TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka

Tutkintotyö

Lari Kaasalainen

PIENI LÄHIVERKKO ZYXEL 660HW-61:LLÄ

Tampere 2006

Työn valvoja: Jorma Punju

Tietotekniikka
Tietoliikkennetekniikka
Kaasalainen, Lari
PIENI LÄHIVERKKO ZYXEL 660HW-61:LLÄ
Tutkintotyö 34sivua
Työn valvoja Yliopettaja, Punju Jorma
Marraskuu 2006
Hakusanat WLAN, Verkon konfigurointi

TIIVISTELMÄ

Tämän tutkintotyön tavoitteena oli perehtyä eri tiedonsiirtotekniikoihin, niin teoriassa, kuin käytännössäkin. Työssä käydään läpi lyhyesti ADSL, langaton lähiverkko, Ethernet-lähiverkko ja TCP/IP-protokolla.

Tutkintotyössä toteutettiin kotiin ja pienyritykseen toimiva ja tietoturvallinen lähiverkko, joka toimii langallisesti ja langattomasti. Työssä on käytetty ZYXEL 660HW-61, 802,11g Wireless ADSL2+ 4-Port Gateway modeemia, jonka avulla on käytännössä käyty läpi eri tekniikat ja perusteltu miksi mikin asetus on valittu.

Työssä perehdyttiin myös tietoturvaan, jotta verkko olisi mahdollisimman turvallinen käyttää. Myöskin verkon helppoon hallittavuuteen on kiinnitetty työtä tehdessä huomiota.

Computer System Engineering
Telecommunicatios Engineering
Kaasalainen, Lari
SMALL LOCAL NETWORK USING ZYXEL 660HW-61
Number of pages 34 pages
Thesis Supervisor Principal lecturer, Punju Jorma
November 2006
Keywords WLAN, Network configuration

ABSTRACT

The purpose of this study was to get acquainted with different techniques of data transfer both in theory and in practice. In this study ADSL, wireless local area network, Ethernet local area network and TCP/IP-protocol are examined in theory .

In this study also wired and wireless, data secure local area network for home and small enterprise is carried out. ZYXEL 660HW-61, 802,11g Wireless ADSL2+ 4-Port Gateway modem is used in this study to examine different techniques in practice and to state reasons why each of the settings have been chosen.

To make the network as safe as possible to use, data security is made familiar in this study. Also the easy controllability of network is paid attention to while producing this study.

ALKUSANAT

Tämä tutkintotyö on tehty huhtikuun 2006 ja Marraskuun 2006 välisenä aikana. Innostuksen tutkintotyöhöni sain työpaikan kautta, jossa joudun olemaan päivittäin tekemisissä käsittelemieni asioiden kanssa. Haluan kiittää työni valmistumisesta kaikkia, jotka ovat tukeneet minua työn tekemisessä ja saaneet minut kirjoittamaan tämän työn valmiiksi erilaisista vastoinkäymisistä huolimatta.

Tampereella 13.marraskuuta 2006

_____

Lari Kaasalainen

SISÄLLYSLUETTELO

LYHENNELUETTELO

LAN	Local area network
ADSL	Asymmetric Digital Subscriber line
MAC	Media Access Control
WLAN	Wireless Local Area Network
SSID	service set identifier
WEB	Wired Equivalent Privacy
WPA	Wireless Fidelity Protected Access
PSK	Pre Shared Key
TKIP	Temporal Key Integrity Protocol
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
NAT	network address translation
DHCP	Dynamic Host Configuration Protocol,
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol

DNS	Domain name system
WWW	World Wide Web
VPI	Virtual Path Identifier
VCI	Virtual Channel Identifier
WAN	Wide Area Network
LLC	Logical Link Control
VPN	Virtual Private Network
SUA	Single User Account

1 JOHDANTO

ADSL on yleisin teknologia, jolla nykyään tuodaan Internet-yhteys kiinteistöön. Yhteys tulee ensimmäiseksi ADSL-reitittimelle, jossa yhteys muutetaan lähiverkkoon sopivaksi, jolloin verkkokortilla varustettu tietokone ymmärtää saamansa tiedon. Valitsin työni aiheeksi ZYXEL 660HW-61, 802,11g Wireless ADSL2+ 4-Port Gateway reitittimen, koska sillä voin opetella ja käydä läpi eri tiedonsiirtotekniikoita.

Työssä käydään aluksi lävitse ADSL, WLAN ja Ethernet teoreettisesti ja teoriassa opittuja tietoja käytetään laitteen konfiguroimisessa ja oman lähiverkon rakentamisessa. Konfiguroinnissa asetukset tehdään käyttäen Internet-selainpohjaista käyttöliittymää ja käydään läpi ne asetukset, joita tarvitaan normaalissa käytössä ja suojauksessa.

Yhteiskunnan nopea verkottuminen asettaa tiedon turvaamiselle uuden haasteen. Langattomat verkot ovat yleistyneet nopeasti, monia töitä tehdään etätyönä ja tietoverkkoihin murtautumiset ovat lisääntyneet huomattavasti. Tällöin verkossa liikkuva data on aina salattava ja verkoista on tehtävä rakenteellisesti sellaisia, että niihin on vaikea murtautua.

2 ADSL

ADSL on modeemitekniikka, jolla on mahdollista siirtää 8 Mbit/s tavallista puhelinlinjaa käyttäen. ADSL:n nopeus perustuu korkeaan taajuusalueeseen, 23 000–1 100 000 Hz. ADSL:n ominaispiirre on sen epäsymmetrisyys tiedonsiirrossa. Tiedonsiirtonopeus on erilainen laskevaan suuntaan ja nousevaan suuntaan. Laskevaan suuntaan se on 8 Mbit/s ja nousevaan suuntaan 800 kbit/s. Tästä syystä ADSL soveltuu hyvin tavallisen Internetin käyttöön, jossa pääpaino on sisällön siirtämisellä kuluttajalle päin eli laskevalla kaistalla./2/

ADSL-tekniikkaa ei tehty alkujaan tiedonsiirtoteknologiana, vaan videopalvelujen siirtotekniikaksi. Ennen vuotta 1997 tehdyt pilottikokeilut keskittyivät tähän sovellukseen, jossa ADSL-teknologiaa käytettiin siirtämään digitaalisesti koodattu (MPEG2) videokanava videopalvelimelta tilaajalle. Siirto tehtiin suoraan ATM-protokollan päällä ilman minkäänlaista verkkokerrosta. Tämän palvelun hallintamekanismit vaihtelivat testistä toiseen ja pohjautuivat toisinaan valmistajien omiin protokolliin ja toisinaan IP-protokollaan. Yleinen pilottikokeiluja koskeva ongelma oli – olisiko tuon ajan teknologiaan pohjautuva videopalvelu kannattava ja lähtisivätkö asiakkaat mukaan palveluun, kun otetaan huomioon vaihtoehtoiset ratkaisut: kaapeli, suora satelliitti ja videovuokraamot. Vastaus tähän valitettavasti oli että ei. Tähän otetaan mukaan vielä se tosiasia, että korkealaatuinen video vaati 4-8 Mbps:n siirtonopeuden, mikä taas rajoittaa modeemien etäisyyksiä ja se puolestaan rajoittaa tilaajien määrää. Internetin räjähdysmäinen kasvu tarjosi ADSL-teknologialle uuden käyttökohteen. ADSL oli ihanteellinen teknologia entistä valveutuneempien kuluttajien vaatimien erittäin nopeiden yhteyksien luomiseen, kun alkuvaikeuksista oli selvitty./1, s18-19/

3 LANGATON LÄHIVERKKO

Langaton lähiverkko eli WLAN on lyhenne englanninkielisistä sanoista Wireless Local Area Network. Sanonta ”langaton ympäristö” on hieman harhaanjohtava, koska se viittaa verkkoon, jossa ei ole lainkaan kaapeleita. Useimmissa tapauksissa tämä ei ole totta. Useimmat langattomat verkot koostuvat tosiasiassa langattomista komponenteista, jotka kommunikoivat kaapeliverkon kanssa./ 3 /

Langaton verkko on järkevä keino tehdä lähiverkko kotiin tai toimistoon. Tekemällä verkko langattomaksi ei tarvitse vetää johtoja seinien läpi tai käyttää silmiinpistäviä johtolistoja tai -kouruja. Tehtäessä verkko langattomana saamme myös liikkuvuuden vapauden verkon kantoalueella. Nykyään käytetään paljon kannettavia tietokoneita, jolloin langaton verkko on järkevä ratkaisu, ja voimme käyttää Internet-yhteyttä, niin tukiaseman vieressä kuin pihalla aurinkoa ottaessamme.

Langattomien verkkojen alkuvaiheessa oli olemassa suljettuja protokollia ja eri verkko eri tarkoituksiin. 1990-luvun puolivälissä ne korvautuivat standardeilla, pääasiassa IEEE 802.11 -standardilla, jossa tiedonsiirtonopeus oli 2 Mbit/s. Myöhemmin tuli IEEE 802.11b -standardi tiedonsiirtonopeudeltaan 11 Mbit/s, ja se on vielä monessa paikassa käytössäkin. Nykyään käytetään pääasiassa IEEE 802.11g -standardia, jossa tiedonsiirtonopeutena on peräti 54 Mbit/s. Todellisuudessa langattoman verkon hyötynopeus on noin 10-30% ilmoitetusta nimellisnopeudesta. Käytännössä osa tiedonsiirtokapasiteetista käytetään aina datapakettien ohjailuun ja virheen korjaukseen. Siksi esim. tiedostoja langattomasti siirrettäessä ei koskaan päästä teoreettiseen maksiminopeuteen./ 4; 5 /

Langattoman verkon suojaus on täysin välttämätön toimenpide, jos halutaan, että verkkoa eivät pääse käyttämään ei-toivotut osapuolet. Verkkokaapeleilla toteutetussa verkossa ei kukaan pääse liittymään verkkoon luvatta, ellei saa johtoa kiinni verkon laitteisiin, mikä taas vaatii murtautumisen rakennukseen sisälle,

missä verkko on. Langattomassa verkossa tieto liikkuu ilmateitse, eivätkä seinät pahasti estä radioaaltojen kulkua. Verkon ollessa suojaamaton voi kuka tahansa verkon kantoalueella oleva henkilö liittyä verkkoon ja käyttää toisen Internet-liittymää ja tarkastella, mitä tiedostaja kyseisessä lähiverkossa on jaossa. Suojaus kannattaa aloittaa muuttamalla tukiaseman salasana, jolloin luvattomat käyttäjät eivät pääse kirjautumaan tukiasemaan eivätkä muuttamaan sen asetuksia. Langattoman verkon nimi eli SSID (Service Set Identifier) on suositeltavaa panna näkymättömäksi, jolloin Windows-käyttöjärjestelmää käyttävät koneet eivät näe kyseistä verkkoa, ellei käytetä erillistä verkkojen etsimiseen tarkoitettua ohjelmaa. SSID:n piilottaminen on hyvä ratkaisu, ellei verkkoon liitetä usein uusia koneita. Seuraavana toimenpiteenä on hyvä panna MAC-osoitteiden suodatus päälle, jolloin verkkoon pääsevät liittymään vain ne laitteet, joiden MAC-osoite on sallittujen listalla. Tämäkään toimenpide ei ole riittävä, koska löytyy paljon ohjelmia, joilla pystyy muokkaamaan laitteen MAC-osoitetta ja näin ollen on mahdollista liittyä verkkoon luvatta, jos saa selville sallittujen listalla olevan MAC-osoitteen. MAC-osoitteiden suodatus on myös hyvä toimenpide silloin, kun verkkoon ei usein liitetä uusia koneita. Verkon nimen piilottamisella ja MAC-osoitteiden suodatuksella pystytään vain vaikeuttaan verkkoon liittymistä. Myös itse liikenne on vielä täysin suojaamatonta, jolloin on suositeltavaa käyttää liikenteen suojaamiseenkin jotain salausta. Nykyään yleisimpinä vaihtoehtoina ovat WEP (Wired Equivalent Privacy) ja WPA (Wireless Fidelity Protected Access). WEP-salaus on vanhin ja heikoin salausmenetelmä WLAN-verkoissa, mutta sekin on paljon parempi kuin täysin suojaamaton verkko. WEP-salaus on suhteellisen helppo murtaa tutkimalla riittävän monta data-pakettia verkosta. WEP-salauksessa, kuten myös WPA-salauksessa, käytetään RSA Securityn RC4-algoritmia datapakettien salaamiseen, jolloin ulkopuolinen ei saa selvää, mitä tietoa verkossa liikkuu, ellei saa salausta murrettua. WEP-salauksen pohjalta kehitetty WPA-salaus on kuitenkin WEP-salausta turvallisempi. WPA-salaus on paranneltu versio 128-bittisestä WEP-salauksesta. WPA-salauksessa datapaketit salataan vaihtuvalla salausavaimella, joten salausta ei voi murtaa WEP-salauksen tapaan vain datapaketteja tutkimalla. WPA on välivaiheen tietoturvatekniikka, joka kehitettiin WEP-salauksen

ongelmien paljastuttua. WPA sisältää tulevan 802.11i-tietoturvastandardin ominaisuuksia ja se on yhteensopiva niin nykyisten kuin tulevienkin laitteiden kanssa. WEP-salauksen heikot aloitusvektorit on korjattu ja lisäksi salausavainta vaihdetaan automaattisesti 10 000 paketin välein. WPA:ssa on käytössä TKIP-salaus (Temporal Key Integrity Protocol) eli WEP-avaimen hajautus mahdollistaa jaetun salaisen avaimen suojaamisen hyökkäyksiltä. TKIP parantaa langattoman verkon turvallisuutta huomattavasti ottamalla käyttöön pakettikohtaiset salausavaimet. TKIP salaa liikenteen RC4-algoritmilla, mutta salausavaimen pituus on 128 bittiä. WPA:n heikkoutena pidetään sen alttiutta palvelunestohyökkäyksille. Haavoittuvuus johtuu WPA:n tavasta selvitä verkkohyökkäyksistä: WPA sulkee koko verkon minuutiksi havaittuaan hyökkäyksen, jolloin myös verkon lailliset käyttäjät jäävät katkon aikana ilman palvelua. Kaikki vanhahkot laitteet eivät välttämättä tue WPA-salausta, jolloin tulee käyttää WEP-salausta tai päivittää laitteen ajurit, jolloin useimpiin vanhahkoihinkin laitteisiin saadaan WPA-tuki ja näin ollen saadaan yhteydestä entistä turvallisempi./ 5; 6; 7; 8; 9 /

4 ETHERNET-LÄHIVERKKO

Tietoliikenteessä maantieteellisesti rajatun pienen alueen sisäistä tietoliikennettä sanotaan lähiverkoksi, josta voidaan käyttää myös nimitystä LAN (Local Area Network). Tavallisesti lähiverkko on yhden organisaation hallinnassa, mutta verkko voi olla myös ulkopuolisen tahon vuokraama tai ylläpitämä. Lähiverkko koostuu verkossa olevista erillisistä työasemista, verkkolaitteista, palvelimista ja kaapeloinneista /2, s. 4/

Ethernet-verkossa tiedon lähetys perustuu yksinkertaiseen CSMA/CD-menettelyyn (Sense Multiple Access/Collision Detection). CSMA/CD on tietoliikenteen siirtotien varausmenetelmä, jolla useat lähettävät tietokoneet jakavat samaa siirtotietä. Siis vain yksi kone saa kerrallaan lähettää tietoa verkkoon. Kuitenkin voi käydä niin, että kaksi konetta lähettääkin tietoa samaan aikaan, jolloin paketit törmäävät toisiinsa. Tällöin törmäyksen havainnut laite vahvistaa törmäyksen, ja

törmäyksen osapuolet arpovat itselleen uuden lähetysajan, jolloin törmäystä tuskin sattuu uudestaan./2, s95; 11/

4.1 Historia

Ensimmäistä Ethernet verkkoa – jota nimitettiin Alto ALOHANetiksi – alettiin kehittää Xeroxin Palo Alton tutkimuskeskuksessa vuonna 1972. Alun perin verkon siirtonopeutena käytettiin 2,94 Mb/s. Nimi Ethernet tuli käyttöön toukokuussa 1973, ja verkon nopeus kasvoi lopulta arvoon 10 Mbit/s. /11/

Laajemmin Ethernet-verkkoa ruvettiin käyttämään 1980-luvulla. Aluksi oli käytössä halkaisijaltaan yli 10 mm. olevaan koaksiaalikaapeliin pohjautuva Ethernet-versio, jota kutsuttiin ”paksu”-Ethernetiksi. Myöhemmin 1980-luvun puolivälissä tuli ohuempaa ja halvempaa kaapelia käyttävä versio, jota kutsuttiin ”ohut”-Ethernetiksi. Seuraavaksi saatiin markkinoille parikaapelointi, jota kutsutaan 10Base T:ksi ja se on nimensä mukaisesti 10 Mbit/s:n tiedonsiirtoon pystyvä. 1990-luvun puolivälissä tuli 100 Mbit/s:n nopeuteen pystyvä fastethernet, josta 100BaseTX on jäänyt käyttöön. Siirtonopeuden kasvu saatiin aikaan tekemällä entistä laadukkaampia verkkolaitteita ja kaapeleita ja ennen kaikkea muuttamalla verkon rakenne väylämäisestä tähtimäiseksi. 1990-luvun loppupuolella tuli Gigabitethernet, jolla saavutettiin jo 1 Gbit/s:n siirtonopeus. Nopeuden nousu saavutettiin ottamalla käyttöön entistä pidemmät kehykset, tehostamalla käytössä olevaa koodausta, pienentämällä CSMA/CD-algoritmille sallitun alueen kokoa, lisäämällä PAM-modulaatioon kaksi uutta jännitetasoa ja siirtymällä half-duplexiin./ 11; 12/

4.2 Silta

Silta (bridge, kytkin,switch) toimii OSI-mallin tasolla kaksi. Silta yhdistää toisiinsa verkkoja välittämällä johonkin porttiin tulevan kehyksen vain siihen porttiin, josta löytyy kehyksen kohdeosoite. Silta tarkkailee myös kehyksen muotoa eli oikeellisuutta ja sisältöä, ja näistä ensisijaisesti kohdeosoitetta. Kehyksen

välityksessä sillä on kolme vaihtoehtoa: välitys, tulva ja suodatus. Paketin saapuessa kytkimelle kytkin tallentaa saapuvan paketin lähettäjän MAC-osoitteen ja portin kytkimen osoitetauluun. Tämän jälkeen kytkin vertaa paketissa olevaa vastaanottajan MAC-osoitetta osoitetauluun ja lähettää paketin eteenpäin oikeaan porttiin. Jos vastaanottajan osoitetta ei löydy taulusta, tai kyseessä on broadcast- tai multicast-paketti, kytkin lähettää paketin kaikkiin portteihin. Jos vastaanottajan portti on sama kuin lähettäjän portti, paketti hävitetään. Porteissa voidaan käyttää erilaisia medioita, kuten parikaapelia tai valokuitua./2, s108-110; 13,s58/

4.3 Reititin

Reititin (router) toimii OSI-tasolla kolme. Reititin on tietoverkkoon liitetty laite, joka välittää tietoliikennepaketteja kohti vastaanottajaa prosessissa, josta käytetään nimeä reititys. Reititin yhdistää verkkoja toisiinsa välittämällä johonkin porttiin tulevan ip-datagrammin, siihen porttiin, josta kohdeosoite löytyy. Helpommin selitettynä reititin toimii tienhaarana kahden eri verkon välillä ja ohjaa paketin oikean verkon suuntaan. Reititin eroaa merkittävästi kytkimestä, joka yhdistää tietokoneet paikalliseen aliverkkoon. Jos kytkintä ajattelee tienä, joka yhdistää kaikki kaupungin kodit, niin reititin on moottoritie, joka yhdistää kaupungit toisiinsa./2, s112; 13/

5 TCP/IP

TCP/IP *(*Transmission Control Protocol / Internet Protocol*)* on usean tietoverkkoprotokollan yhdistelmä, jota käytetään Internet-liikennöinnissä. IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa. Sen päällä voidaan ajaa useita muita verkko- tai kuljetuskerroksen protokollia, joista TCP-protokolla on yleisin. Se vastaa kahden päätelaitteen välisestä tiedonsiirtoyhteydestä, pakettien järjestämisestä ja hukkuneiden pakettien uudelleen lähetyksestä. Vaikka TCP/IP-protokollaperheeseen kuuluu monia muitakin protokollia, pääosa liikennöinnistä

tapahtuu TCP-yhteyksinä IP-protokollien päällä. Tämän takia protokollaperhe yleensä tunnetaan nimellä TCP/IP. / 12 /

5.1 Perusprotokollat

TCP/IP koostuu kahdesta protokollasta: TCP:stä ja IP:stä. Molemmat on määritelty ja kehitetty lukuisten Request For Comments -julkaisuiden kautta (RFC). Kummallakin protokollalla on omat tietyt tehtävänsä, mutta ne toimivat yhdessä muodostaakseen kahden tietokoneen välisen verkkoyhteyden. Nämä kaksi protokollaa muodostavat pohjan Internetin kautta tapahtuvalle tietoliikenteelle. Lisäksi on kaksi muutakin protokollaa, UDP (User Datagram Protocol) ja ICMP (Internet Control Message Protocol), jotka ovat tärkeitä, erityisesti vikojen selvittämisen- ja hallinnollisesta näkökulmasta. /12/

5.2 IP

IP-protokolla tarjoaa yhteydettömän ja kuittaamattoman verkkopalvelun. Se vastaa datapakettien siirtämisestä isäntäkoneelta toiselle. IP ei omaa mekanismeja, joiden avulla se voisi varmistaa paketin saapumisen kohteelle, tästä termi kuittaamaton palvelu. IP-protokollaa ei myöskään kiinnosta paketin Internetissä kulkema polku. Lisäksi IP ei takaa sitä, että paketit saapuisivat vastaanottajalle lähetysjärjestyksessä, mistä puolestaan seuraa termi yhteydetön. IP kuitenkin suorittaa tiettyjä toimintoja. Esimerkkeinä voidaan mainita datapakettien fragmentointi pienemmiksi osiksi ja niiden uudelleen kokoaminen, jolloin paketteja kyetään lähettämään erityyppisten verkkojen ja laitteiden läpi. IP-paketin otsakkeelle lasketaan tarkistussumma, mutta tämä protokolla ei suojaa data-osaa. IP-paketit toimitetaan perille IP-osoitteiden perusteella. IP-osoite on tavallisesti numero, kuten 192.68.11.1 (IPv4) tai 2002:a00::260:1dff:fe22:5a85/64 (IPv6). Selväkielisten osoitteiden muuttamisesta IP-osoitteiksi vastaa DNS-järjestelmä. /12; 15/

5.2.1 IP-osoitteet ja luokat(IPv4)

IP-osoite koostuu neljästä informaatiotavusta eli 32 peräkkäisestä bitistä. Siinä missä MAC-osoitteita ilmaistaan yleensä heksadesimaalimuodossa, IP-osoitteet kirjoitetaan yleensä pisteellisessä desimaalimuodossa. Jokainen tavu muunnetaan siis desimaalimuotoon ja nämä neljä osoitetavua erotetaan toisistaan pistein. Taulukko 1. näyttää 32-bittisen osoitteen 11000000 10101000 00001010 00000001 desimaali- ja binääriarvojen suhteet.

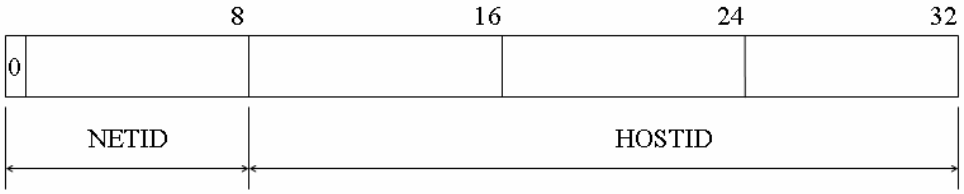
Taulukko 1. Desimaalimuodossa esitetyt IP-osoitteet

Desimaaliarvo	**Binääriarvo**
192	11000000
168	10101000
10	00001010
1	00000001

Kuten voidaan nähdä, on huomattavasti helpompaa kirjoittaa osoite muotoa 192.168.10.1 kuin käyttää sen binäärivastinetta. Toisena esimerkkinä IP-osoite 10.10.10.1 on binäärilukuna ilmoitettuna 00001010 00001010 00001010 00000001. Yksi IP-osoitteen osa yksilöi verkon (net id) ja toinen osa tietokoneen (host id). Kysymyksen, mikä osa tarkoittaa mitäkin, tulisikin olla helppo, mutta itse asiassa se riippuu tilanteesta. IP-osoitteet on jaettu viiteen luokkaan: A-, B-, C-, D- ja E-luokkaan. Jokainen luokka käyttää IP-osoitteesta eri bittijoukkoa verkko-osoitteen ilmaisemiseen. Koska osoitteiston bittien kokonaislukumäärä on aina vakio (32), tämä antaa ymmärtää, että osa luokista kykenee yksilöimään useampia verkkoja kuin toiset ja toisilla on kyky yksilöidä useampia työasemia./12; 15/

A-luokka

Mahdollisten A-luokan osoitteiden arvoalue alkaa sellaisesta binääriluvusta, jonka kaikki 32 bittiä ovat nollia, ja päättyy sellaiseen arvoon, jonka ensimmäinen bitti on nolla ja kaikki muut ovat ykkösiä. Jos nämä tavut muunnetaan desimaalimuotoon, havaitaan, että pisteellisessä desimaalimuodossa A-luokan osoitteet sijoittuvat välille 0.0.0.0–127.255.255.255. Luokan A verkko-osoitteessa on kahdeksan verkkotunnuksen bittiä ja 24 isäntäkoneen tunnuksen bittiä (kuva 1). Näin ollen luokan A verkossa voi olla noin 2^{24} eli 167777216 tietokonetta. Luokan A verkossa osoitteen vasemmanpuoleinen bitti on aina nolla, mutta muut bitit voivat sisältää kumman tahansa arvoista nolla tai yksi. Osoite 0.0.0.0 on varattu laitteiden oletusosoitteeksi ennen osoitteen oikeaan arvoon muuttamista. Osoite mahdollistaa koneen käynnistymisen. A-luokan harmaat IP-osoitesarjat ovat välillä 10.0.0.0–10.255.255.255. Nämä sarjat eivät siis ole julkisessa jakelussa, vaan niitä voi käyttää Intranet-osoitteina./12; 13, s77; 15/

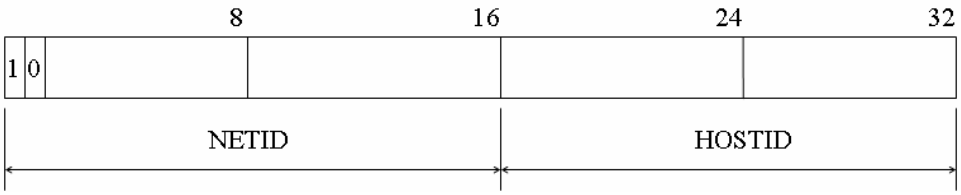


Kuva 1. A-luokan osoitteet

B-luokka

B-luokan osoitteissa kahden ensimmäisen bitin tulee olla muodossa 10 (kuva 2). Tämä merkitsee sitä, että binäärimuodossa esitetyn B-luokan osoitteen numeroalue alkaa sellaisesta luvusta, jonka ensimmäinen numero on 1, jota seuraa 31 nollaa, ja päättyy sellaiseen lukuun, joka alkaa numeroilla 1 ja 0, joita seuraa 30 ykköstä. Desimaalimuodossa B-luokan osoitteen minimi- ja maksimiarvot ovat 128.0.0.0–191.255.255.255. Tässä luokassa voi olla korkeintaan 16384 mahdollista verkko-osoitetta ja jokaisessa B-luokan verkossa voi olla 2^{16} eli 65536 yksittäistä

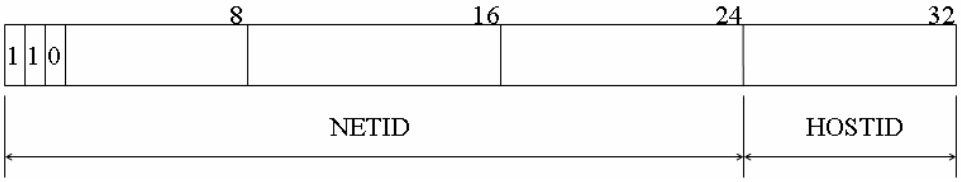
tietokonetta. B-luokan harmaat sarjat sijoittuvat välille 172.16.0.0–172.31.255.255. /12; 13, s78; 15/



Kuva 2. B-luokan osoitteet

C-luokka

C-luokan verkon osoitekentässä on 24 verkkotunnuksen ja kahdeksan isäntäkoneen tunnuksen bittiä (kuva 3). Luokan C verkossa vasemmanpuoleiset kolme bittiä ovat aina arvoltaan 110, mutta loput 29 bittiä voivat sisältää joko nollan tai ykkösen. C-luokan verkkoja voi olla korkeintaan 2097152 kappaletta ja jokaisessa niistä voi olla korkeintaan 256 isäntäkonetta. Tämä luokka käsittää huomattavan vähän isäntäkoneosoitteita, mutta mahdollisia verkkoja on valtavasti. C-luokan harmaat sarjat sijoittuvat välille 192.168.0.0–192.168.255.255. /12; 13, s 79; 15/

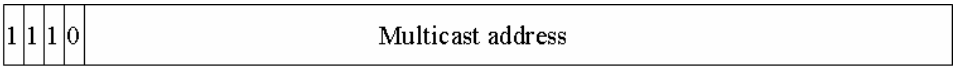


Kuva 3. C-luokan osoitteet

D-luokka

Luokan D IP-osoitteita ei anneta tietokoneille, kuten luokkien A, B ja C osoitteita. Tavallisesti IP-protokolla voi lähettää sanoman tiettyyn osoitteeseen tai tehdä yleislähetyksen. Neljä vasemmanpuoleista bittiä D-luokan verkko-osoitteessa ovat aina 1110 (kuva 4), mikä vastaa osoitteissa lukuja 224.0.0.0–239.255.255.255. Luokan D osoitteita käytetään yhteislähetyksiin. Yhteislähetys (multicast)

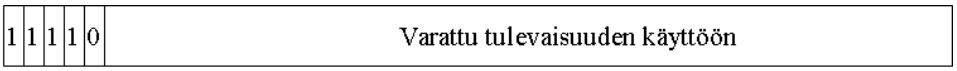
tarkoittaa, että sanoma lähetetään kerralla verkon tietokoneiden osajoukolle./12; 13, s80; 15/



Kuva 4. D-luokka

E-luokka

E-luokan osoitteet on tarkoitettu kokeiluun. Niitä ei tavallisesti käytetä verkoissa. Viisi vasemmanpuoleista bittiä E-luokan verkko-osoitteessa ovat aina 11110 (kuva 5), mikä vastaa osoitteissa lukuja 240.0.0.0–255.255.255.255. /13, 80; 15/



Kuva 5. E-luokka

5.2.2 IPv6

IPv6 on nykyisen IP-protokollan (IPv4) seuraajaksi kehitetty protokolla. IPv6 tunnettiin varhaisessa kehitysvaiheessaan myös nimellä IPng eli *IP next* generation. Sen tärkein ero IPv4:ään on osoitteen pituus ja osoiteavaruuden laajuus. IPv6:ssa käytetään 128-bittisiä osoitteita, eli IPv6:n osoitteita on 2^{128} kpl, joten niitä on monta miljardia jokaiselle maapallon neliömetrille. IPv4:ssä osoitteita on yhteensä vain hieman yli neljä miljardia. IP-numeroita ei riitä siis edes kaikille maapallon ihmisille, saati sitten jos ihmisillä olisi useampi IP-numero käytössä. Tällainen tilanne voi tulla eteen silloin, kun TV-laitteisiin, radioihin, autoihin tai puhelimiin tulevat omat IP-numerot. Myös osoitteen esitysmuoto on uusi verrattuna IPv4:ään. Ne kirjoitetaan kahdeksaan neljän heksatavun ryhmään, esim. 8000:0000:0000:0000:0123:4567:89AB:CDEF osoitteiden sisällä on paljon nollia, näin ollen voidaan osoitetta lyhentää siten, että etunollat voidaan jättää pois. Toiseksi yksi tai useampi 16 nollan ryhmä voidaan korvata kaksoispisteillä. Näin

yllä olevasta osoitteesta tulisi 8000::123:4567:89AB:CDEF. Vanhat IPv4-osoitteet voidaan kirjoittaa kuten ennenkin, mutta eteen lisätään kaksi kaksoispistettä, esim: ::192.168.1.1. /16/

5.3 TCP

TCP käyttää IP-protokollaa tarjoamaan luotettavan yhteyspalvelun kahden Internetissä olevan isäntäkoneen välille. Siinä missä IP vain lähettää paketit matkaan välittämättä niiden kohtalosta, TCP tarjoaa mekanismit, jotka varmistavat pakettien onnistuneen vastaanottamisen ja sen, että ne voidaan koota takaisin oikeaan järjestykseen laitteella. Varsinaiseen dataan kohdistetut tarkistussummat muodostetaan TCP-protokollan kautta. TCP omaa myös mekanismit, jotka säännöstelevät datavuota, jotta vältetään ruuhkautumisen aiheuttamat ongelmat. TCP pyrkii hyödyntämään verkkoa mahdollisimman tehokkaasti yrittämällä luoda paketteja, jotka sisältävät mahdollisimman paljon tietoa.

5.4 DHCP

DHCP (Dynamic Host Configuration Protocol) on verkkoprotokolla, jonka yleisin tehtävä on jakaa IP-osoitteita uusille lähiverkkoon kytkeytyville laitteille. Ylläpitäjä antaa tietyn IP-osoiteavaruuden, jolloin jokainen laite pyytää käynnistyksen yhteydessä DHCP-palvelimelta oman IP-osoitteensa. Annettu osoite on voimassa ennalta määrätyn ajan. Menettely yksinkertaistaa asiakaskoneiden asetuksien hallintaa huomattavasti. DHCP-palvelin voi jakaa asiakkaille myös muita asetuksia, kuten oletusyhdyskäytävän ja nimipalvelimen IP-osoitteen. Käytännössä DHCP-palvelin voi jakaa lähes mitä tahansa asetuksia. DHCP-palvelimen käytöstä lähiverkossa on sekin hyöty, että pystytään varmistamaan se, että tietyllä laitteella on aina sama IP-osoite, mikä puolestaan helpottaa verkon hallintaa. /14/

5.5 NAT

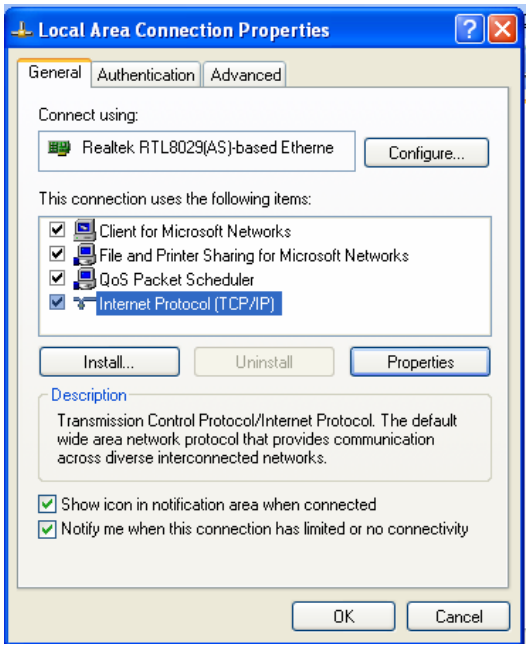
NAT (network address translation) eli osoitteenmuunnos on Internet-tekniikka, jossa julkisesti liikennöityjä IP-osoitteita piilotetaan tai säästetään. Useimmiten osoitteenmuunnosta käytetään, kun Internet-yhteydellä ei ole kuin yksi IP-osoite, mutta useamman koneen tulisi päästä Internetiin. Kaikessa Internetiin lähetetyssä liikenteessä pitää olla julkinen, uniikki IP-osoite, jolloin tässä tapauksessa usean koneen pitää jakaa yksi osoite. Osoitteenmuunnos lisää myös lähiverkossa olevien koneiden tietoturvaa, kun yksittäinen kone ei näy lainkaan ulkomaailmaan. Ainoa asia joka näkyy ulkomaailmaan on reititin tai palomuuri sen mukaan kummalla osoitteenmuunnos on suoritettu. Osoitteenmuutos tuo myös ongelmia, sillä monesti käytettäessä kaksisuuntaisia palveluja monet niistä vaikuttavat toimivan vain toiseen suuntaan, ja Internetistä takaisinpäin kulkeva liikenne jää usein tulematta. Tämän vuoksi NAT-laitteille voidaan määritellä avoimia yhteyksiä, jolloin laitteet pitävät niistä listaa. Yhteys poistetaan listasta, kun se suljetaan./12; 14/

5.6 DNS

Numeerinen IP-osoite on käyttäjän kannalta parempi kuin verkkolaitteen tehtaalla saama fyysinen osoite, mutta IP-osoite on suunniteltu enemmän tietokoneita kuin ihmisiä varten. Ihmisen saattaa olla vaikeaa muistaa, oliko tietokoneen osoite 111.121.131.146 vai 111.121.131.156. Sen vuoksi TCP/IP:hen on tehty vaihtoehtoinen tapa ilmoittaa osoitteet entistä ihmisystävällisemmällä tavalla. Kyseessä on toimialueen nimipalvelu DNS eli Doman Name Service. Nimipalvelimiksi kutsuttavat tietokoneet sisältävät tätä varten taulukoita, joista selviää toimialuenimeä vastaava IP-osoite ja päinvastoin. Sähköpostin ja World Wide Webin yhteydessä käytettävät osoitteet ovat DNS-nimiä, esimerkiksi www.microsoft.com, www.tappara.fi ja idir.net. TCP/IP:n nimipalvelujärjestelmä sisältää hierarkian nimipalvelimista, joissa toimialuenimi ja IP-osoite muutetaan toisikseen nimipalveluun rekisteröityneille tietokoneille. Tästä seuraa, että tavallisen käyttäjän tarvitsee harvoin kirjoittaa IP-osoitetta./12; 14; 15/

6 KONFIGUROINTI

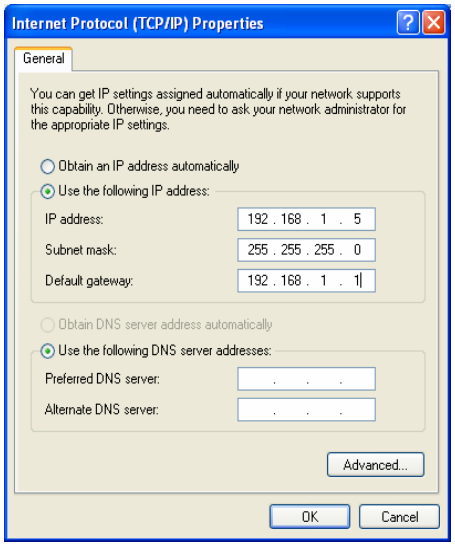
Otettaessa Zyxel 660HW-61 käyttöön kannattaa ensimmäiseksi resetoida laite, jolloin oletusasetukset tulevat varmasti modeemiin. Resetointi tapahtuu painamalla jollakin kapeakärkisellä esineellä, kuten esimerkiksi kynällä, 7 sekunnin ajan reset-painiketta, joka löytyy laitteen takaa. Modeemissa tulee olla virta kytkettynä päälle, ennen kuin resetointia voi tehdä. Aloitettaessa modeemin asetusten kuntoon laittoa tulee Ethernet-kaapelin olla kytkettynä modeemiin ja tietokoneen verkkokorttiin. Modeemi on oletuksena yleensä reitittävässä muodossa, jolloin kirjautuminen onnistuu kirjoittamalla selaimeen osoitteeksi 192.68.1.1. Mikäli modeemi menee resetoinnin jälkeen siltaavaan muotoon, pitää tietokoneelle määrittää dynaaminen IP-osoite: **start->settings->network connections->local area connection**. Seuraavaksi painetaan properties-painiketta, jolloin aukeaa kuvan 6 kaltainen näkymä.



Kuva 6. Verkkoyhteyden hallinta

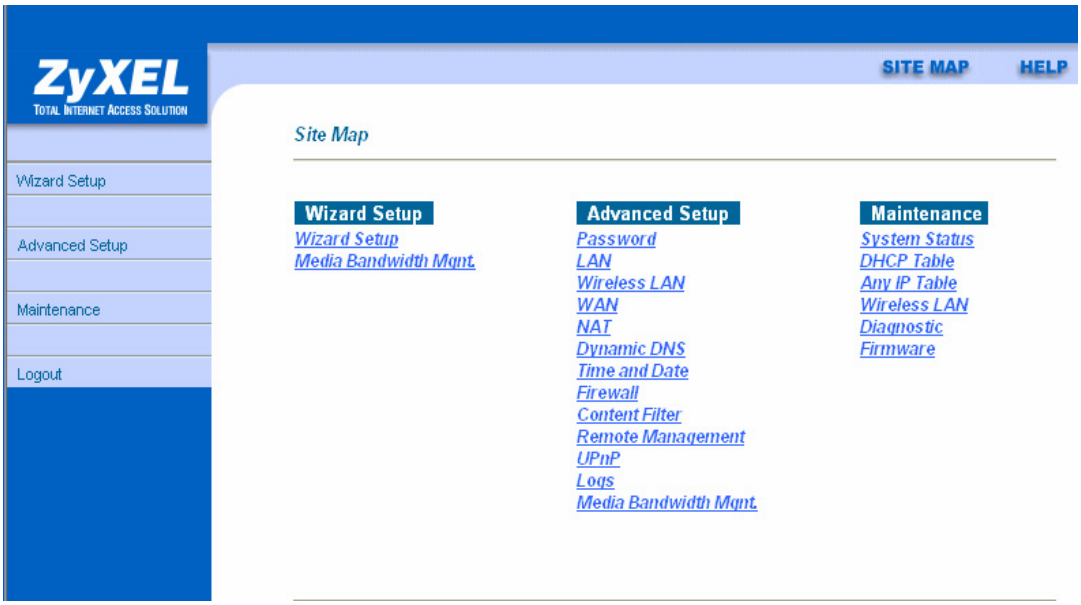
Valitaan **Internet Protocol (TCP/IP)** ja painetaan **properties**-painiketta. Nyt tulee näkyviin kuvan 7 näkymä, johon pitää määrittää käsin koneen IP:ksi 192.168.1.5, subnet maskiksi 255.255.255.0 ja gatewayksi 192.168.1.1 samanlaisesti kuin

kuvassa 7 on tehty. Nyt kone on määritetty kuuluvaksi samaan IP-alueeseen kuin modeemi ja kirjautuminen modeemiin on mahdollista.



Kuva 7. IP:n asentaminen koneelle.

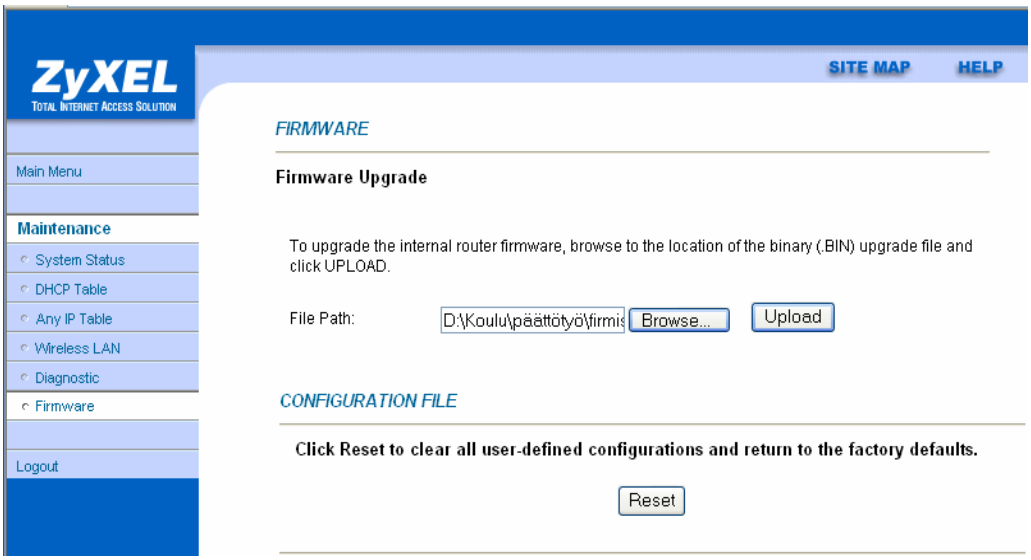
Kirjautuminen modeemin tapahtuu avaamalla Internet-selain ja kirjoittamalla sen osoiteriville 192.168.1.1. Ensimmäiseksi modeemi kysyy salasanaa, joka on oletuksena **1234**. Tämän jälkeen laite kysyy uutta salasanaa, joka on hyvä vaihtaa heti uuteen. Tällöin ulkopuolisten kirjautuminen modeemiin vaiketuu, vielä kun modeemissa on oletusasetuksissa langatonverkko päällä. Sisäänkirjautumisen onnistuttua tulee näkyviin web-hallinnan pääikkuna (kuva 8), josta voidaan valita mitä asetuksia halutaan muuttaa.



Kuva 8. Web hallinnan pääikkuna.

6.1 Firmwaren päivitys

Aluksi on hyvä päivittää modeemin firmware eli ohjelmisto. Uusimmassa firmwaressa on korjattuna erilaiset ohjelmistovirheet, jotka modeemista on löydetty. Samalla voi saada modeemiin uusia ominaisuuksia, jotka ovat tulleet ohjelmistopäivityksen myötä. Joissakin vanhemmissa versioissa ei esimerkiksi toimi langattoman lähiverkon WPA-salaus eikä myöskään WEB-hallinta. Uusimman firmwaren voi ladata Zyxelin kotisivuilta osoitteesta www.zyxel.fi. Uusin julkaistu firmwaren versio on 11. Firmwaren päivittäminen tapahtuu valitsemalla pääikkunasta (kuva. 8) firmware-linkki, josta aukeaa kuvan 9 näkymä. Päivitys tapahtuu valitsemalla *Browse*-painike ja hakemalla koneelta uusin firmwaren versio, joka on ladattu koneelle. Tiedoston valitsemisen jälkeen painetaan *Upload*-painiketta, jolloin modeemi alkaa päivittää firmwarea. Tämä toiminto kestää muutaman minuutin, ja sen valmistuttua modeemi siirtyy kirjautumiseen ja kysyy salasanaa.

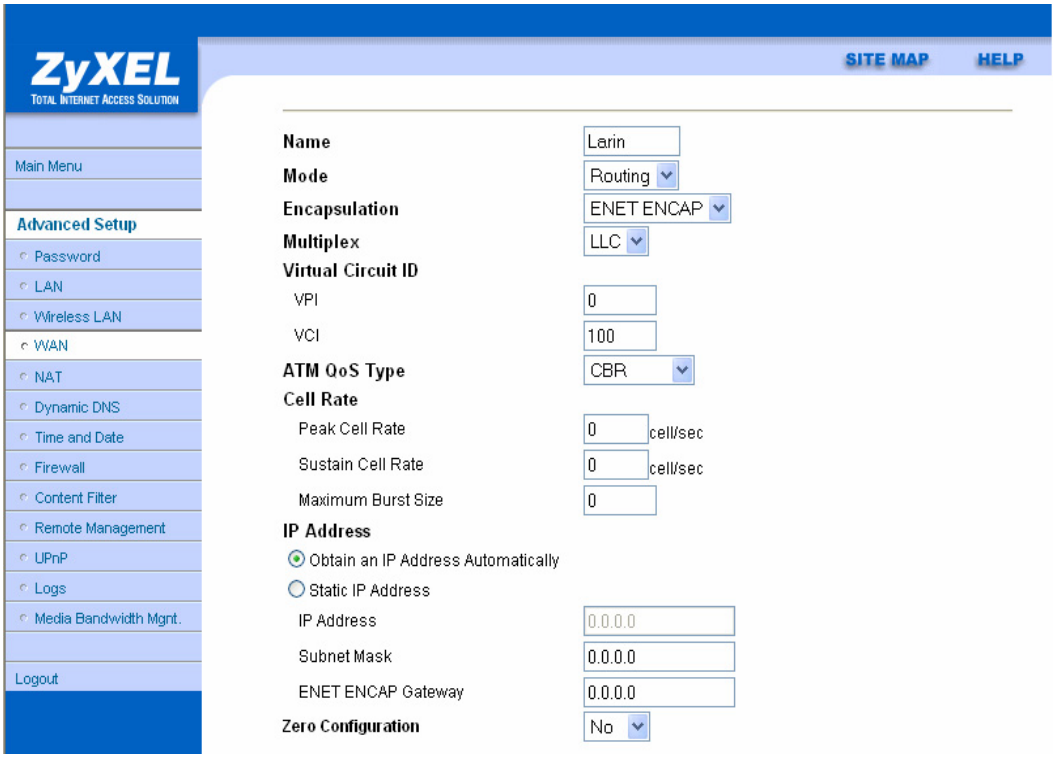


Kuva 9. Firmwaren päivitys.

6.2 WAN

WAN (Wide Area Network) eli laajaverkon asetusten laittaminen on vuorossa seuraavaksi. Tästä valikosta voidaan valita verkolle nimi, joka minulla on *Larin*. Sitten on valittavissa, tuleeko modeemi reitittävään vai siltaavaan muotoon, minä valitsin reitittävän eli **Routing**. Näin omasta lähiverkosta tulee hallittavampi ja tietoturvallisempi, kunhan modeemille tehdään myös myöhemmin LAN ja NAT -asetukset. Valittaessa **Encapsulation**-kohtaan sopiva asetus tuli huomioida, laitetaanko modeemi reitittävään vai siltaavaan muotoon ja millainen yhteys on käytössä. Laitettaessa modeemi reitittävään muotoon pitää valita ENET ENCAP. Näin saadaan Zyxelin modeemi toimimaan reitittävänä. **Multiplex**-kohtaan valitsin LLC:n (Logical Link Control), joka on kaikkien IEEE 802 -verkkojen yhteinen osa siirtoyhteyskerrosta, joka hoitaa samalla tavalla kaikille lähiverkoille yhteiset toiminnot. **Virtual Circuit ID** -kohtaan vaihdetaan VPI (virtual path Identifier) eli virtuaalipolun tunniste, johon tulee yleensä aina 0 ja VCI (virtual channel identifier) eli virtuaalikanavan tunniste, johon tulee yleensä joko 100 tai 33 riippuen operaattorista. VPI/VCI-arvojen tulee olla samat, jotka operaattori on ilmoittanut, koska yhteys ei toimi, jos modeemiin on asetettu väärät arvot. Vielä kannattaa tarkistaa, että **IP Address** -kohdassa on automaattinen IP:n haku päällä.

WAN-puolen asetukset ovat nyt kunnossa ja tehty samanlaisesti, kuin kuvassa 10 on esitetty.

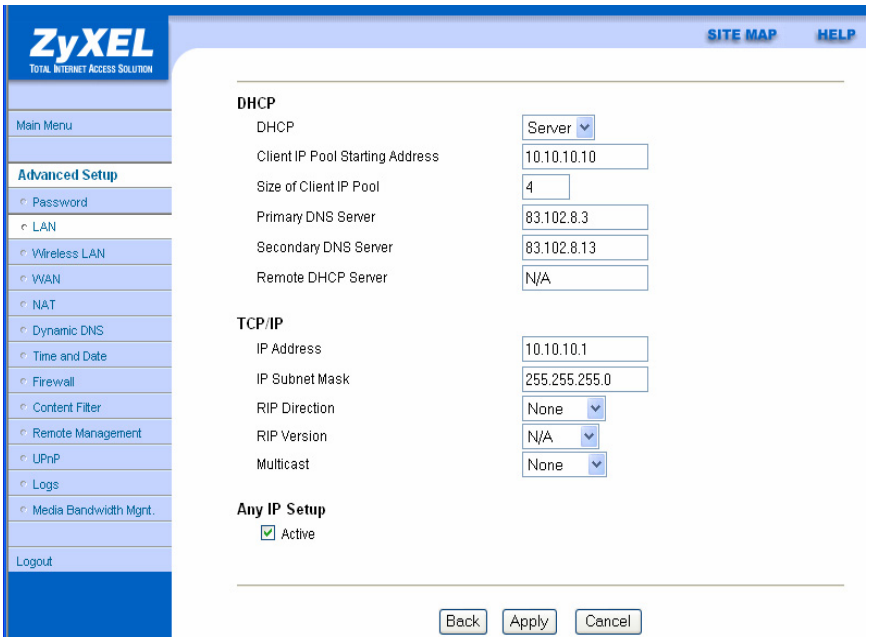


Kuva 10. WAN asetukset

6.3 LAN

LAN-valikosta valitaan ensin **LAN Setup**, jolloin aukeaa kuvan 11 kaltainen näkymä. DHCP-kohtaan valitsin ensin Server, jolloin modeemi toimii DHCP-serverinä ja jakaa IP-osoitteet lähiverkkoon. Valitsin IP-alueen 10.10.10.10 verkosta, koska näin saan verkosta helposti hallittavan ja muistan helposti, mikä IP on milläkin koneella. Valitsin myös 10.10.10.10-alkuisen verkon, koska työpaikallani on 192.168.x.x-verkko, ja joudun ottamaan aina välillä kotoa VPN (virtual private network)-yhteyden työpaikan verkkoon. IP-alueen kooksi valitsin neljä, näin sain lisättyä myös tietoturvaa. Kun kolme IP:tä on määrätty tietyille koneille, niin jää 1. IP vieraita koneita varten, ja se on käytössä vain langallisesti, koska langottomassa verkossa minulla on päällä MAC-suodatus, mutta siitä

myöhemmin lisää WLAN-osiossa. DNS palvelimien IP-osoitteet pitää pistää myös DHCP:lle, jotta se osaa jakaa oikeat osoitteet eteenpäin, ja tietokoneet saavat myös DNS palvelimien IP-osoitteet tietoonsa. Pistin DNS-palvelimiksi Tampereen puhelimen DNS:t, koska minulla on heidän tarjoamansa liittymä ja löysin niiden IP-osoitteet nopeiten. DNS:ksi voi kuitenkin pistää minkä tahansa DNS:än IP-osoitteen, jonka tietää. Itse olen todennut kyseiset DNS-palvelimet hyviksi, enkä näin ollen ole pistänyt muita palvelimia. **TCP/IP** asetuksiin pistin IP-osoitteeksi 10.10.10.1 pitääkseni edelleen verkon hallinnan helppona. Kyseisellä IP-osoitteella tapahtuu myös kirjautuminen sisään reitittimeen.

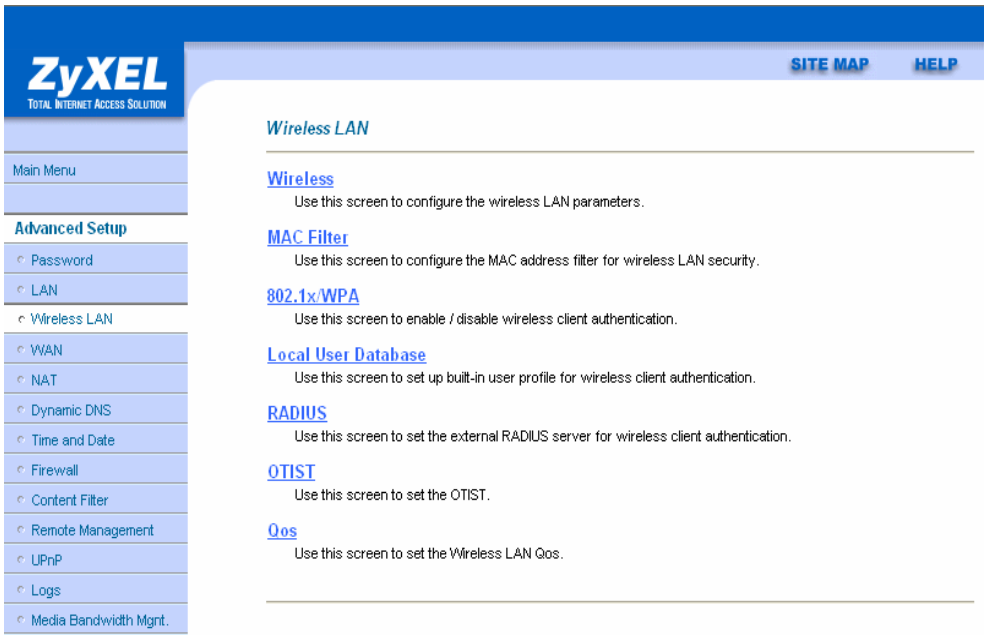


Kuva 11. LAN-asetukset(RFC)

LAN-valikosta löytyy myös **Static DHCP** -valikko, josta voidaan määrittää tietyille koneille MAC-osoitteen perusteella tietty IP-osoite. Määritin DHCP:n kolme ensimmäistä IP-osoitetta koneille, jotka ovat verkossani yleensä, ja näin ollen jokaisella koneella on aina sama IP-osoite, mikä näin ollen myös helpottaa verkon hallintaa.

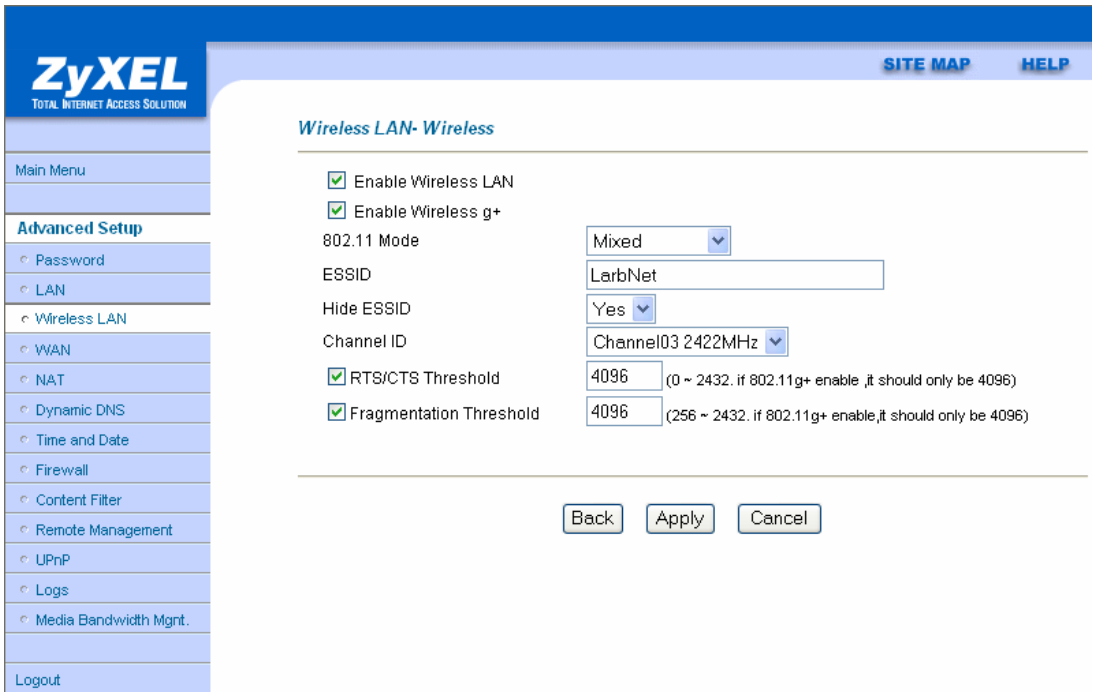
6.3 Wireless LAN

Valittaessa **Wireless LAN** -valikko avautuu kuvan 12 näkymä, josta tarvitsen ainoastaan kolmea ensimmäistä valikkoa *Wireless, MAC Filter ja 802.1x/WPA.*



Kuva 12. WLAN-päävalikko

Avataan ensin **Wireless**-valikko. Sieltä valitaan, että langattoman lähetin on valittu käyttöön, eli enable Wireless LAN -kohta on valittuna. 802.11 mode -kohtaan valitsin mixed, koska tällöin tukiasema käyttää tarpeen mukaan kumpaakin standardia, eikä ainoastaan 802.11b:tä tai g:tä. Kun on kummatkin mahdolliset vaihtoehdot käytössä, niin liittyminen langattomaan verkkoon onnistuu todennäköisemmin, myös vanhemmalla koneella. Seuraavaksi valitaan verkonnimi, eli SSID ja pistettään Hide ESSID kohtaan yes, jolloin langattoman verkon nimi ei ole julkisesti nähtävissä, kuten kuvassa 13 on tehty. Tästä valikosta valitaan myös se, mitä kanavaa halutaan käyttää. Minä valitsin kanavaksi kanava kolmen, koska sillä sain parhaimman kuuluvuuden toiseen huoneeseen siihen kohtaan, missä kannettavaa konetta useimmiten käytetään.



Kuva 13. Langaton verkko päälle ja sen nimeäminen

Seuraavaksi laitoin verkon suojauksen kuntoon, jolloin valitaan kuvan 12 valikosta 802.*1x/WPA*-kohta. Ensimmäiseksi valitaan, että langattomaan verkkoon liittyäkseen pitää syöttää varmenne, eli *Wireless Port Control* -kohtaan valitaan *Authentication reguire.* Valitaan vielä verkon suojaukseksi WPA-PSK ja syötetään vähintään kahdeksan merkkiä pitkä salausavain. Kuvan 12 valikosta valitaan vielä *MAC Filter*, joka valitaan aktiiviseksi ja pistetään, että vain kyseiset MAC-osoitteet sallitaan. Tällöin langatonta verkkoa voivat käyttää vain ne laitteet, joiden MAC-osoite on syötetty tukiasemalle.

6.4 NAT ja Firewall

NAT-valikosta valitsin että SUA (Single User Account) only on käytössä ja tein parille ohjelmalle porttiohjauksen liittyen siihen, mitä porttia ne käyttävät ja mitä IP-osoitetta ne käyttävät lähiverkossa.

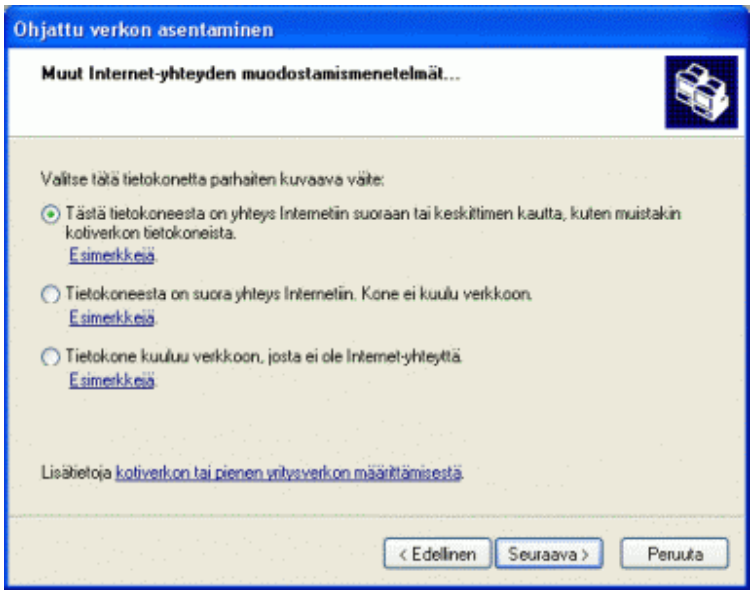
Firewall-valikosta valitaan, että palomuuri on aktiivisena ja sinne tehdään säännöt samoille ohjelmille kuin NAT -valikkoon ja avataan ne samat portit, joille tehtiin

NAT:in porttiohjaus. En käy läpi tässä työssä palomuurin asetuksia enempää, koska sen valikoista ja asetuksista pystyisin tekemään melkein kokonaan oman työn.

7 LÄHIVERKON ASETUKSET

Laitettaessa langatonta lähiverkkoa toimimaan parhaalla mahdollisella tavalla kannattaa testailla, millä asetuksilla ja millaisella modeemin sijoituksella saadaan paras mahdollinen toimivuus ja kuuluvuus. Tähän vaiheeseen käytin Network Stumbler -ohjelmaa, joka näyttää langattomista verkoista kaiken oleellisen. Ohjelma näyttää mm., mitä kanavia kantoalueella olevat muut verkot käyttävät, ja tämän mukaan valitsin itselle kanavan kolme, koska sitä tai sen viereistä kanavaa ei ollut kuuluvuusalueella kenelläkään muulla käytössä. Näin vältin muiden mahdollisten langattomien verkkojen häiriön omaan verkkoon.

Tietokoneillekin tulee tehdä tiettyjä asetuksia, jotta saadaan toimiva lähiverkko, jonka avulla pystytään siirtämään tiedostoja koneelta toiselle. Kaikille verkoissa oleville Windows-koneille tulee tehdä samat asetukset. Avataan ensimmäiseksi *Verkkoympäristö* ja sieltä valitaan *Määritä kotiverkko kotiin tai yrityksen verkkoon.* Sitten painetaan kaksi kertaa vain *seuraava*-painiketta. Laitetaan rasti kohtaan *Älä huomioi poistettuja verkkosovittimia* ja painetaan *seuraava*. Valitaan *muu tapa* ja painetaan *seuraava*-painiketta. Valitaan *Tästä tietokoneesta on yhteys Internetiin suoraan tai keskittimen kautta...* (kuva 14) ja painetaan taas *seuraava*. Valitaan avautuvasta listasta haluttu *lähiverkkoyhteys x*, jossa *x* on jokin numero. Sitten painetaan taas *seuraava*. Sen jälkeen annetaan koneelle jokin kuvaus ja nimi ja painetaan *seuraava.* Vielä pitää antaa lähiverkolle jokin nimi, esim. *LarbNet*. Nyt on tehty yhdelle koneelle lähiverkon asetukset kuntoon. Vielä pitää käynnistää kone uudestaan ja asennus on valmis.



Kuva 14. Ohjattu kotiverkon asentaminen Windows XP:ssä

Käytössäni on F-securen ohjelmistopalomuuri, eikä Windowsin oma. Koska en halua käyttää Windowsin omaa palomuuria, kannattaa kotiverkon asetusten tekemisen jälkeen poistaa käytöstä Windowsin palomuuri, jonka se asensi nyt automaattisesti lähiverkkoyhteyteeni. Nämä samat asetukset pitää tehdä kaikille koneille, jotka käyttävät lähiverkkoa ja joilta halutaan jakaa tiedostoja muille koneille. On tärkeää, että asetuksiin tulee sama verkonnimi, muuten yhteys ei toimi. Kahdessa käytössä olevassa koneessani on F-secure 2006 -ohjelmisto, joihin pitää tehdä palomuurille säännöt, jotka sallivat liikenteen kotiverkossa, eli pitää sallia *Windows file sharing and network Printer* ja *Windows network browsing.* Lähiverkko on nyt rakennettu ja laitettu asetusten puolesta kuntoon, mutta vielä tarvitsee valita, mitä kansioita halutaan vielä miltäkin koneelta jakaa. Se tapahtuu painamalla halutun tiedoston tai kansion kohdalla hiiren oikeanpuoleista näppäintä ja valitaan *Jakaminen ja suojaus* ja sieltä edelleen *Jaa tämä kansio verkossa*. Nyt kyseinen kansio on nähtävissä ja käytettävissä aina kun se tietokone on päällä, jossa jaettava kansio on.

8 YHTEENVETO

Työtä tehdessä tuli minulle itselleni paljon uutta ja arvokasta tietoa ADSL-, Ethernet- ja WLAN-tekniikasta. Työtä tehdessäni opin paljon asioita, joita pystyn suoraan hyödyntämään nykyisessä työpaikassani, ja myös työpaikallani olen oppinut paljon asioita, joita pystyin hyödyntämään tutkintotyötä tehdessäni. Sen olen myös nyt huomannut töissä, kun olen oppinut käyttämään Zyxelin modeemia hyvin, että myös muiden valmistajien modeemien käyttö on ollut paljon helpompaa, kun peruslähtökohta on kuitenkin kaikissa modeemeissa sama –ne on vain toteutettu vähän erilailla.

Ongelmaksi työtä tehdessä tuli sen rajaus, kun modeemin konfigurointiosuudesta olisi voinut tehdä melkein kuinka pitkän vain. Tämän vuoksi laitoin työhön vain ne osuudet asetuksista, joiden avulla saadaan toimiva ja tietoturvallinen yhteys ja lähiverkko käyttöön. Samanlaisilla asetuksilla saadaan myös pienyritykseen toimiva verkko, kuten työnteko aikana tein erääseen yritykseen, jossa oli eri valmistajan laite, mutta pystyin hyvin silti käyttämään tutkintotyössäni opittuja asioita.

LÄHTEET

Painetut lähteet:

1. Ginsburg, Daavid: ADSL. IT Press. Helsinki 2000. 303 s.

2. Jaakohuhta, Hannu: Lähiverkot – Ethernet 4.uudistettu painos. IT Press Helsinki 2005. 380s.

Sähköiset lähteet:

3. Wikipedia. [www-sivu]. [viitattu 4.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/ADSL

4. Verkkotekniikka + - Training Kit. [sähköinen kirja] Itinfo [viitattu 5.10.2006] saatavisaa: http://www.itinfo.fi/ekirja.php?isbn=951-826-316-7

5. Wikipedia [www-sivu]. [viitattu 5.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/Langaton_l%C3%A4hiverkko

6. MVnet [www-sivu] [viitattu 5.10.2006] Saatavissa: http://www.mvnet.fi/index.php?osio=Tietokoneet&sivu=Langaton_kotiverkko

7. Wikipedia [www-sivu]. [viitattu 8.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva

8. Wikipedia [www-sivu]. [viitattu 8.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/WEP

9. Wikipedia [www-sivu]. [viitattu 8.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/WPA

10. Wikipedia [www-sivu]. [viitattu 8.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/TKIP

11. Wikipedia [www-sivu]. [viitattu 10.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/Ethernet

12. Inside Verkot. [sähköinen kirja] Itinfo [viitattu 10.10.2006] saatavisaa: http://www.itinfo.fi/

13. Kallionpää, Risto, lab.ins. [PPT] Luentomoniste, tietokoneverkot S4277-12, S4277-12.ppt, syksy 2005, Tampereen ammattikorkeakoulu

14. TCP/IP. [sähköinen kirja] Itinfo [viitattu 10.10.2006] saatavisaa: http://www.itinfo.fi/

15. TCP/IP Trainer. [sähköinen kirja] Itinfo [viitattu 19.10.2006] saatavisaa: http://www.itinfo.fi/

16. Kallionpää, Risto, lab.ins. [PDF] Luentomonisteet, tietokoneverkkojen jatkokurssi S4278-4, IPv4vsIPv6.pdf, syksy 2005, Tampereen ammattikorkeakoulu