KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / Tietoverkkotekniikka

Sami Viipuri

HÄIRIÖTÖN LANGATTOMAN VERKKOYHTEYDEN VAIHTUMINEN

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

VIIPURI, SAMI	Häiriötön langattoman verkkoyhteyden vaihtuminen
Opinnäytetyö	41 sivua
Työn ohjaaja	Lehtori Jouko Pahlama
Toimeksiantaja	Steveco Oy
Toukokuu 2011	
Avainsanat	langattomat lähiverkot, GSM, roaming, vikasietoisuus

Tämän opinnäytetyön tarkoituksena oli toteuttaa ja testata Columbitech Wireless VPN -ohjelmistoa käyttäen ensisijaisen langattoman verkkotekniikan häiriötön vaihtuminen varayhteydeksi vikatilanteessa. Työ toteutettiin Kotkan Mussalon satamassa. Käytettävissä olivat 3G-, WiMAX- ja WLAN-verkkoliikennetekniikoilla toteutetut ympäristöt.

Testejä suoritettaessa Columbitech Wireless VPN Server- ja Columbitech Wireless VPN Client -sovellusten välille muodostettiin VPN-tunneli langatonta verkkoyhteyttä käyttäen. Tunnelin ylitse testattiin yrityksen operatiivisessa käytössä olevia sovelluksia, ja simuloimalla yhteyskatkoksia testattiin sovellusten vikasietoisuutta siirryttäessä käyttämään seuraavaa varayhteydeksi määritettyä langatonta verkkotekniikkaa. Testit suoritettiin sekä toimisto- että kenttäolosuhteissa. Yhteyskatkoksia simuloitiin irrottamalla päätteen verkkoadapteriin liitettyä kaapelia sekä irrottamalla WiMAX-ulkoyksikköön liitettyä antennia.

Alustavissa testeissä käytettävän tietoliikenneverkon vaihto kesti useita minuutteja. VPN-tunnelin tilan tarkkailua varten toteutettiin scripti, jolla yhteyskatkoksen tapahtuessa siirtymäaikaa saatiin nopeutettua. Käytettävän tietoliikenneverkon vaihtoon kuluva laskennallinen aika saatiin lopulta tiivistettyä välille 6–16 sekuntia, joka on suoraan riippuvainen scriptin suoritushetkestä suhteessa katkoksen tapahtumahetkeen. Testeissä katkoksen todettiin olevan riittävän lyhyt, jotta operatiivinen käyttö ei häiriintynyt ja näin opinnäytetyön tavoite saavutettiin.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

VIIPURI, SAMI	Interference Free Roaming Between Wireless Networks
Bachelor's Thesis	41 pages
Supervisor	Jouko Pahlama, Senior lecturer
Commissioned by	Steveco Oy
May 2011	
Keywords	WLAN, GSM, roaming, redundancy

The purpose of this Bachelors Thesis work was to test and accomplish a seamless switch between wireless networks by using the Columbitech Wireless VPN software. The study was carried out in the Kotka Mussalo port area. 3G-, WiMAX- and WLAN-network technologies were used in testing.

The testing was carried out by forming a VPN tunnel between the Columbitech Wireless VPN Server software and the Columbitech Wireless VPN Client software over a wireless network. Operational software was executed over the tunnel and, by simulating loss of connection, its redundancy was tested while roaming between wireless networks. Tests were carried out both in office and in field conditions. Connection losses were simulated by disconnecting the network cable connected to the network adapter and by disconnecting the antenna that was connected to the WiMAX outdoor unit.

In preliminary testing, roaming between the wireless networks took a long time. A script was created to observe the status of the actual VPN tunnel and to speed up the time used for roaming when loss of connection occurred. The calculated time used for roaming between the networks was eventually condensed to 6 - 16 seconds. The aforementioned time is directly dependant relative to the moment the script is executed in relation to the time loss of connection occurred. The time used for roaming was found to be short enough so that the operational use was not severely disturbed.

SISÄLLYS

SANASTO

2G	Second Generation
3G	Third Generation
3GGP	3rd Generation Partnership Project
4G	Fourth Generation
ASA	Adaptive Security Appliance
CSC	Content Security and Control
DHCP	Dynamic Host Configuration Protocol
DMZ	De-Militarized Zone
DSSS	Direct-Sequence Spread Spectrum
DSSS + CCK	Direct-Sequence Spread Spectrum + Complementary Code Keying
EAP-SIM	Extensible Authentication Protocol – Subscriber Identity Module
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
EAP-TTLS	Extensible Authentication Protocol – Tunneled Transport Layer Security
EDGE	Enhanced Data rates for GSM Evolution
FHSS	Frequency-Hopping Spread Spectrum
GINA	Graphical Identification and Authentication
GPRS	General Packet Radio Service
GPS	Global Positioning System
HSDPA	High-Speed Downlink Packet Access
IDU	Indoor Unit
IEEE	Institute of Electrical and Electronic Engineers
IMT-2000	Internet Mobile Telecommunications-2000
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ITU-R	International Telecommunication Union Radio Communication Sector
LDAP	Lightweight Directory Access Protocol
LEAP	Lightweight Extensible Authentication Protocol
LTE	Long Term Evolution
MIMO	Multiple-input Multiple-output
MMS	Multimedia Messaging Service
NIC	Network Interface Card
ODU	Outdoor Unit

OFDM	Orthogonal Frequency-Division Multiplexing
OFDMA	Orthogonal Frequency-Division Multiple Access
PCMCIA	Personal Computer Memory Card International Association
PEAP	Protected Extensible Authentication Protocol
PMP	Point-to-Multipoint
PTP	Point-to-Point
SIP	Session Initiation Protocol
SMS	Short Message Service
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunications System
VNIC	Virtual Network Interface Card
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WTLS	Wireless Transport Layer Security
WVPN	Wireless Virtual Private Network

1 JOHDANTO

Tämän opinnäytetyön toimeksiantajana on Steveco Oy. Työn tavoitteena oli testata Columbitech Wireless VPN -ohjelmistolla päätelaitteisiin toteutettua automaattista langattoman tietoliikenneverkon vaihtumista toissijaiseksi määritettyyn varayhteyteen, kun ensisijainen langaton verkkoyhteys katkeaa. Testattavana oli myös se, että katkoksen jälkeen yhteys palautuu takaisin ensisijaiseen tietoliikenneverkkoon. Tästä toiminnosta käytetään nimitystä roaming ja se tarkoittaa käytettävissä olevien langattomien verkkojen etsintää ja katkostilanteessa yhteyden automaattista siirtymistä verkosta toiseen. Testaus suoritettiin Mussalon satamassa sekä laboratorio- että kenttäolosuhteissa. Testituloksia tullaan mahdollisesti hyödyntämään Kotkan Hietasen satamanosan ja Haminan konttiterminaalin langattomien verkkojen kehittämisessä.

Erityisesti yritysverkoissa käytössä olevien langattomien verkkojen avulla toteutettujen yhteyksien vikasietoisuuteen ja redundanttisuuteen on alettu kiinnittää enemmän huomiota. Ongelmaksi langattomia verkkoteknologioita hyödynnettäessä on osoittautunut päätelaitteiden herkkyys reagoida yhteyskatkoksiin, joita eri syistä aiheutuu langattoman verkon toiminnassa. Hetkellinenkin yhteyskatkos voi aiheuttaa päätelaitteelta suoritettavan istunnon katkeamisen, jolloin yhteyden käyttäjä voi menettää tallentamattoman aineiston, jota hän langattoman yhteyden välityksellä on käsittelemässä. Käyttäjän täytyy muodostaa istunto kokonaan uudelleen ja pahimmassa tapauksessa aloittaa työnsä alusta. Ongelmiin, joita aiheutuu edellä kuvatuissa tilanteissa, on pyritty kehittämään erilaisia tekniikoita, joilla verkkoyhteyden katkeamiseen voitaisiin reagoida hallitusti, ja siten minimoida vaikutukset käyttäjän työskentelyyn.

Jos yrityksellä on käytössään vain yksi langatonta teknologiaa edustava verkko, voi käytettävänä menetelmänä tulla kyseeseen Citrix-tyyppinen asiakas/palvelin -ratkaisu. Siinä verkkokatkoksen tapahtuessa istunto pysyy palvelimella aktiivisena ja päätelaitteella toimii sellainen asiakassovellus, joka palauttaa yhteyden istuntoon heti verkkoyhteyden palauduttua. Katkoksen aikana päätetyöskentely on kuitenkin mahdotonta.

Jos käytössä on useampi kuin yksi langaton verkko, voidaan ajatella käytettäväksi konseptia, jossa katkoksen tapahduttua päätelaitteella toiminnassa oleva asiakasohjelmisto siirtyy etsimään seuraavaa käytettävissä olevaa tietoliikenneverkkoa ja löytäessään sellaisen ottaa sen käyttöön. Näin aiheutuu mahdollisimman pieni katkos päätе-

laitteen käyttäjän työskentelyyn. Tässä opinnäytetyössä perehdytään Columbitech Wireless VPN -ohjelmistoa hyödyntäen juuri tällaiseen tekniikkaan. Lisäksi perehdytään lyhyesti myös Ciscon AnyConnect Secure Mobility Client -ohjelmistoon.

Sovellusten toimintaan eniten vaikuttavaksi ongelmaksi osoittautui roaming-toiminnon epäonnistuminen WiMAX-tietoliikenneverkosta muihin käytettävissä oleviin verkkoihin, joita olivat 3G- ja WLAN-tietoliikenneverkot. Toimivan yhteyden tilan seurantaa varten tehtiin bat-scripti, joka tarkkaili Columbitech Wireless VPN Serverin ja Columbitech Wireless VPN Clientin välille muodostetun VPN-tunnelin tilaa ja tilanteen niin vaatiessa vapautti WiMAX-adapterin käytössä olleen IP-osoitteen. Se ratkaisi ongelman, ja siirtyminen ensisijaiselta WiMAX-yhteydeltä varayhteydelle saatiin toimimaan riittävän nopeasti, jotta käytössä olevat sovellukset eivät ehdi reagoida verkon vaihtumiseen.

2 LANGATTOMAT VERKOT

Steveco Oy:llä on tämän opinnäytetyön osalta testialueena toimivassa Mussalon satamanosassa käytössään erilaisia langattomia verkkotekniikoita hyödyntäviä verkkoympäristöjä, joten se sopii erinomaisesti roaming-toiminnon testien toteutukseen. Seuraavassa käydään lävitse näitä verkkotekniikoita, joita tässä työssä on hyödynnetty.

2.1 3G-teknologia

3G tarkoittaa kolmannen sukupolven matkapuhelinteknologiaa. Se on standardien kolmas sukupolvi matkapuhelimille ja mobiileille telekommunikaatiopalveluille ja noudattaa ITU:n International Mobile Telecommunications-2000 (IMT-2000) -määrityksiä (1, 21). ITU:n IMT-2000 maailmanlaajuinen standardi 3G:lle on raivannut tietä innovatiivisten sovellusten ja palveluiden käyttöönottamiseksi. (2).

3G-standardeja ovat UMTS- (3GPP:n standardoima) ja CDMA2000- (3GPP2:n standardoima) järjestelmät, joista UMTS on käytössä muun muassa Euroopassa, Japanissa ja Kiinassa. CDMA2000 puolestaan on pääsääntöisesti käytössä Pohjois-Amerikassa ja Etelä-Koreassa. (1, 15).

UMTS-verkkojen suunnittelussa kiinnitettiin erityistä huomiota datasiirron ja mobiilin multimedian kehittämiseen. Aiempien sukupolvien painopiste oli ollut enemmänkin puheluiden välittämisessä, kun datasiirtoa oli pidetty toissijaisena tehtävänä. (3, 171).

CDMA2000-verkkojen suunnittelussa lähtökohdat olivat samankaltaiset UMTS-verkkojen kanssa.

2.2 WiMAX-alueverkko

Mussalon satama-alueella käytössä oleva WiMAX-verkko on toteutettu IEEE 802.16-2004 -standardia noudattavalla tekniikalla, joka on paranneltu versio aiemmin julkaistusta IEEE 802.16-2001 -standardista. Tukiasemakohtainen teoreettinen siirtonopeus WiMAX-verkolla on 75 Mbps (4).

IEEE 802.16-2001 -standardi mahdollistaa vain sellaiset yhteydet, joissa tukiaseman ja päätelaitteen välillä on näköyhteys. Se johtuu käytössä olevasta korkeasta 10-66 GHz:n taajuusalueesta. Tästä syystä sitä ei voi käyttää ympäristöissä, joissa signaalin on pystyttävä läpäisemään esteitä, kuten esimerkiksi konttikasoja. Standardissa on määritelty verkkotopologiat Point-to-Point (PTP) ja Point-to-Multipoint (PMP). Point-to-Point-yhteys on vain yhden tukiaseman ja päätelaitteen välillä toimiva ratkaisu. Point-to-Multipoint puolestaan mahdollistaa useamman päätelaitteen yhteyden yhteen tukiasemaan. (5, 12).

IEEE 802.16-2004 toimii matalammalla 2-11 GHz:n taajuusalueella, jolloin signaaleilla on parempi kiinteiden esteiden läpäisykyky. Tämä mahdollistaa myös sellaiset yhteydet, joissa tukiasema ja päätelaite eivät ole näköyhteydessä toisiinsa. Standardi toi parannuksia myös tapaan, jolla modulointia hyödynnetään. Uudistuksia ovat muun muassa OFDM- modulaatiotekniikka ja adaptiivinen modulaatio. (5, 13). OFDM-modulaatiotekniikka mahdollistaa yhtäaikaisen tiedonsiirron useilla toisiaan häiritsemättömillä taajuuskanavilla (6). Adaptiivisella modulaatiolla saavutetaan käytettävän modulaatiotekniikan vaihtaminen dynaamisesti signaalin laadun perusteella. (5, 13).

IEEE 802.16e-2005 täydentää aiempia versiota tuomalla tuen yhteyden häiriöttömälle siirtymiselle tukiasemalta toiselle. Se pyrkii myös parantamaan verkon suorituskykyä OFDMA teknologialla. (5, 14). OFDMA on usean käyttäjän versio OFDM:stä. Siinä

käytössä olevilta taajuuskanavilta annetaan lohkoja yksittäisille käyttäjille. Tämä mahdollistaa useat yhtäaikaiset alhaisia datamääriä käsittävät yhteydet. (7).

2.3 WLAN-lähiverkko

Mussalon satamassa käytössä oleva WLAN-ratkaisu noudattaa IEEE 802.11 -standardia. Verrattuna lankaverkon lähiverkkotekniikoihin langattomien verkkojen teknologinen kehitys on ollut verrattain nopeaa. Tästä johtuen standardista on julkaistu useita eri versioita. Riippuen standardin IEEE 802.11 käytettävästä versiosta, käytössä olevat taajuusalueet ovat joko 2,4 GHz tai 5 GHz. Molemmat taajuusalueet on puolestaan jaettu useisiin kanaviin. Näiden käytön määrittävät tarkemmin eri maiden kansalliset säädökset. (3, 152).

IEEE 802.11-1997 on standardin alkuperäinen versio. Nykypäivän mittapuun mukaan se on kuitenkin jo vanhentunutta tekniikkaa. Se toimi 2.4 GHz:n taajuusalueella tarjoten enintään 2 Mbps:n tiedonsiirtonopeuden. Käytettävät modulointitekniikat olivat FHSS tai DSSS (3, 152).

IEEE 802.11a toimii 5 GHz:n taajuusalueella, ja sen tiedonsiirtonopeuden teoreettinen maksimiarvo on 54 Mbps. Käytettävä modulointitekniikka on OFDM. (3, 152). Siinä käytettävä virheenkorjauskoodi kuitenkin vähentää todellista saavutettavaa hyötykapasiteettia noin puoleen maksimikapasiteetista. (8, 591).

IEEE 802.11b oli suora laajennus alkuperäiseen standardiin. Se mahdollisti 11 Mbps:n maksimikapasiteetin. Se hyödyntää DSSS + CCK -modulointitekniikkaa. (3, 152). Standardin pohjalta toteutettujen laitteiden heikkoutena oli kuitenkin altistuminen häiriöille, joita muut 2.4 GHz:n taajuudella toimivat laitteet aiheuttivat (9, 23).

IEEE 802.11g toi huomattavaa parannusta 2.4 GHz:n taajuudella toimivaan alkuperäiseen standardiin mahdollistamalla 54 Mbps:n siirtonopeuden. Se voi hyödyntää DSSS + CCK -modulointitekniikkaa tai samaa OFDM -modulointitekniikkaa kuin IEEE 802.11a. (3, 152).

IEEE 802.11n -standardi hyödyntää sekä 2.4 GHz:n että 5 GHz:n taajuuksia. Merkittävin parannus on tuki MIMO- (multiple-input multiple-output) antenneille. (10, 270).

3 TESTAUKSESSA KÄYTETTÄVÄT LAITTEET JA KALUSTO

3.1 Päätelaitteet

Testauksessa käytetään muun muassa ajoneuvoihin asennettavissa olevaa LXE VX3-12 -päätettä (kuva 1), joka on Steveco Oy:lla yleisesti käytössä oleva päätemalli. Tavallisimmat päätteen asennuskohteet ovat konttikurottajat, lukit ja trukit.

Kuva 1. Ajoneuvopääte LXE VX3-12.

LXE:n pääte soveltuu erinomaisesti ankariinkin käyttöolosuhteisiin. Valmistajan ilmoittamat raja-arvot esimerkiksi työskentelylämpötiloista ovat -30–50˚C (11). Koska päätteen suunnittelussa on huomioitu erittäinkin vaihtelevat käyttö- ja sääolosuhteet, sopii se erinomaisesti käytettäväksi myös sataman vaativissa ja vaihtelevissa olosuhteissa.

3.2 Langattoman verkon asiakaslaitteet

3.2.1 3G- ja WLAN-verkot

Testauksessa on käytetty 3G- ja WLAN-yhteyksien osalta ajoneuvopäätteen PCMCIA-väylään liitettävää Option Globetrotter Fusion + HSDPA -yhdistelmäkorttia (kuva 2). Kortti on yhteensopiva lähes kaikkien Type II PC -korttipaikkaa tukevien PC-koneiden ja Microsoft Windows -käyttöjärjestelmien kanssa.

Kuva 2. Option Globetrotter Fusion + HSDPA PCMCIA -kortti.

Kortti tukee WLAN-yhteensopivuuden lisäksi yleisimpiä 2G- ja 3G-sukupolven standardeja. Kolmannen sukupolven standardeista ovat tuettuina (1.8 Mbps:n nopeuteen asti) HSDPA- ja UMTS-standardit. Toisen sukupolven standardeista ovat tuettuina (247 Kbps:n nopeuteen asti) EDGE-, GPRS- ja GSM-standardit. Kortin ominaisuuksiin kuuluu tuki käyttäjän huomaamatta tapahtuvaan häiriöttömään roaming-toimintoon UMTS- ja GSM/EDGE-verkkojen välillä. Roaming-toiminto on mahdollista toteuttaa saumattomasti myös WLAN- ja 2,5G/3G-verkkojen välillä kolmannen osapuolen ohjelmistoa hyödyntämällä. Opinnäytetyössä tähän tarkoitukseen käytettiin Columbitech Wireless VPN -sovellusta.

WLAN-yhteysnopeuksia kortti tukee 2.4 GHz:n taajuusalueella 54 Mbps:iin asti. Myös tuki IPSec- ja VPN-teknologioille on olemassa.

WLAN-yhteydet voidaan salata joko WEP- tai TKIP-menetelmällä käyttäen 64 tai 128 tavun avainta. Käytettävät autentikointimenetelmät ovat WPA-Enterprise, WPA-Personal, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, WPA2-Enterprise ja WPA2-Personal. Korttiin on sisäänrakennettu myös tuki kolmannen osapuolen video-puheluyhteys sovelluksille (3GGP 3G-324M, H.324, H264 Baseline Video) sekä SIP-, SMS-, IM-, MMS-, Internet- ja sähköpostisovelluksille.

Kortin mukana tulee myös GlobeTrotter Mobility Manager -sovellus yhteyksien hallintaan ja SMS-palvelujen käyttöä varten. Edeltävässä Option Globetrotter Fusion + HSDPA -yhdistelmäkortin kuvauksessa on käytetty lähteenä pakkauksen tuoteselostetta (12).

GlobeTrotter Mobility Manager -sovellusta tarvitaan vain WLAN- ja 3G-yhteyksien perusmäärityksiä varten. Tämän jälkeen ohjelmaa ei käytössä tarvita, vaan päätteellä käytössä olevien yhteyksien varsinainen hallinta tapahtuu Columbitech Wireless VPN Clientin kautta. Kortin kattavat ominaisuudet ja käyttöönoton helppous tekevät siitä oivallisen työvälineen monenlaisiin käyttöympäristöihin.

3.2.2 WiMAX-tekniikka

Mussalon satama-alueella on käytössä IEEE 802.16-2004 -standardin mukaisesti toteutettu verkko. Yhteys päätelaitteelta verkkoon on toteutettu Alvarionin BreezeMAX PRO -laitteilla (kuva 3). Päätelaitteeseen liitettävä laitekokonaisuus koostuu sisäyksiköstä (IDU), joka on liitetty verkkokaapelilla (Ethernet 10/100 BaseT) päätelaitteeseen. Sisäyksikkö on liitetty vastaavanlaisella verkkokaapelilla ulkoyksikköön (ODU). Ulkoyksikköön on liitetty WiMAX-antenni, jolla muodostetaan yhteys WiMAX-tukiasemaan.

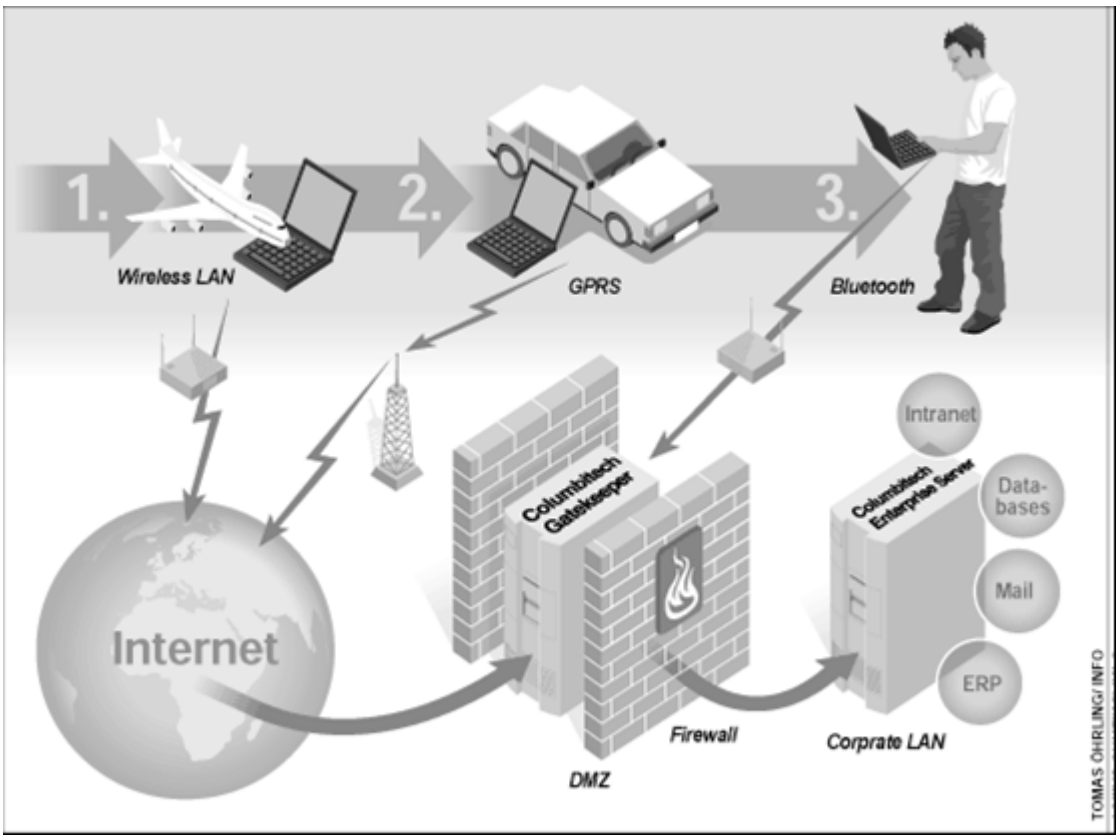
Kuva 3. Vasemmalla ulkoyksikkö ja oikealla sisäyksikkö.

4 TEKNIIKAT KATKENNEEN YHTEYDEN UUDELLEENOHJAAMISEEN

4.1 Columbitech Wireless VPN -ohjelmisto

4.1.1 Esittely

Columbitech Wireless VPN on langattomiin ympäristöihin suunniteltu istuntotason (session level) VPN-arkkitehtuuri. Painopisteenä on ollut eliminoida perinteisten VPN-ratkaisujen heikkoudet, joita ilmenee otettaessa niitä käyttöön langattomissa ympäristöissä. Tavoitteena on ollut turvata suojattu pääsy yritysverkkoihin ajasta, paikasta sekä käytettävästä laitteesta riippumatta (kuva 4) (13).



Kuva 4. Periaatekuva Columbitech Wireless VPN käyttömahdollisuuksista (13, 4).

Columbitech mahdollistaa suojattujen etäyhteyksien toteuttamisen asiakaslaitteiden ja kohdeverkon välillä, katkenneen yhteyden automaattisen uudelleenmuodostamisen, istunnon palauttamisen ja tiedonsiirron palauttamisen. Lisäksi on mahdollista suojattujen, saumattomien langattomien IP-verkkojen hakeminen (roaming-toiminto). Edellä mainitut toiminnallisuudet on mahdollista optimoida kaikille verkko- ja laitetyypeille (13).

Columbitech Wireless VPN -toteutus perustuu asiakas/palvelin (client/server) -periaatteelle. Palvelinohjelmisto asennetaan palvelimelle, ja asiakasohjelmisto puolestaan asennetaan niille mobiililaitteille, joilla suojattua Columbitech Wireless VPN -yhteyttä halutaan käyttää. Taulukossa 1 on luetteloitu Columbitech WVPN ohjelmiston tukemat käyttöjärjestelmä alustat. Asiakkaan muodostaessa yhteyden Columbitech Wireless VPN -palvelimen kautta suojattuun verkkoon avataan laitteiden välille autentikoitu ja suojattu tunneli, jonka lävitse liikenne ohjataan. Yhteys voidaan muodostaa joko Columbitech Gatekeeperin (suositeltu sijoituspaikka yrityksen DMZ-alueella) kautta tai suoraan Columbitech Wireless VPN -palvelimelle. Jos verkosta puuttuu palomuuri, voidaan Columbitech-palvelin konfiguroida myös tähän rooliin. Autenti-

koinnissa hyödynnetään seuraavien menetelmien yhdistelmiä: kertakäyttöinen salasana, asiakassertifikaatti ja käyttäjänimi/salasana (13).

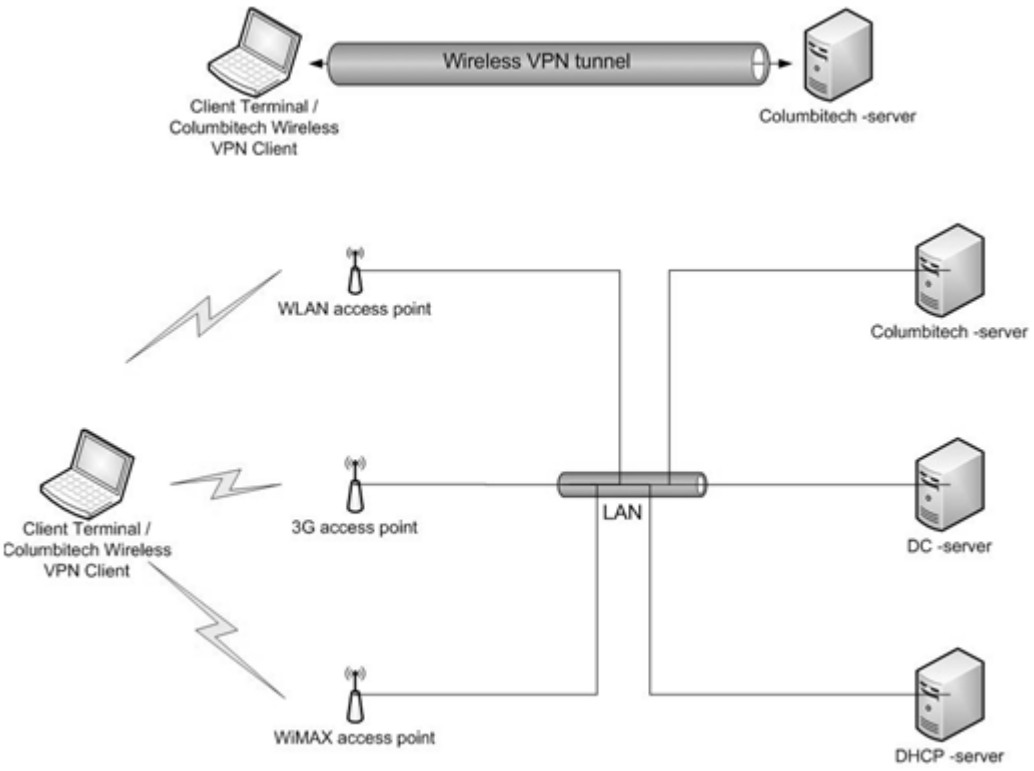
Taulukko1. Tuetut alustat.

Palvelinympäristöt	Asiakasympäristöt
• Windows 2000/2003 Server • Linux (kernel 2.6.8 tai korkeampi)	• Windows 2000 Professional • Windows XP Professional • Windows Vista (32/64 bit) • Windows 7 (32/64 bit) • Windows Mobile 5, Mobile 6 ja Mobile 2003

Columbitech integroituu saumattomasti olemassa oleviin yritysratkaisuihin. Langattomien VPN-ratkaisujen lisäksi sitä voidaan käyttää myös langallisessa verkkoinfrastruktuurissa. Columbitech Wireless VPN on saatu sulautumaan täysin läpinäkyväksi ratkaisuksi integroimalla se suoraan IP-kommunikaatiopinoon (IP communication stack) (13).

4.1.2 Testikonfiguraatio

Tässä testikonfiguraatiossa Columbitech Wireless VPN -ratkaisu on toteutettu käytettäväksi yrityksen sisäverkossa (kuva 5). Columbitech-palvelimen roolina on toimia langattomia yhteyksiä käyttävien laitteiden virtuaalisena yhdyskäytävänä ja turvata sen kautta ohjattavien yhteyksien jatkuvuus ympäristöissä, joissa käytössä on useampia eri yhteystyyppejä.



Kuva 5. Periaatekuva Columbitech Wireless VPN -ratkaisusta. Kuvassa ylimpänä on looginen toimintakuva ja alempana fyysinen pohjakuva.

Columbitech Wireless VPN Server hyödyntää käyttäjien autentikoinnissa Stevecon toimialuepalvelinta käyttämällä LDAP-protokollaa. Päätelaitteelle asennettu Columbitech Wireless VPN Client hyödyntää kirjautumisprosessissa Microsoft XP -käyttöjärjestelmän GINA-moduulia.

IP-osoitteiden jakamiseksi asiakaslaitteiden Columbitech VNIC -adaptereille on käytössä Stevecon DHCP-palvelin, jolloin WVPN-yhteyksiä muodostettaessa Columbitech WVPN Client muodostaa yhteyden Columbitech-palvelimeen. Se puolestaan käy noutamassa IP-osoitteen DHCP-palvelimelta ja välittää sen asiakaslaitteen virtuaaliselle NIC-adapterille. Näin ollen jokaisella asiakaslaitteella on käytössään vähintään kaksi IP-osoitetta. Yksi tai useampi osoite on myönnetty laitteen fyysisille NIC-adaptereille, jotka edustavat laitteen todellista liityntäpistettä verkkoon ja yksi on myönnetty päätelaitteen VNIC-adapterille, joka puolestaan edustaa Columbitech WVPN Clientin virtuaalista liityntäpistettä verkkoon. Fyysisen liittymän IP-osoitteen myöntäminen tapahtuu suoraan DHCP-palvelimen kautta, kun pääte muodostaa yhteyden käytössä oleviin verkkoresursseihin.

Columbitech-palvelimen toimiessa toimialueen DHCP-palvelimen jakamien osoitteiden välittäjänä, on sen verkkoadapterilla oltava osoite, joka on samalla osoitealueella kuin Columbitech Wireless VPN Clientille jaettavat osoitteet. Edellä mainittu pätee myös tilanteessa, jossa Columbitech-palvelin toimii myös DHCP-palvelimena. Tällöin on tärkeää konfiguroida jaettava osoitealue niin, että se ei ole ristiriidassa muiden verkossa käytössä oleville laitteille jaettujen osoitteiden kanssa. Samalla Columbitechin kautta jaettavat osoitteet on aiheellista rajata DHCP-palvelimen jakamien osoitteiden ulkopuolelle.

4.2 Cisco 5500 Series ASA - Cisco AnyConnect Secure Mobility Client

Seuraava teksti pohjautuu kokonaisuudessaan Ciscon julkaisemiin dokumentteihin. Käytännön testejä ei Ciscon ratkaisulla ole ollut mahdollista suorittaa.

Cisco 5500 sarjan ASA-tietoturvalaitteisto on monipuolinen kokonaisuus, jossa on tilallinen (stateful) palomuuri ja VPN-keskitin samassa laitteessa sekä laitteen mallista riippuen myös IPS-tunkeutumisen estojärjestelmä tai vaihtoehtoisesti integroitu CSC-moduuli sisällön valvontaan ja hallintaan. Sen lisäksi että ASA-tietoturvalaitteilla voidaan toteuttaa suojattujen yhteyksien muodostaminen niin yritysverkon sisältä kuin myös ulkoa, käyttämällä sekä langattomia että langallisia tietoliikenneverkkoja, voidaan sitä käyttää myös palomuurina ja verkon turvalaitteena, jolla valvotaan ja kontrolloidaan verkkojen välistä liikennettä (14).

Tässä opinnäytetyössä käsiteltyä Columbitech Wireless VPN -ratkaisua vastaava toteutus voitaisiin saavuttaa hyödyntämällä Cisco AnyConnect Secure Mobility Client -asiakasohjelmistoa. Se on Ciscon ratkaisu langattomien laitteiden turvattujen etäyhteyksien muodostamiseksi. Päätelaitteilla voidaan muodostaa IPSec (IKEv2) tai SSL VPN -yhteydet Cisco 5500 Series ASA -tietoturvalaitteeseen (15).

Cisco AnyConnect Secure Mobility Client voidaan ottaa käyttöön kahdella eri tavalla, joko käyttämällä yrityksen ohjelmistojen jaossa käytettäviä järjestelmiä tai suoraan etäyhteyden muodostaville käyttäjille ASA-tietoturvalaitteeseen. Jaettaessa ohjelma ASA-tietoturvalaitteelta käsin muodostavat käyttäjät yhteyden syöttämällä käyttämänsä Internet-selaimen osoitekenttään palomuurin IP-osoitteen tai DNS-nimen. Tämä yhteydenmuodostusmenetelmä on niin sanottu asiakkaaton SSL VPN (clientless SSL VPN). ASA tuo selaimen ikkunaan kirjautumisruudun, johon käyttäjän on annettava

asianmukaiset autentikoinissa vaadittavat tunnukset. Tämän jälkeen päätteelle ladataan asiakkaan käyttöjärjestelmää vastaava asiakasohjelma. Seuraavaksi Cisco AnyConnect Secure Mobility Client asentaa ja konfiguroi itsensä, jonka jälkeen se muodostaa suojatun yhteyden joko IPSec- (IKEv2) tai SSL-protokollalla ASA-tietoturvalaitteeseen (15).

Cisco AnyConnect Secure Mobility Clientin käynnistys ja käyttäjän autentikointi voidaan automatisoida digitaalisia sertifikaatteja hyödyntämällä. Tällöin Clientin käynnistys ja yhteydenmuodostus käytettäviin verkkoresursseihin voidaan suorittaa täysin automaattisesti. Yhteys Cisco AnyConnect Clientin ja ASA-tietoturvalaitteen välillä pitäisi säilyä aktiivisena myös verkon roaming-toiminnon aikana, kunhan Client on konfiguroitu olemaan aina päällä (15).

5 COLUMBITECH WIRELESS VPN SERVER- JA COLUMBITECH WIRELESS VPN CLIENT -OHJELMISTOJEN KONFIGUROINTI

5.1 Ongelmat DHCP-palvelimelta jaettujen osoitteiden myöntämisessä

Ensimmäisissä testeissä ongelmaksi muodostui IP-osoitteen välittäminen Columbitech Wireless VPN-palvelimen kautta Columbitech Wireless VPN Clientin käyttämälle virtuaaliselle verkkoadapterille. Yhteyden muodostusyrityksestä luotua lokia tarkasteltaessa voitiin havaita, että DHCP-palvelimen myöntämän IP-osoitteen välittämisyritys kilpistyi WTLS-virheeseen. DHCP-palvelimen Leased Address -listalla osoitteet, joita yritettiin Columbitech WVPN Clientille myöntää, näkyivät BAD ADDRESS -tilassa. Nämä BAD ADDRESS -tilassa olevat liittymät eivät olleet myöskään muiden samasta DHCP-poolista osoitteita hakevien laitteiden käytettävissä, ennen kuin niiden aiottu Lease-aika umpeutui, ellei niitä poistettu listalta manuaalisesti.

Columbitech Wireless VPN Clientin toimivuutta testattiin myös myöntämällä virtuaaliselle adapterille IP-osoite manuaalisesti halutulta osoitealueelta. Tällöin yhteyden muodostus Columbitech Clientin kautta onnistui ja VPN-tunnelin kautta saatiin muodostettua yhteys. Tällä keinoin saatiin kuitenkin varmistuttua, että VPN-tunnelin muodostaminen langattoman verkon ylitse on mahdollista.

Lopulta havaittiin, että Columbitech Wireless VPN-palvelimen IP-osoite oli eri osoitealueella kuin Columbitech Wireless VPN Clientille jaetut IP-osoitteet. Kun Colum-

bitech Wireless VPN-palvelimelle myönnettiin oikea IP-osoite, saatiin ongelma korjattua ja DHCP-palvelimen myöntämien osoitteiden välittäminen Columbitech WVPN-palvelimen kautta alkoi toimia.

5.2 Sertifikaattien asennus

Columbitech Wireless VPN palvelimen ja Columbitech Wireless VPN Clientin välillä tarvitaan käyttäjien autentikoinnissa sertifikaattia. Sitä käytetään lisävarmenteena Windowsin käyttämän autentikoinnin lisäksi. Saman sertifikaatin on oltava asennettuna sekä palvelimelle että päätelaitteelle. Sertifikaatti on asennettava kaikille niille käyttäjille, jotka tulevat päätteellä työskennellessään käyttämään Columbitech Wireless VPN Client -sovellusta.

5.3 Columbitech AutoWVPN

Columbitech Wireless VPN Client ei asennuksen jälkeen käynnisty automaattisesti. Tätä varten on päätteelle tarpeen asentaa erillinen palvelu, joka tulee huolehtimaan Columbitech Wireless VPN Clientin automaattisesta käynnistymisestä. Client-ohjelmiston asennuksen yhteydessä tarpeelliset tiedostot AutoWVPN-palvelua varten kopioituivat valmiiksi päätteelle.

AutoWVPN-palvelun (kuva 6) asennus vaatii järjestelmänvalvojan oikeudet. Asennus suoritetaan komentorivillä antamalla komento *`autowvpn.exe -install käyttäjätunnus salasana toimialue`*. Palvelun toimivuuden voi testata välittömästi asennuksen jälkeen käskyllä *`autowvpn -connect`*. Columbitech Wireless VPN Client muodostaa yhteyden VPN-tunnelin ylitse prioriteetissa korkeinta käytettävissä olevaa yhteyttä hyödyntäen. Jatkossa aina päätteen käynnistyessä myös Columbitech Wireless VPN Client käynnistyy, ellei palveluun erikseen tehdä muutoksia.

Alerter	Notifies sel...		Disabled	Local Service
Application Layer G...	Provides s...	Started	Manual	Local Service
Application Manage...	Provides s...		Manual	Local System
ASP.NET State Ser...	Provides s...		Manual	Network S...
Auto WVPN		Started	Automatic	Local System
Automatic Updates	Enables th...	Started	Automatic	Local System
Background Intellig...	Transfers f...		Manual	Local System
ClipBook	Enables Cli...		Disabled	Local System

Kuva 6. Käyttöjärjestelmän Services luetteloon lisätty AutoWVPN-palvelu.

5.4 Columbitech Wireless VPN Client konfigurointi

Columbitech Wireless VPN Clientille on ennen käytön aloittamista tarpeen konfiguroida muutamia asetuksia, ennen kuin se on valmis muodostamaan yhteyden VPN-tunnelin ylitse. Seuraavassa on kuvattu tärkeimmät asetukset.

Profiilikohtaiset asetukset

Columbitech Wireless VPN Client -asetuksia voidaan mukauttaa määrittämällä käyttöön profiileja, joille voidaan määrittää eri asetuksia tilanteen vaatimusten mukaisesti. Profiilien käyttö on pakollista, joten vähintään yksi profiili on luotava.

Profiilikohtaisissa asetuksissa määritetään muun muassa sallitaanko pääsy verkkoon myös WVPN-yhteyden ulkopuolelta. Tämä asetus valitsemalla voidaan käyttäjän oikeuksilla päätteellä työskentelevän henkilön sallia itse valita, käytetäänkö päätettä suojatussa tai suojaamattomassa tilassa. Suojaamattomassa tilassa palomuuri on kytketty pois päältä, kun yhteyttä Columbitech WVPN -palvelimeen ei ole muodostettu. Tämä asetus on tärkeä tilanteissa, joissa Columbitech WVPN Clientillä varustettua päätettä käytetään julkisissa verkoissa. Tällöin asetuksen pitäisi aina olla suojattu, jotta palomuuri on aina aktiivisena.

Profiilikohtaisiin yhteysasetuksiin on määritettävä vähintään yhden Columbitech-palvelimen IP-osoite tai isäntänimi sekä käytettävä porttinumero. Käytettävälle profiilille määritetään saatavilla olevista yhteyksistä ne, joita kyseessä olevan profiilin yhteydessä käytetään. Stevecon testiympäristössä mahdollisia valintoja olivat siis WLAN-, WiMAX- ja 3G-yhteydet. Lisäksi määritetään yhteyksien käyttöprioriteetit ja tarvittaessa Access Point Name, johon yhteys tullaan muodostamaan. Käytettäville

yhteyksille voidaan myös määrittää niiden käynnistys ja katkaisu automaattisesti verkkoyhteyttä käyttöönotettaessa.

5.5 Scripti Columbitech Wireless VPN Clientin muodostaman VPN-tunnelin tarkkailuun

Columbitech vaikuttaa kokonaisuutena tarjoavan varsin tehokkaan ympäristön langattomien verkkoyhteyksien vikasietoisuuden varmentamiseen. Kuitenkin tilanteissa, joissa verkkoyhteyden katkeaminen ei välittömästi heijastu käytettävissä olevaan verkkoliitäntään, kuten WiMAX-yhteyden tapauksessa käy, saattaa Columbitech WVPN Clientiltä kestää pitkäänkin, ennen kuin se saa otettua käyttöön varayhteydeksi määritetyn yhteyden. Päätteellä työskentelevän henkilön kannalta tämä tarkoittaa sitä, että työskentely keskeytyy ja jatkuu vasta, kun istunto on jälleen käytettävissä. Jos katkos on kestänyt useita minuutteja, on todennäköistä, että ennen katkosta aktiivisena olleet istunnot eivät enää palaudu, vaan istunnot on aloitettava uudelleen.

Käytännössä Columbitech WVPN Client reagoi WiMAX-yhteyden katkoksiin seuraavalla tavalla:

> Tilanteessa, jossa verkkokaapelin irrottaa joko päätteen verkkoliittimestä tai toisesta päästä WiMAX-jakajasta, Columbitech WVPN Client pystyy välittömästi vaihtamaan käytettävissä olevaan varayhteyteen.
>
> Jos yhteys puolestaan katkeaa esimerkiksi joko WiMAX-tukiaseman pudottua pois pelistä tai yhteyskatkoa simuloidaan irrottamalla antenni vastaanottimesta, tällöin varayhteyden käyttöönotto kestää pitkään.

Jälkimmäisessä tilanteessa ongelma ilmenee siten, että yhteyden katkettua verkkoliittimelle jää vielä sidosinformaatio adapterille myönnetystä IP-osoitteesta, vaikka tunnelin muodostama yhteys on jo katkennut. Columbitech WVPN Client havaitsee, että liikenne tunnelissa on katkennut, mutta ei pysty kuitenkaan välittömästi siirtymään varayhteyden käyttöön. Client siirtyy Searching -tilaan, mutta johtuen adapterilla edelleen olevasta IP-osoitteesta, yrittää Columbitech WVPN Client sinnikkäästi ottaa WiMAX-yhteyttä käyttöön.

Tilanteen ratkaisemiseksi oli tarpeen kirjoittaa lyhyehkö scripti, joka tarkkailee aktiivisen VPN -tunnelin tilaa pingaamalla verkon yhdyskäytävää ja tarvittaessa vapauttaa

WiMAX-yhteyden käyttämän adapterin IP-osoitteen. Kun scripti havaitsee, että tunnelin läpi kulkeva yhteys on katkennut, se vapauttaa vain WiMAX-yhteyden käyttämän adapterin käytössä olleen IP-osoitteen. Samalla kun adapterin osoite vapautuu, Columbitech WVPN Client aktivoituu etsimään seuraavaa vapaata yhteyttä, ja tämän jälkeen yhteyden käyttöönotto tapahtuu sekunneissa.

Käytännön kenttätestauksessa osoittautui tarpeelliseksi hieman lyhentää scriptin suoritusten välissä käytettävää ajastusväliä, jotta se ehti reagoida riittävällä nopeudella simuloituihin yhteyskatkoksiin. Testattaessa scriptiä ilman ajastusta, jolla säädetään suoritusten aikaväliä, Columbitech WVPN Clientillä ilmeni ongelmia yhteyden vaihtamisessa simuloitaessa yhteyskatkoksia.

Ajastuksessa käytetään Microsoft Windows Server 2003 Resource Kitistä löytyvää sleep.exe-ohjelmaa. Microsoft Windows Server 2003 Resource Kit on ladattavissa ilmaiseksi Microsoft Download Centeristä.

conn_check.bat ja ***sleep.exe*** on sijoitettu samaan C:-aseman alle luotuun batit-kansioon. Testauksen aikana scripti käynnistettiin automaattisesti kopioimalla siihen osoittava pikakuvake **Users** -käyttäjäprofiilin **Startup**-kansioon.

Jos scripti halutaan piilottaa käyttäjältä, voidaan se ajastaa Windows-käyttöjärjestelmän Scheduled Tasks (Ajoitetut tehtävät) -palvelun kautta suoritettavaksi päätteelle kirjautumisen yhteydessä. Ajastusta toteutettaessa on suorittavaksi käyttäjätunnukseksi määriteltävä esimerkiksi paikallisen järjestelmänvalvojan tunnukset, jolloin sitä suoritetaan taustalla käyttäjän näkymättömissä.

Scripti VPN-yhteyden tilan seurantaan:

```
rem BATIN KÄYNNISTYKSEEN 30 SEKUNNIN VIIVE
rem JOTTA KÄYTETTÄVÄT VERKKOYHTEYDET EHTIVÄT KÄYNNISTYÄ
sleep 30

:begin
@echo off

rem TESTATAAN VPN PUTKEN TOIMIVUUS PINGAAMALLA YHDYSKÄYTÄVÄÄ
rem LÄHETETÄÄN KAKSI PYYNTÖÄ TAVANOMAISEN NELJÄN SIJASTA
rem REAGOINTINOPEUDEN LISÄÄMISEKSI MAHDOLLISEN KATKOKSEN
rem TAPAHTUESSA
ping –n 2 XXX.XXX.XXX.XXX

rem ERRORLEVEL: 0 - PING VASTAA
rem ERRORLEVEL: 1 - PING EI VASTAA

echo tulos %errorlevel%

rem JOS YHTEYSVÄLI ON POIKKI, SIIRRYTÄÄN KOHTAAN ONGELMA
if not errorlevel 0 goto ongelma
echo kaikki OK %errorlevel%

:ongelma

rem JOS YHTEYSVÄLI TOIMII, SIIRRYTÄÄN BATIN LOPPUUN
rem JA SIVUUTETAAN KORJAUSTOIMENPITEET
if not errorlevel 1 goto loppu

rem EVENTCREATE KOMENNOLLA KATKOKSET SAADAAN KIRJATTUA EVENT LOGIIN
echo yhteysongelma %errorlevel%
eventcreate /l application /id 900 /so LANTesti /t warning /d "yhtey-
dessä havaittu ongelma"

echo vapautetaan WiMAX osoite
eventcreate /l application /id 901 /so LANTesti /t warning /d "aloi-
tetaan osoitteen vapautus"
rem VAPAUTTAA VAIN WIMAX YHTEYDEN KÄYTTÄMÄN ADAPTERIN OSOITTEEN
ipconfig /release "Local Area Connection"
eventcreate /l application /id 902 /so LANTesti /t warning /d "osoit-
teen vapauttaminen valmis"
```

```
rem OSOITTEEN UUSIMINEN ON VAIN SILTÄ VARALTA ETTÄ HAVAITTU YHTEYS-
KATKOS ON HETKELLINEN.
rem JOS KATKOS ON PIDEMPI, OSOITTEEN UUSIMINEN KESKEYTYY AIKAKAT-
KAISUUN
rem EI KUITENKAAN ONGELMA KUN ADAPTERIN IP-OSOITE ON VAPAUTETTU
rem KUN WIMAX YHTEYS AIKANAAN HERÄÄ HENKIIN, COLUMBITECH CLIENT UU-
DISTAA
rem OSOITTEEN AUTOMAATTISESTI JA VAIHTAA ENSISIJAISEN
rem YHTEYDEN KÄYTTÖÖN ITSENÄISESTI

echo uusitaan osoite
eventcreate /l application /id 903 /so LANTesti /t warning /d "aloi-
tetaan osoitteen uusiminen"
rem UUSII VAIN WIMAX YHTEYDEN KÄYTTÄMÄN ADAPTERIN OSOITTEEN
ipconfig /renew "Local Area Connection"
eventcreate /l application /id 904 /so LANTesti /t warning /d "osoit-
teen uusiminen valmis"
:loppu

rem PIDETÄÄN 1 SEKUNNIN TAUKO ENNEN UUTTA AJOA
rem TAUKO ON SUPISTETTU YHTEEN SEKUNTIIN REAGOINTINOPEUDEN
rem LISÄÄMISEKSI MAHDOLLISEN KATKOKSEN TAPAHTUESSA

sleep 1

rem ALOITETAAN KIERROS UUDESTAAN
goto begin
:end
```

6 ASENNUKSET JA YHTEYSTESTIT LABORATORIO-OLOSUHTEISSA

6.1 Testiympäristön toiminnallisuuden testaus

Testiympäristön toiminnallisuuden testauksen tarkoituksena on varmentaa, että käytössä olevat laitteet toimivat ongelmitta ja että testipäätteellä yhteyden muodostus testissä käytettäviin verkkoihin onnistuu. Testiympäristönä toimii Kotkan Mussalon satama-alue. Testiä varten ei tarvinnut erikseen asentaa tukiasemia WLAN-, 3G- ja WiMAX-yhteyksiä varten, vaan käytettiin satama-alueelle aiemmin asennettuja, kuuluvuusalueella olevia tukiasemia.

WLAN- ja 3G-yhteyksiä varten käytettiin päätelaitteen PCMCIA-liitäntään kytkettyä Option Globetrotter Fusion + HSDPA PCMCIA -korttia, jolle oli konfiguroitu yhteydenmuodostuksessa käytettävät asetukset.

WiMAX-yhteyden muodostuksessa käytettiin IEEE 802.16-2004 -standardin mukaisia Alvarionin BreezeMAX PRO -laitteita. Päätelaitteeseen liitettävä laitekonfiguraatio koostuu sisäyksiköstä (IDU), joka on liitetty verkkokaapelilla (Ethernet 10/100 BaseT) päätelaitteeseen. Sisäyksikkö on liitetty vastaavanlaisella verkkokaapelilla ulkoyksikköön (ODU). Ulkoyksikköön on liitetty WiMAX-antenni, jolla muodostetaan yhteys WiMAX-tukiasemaan.

6.2 Yhteystestit

Yhteystestit suoritettiin ensin muodostamalla yhteydet suoraan käytettävissä oleviin langattomiin verkkoihin (3G, WLAN, WiMAX) yhteyksien toimivuuksien varmistamiseksi. Kun yhteyksien moitteettomasta itsenäisestä toimivuudesta voitiin varmistua, siirryttiin testaamaan yhteyden muodostumista Columbitech Server- ja Client-ohjelmistojen avulla VPN-tunnelin ylitse.

Testipaikkana toimi Steveco Oy:n Mussalon satama-alueella sijaitsevat toimitilat. Testien tavoitteena oli saavuttaa häiriöttömästi tapahtuva käytettävän tietoliikenneverkon vaihtuminen (roaming-toiminto), joka olisi sekä käyttäjille että sovelluksille huomaamaton.

Yhteyskatkoksia simuloitaessa WiMAX-yhteys oli määritetty ensisijaiseksi yhteydeksi ja 3G- sekä WLAN-yhteyttä vaihdeltiin toissijaisina vuoroittain. Toimistossa suoritetuissa testeissä 3G-yhteyden käynnistymistä ei ole automatisoitu. Yhteyskatkoksia simuloitiin WiMAX-yhteyden katkeamisen osalta irrottamalla päätelaitteeseen liitetty verkkokaapeli sekä irrottamalla WiMAX-vastaanottimen ulkoyksikköön liitetty antenni.

6.2.1 Yhteyden muodostus käytettävissä oleviin verkkoihin

Ensimmäisessä Columbitech Wireless VPN Clientiä hyödyntävässä yhteystestissä testattiin, että VPN-tunneli saatiin muodostettua kaikkia käytettävissä olevia yhteystyyppejä hyödyntämällä. Testaus suoritettiin asettamalla kukin käytettävissä oleva yhteys-

tyyppi vuorollaan ensisijaiseksi yhteydeksi ja sitten muodostamalla yhteys Columbitech Wireless VPN Clientin kautta. Yhteyden muodostuksen tarkkailuun käytettiin Columbitech Wireless VPN Monitor -ohjelmaa.

6.2.2 Yhteyden roaming-toiminnon testi irrottamalla Ethernet-verkkokaapeli

Yhteyden katkeamista simuloivassa testissä WiMAX-yhteys katkaistiin irrottamalla verkkokaapeli päätelaitteen verkkoliitännästä. Toissijaiseksi yhteydeksi on asetettu 3G-yhteys.

Kun WiMAX-yhteyden käyttämä verkkokaapeli on irrotettu, havaitsee käyttöjärjestelmä tapahtuman välittömästi. Columbitech Wireless VPN Client havaitsee muuttuneen tilanteen erittäin nopeasti ja päivittää verkkoliitännän tilatiedon sekä aloittaa yhteyden muodostuksen toissijaiseksi määritettyyn verkkoon. Vielä tässä testissä 3G-yhteyttä ei ollut määritetty käynnistymään automaattisesti, joten yhteyden muodostuksen alettua täytyi yhteydenmuodostumista edeltävät ilmoitukset käytettävistä kirjautumistunnuksista vahvistaa.

Kytkettäessä verkkokaapeli takaisin päätteen verkkoliitäntään, tapahtui yhteyden palautuminen käyttämään ensisijaista verkkoa lähes välittömästi. Tässä testissä 3G-yhteys oli määritetty katkaistavaksi välittömästi sen jälkeen, kun palautuminen takaisin ensisijaiseen verkkoon oli suoritettu.

Yhteyden siirtyminen ensisijaisen ja toissijaisen verkon välillä tapahtuu sujuvasti niin katkoksen alkaessa kuin myös liikenteen palautuessa takaisin ensisijaiseen verkkoon.

Testaamisen aikana havaittiin, että jos käytettävien yhteyksien prioriteettimäärityksissä oli käytettävien yhteyksien väliin määritetty yhteyksiä, joilla ei ollut liitettävyyttä testissä käytettävään verkkoon, ei siirtymä käytettävien verkkojen välillä onnistunut. Tällöin yhteyden siirtymä jäi polkemaan paikalleen, eikä Columbitech Wireless VPN Client saanut muodostettua VPN yhteyttä Columbitech palvelimeen.

Columbitech Wireless VPN Client on tarkka siihen määritettävien asetusten osalta. Jos määritykset eivät ole täsmälleen oikein, ei Columbitech Wireless VPN toimi oikein. On siis erittäin tärkeää varmistua, että käytettävät määritykset ovat oikeat. Suori-

tettaessa vastaava testi käyttäen WLAN-yhteyttä toissijaisena yhteytenä tapahtui siirtymä yhteyksien välillä saumattomasti.

6.2.3 Yhteyden roaming-toiminnon testi irrottamalla WiMAX-antenni

Yhteyden katkeamista simuloivassa testissä WiMAX-yhteys katkaistiin irrottamalla WiMAX-vastaanottimen ulkoyksikköön liitetty antenni. Toissijaiseksi yhteydeksi oli asetettu 3G-yhteys. Sitä ei ollut määritetty käynnistymään automaattisesti. Aiemmin kuvattu VPN-tunnelin tilaa tarkkaileva scripti ei ollut käytössä.

Antennin irrotuksen jälkeen Columbitech Wireless VPN Client ei heti havaitse yhteyden ensisijaiseen verkkoon katkenneen, vaan kuvittelee yhteyden edelleen olevan aktiivinen, koska päätteen verkkoliitännän tilassa ei tapahtunut muutosta. Yhteyden tilan muutoksen havaitsemiseen kuluu useita minuutteja, ja kun niin viimein tapahtuu, sen sijaan että Columbitech Wireless VPN Client lähtisi etsimään seuraavaa käytettävissä olevaa verkkoa, se yrittää palauttaa ensisijaisen yhteyden käyttöön. Ensisijaisen yhteyden käyttämän verkkoliittymän IP-osoitteen vapauttaminen ja siirtymä toissijaiseen verkkoon vei useita minuutteja. Tätä testattiin useita kertoja, ja jokaisella testauskerralla siirtymään kului kohtuuttoman pitkä aika.

Yhteyden palautuminen käyttämään ensisijaista verkkoa antennin kiinnittämisen jälkeen tapahtuu vaihtelevalla nopeudella. Päätteen verkkoadapterin saatua IP-osoitteen Columbitech Wireless VPN Client vaihtaa ensisijaisen yhteyden käyttöön. Yhteyden vaihto tapahtuu saumattomasti eikä häiritse päätteellä työskentelevän käyttäjän työskentelyä.

Columbitech Wireless VPN Client tarkkailee yhteyksissä käytettävien verkkoliittymien tilaa, ei niinkään liittymien ylitse muodostettavan VPN-tunnelin tilaa. Jos verkkoyhteyden liitettävyydessä ilmenee ongelmia, toisin sanoen yhteys katkeaa, pystyy Columbitech reagoimaan tilanteeseen erittäin nopeasti ja vaihtamaan yhteyden seuraavaan käytettävissä olevaan varayhteyteen. Jos yhteyskatkos, kuten WiMAX-yhteyden tapauksessa pyrittiin simuloimaan, tapahtuu siten, että verkkoyhteys katkeaa esimerkiksi tukiaseman pimenemisen seurauksena, ei Columbitech Wireless VPN Client välittömästi havaitse yhteyden menetystä. Tämä johtuu siitä, että päätteen verkkoliitännän ja WiMAX-vastaanottimen sisäyksikön välinen yhteys on edelleen aktiivinen. Vaikka ulkoyksikkö rekisteröikin yhteyden katkenneen, ei tieto kuitenkaan välity

WiMAX-vastaanottimelta päätelaitteelle asti, jolloin yhteyden vaihtoon tulee huomattavia viiveitä.

7 ASENNUKSET JA YHTEYSTESTIT KENTTÄOLOSUHTEISSA

7.1 Testiympäristön toiminnallisuuden testaus

Testiympäristön toiminnallisuuden testauksessa varmennettiin, että käytössä olevat laitteet toimivat ongelmitta ja että testipäätteellä yhteyden muodostus testissä käytettäviin verkkoihin onnistuu. Testiympäristönä toimi Kotkan Mussalon satama-alue. Testissä käytettävä laitteisto asennettiin henkilöautoon, jolla ajettiin ympäri satama-aluetta. Testiä varten ei tarvinnut erikseen asentaa tukiasemia WLAN-, 3G- ja WiMAX-yhteyksiä varten, vaan satama-alueelle asennettuja, kuuluvuusalueella olevia tukiasemia käytettiin.

Päätteelle oli testejä varten asennettu konttiterminaalityöskentelyssä käytettävät operatiiviset sovellukset, jotta simuloitujen katkosten vaikutusta niiden toiminnallisuuteen voitiin seurata. Kun laitteisto oli koottu käyttökuntoon, suoritettiin ensin yhteydenmuodostustestit käytettävissä oleviin verkkoihin ajoneuvon ollessa paikallaan.

WLAN- ja 3G-yhteyksiä varten käytettiin päätelaitteen PCMCIA-liitäntään liitettyä Option Globetrotter Fusion + HSDPA PCMCIA -korttia, jolle oli konfiguroitu yhteyden muodostuksessa käytettävät asetukset. 3G-verkon yhteys oli konfiguroitu muodostumaan automaattisesti päätteelle kirjautumisen yhteydessä, jotta tästä ei koidu ylimääräistä viivettä testattaessa yhteyden siirtymää verkkojen välillä.

WiMAX-yhteyden muodostuksessa käytettiin IEEE 802.16-2004 -standardin mukaisia Alvarionin BreezeMAX PRO -laitteita. Päätelaitteeseen liitettävä laitekokonaisuus koostuu sisäyksiköstä (IDU), joka on liitetty verkkokaapelilla (Ethernet 10/100 BaseT) päätelaitteeseen. Sisäyksikkö on liitetty vastaavanlaisella verkkokaapelilla ulkoyksikköön (ODU). Ulkoyksikköön on liitetty WiMAX-antenni, jolla muodostetaan yhteys WiMAX-tukiasemaan. Yhteyden muodostuksen tarkkailuun käytettiin Columbitech Wireless VPN Monitor- ohjelmaa.

7.2 Yhteystestit

Yhteystestit suoritettiin ensin muodostamalla yhteydet suoraan käytettävissä oleviin langattomiin verkkoihin (3G, WLAN, WiMAX) yhteyksien toimivuuksien varmistamiseksi. Kun yhteyksien moitteeton itsenäinen toimivuus oli varmistettu, siirryttiin testaamaan yhteyden muodostumista Columbitech Server- ja Client- ohjelmistojen avulla muodostetun VPN-tunnelin läpi.

Testipaikkana toimi Steveco Oy:n Mussalon satama-alue. Testien tavoitteena oli saavuttaa Columbitech Wireless VPN -tekniikalla mahdollisimman saumaton roaming-toiminto tietoliikenneverkkojen välillä häiriötilanteissa.

Yhteyskatkoksia simuloitaessa WiMAX-yhteys oli määritetty ensisijaiseksi yhteydeksi ja 3G- sekä WLAN-yhteyttä vaihdeltiin toissijaisina vuoroittain. Todellisia käyttötilanteita vastaavien olosuhteiden saavuttamiseksi kaikki muodostettavat fyysiset verkkoyhteydet oli konfiguroitu käynnistymään automaattisesti päätteelle kirjautumisen yhteydessä. Columbitech Wireless VPN Client oli konfiguroitu käynnistymään automaattisesti päätteen käynnistymisen yhteydessä AutoWVPN-palvelun käynnistämänä. Taustalla ajettiin VPN-tunnelin tilaa tarkkailevaa bat-scriptiä. Yhteyskatkoksia simuloitiin WiMAX-yhteyden katkeamisen osalta irrottamalla päätelaitteeseen liitetty verkkokaapeli sekä irrottamalla WiMAX-vastaanottimen ulkoyksikköön liitetty antenni.

7.2.1 Yhteyden muodostus käytettävissä oleviin verkkoihin

Ennen testiajelua Mussalon satama-alueella varmistuttiin, että Columbitech Wireless VPN Clientin kautta saatiin VPN-tunneli muodostettua kaikkia käytettävissä olevia yhteystyyppejä hyödyntämällä. Testaus suoritettiin asettamalla kukin käytettävissä oleva yhteystyyppi vuorollaan ensisijaiseksi yhteydeksi ja sitten muodostamalla yhteys Columbitech Wireless VPN Clientin kautta. Yhteyden muodostuksen tarkkailuun käytettiin Columbitech Wireless VPN Monitor -ohjelmaa.

7.2.2 Yhteyden roaming-toiminnon testaaminen irrottamalla verkkokaapeli

Testi toteutettiin ajamalla henkilöautolla Mussalon satama-alueella langattomien verkkojen kuuluvuusalueella. Samalla operatiivisessa työssä käytettäviä sovelluksia suoritettiin päätteellä. Vertailukohdan saamiseksi ensin testattiin yhteyden roaming-toimintoa irrottamalla Alvarion sisäyksikön ja päätteen välinen verkkokaapeli. Yhteyden roaming-toiminto varayhteyteen tapahtui sekunneissa. Päätteelle avatuilla operatiivisilla sovelluksilla pystyi jatkamaan työskentelyä roaming-toiminnon jälkeen yhteyden palauduttua. Roaming-toiminnon aikana operatiivisia sovelluksia ei kuitenkaan pystynyt käyttämään. Liitettäessä verkkokaapeli takaisin havaitsi Columbitech Wireless VPN Monitor tapahtuman välittömästi ja vaihtoi käytettäväksi ensisijaisen verkon.

7.2.3 Yhteyden roaming-toiminnon testaus irrottamalla antenni

Simuloitaessa WiMAX-yhteyden katkosta irrottamalla antenni ulkoyksiköstä scripti havaitsi muutoksen VPN-putken tilassa ja vapautti sen käyttämän IP-osoitteen verrattain nopeasti pienentäen roaming-toimintoon kuluvaa aikaa minuuteista sekunteihin. Kuten testattaessa verkkokaapelin irrottamista, myös tässä testissä roaming-toiminto tapahtui operatiivisten sovellusten käytön kannalta riittävän nopeasti. Ennen katkosta aloitettua istuntoa pystyi jatkamaan yhteyden palauduttua. Kun antenni liitettiin takaisin ulkoyksikköön, kesti Columbitech Wireless VPN Monitorilta useita minuutteja, ennen kuin se havaitsi WiMAX-yhteyden olevan käytettävissä ja siirtyi taas käyttämään ensisijaista yhteyttä. Palautuminen tapahtui kuitenkin saumattomasti eikä häirinnyt päätetyöskentelyä.

7.2.4 Yhteyden roaming-toiminnon vasteajat

Seuraavassa esitetyt laskennalliset arvot pohjautuvat scriptin yksittäisten vaiheiden suoritetukseen kuluviin aikoihin ja niistä koostettuihin kokonaisaikoihin.

Kenttätesteissä käytettyjen yhteyksien ollessa jo valmiiksi aktiivisena ei yhteydenmuodostuksesta johtuva lisäaika pääse vaikuttamaan yhteyden vaihdoksen kestoon. Verkkokaapelia irrotettaessa Columbitech Wireless VPN Client pääsi suorittamaan siirtymisen varayhteyteen välittömästi. Vaikka scripti saattaakin havaita hetkellisen katkoksen ja reagoida siihen, sen toiminta ei kuitenkaan vaikuta Columbitech Wire-

less VPN Clientin toimivuuteen. Scripti vain yrittää vapauttaa WiMAX-yhteyden käytössä olevan liittymän IP-osoitteen, kun Columbitech Wireless VPN Client on jo ohjannut liikenteen kulkemaan toissijaista yhteyttä käyttäen. Sen toimintaan taas scriptillä ei voida vaikuttaa.

Vertailuaika irrottamalla verkkokaapeli:

Vertailun vuoksi mainittakoon, että verkkokaapelia irrottamalla ja takaisin kiinnittämällä yhteyksien vaihto molemmin päin tapahtuu varsin välittömästi eli arviolta noin yhdessä sekunnissa.

Vertailuajat irrottamalla antenni:

Scriptin suoritukseen kuluva aika vaikuttaa osaltaan kokonaisaikaan, joka yhteyden vaihtamiseen menee. Suoritukseen kuluva aika on suoraan riippuvainen errorlevel-tarkistuksen tuottamasta tuloksesta ping-komentoa suoritettaessa. Tilanteissa, joissa kaikki ping-komennon suorituksen tulokset ovat onnistuneita, palauttaa errorlevel tulokseksi lukuarvon 0, ja tilanteissa, joissa kaikki suoritukset palauttavat request timed out-tuloksen, palauttaa errorlevel tulokseksi 1. Poikkeuksena ovat tilanteet, joissa ping-komennon suorituksen tuloksena on sekä onnistuneita että *request timed out* -ilmoituksen palauttavia tuloksia. Silloin errorlevel voi palauttaa kumman tahansa mahdollisista vastineista, joko 0:n tai 1:n.

Jos scripti palauttaa 0:n, on tuloksena ”yhteys on aktiivinen”. Komentojono odottaa asetetun suoritusvälin mukaisen aikavälin, ennen kuin se suorittaa itsensä uudelleen. IP-osoitteen vapauttamiseen kuluva aika näyttäisi vaihtelevan 1-3 sekunnin välillä. Jos scripti palauttaa tulokseksi 1, siirtyy scripti välittömästi vapauttamaan WiMAX-yhteyden käytössä olevan IP-osoitteen.

Pingin palautumisaika on noin 120 ms. Jos ping puolestaan ei mene läpi, on oletusviive 4000 ms (4s), jonka jälkeen pingin suoritusta yritetään uudelleen. Jos siis komennolla ***ping ip-osoite*** lähtee oletusarvon mukaisesti 4 ping-testiä ja jokainen palauttaa vasteeksi *request timed out*, tarkoittaa se 18 sekunnin aikajaksoa, joka ping-komentojen suorittamiseen kuluu. Vasta tämän jälkeen scripti siirtyy vapauttamaan käytössä olevan IP-osoitteen.

Taulukossa 2 lihavoinnilla ja kursivoinnilla korostetuissa riveissä errorlevel-tulos voi olla vain 1. Tuloksen ollessa 0 odottaa scripti suoritusväliin määritetyn aikajakson, ennen kuin suorittaa ping-testin uudelleen.

Taulukko 2. Vasteajat, kun errorlevel = 0 ensimmäisen ping-kierroksen jälkeen.

Scriptin suoritusväli s.	pingit/kpl	ping 1. kierros onnist./ epäonnist.	pingien suoritukseen kuluva aika s.	errorlevel 1. kierroksen jälkeen	ping 2. kierros onnist./ epäonnist.	pingien suoritukseen kuluva aika s.	ipconfig /release aika s.	Columbitech reagointi ipconfigin jälkeen	kokonais-aika s. (+scriptin suoritusväli)
10	***4***	***0/4***	***16***	***1***	-	-	***1-3***	***1***	***18-20 (+10)***
10	4	1/3	12	0	0/4	16	1-3	1	40-42
10	4	2/2	8	0	0/4	16	1-3	1	36-38
10	4	3/1	4	0	0/4	16	1-3	1	32-34
10	4	4/0	<1	0	0/4	16	1-3	1	18-20 (+10)
5	***4***	***0/4***	***16***	***1***	-	-	***1-3***	***1***	***18-20 (+5)***
5	4	1/3	12	0	0/4	16	1-3	1	35-37
5	4	2/2	8	0	0/4	16	1-3	1	30-32
5	4	3/1	4	0	0/4	16	1-3	1	27-29
5	4	4/0	<1	0	0/4	16	1-3	1	18-20 (+5)
1	***2***	***0/2***	***8***	***1***	-	-	***1-3***	***1***	***10-12 (+1)***
1	2	1/1	4	0	0/2	8	1-3	1	14-16
1	2	2/0	<1	0	0/2	8	1-3	1	10-12 (+1)

Taulukossa 3 lihavoinnilla ja kursivoinnilla korostetuissa riveissä errorlevel-tulos voi olla vain 0. Tuloksen ollessa 1 siirtyy scripti välittömästi suorittamaan WiMAX-liittymän IP-osoitteen vapauttamisen.

Taulukko 3. Vasteajat, kun errorlevel = 1 ensimmäisen ping-kierroksen jälkeen.

Scriptin suoritusväli s.	pingit/kpl	ping 1. kierros onnist./ epäonnist.	pingien suoritukseen kuluva aika s.	errorlevel 1. kierroksen jälkeen	ipconfig /release aika s.	Columbitech reagointi ipconfigin jälkeen	kokonais-aika s. (+scriptin suoritusväli)
10	4	0/4	16	1	1-3	1	18-20 (+10)
10	4	1/3	12	1	1-3	1	40-42
10	4	2/2	8	1	1-3	1	36-38
10	4	3/1	4	1	1-3	1	32-34
10	***4***	***4/0***	***<1***	***0***	-	-	-
5	4	0/4	16	1	1-3	1	18-20 (+5)
5	4	1/3	12	1	1-3	1	35-37
5	4	2/2	8	1	1-3	1	30-32
5	4	3/1	4	1	1-3	1	27-29
5	***4***	***4/0***	***<1***	***0***	-	-	-
1	2	0/2	8	1	1-3	1	10-12 (+1)
1	2	1/1	4	1	1-3	1	14-16
1	***2***	***2/0***	***<1***	***0***	-	-	-

Kahdessa edellisessä taulukossa scriptin suoritusvälien arvoina on käytetty samoja arvoja kuin kenttätestauksessa.

Taulukkoja 2 ja 3 tarkastellessa havaitaan, että yhteyden vaihtoon kuluva aika voi vaihdella huomattavasti suhteessa siihen, millä aikajaksolla yhteyskatkos ensisijaiseen yhteyteen ja scriptin suoritus tapahtuvat toisiinsa nähden. Taulukossa 4 on havainnollistettu kuinka taulukoita 2 ja 3 tulisi lukea. Taulukkoon 5 on kirjattu scriptiä suoritettaessa saavutettu yhteyden vaihtoon kuluva aikaväli eri lähtöarvoilla.

Taulukko 4. Esimerkki taulukon 2 lukemisesta, toisen rivin tapahtumat.

Scriptin suoritusväli s.	pingit/kpl	ping 1. kierros onnist./ epäonnist.	pingien suoritukseen kuluva aika s.	errorlevel 1. kierroksen jälkeen	ping 2. kierros onnist./ epäonnist.	pingien suoritukseen kuluva aika s.	ipconfig /release aika s.	Columbitech reagointi ipconfigin jälkeen	kokonais-aika s. (+scriptin suoritusväli)
10	***4***	***0/4***	***16***	***1***	-	-	***1-3***	***1***	***18-20 (+10)***
10	4	1/3	12	0	0/4	16	1-3	1	40-42
12 s. kuluu kolmen epäonnistuneen pingin suoritukseen, tuloksena errorlevel 0 + 10 s. viive ennen scriptin uudelleen suoritusta + 16 s. kuluu neljän epäonnistuneen pingin suoritukseen, tuloksena errorlevel 1 + 1-3 s. ipconfig /release komennon suoritukseen + 1 s. Columbitech WVPN Clientin käyttämä aika yhteyden vaihtoon = 40 – 42 s. kokonaissuoritusaika. Kokonaisajan jälkeen suluissa () olevaan arvoon on huomioitu se mahdollisuus, että katkos on saattanut alkaa scriptin suorituskertojen välillä tilanteessa, jossa yhteenkään ping kyselyyn ei saada vastausta. Tämä lisää laskennallisen mahdollisuuden sille että katkos on voinut alkaa millä tahansa hetkellä scriptin suorituskertojen välillä. Taulukkoa 2 luetaan samalla periaatteella.									

Taulukko 5. Yhteyden vaihtoon kuluva aika.

Scriptin suoritusväli s.	pingit/kpl	ping 1. kierros onnist./ epäonnist.	kokonaisaika vaihteluväli s. (max. scriptin suoritusaika huomioiden mahdollisuus että kaikki suorituksen **ping** pyynnöt palauttavat ***request timed out*** ilmoituksen)
10	4	0	32-42
10	4	1	6-20 (max. 30)
10	***4***	***0 ja 1***	***6-42***
5	4	0	27-37
5	4	1	6-20 (max. 25)
5	***4***	***0 ja 1***	***6-37***
1	2	0	14-16
1	2	1	6-12 (max. 13)
1	***2***	***0 ja 1***	***6-16***

Kun testaus aloitettiin, suoritusvälin arvo oli 10 sekuntia ja suoritettujen ping-komentojen lukumäärä on 4 kappaletta. Näillä (lähtö)arvoilla suoritetuissa testeissä viiveet olivat käytännössä niin pitkiä, että päätteellä ajettavien operatiivisten sovellusten käyttö täytyi aloittaa uudelleen, koska istunnot katkesivat käytettävän yhteyden vaihtamistoimen aikana. Alkuperäinen laskennallinen vaihteluväli 6–42 sekuntia oli liian laaja ja erittäin suurella todennäköisyydellä istunto on katkoksen jälkeen uusittava.

Muutettaessa suoritusvälin alkuarvoa 5 sekuntiin tilanne ei paljon parantunut, vaikka laskennallisesti vaihteluväli onkin vähän parempi, 6–37 sekuntia. Istunnon uusimisen todennäköisyys katkoksen jälkeen on edelleen erittäin suuri.

Testaamisen aikana päädyttiin lopulta käyttämään scriptin suoritusvälinä yhtä sekuntia ja ajettavien pingien lukumääränä kahta kappaletta. Silloin laskennallinen kokonaissuoritusaika saatiin puristettua riittävän alhaiseksi (6–16 sekuntia), jotta operatiivisten sovellusten käyttöä voi jatkaa normaalisti katkoksen jälkeen.

Kun scripti asetettiin suoriutumaan toistuvasti ilman suoritusväli arvoa, Columbitech WVPN Client ei pystynyt suoriutumaan yhteyden palautumistoimenpiteestä, vaan se jäi Searching-tilaan. Syy tähän on tuntematon.

Kun toissijainen yhteys (3G) on käytössä, onnistuvat scriptin ping-testit VPN-putken ylitse yhdyskäytävään, joten se ei yritä katkoksen jälkeisen osoitteen uusimisyrityksen jälkeen enää palauttaa WiMAX-liittymän IP-osoitetta. Tämä vaihe on kokonaan Windows XP:n ja Columbitech Wireless VPN Clientin varassa.

Yhteyden palautuminen käyttämään ensisijaista yhteyttä sen jälkeen, kun WiMAX-antenni oli kiinnitetty takaisin WiMAX-ulkoyksikköön, tapahtui käytännön testeissä pitkällä viiveellä. Sen jälkeen, kun antenni oli kiinnitetty takaisin ja fyysinen liittymä oli saanut oman IP-osoitteen DHCP-palvelimelta, Columbitech Wireless VPN Clientiltä kesti useita minuutteja, ennen kuin se havaitsi muuttuneen tilanteen ja vaihtoi käyttöön ensisijaisen yhteyden WiMAX-liittymän kautta. Käytännössä tämä ei kuitenkaan ole ongelma, sillä kun siirtymä sitten tapahtuu, se tapahtuu täysin saumattomasti käyttäjän työskentelyä häiritsemättä.

8 TULOSTEN TARKASTELU JA PÄÄTELMÄT

Columbitech Wireless VPN -ohjelmisto saatiin toimimaan onnistuneesti niin toimistossa kuin kentällä suoritetuissa testeissä. Testeissä käytettävät tietoliikenneverkot olivat 3G, WiMAX ja WLAN. Verkkoyhteyden katkeamista simuloitiin WiMAX-yhteyden osalta sekä irrottamalla verkkokaapeli verkkoadapterista että irrottamalla ulkoyksikköön liitetty antenni. WiMAX-yhteys toimi ensisijaisena yhteytenä ja 3G- sekä WLAN-yhteydet toissijaisina.

Columbitech Wireless VPN -ohjelmiston asetuksia määritettäessä on aiheellista tarkastaa tehdyt asetukset mahdollisten virheiden varalta. Columbitech Wireless VPN Server -ohjelmiston osalta on syytä kiinnittää erityistä huomiota Columbitech-palvelimelle myönnettyyn IP-osoitteeseen. Jos käytössä on erillinen DHCP-palvelin,

jonka myöntämiä osoitteita Columbitech-palvelin välittää Columbitech Wireless VPN Clientien virtuaalisille verkkoadaptereille, on palvelimen IP-osoitteen oltava samalla osoitealueella kuin välitettävät osoitteet.

Columbitech Wireless VPN Clientin osalta on tarkistettava erityisesti käytettävissä olevien tietoliikenneverkkojen käyttöprioriteetit. Jos priorisoitujen tietoliikenneverkkojen joukossa on verkkoja, joiden kautta ei ollut liitettävyyttä Columbitech-ohjelmiston käyttämiin verkkoihin, havaittiin sen aiheuttavan pitkiä viiveitä seuraavaa käytettävää tietoliikenneverkkoa etsittäessä (roaming).

Testeissä, joissa irrotettiin verkkokaapeli päätelaitteen verkkoliitännästä, tapahtui roaming-toiminto täysin ongelmattomasti ensisijaisesta verkosta toissijaiseen. Testeissä, joissa 3G-yhteyden käynnistymistä ei ollut vielä automatisoitu, suurimmat viiveet muodostuivat yhteyden muodostusprosessiin kuluneesta ajasta katkoksen tapahduttua. Yhteyden muodostumisen jälkeen toissijaisen yhteyden käyttöönotto tapahtui välittömästi. Liitettäessä verkkokaapeli takaisin tapahtui palautuminen takaisin ensisijaiseen verkkoon välittömästi.

Suoritettaessa testejä, joissa yhteyden katkeamista simuloitiin irrottamalla WiMAX-antenni liitetystä ulkoyksiköstä, havaittiin seuraavan käytettävän tietoliikenneverkon roaming-toiminnon siirtymässä ongelmia. Katkoksen tapahduttua ei Columbitech Wireless VPN Client heti havainnut katkoksen tapahtuneen. Katkoksen havaitsemiseen kului useita minuutteja, ja kun Columbitech Wireless VPN Client viimein havaitsi muutoksen verkkoyhteyden tilassa, sen sijaan että se olisi siirtynyt etsimään (roaming) seuraavaa käytettävissä olevaa verkkoa, se yritti palauttaa yhteyttä WiMAX-tietoliikenneverkon kautta. Kun Columbitech Wireless VPN Client viimein siirtyi suorittamaan roaming-toimintoa ottaakseen käyttöön seuraavan toissijaiseksi asetetun tietoliikenneverkon, oli tähänkin kulunut useita minuutteja. Roaming-toiminto ja käytettävän tietoliikenneverkon käyttöönotto tapahtuivat kuitenkin erittäin nopeasti. Liitettäessä WiMAX-antenni takaisin ulkoyksikköön kesti kauan ennen kuin Client havaitsi yhteyden jälkeen olevan käytettävissä. Tästä aiheutui pitkiä viiveitä roaming-toimintoon liikenteen siirtymisessä takaisin ensisijaiseen verkkoon. Varsinainen verkkoyhteyden vaihto takaisin ensisijaiseen verkkoon tapahtui saumattomasti. Kuitenkin verkon roaming-toiminnon kokonaisaika venyi useisiin minuutteihin, mikä oli kohtuuttoman pitkä aika.

Roaming-toiminnossa ilmennyt ongelma WiMAX-antennia irrotettaessa johtui siitä, että Columbitech Wireless VPN Client tarkkaili käytettävien verkkoadapterien tilaa, mutta ei seurannut muodostetun VPN-tunnelin tilaa. Tätä ongelmaa paikkaamaan kirjoitettiin bat-scripti, joka tarkkaili tunnelin toimivuutta yhdyskäytävän osoitetta pingaamalla. Kun se havaitsi VPN-tunnelin ylitse muodostetun yhteyden katkenneen, vapautti se WiMAX-yhteyden käyttämän adapterin IP-osoitteen, herättäen Columbitech Wireless VPN Clientin välittömästi etsimään (roaming) seuraavaa käytettävissä olevaa yhteyttä.

3G-yhteyden käynnistyminen automatisoitiin tapahtuvaksi päätteelle kirjautumisen yhteydessä. Näin saatiin edellä mainitut yhteyden käynnistymisestä johtuvat viiveet poistettua varsinaisen roaming-toiminnon tapahtuessa. Columbitech Wireless VPN Clientin käynnistys automatisoitiin tapahtumaan päätteen käynnistymisen yhteydessä asentamalla AutoWVPN-palvelu.

Kentällä suoritetuissa testeissä päätelaitteella ajettiin VPN-tunnelin ylitse operatiivisessa työskentelyssä käytettäviä sovelluksia, jotta voitiin nähdä, miten simuloidut katkokset vaikuttavat niiden toimintaan. Aluksi scriptin lähtöarvoiksi asetettiin suoritusväliksi 10 sekuntia ja pingien lukumääräksi 4 kappaletta. Roaming-toiminnon kestäessä pitempään olivat operatiivisten ohjelmien istunnot katkenneet ja niiden käyttö oli aloitettava uudelleen käynnistämällä uusi istunto. Roaming-toiminnon aikana tunnelin ylitse ajettavat sovellukset eivät olleet käytössä. Laskennalliseksi kokonaisajaksi muodostui 6–42 sekuntia riippuen ajanhetkestä, jolla scripti havaitsi katkoksen suhteessa katkoksen tapahtumahetkeen. Nämä lähtöarvot osoittautuivat kuitenkin liian suuriksi. Lopulta scriptin suoritusväliksi asetettiin 1 sekunti ja pingien lukumääräksi 2 kappaletta. Tällöin katkoksia simuloitaessa saatiin operatiivisten sovellusten istunnot pysymään ylhäällä verkon vaihtumisen jälkeenkin. Laskennalliseksi kokonaisajaksi roaming-tapahtumalle saatiin 6–16 sekuntia.

Kun scripti asetettiin suorittamaan toistuvasti ilman suoritusväliarvoa, ei Columbitech WVPN Client pystynyt suoriutumaan yhteyden palautumistoimenpiteestä, vaan se jäi Searching -tilaan. Syy tähän ei selvinnyt.

Ensisijaisen yhteyden ottaminen takaisin käyttöön tapahtui kuitenkin pitkällä viiveellä. Kun antenni oli kiinnitetty takaisin ja fyysinen liittymä oli saanut IP-osoitteen, Columbitech WVPN Clientiltä kesti useita minuutteja, ennen kuin se havaitsi muuttu-

neen tilanteen ja otti käyttöön ensisijaisen yhteyden. Siirtymä verkkojen välillä tapahtui kuitenkin saumattomasti.

Kun Columbitech Wireless VPN -ohjelmiston testaamisen aikana ilmenneet ongelmat onnistuttiin ratkaisemaan, saatiin sen toiminnallisuus sellaiselle tasolle, että katkoksen tapahtuessa käytettävän verkkoliikenneyhteyden roaming-toiminto ei aiheuttanut operatiivisen käytön kannalta kestämättömiä katkoksia. Liitettäessä WiMAX-antenni takaisin ulkoyksikköön, ei pitkä viive suoritettaessa roaming-toimintoa toissijaisesta verkosta takaisin ensisijaiseen verkkoon aiheuta ongelmia, sillä kun siirtymä sitten tapahtuu, se on täysin saumaton.

Tämän opinnäytetyön tuloksia saatetaan tulevaisuudessa käyttää Kotkan Hietasen satamanosan ja Haminan konttiterminaalin langattomien verkkojen kehittämisessä, mikäli Columbitech Wireless VPN -ohjelmisto otetaan Stevecolla tuotantokäyttöön.

LÄHTEET

1. ITU-D Study Group 2. "Guidelines on the smooth transition of existing mobile networks to IMT-2000 for developing countries (GST); Report on Question 18/2".

2. About mobile technology and IMT-2000. Introduction - Evolution of the Mobile Market. ITU – International Telecommunications Union. Saatavissa: http://www.itu.int/osg/spu/imt-2000/technology.html [Viitattu 16.4.2011].

3. Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. Porvoo: Docendo Finland Oy

4. What is the actual throughput (data transfer rate) of WiMAX Technology?.Saatavissa: http://www.wimax.com/wimax-technologies-standards/what-is-the-actual-throughput-data-transfer-rate-of-wimax-technology [viitattu 17.5.2011].

5. Vartiainen, J. 2009. Langattoman tietoliikenneverkon toteuttaminen satama-alueelle. Diplomityö. Lappeenranta: Lappeenrannan Teknillinen Yliopisto.

6. IEEE 802.16 Broadband Wireless Access Working Group.OFDM – sub-channelization improvement and system performance – selected topics.

7. Tutorial on Multi Access OFDM (OFDMA) Technology. Saatavissa: http://www.ieee802.org/22/Meeting_documents/2005_Jan/22-05-0005-00-0000_OFDMA_Tutorial_IEEE802-22_Jan%2005.ppt [viitattu 17.5.2011].

8. IEEE Std 802.11-2007 IEEE Standard for Information Technology – Telecommunications and information exchange between systems – LANs and MANs – Specific requirements – “Part 11: WLAN MAC and PHY Specification”, 17. Orthogonal frequency division multiplexing (OFDM) PHY specification for the 5GHz band.

9. IEEE Std 802.11-2007 IEEE Standard for Information Technology – Telecommunications and information exchange between systems – LANs and MANs – Specific requirements – “Part 11: WLAN MAC and PHY Specification”, 5. General Description.

10. IEEE Std 802.11n-2009 IEEE Standard for Information Technology – Telecommunications and information exchange between systems – LANs and MANs – Specific requirements – Amendment 5: Enhacements for Higher Throughput – "Part 11: WLAN MAC and PHY Specification", 20.3.9.1 Introduction.

11. LXE VX3-12 -spesifikaatio esite.

12. Option GlobeTrotter Fusion + HSDPA -pakkauksen seloste.

13. Columbitech Wireless VPN – Site Preparation Guide.

14. Cisco ASA 5500 Series Configuration Guide using ASDM.

15. Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 3.0.