WRT610N LANGATON REITITIN

Laitteen hyödyntäminen koulun laboratorioverkoissa

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulututkinnon opinnäytetyö

Tietotekniikan ko.

Riihimäki, 11.1.2010

Teri Nikkanen

HAMK
HÄMEEN AMMATTIKORKEAKOULU

OPINNÄYTETYÖ

Tietotekniikan koulutusohjelma
Riihimäki

Työn nimi	WRT610N langaton reititin ja sen hyödyntäminen koulun laboratorioverkoissa
Tekijä	Teri Nikkanen
Ohjaava opettaja	Raimo Hälinen
Hyväksytty	_____._____.20_____
Hyväksyjä	

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Riihimäki
Tietotekniikan ko.
Tietoliikennetekniikan suuntautumisvaihtoehto

Tekijä Teri Nikkanen **Vuosi** 2009

Työn nimi WRT610N langaton reititin

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli luoda laboratorio-ohjeita WRT610N langattomille reitittimille. Laboratorio-ohjeita tullaan käyttämään hyväksi Hämeen ammattikorkeakoulun tietotekniikan kursseilla. Laboratorio-ohjeiden avulla oppilaat voivat harjoitella käytännössä teoriassa oppimiaan asioita laboratorioympäristössä. Laboratoriotyöskentelyn tavoitteena on tutustuttaa oppilaat yleisiin työelämän haasteisiin. Kirjallisen osuuden tavoitteena on selventää langattoman reitittimen ominaisuuksia oppilaille.

Opinnäytetyön käsittelemiin teoria-osioihin tutustuttiin alan kirjallisuuden avulla. WRT610N langattoman reitittimen ominaisuuksiin tutustuttiin laitteen mukana tulleen käyttöoppaan avulla. Käyttöoppaan ohjeiden avulla ominaisuudet testattiin laboratorio-olosuhteissa, ja niistä valittiin sopivimmat laboratorio-ohjeiden aiheiksi.

WRT610N langaton reititin osoittautui sopivan hyvin laboratorioharjoituskäyttöön. Sen lukuisat ominaisuudet ja yksinkertainen käyttöliittymä mahdollistivat kattavan laboratorio-ohjeiden laatimisen. Selvisi kuitenkin, ettei WRT610N langaton reititin sisältänyt tarpeeksi mobiiliteknologian ominaisuuksia. Tästä johtuen mobiiliverkon suunnitteleminen pelkän langattoman reitittimen avulla ei ollut mahdollista, ja laboratorio-ohjetta ei tehty aiheesta. Aiheesta tehdään uusi opinnäytetyö, joka keskittyy lähemmin mobiiliteknologian tarpeisiin.

Avainsanat Langaton reititin, WRT610N, laboratorio-ohje, standardit, langaton verkko

Sivut 33 s. + liitteet 16 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Riihimäki
Degree Programme in Information Technology
Information technology

Author Teri Nikkanen **Year** 2009

Subject of Bachelor's thesis The WRT610N Wireless Router

ABSTRACT

The purpose of this thesis was to create instructions for WRT610N wireless routers used in the laboratory. These instructions will be used in information technology courses at HAMK University of Applied Sciences. With these instructions students can practise those subjects they have learnt in theory in a laboratory environment. The aim of the laboratory experiments is that students become familiarized with common working life challenges. The purpose of the literary part is to explain features of wireless routers to students.

The theoretical part of this thesis work was obtained from information technology literature. The information on the features of the WRT610N wireless router was obtained from the devices' user guide. With the help of the user guide the features were tested in a laboratory environment and the most suitable features were chosen for subjects in the laboratory instructions.

The WRT610N wireless router proved to be a very suitable device for laboratory experiments. The numerous features and the easy-to-use management system made it possible to create comprehensive laboratory instructions. Nevertheless it turned out that the WRT610N wireless router did not include enough mobile technology features. That is why it was not possible to design a mobile network by only using the WRT610N wireless router. For this reason laboratory instructions were not created for that purpose. A new thesis will research this subject and will focus closely on mobile technology purposes.

Keywords Wireless router, WRT610N, laboratory instructions, standards, wireless network

Pages 33 p. + appendices 16 p.

TERMIT JA LYHENTEET

AAA – Authentication Authorization Accountin – RADIUS protokollan kolme ominaisuutta: todentaminen, valtuutus ja tilastointi

AES – Advanced Encryption Standard – Langattomassa tietoliikenteessä käytettävä lohkosalausmenetelmä

CCK - Complementary Code Keying – Komplementaarikoodiavainnusta

CCMP - Counter Mode with CBC-MAC Protocol – Langattomissa verkoissa käytetty salausprotokolla

DHCP - Dynamic Host Configuration Protocol - Protokolla, jonka tehtävänä on jakaa IP -osoitteet uusille verkkoon kytkeytyville laitteille

DMZ - Demilitarized Zone – Fyysinen tai looginen aliverkko, joka yhdistää lähiverkon turvattomampaan tietoliikenneverkkoon esim. Internetiin

DNS - Domain Name System - Järjestelmä, jonka tehtävänä on muuntaa selkokieliset verkkotunnukset IP -osoitteiksi

DSSS - Direct Sequence Spread Spectrum – Modulointimenetelmä

FHSS - Frequency Hopping Spread Spectrum – Taajuushyppelytekniikka, modulointitekniikka

FTP - File Transfer Protocol – Tiedonsiirtoprotokolla kahden eri laitteen välille

HSPA – High-Speed Packet Access – Matkapuhelinteknologiaprotokollien kokoelma, joka parantaa ja laajentaa UMTS protokollien suorituskykyä

HTTP – HyperText Transfer Protocol – Protokolla, jota Internet-selaimet ja palvelimet käyttävät tiedonsiirtoon

HTTPS – HyperText Tranfer Protocol Secure – Protokolla, jota Internet selaimet ja palvelimet käyttävät salattuun tiedonsiirtoon

IEEE - Institute of Electrical and Electronics Engineers – Merkittävä kansainvälinen tekniikan alan järjestö

IP - Internet Protocol – Protokolla, jonka tehtävänä on huolehtia tietoliikennepakettien toimittamisesta määränpäähän Internet-verkossa

IPsec – Internet Protocol Security – Protokolla, joka sisältää tunnistus- ja salaus ominaisuudet mahdollistaen tietoturvallisen tietoliikenteen

L2TP – Layer 2 Tunneling Protocol – Protokolla, jota käytetään VPN yhteyksissä

LOG – Lokitiedostot, johon tallentuu tieto tietoliikenteessä tapahtuvista muutoksista

LTE – Long Term Evolution – 3.9G matkapuhelinteknologia, joka toimii siltana seuraavan neljännen sukupolven 4G matkapuhelinteknologialle

LTE-A – Long Term Evolution Advanced – Neljännen sukupolven 4G matkapuhelinteknologia

MAC-osoite - Media Access Control – Verkkosovittimen osoite, jolla yksilöidään laite tietoliikenneverkoissa

MIC - Message Integrity Code – Paketin eheyden tunnistukseen käytetty koodi

MIMO - Multiple Input, Multiple Output – Tekniikka, jossa langattomassa tiedonsiirrossa käytetään useampaa antennia

MTU – Maximum Transfer Unit – Tietoliikenneyhteydessä käytössä oleva maksimaalinen pakettikoko

NAT – Network Address Translation – Osoitteenmuunnos, jonka avulla voidaan useampi laite liittää Internetiin yhdellä IP – osoitteella

OFDM - Orthogonal Frequency Division Multiplexing - Modulointimenetelmä

PIN – Personal Identification Number – Tässä opinnäytetyössä, PIN numero vastaa tiettyjen sovittujen asetuksien määrittämistä tiettyä PIN tunniste numeroa vastaan

PING – TCP/IP protokolla työkalu, jolla voidaan määritellä halutun laitteen saavutettavuutta

PMK – Pair-Wise Master Key – Langattoman verkon salauksessa käytetty pääavain

PTK – Pair-wise Transient Key – Langattoman verkon salauksessa käytetty pakettikohtainen salausavain

Policy – Internet Access Policy – Säännöstö, johon määritellään ehdot joiden mukaan käyttäjille sallitaan Internet yhteyden toiminta

PPTP – Point-to-Point Tunneling Protocol – Protokolla mitä käytetään hyväksi VPN yhteyksissä

QoS – Quality of Service – Termi, jolla tarkoitetaan tietoliikenteen priorisointia ja luokittelua

RADIUS - Remote Authentication Dial In User Service – Lähiverkko protokolla, jossa tunnistus tapahtuu keskitetyn järjestelmän avulla

RIP – Routing Information Protocol – Reititys protokolla, joka käyttää reitityksen laskemiseen niin sanottua hyppymäärää

SPI – Stateful Packet Inspection – Tilallinen palomuuri, jossa tutkitaan pakettikohtaisesti liikkuvaa liikennettä

SSID – Service Set Identifier – Tunnus, jolla voidaan erottaa samalla alueella olevat langattoman lähiverkot toisistaan

TCP – Transmission Control Protocol – Tietoliikenneprotokolla, jonka avulla luodaan yhteyksiä laitteiden välillä

TKIP – Temporal Key Integrity Protocol – Protokolla, jota käytetään hyväksi langattomien verkkojen salauksessa

TRACEROUTE – TCP/IP protokolla työkalu, jolla voidaan määritellä mitä reittiä paketit siirtyy halutulle laitteelle

UMTS – Universal Mobile Telecommunications System – Kolmannen sukupolven 3G matkapuhelinteknologia

UDP – User Datagram Protocol – Tietoliikenneprotokolla, jonka avulla luodaan yhteyksiä laitteiden välillä

UPnP – Universal Plug and Play – Joukko verkkoprotokollia, joiden tarkoitus on helpottaa media palveluiden tarjoamista ja yhteensopivuutta lähiverkoissa

USB – Universal Serial Bus – Sarjaväyläarkkitehtuuriin perustuva standardi, jolla voidaan liittää oheislaitteita päätelaitteisiin

VOiP – Voice Over Internet Protocol – Tekniikka, jolla voidaan tuottaa puhe ja videopuhelupalveluita Internetin välityksellä

VPN – Virtual Private Network – Termi, jolla tarkoitetaan kahden tai useamman verkon yhdistämistä julkisen verkon yli yksityiseksi verkoksi

WAN – Wide Area Network – Lähiverkkoja isompi ja maantieteellisesti laajempi tiedonsiirtoverkko

WEP – Wired Equivalent Privacy – Salausmenetelmä, joka kehitettiin ensimmäisenä suojaamaan langatonta tietoliikennettä

WLAN – Wireless Local Area Network – Langaton lähiverkko, jossa tiedonsiirto tapahtuu ilman fyysisiä kaapeleita

WMM – Wi-Fi Multimedia – Mahdollistaa QoS – palveluita IEEE 802.11 lähiverkoissa

WPA – Wi-Fi Protected Access – Salausmenetelmä langattomaan tietoliikenteeseen, joka paransi WEP -salauksen sisältämiä puutteita

WPA2 - Wi-Fi Protected Access **–** Salausmenetelmä langattomaan tietoliikenteeseen, joka paransi WPA –salauksen sisältämiä puutteita

WPS – Wi-fi Protected Setup – Standardi, jonka tarkoituksena on ollut helpottaa langattoman verkon tietoturva-asetuksien määrittämistä

SISÄLLYS

1. JOHDANTO 1

2. LANGATTOMAN VERKON STANDARDIT 2

2.1 Langattoman verkon IEEE 802.11 standardit 2
2.1.1 IEEE 802.11 2
2.1.2 IEEE 802.11b 2
2.1.3 IEEE 802.11a 3
2.1.4 IEEE 802.11g 3
2.1.5 IEEE 802.11n 3
2.2 Langattoman verkon salaus 4
2.2.1 WEP 4
2.2.2 WPA 5
2.2.3 WPA2 5
2.3 RADIUS 6
2.4 DMZ - Demilitarized Zone 7
2.5 4G - matkaviestijärjestelmät 10
2.5.1 Long Term Evolution - LTE 10
2.5.2 Long Term Evolution Advanced - LTE-A 10

3. WRT610N OMINAISUUDET 12

4. ASETUKSET (SETUP) 13

4.1 Perusasetukset (Basic Setup) 13
4.2 MAC- osoiteklooni (Mac Address Clone) 15
4.3 Kehittynyt reititys (Advanced Routing) 15

5. LANGATON VERKKO (WIRELESS) 15

5.1 Langattoman verkon perusasetukset (Basic Wireless Settings) 15
5.1.1 Wi-Fi Protected Setup - WPS 16
5.1.2 Perusasetuksien määrittäminen (Wireless Configuration) 16
5.2 Langattoman verkon tietoturva (Wireless Security) 17
5.3 Langattoman verkon MAC - suodatus (Wireless MAC Filter) 18
5.4 Langattoman verkon lisäasetukset (Advanced Wireless Settings) 18

6. TIETOTURVA (SECURITY) 19

6.1 Palomuuri (Firewall) 19
6.2 VPN yhteyksien läpikulku (VPN passthrough) 19

7. MUISTIJÄRJESTELMÄ (STORAGE) 19

7.1 Kovalevy (Disk) 19
7.2 Media -palvelin (Media Server) 20
7.3 FTP -palvelin (FTP Server) 20
7.4 Hallinnointi (Administration) 21

8. KÄYTETTÄVYYDEN RAJOITTAMINEN (ACCESS RESTRICTIONS) 21

8.1 Internet käyttörajoitukset (Internet Access) 21

9. SOVELLUKSET JA PELAAMINEN (APPLICATIONS AND GAMING) 22

9.1 Tietoliikenneportin edelleen lähetys (Single Port Forwarding) 22
9.2 Tietoliikenneporttivälin edelleen lähetys (Port Range Forwarding) 22
9.3 Tietoliikenneportin tunnistus (Port Triggering) 22
9.4 DMZ (Demilitarized zone) 23
9.5 Tietoliikenteen priorisointi (QoS) 23

10. HALLINTA (ADMINISTRATION) 25

10.1 Hallinnointi (Management) 25
10.2 Lokitiedot (Log) 26
10.3 Virheenmääritys (Diagnostics) 28
10.4 Tehdasasetukset (Factory Defaults) 29
10.5 Ohjelmistopäivitys (Firmware Upgrade) 29

11. TILANNETIETO (STATUS) 30

11.1 Reititin (Router) 30
11.2 Lähiverkko (Local Network) 30
11.3 Langaton verkko (Wireless Network) 30

12. MOBIILI LABORATORIO 31

13. LABORATORIOIDEN SUUNNITTELU 31

14. YHTEENVETO 32

LÄHTEET 33

LIITE 1 Laboratorio-ohje 1
LIITE 2 Laboratorio-ohje 2

1. JOHDANTO

Tietoliikennetekniikan opiskelijoiden koulutussuunnitelmaan kuuluu yhtenä osana perehtyminen langattomien verkkojen tekniikoihin. Teoriaopetuksen lisäksi tavoitteena on tarjota oppilaille mahdollisuus hyödyntää teoriatunneilla oppimiaan asioita laboratorioympäristössä. Käytännön harjoitukset vahvistavat teoriatunneilla opittuja asioita ja valmistavat oppilaita kohtaamaan mahdollisesti työelämässä esiin tulevia haasteita.

Hämeen ammattikorkeakoulun Riihimäen yksikkö on hankkinut laboratorioharjoittelua varten useampia Linksysin valmistamia WRT610N langattomia reitittimiä. Koululla on tarve selvittää langattoman reitittimen ominaisuuksia ja sitä, miten langattomia reitittimiä voisi parhaiten hyödyntää laboratoriotyöskentelyssä. Tavoitteena on suunnitella laboratorio-ohjeistuksia tuleville kursseille, joilla perehdytettäisiin oppilaat käytännössä langattoman verkon rakentamiseen.

Laboratorio-ohjeistuksen laatiminen vaatii ensimmäiseksi tutustumista langattomien reitittimien sisältämiin ominaisuuksiin. Ominaisuuksista valitaan laboratorio-ohjeisiin ne, jotka ovat lähinnä työelämän tarpeita. Laboratorio-ohjeiden tavoitteena on olla oppilaille helposti seurattavia, mutta samalla haasteellisia. Ohjeistuksen lisäksi tavoitteena on suunnitella kysymyslista, jolla pystyttäisiin sisäistämään oppilaille laboratoriotyön tavoitteena olevat keskeiset aiheet langattomista verkoista. Tutkimustulokset ja ohjeistukset jäävät opetustarkoituksessa Hämeen ammattikorkeakoulun Riihimäen yksikön vapaaseen käyttöön.

2. LANGATTOMAN VERKON STANDARDIT

2.1 Langattoman verkon IEEE 802.11 standardit

2.1.1 IEEE 802.11

IEEE (Institute of Electrical and Electronics Engineers) julkaisi vuonna 1997ensimmäisen WLAN (Wireless Local Area Network)–tekniikkaan perustuvan standardin IEEE 802.11, jonka teoreettinen bittinopeus oli 1 ja 2 Mbit/s:ssa. Se käyttää taajuusalueena 2.4 GHz ja kanavia väliltä 1 - 14. IEEE 802.11 soveltuu niin sisä- kuin ulkokäyttöön. Hajautukseen IEEE 802.11 käytti Barker-hajautusta, jolla pystyttiin helposti toteuttamaan 1 ja 2 Mbit/s siirtonopeudet. Standardi käytti myös modulointitekniikkana suorasekvenssitekniikkaa DSSS (Direct Sequence Spread Spectrum), jonka avulla pystyttiin lähetettävä data hajauttamaan laajemmalle taajuusalueelle. Tämän jälkeen data lähetettiin samanaikaisesti matemaattisten funktioiden perusteella. Ensimmäisessä standardissa käytettiin myös modulointitekniikkana taajuushyppelyä FHSS (Frequency Hopping Spread Spectrum), jossa lähettäjä vaihtaa lähetystaajuutta sovitun algoritmin perusteella.

Jokaisen kanavan bittivirta hajautetaan 22 MHz:n taajuusalueelle. Kanavat hajautetaan taajuusalueelle 2,400 - 2,495 GHz niin, että jokainen kanava alkaa n. 5 MHz:n välein. Näin taajuusalueelle saadaan mahdutettua yhteensä kaikki 14 kanavaa. Kaikkia kanavia ei kuitenkaan käytetä kaikissa maissa. Jokaiselle maalle on määritelty, mitä kanavia ja millä taajuusalueella laitteet saavat toimia. Euroopassa esimerkiksi käytetään yleisesti kanavia 1 - 13 taajuusalueella 2,400 - 2,485 GHz tietyin maakohtaisin poikkeuksin. Japanissa on sallittua kuitenkin vain 14 kanavan käyttö, jolloin taajuusalueeksi muodostuu ainoastaan 2,473 - 2,495 GHz. Käytettäessä langattomia tiedonsiirtolaitteita on syytä selvittää, onko niiden käyttämät taajuusalueet sallittuja käytettävässä maassa. (Puskala, 2005, 36,46; Chandra, 2008, 266-268.)

2.1.2 IEEE 802.11b

IEEE 802.11b oli vuonna 1999 kehitetty standardi parantamaan vuoden 1997 kehiteltyä IEEE 802.11 standardia. 802.11b käytti edelleen 2.4 GHz:n taajuusaluetta, joka käytti kanavia väliltä 1 - 14 taajuusalueen ollessa 2,400 - 2495. Vanhan IEEE 802.11 standardin nopeudet kävivät nopeasti kehittyvässä tietoliikenteessä liian hitaiksi, joten oli tarve kehittää uusi standardi. Standardi käytti edelleen IEEE 802.11:stä tuttua DSSS suorasekvenssitekniikkaa. FHSS modulointitekniikkaa ei enää IEEE 802.11b standardissa käytetty.

Uudella standardilla kyettiin 1 ja 2 Mbit/s:n teoreettisten siirtonopeuksien lisäksi 5,5 ja 11 Mbit/s:n teoreettisiin siirtonopeuksiin. Siirtonopeuden kasvaessa ei voitu enää käyttää Barker-hajautusta, vaan oli käytettävä komplementaarikoodiavainnusta (CCK, Complementary Code Keying).

Tällä pystyttiin toteuttamaan 5,5 ja 11 Mbit/s:n teoreettiset siirtonopeudet taajuusalueen pysyessä edelleen 2,4 GHz:ssä. (Puska, 2005, 36-40,46.)

2.1.3 IEEE 802.11a

IEEE kehitti vuonna 1999 myös toisen standardin IEEE 802.11a. Se mahdollisti 6 - 54 Mbit/s:n teoreettisen bittinopeuden ja täten nopeamman tiedonsiirtokapasiteetin. Tiedonsiirtokapasiteettia saatiin kasvatettua nostamalla taajuusaluetta n. 5 GHz:iin aiemman n. 2,4 GHz:n sijaan. Tämä 5 GHz:n U-NII (Unlicensed National Information Infrastructure) -taajuusalue oli vapaasti käytettävissä Pohjois-Amerikassa. Kanavia taajuusalueella oli käytössä yhteensä kaksitoista.

IEEE 802.11a standardi siirtyi käyttämään modulointitekniikkana monikantoaaltomodulointia OFDM (Orthogonal Frequency Division Multiplexing), jotta voitiin toteuttaa nopeampi tiedonsiirtokapasiteetti. Siinä lähetettävä data jaetaan useamman taajuuden alikanaviin, joita käytetään rinnakkain yhtäaikaisesti. Standardin heikkous oli sen lyhyt kantama 5 GHz:n taajuusalueen vuoksi. Oli tarve kehittää standardi, joka kykenisi samaan tiedonsiirtokapasiteettiin, mutta pidemmällä kantamalla. IEEE 802.11a ei ollut myöskään yhteensopiva IEEE 802.11b standardisten laitteiden kanssa. (Puska, 2005, 40,45-46.)

2.1.4 IEEE 802.11g

IEEE 802.11g oli vuonna 2003 kehitetty standardi, joka kehitettiin korvaamaan IEEE 802.11b standardi. Se sisältää IEEE 802.11a standardin ominaisuudet, mutta se toimii 2,4 GHz:n taajuusalueella. Tällä taajuusalueella sillä on käytössä yhteensä 12 kanavaa ja sen teoreettinen bittinopeus on 1 - 54 Mbit/s:ssa.

IEEE 802.11g käyttää hajaspektritekniikkana monikantoaaltomodulointia OFDM, mutta se sisältää myös yhteensopivuussyistä CCK-koodauksen sekä 5,5 että 11 Mbit/s:n siirtonopeudet. Näistä syistä IEEE 802.11g on yhteensopiva IEEE 802.11b standardisten laitteiden kanssa. IEEE 802.11g standardista puhutaan myös yleisesti, että se on eurooppalainen standardi sen käyttämän taajuusalueen takia.

Standardin käyttämän taajuusalueen johdosta tiedonsiirtokantamaa pystyttiin lisäämään verrattuna IEEE 802.11a standardiin. On laskettu, että kattaakseen ison alueen IEEE 802.11g standardin laitteilla, olisi IEEE 802.11a standardisia laitteita tarvittu tämän alueen kattamiseen 1,5-kertainen määrä. (Puska, 2005, 36,40,45- 46.)

2.1.5 IEEE 802.11n

IEEE 802.11n on seuraavan sukupolven langattoman verkon standardi. Sillä pyrittiin jälleen pidempään kantomatkaan ja suurempaan tiedonsiirtokapasiteettiin. IEEE 802.11n standardin laitteet tukevat sekä 2.4 että 5 GHz:n taajuusaluetta. Teoreettinen bittinopeus on yli 250 Mbit/s, mutta se

voi olla myös käytännössä huomattavasti enemmän. Kehitystyö on saatu niin pitkälle, että IEEE hyväksyi IEEE 802.11n standardin syyskuussa 2009(IEEE, 2009). Tästä huolimatta markkinoilla on ollut jo lukuisia 802.11n standardia tukevia laitteita ainakin parin vuoden ajan. (Puska, 2005, 46.)

IEEE 802.11n standardi tukee niin sanottua MIMO (Multiple Input, Multiple Output) -tekniikkaa, jossa käytetään useampaa antennia lähettämään ja vastaanottamaan dataa. Useamman antennin yhtäaikaisen käyttämisen lisäksi, IEEE 802.11n pystyy käyttämään myös useampaa kanavaa yhtäaikaisesti lähettämiseen ja vastaanottamiseen. Sen sijaan, että IEEE 801.22n käyttäisi 20 MHz:n laajuisia kanavia, se pystyy käyttämään myös vaihtoehtoisesti jopa 40 MHz:n laajuisia kanavia. Jotta siirtonopeus pystytään mahdollistamaan, IEEE 802.11n käyttää kehiteltyä muunnosta OFDM monikantoaaltomoduloinnista. (Chandra, 2008, 397-400.)

2.2 Langattoman verkon salaus

2.2.1 WEP

WEP (Wired Equivalent Privacy) on IEEE 802.11 standardin ensimmäinen salausmenetelmä, joka oli tarkoitettu salaamaan tietoliikenne langattomissa verkoissa. Salausperiaatteena on, että päätelaitteisiin määritellään sama yleisavain kuin langattoman verkon tukiasemiin. Avain voidaan salata joko 40- tai 104-bittisenä, johon liitetään lisäksi vielä 24-bittinen alustusvektori. Täten salausavaimista muodostuu joko 64- tai 128-bittisiä. WEP käyttää salausalgoritmina RC4 algoritmia.

WEP:n periaate toimii siten, että asiakkaan päätelaite lähettää Authentication Request-pyynnön tukiasemalle, jossa ilmoitetaan sen tukevan WEP salausta. Tukiasema lähettää sen jälkeen haastetekstin, jonka tunnistusalgoritmiksi annetaan jaetun salausavaimen tunnistus. Tämän jälkeen työasema vastaa lähettämällä tukiasemalle saman tunnistusalgoritmin haastetekstin, mutta salaa tämän informaation omalla WEP avaimellaan. Tukiasema yrittää tämän jälkeen purkaa saapuneen datan omalla avaimellaan ja vertaa tätä sen jälkeen lähettämäänsä haasteeseen. Jos nämä vastaavat toisiaan, hyväksytään tunnistus päätelaitteen ja tukiaseman välillä.

Langattoman tiedonsiirron salaaminen WEP:n avulla ei ole nykyaikana enää suositeltavaa, koska sen salausominaisuudet tietoturvanäkökulmasta ovat heikot. Salausta voidaan hiukan parantaa lisäämällä tukiasemaan ja päätelaitteisiin yhteensä 4 erilaista avainta, joita voidaan vaihdella. WEP:n purkaminen nykyaikaisilla ohjelmistoilla ja laitteilla ei ole enää haastava tehtävä. WEP:n toimintaperiaatteen takia staattinen salausavain on helposti ennustettavissa. Tästä syystä WEP:n käyttöä ei enää nykypäivänä suositella langattomissa verkoissa. Sen käyttö on kuitenkin parempi kuin, ettei langatonta verkkoa salata millään tavalla. (Puska, 2005, 74.)

2.2.2 WPA

WPA (Wi-Fi Protected Access) -salaus kehiteltiin paikkaamaan niitä puutteita, joita oli ilmennyt WEP-salauksessa. WPA käyttää salaamisessa TKIP (Temporal Key Integrity Protocol) -protokollaa, jossa käytetään 128-bittistä, pakettikohtaista salausta. WEP:ssä ongelmana ollut staattisen salausavaimen helppo ennustettavuus poistui WPA standardin myötä. WPA käytti kuitenkin edelleen salausalgoritmina RC4 salausalgoritmia. (Puska, 2005, 82.)

WPA:ssa käytetään WEP:stä tuttua yleisavainta, joka syötetään sekä asiakkaan päätelaitteeseen että tukiasemaan. Tästä yhteisestä yleisavaimesta generoidaan parittainen yleisavain PMK (Pair-wise Master Key), jonka avulla tunnistus suoritetaan. Tämän lisäksi WPA:ssa muodostetaan tätä PMK-avainta hyväksikäyttäen pakettikehyskohtaiset PTK (Pair-wise Transient Key) -avaimet TKIP-protokollan avulla. Näitä jatkuvasti muuttuvia PTK-avaimia käytetään tietoliikenteen salaamiseen asiakkaan päätelaitteen ja tukiaseman välillä. Tällä pystytään mahdollistamaan se, että PMK-avainta ei pystytä kaappaamaan tietoliikenteestä yhtä helposti kuin WEP:ssä, vaan tukiaseman ja päätelaitteen välisessä tietoliikenteessä käytetään dynaamisia PTK-avaimia jokaisessa datapakettikehyksessä. (Chandra, 2008, 378-382; Puska, 2005, 84.)

WPA sisältää myös pakettien eheyden tunnistustoiminnon, jossa jokainen pakettikehys sisältää MIC (Message Integrity Check) ominaisuuden paketin tunnistusta varten. Lähetyspäässä jokaiseen pakettiin sisällytetään MIC-koodi, jota verrataan perillä vastaanottopäässä. Järjestelmä olettaa joutuneensa tietoturvahyökkäyksen kohteeksi, jos MIC-arvo ei vastaa vastaanottopäässä samaa kuin se oli lähetettäessä. Tämän jälkeen se poistaa kaikki käytössä olleet avaimet ja katkaisee yhteyden minuutiksi. Minuutin jälkeen yhteys pyritään luomaan uudelleen automaattisesti. (Chandra, 2008, 387-388; Puska, 2005, 82.)

Tunnistus käyttäjän päätelaitteen ja tukiaseman välillä voidaan luoda joko WEP:stä tutulla WPA-Personal toiminnolla, jossa tunnistukseen käytetty PMK avain syötetään sekä asiakkaan päätelaitteeseen että tukiasemaan. WPA-Enterprise mahdollistaa taas tunnistuspalvelimen RADIUS (Remote Authentication Dial In User Service) käytön. (Chandra, 2008,382-386.)

2.2.3 WPA2

WPA2 on uusin langattomien verkkojen tietoturvastandardi, joka on paranneltu versio WPA:sta. Parannuksia WPA2:ssa on esimerkiksi se, että salausalgoritmina käytetään AES (Advanced Encryption Standard) -standardia. Se oli huima parannus verrattuna WEP:ssä ja WPA:sa käytettyyn RC4-standardiin. AES-salausalgoritmi vaati kuitenkin huomattavasti enemmän suorituskykyä laitteelta kuin RC4-salausalgoritmi. Tästä syystä päätelaite tarvitsee erillisen salauspiirin hoitamaan salaustehtävän tai muuten päätelaitteen suorituskyky kärsii merkittävästi. (Puskala, 2005, 83-85.)

WPA2 sisältää myös parannuksen WPA:sta tuttuun pakettien eheyden tunnistukseen MIC. WPA2 käyttää AES salaukseen pohjautuvaa CCMP (Counter Mode with CBC-MAC Protocol) salausprotokollaa. Sen tehtävänä on lisätä lähetyspäässä datakehykseen kahdeksan tavua pitkä bittijono. Tätä kahdeksan tavun sisältämää tietoa vertailemalla vastaanottopäässä varmistutaan siitä, ettei lähetettyä dataa olla muutettu matkan varrella ulkopuolisten toimesta. (Chandra, 2008,390-396.)

2.3 RADIUS

RADIUS (Remote Authentication Dial In User Service) -protokollalla voidaan tarjota langattomalle lähiverkolle keskitetty tunnistuspalvelu. Todentamisella määritellään henkilö, joka yrittää käyttää langattoman lähiverkon palveluita. Todentamisen lisäksi protokolla sisältää palvelun, jolla tarkistetaan, mitä palveluita käyttäjä on valtuutettu käyttämään langattomassa lähiverkossa. Kolmantena ominaisuutena RADIUS-protokolla tilastoi käyttäjän toimia langattomassa lähiverkossa ja kirjaa tiedot tämän jälkeen tietokantaan. Nämä kolme RADIUS-protokollan palvelua tunnetaan paremmin AAA (Authentication, Authorization & Accounting) -palveluna. (Hassel, J. 2002. 2-4.)

RADIUS-todentamisprosessissa on normaalisti mukana käyttäjän päätelaite, RADIUS-asiakas ja RADIUS-palvelin. Käyttäjän päätelaite langattomassa lähiverkossa on yleensä asiakkaan käyttämä tietokone. RADIUS-asiakkaana toimii laite, johon käyttäjä ottaa langattomasti yhteyden esimerkiksi WRT610N langaton reititin. RADIUS palvelimena voi toimia palvelin, joka sisältää ominaisuudet AAA-palveluiden käsittelyyn. (Hassel, J. 2002. 3.)

RADIUS-todentamisprosessi alkaa käyttäjän päätelaitteen lähettämällä tunnistuspyynnöllä RADIUS-asiakkaalle. RADIUS-asiakas muodostaa normaalilla periaatteella tunnistuksen käyttäjän ja asiakkaan välillä. RADIUS-asiakas muodostaa tämän jälkeen Access-Request paketin, joka sisältää kaiken mahdollisen tiedon käyttäjän päätelaitteesta, joka yrittää kirjautua verkkoon. Jos RADIUS-palvelimelta ei saada vastausta pakettiin, voidaan paketti lähettää uudestaan palvelimelle tietyn ajan jälkeen. Access-Request paketti voidaan lähettää myös vaihtoehtoiselle RADIUS-palvelimelle, jos ensisijaiselta palvelimelta ei saada vastausta tietyn aikamääreen sisällä. (Microsoft Corporation. 2008.)

RADIUS-palvelimen saatua Access-Request pyynnön, tarkistaa palvelin, onko pyyntö saapunut palvelimen pariksi konfiguroidulta RADIUS-asiakkaalta. Jos Access-Request pyyntö on saapunut oikealta taholta, tarkistaa RADIUS-palvelin tarvitaanko palvelimen ja RADIUS asiakkaan väliseen yhteyteen yhteistä salausavainta. Jos salausavainta tarvitaan yhteyden hyväksymiseen, tarkistetaan vastaako pyynnön mukana tullut avain yhteistä salausavainta. (Microsoft Corporation. 2008.)

Kun yhteys on varmistettu RADIUS-palvelimen ja RADIUS-asiakkaan välillä, alkaa palvelin tarkistaa Access-Request pyynnön mukana saapuneita tietoja käyttäjän päätelaitteesta. Jos nämä tiedot vastaavat RADIUS-

palvelimella olevia tietoja hyväksytyistä käyttäjistä, liitetään käyttäjälle määritellyt käyttäjäasetukset Access-Accept viestiin. Viesti lähetetään tämän jälkeen RADIUS-asiakkaalle joka hyväksyy yhteyden muodostamisen käyttäjän päätelaitteelle. (Microsoft Corporation. 2008.)

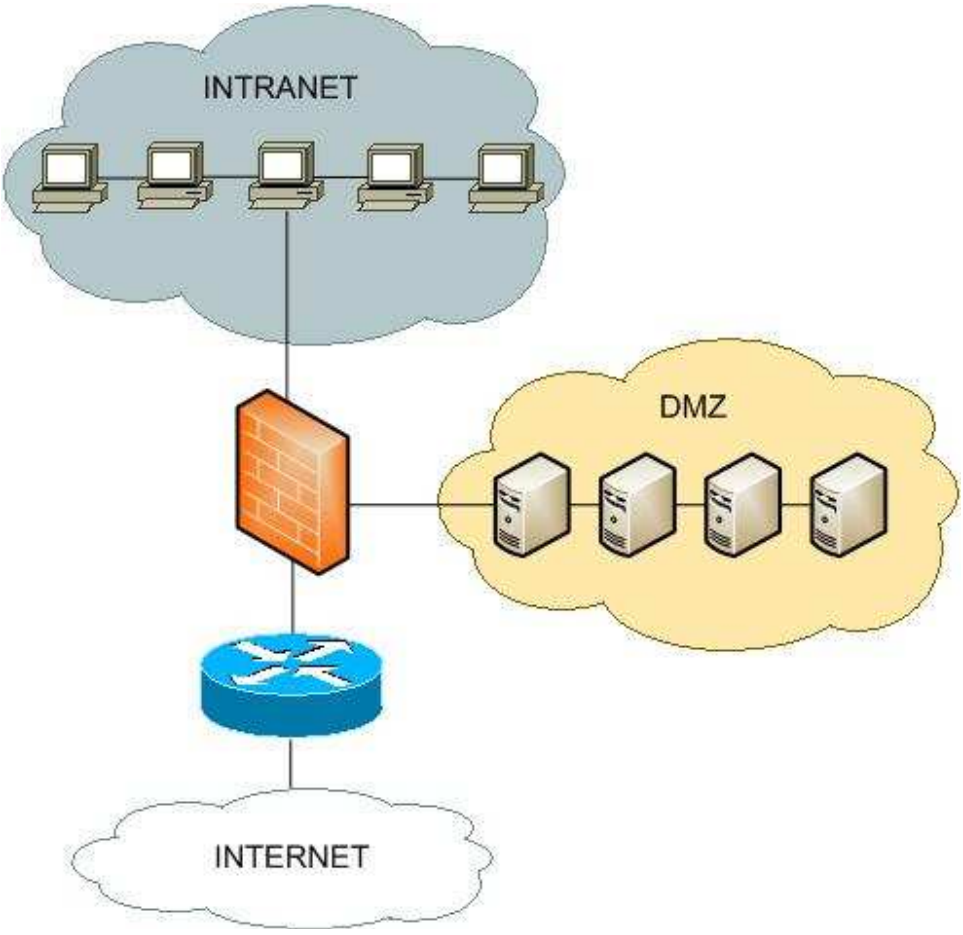
Jos Access-Request pyynnön mukana saapuneet tiedot eivät täsmää RADIUS-palvelimen käyttäjätietokannan tietojen kanssa hyväksytyistä käyttäjistä, lähettää palvelin tämän jälkeen Access-Reject pyynnön RADIUS-asiakkaalle. Tämän jälkeen RADIUS-asiakas lähettää käyttäjän päätelaitteelle tiedon, että todentaminen on epäonnistunut, ja pääsy verkkoon on evätty. (Microsoft Corporation. 2008.)

2.4 DMZ - Demilitarized Zone

DMZ:n (Demilitarized Zone) tarkoitus on luoda yksi tietoturvataso lisää organisaation lähiverkkoon. Sillä eristetään ulkopuolisia käyttäjiä palvelevat palvelimet organisaation haavoittuvasta intranetistä. Näin voidaan tarjota turvallisesti palvelimien tarjoamia palveluita ulkopuolisille käyttäjille ilman pelkoa, että organisaation oma intranet vaarantuisi.

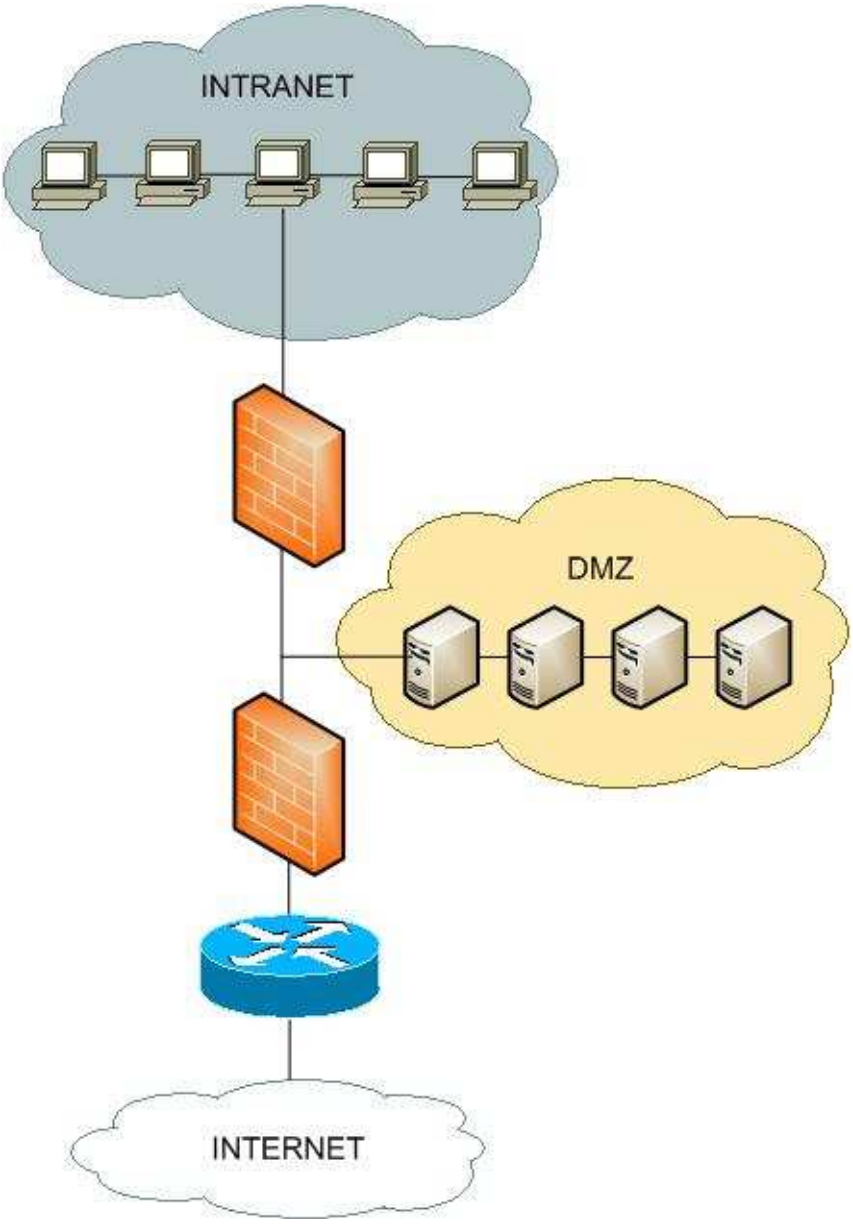
Lähiverkon haavoittuvaisempia kohtia ovat ne, joihin on pääsy lähiverkon ulkopuolelta. Yrityksellä täytyy olla kuitenkin mahdollisuus tarjota ulkopuolisille käyttäjille palveluita, kuten DNS-, sähköposti-, Internet-, FTP- tai muita yrityksen palvelimien palveluita. Näitä samoja palveluita käyttävät myös organisaation intranetin käyttäjät. Tästä syystä DMZ:n tarkoitus on luoda oma aliverkko näille palvelimille, jotka palvelevat sekä intranetin että ulkopuolisia käyttäjiä. Vaikkakin ulkopuolisilla käyttäjillä on pääsy palvelimia sisältävään aliverkkoon ja he pääsisivät murtautumaan sen sisältämiin tietoihin, ei heillä ole pääsyä intranetin käyttäjien tietoihin.

DMZ:n aliverkko voidaan eristää joko yhden tai kahden palomuurin avulla. Yhden palomuurin tekniikassa sama palomuuri käsittelee sekä intranetin että demilitarisointi alueelle menevän liikenteen. Tämä tekniikka on yksinkertainen ja halvempi toteuttaa, mutta se ei tuo samanlaista tietoturvatasoa kuin kahden palomuurin tekniikka. Kuvassa 1 on havainnollistettu verkko, jossa on käytetty yhtä palomuuria DMZ:n rakentamiseen.



KUVA 1 *DMZ -verkko yhdellä palomuurilla*

Kahden palomuurin tekniikassa ensimmäinen palomuuri käsittelee sekä intranetin että demilitarisointi alueelle menevää liikennettä. Toinen palomuuri käsittelee ainoastaan intranetin ja siitä ulospäin suuntautuvaa liikennettä. Kahden palomuurin tekniikka luo suuremman tietoturvatason kuin käytettäessä yhtä palomuuria. Toteutus on monimutkaisempi ja kalliimpi toteuttaa verrattuna yhden palomuurin tekniikkaan. Kuvassa 2 on havainnollistettu verkko, jossa on käytetty kahta palomuuria DMZ:n rakentamiseen.



KUVA 2 *DMZ -verkko kahdella palomuurilla*

Nykyään kotikäyttöön tarkoitetut reitittimet sisältävät niin sanotun DMZ-isäntä ominaisuuden. Tällä tarkoitetaan laitetta, johon kaikki portit, joita ei ole toisin määritelty ovat avoinna. Tämä ei sinänsä täytä DMZ:n määritelmää, koska se ei luo uutta tietoturvatasoa eikä erillistä aliverkkoa intranetin ja DMZ-isännän välille. Tässä tekniikassa DMZ-Isännällä on myös mahdollisuus ottaa suoraan yhteyttä intranetin sisältämiin laitteisiin. Normaalissa DMZ-verkossa palomuuri olisi suodattamassa tämän liikenteen intranetin ja DMZ-Isännän väliltä. (Kerttula, E. 1999. 259-260.)

2.5 4G - matkaviestijärjestelmät

2.5.1 Long Term Evolution - LTE

Nykyisissä kolmannen sukupolven 3G matkaviestintäjärjestelmissä on datapalveluiden käyttö kasvanut huomattavasti lähivuosien aikana. Tämä on osaltaan kasvattanut tarvetta kehittää yhä suuremman datanopeuden omaavia matkajärjestelmätekniikoita tulevaisuuden tarpeisiin. LTE (Long Term Evolution) tekniikan on kaavailtu olevan siltana kolmannen sukupolven 3G matkaviestijärjestelmistä neljännen sukupolven 4G matkaviestintäjärjestelmiin. Tavoitteena on, että datanopeudet jopa kymmenkertaistuisivat 3G tekniikkaan verrattuna. (Penttinen, Prosessori Lehti, 25.)

Monien mielestä LTE ei ole saavuttamassa vielä omilla teknillisillä ratkaisuillaan neljännen sukupolven matkaviestintäjärjestelmän 4G-arvonimeä. Vasta LTE:n rinnalla kehitteillä oleva LTE-Advanced matkaviestintäjärjestelmä olisi saamassa seuraavan sukupolven 4G-arvonimen. LTE matkaviestintäjärjestelmätekniikkaa kutsutaankin nykyisin 3.9G matkaviestintäjärjestelmätekniikaksi. (Penttinen, Prosessori Lehti, 24-25.)

LTE-tekniikan tavoitteina on 150 - 300 Mb/s:n teoreettinen datanopeus ja UMTS (Universal Mobile Telecommunications System) -verkoissa olevan 100 - 150 ms:n latenssin pienentäminen noin kymmenesosaan. LTE toimisi 1,4 - 20 MHz:n kaistaleveydellä, jolla pystyttäisiin toteuttamaan tavoitteena oleva teoreettinen datanopeus. (Penttinen, Prosessori Lehti, 25) LTE-tekniikka ei tule olemaan piirikytkentäinen järjestelmä, koska piirikytkentäisten järjestelmien merkitys on vähenemässä jatkuvasti. Se on tarkoitettu täten pelkästään pakettimuotoisille datasovelluksille. Puhepalveluita se pystyy kuitenkin toteuttamaan VOiP (Voice Over Internet Protocol) -tekniikkaa avuksi käyttäen. (Penttinen, Prosessori Lehti, 28.)

LTE-tekniikkaa pyritään toteuttamaan siten, että se olisi yhteensopiva edeltäjänsä HSPA (High-Speed Packet Access) -tekniikan ja sen johdannaisten tekniikoiden kanssa. LTE-tekniikka ei eroa merkittävästi uusimmista HSPA-tekniikoista, joten LTE-tekniikan oletetaan tulevan hyvinkin pian markkinoille. Ensimmäisiä prototyyppejä LTE-matkapuhelimista on jo esitelty julkisuuteen. Tavoitteena olisi, että LTE-verkkoja olisi toiminnassa laajemmalti vuoden 2010 loppuun mennessä. (Penttinen, Prosessori Lehti, 25.)

2.5.2 Long Term Evolution Advanced - LTE-A

Neljännen sukupolven 4G matkaviestintäjärjestelmistä puhuttaessa, nousee esiin vasta suunnitteluasteella oleva LTE-A (Long Term Evolution Advanced) -tekniikka. Sen tavoitteet ovat jo päätä huimaavia tiedonsiirron ja tiedonsiirtoviipeen osalta. Siinä missä LTE-tekniikan tavoitteena oli teoreettisen datanopeuden osalta 150 - 300 Mb/s, niin LTE-A-tekniikan tavoite on niinkin huima kuin yhden gigabitin huippunopeus downlink-siirtosuunnassa. Uplink-suunnassakin nopeuden suunnitellaan olevan puo-

let downlink-siirtosuunnan nopeudesta, eli teoriassa noin 500Mb/s. (Penttinen, Prosessori Lehti, 25.)

Yhtä tärkeänä osana matkaviestijärjestelmissä, teoreettisen datanopeuden nostamisen kanssa, on latenssin pienentäminen. LTE-A-tekniikan tavoitteena onkin latenssin pienentämisen 50 millisekuntiin merkinannon ja 5 millisekuntiin yhdensuuntaisen radioliikenteen osalta. Jo näiden teknisten parannusten osalta LTE-A-tekniikka onnistuisi kolminkertaistamaan kapasiteettivaatimuksen LTE-tekniikkaan verrattuna. Pelkästään suuren kapasiteetin kasvattaminen ei takaa suurta suosiota matkaviestintäjärjestelmämarkkinoilla. Työryhmän tavoitteena onkin, että LTE-A-tekniikka olisi mahdollisimman yhteensopiva LTE-tekniikan kanssa. (Penttinen, Prosessori Lehti, 25.)

Jotta näihin tavoitteisiin päästäisiin, tulee työryhmän kehitellä uusia tekniikoita, joilla kapasiteettia ja latenssia saadaan parannettua. Uusina mahdollisina tekniikoina ollaan suunnittelemassa taajuuskaistan kasvattamista maksimaalisesta kahdestakymmenestä megahertsistä sataan megahertsiin. Tämä pystytään toteuttamaan yhdistelemällä eri kaistalohkoja yhdeksi loogiseksi kaistalohkonipuksi. (Penttinen, Prosessori Lehti, 26.)

Kapasiteettitavoite LTE-A-tekniikalle tarkoittaa käytännössä sitä, että downlink-suunnassa tukiaseman pitäisi pystyä siirtämään 30 bittiä sekunnissa ja päätelaitteen 15 bittiä sekunnissa hertsiä kohden. Tämä vaatii siis nykyisiin tekniikoihin verrattuna huomattavasti parempaa spektritehokkuutta. (Penttinen, Prosessori Lehti, 26.)

Oleellisena osana tavoiteltaessa LTE-A-tekniikan datanopeuksia on MIMO-tekniikan käyttäminen. MIMO-tekniikassa käytetään useita antenneja tiedonsiirron lähetykseen sekä vastaanottoon. LTE-A-järjestelmä tukisi jopa kahdeksan yhtäaikaisen antennin käyttöä ja täten käyttäisi tyypiltään 8x8 MIMO-tekniikkaa. Bittinopeuden on tutkittu moninkertaistuvan suhteessa antennien määrään. Antennimäärän kuitenkin kasvaessa suureksi, aiheuttaa se myös häviötä signaalien häiritessä toisiaan, joten loputtomasti antennien määrää ei voi kasvattaa. (Penttinen, Prosessori Lehti, 26.)

Yksi suunnitteilla olevista kehityskohdista LTE-A-tekniikassa on erillisten toistinelementtien (Relay nodes) käyttö. Toistinelementtien käyttö parantaisi erityisesti katvealueiden suorituskykyä. Toistinelementtien avulla katvealueiden datasiirtonopeuksia pystyttäisiin kasvattamaan jopa 50 prosenttia. Toistinelementtien käyttö ei vaatisi erityisiä muutoksia LTE-A-verkkorakenteeseen, vaan toistinelementtejä voisi lisätä niille alueille missä suorituskyky kärsisi katvealueiden takia. (Penttinen, Prosessori Lehti, 27.)

Aika näyttää, millaisen lopullisen muodon LTE-A-tekniikka tulee saavuttamaan. Melko varmaa kuitenkin on, että LTE-A tullaan rakentamaan LTE-tekniikan päälle. Se on kuitenkin arvoitus, että miten nopealla aikataululla tämä pystytään toteuttamaan. Vielä on monia teknillisiä ratkaisuja, joita työryhmien on lyötävä lukkoon, ennen kuin lopullinen konsepti LTE-A-tekniikasta on julkaisukelpoinen. Hyvin varmaa on kuitenkin se, että LTE-A-tekniikka tulee olemaan yksi niistä tekniikoista, jotka täyttävät

neljännen sukupolven 4G matkaviestintäjärjestelmän määritykset. (Penttinen, Prosessori Lehti, 27)

3. WRT610N OMINAISUUDET

WRT610N on yksi Linksysin valmistamista langattomista reitittin malleista. Se eroaa vanhempiin malleihin verrattuna siinä, että sen tekniikka tukee IEEE 802.11n-standardia. Se tukee sekä 2.4 että 5 GHz:n taajuuksia ja mahdollistaa myös näiden yhtäaikaisen käytön. Langattoman verkon ominaisuuksia voidaan täten tarjota sekä 2,4 että 5 GHz:n taajuuksia käyttäville päätelaitteille ilman, että ne häiritsevät toisiaan. (Linksys, Data Sheet, 1-2.) Samalla sen sisäänrakennettu palomuuri pitää huolta langallisen sekä langattoman tietoliikenteen tietoturvallisuudesta. Palomuurin lisäksi WRT610N sisältää lukuisia muita tietoturvallisuuteen liittyviä ominaisuuksia. Kuvassa 3 on nähtävissä, miltä WRT610N langaton reititin näyttää. (Linksys, User Guide, 18.)

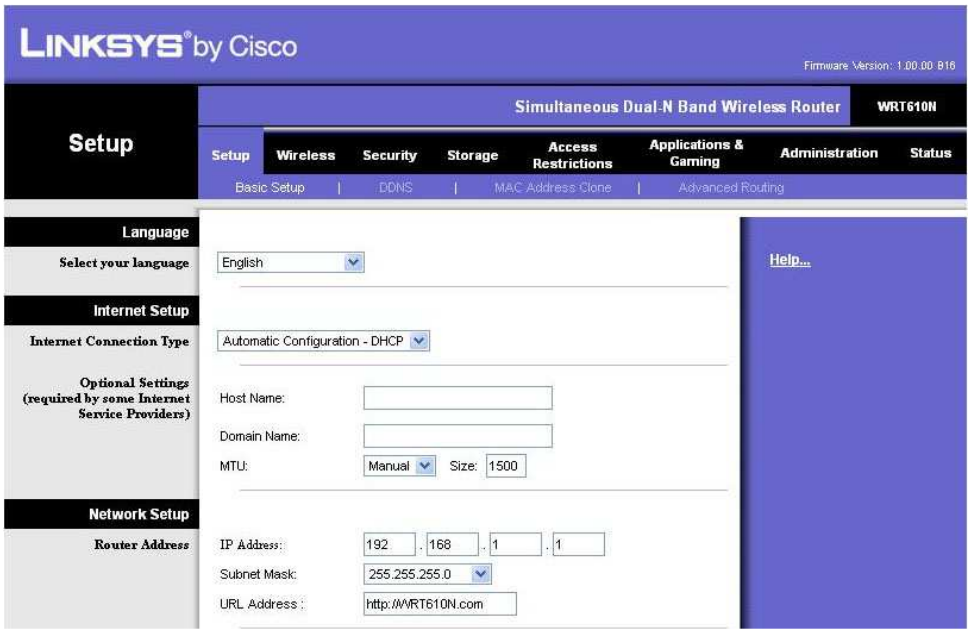
WRT610N sisältää myös USB (Universal Serial Bus)-portin, johon voidaan liittää erillinen ulkoinen kovalevy tai muistitikku. Tämä mahdollistaa erillisen media- tai FTP (File Transfer Protocol) -palvelimen jakamisen verkon käyttäjille. Tällä tavoin voidaan myös luoda vaivattomasti yhteinen verkkoasema esimerkiksi tiedostojen jakamista tai varmuuskopiointia varten. (Linksys, User Guide, 19-21.)

Langaton reititin sisältää myös lukuisia ominaisuuksia, jotka on tarkoitettu erilaisille sovelluksille ja peleille. Sovelluksien ja pelien osalta langattomalla reitittimellä voidaan ohjata tietyt ohjelmat olemaan yhteydessä johonkin tiettyyn päätelaitteeseen tai palvelimeen. Myös langattomaan reitittimeen voidaan priorisoida sovittujen sovelluksien tärkeys, jotta niiden palvelut voidaan taata käyttäjille tietoliikennekapasiteetin ollessa täydessä käytössä. (Linksys, User Guide, 25-26.)

KUVA 3 *WRT610N langaton reititin*

4. ASETUKSET (SETUP)

WRT610N käyttöönotto tulee aloittaa langattoman reitittimen kytkemisellä tietokoneeseen ja sähköverkkoon. Pakkauksen mukana tulevan CD:n avulla voidaan asentaa langaton reititin toimintavalmiuteen yksinkertaisen, ohjatun toiminnon avulla. Ohjatun toiminnon asetukset keskittyvät perusasetuksiin, joilla voidaan mahdollistaa Internet yhteyden toimivuus niin langallisille kuin langattomille työasemille. Tässä opinnäytetyössä keskitytään perusasetusten lisäksi myös perusteellisempiin asetuksiin, joita ei voi muokata ohjatun toiminnon avulla. Jotta mahdollistettaisiin pääsy monipuolisempiin asetustyökaluihin, tarvitsee käyttäjän muodostaa etäyhteys suoraan langattoman reitittimen hallinnointisivulle. Etäyhteys muodostetaan langattoman reitittimen hallinnointisivulle ottamalla yhteyttä reitittimen omaan IP-osoitteeseen WWW-selaimen avulla. Kuvassa 4 on esitetty langattoman reitittimen hallinnointisivun käyttöliittymän rakenne. (Linksys, User Guide, 6.)



KUVA 4 *WRT610N langattoman reitittimen hallinnointisivu*

4.1 Perusasetukset (Basic Setup)

Perusasetuksista voidaan määritellä yksinkertaisia, mutta langattoman reitittimen käytön kannalta tärkeitä asetuksia. Näitä perusasetuksia on mahdollista muokata myös ohjatun toiminnon avulla. Ensimmäisenä asetuksena sivulta on mahdollista valita hallinnointisivuston kieli. Langattoman reitittimen hallinnointisivuston oletuskieli on englanti, mutta vaihtoehtoja ovat esimerkiksi ranska, espanja tai ruotsi. Suomenkieltä ei ole mahdollista valita asennussivuston kieleksi WRT610N mallissa. (Linksys, User Guide, 6.)

Langattoman reitittimen Internet asetukset-kohdasta voidaan valita se yhteystapa, jolla on tarkoitus muodostaa yhteys Internetiin. Vaihtoehtoja on yhteensä kuusi, joista yleisimmät ovat automaattinen konfigurointi

DHCP:tä (Dynamic Host Configuration Protocol) tai kiinteää IP (Internet Protocol) -osoitetta hyväksi käyttäen. WRT610N käyttää oletuksena Internet yhteyden muodostamiseen konfigurointia DHCP:n avulla. Tämä vaatii kuitenkin sen, että Internet palveluntarjoaja tukee tätä ominaisuutta. Nykypäivänä Internet palveluntarjoajat lähes poikkeuksetta tukevat kyseistä protokollaa. Toinen yleinen tapa on käyttää kiinteää IP-osoitetta muodostettaessa Internet yhteyttä. Jos Internet yhteys halutaan muodostaa kiinteää IP osoitetta hyväksi käyttäen, täytyy asetussivustolle määritellä silloin Internet palveluntarjoajan luomat tiedot IP-osoitteesta, aliverkon peitteestä, oletus yhdyskäytävästä ja DNS:stä (Domain Name System). (Linksys, User Guide, 6-7.)

Verkkoasetukset kohdasta on mahdollista määrittää IP-osoite, jolla otetaan yhteyttä verkkokaapelin avulla langattoman reitittimen hallinnointisivulle. IP-osoitteen voi myös korvata selkokielisellä Internet osoitteella, esimerkiksi http://minunreititin.com. (Linksys, User Guide, 9.)

Verkko-osoitepalvelimen asetukset kohdasta on mahdollisuus määrittää reitittimen DHCP:n asetuksia. Tästä kohdasta voidaan määrittää, onko DHCP-palvelu käytössä vai ei. Jos DHCP palvelua päätetään käyttää, on tärkeää, ettei verkossa ole muita DHCP-palveluita yhtäaikaisesti käytössä. Jos DHCP-palvelua käytetään, voidaan sen IP-osoiteavaruus määrittää myös asetuksista. Ensin tulee valita IP-osoite, josta aloitetaan dynaamisten IP-osoitteiden määrittäminen. Tämän jälkeen voidaan määrittää reitittimelle yhtäaikaisten käyttäjien maksimimäärä. Kun nämä asetukset määritetään reitittimelle, laskee reititin automaattisesti IP-osoiteavaruuden, josta DHCP-palvelu jakaa päätelaitteille käytettävissä olevia IP-osoitteita.

Lainausaika-kohdasta voidaan määrittää, kuinka kauan käyttäjän päätelaitteelle lainataan määriteltyä IP-osoitetta. Haluttu lainausaika syötetään minuuttiarvona asetussivulle. Jos määritelty aika on mennyt umpeen, kun päätelaite yrittää muodostaa yhteyttä uudelleen Internetiin, määritellään sille uusi vapaa IP-osoite sovitusta osoiteavaruudesta.

Jos ei haluta käyttää Internet palveluntarjoajan oletus DNS-palvelua, niin kiinteiden DNS-osoitteiden kohtaan voidaan määrittää yhdestä kolmeen erillistä DNS-palvelimen IP-osoitetta. Jos halutaan käyttää ainoastaan palveluntarjoajan oletus DNS-palvelinta, voidaan nämä kolme riviä jättää silloin tyhjäksi. (Linksys, User Guide, 9.)

DHCP:n IP-osoitevarausominaisuudesta voidaan lukita IP-osoitteita tietyille päätelaitteille. Tällöin asetetaan tietyille IP-osoitteille haluttujen päätelaitteiden verkkokortin MAC (Media Access Control) -osoitteet. Näin langaton reititin tietää varata nämä IP-osoitteet näille kyseisille päätelaitteille eikä lainaa niitä mihinkään muuhun käyttöön. Kuitenkin on huomioitava, että halutut IP-osoitteet voidaan varata ainoastaan määritellyn IP-osoiteavaruuden joukosta.

Aikavyöhykeasetuksista voidaan määrittää, millä aikavyöhykkeellä langaton reititin on käytössä. Tämä asetus on tärkeä, jos myöhemmässä vaiheessa määritellään Internet rajoituksia päivämäärien ja aikojen perusteella. (Linksys, User Guide, 10.)

4.2 MAC- osoiteklooni (Mac Address Clone)

Jotkin Internet palveluntarjoajat vaativat käytössä olevan verkkosovittimen MAC-osoitteen rekisteröimistä heidän tietokantaansa, ennen kuin Internet yhteyden luominen on mahdollista. Jos käyttäjä on aikaisemmin rekisteröinyt jonkin toisen kuin tällä hetkellä käytössä olevan verkkosovittimen MAC-osoitteen tietokantaan, voidaan langaton reititin määrittää käyttämään tätä vanhaa MAC-osoitetta tunnistuksessa. Tällöin ei ole tarvetta rekisteröidä uutta MAC-osoitetta tietokantaan, vaan palveluntarjoaja tunnistaa tutun käyttäjänsä MAC-osoiteklooni ominaisuudessa olevan vanhan MAC-osoitteen avulla. (Linksys, User Guide, 11.)

4.3 Kehittynyt reititys (Advanced Routing)

Kehittyneen reitityksen asetuksilla voidaan luoda erilaisia reititysmahdollisuuksia, riippuen verkon rakenteesta. Jos langatonta reititintä käytetään isännöimään liikennettä suoraan Internetiin, tulee asetuksissa olla valittuna NAT (Network Address Translation) -ominaisuus päällä. Tämä on myös langattoman reitittimen oletusasetus. Jos taas langatonta reititintä käytetään yhtenä muusta verkon reitittimistä, tulee NAT-ominaisuus kytkeä pois päältä. Tämän jälkeen langattomalle reitittimelle on mahdollista määritellä RIP (Routing Information Protocol) -ominaisuuksia.

Dynaaminen reititys RIP mahdollistaa langattoman reitittimen mukautumisen verkon muutoksiin automaattisesti ja jakaa reititystietoja muiden reitittimien kanssa. RIP määrittää lyhyimmän mahdollisen reitin tietoliikenteelle hyppylukujen perusteella. Hyppyluvuilla määritellään, kuinka pitkä matka tietyllä reitittimellä on määriteltyyn määränpäähän. Dynaaminen reititys RIP on oletuksena pois päältä reitittimestä.

Reititys reitittimien välillä voidaan määrittää verkossa myös manuaalisesti kiinteällä reitityksellä. Tällöin pitää määrittää konfiguroitavalle langattomalle reitittimelle muiden verkossa olevien reitittimien tietoja. Näitä tietoja ovat esimerkiksi kohdereitittimen IP-osoite, aliverkon peite, hyppyluku, yhdyskäytävä ja liitäntätyyppi. Liitäntätyypeistä on mahdollisuus valita joko lähiverkko & langaton verkko tai WAN (Wide Area Network) -verkko. Reititystauluominaisuus mahdollistaa reitittimelle määriteltyjen reitityksien tarkastelemisen. (Linksys, User Guide, 11-12.)

5. LANGATON VERKKO (WIRELESS)

5.1 Langattoman verkon perusasetukset (Basic Wireless Settings)

Langattoman verkon perusasetukset voidaan luoda WRT610N langattomalle reitittimelle joko manuaalisesti tai WPS (Wi-Fi Protected Setup) -toiminnon avulla. Langattoman reitittimen oletusasetuksena on langattoman verkon asetuksien määrittäminen WPS:n avulla. Jos langattoman verkon asetukset halutaan määrittää manuaalisesti reitittimelle, tulee asetuksista silloin valita ensimmäiseksi manuaaliasetus -valinta.

5.1.1 Wi-Fi Protected Setup - WPS

Jos langattoman verkon asetukset halutaan määritellä WPS-toiminnon avulla, silloin täytyy käyttäjän langattoman verkkosovittimen tukea WPS-standardia. WRT610N tukee kahta erilaista tapaa määrittää langattoman verkon asetukset WPS:n avulla.

Ensimmäisessä vaihtoehdossa käyttäjän langattomasta verkkosovittimesta painetaan painiketta, joka alkaa lähettää sen tietoja perusasetuksista radiosignaaleina. Tämän jälkeen langattoman reitittimen asetussivustolta painetaan painiketta, joka asettaa reitittimen etsimään radiosignaaleja käyttäjien langattomista verkkosovittimista. Kun langaton reititin vastaanottaa nämä signaalit, saadaan langattoman verkon perusasetukset helposti asetettua oikeaksi reitittimelle.

Toisessa vaihtoehdossa asetukset voidaan määritellä PIN (Personal Identification Number) -tunnistenumeroa käyttäen. Jos käyttäjän langaton verkkosovitin tukee WPS-standardia, niin sen pakkauksessa tai itse laitteessa tulisi lukea PIN-tunnistenumero. Kun tämä PIN-tunnistenumero syötetään langattoman reitittimen hallinnointisivulla sijaitsevaan syötekenttään, saadaan langattoman verkon perusasetukset täten määritettyä. Tarvittaessa käyttäjän langattomalle verkkosovittimelle pitää myös syöttää langattoman reitittimen PIN-tunnistenumero. (Linksys, User Guide, 13.)

5.1.2 Perusasetuksien määrittäminen (Wireless Configuration)

WRT610N langattomalle reitittimelle voidaan määritellä langattoman verkon asetukset manuaalisesti erikseen 2.4 ja 5 GHz:n taajuusalueen verkoille. Molemmat verkot ovat tällöin käyttäjien käytössä riippuen siitä, mitä standardia käyttäjä haluaa hyödyntää. (Linksys, User Guide, 12.)

Hallinnointisivulle voidaan määritellä mitä langattoman lähiverkon IEEE 802.11 standardia kullakin taajuusalueen verkolla voidaan käyttää reitittimessä. 5 GHz:n taajuusalueelle on mahdollisuus määrittää 802.11a ja 802.11n standardin käyttömahdollisuudet. 2.4 GHz:n taajuusalueelle on mahdollista määritellä 802.11b, 802.11g ja 802.11n standardin käyttömahdollisuudet. Jos langattomalle reitittimelle on määritelty useamman standardin käyttömahdollisuus, osaa langaton reititin tunnistaa, mitä standardia käyttäjä pyrkii hyödyntämään muodostaessaan yhteyttä langattomaan verkkoon. Langaton reititin pystyy myös vaihtamaan senhetkiselle tietoliikenteelle sopivan standardin automaattisesti. (Linksys, User Guide, 12.)

Langattomalle lähiverkolle voidaan määritellä myös SSID (Service Set Identifier) -tunniste, jolla tunnistetaan kyseinen langaton lähiverkko muista samalla alueella toimivista langattomista lähiverkoista. Tietoturvasyistä SSID-tunnus kannattaa muuttaa alkuperäisestä tunnuksesta omaperäiseksi lähiverkon tunnukseksi. (Linksys, User Guide, 12.) Asetuksista voidaan määritellä myös, mainostetaanko SSID-tunnusta yleisesti lähiverkon pää-

telaitteille. Jos mainostamisen ottaa pois käytöstä, ei lähiverkon tunnusta ole nähtävissä päätelaitteiden verkkoluetteloissa. Oletuksena langattomassa reitittimessä mainostetaan SSID-tunnusta langattoman verkon päätelaitteille. (Linksys, User Guide, 13.)

Hallinnointisivun asetuksista on mahdollista määritellä myös tarkkaan taajuusalueen kanava, jota hyödyntämällä langaton yhteys muodostetaan päätelaitteelle. Oletuksena langaton reititin kuitenkin määrittelee automaattisesti taajuusalueen kanavan kullekin yhteydelle. 802.11n standardia käytettäessä on mahdollista valita käytetäänkö yhteyden muodostamiseen 20 vai 40 MHz:n laajuisia kanavia yhteyksiä muodostettaessa. (Linksys, User Guide, 12.)

5.2 Langattoman verkon tietoturva (Wireless Security)

Wireless Security -sivulta voidaan määritellä langattomassa verkossa käytettävät tietoturva-asetukset. Ensimmäisenä asetuksena määritellään, mitä langattomaan verkkoon soveltuvaa tietoturvatekniikkaa halutaan käyttää langattoman tietoliikenteen salaamiseen. WRT610N langaton reititin tukee WPA-Personal, WPA2-Personal, WPA-Enterprise, WPA2-Enterprise, WEP ja RADIUS tietoturvatekniikoita. Langattomalle tietoliikenteelle voidaan määritellä myös, ettei se käytä mitään tietoturvatekniikkaa langattoman tietoliikenteen salaamiseen, mutta tämä ei ole suotavaa.

Tietoturvamääritykset voidaan suorittaa erikseen 2.4 tai 5 GHz käyttäville verkoille. Esimerkiksi 2.4 GHz:n verkko voidaan asettaa salaamaan tietoliikenteensä WPA-Personal salaustekniikalla, kun taas 5 GHz:n verkko WPA2-Personal salaustekniikalla.

WEP-salaustekniikkaa käytettäessä määritellään ensin halutaanko salausavaimen koodaus suorittaa 40/64 vai 104/128 bitin salauksella. Tämän jälkeen asetuksiin voidaan määritellä salausavain, joka syötetään hallinnointisivulle. Generate-painikkeesta langaton reititin generoi tämän jälkeen salausavaimesta neljä koodattua salausavainta langattoman tietoliikenteen käyttöön. TX Key-valikosta voidaan valita avain, jota halutaan käyttää senhetkisen tietoliikenteen salaamiseen.

WPA2-Personal salaustekniikkaa käytettäessä määritellään ensin halutaanko salausalgoritmina käyttää AES vai WPA-TKIP/WPA2-AES tietoturvaprotokollaa. Tämän jälkeen langattomalle reitittimelle voidaan syöttää salausavain, jota halutaan käyttää langattoman tietoliikenteen salaamisessa. Salausavaimen täytyy olla enemmän kuin kahdeksan merkkiä pitkä, mutta se ei saa olla pidempi kuin 63 merkkiä pitkä. Asetuksiin voidaan määritellä aika, kuinka usein langaton reititin vaihtaa salatut avaimet. Oletuksena WPA2-Personal salaustekniikka vaihtaa salatut avaimet 3 600 sekunnin välein. WPA-Personal salaustekniikka sisältää samat asetukset kuin WPA2-Personal, mutta salausalgoritmivaihtoehtoina ovat AES tai TKIP tietoturvaprotokollat.

WPA2-Enterprise salaustekniikkaa käytettäessä määritellään samat asetukset kuin WPA2-Personal salaustekniikkaa käytettäessä. Lisäksi määri-

tellään käytettävän RADIUS-palvelimen IP-osoite ja käytettävän TCP protokollan porttinumero. WPA-Enterprise eroaa WPA2-Enterprise asetuksista ainoastaan salausalgoritmivaihtoehdoissa.

RADIUS-salaustekniikkavaihtoehtoa käytetään silloin, kun lähiverkossa halutaan käyttää RADIUS-palvelinta, ja jos salaus reitittimen ja langattoman päätelaitteiden välillä halutaan suorittaa yksinkertaisella WEP-salaustekniikalla. Asetuksiin tarvitsee ensiksi asettaa RADIUS-palvelimen IP-osoite ja käytettävän TCP protokollan porttinumero. Tämän jälkeen asetetaan asetuksiin jaettuavain, jota käytetään langattoman reitittimen ja RADIUS-palvelimen välillä. Tämän jälkeen määritellään WEP-salaustekniikassa käytettävät salausasetukset. (Linksys, User Guide, 14-16.)

5.3 Langattoman verkon MAC - suodatus (Wireless MAC Filter)

Käyttäjien langattoman verkon käyttöä voidaan rajoittaa MAC-osoitteiden avulla. Langattomasta reitittimestä voidaan joko sallia tai estää tiettyjen käyttäjien langattoman verkon käyttöä MAC-osoitteita hyväksi käyttäen. Käyttäjien MAC osoitteet voidaan lisätä listaan joko kirjoittamalla ne suodatusriveille manuaalisesti, tai osoitteet voidaan helposti poimia langattoman verkon käyttäjien listasta. Langattoman verkon käyttöä ei ole rajoitettu MAC-osoitteiden perusteella oletuksena.

Käyttäjien suodatukseen on kaksi erilaista vaihtoehtoa. Ensimmäisessä vaihtoehdossa reitittimelle lisätään MAC-osoitteita, joille halutaan antaa oikeus käyttää langatonta verkkoa. Tällöin haluttujen käyttäjien verkkosovittimien MAC-osoitteet lisätään reitittimen MAC-suodatuslistaan ja annetaan lupa käyttää langatonta verkkoa. Käyttäjien, joiden MAC-osoite ei löydy MAC-suodatuslistasta, langattoman verkon käyttö on silloin estetty. Toinen mahdollisuus on listata niiden käyttäjien verkkosovittimien MAC-osoitteet suodatuslistaan, joiden käyttö halutaan estää langattomassa verkossa. Käyttäjien, joiden MAC-osoite ei löydy suodatuslistalta, langattoman verkon käyttöä ei ole silloin estetty. (Linksys, User Guide, 16-17.)

5.4 Langattoman verkon lisäasetukset (Advanced Wireless Settings)

WRT610N langaton reititin sisältää perusasetuksien lisäksi langattomalle verkolle monia lisäasetuksia, joilla verkon toimintaa voidaan monipuolistaa. Nämä asetukset on tarkoitettu kokeneemmille langattoman verkon ylläpitäjille. Näiden asetuksien väärinkäyttö saattaa rajoittaa tai heikentää langattoman verkon toimintaa. Jos näiden asetuksien muuttamiselle ei ole perusteltua syytä, kannattaa ne pitää silloin oletusasetuksilla. Tässä opinnäytetyössä ei sen tarkemmin perehdytä näiden lisäasetuksien sisältöön. (Linksys, User Guide, 17.)

6. TIETOTURVA (SECURITY)

6.1 Palomuuri (Firewall)

Palomuurin tehtävä langattomassa reitittimessä on suodattaa ei-halutun tietoliikenteen pääsemistä lähiverkkoon. Suodatuksen tasoa voidaan mukauttaa langattoman reitittimen palomuuriasetuksista. SPI (Stateful Packet Inspection)-palomuuri on päällä oletuksena langattomassa reitittimessä, mutta tarvittaessa sen saa kytkettyä pois päältä. Tämä ei ole kuitenkaan suositeltavaa, ellei käyttäjällä ole käytössä jotakin muuta palomuuriratkaisua lähiverkon suojelemiseksi.

Palomuuriasetuksista voidaan esimerkiksi estää TCP portin 113 käyttö tai tuntemattomien Internet pyyntöjen pääseminen langattoman reitittimen kautta. Joukkolähetyksen suodatusasetus estää useamman lähetyksen välittämisen tietyille vastaanottajille samanaikaisesti. Jos tämä estetään, niin reititin ei salli IP joukkolähetyksien välittämistä kyseisille päätelaitteille. Joukkolähetyksen suodatusasetus on pois päältä oletuksena reitittimellä. Palomuurista voidaan lisäksi estää lähiverkon koneiden etäyhteyden muodostaminen lähiverkon palvelimiin Internet- tai IP-osoitteen avulla. Tämä toiminto on pois päältä langattoman reitittimen asetuksista.

Palomuurilta voidaan estää myös tiettyjen Internet sovelluksien käyttö lähiverkosta. Mahdollisia estettäviä sovelluksia ovat Proxy-, Java-, ActiveX- ja Cookies ominaisuuksia sisältävät sovellukset. (Linksys, User Guide, 18.)

6.2 VPN yhteyksien läpikulku (VPN passthrough)

VPN (Virtual Private Network)-yhteyksien läpikulkuasetukset sallivat VPN-yhteyksien muodostamisen langattoman reitittimen kautta. WRT610N langaton reititin tukee kolmea erilaista protokollaa, IPSec (Internet Protocol Security), PPTP (Point-to-Point Tunneling Protocol) ja L2TP (Layer 2 Tunneling Protocol), joiden avulla voidaan muodostaa VPN yhteyksiä. Oletuksena langaton reititin sallii VPN yhteyksien muodostamisen sen kautta kaikilla kolmella eri protokollalla. (Linksys, User Guide, 18.)

7. MUISTIJÄRJESTELMÄ (STORAGE)

7.1 Kovalevy (Disk)

Tallennusominaisuutta langattomalla reitittimellä voidaan hyödyntää USB-liitännällä varustetulla kovalevyllä tai muistitikulla. Kun kovalevy tai muistitikku on liitetty langattomaan reitittimeen, on asetussivuston muistijärjestelmäsivulta mahdollista tutkia muistin tilaa. Muistijärjestelmän oletussivulta on mahdollista formatoida, poistaa tai tyhjentää muisti turvallisesti. Langattomaan reitittimeen liitettyä kovalevyä tai muistitikkua

formatoidessa tulee muistaa, että jos ne on alustettu aikaisemmin useampaan osioon, poistaa langaton reititin nämä aikaisemmat osiot luoden yhden ainoan osion muistille.

Muistijärjestelmän oletussivulle on kerätty tärkeitä tietoja kiinni olevasta muistista, kuten muistin jokaisen osioinnin tiedostojärjestelmästä, kapasiteetista ja vapaasta tilasta. Sivulta voidaan tarvittaessa luoda jaettavia kansioita muistille, joiden käytettävyyttä voidaan hallinnoida erilliseltä hallinnointisivulta.

Luotavalle kansiolle on annettava yksiselitteinen nimi, joka tulee näkymään käyttäjille jaettuna kansiona. Yksiselitteisen nimen lisäksi voidaan luoda kokonaan uusi osio, jos ei haluta käyttää hyväksi muistin oletusosiota tai muistiin ennestään luotuja osioita. Kansiolle on myös annettava nimi, joka näkyy fyysisesti muistin resurssienhallinnassa. Tämän kansion nimen tulee myös poiketa muista kyseisen juuren sisällä olevista kansioiden nimistä. Yhden kansion sijasta voidaan käyttäjille jakaa myös kokonainen osio muistilta.

Luoduille kansioille voidaan tämän jälkeen määritellä käyttäjäoikeuksia, joiden perusteella määritellään kenellä on lupa kansioihin. Oikeudet on jaettu oletuksena joko lukuoikeuksiin (vieraat) tai luku- ja kirjoitusoikeuksiin (pääkäyttäjät). Oikeusvaihtoehtoja on mahdollista luoda muistijärjestelmän hallinnointisivulta.

Jaettujen kansioiden listasta voidaan nähdä tarkat tiedot jo luoduista jaetuista kansioista ja osioista. Listalta voidaan muokata jaettujen kansioiden ja osioiden ominaisuuksia jälkikäteen editointi painikkeen avulla. (Linksys, User Guide, 19-20.)

7.2 Media -palvelin (Media Server)

WRT610N:n ominaisuuksiin kuuluu UPnP (Universal Plug and Play)-tekniikkaan perustuva mediapalvelin. Mediapalvelimella voidaan tarjota lähiverkon käyttäjille mediakeskus, jonka kautta käyttäjät voivat esimerkiksi kuunnella musiikkia tai katsella valokuvia. Mediapalvelimen asetuksista voidaan määrittää kansio tai osio, josta mediatiedostoja haetaan palvelimen käyttöön. Valitulle kansiolle tai osiolle voidaan määrittää tämän jälkeen selausaika, miten usein kansion tiedostot päivitetään palvelimen käyttöön. Oletuksena mediapalvelin ei ole käytössä reitittimessä. (Linksys, User Guide, 20.)

7.3 FTP -palvelin (FTP Server)

Muistijärjestelmän tiedostoja voidaan hallinnoida myös FTP-palvelimen avulla. Langattomaan reitittimeen voidaan luoda oma FTP-palvelin, johon voidaan ottaa yhteyttä lähiverkosta. Langattomalle reitittimelle voidaan mahdollistaa myös FTP-palvelimeen yhteyden ottaminen lähiverkon ulkopuolelta. Langattomasta reitittimestä voidaan määrittää, mitkä kansiot tai osiot halutaan tarjota FTP-palvelimen käyttöön. Kansioille ja osioille voidaan jakaa luku- ja kirjoitusoikeuksia käyttö tarpeen mukaan. Oletuksena

FTP-palvelin käyttää TCP:n porttia 21 yhteyden luomiseen, mutta porttia on mahdollista myös muuttaa. FTP-palvelinominaisuus ei ole langattomalla reitittimellä oletuksena päällä. (Linksys, User Guide, 21.)

7.4 Hallinnointi (Administration)

Hallinnointisivustolta löytyy palvelimen käytön kannalta oleellisia tietoja, kuten palvelimen nimi, työryhmän nimi, palvelimen lähiverkko IP-osoite ja palvelimen Internet IP-osoite. Sivun avulla voidaan luoda myös uusia käyttäjä- ja ryhmäoikeuksia oletustunnuksien lisäksi. Käyttäjille ja ryhmille voidaan jokaiselle määrittää oma salasana ja heidän luku- ja kirjoitusoikeutensa. Sivulta voidaan myös tilapäisesti sulkea käyttäjätilejä ilman, että niitä tarvitsee kokonaan poistaa tietokannasta. (Linksys, User Guide, 22-23.)

8. KÄYTETTÄVYYDEN RAJOITTAMINEN (ACCESS RESTRICTIONS)

8.1 Internet käyttörajoitukset (Internet Access)

Langattomalta reitittimeltä voidaan rajoittaa käyttäjien Internetin ja erilaisten verkkosovelluksien käyttöä monilla eri kriteereillä. Langattomalle reitittimelle voidaan luoda viisi erilaista Policy (Internet Access Policy) ehtoa, joiden perusteella joko hyväksytään tai kielletään haluttu tietoliikenne. Policy voi hyväksyä tai kieltää tietoliikenteen kulun perustuen moneen eri kriteeriin. Kriteereitä voivat olla kellonaika, viikonpäivä, Internet osoite, Internet sivun sisältämä sana, sovellus tai sovelluksen käyttämä portti. Kun on määritelty halutut Policy ehdot, voidaan nämä osoittaa koskemaan tiettyjä päätelaitteita joko MAC- tai IP-osoitteen perusteella. Päätelaitteet, joita Policy ehdot koskevat, voidaan myös määritellä tietystä IP-osoiteavaruudesta. Halutut päätelaitteet kerätään hallinnointisivun erilliselle päätelaitelistalle.

Jos Policy-ehtoihin on määritelty estettävät sovellukset tai ominaisuudet, silloin kyseiset ominaisuudet eivät toimi päätelaitteilla, jotka on lisätty päätelaitelistaukseen. Muiden käyttäjien päätelaitteilla kyseiset ominaisuudet ja sovellukset toimivat. Jos taas Policy ehtoihin on määritelty sallivat sovellukset tai ominaisuudet, silloin kyseiset ominaisuudet toimivat päätelaitteilla, jotka on liitetty päätelaitelistaan. Muiden käyttäjien päätelaitteilla kyseiset ominaisuudet ja sovellukset eivät toimi.

Jos useamman Policy-ehdon määrittelyt ovat ristiriidassa keskenään, on numerojärjestyksessä pienimmällä säännöllä aina etuoikeus. Internetin käyttöä ei rajoiteta oletuksena Policy-ehdoin millään tavoin. (Linksys, User Guide, 23-24.)

9. SOVELLUKSET JA PELAAMINEN (APPLICATIONS AND GAMING)

9.1 Tietoliikenneportin edelleen lähetys (Single Port Forwarding)

Tietoliikenneportin edelleen lähetyksellä voidaan määritellä tiettyjen sovellusliikenteiden ohjaamisesta halutulle palvelimelle tai päätelaitteelle sisäverkossa. Ensimmäiseksi palvelimelle tai päätelaitteelle on määriteltävä reitittimeltä kiinteä IP-osoite lähiverkon osoiteavaruudesta. Täten tämä kiinteä IP-osoite pysyy muuttumattomana, joten sovelluksien tiedot voidaan aina tarvittaessa välittää oikeaan osoitteeseen. (Linksys, User Guide, 24.)

Hallinnointisivun listasta voidaan valita halutulle riville sovelluksen nimi kuvaamaan sovelluksen käyttötarkoitusta. Jos listasta ei löydy halutulle sovellukselle kuvaavaa nimeä, voidaan halutulle riville kirjoittaa kuvaava nimi sovelluksen käyttötarkoituksesta. Seuraavana on palvelulle määriteltävä sovelluksen käyttämä ulkoinen ja sisäinen porttinumero. Kaikki näihin portteihin suuntautuva liikenne välitetään tämän jälkeen määriteltyyn IP-osoitteeseen. Palvelulle on määriteltävä myös, käyttääkö sovellus UDP (User Datagram Protocol), TCP vai molempia protokollia tietoliikenteessä. Viimeisenä tietona hallinnointisivulle on määriteltävä lähiverkossa olevan palvelimen tai päätelaitteen kiinteä IP-osoite, johon kyseiseen sovellukseen liittyvä tietoliikenne ohjataan. (Linksys, User Guide, 24.)

9.2 Tietoliikenneporttivälin edelleen lähetys (Port Range Forwarding)

Kuten kohdassa 9.1 tietoliikenneportin edelleen lähetyksessä, voidaan tietoliikenneporttivälin edelleen lähetyksessä määritellä tiettyjen sovellusliikenteiden ohjaamisesta halutulle palvelimelle tai päätelaitteelle. Tietoliikenneporttivälin edelleenlähetyksessä voidaan kuitenkin yhden portin sijasta määritellä porttiväli, jonka tietoliikenne välitetään tietylle palvelimelle tai päätelaitteelle. Hallinnointisivulle on määriteltävä sovelluksen käyttämien porttien ensimmäinen ja viimeinen porttiluku. Kaikki tietoliikenne, mikä vastaa tietoja kyseisestä porttivälistä, välitetään tämän jälkeen määriteltyyn IP-osoitteeseen. Koska kyseessä on porttiväli, niin sovellukselle ei voida valita listasta yksittäistä sovelluskuvausta kuvaamaan kokonaista porttiväliä, vaan riville on kirjoitettava kuvaava nimi sen perusteella, mitä sovelluksia kyseinen porttiväli edustaa. Muuten määritykset hallinnointisivulla ovat samanlaisia kuin kohdassa 9.1 tietoliikenneportin edelleen lähetys. (Linksys, User Guide, 25.)

9.3 Tietoliikenneportin tunnistus (Port Triggering)

Tietoliikenneportin tunnistus ominaisuus mahdollistaa reitittimen läpi liikkuvan tietoliikenteen seuraamisen halutuista protokollaporteista. Reititin lisää lähetetyn päätelaitteen IP-osoitteen muistiin, jos sen lähettämä tietoliikenne vastaa asetuksiin määriteltyjä protokollaporttivälejä. Pyydetyn tietoliikenteen palatessa lähettäjälle, reititin tulkitsee määriteltyjä asetuksia ja muistiin lisättyjä IP-osoitteita, ja näiden perusteella osaa ohjata tietolii-

kenteen oikeisiin protokollaportteihin vastaanottajalle. (Linksys, User Guide, 25.)

Hallinnointisivulle tulee ensimmäisenä määritellä asetukselle ominainen 12 merkin pituinen kuvaus. Seuraavassa kohdassa määritellään porttiväli, josta haluttua tietoliikennettä halutaan reitittimellä seurata portin tunnistusta varten. Asetuksiin on määriteltävä tämän jälkeen porttiväli, johon palaava tietoliikenne halutaan välittää vastaanottajalle. (Linksys, User Guide, 25.)

9.4 DMZ (Demilitarized zone)

DMZ-ominaisuus mahdollistaa yhden palvelimen tai päätelaitteen näkymisen Internetiin lähiverkosta. Tämä mahdollistaa lähiverkon palveluiden jakamisen lähiverkon ulkopuolella oleville käyttäjille. DMZ-ominaisuus toimii samalla periaatteella kuin tietoliikenneportin edelleen lähetys, mutta DMZ-ominaisuuteen ei voida määritellä erikseen portteja, joita edelleen lähetetään. Tietoliikenne välitetään IP-osoitteen perusteella halutulle DMZ-päätelaitteelle, tapahtui tietoliikenne sitten millä tietoliikenneprotokollaportin välityksellä tahansa. Täten palvelin tai päätelaite paljastetaan kokonaisuudeltaan avoimesti Internetiin. (Linksys, User Guide, 26.)
DMZ-ominaisuuden päätelaitteelle on määriteltävä reitittimeltä kiinteä IP-osoite lähiverkon osoiteavaruudesta. Hallinnointisivulle on tämän jälkeen määriteltävä, halutaanko pääsy DMZ-laitteelle sallia kaikista Internetin IP-osoitteista vai jostakin tietystä IP-osoiteavaruudesta. Tämän jälkeen DMZ-päätelaite on määriteltävä kohteeksi hallinnointisivulle joko kiinteän IP-osoitteen tai MAC-osoitteen perusteella. Päätelaite voidaan valita kohteeksi myös DHCP-asiakaslistalta. (Linksys, User Guide, 26.)

9.5 Tietoliikenteen priorisointi (QoS)

Tietoliikenteen priorisoinnilla voidaan määritellä sovelluksia, joille tietoliikennekapasiteetin saatavuus on tärkeätä. Tärkeänä sovelluksena voidaan pitää esimerkiksi VoIP-sovelluksia, joissa tiedon välittyminen reaaliajassa on hyvin tärkeää. (Linksys, User Guide, 26.)

Hallinnointisivun WMM (Wi-Fi Multimedia) -ominaisuudella voidaan parantaa langatonta verkkoa käyttävien audio-, video- tai äänipalveluiden laatua. Tämä voidaan mahdollistaa priorisoimalla verkon kapasiteettia näitä ominaisuuksia käyttäville sovelluksille. Jotta WMM-ominaisuutta voidaan hyödyntää langattomassa verkossa, täytyy langattomassa verkossa käytettävien päätelaitteiden tukea langatonta WMM-standardia. Oletuksena WRT610N langattomassa reitittimessä langaton WMM-ominaisuus on päällä. (Linksys, User Guide, 26.)

No Acknowledgement -ominaisuudesta on mahdollista määritellä, ettei reititin lähetä tietoliikennedataa uudelleen, jos tiedon lähettämisessä on tapahtunut virheitä. WTR 610N langaton reititin lähettää oletuksena uudelleen tietoliikennedatat, joissa on siirron yhteydessä tapahtunut virheitä. (Linksys, User Guide, 26.)

Internet-pääsyn priorisoinnilla voidaan määritellä tietoliikennekapasiteetin tärkeyttä tietyille sovelluksille ja laitteille. Sovelluksille ja laitteille on mahdollista määritellä neljä erilaista priorisointitasoa: korkea, keskitasoinen, normaali ja alhainen. Sovellusmäärittelyissä tulisi kuitenkin välttää määrittelemästä korkeaa tasoa jokaiselle sovellukselle. Ominaisuuden hyödyt ovat olemattomat, kun kapasiteettia pyritään tarjoamaan täydellä teholla jokaiselle sovellukselle. Jos jollekin sovellukselle halutaan määrittää normaalia alhaisempi tärkeys kapasiteetissa, voidaan tälle sovellukselle määrittää silloin alhainen taso. (Linksys, User Guide, 26.)

Internet-pääsyn priorisointiominaisuus on WRT610N langattomassa reitittimessä oletuksena pois päältä. Jotta määrityksiä Internet-pääsyn priorisoinnille voidaan tehdä, on ominaisuus kytkettävä hallinnointisivulta päälle. (Linksys, User Guide, 26.) Sovellukset ja laitteet Internetin pääsyn priorisoinnille voidaan valita viidestä eri kategoriasta: Sovellukset, Online-pelit, MAC-osoitteet, Ethernet-portit ja Äänilaitteet. (Linksys, User Guide, 27.)

Hallinnointisivulta on mahdollisuus valita sovelluslistalta haluttu sovellus, johon halutaan Internet pääsyn priorisointi määritellä. Kun haluttu sovellus on valittu listalta, voidaan sovellukselle määritellä haluttu priorisointitaso neljästä mahdollisesta tasosta. Jos sovelluslistalta ei löydy haluttua sovellusta, voidaan hallinnointisivulle määritellä haluttu sovellus. Ensimmäiseksi sovellukselle on määriteltävä kuvaava nimi, jonka avulla sovellus on tunnistettavissa priorisointilistalta. Tämän jälkeen sivulle on määriteltävä, käyttääkö sovellus TCP, UDP vai molempia tietoliikenneprotokollia tietoliikenteessä. Sivulle voidaan määritellä myös kolme porttivälimääritystä, joita sovellus käyttää tietoliikenteessä. Tiedot halutun sovelluksen tietoliikenneprotokollista ja sen käyttämistä porttiväleistä on syytä selvittää ohjelman dokumenteista ennen Internet pääsyn priorisointiasetuksien määrittämistä. (Linksys, User Guide, 27.)

Online-pelille Internet-pääsyn priorisointia määriteltäessä on pelilistalta valittava haluttu peli, johon halutaan priorisointi määritellä. Valitulle pelille voidaan tämän jälkeen määritellä haluttu priorisointitaso neljästä mahdollisesta tasosta. Jos pelilistalta ei löydy haluttua peliä, voidaan hallinnointisivulta määritellä halutulle pelille tarvittavat ominaisuuden samalla periaatteella kuin sovelluksillekin. (Linksys, User Guide, 27.)

Internet-pääsyn priorisointia voidaan määritellä hallinnointisivulle myös Mac-osoitteen perusteella. Halutulle päätelaitteelle on annettava kuvaava nimi, jotta päätelaite on tunnistettavissa priorisointilistalta. Sivulle on määriteltävä tämän jälkeen päätelaitteen käyttämä MAC-osoite, jotta haluttu päätelaite osataan yksilöidä langattomalla reitittimellä. Päätelaitteelle on määriteltävä priorisointitaso neljästä mahdollisesta tasosta. (Linksys, User Guide, 28.)

Langattomassa reitittimessä oleville neljälle Ethernet-portille voidaan erikseen myös määritellä Internet-pääsyn priorisointi. Hallinnointisivulle on määriteltävä, mihin neljästä Ethernet-portista määrittely halutaan suorittaa. Portin valitsemisen jälkeen, voidaan portille valita priorisointitaso neljästä mahdollisesta tasosta. (Linksys, User Guide, 28.)

Langattomassa lähiverkossa käytettävälle äänilaitteelle voidaan määritellä erikseen oma Internet-pääsyn priorisointitaso. Äänilaitteelle on määritettävä kuvaava nimi, jotta äänilaite on tunnistettavissa priorisointilistalta. Äänilaitteen käyttämä MAC-osoite on määritettävä tämän jälkeen hallinnointisivulle, jotta äänilaitteet osataan yksilöidä langattomalla reitittimellä. MAC-osoitteen määrittämisen jälkeen, voidaan äänilaitteelle määritellä priorisointitaso neljästä mahdollisesta tasosta. (Linksys, User Guide, 28.)

Priorisointilistalta on nähtävissä kaikki sovellukset ja päätelaitteet joille on määritelty Internet pääsy priorisointitasoja. Listalta on nähtävissä tiedot sovelluksien ja päätelaitteiden nimistä, priorisointitasoista ja yksityiskohtaisempia tietoja riippuen priorisoinnin kohteesta. Priorisointilistalta on mahdollisuus muokata priorisointi kohteita tai poistaa halutut priorisoinnit. (Linksys, User Guide, 28.)

10. HALLINTA (ADMINISTRATION)

10.1 Hallinnointi (Management)

Hallinnointisivuston Management-sivulta voi muuttaa asetuksia, jotka liittyvät langattoman reitittimen hallinnointisivuston sisäänpääsyyn. Sivulta voi määritellä, mistä hallinnointisivulle on oikeus päästä. Sivulta voidaan määritellä salasana, joka vaaditaan kirjautumiseen hallinnointisivustolle. Oletus salasanana toimii ”admin” kirjautuessa hallinnointisivulle. (Linksys, User Guide, 29.)

Management sivulta voidaan määritellä myös tapahtuuko kirjautuminen hallinnointisivustolle HTTP (Hypertext Transfer Protocol) vai HTTPS (Hypertext Transfer Protocol Secure) protokollaa käyttäen. Management-sivulta voi määritellä myös, voiko hallinnointisivustolle kirjautua sisään myös langattoman verkon kautta vai ainoastaan verkkokaapeliyhteyden avulla. (Linksys, User Guide, 29.)

Management-sivulle voi määritellä myös mahdollisuuden kirjautua sisään hallinnointisivulle etäyhteyden avulla. Sivulle määritetään IP-osoite, josta kirjautuminen hallinnointisivulle sallitaan. Sivulle voi määritellä, käytetäänkö tällöin kirjautumiseen HTTP vai HTTPS protokollaa. Asetuksiin on mahdollista määritellä myös, mitä TCP-protokollaporttia yhteyden muodostamisessa käytetään. Oletuksena langattomalle reitittimelle on asetettu 8080 portin käyttö etäyhteyskirjautumiselle. Kirjautuminen hallinnointisivulle voidaan sallia myös mistä tahansa IP-osoitteesta, mutta tämä ei ole suositeltavaa tietoturvasyistä. Sivulta voi sallia ohjelmistopäivityksen suorittamisen myös etäyhteyden avulla. (Linksys, User Guide, 29.)

Management-sivulta voi sallia myös UPnP-protokollaan liittyvien yhteyksien sallimisen langattomalle reitittimelle. Sivun asetuksista voi erikseen myös määritellä UPnP-protokollaa käyttävien käyttäjien oikeuksia muutel-

la UPnP Media -palvelimen asetuksia ja heidän Internet-oikeuksiaan. (Linksys, User Guide, 29.)

Management-sivulta voi myös hallinnoida langattoman reitittimen asetuksien varmuuskopioita. Backup Confgigrations -painikkeesta voi tallettaa varmuuskopiotiedoston langattoman reitittimen asetuksista. Restore Configurations -painikkeesta voidaan myös palauttaa varmuuskopiotiedosto langattomalle reitittimelle ongelmatilanteessa. Tämän jälkeen langattoman reitittimen asetukset saadaan palautettua asetuksille, jotka olivat voimassa varmuuskopiotiedoston luomisen aikana. (Linksys, User Guide, 29.)

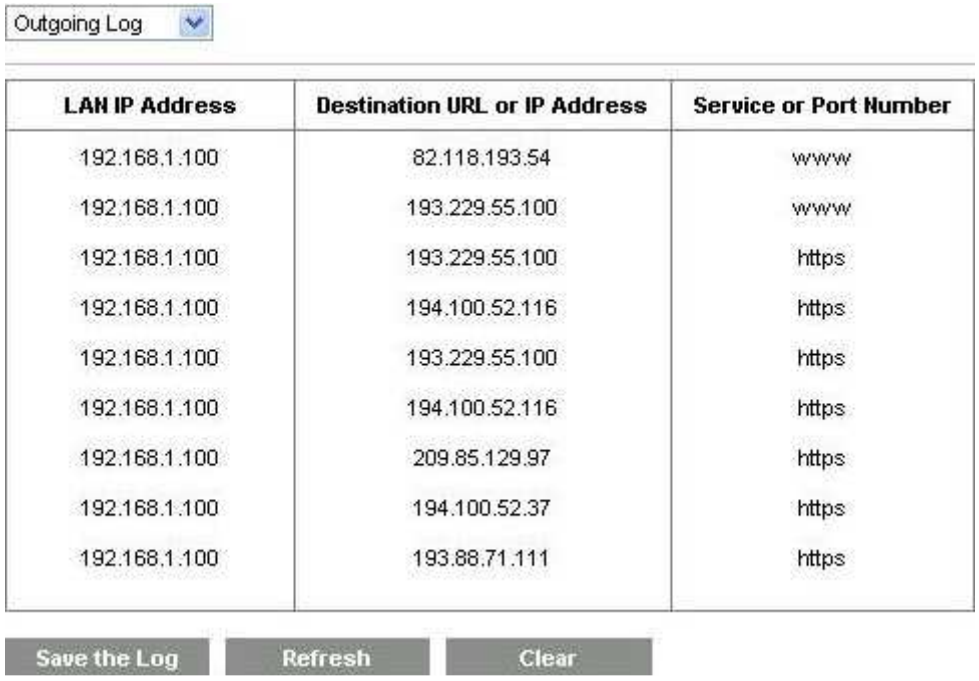
10.2 Lokitiedot (Log)

Langattomaan reitittimeen voidaan määritellä lähiverkossa olevan päätelaitteen IP-osoite, jossa on erillinen Logviewer -ohjelmisto. Jos kyseistä ohjelmistoa ei ole missään lähiverkon päätelaitteessa, voidaan lokitiedostoja selata myös hallinnointisivustolta.

Jotta lähiverkon liikennettä voidaan seurata, tulee lokitoiminto asettaa päälle. Oletuksena WRT610N langaton reititin ei kirjaa tietoliikennemuutoksia lokitiedostoihin. Lokitoiminnon ollessa päällä, voidaan lokitietoja selata erilliseltä sivustolta, joka aukeaa View Logs -painikkeesta. Lokitietoja on mahdollista selata neljästä eri lokikategoriasta. Näitä ovat Incoming logs, Outgoing logs, Security logs ja DHCP Client logs.

Incoming logs -tiedoista voidaan selata muutoksia, joita tapahtuu langattomaan reitittimeen nähden sisäänpäin tulevassa tietoliikenteessä. Tiedoista on nähtävissä, mistä IP-osoitteesta pyritään lähiverkkoon liikennöimään ja mitä porttia hyväksikäyttäen.

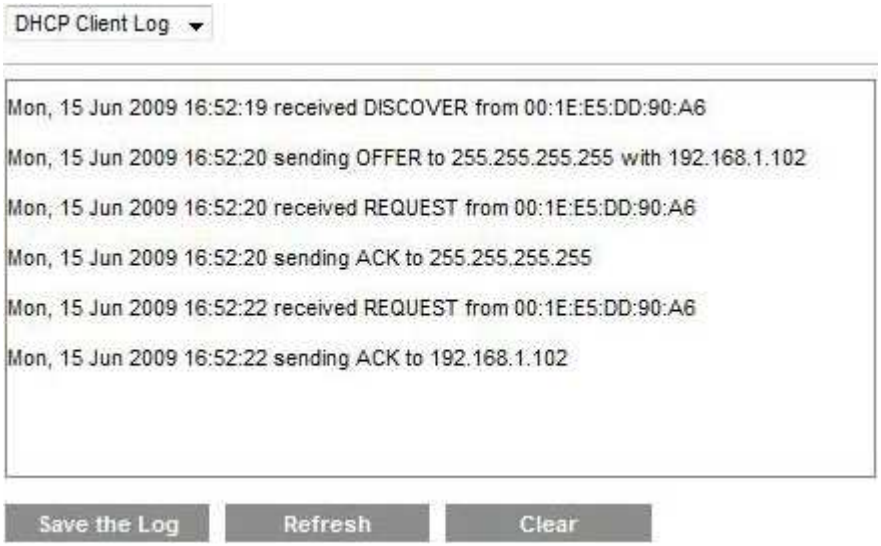
Outgoing logs -tiedoista voidaan selata muutoksia, joita tapahtuu langattomaan reitittimeen nähden ulospäin tulevassa tietoliikenteessä. Tiedoista on nähtävissä, mistä lähiverkon osoitteesta pyritään yhteyttä muodostamaan. Samalla nähdään kohdeosoite ja mitä porttia tähän yhteyteen pyritään käyttämään. Kuvasta 5 on nähtävissä Outgoing -logs tiedoston näkymä sen jälkeen, kun käyttäjä on pyrkinyt ottamaan yhteyttä Internetiin.



KUVA 5 *Outgoing Log näkymä*

Security Log -tiedot keräävät tietoja, jotka liittyvät langattoman reitittimen turvallisuuteen. Lokitietoihin jää esimerkiksi merkintä niistä yrityksistä, joissa on yritetty käyttää sovelluksia, jotka on estetty langattoman reitittimen palomuurin asetuksissa. Myös mahdollisista tietomurtoyrityksistä jää tiedot Security log -tietoihin.

DHCP Client log -tiedot keräävät tietoa DHCP:n avulla jaetuista IP-osoitteista. Lokitiedoista on nähtävissä, miltä koneelta IP-osoite pyyntö on tullut ja minkä IP-osoitteen langaton reititin laitteelle määritteli. Lokeista on myös nähtävissä, jos IP-osoitetta ei jostakin syystä voitu määritellä. Lokeista on helppo määritellä ongelmatilanteissa, jos jokin laite ei jostakin syystä saa IP-osoitetta DHCP:n avulla. Kuvasta 6 on nähtävissä, kuinka päätelaite on anonut DHCP:ltä IP-osoitetta. DHCP on tämän jälkeen määritellyt sille IP-osoiteavaruudesta osoitteen 192.168.1.102. (Linksys, User Guide, 29-30.)



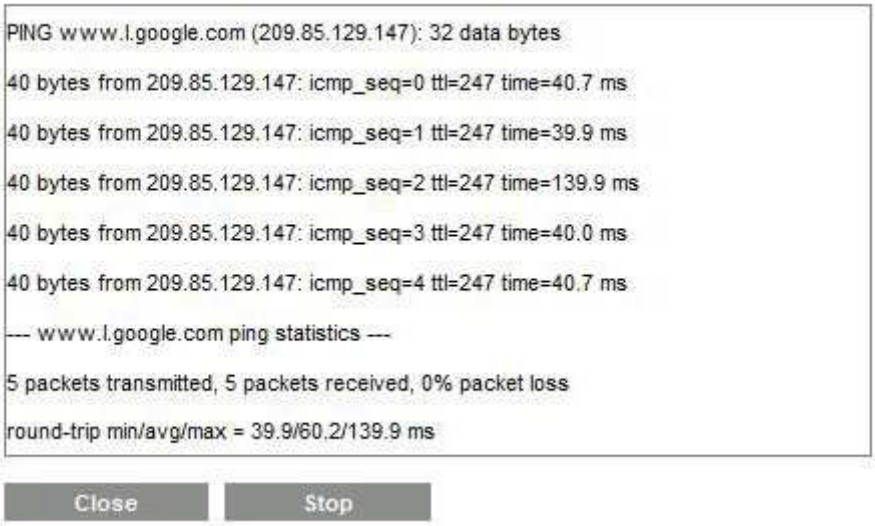
KUVA 6 *DHCP Client log näkymä*

10.3 Virheenmääritys (Diagnostics)

Diagnostics -sivulta voi suorittaa testejä, joiden avulla voi määritellä langattoman verkon toimivuutta. Diagnostics -sivulta löytyy Ping ja Traceroute mahdollisuudet, joiden avulla voi vikatilanteissa etsiä, mistä verkkoongelma voi mahdollisesti johtua.

Ping -kohtaan voi määrittää joko halutun päätelaitteen Internet -osoite tai IP-osoite. Tämän jälkeen voi määritellä, kuinka monta kertaa yhteyttä yritetään muodostaa ja miten isolla pakettikoolla. Kertavaihtoehtoja on joko 5,10,15 tai jatkuva testaus. Pakettikokoa voidaan vaihdella 32 tavusta aina 65 500 tavuun.

Haluttujen määrityksien jälkeen, voidaan testaaminen aloittaa Start to Ping -painikkeesta. Selaimeen avautuu erillinen ikkuna, josta nähdään Ping -testin tulos. Kuva 7 havainnollistaa miten voi todeta halutun kohteen saavutettavuuden.



KUVA 7 *Onnistuneen Pingi - testin näkymä*

Traceroute -toiminto toimii samalla periaatteella kuin Ping -testi. Osoitekenttään syötetään joko tavoitellun kohteen Internet osoite tai IP-osoite. Start to Traceroute -painikkeesta avautuu erillinen ikkuna, josta voidaan havainnoida reitti, mitä pitkin on päästy tavoiteltuun kohteeseen. (Linksys, User Guide, 30.)

10.4 Tehdasasetukset (Factory Defaults)

Factory Defaults -asetus mahdollistaa langattoman reitittimen asetuksien palauttamisen oletusasetustilaan. Painamalla Restore Factory Defaults -painiketta häviää kaikki asetukset, jotka on langattomalle reitittimelle tallennettu.

Tehdasasetukset voidaan asettaa langattomalle reitittimelle myös laitteessa olevasta painikkeesta. Langattomassa reitittimessä sijaitsee pieni punainen reikä, jossa lukee Reset. Pientä painiketta painamalla noin viiden sekunnin ajan saadaan langattoman reitittimen asetukset palautettua tehdasasetuksille. Tämä tulisi huomioida myös, kun langatonta reititintä sijoitetaan kohteeseen. Ulkopuoliselle ei tulisi antaa mahdollisuutta ilkivaltaisesti tyhjentää langattoman reitittimen asetuksia. (Linksys, User Guide, 30.)

10.5 Ohjelmistopäivitys (Firmware Upgrade)

Firmware Upgrade kohdasta voidaan päivittää langattoman reitittimen laiteohjelmisto. Laiteohjelmistoa ei suositella päivitettäväksi, ellei langattoman reitittimen toiminnassa ole vakavia ongelmia tai uusi laiteohjelmistoversio tuo tarvittavia uusia ominaisuuksia laitteelle.

Uusimman laiteohjelmistoversion voi hakea valmistajan kotisivuilta. Kun tiedosto on ladattu päätelaitteelle, tulee se ensin purkaa käyttöön soveltu-

valla ohjelmistolla. Purettu tiedosto valitaan tämän jälkeen hallinnointisivustolta Selaa -painikkeen avulla. Laiteohjelmiston asentaminen langattomalle reitittimelle alkaa heti kun Start Upgrade -painiketta painaa ohjelmistosivustolta. Hallinnointisivustolle ilmestyy tieto asennuksen etenemisestä ja mahdollisista toimenpiteistä, jotka käyttäjän tulee suorittaa saattaakseen asennuksen loppuun. (Linksys, User Guide, 30-31.)

11. TILANNETIETO (STATUS)

11.1 Reititin (Router)

Hallinnointisivulta on mahdollista nähdä reitittimen todellinen tilanne kyseisellä hetkellä. Sivulta on nähtävissä reitittimellä ajossa olevan ohjelmiston versio ja sen tunnistuskoodi, jolla käyttäjä voi taata ohjelmiston aitouden. Sivulta on luettavissa myös päiväys- ja kellonaikatiedot, jotka reitittimelle on määritelty. Sivulta löytyvät tiedot myös reitittimen ISP:lle näkyvästä MAC-osoitteesta, verkkoaseman tunnuksesta ja verkkotunnuksesta. Reitittimen ollessa kytkettynä Internetiin, näkyvät sivulta tiedot yleisestä Internet IP-osoitteesta, aliverkon peitteestä, oletusyhdyskäytävästä, DNS IP-osoitteista, MTU (Maximum Transfer Unit) arvosta ja DCHP-lainausajasta. (Linksys, User Guide, 31.)

11.2 Lähiverkko (Local Network)

Hallinnointisivulta on mahdollisuus nähdä lähiverkon todellinen tilanne kyseisellä hetkellä. Sivulta on nähtävissä reitittimen lähiverkon suunnan sovittimen MAC-osoite, IP-osoite ja aliverkon peite. Sivulta saadaan tiedot myös DHCP-palvelimen asetuksista. Sivulta löytyy tieto, onko DHCP-palvelu käytössä vai pois päältä. DHCP palvelun ollessa päällä, löytyy sivulta tieto, mistä IP-osoiteavaruudesta IP-osoitteita jaetaan lähiverkon päätelaitteille. Sivulta on mahdollista myös avata DHCP-asiakaslista, josta näkee kaikki DHCP-palvelun sen hetkiset oleelliset tiedot. (Linksys, User Guide, 31-32.)

11.3 Langaton verkko (Wireless Network)

Hallinnointisivulta on mahdollisuus nähdä langattomalle lähiverkolle kyseisellä hetkellä määritellyt asetukset. Sivulta on mahdollisuus nähdä erikseen asetukset, jotka on määritelty 2.4 ja 5 GHz:n langattomille verkoille. Sivulta nähdään molemmille verkoille ominainen liitäntä MAC-osoite, jota käytetään hyväksi päätelaitteen liittyessä langattomaan lähiverkkoon. Sivulla on nähtävissä myös molemmille verkoille määritellyt SSID-tunnukset ja mainostetaanko niitä yleisesti verkon päätelaitteille. Sivulta on nähtävissä myös asetukset, jotka on määritelty langattoman verkon perusasetuksissa. Asetukset sisältävät tiedot määritetyistä kanavien laajuuksista ja mikä kanava on oletuksena käytössä kullekin langattomalle lähiverkolle. Sivulta nähdään, mitä langattoman verkon salausprotokollaa käy-

tetään salaamaan tietoliikenne kyseisissä langattomissa verkoissa. (Linksys, User Guide, 32.)

12. MOBIILI LABORATORIO

Opinnäytetyön tavoitteena oli alun perin kehittää kaksi laboratorio-ohjetta langattoman verkon tekniikoita käsittelevälle kurssille ja yksi laboratorio mobiiliteknologian kurssille. Kun oli tutustuttu WRT610N langattoman reitittimen ominaisuuksiin, todettiin, että se ei sisällä muita kuin QoS-ominaisuuksia, joita voisi suoranaisesti hyödyntää mobiiliteknologian kurssilla. Jotta laboratorio-ohjeesta olisi saatu tarkoituksenmukaisempi juuri mobiiliteknologian opiskelijoille, olisi se vaatinut erillisen palvelimen käyttöönottoa tähän tarkoitukseen. Tähän palvelimeen olisi voitu lisätä VoIP-teknologiassa käytössä olevia sovelluksia ja ominaisuuksia. WRT610N olisi voinut toimia yhteyspisteenä palvelimen ja puhelinpäätelaitteen välillä.

Pelkillä WRT610N langattoman reitittimen ominaisuuksilla ei olisi saatu täysipainoista kuvaa VoIP-verkon rakenteesta ja sen ominaisuuksista opiskelijoille. Ohjaavan opettajan kanssa käydyn keskustelun jälkeen päädyttiin siihen johtopäätökseen, että palvelimen ominaisuudet ja käyttöönotto eivät kuulu tämän opinnäytetyön sisältöön, vaan tarvittaessa siitä luodaan uusi opinnäyteprojekti asiakkaalle.

13. LABORATORIOIDEN SUUNNITTELU

Laboratorioiden suunnittelu aloitettiin kartoittamalla WRT610N langattoman reitittimen ominaisuuksia. Ominaisuuksille määriteltiin, olivatko ne keskeisessä osassa laboratorio-opiskelua vai olivatko ne vähemmän tärkeitä opetuksen kannalta. Keskeisempiin ominaisuuksiin perehdyttiin laboratorio-ohjeissa syvällisemmin. Ominaisuudet jaettiin myös kahteen osaan, joista pyrittiin muodostamaan kaksi erillistä laboratorio-ohjetta. Ensimmäinen laboratorio-ohje pyrki sisältämään langattoman reitittimen yksinkertaiset perusasetukset. Toinen laboratorio-ohje sisälsi vaativimmat ja käytön kannalta monimutkaisemmat asetukset.

Kartoituksen jälkeen langattoman reitittimen ominaisuuksia kokeiltiin koulun laboratorioympäristössä. Jokaisen ominaisuuden vaatimat asetukset ja määritykset kirjattiin ylös. Tavoitteena oli kirjata ohjeet oppilaiden käyttöön yksiselitteisesti, jotta oppilaiden olisi helppo määritellä asetukset laitteille. Tämän avulla pyrittiin eliminoimaan mahdollisuus, jossa jokin ominaisuus ei toimisi käyttäjän tekemän virheen takia. Kun jokainen ominaisuus oli kokeiltu ja todettu toimivaksi, kirjattiin ne ylös kahdeksi eri laboratorio-ohjeeksi. Laboratorio-ohjeiden kokoamisen jälkeen, ohjeet käytiin läpi vielä kertaalleen käytännössä alusta loppuun laboratorioympäristössä. Laboratorio-ohjeiden loppuun lisättiin kysymyksiä, joihin oppilaiden tulisi osata vastata laboratoriotyön suoritettuaan. Kysymyksillä pyrittiin varmistamaan, että oppilaat olivat sisäistäneet laboratoriotyön aikana keskeisimmät asiat.

14. YHTEENVETO

Hämeen ammattikorkeakoulun hankkimat WRT610N langattomat reitittimet osoittautuivat sopiviksi laitteiksi yksinkertaista laboratoriotyöskentelyä varten. Laitteiden käyttöliittymän yksinkertaisuus helpotti yksiselitteisien laboratorio-ohjeiden laatimista laboratoriotyöskentelyä varten. Laitteen rajoitukset, esimerkiksi osoiteavaruuden määrittämisessä, rajaavat kuitenkin laitteiden käyttöä monimutkaisemmissa verkoissa.

RADIUS-palvelua ei saatu useista yrityksistä huolimatta toimimaan koulun laboratorioympäristössä. Syynä toimimattomuuteen oli RADIUS-palvelimen ja laboratorioverkon hallinta-alueen eroavaisuus. Myöskään palvelimen ohjelmistoversiot eivät olleet ajan tasalla, jotta RADIUS-palvelu olisi saatu luotua verkkoon.

Laboratoriotyöskentelyn aikana huomattiin myös ongelmia WRT610N langattoman reitittimen ominaisuuksien toiminnassa. Laite hävitti välillä määritellyt 2.4 GHz:n langattoman verkon salausasetukset reitittimen muistista. Myös langattoman reitittimen hallinnointisivulle pääsy estyi ajoittain sen jälkeen, kun oli tehty muutoksia hallinnointisivulle.

Langattoman reitittimen ominaisuuksista onnistuttiin kuitenkin luomaan kaksi toimivaa laboratorio-ohjetta Hämeen ammattikorkeakoulun käyttöön. Laboratorio-ohjeisiin onnistuttiin sisällyttämään useita konkreettisessa työympäristössä vaadittavia langattoman verkon määrityksiä. Opinnäytetyön sisältämään kirjalliseen osuuteen saatiin sisällytettyä tarvittavat tiedot WRT610N langattoman reitittimen ominaisuuksista. Sitä voidaan hyödyntää opetusmateriaalina, kun tutustutaan laitteen toimintaan.

LÄHTEET

Chandra, P., Dobkin, D. M., Bensky, A., Olexa, R., Lide, D. A. & Dowla, F. 2008. Wireless Networking. United States of America: Elsevier Inc.

Hassel, J. O'Reilly. 2002. RADIUS. Viitattu 29.7.2009 http://books.google.fi/books?id=9h7vHT-l6uMC&printsec=frontcover&source=gbs_ViewAPI

IEEE, 2009, Official IEEE 802.11 Working Group Project Timelines, Viitattu 06.11.2009, http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Kerttula, E. 1999. Tietoverkkojen Tietoturva. Helsinki

Linksys, Cisco Systems Inc, 2009, User Guide Version 10, Viitattu 22.05.2009, http://www.linksysbycisco.com/US/en/products/WRT610N

Linksys, Cisco Systems Inc, 2009, Data Sheet, Viitattu 22.05.2009, http://www.linksysbycisco.com/US/en/products/WRT610N

Microsoft Corporation. 2008. Microsoft Technet. RADIUS Authentication Process, 21 lokakuu 2008. Viitattu 29.7.2009. http://technet.microsoft.com/en-us/library/dd197520(WS.10).aspx

Penttinen, J, 2/2009, Prosessori Lehti - Kohti todellista 4G-tekniikkaa, 18.6.2009

Puska, M. 2005. Langattomat Lähiverkot. Helsinki.

LIITE 1

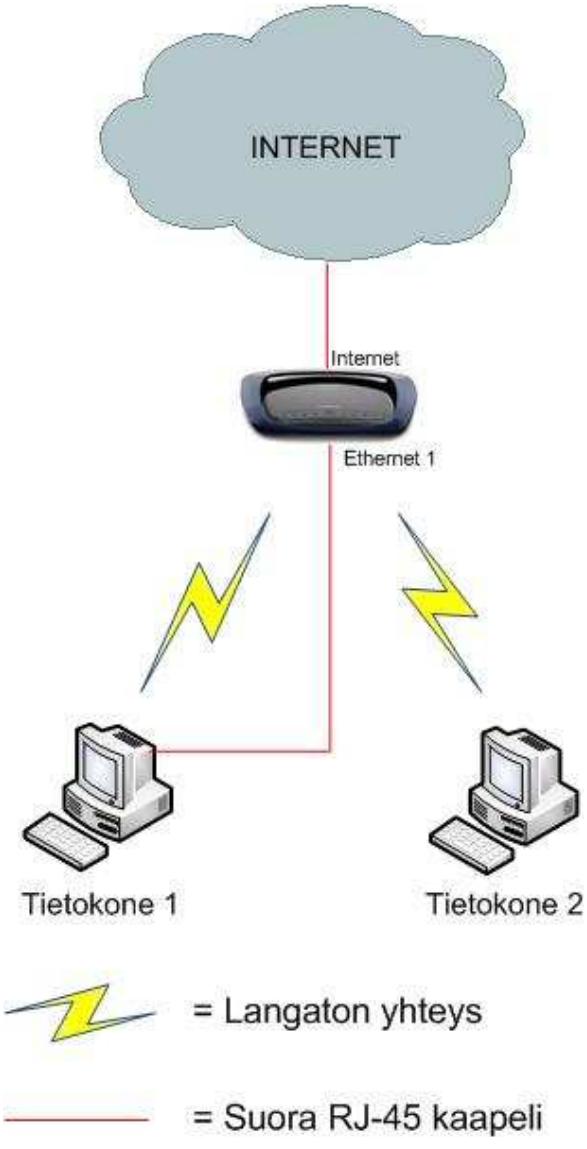
LABORATORIO-OHJE 1

1. Valmistelut

Laboratoriotyön tavoitteena on opettaa ja havainnollistaa perusasiat langattomista verkoista. Oppilaan tulisi tuntea laboratorion jälkeen seuraavat asiat:

- IEEE 802.11 standardit ja niiden erot
- langattomanverkon yleisimmät salaukset
- langattomanverkon rakentaminen ja yhteyden muodostus
- langattomanverkon tietoturva
- langattomanverkon vian määritys ja niiden työkalujen käyttö

Laboratorio-ohje on suunniteltu ja tarkoitettu Windows XP SP3 käyttöjärjestelmälle. Laboratorio aloitetaan rakentamalla alla olevan kuvan mukainen verkko.



2. Käyttöönotto

Aloita laboratoriotyö palauttamalla oletusasetukset WRT610N langattomaan reitittimeen. Langattoman reitittimen oletusasetukset saat palautettua painamalla pientä painiketta laitteen takapaneelista teräväkärkisellä esineellä n. 5 sekunnin ajan. Laitteen täytyy olla tällöin kytkettynä sähköverkkoon. Virtavalo alkaa vilkuttaa, kun oletusasetukset ovat palautuneet laitteeseen.

Kirjaudu langattoman reitittimen hallinnointisivulle selaimella osoitteeseen http://192.168.1.1. Jätä käyttäjätunnus tyhjäksi ja käytä salasanana ”admin”.

**** Jos yhteyden muodostus ei onnistus Internet Explorer -selaimella, yritä muodostaa yhteys Mozilla Firefox.selaimella****

3. Perusasetukset

Kirjautumisen jälkeen saavut sivulle **Setup → Basic Setup.** Tarkasta sivulta, että seuraavat asetukset on määritelty sivulle.

Language:	englanti
Internet connection type:	DHCP
IP Address:	192.168.1.1
Subnetmask:	255.255.255.0
DHCP server:	enable
Start ip address:	192.168.1.100
Maximum number of users:	50
Client lease time:	0
Time zone:	Määritä oikea aikavyöhyke

Tallenna muutokset.

Mene seuraavaksi hallinnointisivulla sivulle **Setup → Advanced Routing.** Määrittele sivulta NAT-asetus päälle, jos langaton reititin isännöi lähiverkon liikennettä suoraan Internetiin. Määritä NAT asetus pois päältä, jos langaton reititin toimii lähiverkon sisäisenä reitittimenä. Tallenna muutokset.

4. Langattoman verkon salaus ja tietoturva

Mene hallinnointisivulla sivulle **Wireless → Wireless Security**. Määrittele seuraavat asetukset sivulle:

5 GHz Wireless Security

Security Mode:	WPA2-Personal
Encryption:	WPA-TKIP or WPA2-AES
Passphrase:	*Määrittele omaperäinen salasana*
Key Renewal:	3600 seconds

Tallenna muutokset.

2.4 GHz Wireless Security

Security Mode:	WPA-Personal
Encryption:	TKIP
Passphrase:	*Määrittele omaperäinen salasana*
Key Renewal:	3600 seconds

Tallenna muutokset.
Muista kumpi salasana on määritelty 5 GHz:n ja kumpi 2.4 GHz:n verkolle.

Mene hallinnointisivulla **Security → Firewall** sivulle ja tarkasta, että tilallinen palomuuri on kytketty päälle.

5. Langattoman verkon asetukset

Mene hallinnointisivulla **Wireless → Basic Wireless Settings** sivulle. Valitse Manual määritys sivulta**.** Määrittele seuraavat asetukset avautuvalle sivulle:

5 GHz Wireless Settings

Network Mode:	Wireless-N Only
Network Name (SSID):	*Määritä omaperäinen verkon nimi*
Channel width:	Auto
SSID Broadcast:	Enable

2.4 GHz Wireless Settings

Network Mode:	B/G Mixed
Network Name (SSID):	*Määritä omaperäinen verkon nimi*
Standard Channel:	Auto
SSID Broadcast:	Enable

Ota huomioon, että 5 ja 2.4 GHz:n verkkojen Network Name (SSID) tulisi poiketa toisistaan laboratoriotyön helpottamiseksi. Tallenna Muutokset.

6. Log -ominaisuus

Mene hallinnointisivulta **Administration → Log** sivulle. Aseta lokitoiminto päälle. Tallenna muutokset.

Tehdessäsi muutoksia tai muodostaessasi yhteyksiä, näet lokeista tapahtumien kulun. Paina View Log painiketta päästäksesi selaamaan lokitietoja. Voit valita kohdelokin seuraavista vaihtoehdoista: Incoming log, Outgoing log, Security Log ja DHCP Client Log.

7. Yhteyden muodostaminen manuaalisesti langattomaan verkkoon

Kytke langattoman verkon USB adapteri kiinni sen mukana tulevaan telakkaan ja kytke telakka kiinni tietokoneeseen 1. Laboratorioluokan tietokoneissa pitäisi olla langattoman verkon USB adapterin ajurit asennettuna.

**** Jos tietokone ei tunnista adapteria ja vaikuttaa siltä, ettei tietokoneessa ole ajureita asennettuna, irrota telakka tietokoneesta. Aseta USB adapterin mukana tullut CD tietokoneeseen ja seuraa asennuksen ohjeita. Löydät ohjeet myös paketin mukana tulleesta ohjekirjasta. Kiinnitä USB adapteri + telakka vasta sitten, kun asennusohjelma sitä erikseen pyytää. ****

Mene seuraavaksi **Start → Control Panel → Network** Connections sivulle ja mene wireless network connection kuvakkeen kautta Properties. Avautuvasta ikkunasta mene Wireless Networks -välilehdelle, josta valitaan view wireless networks.

**** Ikkunaan saattaa tulla ilmoitus, että " windows cannot configure this wireless connection…". Tarkasta tämän jälkeen oikeasta alakulmasta, onko siellä vihreä neliö, jossa lukee " linksys wireless network monitor". Sammuta ohjelma ja yritä saada lista auki avoinna olevista langattomista verkoista. ****

Etsi listasta jompikumpi luomistasi langattomista verkoista. Valitse verkko ja paina connection -painiketta. Syötä avautuvaan ikkunaan kyseisen verkon salasana kahdesti. Testaa Internetin toimivuus. Jos kyseisen tietokoneen ja langattoman reitittimen välillä on RJ-45 kaapeli, niin irrota se yhteyden testaamisen ajaksi.

**** Jos yhteys ei jostakin syystä toimi, voit tarkistaa seuraavat asiat: Onko salasana varmasti oikea halutulle verkolle ja onko liitännät kunnolla kiinni. Tarkasta tehdyt asetukset, onko muistettu tallettaa asetukset, ovatko johdot ehjät, onko Setup → Advanced routing: NAT asetus päällä… ****

Seuraavaksi testataan toisen luodun verkon toimivuus. Mennään **Start → Connection to → Wireless Network Connection** sivulle ja suljetaan yhteys luotuun verkkoon disconnect painikkeesta. Valitaan toinen luoduista verkoista ja muodostetaan yhteys siihen. Syötä kokeilumielessä salasana väärin samalla tavalla molempiin salasanakenttiin (väärä salasana kuitenkin yli 8 kirjainta). Yritä muodostaa yhteys connect painikkeesta. Testaa toimivuus.

Suljetaan yhteys ja yritetään muodostaa yhteys uudestaan oikean salasanan avulla. Testaa toimivuus. Jos kyseisen tietokoneen ja langattoman reitittimen välillä on RJ-45 kaapeli, niin irrota se yhteyden testaamisen ajaksi.

8. Yhteyden muodostaminen Wi-Fi Protectionin avulla langattomaan verkkoon

Aseta tietokoneeseen 2 USB adapterin mukana tullut CD ja asenna CD:n mukana tulevat ajurit ja ohjelmisto. Asenna ohjelmisto ja ajurit uudelleen tietokoneelle, vaikka ohjelma huomauttaisi niiden olevan jo asennettuina.

Langattoman verkon USB adapteri ei saa olla kytkettynä tietokoneeseen, kun ajureita ja ohjelmistoa asennetaan. Kytke USB adapteri ja telakka kiinni tietokoneeseen vasta, kun asennusohjelma sitä pyytää. Asennuksen onnistuttua siirry käyttämään asennuksen mukana tullutta Linksys Wireless Network Monitor ohjelmaa. Asennuksen loputtua sinulle tarjotaan mahdollisuutta muodostaa langattoman verkon yhteys käyttäen Wi-Fi Protected Setup ominaisuutta. Jos ohjelma ei kuitenkaan anna mahdollisuutta käyttää Wi-Fi ominaisuutta, pääset käyttämään sitä ohjelman oikeassa reunassa sijaitsevasta painikkeesta, jossa on kaksi nuolta. Seuraa ohjelman ohjeita muodostaaksesi yhteyden langattomaan verkkoon. Pyri muodostamaan yhteys Push Button -menetelmän avulla.

**** Varmista, ettei kukaan muu ryhmä muodosta yhteyttä Wi-Fi ominaisuuden avulla samaan aikaan. Jos kaksi ryhmää tekee Wi-Fi toimintoa yhtäaikaisesti, laitteet eivät tiedä mihin tukiasemaan yhteys olisi tarkoitus muodostaa. ****

Mene hallinnointisivulla **Wireless → Basic Wireless Settings** sivulle ja laita ruksi kohtaan Wi-Fi Protected Setup. Kytke sivulta Wi-Fi Protected Setup toiminto päälle kuvasta, jossa on kaksi nuolta. Tämän jälkeen voit kytkeä saman toiminnon päälle myös Network Monitor ohjelmasta. Wi-Fi Protected Setup ominaisuuden pitäisi nyt muodostaa yhteys päätelaitteen ja langattoman reitittimen välille. Yhteyden muodostuttua, Network Monitor ohjelma antaa tiedot muodostetusta langattomasta yhteydestä. Testaa yhteyden toimivuus.

Suljetaan Linksys Wireless Network Monitor ohjelma molemmilta tietokoneilta, jos se on vielä auki.

9. Langattomien verkkojen ominaisuudet

Muodosta manuaalisesti toisella tietokoneella yhteys 2.4 GHz:n verkkoon ja toisella tietokoneella 5 GHz:n verkkoon. Testaa toimivuus. Avaa molemmista tietokoneista käytössä olevan langattoman verkon Status tiedot. Tarkastele ja vertaa muodostettujen yhteyksien ominaisuuksia Status ikkunasta. Kiinnitä huomiota eritoten yhteysnopeuteen.

10. SSID Broadcast

Sammuta langattoman verkon yhteys tietokoneesta, jossa on käytössä 2.4 GHz:n langaton yhteys. Mene hallinnointisivulla **Wireless → Basic Wireless Settings** sivulle ja kytke Manual -asetus takaisin päälle. Kytke 2.4 GHz:n verkosta SSID Broadcast ominaisuus pois päältä.

Seuraavaksi tarkoituksena on muodostaa yhteys takaisin tietokoneelta, josta katkaisit 2.4 GHz:n langattoman verkon yhteyden. Mene seuraavaksi **Control Panel → Network Connections** ja sieltä wireless network connection kuvakkeen alta Properties sivulle. Etene avautuneesta ikkunasta wireless networks välilehdelle.

Jos sivulla on näkyvissä Preferred networks listassa yhteyksiä, niin poista ne. Lisää uusi verkko Add painikkeesta. Lisää avautuneeseen ikkunaan Network Name (SSID) kohtaan 2.4 GHz:n käytössä olevan verkon Network Name (SSID) tunnus. Valitse Network Authentication kohtaan WPA-PSK ja Data Encryption kohtaan TKIP. Määritä Network key kohtaan 2.4 GHz:n verkossa olevan salauksen salasana ja toista salasana seuraavalle riville. Tarkista, että sivulle on valittu Connect even if this network is not broadcasting toiminne päälle. Connection välilehdellä tulisi olla määritettynä asetus Connect when this network is in range päällä. Hyväksy asetukset sivulta OK-painikkeella ja myös seuraavalta sivulta. Ota Wireless Network Connection kohdasta oikealla hiiren napilla View available wireless networks valinta. Löydätkö listasta 2.4 GHz:n verkkoa? Testaa yhteyden toimivuus.

**** Jos yhteyden muodostus ei onnistu SSID broadcastin ollessa poispäältä niin tarkista, että SSID ja salasana on varmasti määritetty oikein. Jos yhteyden muodostus ei silti onnistu, käynnistä tietokone uudelleen ja määritä tietokoneelle langattoman verkon asetukset uudelleen. ****

Kun yhteys on saatu muodostettua SSID Broadcastin ollessa pois päältä, määritä SSID Broadcast takaisin päälle **Wireless → Basic Wireless Settings** sivulta.

Tallenna muutokset.

11. Internet yhteyden muodostaminen staattisesti

Mene hallintasivulla **Status → Router** sivulle ja tutki Router Information sekä Internet Connection näyttämiä tietoja. Ota tiedot ylös esimerkiksi kopioimalla ne muistioon. Kun tiedot on otettu ylös, irrota RJ45 johto langattoman reitittimen ja Internet yhteyden väliltä. Tämän jälkeen vapauta IP-osoite tiedot Release IP Address painikkeesta. IP-osoitetietojen kohdalle pitäisi nyt ilmestyä oletus 0.0.0.0 IP-osoite.

Mene seuraavaksi hallinnointisivulla **Setup → Basic Setup** sivulle. Valitse Internet Connection Type kohdasta Static IP. Täytä sivulle ilmestyvät asetukset ylös ottamiesi tietojen pohjalta. Tallenna tämän jälkeen muutokset. Kytke takaisin RJ45 johto langattoman reitittimen ja Internet yhteyden välille. Testaa Internet-yhteyden toimivuus.

Internet-yhteyden toimiessa Static IP ominaisuuden avulla, määritä tämän jälkeen Internet Connection Type takaisin automatic configuration DHCP tilaan **Setup → Basic Setup** sivulta.

Tallenna muutokset

12. Kiinteän IP-osoitteen määrittäminen

Mene molemmilla tietokoneilla **Start → Run** ja syötä avautuvaan kenttään ”cmd” komento, jolla pääset komentokehotteeseen. Tarkastele molempien tietokoneiden IP-tietoja kirjoittamalla komentokehotteeseen ”ip-

config /all” komento. Ota molempien tietokoneiden IP-tiedot ylös muistioon.

**** Jos” ipconfig /all” komento ei toimi, tarkasta että olet sellaisessa juuressa, jossa komennon suorittaminen on sallittua ****

Mene seuraavaksi hallinnointisivun **Setup → Basic Setup** sivulle. Vaihda seuraavaksi kohtaan Start IP Address IP-osoitteiden alkaminen 192.168.1.110 IP-osoitteesta. Määritä samalla Maximum Number of Users kolmeenkymmeneen IP-osoitteeseen. Tallenna muutokset.

**** Jos muutosten jälkeen et pääse enää muodostamaan yhteyttä reitittimen hallinnointisivulle, ota langattomasta reitittimestä virrat hetkeksi pois päältä ja laita ne hetken päästä takaisin. Yritä muodostaa yhteys uudestaan tämän jälkeen. ****

Seuraavaksi siirry DHCP Reservation tilaan painikkeen avulla. Määritä molemmille tietokoneille kiinteät uudet IP-osoitteet äskettäin määritellystä verkosta. Käytä hyväksi IP-osoitteiden varaamiseen langattoman verkon päätelaitteiden MAC-osoitteita. Tallenna muutokset.

Tyhjennä molempien koneiden IP-tiedot komentokehotteesta ”ipconfig /release” komennolla. Uudista IP-tiedot käyttämällä komentoa ”ipconfig /renew”**.** Tarkasta molempien koneiden uudet IP-tiedot ja vertaa niitä ylös ottamiisi tietoihin. Testaa myös molempien koneiden Internetin toimivuus.

Mene hallinnointisivulla **Administration → Log** sivulle ja tarkastele DHCP lokeihin tallentuneita tietoja. Vertaa vastaavatko tiedot tekemiäsi muutoksia? Tallenna tallentuneet lokitiedot kovalevylle Save The Log painikkeen kautta.

Mene hallinnointisivulla **Status → Local Network** sivulle. Tarkastele sivun tietoja ja samalla myös DHCP Client table painikkeen takaa aukeavalta sivulta.

13. Wireless MAC filter

Kytke langattoman reitittimen ja tietokone1:sen välinen rj-45 johto takaisin paikoilleen.

Testaa molempien tietokoneiden langattoman verkon ja Internetin toimivuus. Mene seuraavaksi hallinnointisivulla **Wireless → Wireless MAC Filter** sivulle. Määritä Wireless Mac Filter asetus päälle. Valitse samalla kohtaan Permit PCs listed below to access the wireless network valinta päälle. Tallenna muutokset. Testaa molempien tietokoneiden langattoman verkon ja Internetin toimivuus muutoksien jälkeen. Määritä tämän jälkeen **Wireless → Wireless MAC Filter** sivulle molempien tietokoneiden langattoman päätelaitteiden MAC-osoitteet. MAC-osoitteiden lisäämisen jälkeen tallenna muutokset. Testaa langattoman verkon toimivuus molemmilla tietokoneilla.

Yhteyksien toimiessa, määritä **Wireless → Wireless MAC Filter** sivulta MAC Filter ominaisuus takaisin pois päältä. Tallenna muutokset ja testaa toimivuus.

14. Palomuurin ominaisuudet

Testaa jonkin seuraavan ominaisuuden toimivuus jommallakummalla tietokoneella: Proxy, Java, Active X tai Cookies. Varmista, että kyseinen ominaisuus varmasti toimii kokeilemallasi sivulla. Mene hallinnointisivulla **Security → Firewall** sivulle. Web Filter kohdasta määritä kyseisen ominaisuuden esto päälle langattomaan reitittimeen. Tallenna muutokset. Testaa toimivuus.

Palauta palomuurin asetukset oletusasetuksille. Tallenna muutokset.

15. Virheiden ja ongelmien määritys

Mene hallinnointisivulla **Administration → Diagnostics** sivulle. Pingaa sivulta molempien koneiden IP-osoitteita. Pingaa sen jälkeen langattoman reitittimen IP-osoitetta ja www.google.fi osoitetta. Suorita samat pingaustestit tietokoneiden komentokehotteesta. Suorita samalla traceroute testi langattoman reitittimen hallinnointisivulta toisen tietokoneen IP-osoitteeseen.

16. Varmuuskopiointi

Kytke tietokone1 ja langattoman reitittimen välinen RJ-45 johto takaisin kiinni.

Mene hallinnointisivun **Administration → Management** sivulle. Vaihda Router Access kohtaan reitittimen kirjautumissalasana. Tallenna muutokset ja testaa toimivuus. Vaihda tämän jälkeen salasana takaisin oletussalasanalle ”admin”. Tallenna muutokset ja testaa toimivuus.

Muodosta **Administration → Management** sivulla varmuuskopiotiedosto kohdasta Backup Configurations. Talleta tiedosto tietokoneen kovalevylle. Mene tämän jälkeen **Administration → Factory Defaults** sivulle ja palauta langattoman reitittimen oletusasetukset Restore Factory Defaults kohdasta. Tarkista langattoman reitittimen hallinnointisivulta, että oletusasetukset ovat palautuneet reitittimelle.

Palauta laboratoriotyön aikana määritellyt asetukset varmuuskopiotiedoston avulla takaisin **Administration → Management** sivun Restore Configurations ominaisuuden kautta. Tarkista asetuksien palautuminen ennalleen langattomaan reitittimeen.

Mene tämän jälkeen **Status → Wireless Network** sivulle ja tarkastele mitä tietoja langattoman verkon asetuksiin on määritelty.

**** Palautathan langattoman reitittimen asetukset oletusasetuksille käyttösi jälkeen. Säilytä varmuuskopio, jos tarkoituksena on suorittaa myös laboratorio-ohje 2 osio****

KYSYMYKSIÄ

1. Mistä johtuu 2.4 ja 5 GHz:n verkkojen status tiedoissa näkynyt ero nopeudessa?
2. Mitä käytännön eroja langattoman verkon muodostamisessa oli Wi-Fi Protectedin ja manuaalisen muodostamisen välillä? Millä muilla tavoilla on mahdollista muodostaa yhteys Wi-Fi protected Setupin avulla, kuin laboratorion yhteydessä käytetyn Wi-Fi painikkeen avulla?
3. Miksi toisen tietokoneen Internet toimi kohdassa 12. Wireless MAC filter, vaikka määriteltiin, ettei yhdenkään koneen yhteys toimi jonka MAC osoitetta ei ole listalle määritelty?
4. Mitä ominaisuus Key Renewal tekee? Miksi WEP käyttöä ei enää suositella langattoman verkon salauksena?
5. Mikä merkitys SSID Broadcastin disabloimisella on tietoturvanäkökulmasta?

LIITE 2

LABORATORIO-OHJE 2

1. Valmistelu

Laboratorion tavoitteena on opettaa ja havainnollistaa laajemmin langattoman reitittimen toimintaa ja sen monipuolisia ominaisuuksia. Oppilaan tulisi tuntea laboratorion jälkeen seuraavat asiat:

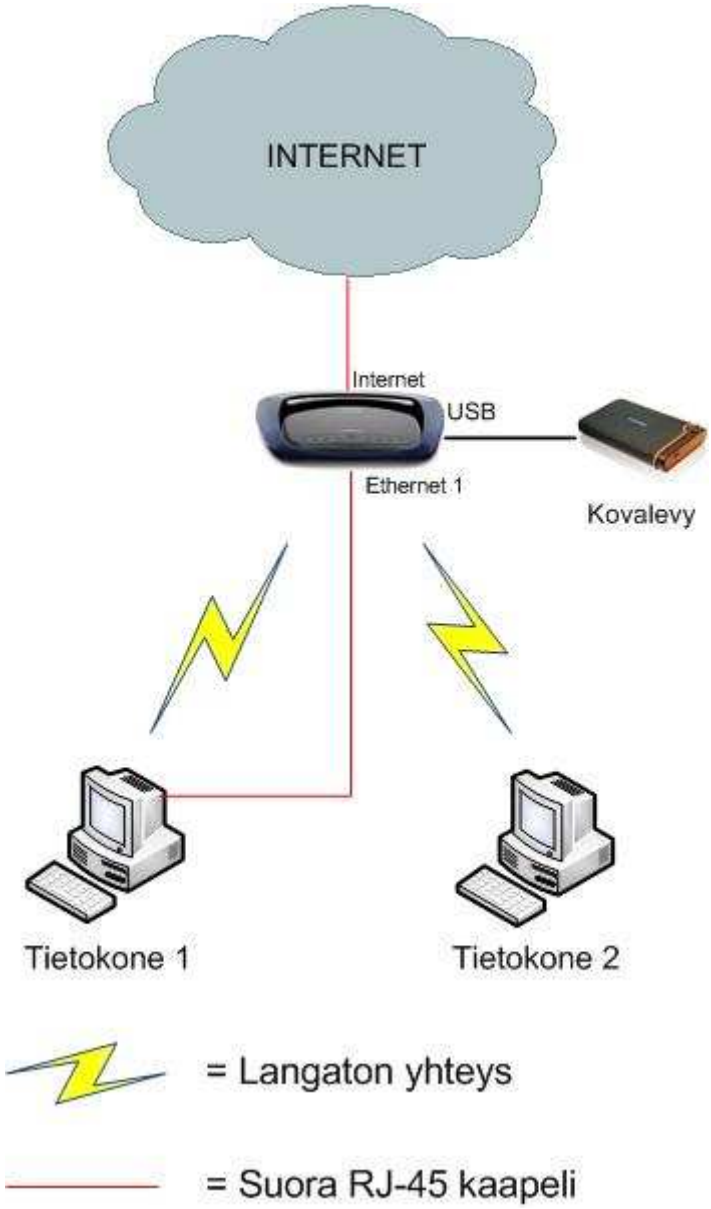
- DMZ / Demilitarized Zone
- Internet käyttörajoitukset
- reitittimen reititys
- QoS / Quality of Service
- Muistijärjestelmät verkossa

Laboratorio-ohje on suunniteltu ja tarkoitettu Windows XP SP3 käyttöjärjestelmälle. Laboratoriotyö tulisi aloittaa lataamalla laboratoriotyö 1 osuuden aikana tallennettu varmuuskopio langattomaan reitittimeen. Näin saadaan ensimmäisessä laboratoriotyössä luodut asetukset palautettua nopeasti langattomalle reitittimelle. Jos varmuuskopiotiedostoa ei ole saatavilla, on käyttäjän varmistettava, että ainakin seuraavat asetukset on määritelty langattomalle reitittimelle. Ohjeet asetuksien määrittämiselle löytyy laboratorio-ohje 1 osiosta:

- Setup → Basic setup
- Wireless → Basic wireless settings
- Wireless → Wireless security

Tämän jälkeen tulisi rakentaa seuraavalla sivulla olevan kuvan mukainen verkko. Laboratorion suorittamiseen tarvitaan WRT610N langattoman reitittimen lisäksi, joko ulkoinen kovalevy tai muistitikku. Langattoman verkon toiminta tulisi tarkistaa molemmilla verkoilla ja päätelaitteilla ennen siirtymistä kohtaan 2 - Langattoman verkon lisäasetuksiin.

**** Hallinnointisivun asetuksista löydät lisää tietoa help -linkin takaa, joka sijaitsee jokaisen sivun oikeassa reunassa ****



2. **Langattoman reitittimen lisäasetukset**

Kirjaudu langattoman reitittimen hallinnointisivulle selaimella osoitteeseen http://192.168.1.1. Jätä käyttäjätunnus tyhjäksi ja käytä salasanaa ”admin”. Mene hallinnointisivulta **Wireless → Advanced Wireless Settings** sivulle. Selvitä mitä sivun AP Isolation asetus määrittelee. Kytke asetus päälle sekä 2.4 että 5 GHz:n verkoille. Tallenna muutokset. Testaa ominaisuuden toiminta käytännössä verkossa esim. pingaamalla päätelaitteiden ja langattoman reitittimen IP-osoitteita ennen ja jälkeen asetuksen päälle asettamista. Muista käyttää langatonta yhteyttä testatessasi ominaisuuden toimintaa. Molempien tietokoneiden tulee olla yhteydessä samaan langattomaan verkkoon. Testattuasi ominaisuutta, kytke asetus pois päältä molemmista verkoista. Tallenna muutokset. Tutki mitä muita asetuksia **Wireless → Advanced Wireless Settings** sivulta löytyy.

3. VPN yhteyksien läpikulku

Mene hallinnointisivulta **Security → VPN Passthrough** sivulle. Selvitä, mihin hyötykäyttöön sivun asetukset on tarkoitettu?

4. Muistijärjestelmä

Kytke ulkoinen kovalevy tai muistitikku langattomaan reitittimen USB porttiin. Varmista, ettei kovalevyllä tai muistitikulla ole mitään tärkeitä tiedostoja. Mene hallinnointisivulla **Storage → Disk** sivulle. Varmista, että langaton reititin on tunnistanut liitetyn ulkoisen muistin. Sivun alalaidassa tulisi näkyä tiedot langattomaan reitittimeen liitetystä muistista. Valitse ruksi muistin kohdalta ja paina Format Disk**.** Määritä uudelle osiolle kuvaava nimi ja jatka painamalla Format.

Mene tämän jälkeen hallinnointisivulta **Storage → Administation** sivulle. Määritä Server Name -kohtaan kuvaava palvelin nimi. Tallenna muutokset.

Hae Linksysin sivuilta WRT610N User Guide PDF (osoite: http://www.linksysbycisco.com/APAC/en/products/WRT610N?lid=Learn More_WRT610N). Kohdasta ”How to install and access to USB storage” alkaen seuraa ohjeita ulkoisen muistin tunnistamiseen Windows XP käyttöjärjestelmässä. Suorita tämä toimenpide ensin Tietokone1:lle.

Kun olet saanut tunnistettua ja lisättyä ulkoisen muistin tietokoneelle, mene **My Computer →** ja luomasi aseman sisälle. Luo aseman sisälle jokin tiedosto esimerkiksi tekstitiedosto. Toteuta User Guide ohjeiden mukaisesti muistin tunnistus Tietokone 2:lle. Mene tämän jälkeen **My Computer →** ja luomasi aseman sisälle. Näetkö aseman sisällä tiedoston, joka luotiin Tietokone 1 avulla? Editoi tiedostoa Tietokone 2:n asemalta ja tallenna muutokset. Tarkista Tietokone 1:n asemalta, näkyykö tiedostolle tehdyt muutokset asemalla.

Tämän jälkeen voit poistaa luomasi asemat molemmilta tietokoneilta **My Computer →** luomasi aseman kohdalta oikealla hiiren napilla Disconnect. Mene tämän jälkeen langattoman reitittimen hallinnointisivulta **Storage → Disk** ja paina painikkeesta Safely Remove Disk. Tämän jälkeen voit turvallisesti poistaa muistitikun/kovalevyn langattomasta reitittimestä.

5. Tietoliikenneportin uudelleen lähetys

Mene seuraavaksi hallinnointisivulta **Applications and Gaming → Single Port Forwarding** tai **Applications and Gaming → Port Range Forwarding** sivulle. Selvitä mihin hyötykäyttöön sivun asetukset on tarkoitettu?

6. Internet käyttörajoitukset

Mene hallinnointisivulta **Access Restrictions → Internet Access Policy** sivulle. Tehtävänä on luoda kaksi sääntöä sääntökantaan, joilla rajoitetaan Internetin käyttöä verkossa. Määritä asetukset sääntöön numero 1, jossa

estät tietokoneelta 1 pääsyn tietylle Internet -sivulle Internet osoitteen perusteella. Tämän jälkeen määritä samalle säännölle numero 1, jossa estät tietyille Internet sivuille pääsyn avainsanojen perusteella. Keksi useampia avainsanoja, joiden perusteella esto suoritetaan. Määritä säännöt koskemaan pelkästään tietokonetta 1 IP-osoitteen perusteella. Anna säännölle kuvaava nimi ja aseta se päälle. Tallenna muutokset. Testaa säännön toimivuus molemmilla tietokoneilla.

Luo tämän jälkeen sääntö numero 2, jossa määrität eston Internetin käytölle ajan perusteella. Määritä ajaksi kyseinen viikonpäivä tai tunti ja määritä se koskemaan tietokonetta 2 MAC-osoitteen perusteella. Anna säännölle kuvaava nimi ja aseta se päälle. Tallenna muutokset ja testaa säännön toimivuus molemmilla tietokoneilla.

Mene tämän jälkeen hallinnointisivulla **Access Restrictions → Internet Access Policy** sivulle ja tutki luomiasi estolistoja Summary painikkeen kautta. Poista tämän jälkeen säännöt sääntötietokannasta. Tallenna muutokset.

7. Tietoliikenneportin tunnistus

Mene seuraavaksi hallinnointisivulla **Application & Gaming → Port Range Triggering** sivulle. Selvitä, mihin hyötykäyttöön sivun asetukset on tarkoitettu?

8. Ohjelmistopäivitys

Seuraavat asetukset tulee määrittää langattomalle reitittimelle tietokoneelta, joka on kaapelilla yhteydessä reitittimeen. Tätä toimenpidettä ei suositella suoritettavaksi langattoman verkon avulla.

Tarkista langattoman reitittimen nykyinen ohjelmistoversio. Tämän saat selville hallinnointisivun oikeassa yläkulmassa sijaitsevasta versionumerosta. Hae uusin ohjelmistoversio Linksysin kotisivuilta (osoite: http://www.linksysbycisco.com/US/en/support/WRT610N/download). Tallenna tiedosto tietokoneen kovalevylle.

Mene seuraavaksi hallinnointisivun **Administration → Firmware Upgrade** sivulle. Valitse tallentamasi tiedosto kovalevyltä hallinnointisivulla sijaitsevan ”selaa” painikkeen avulla. Aloita ohjelmistopäivitys Start Upgrade painikkeesta. Odota, kunnes ohjelmistopäivitys on saavuttanut 100 % tilan ja ikkunaan ilmestyy teksti ”Upgrade is successful”. Laitteelle voidaan päivittää myös sama ohjelmistoversio uudestaan, ellei uudempaa versiota ohjelmistoversiosta ole saatavilla.

Tarkista hallinnointisivun oikeasta yläkulmasta, onnistuiko ohjelmistoversion päivitys. Ohjelmistoversionumero pysyy samana, ellei uudempaa versiota ohjelmistoversiosta ollut saatavilla.

9. MAC-Address Clone

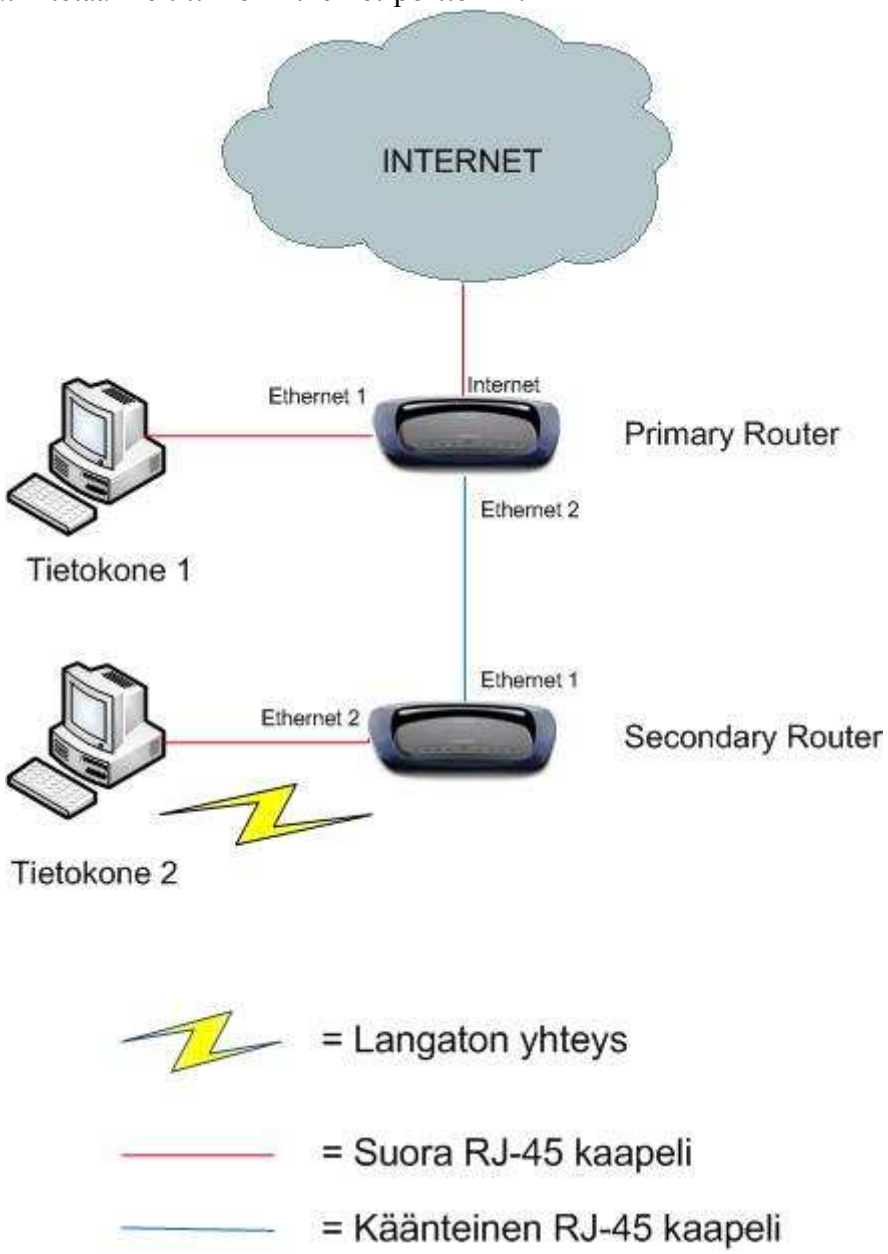
Mene seuraavaksi hallinnointisivulta **Setup → MAC Address Clone** sivulle. Selvitä mihin hyötykäyttöön sivun asetukset on tarkoitettu?

10. QoS - Quality of Service

Mene seuraavaksi hallinnointisivulta **Application & Gaming → QoS** sivulle. Selvitä, mitä QoS-termillä tarkoitetaan. Selvitä mihin hyötykäyttöön sivun asetukset on tarkoitettu?

11. Advanced Routing

Rakenna seuraavaksi alla olevan kuvan mukainen verkko. Tarvitset verkon rakentamiseen kahta WRT610N langatonta reititintä. Voit suorittaa tämän kohdan toisen ryhmän kanssa, ellei langattomia reitittimiä riitä muuten tarpeeksi jokaiselle ryhmälle. Huomioithan, että kahden langattoman reitittimen välillä tulee käyttää käänteistä RJ-45-kaapelia. Molemmat päät liitetään reitittimen Ethernet-portteihin.



Pidä edellisissä kohdissa käyttämäsi langaton reititin ensisijaisena reitittimenä ja lisää uusi reititin toissijaiseksi reitittimeksi. Palauta toissijaisen reitittimen asetukset laitteen oletusasetuksille.

Kirjaudu sisään toissijaisen reitittimen hallinnointisivulle. Määrittele hallinnointisivun **Setup → Basic** sivulta toissijaisen reitittimen IP-osoitteeksi jokin osoite, joka ei sisälly ensisijaisen reitittimen DHCP osoiteavaruuteen, esimerkiksi 192.168.1.253. Käytä aliverkon peitteenä osoitetta 255.255.255.0. Kytke samalta sivulta toissijaisen reitittimen DHCP palvelu pois käytöstä. Tallenna muutokset.

Kirjaudu toissijaisen reitittimen hallinnointisivulle käyttäen uutta määrittelemääsi IP-osoitetta. Mene seuraavaksi hallinnointisivulta **Wireless → Basic Wireless Settings** sivulle. Valitse langattoman verkon määrittäminen manuaalisesti. Määritä 2.4 GHz:n langattomalle verkolle omaperäinen tunnus kohtaan Network Name (SSID). Aseta Network mode asetus BG-Mixed asetukselle. Tallenna muutokset.

Mene seuraavaksi hallinnointisivun **Wireless → Wireless Security** sivulle ja määrittele 2.4 GHz:n verkolle salaukset. Käytä Security Modena WPA2-Personal ja pidä Encryption oletusasetuksella. Määritä Passphrase kohtaan omaperäinen salausavain. Tallenna muutokset. Tarkista ensisijaiselta reitittimeltä, että reitittimen IP-osoite on 192.168.1.1 ja **Setup → Advanced Routing** sivulla NAT-asetus on päällä.

Mene seuraavaksi toissijaisen reitittimen hallinnointisivun **Setup → Advanced Routing** sivulle. Määritä sivulta NAT-asetus ja Dynamic Routing (RIP) pois päältä. Määritä Destination LAN IP osoitteeksi kohdeverkon verkko-osoite, esimerkiksi koulun laboratorioluokan 10.0.0.0. Määritä aliverkon peitteeksi kohdeverkon aliverkon peitteen osoite, esimerkiksi 255.0.0.0. Yhdyskäytäväosoitteeksi määritetään osoite, mitä kautta kyseiseen verkkoon päästään. Tässä tapauksessa osoitteeksi määritetään ensisijaisen reitittimen IP-osoite 192.168.1.1. Interface -määritteeksi määritetään LAN & Wireless. Määritä Enter Route Name kohtaan kuvaava nimi tulevalle reititykselle. Tallenna muutokset.

Katso Show routing table painikkeesta, onko määrittelemäsi reitti ilmestynyt reititystauluun. Jos määrittelemääsi reittiä ei näy listalla, voit yrittää refresh painiketta painamalla saada reitityksen näkyviin reititystauluun. Toinen vaihtoehto on määritellä Dynamic Routing (RIP) asetus päälle. Tarkista ilmestyikö reititys tämän jälkeen reititystauluun. Tallenna muutokset.

Yhdistä tietokoneella 2 toissijaiselle langattomalle reitittimelle määrittelemääsi 2.4 GHz:n langattomaan verkkoon. Testaa tämän jälkeen langattoman verkon ja Internetin toiminta.

12. DMZ - Demilitarized zone

Mene ensisijaisen reitittimen hallinnointisivun **Applications & Gaming → DMZ** sivulle. Selvitä mitä DMZ määritelmä tarkoittaa. Aseta ominai-

suus päälle reitittimelle. Määritä Tietokone 2 toimimaan DMZ-Isäntänä verkossa, joko IP-osoitteen tai MAC-osoitteen perusteella. Tallenna muutokset.

**** Palautathan langattoman reitittimen asetukset oletusasetuksille käyttösi jälkeen. *****

KYSYMYKSIÄ

1. Mitä ”AP Isolation” termi tarkoittaa langattomassa verkossa? Miten se näkyy käyttäjille langattomassa verkossa?

2. Liittyen kohtaan 10. QoS - Quality of Service, mitkä lähiverkon ominaisuudet mielestäsi ovat tärkeimmät ja yhteyden kannalta tärkeysjärjestyksessä ensimmäisinä? Mitkä palvelut listalta mielestäsi taas eivät ole niin tärkeitä? Miksi kaikille ohjelmille ei kannata määritellä QoS ominaisuutta High -arvolle?

3. Selvitä mitä DMZ - Demilitarized Zone käsite tarkoittaa?

4. Mikä tarkoitus MAC-address clone asetuksella on?

5. Miksi ohjelmistopäivitystä ei suositella suoritettavaksi langattoman verkon avulla?