Harri Koskinen

Tilastokeskuksen tietoliikenneverkon kehittäminen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

25.11.2013

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Harri Koskinen Tilastokeskuksen tietoliikenneverkon kehittäminen 26 sivua + 1 liite 25.11.2013
Tutkinto	insinööri (AMK)
Koulutusohjelma	tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	tietoverkot
Ohjaaja(t)	IT-kehittämispäällikkö Tenho Vastaranta lehtori Marko Uusitalo

Opinnäytetyön tarkoituksena oli parantaa Tilastokeskuksen tietoliikenneverkon teknistä luotettavuutta ja tietoturvaa. Tavoitteena oli samalla myös saattaa tietoliikenneverkon tekninen dokumentaatio vastaamaan nykytilaa.

Tietoliikenneverkon luotettavuutta parannettiin ottamalla Spanning Tree -protokolla käyttöön viraston kerrosverkoissa. Tarkoituksena oli estää esimerkiksi verkkojohtojen kytkentävirheistä johtuvat verkkomyrskyt.

Verkon tietoturvan parantamiseksi tehtiin suunnitelma porttikohtaisen todentamisen (IEEE 802.1X) käyttöönottamiseksi verkkokytkimissä. Todentamiseen käytettiin käyttäjien Active Directory –tunnuksia sekä päätelaitteiden MAC-osoitteita. Tällä hankaloitetaan merkittävästi tuntemattomien laitteiden liittämistä verkkoon.

Lisäksi suunniteltiin vanhan, vain vierailijoiden käyttöön tarkoitetun langattoman verkon tilalle ratkaisu, joka mahdollistaa verkon turvallisen käyttämisen myös viraston omille työntekijöille.

Tietoliikenneverkon dokumentointia parannettiin päivittämällä vanhentuneita verkkokuvia sekä laatimalla suunnitelma, jonka avulla dokumentit saadaan versionhallinnan piiriin.

Avainsanat	langattomat lähiverkot, reitittimet, tietoliikenne, tietoturva

Author(s) Title Number of Pages Date	Harri Koskinen Improving Statistics Finland's data network 26 pages + 1 appendix 25 November 2013
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications and Data Networks
Instructor(s)	Tenho Vastaranta, IT Development Manager Marko Uusitalo, Senior Lecturer

The main goal of this thesis was to improve Statistics Finland's data network's fault tolerance, security and documentation.

The network's fault tolerance was improved by enabling Spanning Tree Protocol (STP) on the switches, which handle the traffic for all the workstations. STP protects the network from bridge loops and broadcast storms.

To improve the security of the network, a plan was developed for using port based authentication (IEEE 802.1X) on the network switches. This makes it more difficult to attach unknown devices to the network. MAC addresses from client devices (laptops and workstations) and Active Directory credentials were used for authentication.

Also, a plan was developed to replace the current wireless network solution. The proposed solution would make it possible for Statistics Finland's employees to use the wireless network in a secure way. The previous implementation was only for a limited visitor use.

The documentation of the data network was improved by updating the old network diagrams. A plan to add version controlling into the documentation process was also made.

Keywords	wireless networks, routers, networking, information security

Sisällys

Liitteet

Liite 1. FreeRADIUS-palvelimen asetustiedostot

Lyhenteet

AAA Protokolla, jonka avulla voidaan tietoverkoissa tunnistaa toinen osapuoli. Lyhenne tulee sanoista authentication, authorization ja accounting.

AES Advanced Encryption Standard on symmetrinen lohkosalausmenetelmä, jota käytetään yleisesti tietoliikenteen ja tiedostojen salaamiseen. AES:ssä käytetty salausalgoritmi on nimeltänsä Rijndael.

DMZ De-Militarized Zone. Termi, jota käytetään yleisesti kuvaamaan tietoliikenneverkon sellaista osaa, jonne voidaan ottaa yhteys Internet-verkosta.

EAPS Ethernet Automatic Protection Switching. Ethernet-verkoissa käytettävä tekniikka vikasietoisen verkkotopologian luomiseen.

IEEE Institute of Electrical and Electronics Engineers on kansainvälinen tekniikan alan järjestö. Sen toiminnan piiriin kuuluu muun muassa monien alan keskeisten standardien määrittely.

MAC Media Access Control. IEEE 802-verkoissa (esimerkiksi Ethernet) käytettävä verkon varaamisen ja liikennöinnin hoitava järjestelmä. Ethernetissä verkkoon kytkeytyvät laitteet tunnistetaan MAC-tason osoitteella, joka on 48-bittinen yksilöllinen osoite jokaiselle verkkolaitteelle.

RADIUS Remote Authentication Dial In User Service. Protokolla, jonka avulla voidaan toteuttaa AAA-protokollan mukainen käyttäjän tai päätelaitteen tunnistaminen.

RFC Request For Comments -dokumentit ovat Internet Engineering Task Force -organisaation julkaisemia Internetiä koskevia standardeja.

STP Spanning tree-protokolla. Määritelty IEEE:n standardeissa 802.1d, 802.1s ja 802.1w, on siltojen ja kytkimien käyttämä toiminto, jonka avulla voidaan estää mahdolliset silmukat verkossa.

WLAN	Wireless Local Area Network. Langaton lähiverkkotekniikka, joka on määritelty IEEE:n standardissa 802.11.
WPA2	Wi-Fi Protected Access II, on IEEE:n standardissa 802.11i määritelty tapa langattoman tietoliikenteen salaamiseen.
VLAN	Virtual LAN on tekniikka, jolla fyysinen lähiverkko voidaan jakaa loogisiin osiin.

1 Johdanto

Tämän opinnäytetyön tarkoituksena on selvittää ja kuvata Tilastokeskuksen tietoliikenneverkon nykytila sekä esittää konkreettisia tapoja parantaa verkon luotettavuutta ja tietoturvaa.

Opinnäytetyön alussa esitellään opinnäytetyön toimeksiantaja Tilastokeskus, jonka jälkeen kerrotaan lyhyesti työn eri vaiheista. Tämän jälkeen esitellään tietoliikenneverkon nykyinen toteutus sekä perehdytään muutamiin tärkeimpiin viraston tietoliikenneverkossa käytettävistä verkkotekniikoista.

Omassa luvussaan käsitellään Tilastokeskuksen tietoliikenneverkossa havaittuja teknisiä heikkouksia, minkä jälkeen esitetään keinoja verkon toiminnan parantamiseksi. Lopuksi käydään läpi, mikä on verkon nykytila opinnäytetyötä lopetettaessa: mitä on saavutettu työn aikana ja mitä voitaisiin vielä tulevaisuudessa tehdä, jotta verkon toiminta saataisiin mahdollisimman luotettavaksi ja turvalliseksi.

2 Tilastokeskus

Vuonna 1865 perustettu Tilastokeskus on tulosjohdettu valtiovarainministeriön alainen virasto. Päätoimipaikka sijaitsee Helsingissä ja aluepalvelupisteet Turussa, Tampereella, Seinäjoella ja Oulussa. Tilastokeskuksella on palveluksessaan noin tuhat henkilöä. [1.]

Tilastokeskuksen toimintaa säätelevät muun muassa laki Tilastokeskuksesta sekä tilastolaki. Ensimmäisessä on tiivistetysti määritelty viraston tehtävät:

> Tilastokeskuksen tehtävänä on laatia yhteiskuntaoloja koskevia tilastoja ja selvityksiä sekä huolehtia valtion tilastotoimen yleisestä kehittämisestä yhteistyössä muiden valtion viranomaisten kanssa. [2.]

Tilastokeskus julkaisee säännöllisesti noin kahtasataa eri tilastoa. Tilastojen laatimiseen kehitetään viraston oman henkilöstön toimesta jatkuvasti uusia ohjelmistoja sekä me-

netelmiä. Käytettäviä ohjelmointikieliä on useita, mutta suurin osa nykyisestä tuotannosta tehdään käyttäen C#- ja SAS -ohjelmointikieliä.

Tilastokeskus käyttää tilastojen laadinnassa useista eri lähteistä koottuja tietoja. Näitä tietoja saadaan muun muassa yksityishenkilöiltä, yrityksiltä ja viranomaisilta.

Tiedonhankintaa voidaan tehdä esimerkiksi puhelinhaastattelujen ja sähköisten lomakkeiden avulla. Tietoja voidaan kerätä myös suoraan esimerkiksi jonkin toisen viranomaisen tietojärjestelmästä.

Tilastokeskuksen ydintoiminnan kannalta hyvät ja luotettavat tietoliikenneyhteydet ovat siis erittäin tärkeät.

3 Työn kulku

Opinnäytetyön tekeminen aloitettiin perehtymällä viraston tietoliikenneverkosta saatavilla olleisiin dokumentteihin. Lisäksi verkon ylläpidosta vastaavia henkilöitä haastateltiin. Haastattelujen tarkoituksena oli selvittää, oliko sillä hetkellä tiedossa verkon luotettavuuteen ja turvallisuuteen vaikuttavia ongelmia.

Tämän jälkeen verkon rakennetta tutkittiin tarkemmin selvittämällä reitittimistä ja kytkimistä käsin vanhan dokumentaation paikkansapitävyys. Myös fyysiset kytkennät kiinteistössä käytiin läpi.

Verkkokuvien laadinnassa käytettiin Microsoftin Visio -ohjelmistoa. Kuvista piirrettiin aina kahdet versiot; kaapelointikuvat fyysisten johtojen sijainnin näyttämistä varten sekä loogiset kytkentäkuvat kytkimien ja reitittimien asetusten ylläpitoa varten.

Osa opinnäytetyössä piirretyistä verkkokuvista sisältää luottamuksellista tietoa, joten niitä ei ole sisällytetty tähän raporttiin.

4 Tietoturva

4.1 Tietoturva käsitteenä

Tietoturvalla tarkoitetaan yleisesti ottaen menettelyjä ja järjestelyjä, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuus tarkoittaa sitä, ettei kukaan sivullinen saa tietoa käsiinsä. Eheys taasen tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja käytettävyys sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. [3, s. 109.]

Tietoturvapoikkeamalla taasen tarkoitetaan haitallista tapahtumaa tai olotilaa. Tämän seurauksena yksi tai useampi edellä kuvattu tietoturvan osa-alue on tai saattaa olla vaarantunut. [3, s. 110.]

4.2 Tietoturva tietoliikenneverkossa

Valtionhallinnon organisaatioita koskettava vuonna 2010 annettu tietoturva-asetus velvoittaa ottamaan tietoturvan huomioon kaikilla toiminnan osa-alueilla ja tähän kuuluu siis myös tietoliikenneyhteyksien suunnittelu ja toteutus. Tietoturva-asetuksen ohje, VAHTI 2/2010, sekä tätä ohjetta täydentävä erillinen sisäverkko-ohje, VAHTI 3/2010, määrittävät, mitä kaikkea tulisi huomioida eri tietoturvallisuuden tasoilla. Tasoja ohjeissa on määritelty kolme: perustaso, korotettu, ja korkea. Tietoturva-asetus vaatii kaikkia valtionhallinnon organisaatioita täyttämään vähintäänkin perustason vaatimukset. [4; 5; 6.]

Taulukko 1. Sisäverkko-ohjeen vaatimukset verkon aktiivilaitteille.

Viite	Vaatimus	Perustaso	Korotettu taso	Korkea taso
12.1	Organisaation liiketoiminnan vaatimusten pohjalta on arvioitu yhteyksien kriittisyys ja sovittu palvelutasoista (SLA) palveluntarjoajan kanssa.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.2	Kriittiset toimipisteiden väliset tai internet-yhteydet on kahdennettu.	suositus	suositus	pakollinen vaatimus
12.3	Kriittiset sovellukset ja protokollat luokitellaan palvelulaatumäärittelyssä (QoS) muita sovelluksia korkeammalle tasolle.	suositus	vahva suositus	pakollinen vaatimus
12.4	Kansallisen salassa pidettävän tiedonsiirrossa käytetään salausta, kun verk-	suositus	suositus	pakollinen vaatimus

	ko menee viranomaisen valvoman tilan ulkopuolelle.			
12.5	Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle.	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus
12.6	Salaukseen tulee käyttää vähintään-siirrettävän aineiston suojaustasolle-hyväksyttyjä salausratkaisuja	pakollinen vaatimus	pakollinen vaatimus	pakollinen vaatimus

Taulukossa 1. on esitetty esimerkin vuoksi muutamia niistä vaatimuksista, joita sisäverkon tietoturvalle on asetettu. Sisäverkko-ohjeen vaatimukset kattavat hyvin laajan kokonaisuuden aina verkon arkkitehtuurista toiminnan valvontaan asti.

Tilastokeskus on vuoden 2011 lopulla auditoitu. Toiminta täyttää perustason vaatimukset sekä osittain myös korotetun tason vaatimukset.

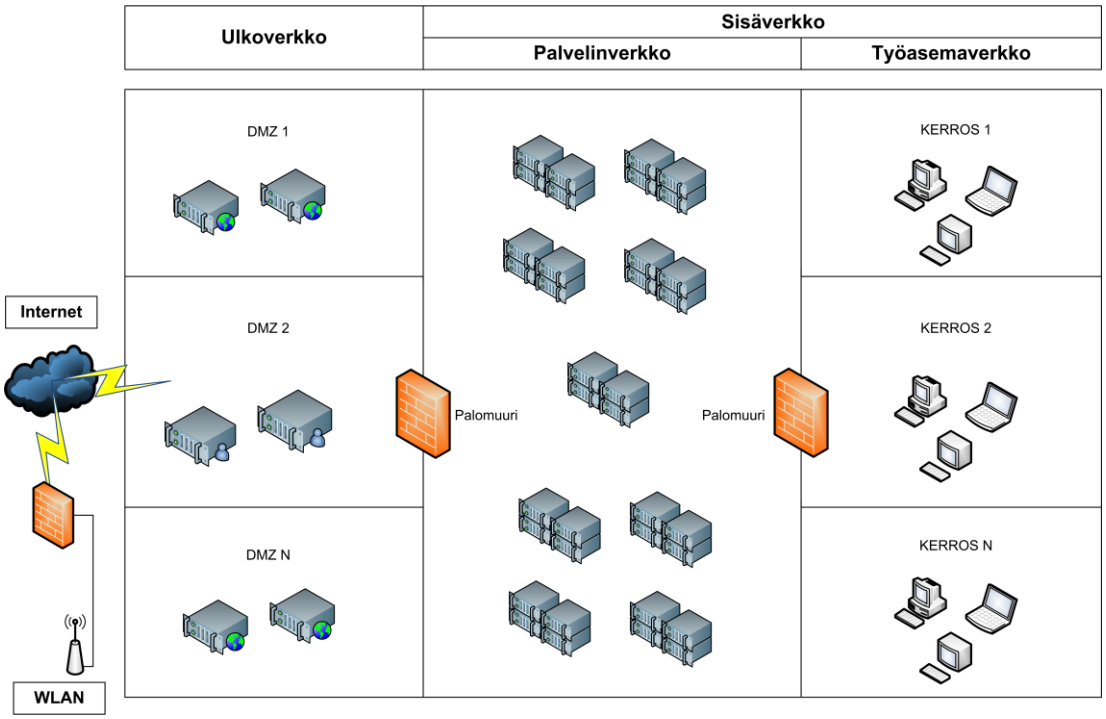
5 Tilastokeskuksen tietoliikenneverkko

5.1 Historiaa

Tilastokeskus siirtyi Token Ring -verkkotekniikasta Ethernetiin 90-luvun lopussa. Vaihdoksella haettiin tuolloin verkon helpompaa hallittavuutta ja suurempaa nopeutta. Token Ring -verkon maksiminopeus oli 16 Mb/s, kun taas ns. Fast Ethernet -verkko pääsi 100 Mb/s nopeuteen. Nykyään viraston verkon nopeudet vaihtelevat verkon osien käyttötarkoituksen mukaan 100 Mb/s - 10 Gb/s. Verkon teknisestä toteutuksesta ja kehittämisestä vastaa viraston oma tietotekniikkayksikkö.

5.2 Verkon rakenne

Karkeasti kuvattuna viraston verkko koostuu ulkoverkosta, eli niin kutsutusta DMZ-alueesta ja sisäverkosta. Sisäverkko jakautuu vielä lisäksi työasemaverkkoon, palvelinverkkoon ja kerrosverkkoon. Lisäksi osassa viraston tiloja on käytettävissä rajoitetun palvelun langaton WLAN-verkko, joka ei kuitenkaan ole osa sisäverkkoa.



Kuva 1. Tilastokeskuksen verkon yksinkertaistettu periaatekuva.

Ulkoverkko

Ulkoverkko on rajattu palomuurin avulla täysin omaksi alueekseen. Verkon alueelle ei pääse mistään muusta verkkoalueesta ilman rajoituksia. Myös ulkoverkon sisällä palomuuri rajoittaa ulkoverkossa olevien palvelinten välistä tietoliikennettä. Ulkoverkon palvelimilta on estetty tietoliikenneyhteyksien avaus sisäverkon suuntaan.

Tässä verkossa sijaitsevat kaikki ne palvelut, joihin Tilastokeskuksen asiakkailla on tarve päästä, kuten esimerkiksi viraston ulkoiset Internet-sivut ja yksityishenkilöiden sekä yritysten käyttöön tarkoitetut tiedonantopalvelut. Verkossa käytetään IPv4-osoitteita.

Sisäisesti ulkoverkko on jaettu useisiin DMZ-alueisiin palvelinten käyttötarkoituksen mukaan.

Sisäverkko

Sisäverkko-nimeä käytetään kuvaamaan työasemaverkosta, palvelinverkosta ja kerrosverkosta koostuvaa kokonaisuutta. Verkko tarjoaa kaikki tilastotuotannon tarvitsemat palvelut.

Työasemaverkko

Työasemaverkossa sijaitsevat kaikki työntekijöiden työasemat. Työasemat on kytkettyinä kerrosverkon kautta muuhun verkkoon joko 100 Mb/s tai 1 Gb/s nopeudella, hieman työntekijän tarpeista riippuen. Työasemissa käytetään julkisia IPv4-osoitteita. Tietoliikennettä rajoitetaan koko verkon palomuurilla sekä työasemien omalla keskitetysti hallitulla palomuurilla. Suorat yhteydet työasemilta Internet-verkkoon on estetty, ja kaikki tietoliikenne kulkee proxy-klusterin kautta.

Palvelinverkko

Palvelinverkossa sijaitsevat kaikki ne palvelimet, joihin pääsy voidaan sallia vain työasemaverkosta. Osa palvelimista käyttää julkisia, osa RFC 1918 mukaisia IPv4-osoitteita. Palvelimet ovat kytkettyinä verkkoon käyttäen joko valokuituja tai kuparikaapeleita. Nopeudet vaihtelevat välillä 1-4 Gb/s. Yli gigabitin nopeudet on saavutettu käyttäen IEEE 802.1AX-2008 -standardin mukaista linkkien yhdistämistä.

Kerrosverkko

Kerrosverkolla tarkoitetaan viraston kiinteistön eri kerrokset toisiinsa yhdistävää verkkoa. Yhteydet kerroksien välillä on toteutettu kahdennetuilla valokuiduilla. Kerrosverkko yhdistää myös viraston kaksi konesalia toisiinsa.

Jokaisessa kerroksessa on yksi tai useampia kytkinkaappeja, joista työasemien kaapelointi on työhuoneisiin vedetty. Kytkimiä kaapeissa on yleensä 3-4 kappaletta. Kytkimet on standardoitu, eli virasto hankkii aina tietyn tyyppisiä kytkimiä valituilta valmistajilta. Tietotekniikkayksikkö säilyttää varastossaan aina muutamia ylimääräisiä kytkimiä, jotta mahdolliset laiterikoista aiheutuvat käyttökatkot saadaan pidettyä lyhyinä.

Kytkimien hallintaan käytetään Extreme Networksin EPICenter-ohjelmistoa. Ohjelmiston avulla voidaan muun muassa seurata kytkinten tilaa, hallita asetuksia sekä päivittää kytkinten ohjelmistot. EPICenter koostuu palvelinohjelmistosta, joka asennetaan omalle palvelimelleen, sekä Java-pohjaisesta asiakasohjelmistosta, jota voidaan käyttää työasemista käsin.

WLAN-verkko

Viraston langaton verkko on tarkoitettu pääasiassa virastossa vierailevia ulkopuolisia varten. Verkon tietoliikenne kulkee erillisen palomuurin rajoittamana siten, että vain http- ja https -protokollia on mahdollista käyttää. Lisäksi verkosta ei pääse Tilastokeskuksen sisäverkon palveluihin lainkaan. Myös verkon kuuluvuus on rajoitettu niihin kerroksiin, joissa vierailijoita normaalisti liikkuu. Langattomassa verkossa käytetään RFC 1918:n mukaisia IPv4-osoitteita, joten verkon osoitteille tehdään koko verkon pääpalomuurissa NAT-muunnos Internet-verkkoon liikennöitäessä. Verkossa ei ole käytössä salausta tai tunnistautumista, mutta liikenne välitetään proxy-palvelimen lävitse mikä rajoittaa mahdollisten kohdeporttien määrää ja pitää tapahtumista normaalia http-lokia.

5.3 Vikasietoisuus

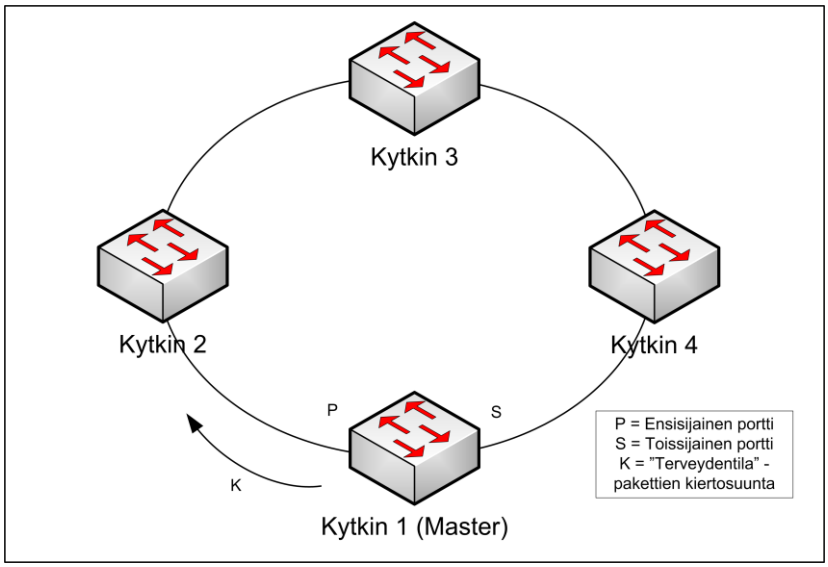
Verkon luotettavuutta on viimeisen seitsemän vuoden aikana saatu kehitettyä merkittävästi. Tähän on päästy pääasiassa kahdentamalla niin sisä- kuin ulkoverkonkin yhteyksiä. Vaikka tietoliikenneverkossa esiintyy muutamia kertoja vuodessa erilaisia vikoja, eivät nämä kovinkaan usein ole käyttäjille asti näkyneet. Verkon vikasietoisuuden lisäämisessä on avainasemassa ollut tekniikka nimeltä EAPS, jonka avulla on saatu palvelin- ja ulkoverkko suojattua.

EAPS

EAPS, eli Ethernet Automatic Protection Switching, on Extreme Networksin kehittämä tekniikka vikasietoisen rengasmaisen verkkotopologian luomiseksi. EAPS toimii OSI-mallin siirtoyhteyskerroksessa (Data Link layer). [7.]

EAPS-rengas muodostuu kahdesta tai useammasta kytkimestä, joista yksi määritellään master (isäntä) -kytkimeksi (kuva 2). Kuhunkin kytkimeen määritellään kaksi porttia, ensisijainen ja toissijainen. Master-kytkin lähettää säännöllisin väliajoin ensisijaisen portin kautta verkon tilan seurantapaketteja (Health Messages) renkaan muille kytkimille (transit-kytkimet). Master-kytkin vastaanottaa seurantapaketit toissijaisesta portistansa. Toissijaisesta portista ei normaalin toiminnan aikana sallita läpi muuta kuin EAPS-renkaan hallintaan kuuluvaa tietoliikennettä.

EAPS-domainilla tarkoitetaan ryhmää virtuaalisia verkkoja (VLAN), joista yksi on varattu EAPS:n toiminnan hallintaan (control-VLAN) ja loput kuljettavat varsinaista verkon hyötyliikennettä. Samassa kytkimessä voi olla yhtäaikaisesti useita EAPS-domaineja, joista jokaisella on siis oma hallinta-VLAN. Hallinta-VLAN:n tietoliikenne on luokiteltu kaikkea muuta verkon liikennettä tärkeämmäksi. [8, s. 2.]

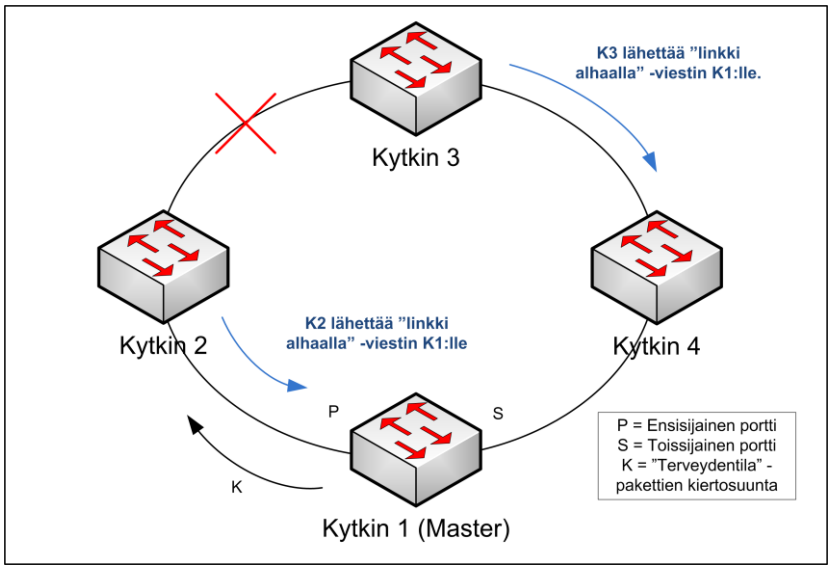


Kuva 2. EAPS-rengas.

Vikatilanteessa (kuva 3) master-kytkin havaitsee tapahtuneen joko muiden kytkimien lähettämistä ”vika havaittu” -viestipaketeista tai sitten väliin jääneistä verkon tilan seurantapaketeista. Master-kytkin lähettää oletusarvoisesti seurantapaketteja yhden sekunnin välein. Tämä hellotime-asetus voidaan tarvittaessa vaihtaa. Kahden seurantapaketin välinen aika saa oletusarvoisesti olla korkeintaan kolme sekuntia. Myös tämä failtime-asetus on vaihdettavissa. Failtime-asetuksen kasvattaminen voi tulla kyseeseen verkoissa, joiden kuormitus on jatkuvasti erittäin suuri. Tällöin vikatilanteen havain-

nointi seurantapakettien avulla tietenkin hidastuu. Samalla vähennetään kuitenkin riskiä siitä, että verkkovika todettaisiin väärin perustein.

Vian todettuaan master-kytkin avaa toissijaisen porttinsa myös muulle kuin hallintaliikenteelle. Tämän jälkeen master-kytkin tyhjentää FDB-tietokantansa (forwarding database), joka pitää siis sisällänsä kytkimen oppiman tiedon siitä, minne porttiin kytkimelle saapunut datapaketti tulee välittää. Käsky tyhjentää FDB-tietokanta lähetetään myös kaikille muille kytkimille hallinta-VLAN:n kautta. Tietokannan tyhjentämisen jälkeen kytkimet tekevät normaaliin tapaan päätökset siitä, minne paketit tulee välittää. [8, s. 3; 9.]



Kuva 3. Vian havaitseminen EAPS-renkaassa.

Master-kytkin jatkaa verkon tilan seurantapakettien lähettämistä myös vikatilanteen aikana. Vasta kun seurantapaketti jälleen saapuu master-kytkimen toissijaiseen porttiin, voidaan todeta EAPS-renkaan olevan ehjä. Tämän jälkeen toissijaisessa portissa estetään jälleen kaikki muu paitsi EAPS:n hallintaan liittyvä tietoliikenne. Vikatilanteessa transit-kytkimet saavat välittää hyötyliikennettä vasta, kun master-kytkin toteaa renkaan olevan ehjän.

Yhden polun vikaantuessa tietoliikenne saadaan siis siirrettyä pienellä, käytännössä alle 50 ms, viiveellä käyttämään toista reittiä. EAPS soveltuu käytettäväksi niin LAN- kuin

MAN -verkoissa. EAPS kehitettiin nopeammaksi vaihtoehdoksi Spanning Tree -protokollalle. [7.]

Internet-yhteys

Tilastokeskuksen yhteys Internetiin on myös kahdennettu. Pääyhteytenä on nopeudella 1 Gb/s toimiva valokuitu. Varayhteytenä on radiolinkki, jonka kautta siirtonopeus on maksimissaan 200 Mb/s. Pääyhteyden vikaantuessa varayhteys otetaan käyttöön VRRP:n avulla.

VRRP, eli Virtual Router Redundancy Protocol, on määritelty IETF:n julkaisemassa RFC 5798 -dokumentissa. VRRP-prokollan avulla saadaan poistettua staattisissa reitityksissä oleva heikko kohta, eli mahdollinen oletusreitittimen hajoaminen. VRRP:ssä reitittimenä toimii virtuaalinen reititin, jonka tehtävän toteuttaa kullakin hetkellä valittuna oleva fyysinen reititin. Päätelaite ei siis koskaan käytä reitittimien fyysistä IP- tai MAC-osoitetta vaan virtuaalista. [10.]

VRRP määrittelee valintaprotokollan, jonka avulla fyysiset reitittimet valitsevat keskuudestaan reitityksen toteuttavan laitteen. Keskinäisessä kommunikoinnissa reitittimet käyttävät multicast IP-osoitetta 224.0.0.18.

6 Havaitut ongelmat ja niiden korjausehdotukset

6.1 Puutteellinen dokumentointi

Kerättäessä yhteen verkon rakenteesta ja palveluista olevaa dokumentaatiota havaittiin, että ulkoverkkoa käsittelevä dokumentaatio oli sisäverkon kuvauksia paljon paremmin ajan tasalla. Syyksi tälle löydettiin se, että virastolla oli ollut ulkoverkkoon liittyviä hankkeita ulkopuolisten toimijoiden kanssa, jolloin ajan tasalla olevaa dokumentaatiota oli tarvittu.

Alun perin oli ajateltu, että vanhoja dokumentteja ei tarvitsisi uudelleen piirtää, vaan ainoastaan päivittää. Alkuperäisissä Microsoft Visiolla piirretyissä kuvissa oli kuitenkin

ongelmia. Nämä johtuivat muun muassa piirto-ohjelman version vaihtumisesta. Osasta kuvia oli olemassa vain PDF-versiot. Vanhojen kuvien osalta päädyttiin siis piirtämään ne kokonaan uusiksi.

Syynä kuvien puutteellisuuteen ja vanhenemiseen todettiin pääasiassa olevan verkosta vastaavien asiantuntijoiden suuresta työkuormasta johtuva ajanpuute. Myöskään suunnitteluvaiheessa syntyneet dokumentit eivät kovin usein ole olleet sellaisinaan kelvollisia kuvaamaan syntynyttä lopputulosta. Lisäksi aikaa dokumentaation tekemiseen ei verkon muutostöissä ole erikseen varattu silloin, kun on arvioitu työn kestoa.

Dokumentaation säilytyksestä ei myöskään ollut yhtenäistä käytäntöä. Osa asiantuntijoista tallensi dokumentteja Tietotekniikka-yksikön sisäiseen wiki-sivustoon, mutta osa tallensi dokumentteja vain itselleen jakamatta niitä muille asiantuntijoille.

Näiden havaintojen pohjalta Tietotekniikka-yksikölle ehdotettiin menettelyä, jossa verkon muutostöissä dokumentaatiolle varattaisiin huomattavasti enemmän aikaa. Lisäksi pyrittäisiin tuottamaan mahdollisimman paljon hyvää dokumentaatiota jo työn suunnitteluvaiheessa. Dokumentaation säilyttämiseen ehdotettiin ratkaisua, jossa kaikki dokumentaatio vietäisiin saman versiohallinnan piiriin, jota käytettiin viraston sisäisessä sovelluskehityksessä.

6.2 Tuntemattomat päätelaitteet

Verkon ylläpitäjien haastatteluissa tuli selkeästi esiin tarve saada estettyä tuntemattomien päätelaitteiden luvaton kytkentä viraston verkkoon. Ajatus siitä, miten esto tehtäisiin, oli olemassa, mutta tarjolla olevaan tekniikkaan ei ollut vielä ehditty kunnolla perehtyä. Tarkoituksena oli ollut rajoittaa verkkoon pääsy vain niihin laitteisiin, joiden MAC-osoite on tiedossa.

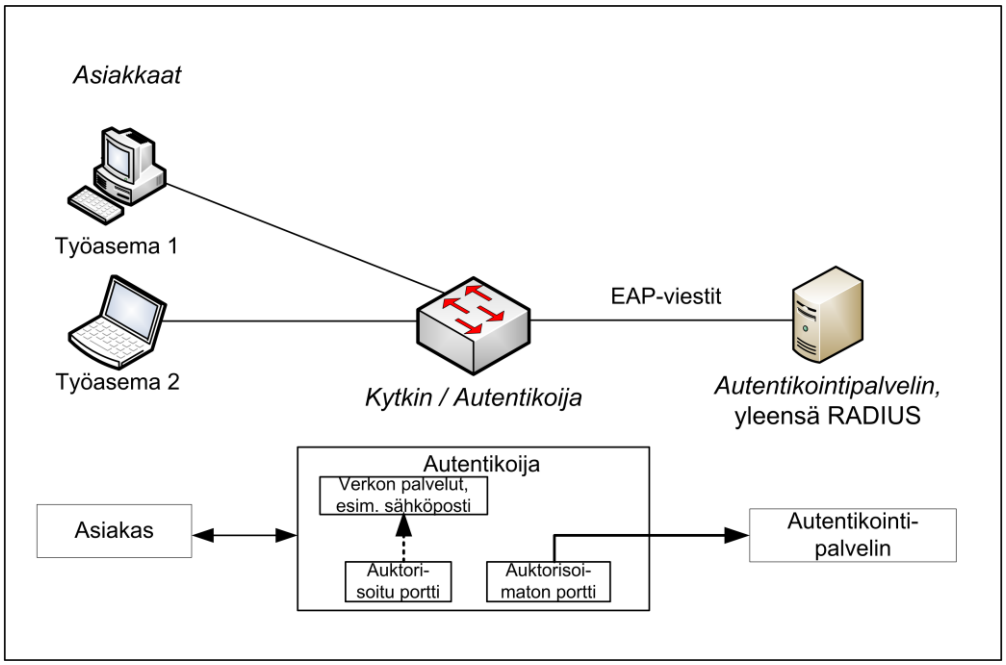
Päätelaitteen tunnistus verkkosovittimen MAC-osoitteen avulla

MAC-osoite (Media Access Control) on verkkosovittimen Ethernet-verkossa yksilöivä osoite. Se koostuu kuudesta kaksinumeroisesta heksadesimaalisesta luvusta, joista kolme ensimmäistä muodostavat sovittimen valmistajan itselleen varaaman etuliitteen ja kolme viimeistä lukua juoksevan sarjanumeron. Näin jokaisella verkkosovittimella pitäisi siis käytännössä olla uniikki, yksilöivä osoite, mikä puolestaan mahdollistaa osoitteen käytön laitetunnisteena. Osoite esitetään usein siten, että heksadesimaaliset luvut ovat toisistaan erotettuina joko käyttäen kaksoispistettä tai väliviivaa, esimerkiksi 00:aa:aa:aa:64:ce. [11.]

MAC-osoite on yleensä fyysisesti kirjoitettuna verkkosovittimeen jo tehtaalla. Osoite on voitu tallentaa esimerkiksi muistipiiriin, jonka sisältöä voidaan lukea, muttei muokata. Normaalisti osoitetta ei ole siis mahdollista pysyvästi vaihtaa, mutta useat verkkosovittimet sallivat osoitteen väliaikaisen vaihtamisen. Tästä syystä MAC-osoitteisiin ei pidä koskaan täysin luottaa, vaan niiden rinnalla tulisi käyttää myös muita tunnistautumistapoja.

Porttikohtainen todentaminen

IEEE 802.1X Port Based Authentication, eli porttikohtainen todentaminen, on standardi, jota käytetään Ethernet-verkoissa estämään luvattoman päätelaitteen liikennöinti verkon liityntäpisteen kautta. Liityntäpiste on Ethernet-verkoissa esim. kytkimen portti tai langattoman tukiaseman looginen portti. [12.]



Kuva 4. 802.1X:n komponentit.

802.1X-standardissa tunnistettavalle päätelaitteelle luodaan kaksi erillistä loogista porttia: auktorisoitu ja auktorisoimaton looginen portti. Alkuvaiheessa, kun päätelaitetta ei ole vielä tunnistettu, on liikennöinti mahdollista ainoastaan auktorisoimattoman portin kautta, mikä tarkoittaa sitä, että autentikoija ohjaa liikenteen autentikointipalvelimelle. Auktorisoimattoman portin kautta välitetään vain autentikointiviestit (EAP) autentikoinpalvelimelle. Autentikointipalvelin tekee varsinaisen päätöksen verkkoon pääsyn sallimisesta tai kieltämisestä. Onnistuneen autentikoinnin jälkeen autentikoijan looginen portti voidaan muuttaa auktorisoituun tilaan ja päätelaite voi aloittaa normaalin liikennöinnin.

Autentikointi itsessään voidaan tehdä usealla eri tavalla. Se voi pohjautua esimerkiksi ihan vain pelkkään päätelaitteen MAC-osoitteeseen. Tällöin voidaan käyttää käyttäjätunnuksia ja salasanoja, sertifikaatteja, tai edellä mainittujen yhdistelmiä.

RADIUS

IEEE 802.1X -standardissa autentikointi tehdään AAA-palvelun toteuttavalla protokollalla. Lyhenne tulee sanoista Authentication (todentaminen tai autentikointi), Authorization (valtuutus) ja Accounting (tilastointi). Yleensä tämä protokolla on RADIUS, eli Re-

mote Authentication Dial In User Service -protokolla. RADIUS on tyypillinen asiakas/palvelinprotokolla, ja se käyttää UDP-protokollaa liikennöintiin. [13.]

MAC-osoitteiden kerääminen RADIUS-palvelinta varten

Jotta RADIUS-palvelin voisi tehdä MAC-osoitteeseen perustuvan tunnistamisen, tulee sillä olla pääsy osoitteet sisältävään tiedostoon tai tietokantaan. Tietojen tulisi myös pysyä ajan tasalla jatkuvasti.

Tilastokeskuksessa on käytössä työasemien hallinnointiin tarkoitettu ohjelmisto nimeltä Novell Zenworks. Se on asennettuna jokaisessa viraston työasemassa ja kannettavassa ja sen avulla voidaan muun muassa jaella ohjelmistopaketteja ja hallita koneita etänä. Lisäksi ohjelmisto pitää yllä luetteloa kaikista asennetuista sovelluksista. Kerättyjen tietojen joukossa ovat myös päätelaitteiden MAC-osoitteet.

Aluksi MAC-osoitteiden kerääminen vaikuttikin suoraviivaiselta, mutta Zenworksin tietokannan tarkempi tutkiminen paljasti, ettei siellä olekaan pelkästään käytössä olevien verkkolaitteiden MAC-osoitteet. Hallintaohjelmisto keräsi siis tietokantaansa myös erilaisten virtuaalisten verkkosovittimien osoitteet, joita käyttivät muun muassa työasemiin asennetut VPN-ohjelmistot. Koska tietokannasta ei voitu siis helposti ja yksiselitteisesti hakea pelkästään kiinteän verkkokortin ja WLAN-adapterin MAC-osoitteita, päätettiin Zenworks hylätä RADIUS-palvelimen tietolähteenä.

Lopuksi päädyttiin menettelyyn, jossa työasemien hankinnasta vastaavat ihmiset keräävät uusista laitteista MAC-osoitteet talteen erilliseen tietokantaan. Tietokannan pohja päätettiin kuitenkin luoda Zenworksin sisältämistä tiedoista suodattamalla sieltä käsityönä pois ylimääräiset osoitteet.

Kuten jo aiemmin todettiin, MAC-osoitteita ei suositella käytettäväksi ainoana päätelaitteiden tunnistamiskeinona. Tunnistautumisprosessiin päätettiin tästä syystä liittää myös käyttäjien Active Directory -verkkotunnukset. Näin työntekijöille tarkoitettuun verkkoon liittyäkseen tulee sekä päätelaitteen että käyttäjän olla tunnistettuja.

FreeRADIUS

RADIUS-toteutuksia on olemassa useita, joista osa on ilmaisia, osa kaupallisia. Ilmainen FreeRADIUS on saavuttanut hyvän jalansijan ja on projektin oman näkemyksen mukaan myös maailman eniten käytetyin. Tuotteelle on saatavilla myös maksullinen tukipalvelu. FreeRADIUS toimii lisäksi lähes minkä tahansa modernin Unix-käyttöjärjestelmän kanssa. Näiden tietojen pohjalta päädyttiin tutkimaan, miten tuote soveltuu Tilastokeskuksen laiteympäristöön. [14.]

FreeRADIUS päätettiin asentaa viraston VMware-virtualisointialustalle openSUSE Linux -käyttöjärjestelmän alle.

FreeRADIUS-palvelin

FreeRADIUS-ohjelmisto löytyi suoraan openSUSE:n valmiiksi kääntämistä ohjelmistopaketeista. Näin ollen ohjelmistoa ei tarvinnut itse kääntää lähdekoodista ja ohjelmaan tulevat päivitykset saadaan normaalien käyttöjärjestelmäpäivitysten mukana.

FreeRADIUS sisältää tuen hyvin monille erilaisilla tunnistautumistavoille, protokollille ja laitealustoille. Tästä syystä sen asetusten tekeminen ja käyttöönotto vaatii aikaa sekä huolellisuutta.

Testausta varten FreeRADIUS asetettiin aluksi käyttämään tietokantayhteyksien sijaan tavallista tekstitiedostoa MAC-osoitteiden lähteenä. Lisäksi Active Directory -tuki jätettiin myös pois käytöstä. Näin saatiin suhteellisen nopeasti todettua, että ohjelmisto toimii. Tarvittavat asetukset löydettiin FreeRADIUS-tuotteen omasta dokumentaatiosta.

FreeRADIUS-ohjelmiston asetustiedostot löytyvät Linux-palvelimen hakemistosta /etc/freeradius. Tiedostoja, joihin siellä tarvitsee tehdä muutoksia on neljä. Liitteessä 1 on lyhyesti kuvattu testausta varten tarvittavat asetukset.

Tiedostossa radius/policy.conf muokataan säännöllisellä lausekkeella palvelimelle saapuva MAC-osoite yhtenäiseen muotoon. Muotona on pienet kirjaimet väliviivalla eroteltuina.

Tiedostossa raddb/modules/file määritellään, minkä nimisestä tiedostosta MAC-osoitteet haetaan ja tiedostossa raddb/authorized_macs puolestaan kerrotaan itse osoitteet. Tiedostossa raddb/sites-available/default käsitellään itse tunnistautuminen.

Kytkinten RADIUS-asetukset

FreeRADIUS-palvelimen lisäksi tulee tietysti tehdä tarvittavat asetukset myös kytkimiin. Tilastokeskus käyttää Extreme Networksin kytkimiä ja näiden osalta tarvittavat komennot on kuvattu oppaissa ExtremeXOS Concepts ja ExtremeXOS Commands [15, s. 874; 16].

Aluksi kytkimeen tulee määritellä käytettävä RADIUS-palvelin:

```
configure radius netlogin primary server radius.server.stat.fi client-
ip 192.168.98.101
```

Komennossa oleva ”client-ip”–parametri on kytkimen IP-osoite. RADIUS-palvelimia voidaan määritellä vikasietoisuuden parantamiseksi kaksi. Toinen palvelin määritellään vaihtamalla parametrin ”primary” tilalle ”secondary”. Kytkin yrittää tunnistautumista kunkin RADIUS-palvelimen kanssa kolme kertaa.

Palvelimen määrittelyn jälkeen asetetaan kytkimen ja RADIUS-palvelimen välisen liikenteen salauksessa käytettävä avain:

```
configure radius netlogin primary shared-secret salainen-rad-avain
```

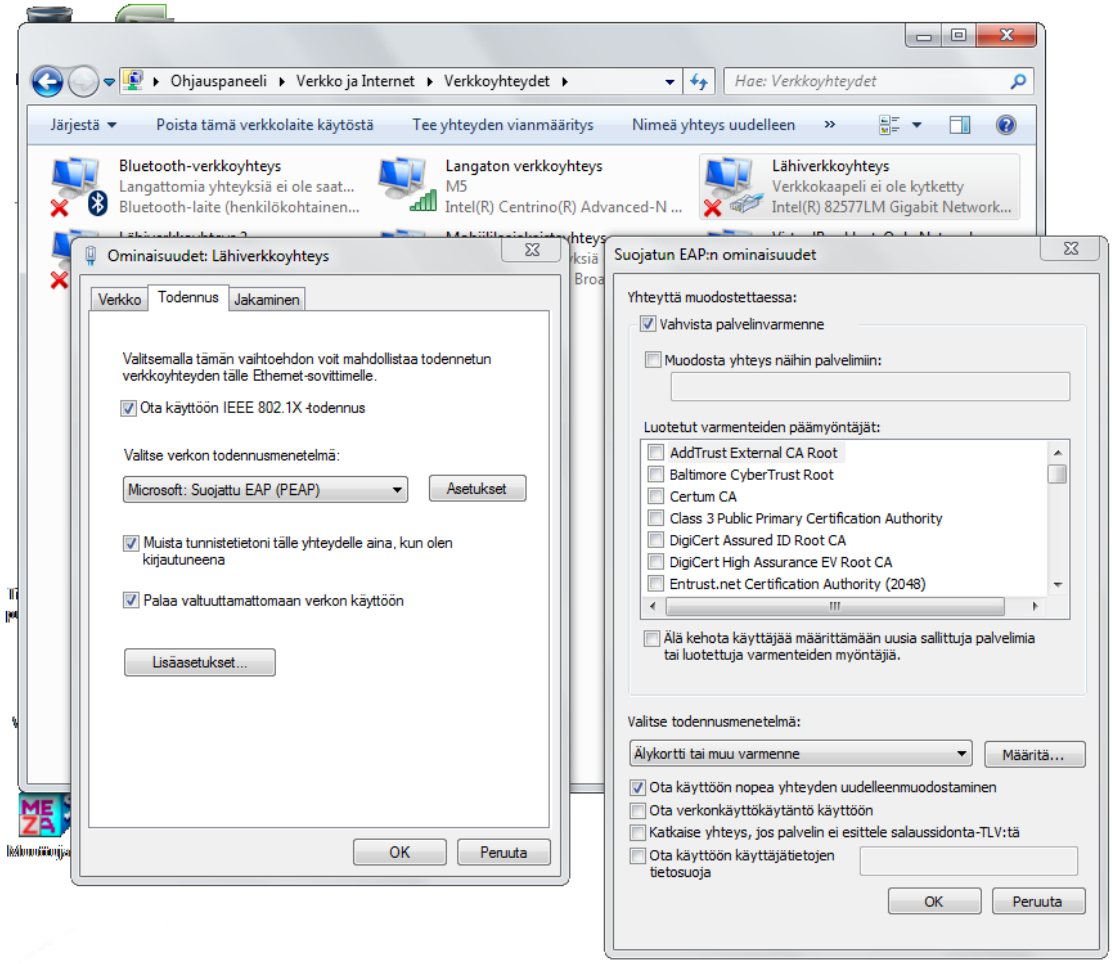
Molemmille palvelimille voidaan määritellä oma salausavain. Asetusten tekemisen jälkeen tulee RADIUS-tunnistautumispalvelu ottaa vielä käyttöön:

```
enable radius netlogin
```

Opinnäytetyön aikana ei ehditty kytkinten porttikohtaista tunnistaumista vielä testata, vaan testauksessa käytettiin WLAN-tukiasemaa sekä FreeRADIUS-ohjelmiston mukana tulevaa testaustyökalua.

Microsoft Windows 7 ja 802.1X

Tilastokeskus käyttää työaseminaan pääasiassa Microsoftin Windows-käyttöjärjestelmällä varustettuja tietokoneita. Tuki 802.1X:lle on käyttöjärjestelmässä ollut sisäänrakennettuna Windows XP:stä lähtien.



Kuva 5. Windows 7 ja verkkosovittimen 802.1X-asetukset.

Windows 7:ssä tarvittavat asetukset tehdään per verkkosovitin (ks. kuva 5). Mikäli 802.1X otetaan käyttöön langallisessa verkkosovittimessa, tulee käyttöjärjestelmän palvelu nimeltä Wired AutoConfig olla myös päällä. Oletuksena tämä on sammutettuna. Mikäli palvelu on sammutettuna, ei verkkosovittimen asetusten todennus-välilehti näy, eikä asetuksia pääse siis tekemään.

Linux ja 802.1X

Osa Tilastokeskuksen ylläpitäjistä ja sovelluskehittäjistä käyttää Linuxia työasemissaan. Näissä koneissa 802.1X-tuki voidaan toteuttaa wpa_supplicant-nimisellä ohjelmistolla. Seuravaana on lyhyt esimerkki asetustiedostosta, jolla saadaan työasema liitettyä verkkoon, jossa WPA-Enterprise on käytössä:

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=wheel

network={

# Verkon SSID
ssid="_STAT"
scan_ssid=1
key_mgmt=WPA-EAP

# AES-salaus
pairwise=CCMP
group=CCMP
eap=TLS
identity="harri@stat.fi"

# Sertifikaatit
ca_cert="/etc/cert/ca.pem"
client_cert="/etc/cert/user.pem"
private_key="/etc/cert/user.prv"
private_key_passwd="salasana"
}
```

Wpa_supplicant kuuluu nykyään kaikkien Linux-jakelujen vakio-ohjelmistoihin.

6.3 Verkkomyrskyt

Tilastokeskuksessa tapahtuneiden verkon häiriöiden kuvauksia läpikäytäessä havaittiin, että aina silloin tällöin joku työntekijöistä oli joko kytkinkaapissa tai työhuoneessa kytkenyt verkkokaapelin siten, että kytkentä aiheutti kyseisen kerroksen alueelle verkkomyrskyn. Ongelmaan oli tiedossa yksinkertainen ratkaisu, mutta sitä ei ollut missään vaiheessa ehditty toteuttaa. Ratkaisuna olisi Spanning Tree -protokollan ottaminen käyttöön kerroskytkimissä. Niinpä opinnäytetyön aikana päätettiin tehdä tämä korjaus viraston verkkoon.

STP

STP, eli Spanning tree-protokolla, joka on määritelty IEEE:n standardeissa 802.1d, 802.1s ja 802.1w, on siltojen ja kytkimien käyttämä toiminto, jonka avulla voidaan estää mahdolliset silmukat verkossa. Kytkin välittää liikennettä MAC-osoitteiden perusteella oikeaan porttiin. Jos Ethernet kehyksen kohde-MAC -osoite on tuntematon tai kehys on broadcast- tai multicast-tyyppiä, annetaan kehyksen ylivuotaa kaikkiin muihin paitsi tuloporttiin. Nämä ylivuotavat kehykset muodostavat helposti silmukoita ja broadcast-myrskyjä. [17; 18.]

Kytkimet neuvottelevat STP:n avulla silmukattoman verkkohierarkian. Neuvottelu tapahtuu lähettämällä STP:n käyttämiä Bridge Protocol Data Unit -paketteja (BPDU) toisille kytkimille, oletusarvoisesti joka portista. Tätä prosessia kutsutaan juurikytkimen äänestykseksi. Juurikytkimen valinta ei ole nopea prosessi, vaan se voi kestää 30-50 sekuntia.

Muut kytkimet laskevat edullisimman reitin juurikytkimelle. Ne käyttävät valinnassa taulukossa 2 esitettyjä hintoja, jotka määräytyvät portin nopeuden mukaan.

Taulukko 2. IEEE 802.1d:n mukaisia STP:n polun hintoja nopeuteen suhteutettuna.

Nopeus	10 Gb/s	1 Gb/s	100 Mb/s	10 Mb/s
Hinta	2	4	19	100

Juurikytkin tekee päätöksen siitä, mikä yhteys kytkinten välillä asetetaan aktiiviseksi. Muut yhteydet jäävät varalle. Näin siis yhteydet kytkinten välillä ovat vain näennäisesti rinnakkaisia, kun vain yksi yhteys on kerrallaan käytössä.

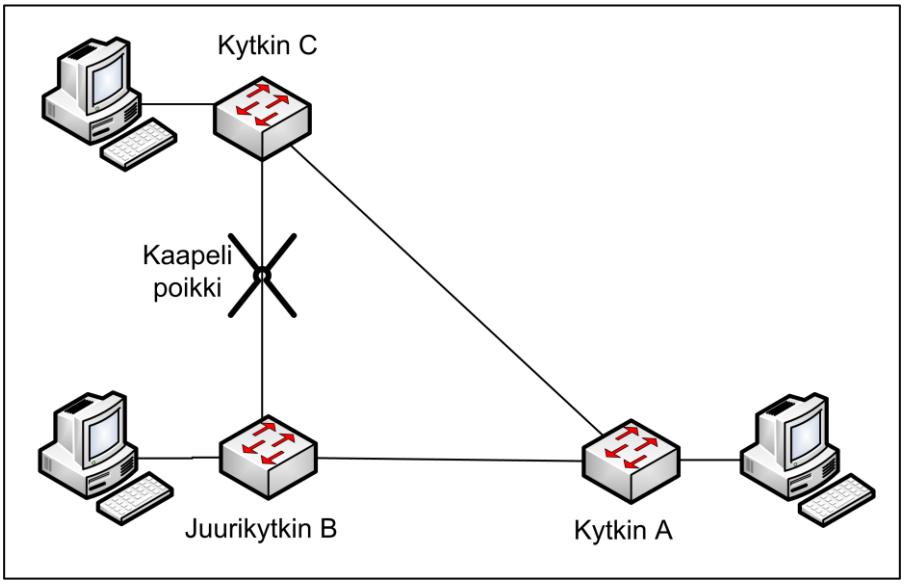
Verkon vikaantuessa tai topologian muuten muuttuessa kytkimet pysäyttävät hyötyliikenteen välityksen siksi, kunnes uusi reitti verkon eri osien välille on saatu selville.

Kun kytkimen porttiin liitetään kaapeli tai verkon topologia muuten muuttuu, on kytkimen portti aluksi suljetussa tilassa, jolloin se vastaanottaa BPDU-paketteja mutta ei välitä liikennettä. Oletusarvoisesti kytkin odottaa 20 sekunttia BPDU-viestiä juurikytkimeltä alkuperäistä polkua pitkin. Tätä aikaa kutsutaan nimellä Max-Age.

Suljetun tilan jälkeen kytkimen portti siirtyy kuuntelutilaan. Tätä kestää oletusarvoisesti 15 sekuntia (Forward Delay). Tässä tilassa portti ei välitä liikennettä, mutta vastaanottaa BPDU-paketteja sekä poistaa siltaustaulustaan ne reitit, jotka on opittu katkenneen yhteyden kautta.

Tämän jälkeen portti siirtyy oppivaan tilaan, jonka aikana liikennettä ei edelleenkään välitetä, mutta siltaustaulu rakennetaan uudestaan. Kesto on oletusarvoisesti 15 sekuntia. Lopuksi portti siirtyy liikennettä välittävään tilaan.

Spanning Tree -protokollan oletusasetuksilla topologian muutos pysäyttää kytkimen portin liikenteen välityksen 50 sekunnin ajaksi, kun kyseessä on epäsuora linkkivika. Suorasta linkkiviasta toipuminen kestää puolestaan 30 sekunttia.



Kuva 6. Esimerkki vikatilanteesta STP:tä käyttävässä verkossa.

Kuvassa 6 olevassa vikatilanteessa juurisilta lähettää STP-protokollan Hello-paketteja kahden sekunnin välein. Kytkin C havaitsee, ettei Hello-paketti tule kuin yhtä kautta aiemman kahden sijaan ja lähettää topologian muuttumisesta viestin takaisin juurelle. Juurikytkin lähettää tämän jälkeen topologian muutosviestin kaikille kytkimille topologien korjaamiseksi. Kyseessä on suora linkkivika.

Spanning Tree -protokollasta on olemassa myös nopeammin toimiva versio, Rapid Spanning Tree (RSTP) -protokolla. Tätä ei viraston verkossa voitu kuitenkaan ottaa

käyttöön, koska kerrosverkon kytkimistä vain uusimmat tukivat sitä. Lisäksi STP-protokollan ominaisuuksien katsottiin olevan riittävät suojaamaan verkkomyrskyiltä niitä kytkimiä, joihin työasemat oli kytketty.

STP-protokolla suojaa viraston verkossa siis vain niitä kytkimiä, joihin työasemat on kiinnitetty. Muun verkon osalta suojauksesta vastaa EAPS. Mahdollinen ongelma työasemakytkimessä ei siis vaikuta muuhun verkkoon.

6.4 WLAN-verkko

Nykyään viraston työasemista yhä useampi on kannettava. Monet työntekijät ovat siirtyneet käyttämään pelkkää kannettavaa tietokonetta perinteisen pöytäkoneen sijaan. Tämän on tehnyt mahdolliseksi kannettavien tietokoneiden nopeuden kasvu ja hintojen lasku.

Samalla kun kannettavat tietokoneet virastossa lisääntyivät, alkoivat myös vaatimukset työnteon mahdollistavasta langattomasta verkosta kasvaa. Käyttäjiltä saadun palautteen pohjalta voitiin todeta, että kaksi suurinta ongelmaa nykyisessä WLAN-verkossa olivat sallittujen liikennöintiprotokollien vähyys ja verkon heikko kuuluvuus kiinteistössä.

Erityisesti käyttäjät kaipasivat mahdollisuutta muodostaa WLAN-verkosta yhteys sisäverkkoon. Nyt jos käyttäjä halusi esimerkiksi lukea työpostiaan neuvotteluhuoneesta kannettavallansa, tuli hänen avata VPN-yhteys sisäverkkoon käyttäen 3G-yhteyttä. Kokoushuoneet ovat kyllä varustettu tietokoneilla, mutta verkkopistokkeita ei yleensä niissä ole kuin juuri tälle vakiovarustukseen kuuluvalle tietokoneelle.

Syy nykyisen WLAN-verkon rajoituksiin löytyi viraston aiemmasta suhtautumisesta langattomaan verkkotekniikkaan. Tekniikkaa ei tuolloin pidetty riittävän turvallisena ja lisäksi langattoman verkon tarpeellisuudesta oltiin erimielisiä. Näistä syistä verkko rakennettiin vain vierailijoiden käyttöön.

Tietoliikenteen salaaminen

Langattomien verkkojen tietoliikenteen salaamiseen on useita eri tapoja. Nykyään useimmiten käytetään kuitenkin standardia IEEE 802.11i, joka tunnetaan paremmin nimellä Wi-Fi Protected Access II (WPA2). WPA2 käyttää kahta eri tapaa tietoliikenteen salaamiseen. WPA2-Personal on tarkoitettu koteihin ja pieniin toimistoihin eikä se vaadi erillistä autentikointipalvelinta. Tällöin jokainen verkkoon liittyvä laite käyttää samaa 256-bittistä Advanced Encryption Standard (AES) -avainta. WPA2-Enterprise (WPA-802.1X) on taasen suunniteltu suurempiin verkkoihin ja vaatii aina erillisen autentikointipalvelimen. [19.]

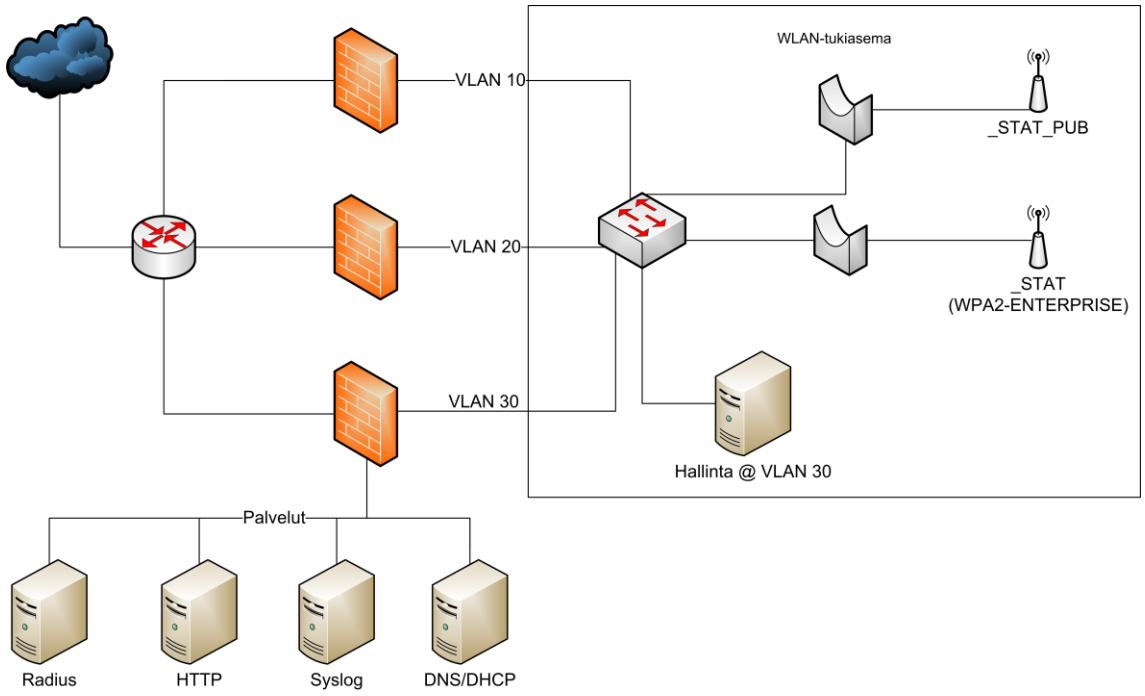
Ehdotus uudeksi langattomaksi verkoksi

Uudeksi WLAN-verkoksi päädyttiin ehdottamaan ratkaisua, jossa varsinaisia verkkoja on kaksi. Ensimmäinen verkko olisi viraston työntekijöiden käyttöön ja toinen vierailijoita varten. Kuvassa 7 on havainnollistettu verkon rakennetta tukiasemasta katsottuna.

Radioverkon tietoturvan kannalta pidettiin tärkeänä, ettei tukiasemilla ole sellaista hallintaliittymää, johon pääsisi radioverkon kautta. Hallinta tapahtuisi siis kuvassa 7 näkyvän VLAN 30 -verkon kautta kiinteää verkkoyhteyttä käyttäen. Radioverkoissa (VLAN 10-20) ei tulisi myöskään olla lainkaan palvelimia.

Vierailijoille tarkoitetussa verkossa (_STAT_PUB) käytettäisiin WPA2-Personal salausta. Alueelta sallittaisiin lähes rajoittamaton liikenne Internetiin. Tietyt liikennetyypit kuitenkin suodatettaisiin, kuten vertaisverkkoliikenne, ja kaistaa myös säännösteltäisiin.

Työntekijöille tarkoitettuun _STAT-verkkoalueeseen, josta siis pääsisi rajatusti Tilastokeskuksen sisäverkon palveluihin, tunnistauduttaisiin käyttäen päätelaitteen MAC-osoitetta sekä käyttäjän Active Directory -tunnuksia. Vain viraston hallinnoimat laitteet hyväksyttäisiin tälle verkkoalueelle. Tällä verkkoalueella käytettäisiin WPA2-Enterprise salausta ja RADIUS-autentikointia.



Kuva 7. WLAN-verkon rakenne

Isoimpana muutoksena aiempaan WLAN-toteutukseen nähden olisi siis viraston omille työntekijöille pääsy tiettyihin sisäverkon palveluihin, kuten Intranetiin ja sähköpostiin. Varsinaisiin tuotantojärjestelmiin, kuten UNIX-laskentaympäristöön, pääsy vaatisi lisäksi vielä VPN-yhteyden.

7 Yhteenveto

7.1 Verkon nykytila

Viraston sisäverkon MAC-osoitteisiin pohjautuva päätelaitetunnistuksen tekniikka on saatu testattua ja todettu toimivaksi. MAC-osoitteet sisällään pitävä tietokanta ei ole kuitenkaan vielä täysin valmis, ja Extreme Networksin kytkinten liittäminen RADIUS-palvelimeen on vielä kesken.

Työasemaverkossa väärin kytketty verkkokaapeli ei enää aiheuta ko. kerrosverkon alueelle näkyvää verkkomyrskyä, vaan ongelma on saatu poistettua STP-protokollaa käyttäen.

Opinnäytetyön aikana Tilastokeskuksen radiolinkki purettiin ja tilalle rakennettiin toinen valokuituyhteys. Varayhteyden nopeus on nyt siis sama kuin pääyhteyden.

WLAN-verkko

WLAN-verkon toteutus päätettiin tehdä kuluttajatason tukiasemilla ja korvata niiden valmistajan ohjelmisto OpenWRT:llä. OpenWRT on sulautetuille laitteille, kuten esimerkiksi reitittimille, tarkoitettu vapaasti saatavissa oleva Linux-jakelu, ja se keskittyy erilaisissa tietoverkoissa tarvittavien palveluiden toteuttamiseen. [20.]

Tukiasemaksi valittiin TP-LINK Technologies Companyn valmistama TP-LINK WDR4300 [21]. Ratkaisulla haettiin ensisijaisesti kustannussäästöjä mutta kuitenkin niin, että toteutus on mahdollisimman hyvin toimiva ja hallittava.

Tukiasema perustuu Qualcomm Atheroksen valmistamaan MIPS-arkkitehtuurin mukaiseen AR9344-piiriin. Tähän järjestelmäpiiriin on integroitu 2.4 GHz:n taajuusalueella toimiva IEEE 802.11b/g/n -standardin mukainen radiolähetin. Erillisellä AR9580-piirillä on 5 GHz:n taajuusalueella toimiva radiolähetin. Tukiasemassa oleva 5-porttinen kytkin on toteutettu AR8327N-piirillä. Porttinopeus kytkimessä on 1 Gb/s. Muistia laitteessa on 128 MB. [22.]

7.2 Tulevaisuus

Tilastokeskuksen verkon kehittämiskohteina voidaan tulevaisuudessa nähdä olevan ainakin kaikkien työasemien yhteyksien nopeuksien nostot. Kerrosverkon kytkinten uusiutuessa myös Rapid Spanning Tree -protokollan käyttöönottoa tulisi harkita. Lisäksi verkon dokumentointiin on syytä panostaa jatkossa enemmän.

Lähteet

1 Tilastokeskus - tiedolla tulevaisuuteen. 2011. Verkkodokumentti. <http://www.tilastokeskus.fi/org/>. Luettu 10.11.2012.

2 Laki Tilastokeskuksesta. 1992. Verkkodokumentti. <http://www.finlex.fi/fi/laki/ajantasa/1992/19920048>. Luettu 13.9.2013.

3 Valtiovarainministeriö. 2008. Valtionhallinnon tietoturvasanasto. Helsinki: Edita Prima Oy

4 Tietoturva-asetus. 2010. Verkkodokumentti. <http://www.finlex.fi/fi/laki/ajantasa/2010/20100681>. Luettu 13.9.2013.

5 Valtiovarainministeriö. 2010. Tietoturva-asetuksen ohje. Helsinki: Edita Prima Oy

6 Valtiovarainministeriö. 2010. Sisäverkko-ohje. Helsinki: Edita Prima Oy

7 Ethernet Automatic Protection Switching (EAPS). 2011. Verkkodokumentti. <http://datatracker.ietf.org/doc/draft-shah-extreme-rfc3619bis/?include_text=1>. Luettu 30.9.2013.

8 EAPS-esite. 2013. Verkkodokumentti. <https://www.extremenetworks.com/libraries/whitepapers/WEAPS_1293.pdf>. Luettu 14.9.2013.

9 Forwarding information base. 2013. Verkkodokumentti. <http://en.wikipedia.org/wiki/Forwarding_table>. Luettu 14.9.2013.

10 Virtual Router Redundancy Protocol (VRRP). 2010. Verkkodokumentti. <http://www.rfc-editor.org/rfc/rfc5798.txt>. Luettu 15.11.2013.

11 Media Access Control Address. 2013. Verkkodokumentti. <http://en.wikipedia.org/wiki/MAC_Address>. Luettu 14.9.2013.

12 IEEE 802.1X Port Based Authentication. 2013. Verkkodokumentti. <http://en.wikipedia.org/wiki/IEEE_802.1X>. Luettu 14.9.2013.

13 RADIUS. 2013. Verkkodokumentti. <http://en.wikipedia.org/wiki/RADIUS>. Luettu 14.9.2013.

14 FreeRADIUS. 2013. Verkkodokumentti. <http://www.freefradius.org>. Luettu 14.9.2013.

15 EXOS Concepts Guide. 2013. Verkkodokumentti. <http://www.extremenetworks.com/libraries/techpubs/EXOS_All/downloads/EXOS_Concepts_Guide_15_3_2.pdf>. Luettu 1.11.2013.

16 EXOS Command Reference Guide. 2013. Verkkodokumentti. <http://www.extremenetworks.com/libraries/techpubs/EXOS_All/downloads/EXOS_Command_Reference_Guide_15_3_2.pdf>. Luettu 1.11.2013.

17 Spanning Tree -protokolla. 2013. Verkkodokumentti. <http://en.wikipedia.org/wiki/Spanning_Tree_Protocol>. Luettu 14.9.2013.

18 IEEE 802.1d Spanning Tree Protocol. 2004. Verkkodokumentti. <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>. Luettu 11.10.2013.

19 IEEE 802.1i Wi-Fi Protected Access. 2013. Verkkodokumentti. <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>. Luettu 15.9.2013.

20 OpenWRT-projekti. 2013. Verkkodokumentti. <http://www.openwrt.org>. Luettu 12.10.2013.

21 TP-LINK WDR4300 –tukiasema. 2013. Verkkodokumentti. <http://www.tplink.com/en/products/details/?categoryid=2166&model=TL-WDR4300>. Luettu 15.11.2013.

22 OpenWRT:n wikisivu TP-LINK WDR4300 –tukiasemasta. 2013. Verkkodokumentti. <http://wiki.openwrt.org/toh/tp-link/tl-wdr4300>. Luettu 15.11.2013.

FreeRADIUS-palvelimen asetustiedostot

Tiedosto: raddb/policy.conf

```
rewrite_calling_station_id {
        if (Calling-Station-Id =~ /([0-9a-f]{2})[-:]?([0-9a-f]{2})[-
:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-f]{2})[-:]?([0-9a-
f]{2})/i){
                update request {
                        Calling-Station-Id := "%{tolower:%{1}-%{2}-
%{3}-%{4}-%{5}-%{6}}"
                }
        }
        else {
                noop
        }
}
```

Tiedosto: raddb/modules/file

```
files authorized_macs {
        key = "%{Calling-Station-ID}"

        usersfile = ${confdir}/authorized_macs

        compat = no
}
```

Tiedosto: raddb/authorized_macs

```
00-11-22-33-44-55
  Reply-Message = "%{Calling-Station-Id} authorized for network ac-
cess"
```

Tiedosto: raddb/site-available/default

```
authorize {
        preprocess
        # Uudelleen kirjoitetaan MAC-osoitteet
        rewrite_calling_station_id
        # Tarkistetaan MAC-osoitteet
        authorized_macs

        if (!ok) {
                reject
        }
        else {
```

```
        # MAC OK
                update control {
                        Auth-Type := Accept
                }
        }
}
```