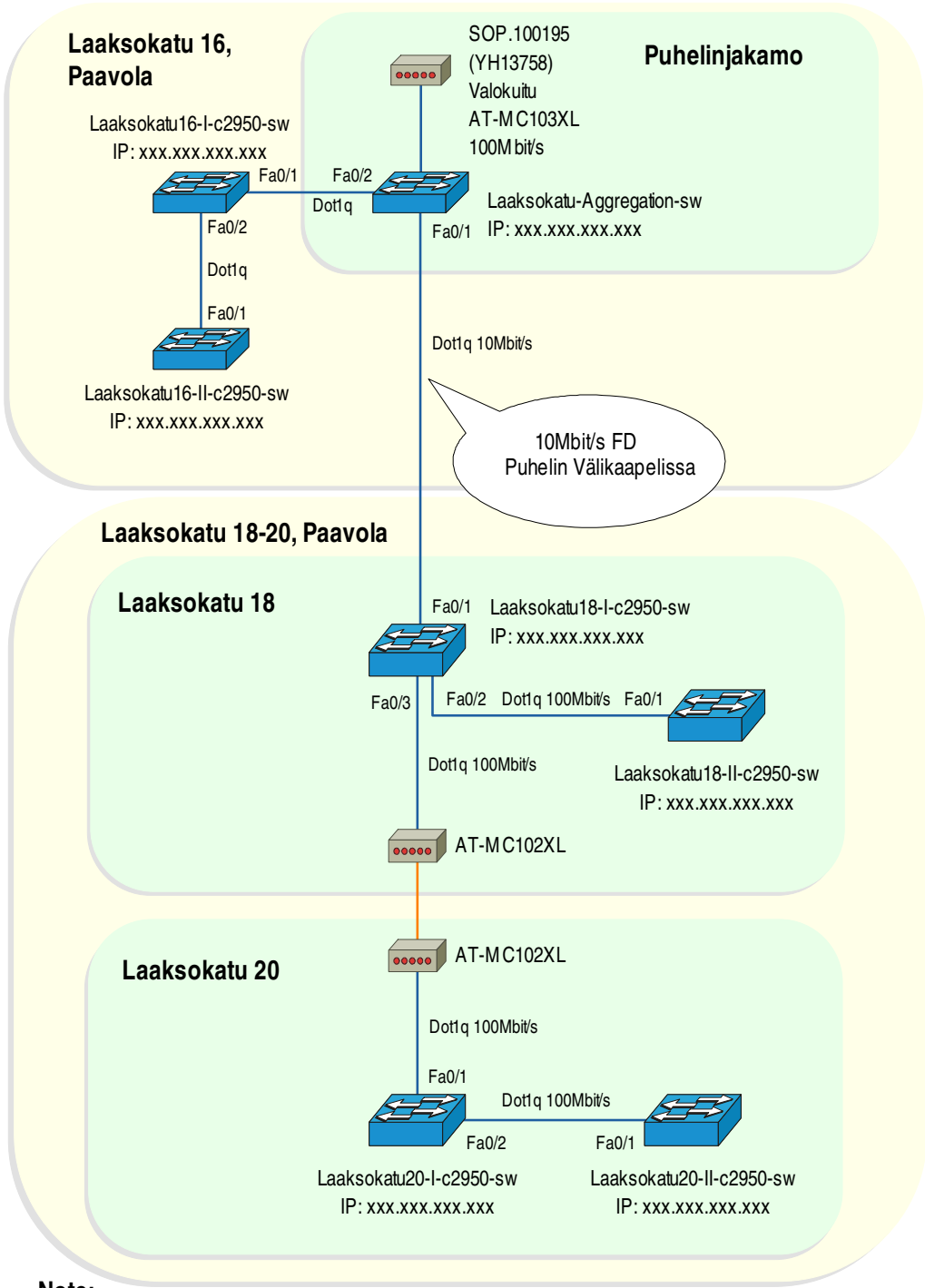


Note:
VLAN-407 "Hirsimetsäntie94"
IP: xxx.xxx.xxx.xxx/24

Note:
VTP DOMAIN: "hirsimetsantie"

Oppilastalo Oy	
Kiveriö Sub-diagram	
9.9.2005	Riihp

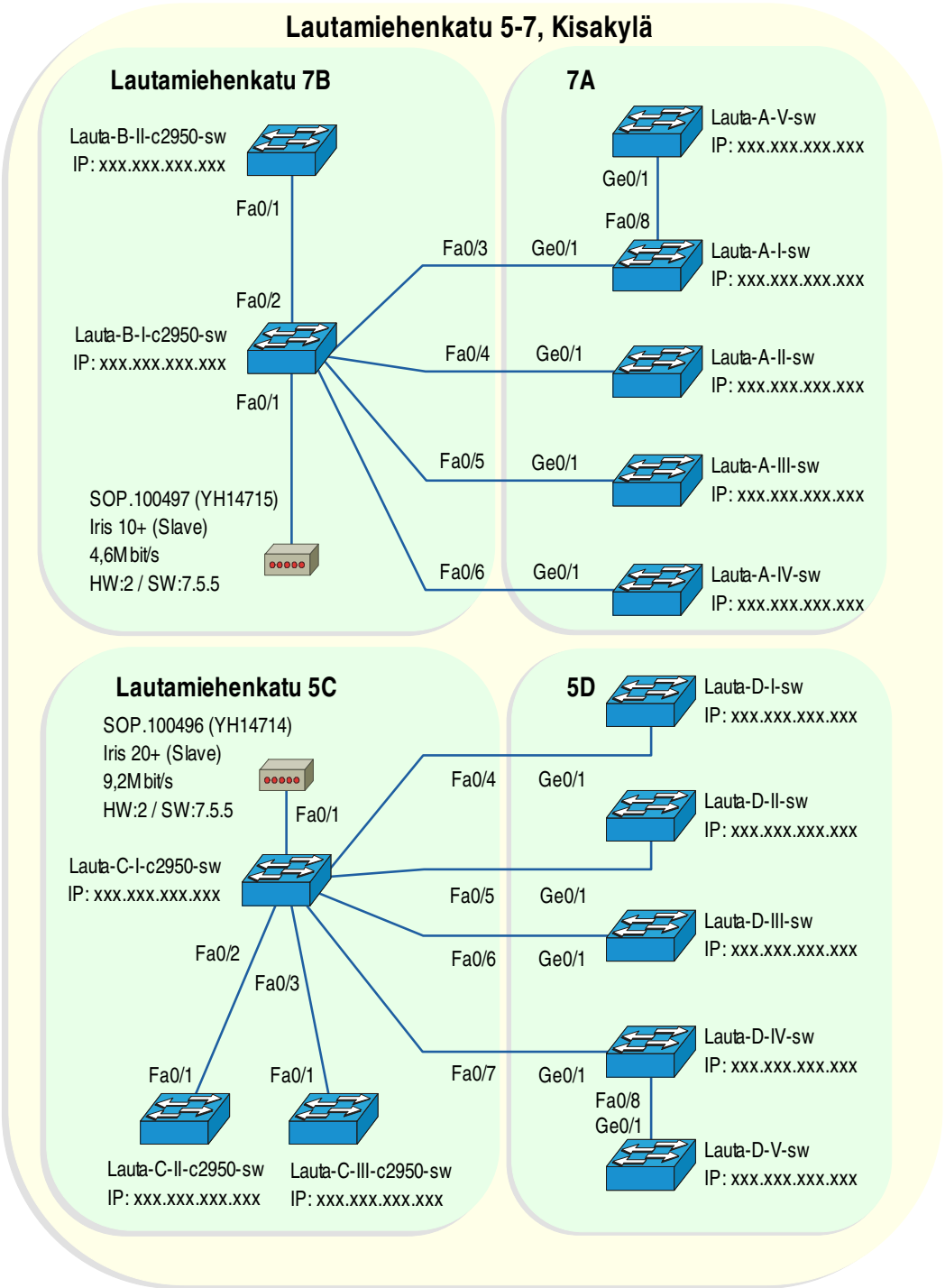
LIITE 2



Note:
VLAN-402 "Laaksokatu"
IP: xxx.xxx.xxx.xxx/24

Oppilastalo Oy	
Laaksokatu Sub-diagram	
10.9.2005	Riihp

LIITE 2

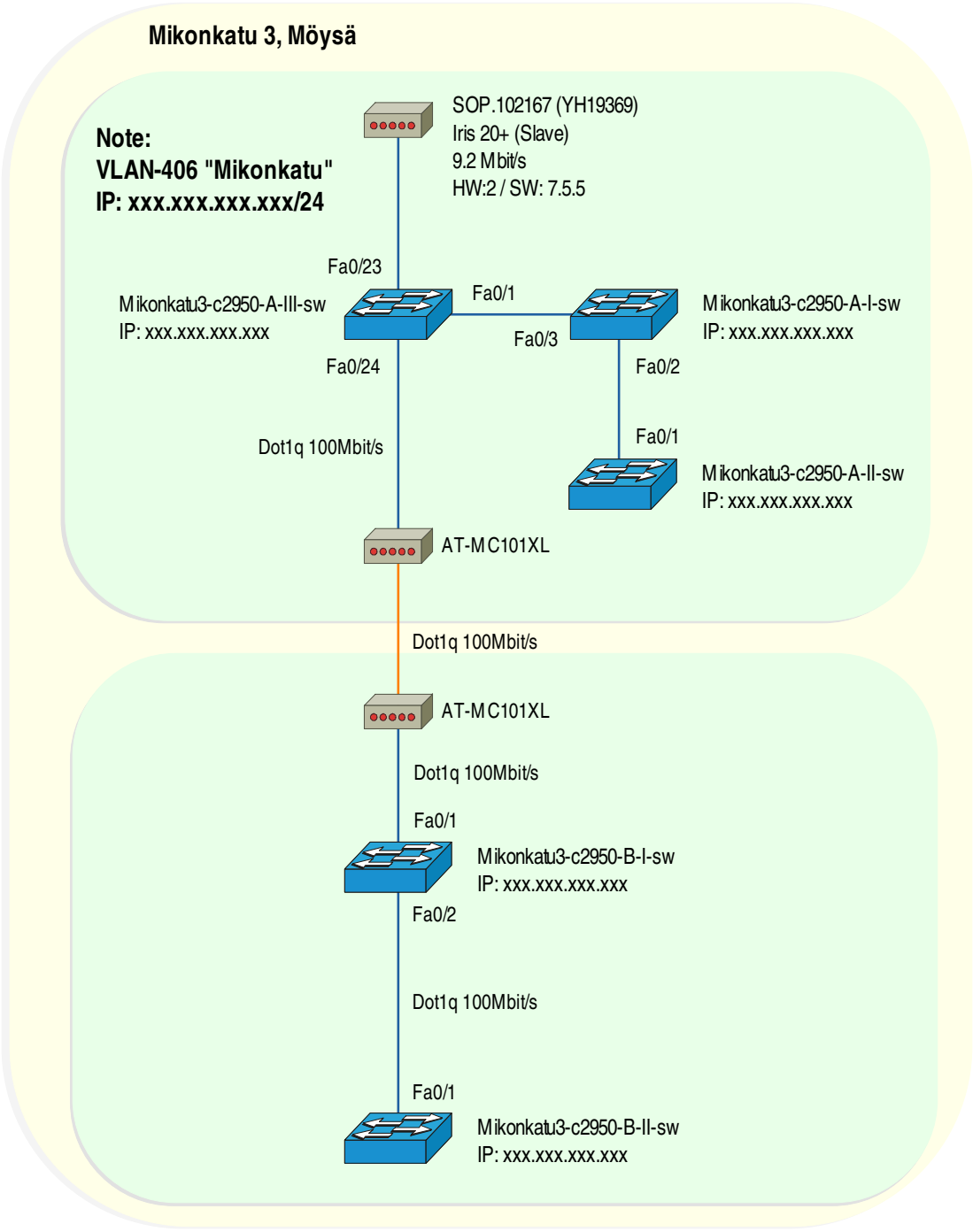


Note:
VLAN-404 "Lautamiehenkatu"
10.254.5.0/24

Note:
VTP DOMAIN: "lautamiehenkatu"

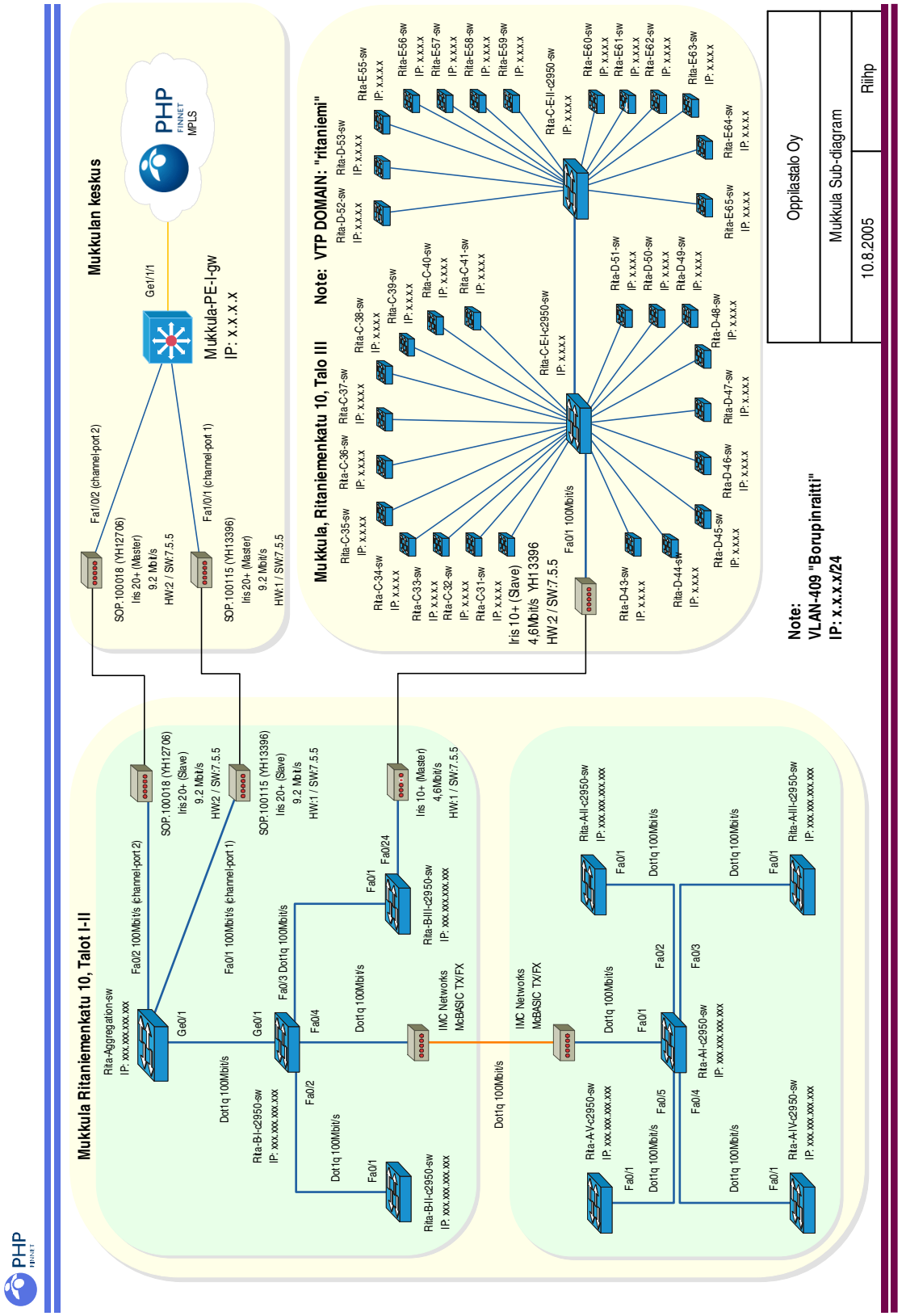
Oppilastalo Oy	
Lautamiehenkatu Sub-diagram	
10.8.2005	Riihp

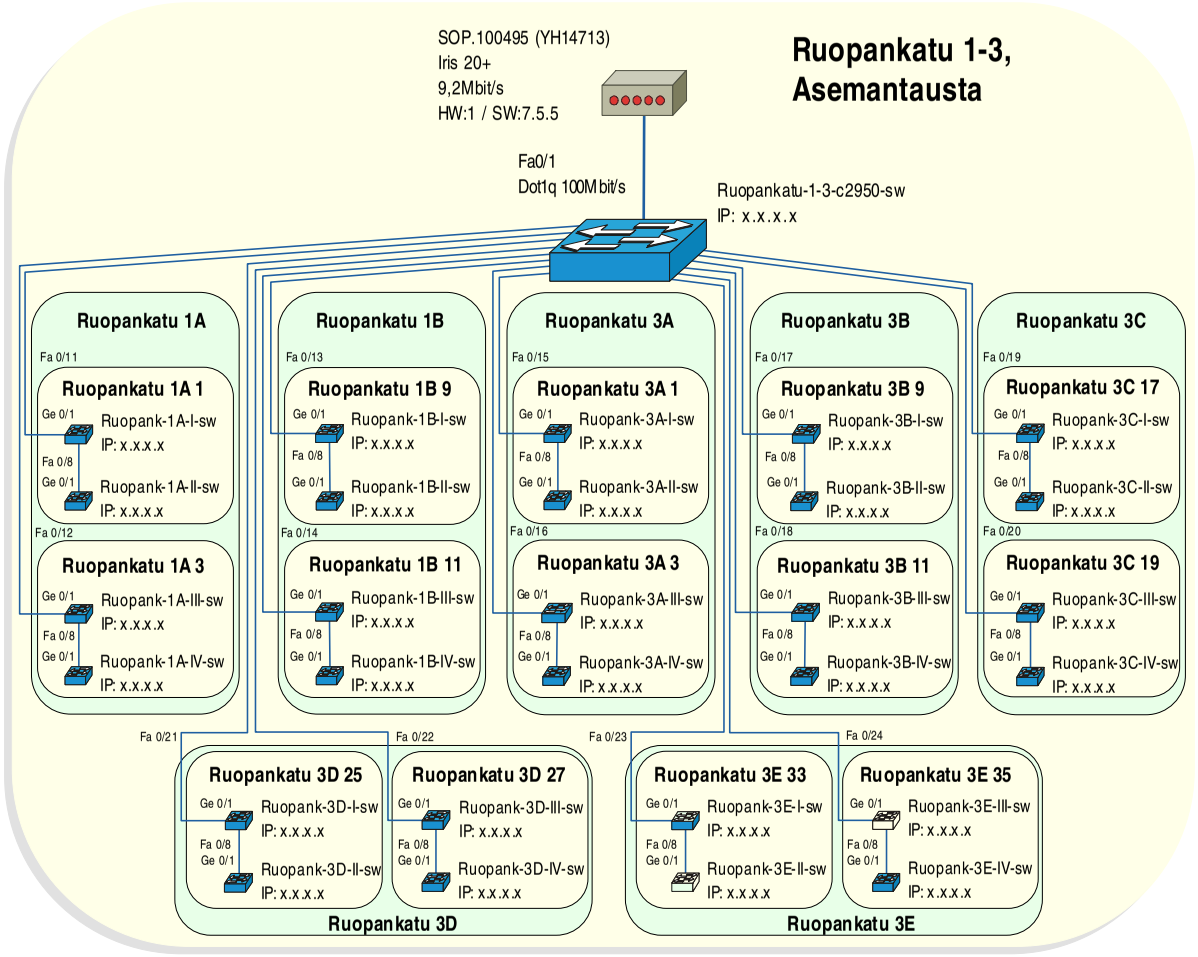
LIITE 2



Oppilastalo Oy	
Mikonkatu Sub-diagram	
10.8.2005	Riihp

LIITE 2


Mukkulan keskus
PHP FINNET MPLS
Mukkula-PE-I-gw
IP: x.x.x.x
Ge1/1
Fa1/0/2 (channel-port 2)
Fa1/0/1 (channel-port 1)
SOP:100018 (YH12706)
Iris 20+ (Master)
9.2 Mbit/s
HW:2 / SW:7.5.5
SOP:100115 (YH13396)
Iris 20+ (Master)
9.2 Mbit/s
HW:1 / SW:7.5.5
Mukkula, Ritaniemenkatu 10, Talo III
Note: VTP DOMAIN: "ritaniemi"
Rita-C-E-II-c2950-sw
IP: x.x.x.x
Fa0/1 100Mbit/s
Iris 10+ (Slave)
4,6Mbit/s YH13396
HW:2 / SW:7.5.5
Rita-C-35-sw
Rita-C-36-sw
Rita-C-37-sw
Rita-C-38-sw
Rita-C-39-sw
Rita-C-40-sw
Rita-C-41-sw
Rita-C-34-sw
Rita-C-33-sw
Rita-C-32-sw
Rita-C-31-sw
Rita-D-52-sw
Rita-D-53-sw
Rita-E-55-sw
Rita-E-56-sw
Rita-E-57-sw
Rita-E-58-sw
Rita-E-59-sw
Rita-D-51-sw
Rita-D-50-sw
Rita-D-49-sw
Rita-D-48-sw
Rita-D-47-sw
Rita-D-46-sw
Rita-D-45-sw
Rita-D-43-sw
Rita-D-44-sw
Rita-E-60-sw
Rita-E-61-sw
Rita-E-62-sw
Rita-E-63-sw
Rita-E-64-sw
Rita-E-65-sw
Mukkula Ritaniemenkatu 10, Talot I-II
Rita-Aggregation-sw
IP: xxx.xxx.xxx.xxx
Fa0/2 100Mbit/s (channel-port 2)
Fa0/1 100Mbit/s (channel-port 1)
Ge0/1
Dot1q 100Mbit/s
Fa0/3 Dot1q 100Mbit/s
Fa0/4
Fa0/2
Rita-B-I-c2950-sw
IP: xxx.xxx.xxx.xxx
Fa0/1
Rita-B-II-c2950-sw
IP: xxx.xxx.xxx.xxx
Fa0/24
IMC Networks
McBASIC TX/FX
Rita-A-I-c2950-sw
IP: xxx.xxx.xxx.xxx
Fa0/5
Fa0/3
Rita-A-II-c2950-sw
IP: xxx.xxx.xxx.xxx
Rita-A-III-c2950-sw
IP: xxx.xxx.xxx.xxx
Rita-A-IV-c2950-sw
IP: xxx.xxx.xxx.xxx
Note:
VLAN-409 "Borupinraitti"
IP: x.x.x.x/24
Oppilastalo Oy
Mukkula Sub-diagram
10.8.2005
Riihp



Note:
VLAN-403 "Ruopankatu"
IP: x.x.x.x/24

Note:
VTP DOMAIN: "ruopankatu"

Oppilastalo Oy	
Ruopankatu Sub-diagram	
11.8.2005	Riihp

LIITE 3

```
version 12.1
!
hostname Liityntäkytkin Kohde 1
!
ip subnet-zero
!
ip dhcp snooping vlan 407
ip dhcp snooping vlan 425
ip dhcp snooping vlan 430
ip dhcp snooping
!
interface FastEthernet0/1
 description Solu1 - huone1
 switchport access vlan 407
 switchport mode access
 switchport protected
 switchport port-security
 switchport port-security maximum 10
 switchport port-security aging time 10
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 shutdown
 speed 10
 duplex half
 mls qos cos override
 storm-control broadcast level 10.00 8.00
 storm-control multicast level pps 2000 1000
 storm-control unicast level pps 2000 1000
 storm-control action trap
 no cdp enable
 spanning-tree portfast
!

…

!
interface GigabitEthernet0/1
 description Uplink Jakelu/liityntäkytkin Kohde 1 Talo 1 Rappu A
(192.168.0.140)
 switchport trunk native vlan 168
 switchport mode trunk
 speed 100
 duplex full
 ip dhcp snooping trust
!
interface Vlan168
```

LIITE 3

```
 description Hallinta VLAN
 ip address 192.168.0.150 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.0.1
!
end
```

LIITE 4

```
version 12.1
!
hostname Jakelu/liityntäkytkin Kohde 1 Talo 1 Rappu A
!
ip subnet-zero
!
ip dhcp snooping vlan 407
ip dhcp snooping vlan 425
ip dhcp snooping vlan 430
ip dhcp snooping
!
interface FastEthernet0/1
 description Uplink Runkokytkin 9,6 Mbit/s G.SHDSL (192.168.0.40)
 switchport trunk native vlan 168
 switchport trunk allowed vlan 1,168,407,425,430
 switchport mode trunk
 speed 100
 duplex full
 ip dhcp snooping trust
!
interface FastEthernet0/2
 description Syöttö Jakelu/liityntäkytkin Kohde 1 Talo 1 Rappu B
100Mbit/s (192.168.0.141)
 switchport trunk native vlan 168
 switchport mode trunk
 switchport protected
 speed 100
 duplex full
 ip dhcp snooping trust
!
interface FastEthernet0/3
 description Syöttö Jakelu/liityntäkytkin Kohde 1 Talo 2 Rappu C 4,6
Mbit/s G.SHDSL (192.168.0.142)
 switchport trunk native vlan 168
 switchport mode trunk
 switchport protected
 speed 100
 duplex full
 ip dhcp snooping trust
!
interface FastEthernet0/6
 description Syöttö Liityntäkytkin Kohde 1 Solu 1 (192.168.0.150)
 switchport trunk native vlan 168
 switchport mode trunk
 switchport protected
 speed 100
 duplex full
```

LIITE 4

```
!
ip dhcp snooping trust
interface FastEthernet0/7
 description Syöttö Liityntäkytkin Kohde 1 Solu 2 (192.168.0.151)
 switchport trunk native vlan 168
 switchport mode trunk
 switchport protected
 speed 100
 duplex full
 ip dhcp snooping trust
!
interface FastEthernet0/17
 description Kerhohuone rasia 1
 switchport access vlan 407
 switchport mode access
 switchport protected
 switchport port-security
 switchport port-security maximum 10
 switchport port-security aging time 10
 switchport port-security violation protect
 switchport port-security aging type inactivity
 load-interval 30
 shutdown
 speed 10
 duplex half
 mls qos cos override
 storm-control broadcast level 10.00 8.00
 storm-control multicast level pps 2000 1000
 storm-control unicast level pps 2000 1000
 storm-control action trap
 no cdp enable
 spanning-tree portfast
!
…

!
interface Vlan168
 description Hallinta VLAN
 ip address 192.168.0.140 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.0.1
!
end
```

LIITE 5

```
version 12.2
!
hostname Runkokytkin
!
ip subnet-zero
no ip source-route
ip routing
ip domain-name oppilastalo.fi
ip name-server 62.165.128.10
ip name-server 62.165.128.11
!
!
no file verify auto
!
mac access-list extended testi
!
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
 description Yhteys Reitittimelle (192.168.0.1)
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,400-415,425,430
 switchport mode trunk
 load-interval 30
 duplex full
 speed 100
!
!
interface FastEthernet0/4
 description Syöttö jakelu/liityntäkytkimelle Kohde 1 Talo 1 Rappu A
(192.168.0.140)
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 168
 switchport trunk allowed vlan 1,168,407,425,430
 switchport mode trunk
 load-interval 30
 duplex full
 speed 100
!
interface Vlan168
 description Hallinta VLAN
 ip address 192.168.0.40 255.255.255.0
 no ip unreachables
 no ip proxy-arp
!
ip classless
```

LIITE 5

```
!
no logging trap
control-plane
!
!
end
```

LIITE 6

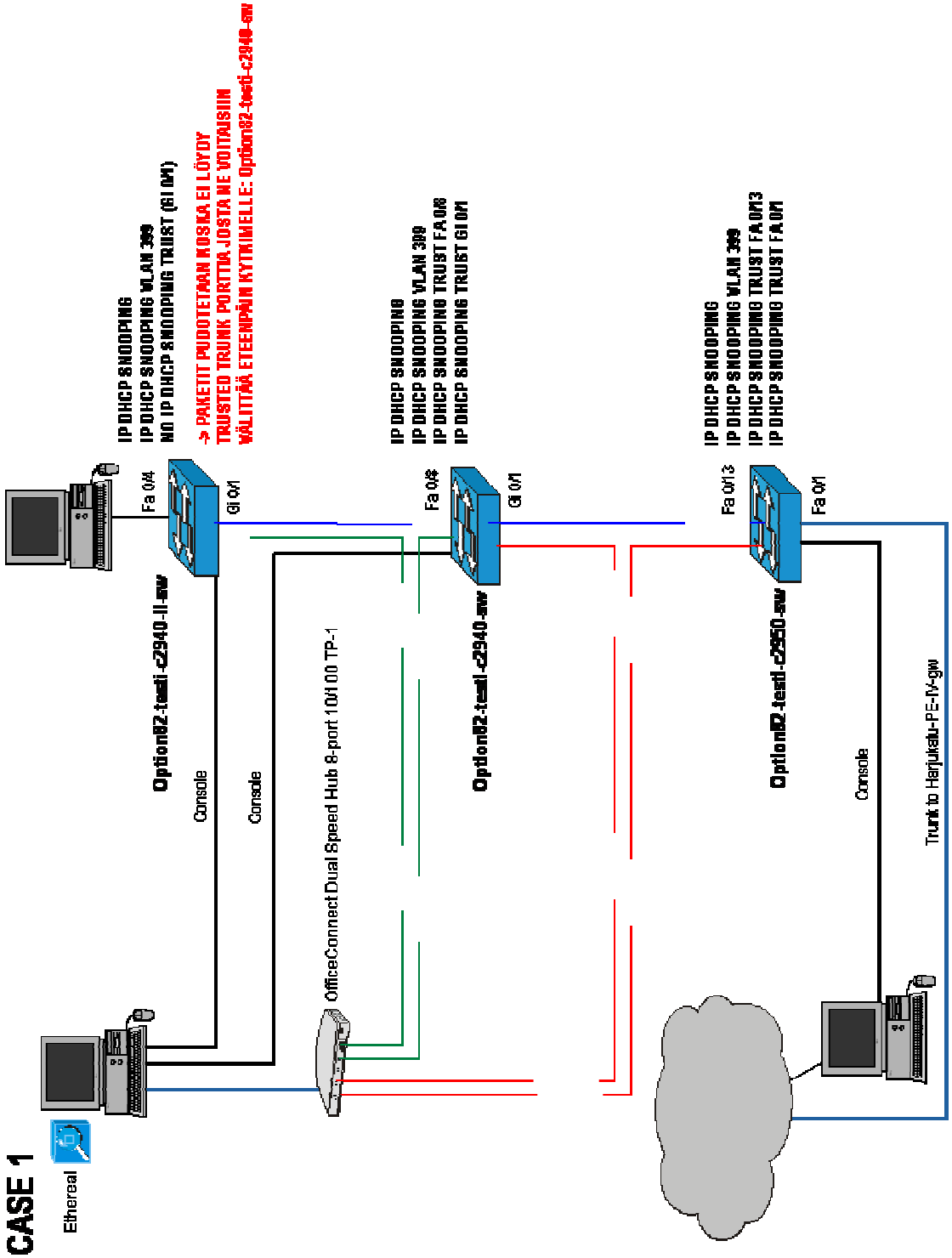
```
version 12.3
!
hostname Reititin
!
ip subnet-zero
ip flow-cache feature-accelerate
!
!
ip cef
ip dhcp excluded-address 10.0.140.1 10.0.140.16
ip dhcp relay information option
ip dhcp relay information policy keep
no ip dhcp relay information check
!
!
ip multicast-routing
ip dhcp-server 192.168.100.1
!
interface Loopback1
 description Oppilastalo Unnumbered Interface
 ip address 10.0.140.1 255.255.252.0
!
!
interface FastEthernet4/0
 description Yhteys Runkokytkimelle
 no ip address
 load-interval 30
 duplex full
!
interface FastEthernet4/0.1
 encapsulation dot1Q 1 native
 ip unnumbered Loopback1
!
interface FastEthernet4/0.407
 description Kohde 1
 encapsulation dot1Q 407
 ip unnumbered Loopback1
 ip access-group Oppilastalo out
 ip verify unicast source reachable-via rx
 ip helper-address 192.168.100.2
 no ip redirects
 no ip unreachables
 ip local-proxy-arp
 ip dhcp relay information trusted
!
```

LIITE 7

DHCP-palvelimia on kaksi ja tässä on esimerkki toisen konfiguraatiosta.

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
ddns-update-style none;
#deny duplicates;
# option definitions common to all supported networks...

default-lease-time 3600;
max-lease-time 7200;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# DHCP-server identifier

server-identifier 192.168.100.2;

class "oppilastalo" {
        spawn with option agent.circuit-id;
}

# Oppilastalo network
subnet 10.0.140.0 netmask 255.255.252.0 {
  pool {
        allow members of "oppilastalo";
        range 10.0.140.17 10.0.140.254;
        range 10.0.141.1 10.0.141.254;
        range 10.0.142.1 10.0.142.254;
        range 10.0.143.1 10.0.143.254;
        option routers 10.0.140.1;
        option domain-name "oppilastalo.phnet.fi";
  }
}
```

LIITE 8


CASE 1
Ethereal
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Console
Console
Console
Option82-testi-c2940-II-sw
Fa 0/4
Gi 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
NO IP DHCP SNOOPING TRUST (Gi 0/1)
-> PAKETIT PUDOTETAAN KOSKA EI LÖYDY
TRUSTED TRUNK PORTTIA JOSTA NE VOITAISIIN
VÄLITTÄÄ ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw
Option82-testi-c2940-sw
Fa 0/8
Gi 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST Gi 0/1
Option82-testi-c2950-sw
Fa 0/13
Fa 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1
Console
Trunk to Harjukatu-PE-M-gw

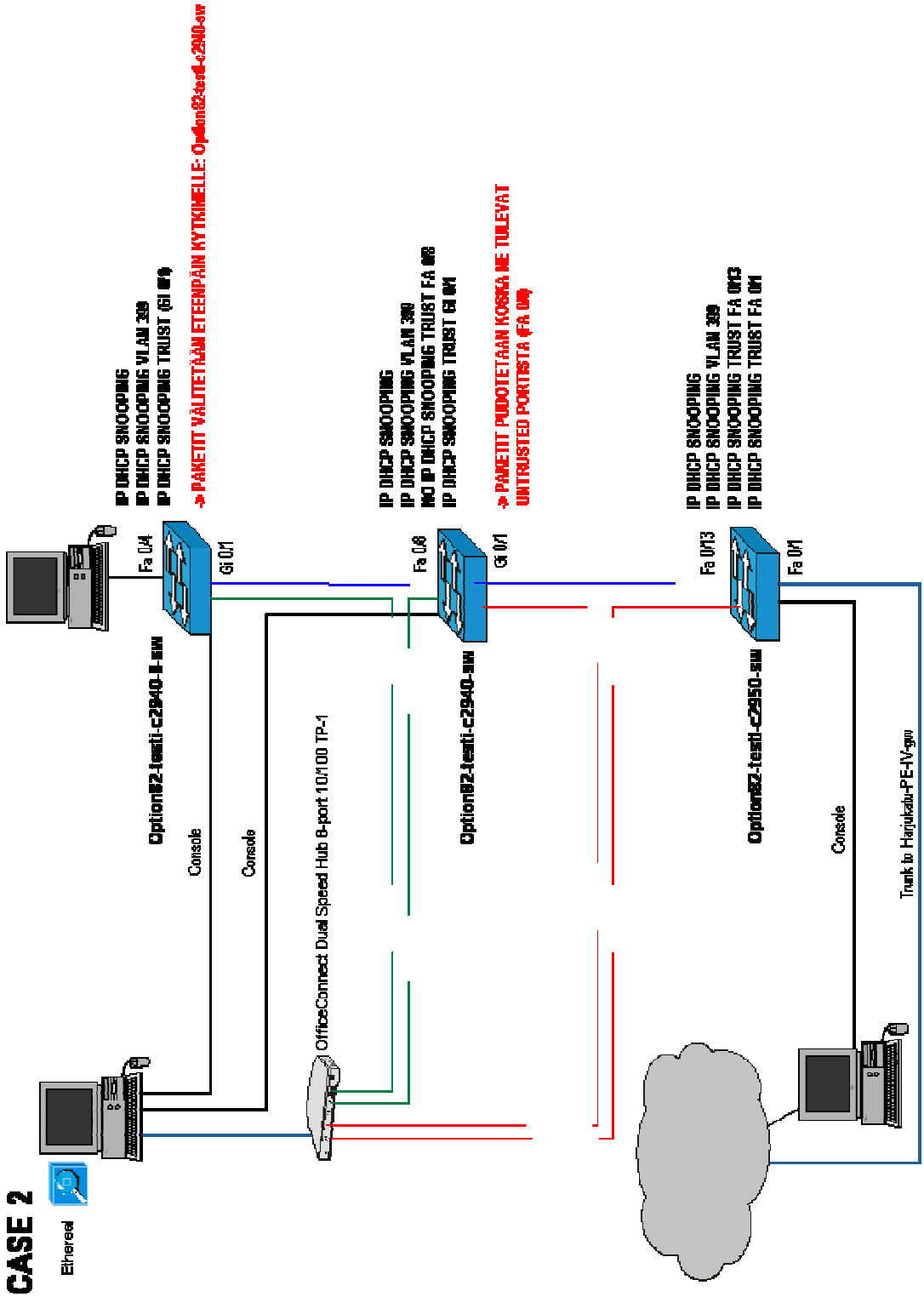
LIITE 8

CASE 1.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(NO IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT EI LÄHDE ETEENPÄIN

00:59:38: DHCP packet (count 42) on Fa0/4, VLAN 399
00:59:38: DHCP: Sent to DHCP Snooping on Fa0/4, VLAN 399
00:59:38: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
00:59:38: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPDISCOVER**
00:59:38: DHCP_SNOOPING: add relay information option.
00:59:38: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
00:59:38: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
00:59:38: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
00:59:38: DHCP_SNOOPING_SW: bridge packet output port set is null, packet is dropped.

LIITE 9


CASE 2
Ethereal
Option82-testi-c2940-II-sw
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Option82-testi-c2940-sw
Option82-testi-c2950-sw
Console
Trunk to Harjukatu-PE-IV-gw
Fa 0/4
Gi 0/1
Fa 0/8
Gi 0/1
Fa 0/13
Fa 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST Gi 0/1
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-test-c2940-sw
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
NO IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST Gi 0/1
-> PAKETIT PUDOTETAAN KOSKA NE TULEVAT
UNTRUSTED PORTISTA (FA 0/8)
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1

LIITE 9

CASE 2.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw

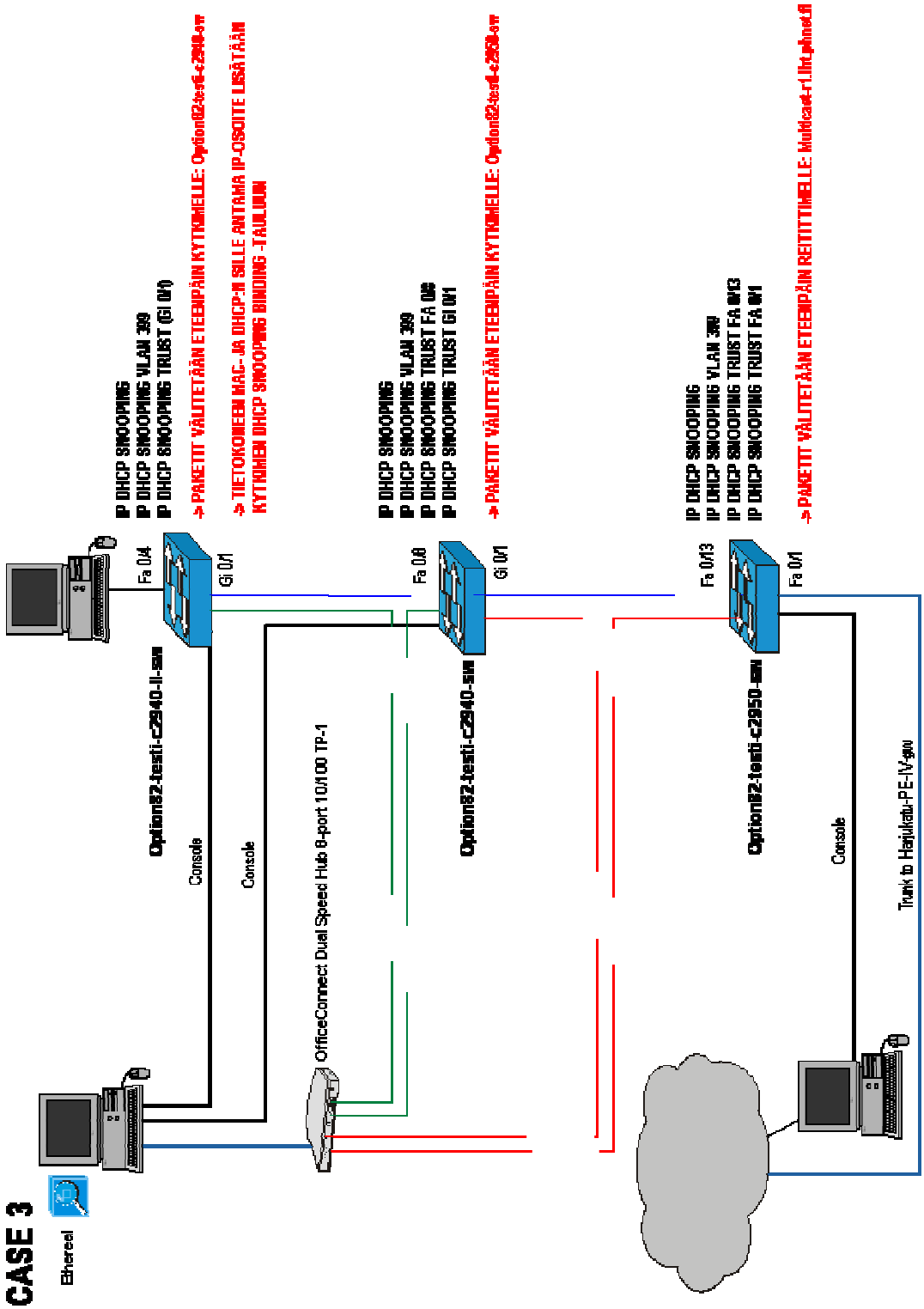
01:47:48: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
01:47:48: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPDISCOVER**
01:47:48: DHCP_SNOOPING: add relay information option.
01:47:48: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
01:47:48: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
01:47:48: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
01:47:48: DHCP_SNOOPING_SW: bridge packet send packet to port: GigabitEthernet0/1.

CASE 2.
(LOKI 2940) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(NO IP DHCP SNOOPING TRUST FA 0/8)
-> PAKETIT PUDOTETAAN KOSKA NE TULEVAT UNTRUSTED-PORTISTA (FA 0/8)
(IP DHCP SNOOPING TRUST GI 0/1)

*Mar 1 03:41:55: DHCP packet (count 72) on Fa0/8, VLAN 399
*Mar 1 03:41:55: DHCP: Sent to DHCP Snooping on Fa0/8, VLAN 399
*Mar 1 03:41:55: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/8)
*Mar 1 03:41:55: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPDISCOVER**
*Mar 1 03:41:55: DHCP_SNOOPING: drop message with non-zero giaddr or option 82 value on untrusted port, message type: DHCPDISCOVER

LIITE 10


CASE 3
Ethereal
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST (Gi 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82test-c2940-sw
-> TIETOKONEEN MAC- JA DHCP-IP SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
Fa 0/4
Gi 0/1
Option82-testi-C2940-II-sw
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST Gi 0/1
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82test-c2950-sw
Fa 0/8
Gi 0/1
Option82-testi-C2940-sw
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1
-> PAKETIT VÄLITETÄÄN ETEENPÄIN REITITTIMELLE: Multicast-r1.linxuhost.fi
Fa 0/13
Fa 0/1
Option82-testi-c2950-sw
Console
Trunk to Haijukatu-PE-IV-gw

LIITE 10

CASE 3.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE Option82-testi-c2940-sw

```
04:38:05: DHCP packet (count 360) on Fa0/4, VLAN 399
04:38:05: DHCP: Sent to DHCP Snooping on Fa0/4, VLAN 399
04:38:05: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
04:38:05: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER
04:38:05: DHCP_SNOOPING: add relay information option.
04:38:05: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
04:38:05: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
04:38:05: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
04:38:05: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.
04:38:06: DHCP packet (count 361) on Gi0/1, VLAN 399
04:38:06: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
04:38:06: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
04:38:06: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPOFFER
04:38:06: DHCP_SNOOPING: binary dump of extracted circuit id,
length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
04:38:06: DHCP_SNOOPING: binary dump of extracted remote id,
length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
04:38:06: DHCP_SNOOPING_SW: opt82 data indicates local packet
04:38:06: DHCP_SNOOPING: remove relay information option.
04:38:06: DHCP : hwidb is FastEthernet0/4
04:38:06: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.
04:38:06: DHCP packet (count 362) on Fa0/4, VLAN 399
04:38:06: DHCP: Sent to DHCP Snooping on Fa0/4, VLAN 399
04:38:06: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
04:38:06: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPREQUEST
04:38:06: DHCP_SNOOPING: add relay information option.
04:38:06: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
04:38:06: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
04:38:06: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
```

LIITE 10

```
04:38:06: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.
04:38:06: DHCP packet (count 363) on Gi0/1, VLAN 399
04:38:06: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
04:38:06: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
04:38:06: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPACK
04:38:06: DHCP_SNOOPING: binary dump of extracted circuit id,
length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
04:38:06: DHCP_SNOOPING: binary dump of extracted remote id,
length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
04:38:06: DHCP_SNOOPING_SW: opt82 data indicates local packet
04:38:06: DHCP_SNOOPING_SW: opt82 data indicates local packet
04:38:06: DHCP : hwidb is FastEthernet0/4
04:38:06: DHCP_SNOOPING: add binding on port FastEthernet0/4.
04:38:06: DHCP_SNOOPING: added entry to table (index 112)

04:38:06: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/4
04:38:06: DHCP_SNOOPING: remove relay information option.
04:38:06: DHCP : hwidb is FastEthernet0/4
04:38:06: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN ACCESS KYTKIMEN (2940-II) BINDING TAULUUN:

```
Option82-testi-c2940-II-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN
------------------  ---------------  ----------  -------  ----
00:08:74:94:C1:73   81.175.165.250   3373        dynamic  399

Interface
--------------------
FastEthernet0/4
```

LIITE 10

CASE 3.
(LOKI 2940) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST FA 0/8)
-> PAKETIT OTETAAN VASTAAN ACCESS KYTKIMELTÄ: Option82-testi-c2940-II-sw
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw

```
*Mar  1 06:30:31: DHCP packet (count 295) on Fa0/8, VLAN 399
*Mar  1 06:30:31: DHCP: Sent to DHCP Snooping on Fa0/8, VLAN 399
*Mar  1 06:30:31: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 06:30:31: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPDISCOVER
*Mar  1 06:30:31: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 06:30:31: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 06:30:32: DHCP packet (count 296) on Gi0/1, VLAN 399
*Mar  1 06:30:32: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
*Mar  1 06:30:32: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 06:30:32: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPOFFER
*Mar  1 06:30:32: DHCP_SNOOPING: binary dump of extracted circuit
id, length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
*Mar  1 06:30:32: DHCP_SNOOPING: binary dump of extracted remote
id, length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
*Mar  1 06:30:32: DHCP_SNOOPING_SW: opt82 data indicates not a
local packet
*Mar  1 06:30:32: DHCP_SNOOPING: can't parse option 82 data of
the message,it is either in wrong format or not inserted by local
switch
*Mar  1 06:30:32: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.

*Mar  1 06:30:32: DHCP packet (count 297) on Fa0/8, VLAN 399
*Mar  1 06:30:32: DHCP: Sent to DHCP Snooping on Fa0/8, VLAN 399
*Mar  1 06:30:32: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 06:30:32: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPREQUEST
*Mar  1 06:30:32: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 06:30:32: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 06:30:32: DHCP packet (count 298) on Gi0/1, VLAN 399
*Mar  1 06:30:32: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
*Mar  1 06:30:32: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
```

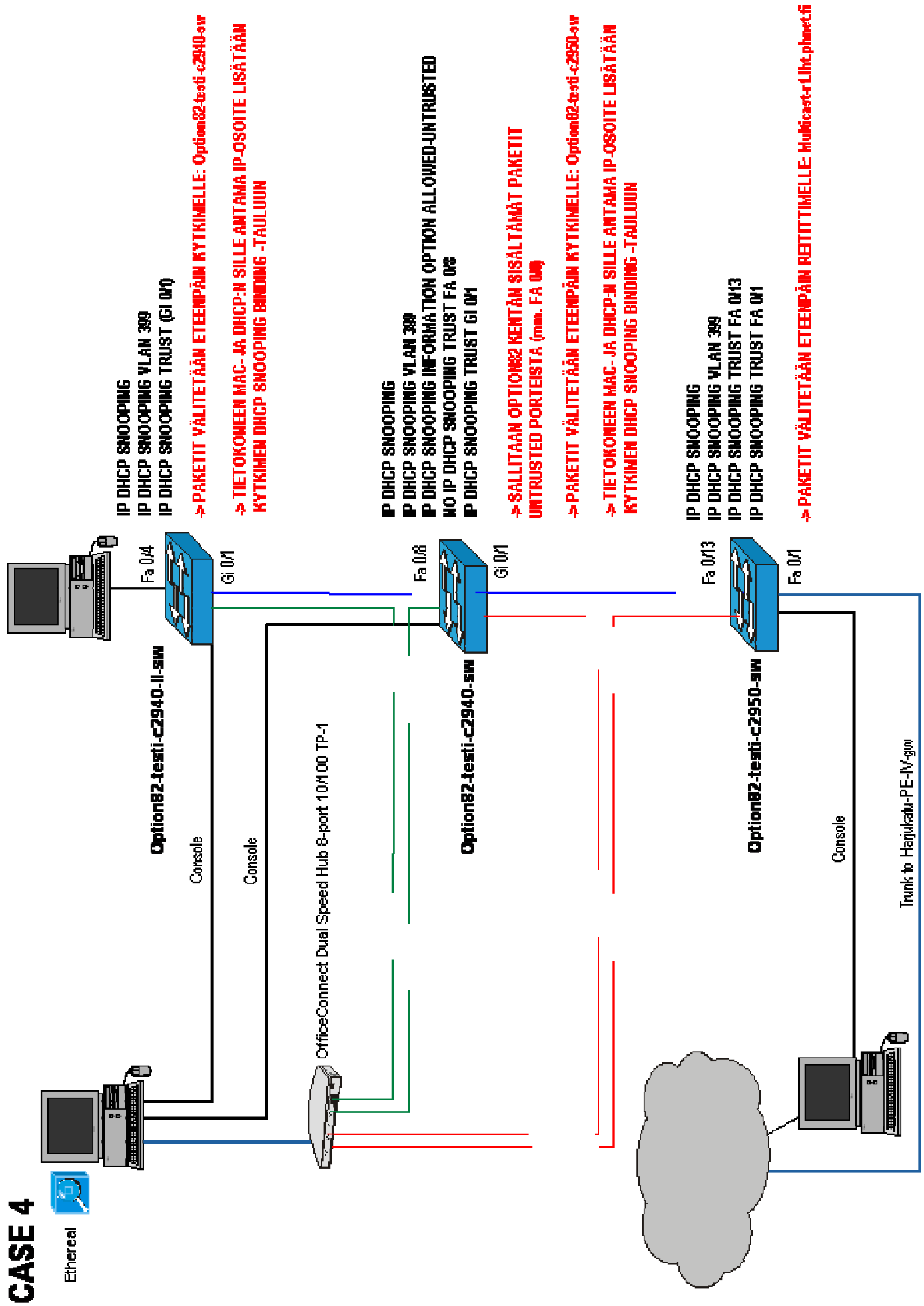
LIITE 10

```
*Mar  1 06:30:32: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPACK
*Mar  1 06:30:32: DHCP_SNOOPING: binary dump of extracted circuit
id, length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
*Mar  1 06:30:32: DHCP_SNOOPING: binary dump of extracted remote
id, length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
*Mar  1 06:30:32: DHCP_SNOOPING_SW: opt82 data indicates not a
local packet
*Mar  1 06:30:32: DHCP_SNOOPING: can't parse option 82 data of
the message,it is either in wrong format or not inserted by local
switch
*Mar  1 06:30:32: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.
```

KANNETTAVAN MAC- JA IP-OSOITETTA EI LISÄTÄ KYTKIMEN (2940) BINDING TAULUUN, KOSKA SEURAAVA PORTTI JOHON VIESTI VÄLITETÄÄN ON TRUSTED-PORTTI (FA 0/8):

```
Option82-testi-c2940-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN
------------------  ---------------  ----------  -------  ----

Interface
--------------------
```

LIITE 11


CASE 4
Ethereal
Option82-testi-c2940-II-sw
Fa 0/4
Gi 0/1
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Option82-testi-c2940-sw
Fa 0/8
Gi 0/1
Option82-testi-c2950-sw
Fa 0/13
Fa 0/1
Console
Trunk to Harjukatu-PE-IV-gw
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST (GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw
-> TIETOKONEEN MAC- JA DHCP:N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING INFORMATION OPTION ALLOWED-UNTRUSTED
NO IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST GI 0/1
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (mm. FA 0/8)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw
-> TIETOKONEEN MAC- JA DHCP:N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1
-> PAKETIT VÄLITETÄÄN ETEENPÄIN REITITTIMELLE: Multicast-r1.lht.phnet.fi

LIITE 11

CASE 4.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw

02:49:21: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
02:49:21: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPDISCOVER**
02:49:21: DHCP_SNOOPING: add relay information option.
02:49:21: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
02:49:21: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
02:49:21: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
02:49:21: DHCP_SNOOPING_SW: bridge packet send packet to port: GigabitEthernet0/1.

02:59:00: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet0/1)
02:59:00: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPOFFER**
02:59:00: DHCP_SNOOPING: binary dump of extracted circuit id, length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
02:59:00: DHCP_SNOOPING: binary dump of extracted remote id, length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
02:59:00: DHCP_SNOOPING_SW: opt82 data indicates local packet
02:59:00: DHCP_SNOOPING: remove relay information option.
02:59:00: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/4.

02:59:00: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/4)
02:59:00: DHCP_SNOOPING: process new DHCP packet, message type: **DHCPREQUEST**
02:59:00: DHCP_SNOOPING: add relay information option.
02:59:00: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
02:59:00: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
02:59:00: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
02:59:00: DHCP_SNOOPING_SW: bridge packet send packet to port: GigabitEthernet0/1.

02:59:00: DHCP_SNOOPING: received new DHCP packet from input interface (GigabitEthernet0/1)

LIITE 11

```
02:59:00: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPACK
02:59:00: DHCP_SNOOPING: binary dump of extracted circuit id,
length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
02:59:00: DHCP_SNOOPING: binary dump of extracted remote id,
length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
02:59:00: DHCP_SNOOPING_SW: opt82 data indicates local packet
02:59:00: DHCP_SNOOPING_SW: opt82 data indicates local packet
02:59:00: DHCP_SNOOPING: add binding on port FastEthernet0/4.
02:59:00: DHCP_SNOOPING: added entry to table (index 112)

02:59:00: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/4
02:59:00: DHCP_SNOOPING: remove relay information option.
02:59:00: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN ACCESS KYTKIMEN (2940-II) BINDING TAULUUN:

```
Option82-testi-c2940-II-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
------------------  ---------------  ----------  -------  ----
00:08:74:94:C1:73   81.175.165.250   2586        dynamic  399

Interface
--------------------
FastEthernet0/4
```

CASE 4.
(LOKI 2940) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING INFORMATION OPTION ALLOWED-UNTRUSTED)
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(NO IP DHCP SNOOPING TRUST FA 0/8)
-> PAKETIT OTETAAN VASTAAN EDELLISELTÄ KYTKIMELTÄ KOSKA KONFIGURAATIOSSA ON SALLITTU OPTION-KENTTÄ UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw

```
*Mar  1 04:42:13: DHCP packet (count 156) on Fa0/8, VLAN 399
*Mar  1 04:42:13: DHCP: Sent to DHCP Snooping on Fa0/8, VLAN 399
*Mar  1 04:42:13: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 04:42:13: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPDISCOVER
```

LIITE 11

```
*Mar  1 04:42:13: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 04:42:13: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 04:49:49: DHCP packet (count 169) on Gi0/1, VLAN 399
*Mar  1 04:49:49: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
*Mar  1 04:49:49: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 04:49:49: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPOFFER
*Mar  1 04:49:49: DHCP_SNOOPING: binary dump of extracted circuit
id, length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
*Mar  1 04:49:50: DHCP_SNOOPING: binary dump of extracted remote
id, length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
*Mar  1 04:49:50: DHCP_SNOOPING_SW: opt82 data indicates not a
local packet
*Mar  1 04:49:50: DHCP_SNOOPING: can't parse option 82 data of
the message,it is either in wrong format or not inserted by local
switch
*Mar  1 04:49:50: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.

*Mar  1 04:49:50: DHCP packet (count 170) on Fa0/8, VLAN 399
*Mar  1 04:49:50: DHCP: Sent to DHCP Snooping on Fa0/8, VLAN 399
*Mar  1 04:49:50: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 04:49:50: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPREQUEST
*Mar  1 04:49:50: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 04:49:50: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 04:49:50: DHCP packet (count 171) on Gi0/1, VLAN 399
*Mar  1 04:49:50: DHCP: Sent to DHCP Snooping on Gi0/1, VLAN 399
*Mar  1 04:49:50: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 04:49:50: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPACK
*Mar  1 04:49:50: DHCP_SNOOPING: binary dump of extracted circuit
id, length: 8 data:
0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3
*Mar  1 04:49:50: DHCP_SNOOPING: binary dump of extracted remote
id, length: 10 data:
0x2 0x8 0x0 0x6 0x0 0x13 0xC4 0x6C 0x56 0x0
*Mar  1 04:49:50: DHCP_SNOOPING_SW: opt82 data indicates not a
local packet
*Mar  1 04:49:50: DHCP_SNOOPING: can't parse option 82 data of
the message,it is either in wrong format or not inserted by local
switch
*Mar  1 04:49:50: DHCP_SNOOPING: add binding on port
FastEthernet0/8.
*Mar  1 04:49:50: DHCP_SNOOPING: added entry to table (index 112)
```

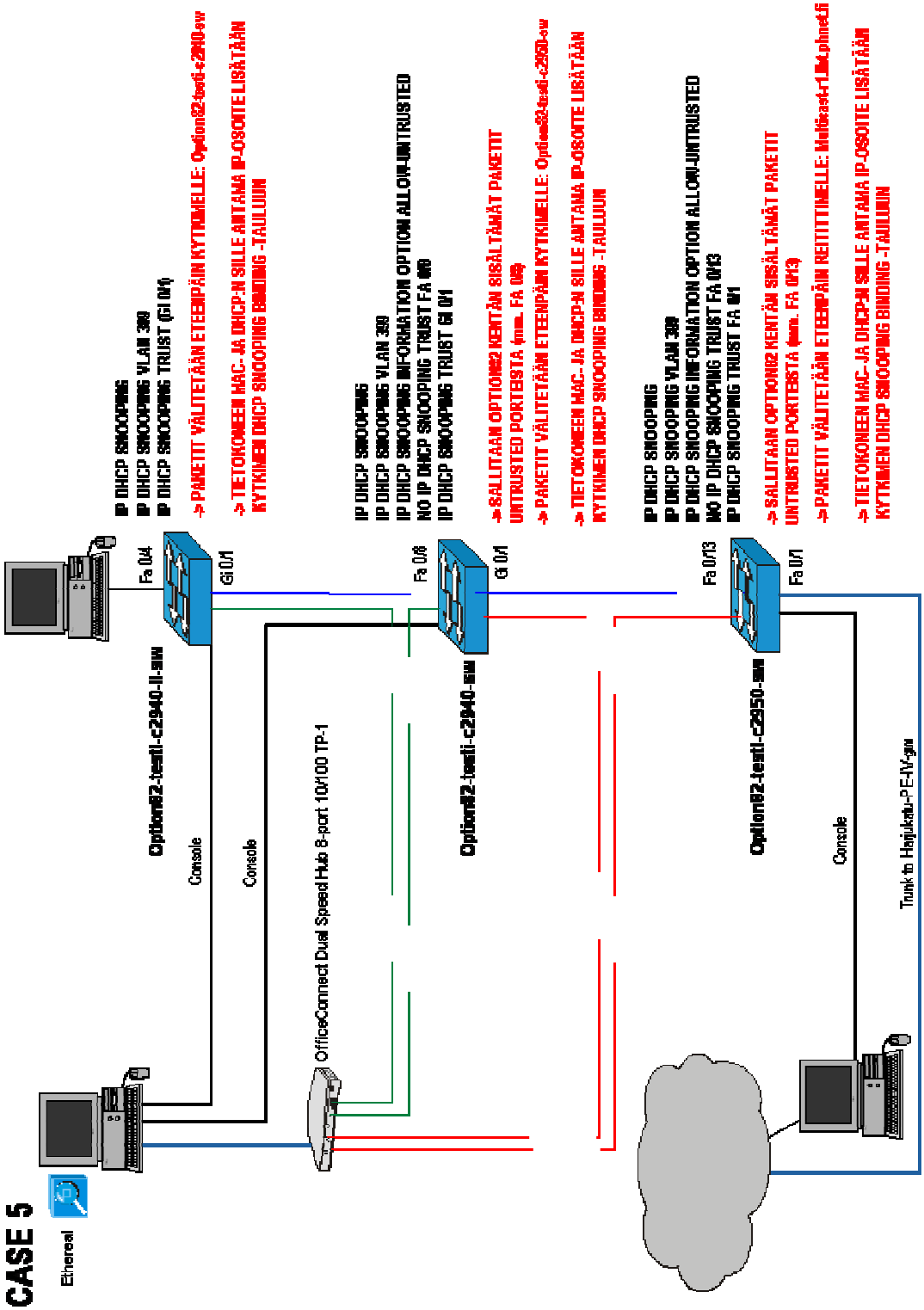
LIITE 11

```
*Mar  1 04:49:50: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/8
*Mar  1 04:49:50: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS KYTKIMEN (2940) BINDING TAULUUN, KOSKA SEURAAVA PORTTI JOHON VIESTI VÄLITETÄÄN ON UNTRUSTED-PORTTI (FA 0/8):

```
Option82-testi-c2940-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN
------------------  ---------------  ----------  -------  ----
00:08:74:94:C1:73   81.175.165.250   3109        dynamic  399

Interface
--------------------
FastEthernet0/8
```

LIITE 12


CASE 5
Ethereal
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Console
Trunk to Haijukatu-PE-1/-gw
Fa 0/4
Gi 0/1
Fa 0/8
Gi 0/1
Fa 0/13
Fa 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
IP DHCP SNOOPING TRUST (Gi 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw
-> TIETOKONEEN MAC- JA DHCP-N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED
NO IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST Gi 0/1
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (mm. FA 0/8)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw
-> TIETOKONEEN MAC- JA DHCP-N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 300
IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED
NO IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (mm. FA 0/13)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN REITITTIMELLE: Meliteast-r1.Mt.phnet.fi
-> TIETOKONEEN MAC- JA DHCP-N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN

LIITE 12

CASE 5.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw

```
01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER
01:52:04: DHCP_SNOOPING: add relay information option.
01:52:04: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
01:52:04: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
01:52:04: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
01:52:04: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPOFFER
01:52:04: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPREQUEST
01:52:04: DHCP_SNOOPING: add relay information option.
01:52:04: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
01:52:04: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
01:52:04: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
01:52:04: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPACK
01:52:04: DHCP_SNOOPING: add binding on port FastEthernet0/4.
01:52:04: DHCP_SNOOPING: added entry to table (index 112)

01:52:04: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/4
```

LIITE 12

```
01:52:04: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN ACCESS KYTKIMEN (2940-II) BINDING TAULUUN:

```
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
------------------  ---------------  ----------  -------  ----  -
00:08:74:94:C1:73   81.175.165.250   2765        dynamic  399

Interface
--------------------
FastEthernet0/4
```

LIITE 12

CASE 5.
(LOKI 2940) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED)
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(NO IP DHCP SNOOPING TRUST FA 0/8)
-> PAKETIT OTETAAN VASTAAN ACCESS KYTKIMELTÄ: Option82-testi-c2940-II-sw, KOSKA KONFIGURAATIOSSA ON SALLITTU OPTION-KENTTÄ UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw

```
*Mar  1 03:52:10: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 03:52:10: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPDISCOVER
*Mar  1 03:52:10: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:10: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPOFFER
*Mar  1 03:52:11: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPREQUEST
*Mar  1 03:52:11: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:11: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPACK
*Mar  1 03:52:11: DHCP_SNOOPING: add binding on port
FastEthernet0/8.
*Mar  1 03:52:11: DHCP_SNOOPING: added entry to table (index 112)

*Mar  1 03:52:11: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/8
*Mar  1 03:52:11: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.
```

LIITE 12

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS TÄMÄN KYTKIMEN (2940) BINDING TAULUUN, KOSKA SEURAAVA PORTTI JOHON VIESTI VÄLITETÄÄN ON UNTRUSTED-PORTTI (FA 0/8):

```
Option 82 on untrusted port is allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
------------------  ---------------  ----------  -------  ----  -
00:08:74:94:C1:73   81.175.165.250   2687        dynamic  399

Interface
--------------------
FastEthernet0/8
```

LIITE 12

CASE 5.
(LOKI 2950) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED)
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (muun muassa FA 0/13)
(NO IP DHCP SNOOPING TRUST FA 0/13)
-> PAKETIT OTETAAN VASTAAN EDELLISELTÄ KYTKIMELTÄ: Option82-testi-c2940-sw, KOSKA KONFIGURAATIOSSA ON SALLITTU OPTION-KENTTÄ UNTRUSTED PORTEISTA (muun muassa FA 0/13)
(IP DHCP SNOOPING TRUST FA 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN REITITTIMELLE: Multicast-r1.lht.phnet.fi

```
*Mar  1 03:52:36: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/13)
*Mar  1 03:52:36: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPDISCOVER
*Mar  1 03:52:36: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:36: DHCP_SNOOPING_SW: bridge packet send packet to
port: FastEthernet0/1.

*Mar  1 03:52:36: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/1)
*Mar  1 03:52:36: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPOFFER
*Mar  1 03:52:36: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/13.

*Mar  1 03:52:36: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/13)
*Mar  1 03:52:36: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPREQUEST
*Mar  1 03:52:36: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:36: DHCP_SNOOPING_SW: bridge packet send packet to
port: FastEthernet0/1.

*Mar  1 03:52:36: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/1)
*Mar  1 03:52:36: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPACK
*Mar  1 03:52:36: DHCP_SNOOPING: add binding on port
FastEthernet0/13.
*Mar  1 03:52:36: DHCP_SNOOPING: added entry to table (index 112)

*Mar  1 03:52:36: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/13
*Mar  1 03:52:36: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/13.
```

LIITE 12

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS TÄMÄN KYTKIMEN (2950) BINDING TAULUUN, KOSKA SEURAAVA PORTTI JOHON VIESTI VÄLITETÄÄN ON UNTRUSTED-PORTTI (FA 0/13):

```
Option 82 on untrusted port is allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
------------------  ---------------  ----------  -------  ----
00:08:74:94:C1:73   81.175.165.250   1096        dynamic  399

Interface
------------------
FastEthernet0/13
```

LIITE 12

CASE 5.
(LOKI Multicast) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

```
Jul 25 13:10:23: DHCPD: message is from trusted interface
GigabitEthernet0/2.399
Jul 25 13:10:23: DHCPD: Sending notification of DISCOVER:
Jul 25 13:10:23:   DHCPD: htype 1 chaddr 0008.7494.c173
Jul 25 13:10:23:   DHCPD: remote id 020a000051afa4010200018f0000
// TULKATTU ALLA
Jul 25 13:10:23:   DHCPD: circuit id 00000000
// ILMEISESTI EI KÄYTÖSSÄ
Jul 25 13:10:23: DHCPD: Removing previous binding
Jul 25 13:10:23: DHCPD: dhcpd_lookup_route: host = 81.175.165.250
Jul 25 13:10:23: DHCPD: dhcpd_lookup_route: index = 161
Jul 25 13:10:23: DHCPD: Adding binding to hash tree
Jul 25 13:10:23: DHCPD: relay binding created for client
0100.0874.94c1.73.
Jul 25 13:10:23: DHCPD: Keeping state for received DHCPDISCOVER,
from UNNUM-IF
Jul 25 13:10:23: DHCPD: setting giaddr to 81.175.164.1.
Jul 25 13:10:23: DHCPD: leaving relay information in tact.
Jul 25 13:10:23: DHCPD: BOOTREQUEST from 0100.0874.94c1.73
forwarded to 172.20.0.10.

Jul 25 13:10:23: DHCPD: forwarding BOOTREPLY to client
0008.7494.c173.
Jul 25 13:10:23: DHCPD: Forwarding reply while saving lease
state, on UNNUM-IF
Jul 25 13:10:23: DHCPD: Keeping state: Received DHCPOFFER, from
UNNUM-IF
Jul 25 13:10:23:  DHCPD: lease time of offer = 3600
Jul 25 13:10:23:  DHCPD: Server Address = 172.20.0.10
Jul 25 13:10:23:  DHCPD: Giaddr Address = 81.175.164.1
Jul 25 13:10:23:  outbound IF index  = 4
Jul 25 13:10:23:  outbound IF sub-index = 399
Jul 25 13:10:23: DHCPD: Keeping state: Forwarding BOOTREPLY to
client 0008.7494.c173, on UNNUM-IF

Jul 25 13:10:23: DHCPD: message is from trusted interface
GigabitEthernet0/2.399
Jul 25 13:10:23: DHCPD: Finding a relay for client
0100.0874.94c1.73 on interface GigabitEthernet0/2.399.
Jul 25 13:10:23: DHCPD: Seeing if there is an internally
specified pool class:
Jul 25 13:10:23:   DHCPD: htype 1 chaddr 0008.7494.c173
Jul 25 13:10:23:   DHCPD: remote id 020a000051afa4010200018f0000
Jul 25 13:10:23:   DHCPD: circuit id 00000000
Jul 25 13:10:23: DHCPD: there is no pool for 81.175.164.1.
Jul 25 13:10:23: DHCPD: Found previous binding with giaddr
81.175.164.1
Jul 25 13:10:23: DHCPD: Keeping state for received DHCPREQUEST,
from UNNUM-IF
Jul 25 13:10:23:  DHCPD: keeping state: Real Server =
172.20.0.10, from UNNUM-IF
Jul 25 13:10:23: DHCPD: setting giaddr to 81.175.164.1.
Jul 25 13:10:23: DHCPD: leaving relay information in tact.
Jul 25 13:10:23: DHCPD: BOOTREQUEST from 0100.0874.94c1.73
forwarded to 172.20.0.10.
```

LIITE 12

```
Jul 25 13:10:23: DHCPD: forwarding BOOTREPLY to client
0008.7494.c173.
Jul 25 13:10:23: DHCPD: Forwarding reply while saving lease
state, on UNNUM-IF
Jul 25 13:10:23: DHCPD: Keeping state: Received DHCPACK, from
UNNUM-IF
Jul 25 13:10:23:  DHCPD: lease time = 3600
Jul 25 13:10:23:  DHCPD: Server ID saved in Binding = 172.20.0.10
Jul 25 13:10:23:  DHCPD: Giaddr Address = 81.175.164.1
Jul 25 13:10:23: DHCPD: Adding binding to radix tree
(81.175.165.250)
Jul 25 13:10:23: DHCPD: Sending notification of ASSIGNMENT:
Jul 25 13:10:23:  DHCPD: address 81.175.165.250 mask
255.255.254.0
Jul 25 13:10:23:   DHCPD: htype 1 chaddr 0008.7494.c173
Jul 25 13:10:23:   DHCPD: lease time remaining (secs) = 3600
Jul 25 13:10:23: DHCPD: dhcpd_lookup_route: host = 81.175.165.250
Jul 25 13:10:23: DHCPD: dhcpd_lookup_route: index = 161
Jul 25 13:10:23: DHCPD: dhcpd_create_and_hash_route: host =
81.175.165.250
Jul 25 13:10:23: DHCPD: dhcpd_create_and_hash_route index = 161
Jul 25 13:10:23: DHCPD: dhcpd_add_route: lease = 3600
Jul 25 13:10:23:  outbound IF index  = 4
Jul 25 13:10:23:  outbound IF sub-index = 399
Jul 25 13:10:23: DHCPD: Keeping state: Forwarding BOOTREPLY to
client 0008.7494.c173, on UNNUM-IF
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS REITITTIMEN DHCP BINDING TAULUUN:

```
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration        Type
                Hardware address/
                User name
81.175.164.3    00d0.591c.9118      Jul 25 2005 01:59 PM    Relay
81.175.164.9    fe02.2144.0035      Jul 25 2005 01:47 PM    Relay
81.175.164.245  fe00.2944.0035      Jul 25 2005 01:54 PM    Relay
81.175.164.246  fe01.1908.000f      Jul 25 2005 02:11 PM    Relay
81.175.164.249  fe03.1908.000f      Jul 25 2005 02:30 PM    Relay
81.175.165.243  fe02.0108.000f      Jul 25 2005 01:54 PM    Relay
81.175.165.249  fe02.1908.000f      Jul 25 2005 01:46 PM    Relay
81.175.165.250  0008.7494.c173      Jul 25 2005 02:10 PM    Relay
81.175.165.252  fe02.4950.0035      Jul 25 2005 02:02 PM    Relay
```

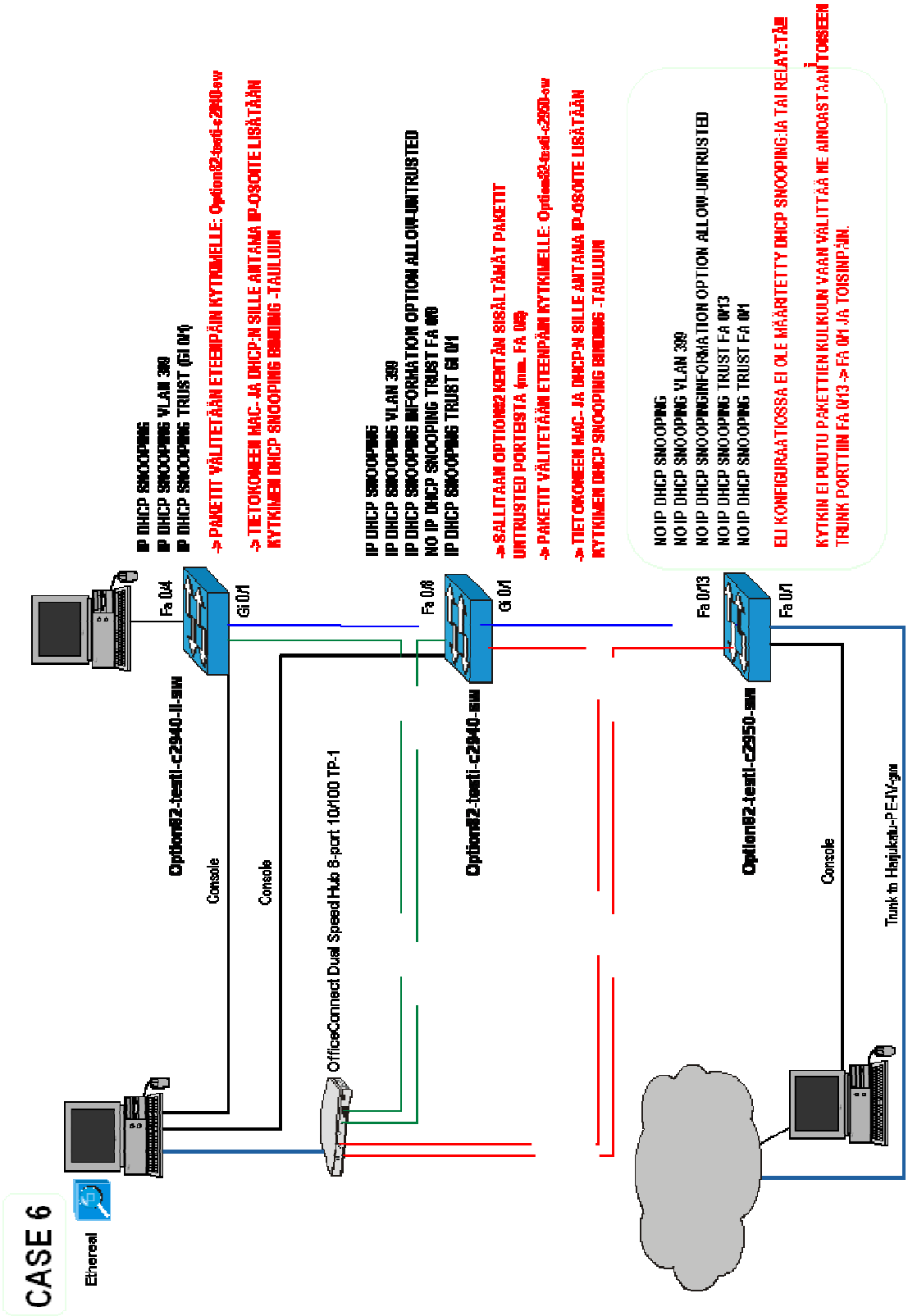
LIITE 12

FORMAT OF THE AGENT REMOTE ID SUBOPTION (VLANS OVER UNNUMBERED INTERFACE)

remote id 020a0000**51afa401**02**00018f**0000

02	**= Format type 02 = 2 (vlan over unnumbered)**
0a	**= Lenght 0a = 10 bytes (not including the type & lenght fields)**
00 00	= reserved (2 bytes)
51 af a4 01	**= NAS IP address (4 bytes) 51=81 af=175 a4=164 01=1 => 81.175.164.1**
02	**= Physical interface (slot=4bits|mod=1bit|port=3bits)(0000 = slot 0 | 0 = mod 0 | 010 = port 2)**
00	= reserved (1 byte)
018f	**= VLAN id 018f = 399**
00 00	= ????

LIITE 13


CASE 6
Ethereal
Option82-testi-c2940-II-sw
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Option82-testi-c2940-sw
Option82-testi-c2950-sw
Console
Trunk to Haijukatu-PE-1/-gw
Fa 0/4
Gi 0/1
Fa 0/8
Gi 0/1
Fa 0/13
Fa 0/1
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING TRUST (Gi 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw
-> TIETOKONEEN MAC- JA DHCP-N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 399
IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED
NO IP DHCP SNOOPING TRUST FA 0/8
IP DHCP SNOOPING TRUST Gi 0/1
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (mm. FA 0/8)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw
-> TIETOKONEEN MAC- JA DHCP-N SILLE ANTAMA IP-OSOITE LISÄTÄÄN KYTKIMEN DHCP SNOOPING BINDING -TAULUUN
NO IP DHCP SNOOPING
NO IP DHCP SNOOPING VLAN 399
NO IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED
NO IP DHCP SNOOPING TRUST FA 0/13
NO IP DHCP SNOOPING TRUST FA 0/1
ELI KONFIGURAATIOSSA EI OLE MÄÄRITETTY DHCP SNOOPING:IA TAI RELAY:TÄ
KYTKIN EI PUUTU PAKETTIEN KULKUUN VAAN VALITTÄÄ ME AINOASTAAN TOISEEN TRUNK PORTTIIN FA 0/13 -> FA 0/1 JA TOISINPÄIN.

LIITE 13

CASE 6.
(LOKI 2940-II) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2940-sw

LOKI ON VASTAAVA KUIN CASE 5:SSÄ (KOPIO ALLA).

```
01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPDISCOVER
01:52:04: DHCP_SNOOPING: add relay information option.
01:52:04: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
01:52:04: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
01:52:04: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
01:52:04: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPOFFER
01:52:04: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (FastEthernet0/4)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPREQUEST
01:52:04: DHCP_SNOOPING: add relay information option.
01:52:04: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port
format
01:52:04: DHCP_SNOOPING: binary dump of relay info option,
length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x8F 0x0 0x3 0x2 0x8 0x0 0x6 0x0
0x13 0xC4 0x6C 0x56 0x0
01:52:04: DHCP_SNOOPING_SW: bridge packet get invalid mat entry:
FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
01:52:04: DHCP_SNOOPING_SW: bridge packet send packet to port:
GigabitEthernet0/1.

01:52:04: DHCP_SNOOPING: received new DHCP packet from input
interface (GigabitEthernet0/1)
01:52:04: DHCP_SNOOPING: process new DHCP packet, message type:
DHCPACK
01:52:04: DHCP_SNOOPING: add binding on port FastEthernet0/4.
01:52:04: DHCP_SNOOPING: added entry to table (index 112)
```

LIITE 13

```
01:52:04: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/4
01:52:04: DHCP_SNOOPING: direct forward dhcp reply to output
port: FastEthernet0/4.
```

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN ACCESS KYTKIMEN (2940-II) BINDING TAULUUN:

```
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
-----------------  ---------------  ----------  -------  ----  -
00:08:74:94:C1:73   81.175.165.250   2765        dynamic  399

Interface
-------------------
FastEthernet0/4
```

LIITE 13

CASE 6. (LOKI 2940) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(IP DHCP SNOOPING)
(IP DHCP SNOOPING VLAN 399)
(IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED)
-> SALLITAAN OPTION82 KENTÄN SISÄLTÄMÄT PAKETIT UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(NO IP DHCP SNOOPING TRUST FA 0/8)
-> PAKETIT OTETAAN VASTAAN ACCESS KYTKIMELTÄ: Option82-testi-c2940-II-sw, KOSKA KONFIGURAATIOSSA ON SALLITTU OPTION-KENTTÄ UNTRUSTED PORTEISTA (muun muassa FA 0/8)
(IP DHCP SNOOPING TRUST GI 0/1)
-> PAKETIT VÄLITETÄÄN ETEENPÄIN KYTKIMELLE: Option82-testi-c2950-sw

LOKI ON VASTAAVA KUIN CASE 5:SSÄ (KOPIO ALLA).

```
*Mar  1 03:52:10: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 03:52:10: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPDISCOVER
*Mar  1 03:52:10: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:10: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPOFFER
*Mar  1 03:52:11: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/8)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPREQUEST
*Mar  1 03:52:11: DHCP_SNOOPING_SW: bridge packet get invalid mat
entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (399)
*Mar  1 03:52:11: DHCP_SNOOPING_SW: bridge packet send packet to
port: GigabitEthernet0/1.

*Mar  1 03:52:11: DHCP_SNOOPING: received new DHCP packet from
input interface (GigabitEthernet0/1)
*Mar  1 03:52:11: DHCP_SNOOPING: process new DHCP packet, message
type: DHCPACK
*Mar  1 03:52:11: DHCP_SNOOPING: add binding on port
FastEthernet0/8.
*Mar  1 03:52:11: DHCP_SNOOPING: added entry to table (index 112)

*Mar  1 03:52:11: DHCP_SNOOPING: dump binding entry:
Mac=00:08:74:94:C1:73 Ip=81.175.165.250 Lease=3600 Type=dynamic
Vlan=399 If=FastEthernet0/8
*Mar  1 03:52:11: DHCP_SNOOPING: direct forward dhcp reply to
output port: FastEthernet0/8.
```

LIITE 13

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS TÄMÄN KYTKIMEN (2940) BINDING TAULUUN, KOSKA SEURAAVA PORTTI JOHON VIESTI VÄLITETÄÄN ON UNTRUSTED-PORTTI (FA 0/8):

```
Option 82 on untrusted port is allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  -
----------------  ---------------  ----------  -------  ----  ---
00:08:74:94:C1:73   81.175.165.250   2687        dynamic  399

Interface
--------------------
FastEthernet0/8
```

LIITE 13

CASE 6.
(LOKI 2950) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

(NO IP DHCP SNOOPING)
(NO IP DHCP SNOOPING VLAN 399)
(NO IP DHCP SNOOPING INFORMATION OPTION ALLOW-UNTRUSTED)
(NO IP DHCP SNOOPING TRUST FA 0/13)
(NO IP DHCP SNOOPING TRUST FA 0/1)

ELI KONFIGURAATIOSSA EI OLE MÄÄRITETTY DHCP SNOOPING:IA TAI RELAY:TÄ!!

LOKIIN EI KERRY TIETOA KOSKA KYTKIN EI PUUTU PAKETTIEN KULKUUN VAAN VÄLITTÄÄ NE AINOASTAAN TOISEEN TRUNK PORTTIIN FA 0/13 -> FA 0/1 JA TOISINPÄIN.

CASE 6.
(LOKI Multicast) KANNETTAVA KYTKETTY 2940-II PORTTIIN FA 0/4

GLOBAALI
(ip dhcp relay information option)
(ip dhcp relay information policy keep)
(no ip dhcp relay information check)

INTERFACE GI 0/2.399
(ip dhcp relay information trusted)
(ip helper-address 172.20.0.10)

Jul 26 13:49:43: DHCPD: message is from trusted interface GigabitEthernet0/2.399
Jul 26 13:49:43: DHCPD: Sending notification of DISCOVER:
Jul 26 13:49:43: DHCPD: htype 1 chaddr 0008.7494.c173
Jul 26 13:49:43: DHCPD: remote id 020a000051afa4010200018f0000
Jul 26 13:49:43: DHCPD: circuit id 00000000
Jul 26 13:49:43: DHCPD: Removing previous binding
Jul 26 13:49:43: DHCPD: dhcpd_lookup_route: host = 81.175.165.250
Jul 26 13:49:43: DHCPD: dhcpd_lookup_route: index = 161
Jul 26 13:49:43: DHCPD: Adding binding to hash tree
Jul 26 13:49:43: DHCPD: relay binding created for client 0100.0874.94c1.73.
Jul 26 13:49:43: DHCPD: Keeping state for received **DHCPDISCOVER**, from UNNUM-IF
Jul 26 13:49:43: DHCPD: setting giaddr to 81.175.164.1.
Jul 26 13:49:43: DHCPD: leaving relay information in tact.
Jul 26 13:49:43: DHCPD: BOOTREQUEST from 0100.0874.94c1.73 forwarded to 172.20.0.10.

Jul 26 13:49:43: DHCPD: forwarding BOOTREPLY to client 0008.7494.c173.
Jul 26 13:49:43: DHCPD: Forwarding reply while saving lease state, on UNNUM-IF
Jul 26 13:49:43: DHCPD: Keeping state: Received **DHCPOFFER**, from UNNUM-IF
Jul 26 13:49:43: DHCPD: lease time of offer = 3600
Jul 26 13:49:43: DHCPD: Server Address = 172.20.0.10
Jul 26 13:49:43: DHCPD: Giaddr Address = 81.175.164.1
Jul 26 13:49:43: outbound IF index = 4
Jul 26 13:49:43: outbound IF sub-index = 399
Jul 26 13:49:43: DHCPD: Keeping state: Forwarding BOOTREPLY to client 0008.7494.c173, on UNNUM-IF

LIITE 13

```
Jul 26 13:49:43: DHCPD: message is from trusted interface
GigabitEthernet0/2.399
Jul 26 13:49:43: DHCPD: Finding a relay for client
0100.0874.94c1.73 on interface GigabitEthernet0/2.399.
Jul 26 13:49:43: DHCPD: Seeing if there is an internally
specified pool class:
Jul 26 13:49:43:   DHCPD: htype 1 chaddr 0008.7494.c173
Jul 26 13:49:43:   DHCPD: remote id 020a000051afa4010200018f0000
Jul 26 13:49:43:   DHCPD: circuit id 00000000
Jul 26 13:49:43: DHCPD: there is no pool for 81.175.164.1.
Jul 26 13:49:43: DHCPD: Found previous binding with giaddr
81.175.164.1
Jul 26 13:49:43: DHCPD: Keeping state for received DHCPREQUEST,
from UNNUM-IF
Jul 26 13:49:43:  DHCPD: keeping state: Real Server =
172.20.0.10, from UNNUM-IF
Jul 26 13:49:43: DHCPD: setting giaddr to 81.175.164.1.
Jul 26 13:49:43: DHCPD: leaving relay information in tact.
Jul 26 13:49:43: DHCPD: BOOTREQUEST from 0100.0874.94c1.73
forwarded to 172.20.0.10.

Jul 26 13:49:43: DHCPD: forwarding BOOTREPLY to client
0008.7494.c173.
Jul 26 13:49:43: DHCPD: Forwarding reply while saving lease
state, on UNNUM-IF
Jul 26 13:49:43: DHCPD: Keeping state: Received DHCPACK, from
UNNUM-IF
Jul 26 13:49:43:  DHCPD: lease time = 3600
Jul 26 13:49:43:  DHCPD: Server ID saved in Binding = 172.20.0.10
Jul 26 13:49:43:  DHCPD: Giaddr Address = 81.175.164.1
Jul 26 13:49:43: DHCPD: Adding binding to radix tree
(81.175.165.250)
Jul 26 13:49:43: DHCPD: Sending notification of ASSIGNMENT:
Jul 26 13:49:43:  DHCPD: address 81.175.165.250 mask
255.255.254.0
Jul 26 13:49:43:   DHCPD: htype 1 chaddr 0008.7494.c173
Jul 26 13:49:43:   DHCPD: lease time remaining (secs) = 3600
Jul 26 13:49:43: DHCPD: dhcpd_lookup_route: host = 81.175.165.250
Jul 26 13:49:43: DHCPD: dhcpd_lookup_route: index = 161
Jul 26 13:49:43: DHCPD: dhcpd_create_and_hash_route: host =
81.175.165.250
Jul 26 13:49:43: DHCPD: dhcpd_create_and_hash_route index = 161
Jul 26 13:49:43: DHCPD: dhcpd_add_route: lease = 3600
Jul 26 13:49:43:  outbound IF index  = 4
Jul 26 13:49:43:  outbound IF sub-index = 399
Jul 26 13:49:43: DHCPD: Keeping state: Forwarding BOOTREPLY to
client 0008.7494.c173, on UNNUM-IF
```

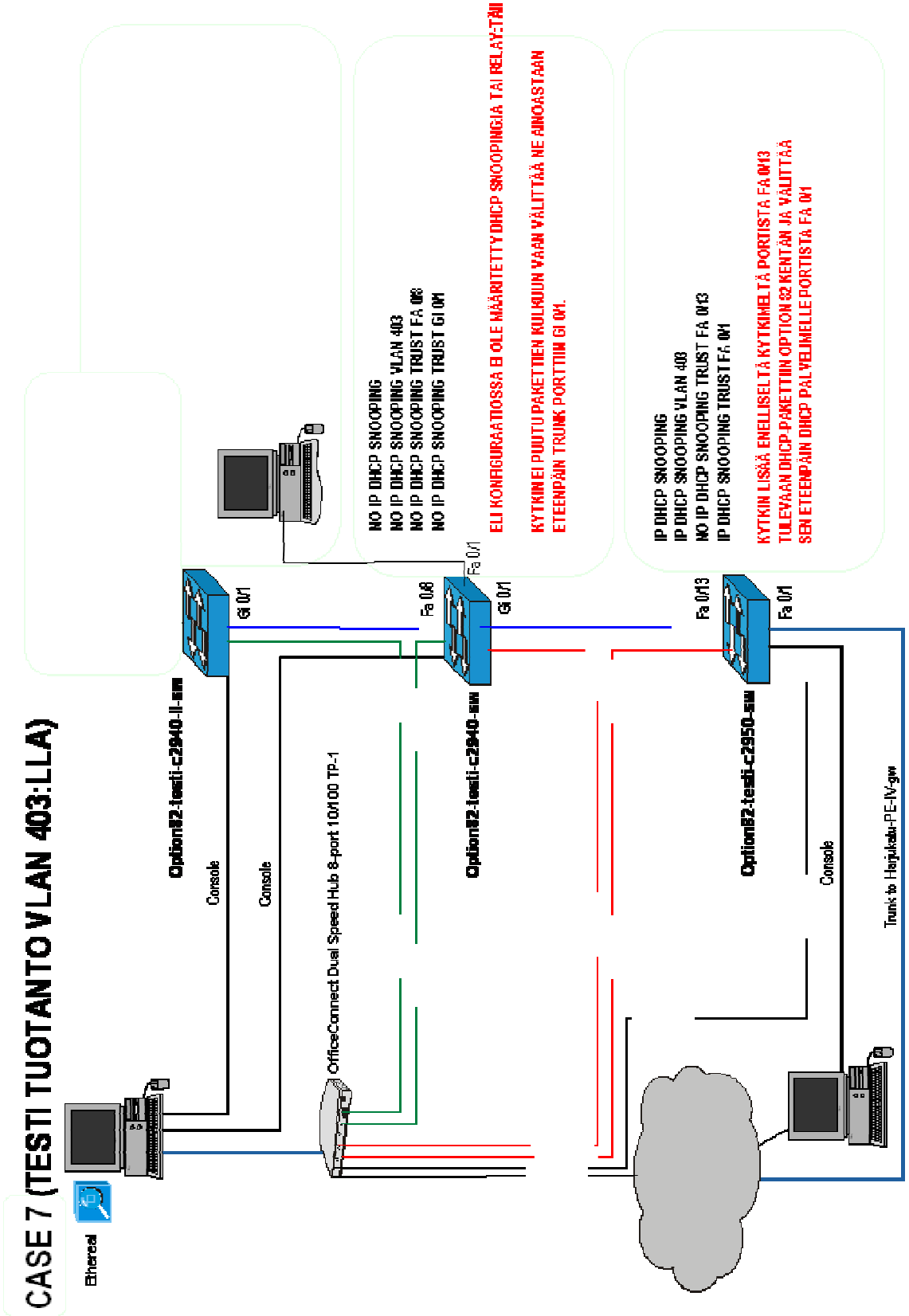
LIITE 13

KANNETTAVAN MAC- JA IP-OSOITE LISÄTÄÄN MYÖS REITITTIMEN DHCP BINDING TAULUUN:

Bindings from all pools not associated with VRF:

IP address	Client-ID/ Hardware address/ User name	Lease expiration	Type
81.175.164.3	00d0.591c.9118	Jul 26 2005 02:54 PM	Relay
81.175.164.9	fe02.2144.0035	Jul 26 2005 02:07 PM	Relay
81.175.164.243	fe04.1908.000f	Jul 26 2005 02:39 PM	Relay
81.175.164.245	fe00.2944.0035	Jul 26 2005 02:51 PM	Relay
81.175.164.246	fe01.1908.000f	Jul 26 2005 02:41 PM	Relay
81.175.164.249	fe03.1908.000f	Jul 26 2005 03:30 PM	Relay
81.175.165.242	0011.2fde.4db3	Jul 26 2005 01:55 PM	Relay
81.175.165.243	fe02.0108.000f	Jul 26 2005 02:48 PM	Relay
81.175.165.249	fe02.1908.000f	Jul 26 2005 02:47 PM	Relay
81.175.165.250	0008.7494.c173	Jul 26 2005 02:49 PM	Relay
81.175.165.252	fe02.4950.0035	Jul 26 2005 02:55 PM	Relay

LIITE 14


CASE 7 (TESTI TUOTANTO VLAN 403:LLA)
Ethereal
Option82-testi-c2940-II-sw
Console
Console
OfficeConnect Dual Speed Hub 8-port 10/100 TP-1
Option82-testi-c2940-sw
Option82-testi-c2950-sw
Console
Trunk to Harjukatu-PE-IV-gw
Gi 0/1
Fa 0/6
Fa 0/1
Gi 0/1
Fa 0/13
Fa 0/1
NO IP DHCP SNOOPING
NO IP DHCP SNOOPING VLAN 403
NO IP DHCP SNOOPING TRUST FA 0/6
NO IP DHCP SNOOPING TRUST Gi 0/1
ELI KONFIGURAATIOSSA EI OLE MÄÄRITETTY DHCP SNOOPINGIA TAI RELAY:TÄHI
KYTKIN EI PUUTU PAKETTIEN KULKUUN VAAN VÄLITTÄÄ NE AINOASTAAN ETEENPÄIN TRUNK PORTTIIN Gi 0/1.
IP DHCP SNOOPING
IP DHCP SNOOPING VLAN 408
NO IP DHCP SNOOPING TRUST FA 0/13
IP DHCP SNOOPING TRUST FA 0/1
KYTKIN LISÄÄ ENELLISELTÄ KYTKIMELTÄ PORTISTA FA 0/13 TULEVAAN DHCP-PAKETTIIN OPTION 82 KENTÄN JA VÄLITTÄÄ SEN ETEENPÄIN DHCP PALVELIMELLE PORTISTA FA 0/1

LIITE 14

Option82-testi-c2940-sw

EI DHCP SNOOPING TAI RELAY KONFISTA AINOASTAAN DEFAULT ASETUKSET.

```
Option82-testi-c2940-sw#sh ip dhcp snooping
Switch DHCP snooping is disabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Interface                Trusted    Rate limit (pps)
------------------------    -------    ----------------

Option82-testi-c2940-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress          IpAddress        Lease(sec)  Type     VLAN  Interface
------------------  ---------------  ----------  -------  ----  --------------------
```

****

Option82-testi-c2950-sw

```
ip dhcp snooping vlan 403
ip dhcp snooping
!
vlan 403
 name testia_varten
!
interface FastEthernet0/1
 switchport trunk allowed vlan 403
 switchport mode trunk
 speed 10
 duplex full
 ip dhcp snooping trust
!
!
interface FastEthernet0/13
 switchport trunk allowed vlan 403
 switchport mode trunk
!
```

```
*Mar  1 02:58:24: DHCP packet (count 36) on Fa0/13, VLAN 403
*Mar  1 02:58:24: DHCP: Sent to DHCP Snooping on Fa0/13, VLAN 403
*Mar  1 02:58:24: DHCP_SNOOPING: received new DHCP packet from
input interface (FastEthernet0/13)
*Mar  1 02:58:24: DHCP_SNOOPING: process new DHCP packet,
message type: DHCPDISCOVER
*Mar  1 02:58:24: DHCP_SNOOPING: add relay information option.
```

*Mar 1 02:58:24: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
*Mar 1 02:58:24: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x93 0x0 0xC 0x2 0x8 0x0 0x6 0x0 0x11 0x21 0x41 0x19 0x40
*Mar 1 02:58:24: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (403)
*Mar 1 02:58:24: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/1.
*Mar 1 02:58:25: DHCP packet (count 37) on Fa0/1, VLAN 403
*Mar 1 02:58:25: DHCP: Sent to DHCP Snooping on Fa0/1, VLAN 403
*Mar 1 02:58:25: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
*Mar 1 02:58:25: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER
*Mar 1 02:58:25: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/13.
*Mar 1 02:58:25: DHCP packet (count 38) on Fa0/13, VLAN 403
*Mar 1 02:58:25: DHCP: Sent to DHCP Snooping on Fa0/13, VLAN 403
*Mar 1 02:58:25: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/13)
*Mar 1 02:58:25: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST
*Mar 1 02:58:25: DHCP_SNOOPING: add relay information option.
*Mar 1 02:58:25: DHCP_SNOOPING_SW: Encoding opt82 in vlan-mod-port format
*Mar 1 02:58:25: DHCP_SNOOPING: binary dump of relay info option, length: 20 data:
0x52 0x12 0x1 0x6 0x0 0x4 0x1 0x93 0x0 0xC 0x2 0x8 0x0 0x6 0x0 0x11 0x21 0x41 0x19 0x40
*Mar 1 02:58:25: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is flooded to ingress VLAN: (403)
*Mar 1 02:58:25: DHCP_SNOOPING_SW: bridge packet send packet to port: FastEthernet0/1.
*Mar 1 02:58:25: DHCP packet (count 39) on Fa0/1, VLAN 403
*Mar 1 02:58:25: DHCP: Sent to DHCP Snooping on Fa0/1, VLAN 403
*Mar 1 02:58:25: DHCP_SNOOPING: received new DHCP packet from input interface (FastEthernet0/1)
*Mar 1 02:58:25: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK
*Mar 1 02:58:25: DHCP_SNOOPING: add binding on port FastEthernet0/13.
*Mar 1 02:58:25: DHCP_SNOOPING: added entry to table (index 207)

LIITE 14

*Mar 1 02:58:25: DHCP_SNOOPING: dump binding entry: Mac=00:08:74:94:C1:73 Ip=81.175.143.84 Lease=3600 Type=dynamic Vlan=403 If=FastEthernet0/13

*Mar 1 02:58:25: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/13.

Option82-testi-c2950-sw#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
403
Insertion of option 82 is enabled
Interface Trusted Rate limit (pps)
----------- ------- ----------
FastEthernet0/1 yes unlimited

Option82-testi-c2950-sw#sh ip dhcp snooping binding
Option 82 on untrusted port is not allowed
MacAddress IpAddress Lease(sec) Type VLAN Interface
----------- ---------- ---------- ------- ---- ----------
00:08:74:94:C1:73 81.175.143.84 2520 dynamic 403 FastEthernet0/13

****
edge-r2.lht.phnet.fi

ip dhcp relay information option
ip dhcp relay information policy keep
no ip dhcp relay information check
!
!
interface FastEthernet4/0.403
ip helper-address 172.20.0.11
ip dhcp relay information trusted
!

Jul 28 12:22:29: DHCPD: message is from trusted interface FastEthernet4/0.403
Jul 28 12:22:29: DHCPD: relay binding created for client 0100.0874.94c1.73.
Jul 28 12:22:29: DHCPD: Received DHCPDISCOVER on UNNUM-IF
Jul 28 12:22:29: DHCPD: setting giaddr to 81.175.140.1.
Jul 28 12:22:29: DHCPD: leaving relay information in tact.
Jul 28 12:22:29: DHCPD: BOOTREQUEST from 0100.0874.94c1.73 forwarded to 172.20.0.11.

LIITE 14

Jul 28 12:22:29: DHCPD: forwarding BOOTREPLY to client 0008.7494.c173.
Jul 28 12:22:29: DHCPD: Forwarding reply on un-numbered intf
Jul 28 12:22:29: DHCPD: Unnum: Received DHCPOFFER
Jul 28 12:22:29: DHCPD: Server Address = 172.20.0.11
Jul 28 12:22:29: DHCPD: Giaddr Address = 81.175.140.1
Jul 28 12:22:29: outbound IF index = 4
Jul 28 12:22:29: outbound IF sub-index = 403
Jul 28 12:22:29: DHCPD: unnum: Forwarding BOOTREPLY to client 0008.7494.c173.
Jul 28 12:22:29: DHCPD: message is from trusted interface FastEthernet4/0.403
Jul 28 12:22:29: DHCPD: Received DHCPREQUEST on UNNUM-IF
Jul 28 12:22:29: DHCPD: request_on_unnumif ():Real Server = 172.20.0.11
Jul 28 12:22:29: DHCPD: setting giaddr to 81.175.140.1.
Jul 28 12:22:29: DHCPD: leaving relay information in tact.
Jul 28 12:22:29: DHCPD: BOOTREQUEST from 0100.0874.94c1.73 forwarded to 172.20.0.11.
Jul 28 12:22:29: DHCPD: forwarding BOOTREPLY to client 0008.7494.c173.
Jul 28 12:22:29: DHCPD: Forwarding reply on un-numbered intf
Jul 28 12:22:29: DHCPD: Unnum: Received DHCPACK
Jul 28 12:22:29: DHCPD: lease time = 3600
Jul 28 12:22:29: DHCPD: Server ID saved in Binding = 172.20.0.11
Jul 28 12:22:29: DHCPD: Giaddr Address = 81.175.140.1
Jul 28 12:22:29: DHCPD: dhcpd_lookup_route: host = 81.175.143.84
Jul 28 12:22:29: DHCPD: dhcpd_lookup_route: index = 37
Jul 28 12:22:29: DHCPD: dhcpd_create_and_hash_route: host = 81.175.143.84
Jul 28 12:22:29: DHCPD: dhcpd_create_and_hash_route index = 37
Jul 28 12:22:29: DHCPD: dhcpd_add_route: lease = 3600
Jul 28 12:22:29: outbound IF index = 4
Jul 28 12:22:29: outbound IF sub-index = 403
Jul 28 12:22:29: DHCPD: unnum: Forwarding BOOTREPLY to client 0008.7494.c173.
Jul 28 12:22:29: DHCPD: removed relay binding