

Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Jukka Lampikoski

**TURUN
AMMATTIKORKEAKOULUN
LEMMINKÄISENKADUN
TOIMIPISTEEN
LABORATORIOVERKON
KEHITYS**



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

Toukokuu 2014 | Sivumäärä 31

Esko Vainikka

Jukka Lampikoski

TURUN AMMATTIKORKEAKOULUN LEMMINKÄISENKADUN TOIMIPISTEEN LABORATORIOVERKON KEHITYS

Opinnäytetyön tavoitteena on kehittää Lemminkäisenkadun toimipisteen tietojenkäsittelyn laboratorioverkkoa vastaamaan paremmin nykyistä tarvetta.

Työ jakautuu niin, että ensin käsitellään tietoverkon suunnittelun vaiheita ja ylläpitoa. Tämän jälkeen esitellään verkossa käytettyjä aktiivilaitteita, palvelimia, kaapelointia, nykyistä verkon tilaa ja siihen suunniteltuja muutoksia. Kolmannessa vaiheessa toteutetaan laboratorioverkko niin, että se vastaa suunniteltua rakennetta ja toteutetaan muutkin verkkoympäristöön suunnitellut parannukset ja hankinnat, sekä luodaan ja päivitetään verkon ylläpidossa tarvittavat dokumentit. Lopuksi kerrotaan yleisesti tietoverkon elinkaarimallista ja verkon hallitsemisesta ja seurannasta.

Kehitystyö saatiin toteutettua lähes täysin suunnitelmien pohjalta. Kehityksen jälkeen laboratorioverkko vastaa tarvetta useamman vuoden, ainakin siihen asti kunnes 10 gigabitin yhteydet alkavat yleistyä tai niitä aletaan vaatia.

ASIASANAT:

Dokumentointi, lähiverkko, palomuri, verkon suunnittelu, verkon kehitys

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

May 2014 | 31 pages

Esko Vainikka

Jukka Lampikoski

DEVELOPING LABORATORY NETWORK AT TURKU UNIVERSITY OF APPLIED SCIENCES, LEMMINKÄISENKATU

The aim of this thesis is to develop Turku University of Applied Sciences' laboratory network in Lemminkäisenkatu campus to meet requirements of current need.

The thesis is divided to three bigger chapters, which first describes the common phases of maintaining and designing a network. The next part of thesis presents active components, servers, cabling, current status and planned modifications for a network. The last part implements the planned changes to the laboratory network, as well creates and upgrades documents to perform network maintenance easier and shortly presents principles of good documentation and basics how to maintain the network.

Development was taken place at summer 2013. The new network will match the needs for several years, at least until 10 Gigabit networks start to be more common and are demanded.

KEYWORDS:

Documentation, internal network, firewall, network design, network development.

SISÄLTÖ

KÄYTETYT LYHENTEET	6
1 JOHDANTO	7
2 TIETOVERKON SUUNNITTELU	8
2.1 Esitutkimus	8
2.2 Määrittely	9
2.3 Suunnittelu	9
2.4 Rakenteen suunnittelu	10
2.5 Toteutus	10
2.6 Testaus	11
2.7 Verkon ylläpito	11
2.8 Dokumentointi	11
3 VERKON AKTIIVILAITTEET JA KAAPELIT	13
3.1 Kytkimet	13
3.2 Reitittimet	14
3.3 Palvelimet	15
3.4 Kaapelit	15
4 LABORATORIOVERKKO	17
4.1 Liikenteen priorisointi (Quality of Service)	17
4.2 Virtuaaliset lähiverkot (VLAN)	17
4.3 Nimipalvelut (DNS)	18
4.4 IP-osoitteet	18
4.5 Osoitteenmuuntaja (NAT)	19
4.6 DHCP-palvelu	19
4.7 MAC-osoite	19
4.8 Verkon seuranta	20
4.9 Verkon ylläpito ja huolto	20
5 YHTEENVETO JA JATKOKEHITYSKOHTTEET	22
LÄHTEET	24

LIITTEET (SALATTU)

- Liite 1. Looginen verkkokuva
- Liite 2. Fyysinen verkkokuva
- Liite 3. B155-labraluokka
- Liite 4. Looginen verkkorakenne
- Liite 5. Fyysinen verkkorakenne
- Liite 6. Palvelinhuoneen rakkikaappi
- Liite 7. Laboratorioluokan rakkikaappi

TAULUKOT

Taulukko 1. HP Procurve -kytkimet	14
Taulukko 2. Kaapeliluokat	16

KÄYTETYT LYHENTEET

Alla lueteltu tähän työhön liittyviä termejä ja lyhenteitä selityksineen.

Lyhenne	Selitys
CARP	Reitittimien kahdennusprotokolla, jolla voidaan varmentaa reitittimen toimintaa käyttämällä kahden reitittimen välissä virtuaalista IP-osoitetta.
DHCP	Verkkoprotokolla, jonka tehtävä on jakaa IP-osoitteita tietystä osoiteavaruudesta uusille lähiverkkoon liitetyille laitteille.
DNS	Internetin nimipalvelujärjestelmä, joka muuttaa verkkotunnukset IP-osoitteiksi.
Ethernet	Paketteihin perustuva lähiverkkotekniikka, joka on laajassa ja yleisessä käytössä.
IEEE	Järjestö, joka määrittää tietoliikennealan keskeisiä standardeja.
NAT	NATin avulla lähiverkon yksityiset IP-osoitteet muunnetaan julkisiksi IP-osoitteiksi.
Protokolla	Standardi, joka määrittää ja mahdollistaa laitteiden ja ohjelmistojen väliset yhteydet.
SNMP	Verkon hallinnassa käytettävä tietoliikenneprotokolla, jonka avulla voi kysellä verkossa olevan laitteen tilaa.
VLAN	Tekniikka, jolla voidaan jakaa tietoliikenneverkko loogisiin osiin.
VPN	VPN:llä voi luoda loogisia verkkoja eri toimipisteiden välille.

1 JOHDANTO

Opinnäytetyön tavoitteena oli suunnitella ja päivittää Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteen laboratorioverkko ajan tasalle ja luoda siitä selkeät ylläpitoa helpottavat dokumentit sekä verkkokuvat. Suunnittelu aloitettiin haastattelemalla laboratorioverkon ylläpitäjiltä verkon nykytilanteesta ja selvittämällä minkälainen verkon haluttaisiin jatkossa olevan, sekä selvitettiin minkälaista dokumentaatiota verkosta on valmiiksi saatavilla. Seuraavaksi suunnittelua vietiin eteenpäin verkon suunnitteluohjeistuksen mukaisesti niin, että kaikki haastatteluissa ilmenneet ja ennalta määritellyt ominaisuudet, kuten VLAN-verkot sekä tarvittava tietoturva otetaan huomioon.

Pohjana dokumentoinnissa käytettiin uusinta ajan tasalla olevaa tietoa Joonas Rantaperen opinnäytetyöstä Turun ammattikorkeakoulun Lemminkäisenkadun toimipisteen laboratorioverkon dokumentointi (Rantapere 2012), sekä muuta tietoa, jota verkon rakenteesta oli saatavilla ylläpitäjiltä.

Kehitysprojekti oli aiheena mielenkiintoinen ja haastava, koska laboratorioverkosta ei ollut etukäteen paljon dokumentteja olemassa ja verkon täysimittaiseen kehitykseen voitiin soveltaa osaamista usealta eri osa-alueelta fyysisestä kaapeloinnista aina yksittäisten palvelinten konfigurointiin.

Laboratorioverkon muutokset toteuttiin kesän aikana, jolloin päivitystyöt eivät häirinneet toteutettavaa opetusta, sekä verkon testaukseen jäi runsaasti aikaa. Toimiva laboratorioverkko ja sen ylläpitäminen jatkossa jäi verkkovastaavalle, jonka on mahdollista jatkokehittää laboratorioverkkoa ajantasaisten dokumenttien pohjalta.

2 TIETOVERKON SUUNNITTELU

Suunnittelussa tulee ottaa huomioon OSI-mallin kaikki kerrokset fyysisistä laitteista ja kaapeloinnista aina sovelluskerrokselle asti. Verkkoinfrastruktuurin päivittäminen kannatti paloitella siltä osin kuin se oli mahdollista, jotta voitiin uudistaa verkkoa osio kerrallaan.

Suunnittelua toteutetaan yleensä useammassa vaiheessa, joita voidaan tarpeen mukaan työstää myös rinnakkain:

- Esitutkimus
- Määrittely
- Suunnittelu
- Toteutus
- Testaus
- Ylläpito.

Suunnittelun vaiheista on tehtävä hyvä dokumentaatio, jotta verkkoa voidaan ylläpitää ja kehittää myös jatkossa (Hakala & Vainio 2005, 406).

2.1 Esitutkimus

Verkkoa harvoin pääsee suunnittelemaan täysin tyhjältä pohjalta. Tässäkin tapauksessa suunnittelua ja päivitystä tehtiin vanhan, jo osittain vanhentuneeseen dokumentaatioon perustuen. Vanhan tietoverkon toimintaa ei saa keskeyttää pitkäksi aikaa kerrallaan, joten päivitysprojektia viedään eteenpäin vaiheittain (Huhtanen 2008).

Esitutkimus on selvitys siitä miksi ja miten nykyinen verkko toimii ja mitä verkossa voi särkyä projektin edetessä. Esitutkimuksessa selvitetään vähintään käytössä olevat IP-alueet, VLANit, laitteet, ohjelmistot sekä mitä niillä tehdään.

2.2 Määrittely

Kun verkkoa määritellään, on hyvä selvittää, mihin käyttöön verkkoa ollaan toteuttamassa ja kuinka pitkälle verkon suunnittelussa mennään, jotta vaatimukset voitaisiin määritellä mahdollisimman tarkasti (Jaakohuhta 2005, 275 – 283).

Tämän projektin puitteissa määrittely rajataan laboratorioverkon sekä reitittimen uusimiseen niin, että saadaan käyttöön tarpeellisia ominaisuuksia, joista esimerkkinä VLANit.

Määrittelyssä selvitetään myös tarpeet kuten verkon nopeus, suorituskyky, turvallisuus ja käytettävyys. Lisäksi selvitetään, tarvitseeko uutta verkkoa testata ennen käyttöönottoa ja selvitetään, voiko uudistuksen ottaa käyttöön kertamuutoksena vai vaiheittain.

2.3 Suunnittelu

Suunnitteluvaiheessa pyritään löytämään ratkaisuja, joilla voitaisiin toteuttaa kaikki määritellyt tarpeet. Aina se ei ole kuitenkaan mahdollista ja kriteerit voivat olla ristiriidassa keskenään. Suunnitteluvaiheessa mietitään, mikä on paras kustannus-hyötysuhde ja mitkä ominaisuudet määrittelyn pohjalta ovat taloudellisesti järkevää toteuttaa. (Hakala & Vainio 2005, 409-410.)

Suunnittelussa huomioon otettavia asioita olivat:

- Miten laitteet sijoitetaan loogisesti ja fyysisesti sekä mitä teknologioita ja kaapelointeja käytetään?
- Miten verkkoa voitaisiin kehittää ja laajentaa tulevaisuudessa?
- Mitä erillisiä verkkopalveluita tarvitaan ja mitä voidaan yhdistää samoihin laitteisiin?
- Miten verkkoa hallitaan ja miten laitteet toimivat yhteen keskenään?

2.4 Rakenteen suunnittelu

Loogista rakennetta suunniteltaessa selvitetään, minkälaisia IP-verkkoja käytetään ja mitä varten.

Myös seuraavanlaisia kysymyksiä voitiin esittää tehtäessä loogisen rakenteen dokumentointia:

- Miten estetään, että verkon rakenne ei tulisi liian laajaksi ja niin että se olisi jatkossakin hallittavissa?
- Onko käytössä NAT vai käytetäänkö julkisia IP-osoitteita?
- Mitä IP-verkkoja liitetään mihinkin VLANiin?
- Mihin verkkoliitännöihin mitkäkin IP-verkot ja VLANit liittyvät?

Verkon fyysinen rakenne on havainnollistus siitä, mitkä kaapelit menevät minnekin, ja mikä on verkkolaitteiden sijainti. Rakenteeseen merkitään myös onko käytössä valokuitu vai parikaapeli.

2.5 Toteutus

Kun verkkoa toteutetaan, pyritään se tekemään ensisijaisesti suunniteltujen dokumenttien pohjalta. Aina verkkoja ei pystytä toteuttamaan täysin sillä tavalla kuin on suunniteltu. Tämän takia verkon toimivuutta pitää aina testata muutosten jälkeen.

Laboratorioverkon toteutusvaiheessa opiskelijat olivat kesälomalla, joten erillistä tiedotetta käyttäjille ei tarvittu, vaan muutokset voitiin toteuttaa ja testata ilman erillistä ilmoitusta.

Toteutusvaiheessa pidettiin auki mahdollisuutta palata vanhaan järjestelmään sen varalta, että kaikkea tarpeellista ei oltukkaan huomioitu.

2.6 Testaus

Uutta laboratorioverkkoa testattiin niin, että ensin asennettiin aktiivilaitteet sekä kaapelit suunnitelman mukaisesti ja määritettiin laboratorioverkon kytkimille VLAN-asetukset. Uusi reititin-palomuuuri asennettiin kiinni vanhaan reitittimeen, jotta voitiin testata päivitysten vaikutusta ja VLAN-määritysten toimivuutta. Testauksen jälkeen uudella reitittimellä korvattiin jo olemassa oleva vanhentunut reititin ja testattiin päivitetyin reitittimen läpi kulkevien muidenkin verkkojen toimivuutta.

Verkkoa voitaisiin testata tekemällä verkossa liikenne- ja kuormitusanalyysyjä niin, että verkkoa kuormitettaisiin käsin vastaamaan ruuhkakäyttöä vastaavaa liikennemäärää. Kuormituksen aikana seurattaisiin, kestäisivätkö kaikki laitteet niille määritellyn kuorman ja paljonko virheitä verkossa ilmenisi. (Hakala & Vainio 2005, 410-411.)

2.7 Verkon ylläpito

Usein vanhatkin tietoverkot on alkujaan hyvin suunniteltu ja luotu tämän kaltainen dokumentaatio, jotta verkko olisi ylläpidettävissä. Tämän jälkeen verkkoon on tuotu uusia elementtejä yksi kerrallaan sekä tehty ongelmia kiertäviä "asennuksia", joita ei ole päivitetty alkuperäiseen dokumentaatioon. Tästä syystä verkon dokumentaation päivittäminen tulisi pitää mahdollisimman yksinkertaisena, jotta sitä myös tulisi päivitettyä, kun muutoksia tehdään. Yksi hyvä tapa tähän ovat erilaiset Wiki-ohjelmistot, joihin voitaisiin antaa oikeudet verkon ylläpitäjille.

2.8 Dokumentointi

Dokumentoinnilla tarkoitetaan sellaisia ajan tasalla olevia fyysisiä tai digitaalisia asiakirjoja, joissa on kuvattu tietoverkon rakenne ja sen komponenttien toiminta. Dokumentointi tulee antaa jonkun tai joidenkin henkilöiden hallittavaksi.

Dokumentoinnilla esimerkiksi vikaselvitykset lyhentyvät ja verkon suunnittelu helpottuu. (Jaakohuhta 2005, 325.)

Hyvä dokumentaatio on edellytys toimivalle verkonhallinnalle ja ylläpidolle. Dokumentaatiolla saadaan tarkka tieto verkossa olevista laitteista, kuten mikä on niiden fyysinen ja looginen sijainti. (Jaakohuhta 2005, 325.)

Keskeisimmät verkon toiminnan kannalta tärkeät komponentit on hyvä olla dokumentoituina mahdollisia vikatilanteita silmällä pitäen. Näitä komponentteja ovat:

- Kaapelointi ja liitännät
- Jakamot
- Verkon aktiivilaitteet
- Laitteiden asetukset
- Palvelimet
- Varmistusmenetelmät
- VLANit.

3 VERKON AKTIIVILAITTEET JA KAAPELIT

Laboratorioverkon aktiivilaitteita ovat esimerkiksi siihen kuuluvat tietokoneet, palvelimet, kytkimet sekä reitittimet. Riittävien ominaisuuksien valinta kaikkiin käytössä oleviin laitteisiin oli hyvä ottaa huomioon. Laboratorioverkkoa toteutettaessa oli hyvä huomioida jo olemassa olevat laitteet, jotta hankintojen kustannukset voitaisiin pitää mahdollisimman pieninä.

3.1 Kytkimet

Nykyiset lähiverkot ovat yleensä rakenteeltaan tähtimuodossa, jossa kytkin on asetettu verkon keskelle. Lähiverkossa olevat koneet ja laitteet liitetään suoraan kytkimeen, joka hoitaa kaiken liikenteen suoraan lähettämisen ja vastaanottamisen. Verkkoon kytketyt laitteet keskustelevat vain kytkimen kanssa ja näin ollen pakettien törmäyksiä ei tapahdu. (Hakala & Vainio 2005, 85.)

Turun ammattikorkeakoulun laboratorioverkossa käytetään HP ProCurve-kytkimiä, joista käytössä oli mallit 2530-48G, 2626, 2810-24G, 2824 sekä modulaarinen 5304XL (Taulukko 1). Kaikki nämä tukivat verkon rakenteelle tärkeitä protokollia kuten VLAN, Port Trunking ja Quality of Service. Kytkimiä verkossa oli lähtötilanteen mukaan kahdeksan kappaletta, mutta suurimmassa osassa näistä oli kytkettynä vain muutama kaapeli. Poistettiin mahdollisimman monta kytkintä, joilla ei ollut funktiota verkon toimivuuden kannalta. Lisäksi otettiin käyttöön erillinen palvelinkytkin, joka käsittelee palvelinten välisen liikenteen sekä liikenteen keskuskytkimelle. Välillä käytössä on opetustarkoituksessa myös Ciscon 3500XL kytkimiä, jotka on liitetty laboratorioluokan pääkytkimeen (Rantapere 2012, 30-32).

Koska verkko on rakenteeltaan tähti, ei spanning treen hyödyntäminen ole tarpeellista. Spanning tree -protokollalla voitaisiin tarvittaessa toteuttaa varayhteyksiä aktiivilaitteiden välille.

Taulukko 1. HP Procurve -kytkimet

Kytkintyyppi	2530-48G	2626	2810-24G	2824	5304XL
Porttimäärä	48x 1 Gb	24x 100 Mb	20x 1 Gb	20x 1 Gb	48x 100 Mb 4x 1 Gb
Kompoportit	4x	2x	4x	4x	4x
Koko (19")	1U	1U	1U	1U	3U
Kapasiteetti	18.3 Gbps	9.6 Gbps	48 Gbps	48 Gbps	38.4 Gbps

3.2 Reitittimet

Reittimen tehtävänä on yhdistää verkkoja toisiinsa. Reititin luo ARP-taulun, josta se saa selville käytössä olevat portit, joita voidaan käyttää kehyksien käsittelyyn. Reititin käyttää ulkoisia ja sisäisiä reititysprotokollia tiedonsiirtoon. Sisäiset protokollat hoitavat lähiverkon sisäisen liikenteen ja ulkoiset protokollat hoitavat internetiin päin toimivien verkkojen välisen liikenteen.

Laboratorioverkossa oli käytössä kaksi reititintä. Gnatbox, joka hoiti palomuurin ja reitityksen tehtäviä, sekä reunareititin, joka yhdisti laboratorioverkon Funetiin. Nämä molemmat korvattiin PfSense-reitittimellä, joka tukee määrittelyssä ilmenneitä tarpeita, kuten VLANeja. Molemmat reitittimet korvattiin yhdellä laitteella, jotta verkon vianetsintä ja hallitseminen yksinkertaistuu ja verkon ylläpitoa voidaan hoitaa yhdestä paikasta.

PfSense-reititin asennettiin ensin Vmware-alustalle, mutta Vmwaren hankaluuksien takia päätettiin se kuitenkin asentaa suoraan fyysiselle palvelimelle. Ongelmaksi tuli Vmwaren hallintamahdollisuuksien puuttuminen, jos verkko ei ole käytettävissä. Vmwaren hallitseminen vaatii aina erillistä asiakasohjelmaa, joten jo pelkästään konsoliin asti pääseminen oli suuren työn takana, ja useampien verkkokorttien virtualisointi reitittimelle asti oli hankalaa. Asentamalla PfSense suoraan fyysiseen laitteeseen saadaan käyttöön

virtualisoimattomat verkkokortit sekä suora konsolilyhteys helpottamaan reitittimen ylläpitoa.

3.3 Palvelimet

Verkossa oli suunnitteluhetkellä kuusi palvelinta, joista osa oli vanhempaa 32-bit-mallia, joissa on oltava ajossa vanhentunut Wmware-versio. Verkossa on myös erillinen verkkotallennuslaite varmuuskopiontia varten (NAS). Palvelimet hyödyntävät RAID-tekniikkaa, joka parantaa vikasietoisuutta huomattavasti.

Palvelimilla on ajossa koulun opetuskäytössä hyödynnettäviä virtuaalipalvelimia, joista esimerkkinä Stonesoft-, Active Directory-, INFO-TV-palvelin sekä verkon yleiseen käyttöön tarkoitettuja palveluita kuten DNS- ja DHCP-palvelut. Edellämainitut yleiset palvelut siirrettiin PfSensen hoidettavaksi.

3.4 Kaapelit

Kaapelityyppeinä oli käytössä parikaapelia koneiden ja kytkinten välillä, sekä optista kuitua joidenkin kytkinten väliseen liikenteeseen. Kuitua käytettiin siksi, että verkon kapasiteetti saatiin mahdollisimman suureksi ja turha hidastelu vältettyä.

Parikaapeli

Parikaapeli on yleinen kaapelityyppi, joka perustuu ympärikerettyihin johdinpareihin, jotka on kiedottu toistensa ympäri. Kiertämisellä estetään tehokkaasti häiriöiden pääsy johtimeen. (Parikaapeli 2013.)

Parikaapelit on laatuluokiteltu siten, että mitä parempi laatuluokka, sitä suurempi tiedonsiirtonopeus saavutetaan huonoissakin sähköisissä olosuhteissa. Maksimipituus kaikissa kaapeliluokissa on 100 metriä. (i&i Solutions 2006.)

Yleisimmät Suomessa nykyään käytössä olevat kaapelit ovat kategorialtaan Cat 6, joka soveltuu yhden gigabitin yhteyksiin, mutta koulussa on vielä suurimmassa osassa laitteita käytössä Cat 5e -kaapeliluokka.

Taulukko 2. Kaapeliluokat.

Luokka	Standardinopeus
Cat 5	100 Mbps
Cat 5e	1 Gbps
Cat 6	1 Gbps
Cat 7	10 Gbps
Cat 8	10 Gbps

Optinen kuitu

Runkoverkkoyhteyksissä ja nopeutta vaativissa lähiverkoissa valokuitu yleistyy kaiken aikaa. Kuitukaapeleita on kahta tyyppiä: yksimuotokuitu sekä monimuotokuitu. Yksimuotokuitu on kallis ja tarkoitettu fyysisesti pitkille yhteyksille. Monimuotokuitua käytetään lyhyemmällä matkoilla ja lähiverkoissa, ja se on usein tyyppiä 62,5/125 µm, jossa 62,5 merkitsee ytimen halkaisijaa ja 125 vaipan halkaisijaa mikrometreinä. Yhteen kaapeliin voidaan tuoda useita kuituja. (Jaakohuhta 2005, 251-253)

Toisin kuin parikaapeleissa, vanhemmissa kuiduissa data liikkuu vain yhteen suuntaan kaapelissa, ja tästä syystä kuituverkkokortissa on kaksi liittintä, toinen sisäänpäin tulevalle datalle ja toinen lähtevälle datalle. Uusimmissa kuiduissa on mahdollista kuljettaa paketteja molempiin suuntiin samassa kaapelissa. Kuiduille on useita eri liittimiä, mutta yleisimmin käytössä ovat SC ja MT-RJ, joissa yhdessä liittimessä on molempiin suuntiin liittäntä. (Jaakohuhta 2005, 251-253)

4 LABORATORIOVERKKO

Seuraavassa on lueteltuina uuteen laboratorioverkkoon käyttöön otettuja ominaisuuksia ja niiden tarkoituksia.

4.1 Liikenteen priorisointi (Quality of Service)

Priorisoinnilla tarkoitetaan verkon ruuhkatilanteiden käsittelyä hallitusti. Jos kytkimeen tulee enemmän paketteja kuin se pystyy edelleen lähettämään, syntyy tilanne, jolloin kytkin pudottaa pois ethernet-kehysä, joita se ei ehdi välittämään eteenpäin tai joita vastaanottava laite ei pysty käsittelemään. Liikenteen priorisointi onkin lista, jossa määritetään mitä kehysä ensisijaisesti välitetään. Priorisointi on käytössä vain, kun verkko on ruuhkautunut ja normaalitilanteessa kaikilla prioriteeteilla voi saada täyden kapasiteetin verkon liikenteestä.

4.2 Virtuaaliset lähiverkot (VLAN)

Laboratorioverkon kehityksen määrittelyvaiheessa todettiin, että käyttöön halutaan VLANit, joilla halutaan erottaa eri osastot toisistaan ja työasemat palvelimista. Lisäksi haluttiin erottaa hallintaverkot normaaleista verkoista.

Nykyaikaisissa verkoissa on mahdollisuus käyttää VLANeja virtuaaliverkkojen määrittämiseen. Ryhmittely voidaan tehdä joko MAC-osoitteen, kytkimen portin, IP-osoitteen tai tietoliikenneprotokollan perusteella.

Helpoin tapa on kytkimen portteihin perustuvat VLAN-määritykset. Kytkimen portteihin voidaan määrittää, mihin VLANeihin ne kuuluvat, esimerkiksi

VLAN1, portit 1-11 ja VLAN2, portit 12-24.

Tällöin portit 1-11 muodostavat oman verkkonsa ja voivat kommunikoida keskenään. Vastaavasti portit 12-24 kuuluvat omaan verkkoonsa ja kommunikoivat keskenään.

Virtuaalisia verkkoja voidaan määrittää useampia samoihin portteihin, jos käytetään pakettien merkitsemistä (tagging), jotta tiedetään, mihin VLANiin paketti pitää ohjata.

Laitteisiin ei voida merkitä kuin yksi oletus-VLAN merkitsemättömänä yhteen tiettyyn porttiin. Merkittyjä VLAN-verkkoja voi olla useita.

Laboratorioverkon aktiivilaitteille, palvelimille ja luokkien koneille on asetettu erillisen suunnitelman mukaisesti VLAN-määriykset. Keskeistä osaa verkkoinfrastruktuurista ajetaan Vmware-alustalla ja sen rajoituksista johtuen verkkoliitännöiden määrä rajoittuu kymmeneen. Liitännöiden määrä rajoittaa myös käytössä olevien VLANien määrän, koska VMware ei mahdollista kuin yhden VLANin käyttämistä jokaisessa virtuaalisessa liitännässä.

4.3 Nimipalvelut (DNS)

DNS-palvelulla voidaan ylläpitää tietoa IP-osoitteista ja laitteiden nimistä sekä tehdä tiettyjen nimien osoituksia tiettyihin IP-osoitteisiin, esimerkiksi

ping.funet.fi IN A 128.214.248.132.

Laboratorioverkossa olevat nimipalvelimet korvattiin Windows palvelimilla, joissa on ajossa myös Active-Directory. DNS-palvelin voitaisiin toteuttaa myös miltei millä tahansa käyttöjärjestelmällä asentamalla siihen soveltuva ohjelmisto.

4.4 IP-osoitteet

Jokaisella verkossa toimivalla laitteella on oltava jokin yksilöllinen osoite, joka yksilöi laitteen muista verkon laitteista. IP-osoite (IPv4) kirjoitetaan neljänä

lukuna, jotka ovat arvoltaan 0-255 ja niitä erottelee piste, esimerkiksi 192.168.1.2.

Koneilla voi olla staattinen IP-osoite, joka pysyy aina samana. Osoitetta voidaan pyytää DHCP-palvelimelta väliaikaisesti. Kun kone suljetaan, varattu IP-osoite vapautuu muiden koneiden käytettäväksi. (i&i Solutions 2006.)

Laboratorioverkkoon on varattu vain maskin /29 kokoinen IP-osoiteluokka, joka tarkoittaa kahdeksaa IP-osoitetta, ja niistä käytössä laitteille on kuusi kappaletta koska yksi osoite kuuluu verkon määrittämiseen (Broadcast) ja yksi yhdyskäytävän määrittämiseen (Gateway).

4.5 Osoitteenmuuntaja (NAT)

NAT (Network Address Translation) on tekniikka, jonka avulla lähiverkon yksityiset IP-osoitteet muunnetaan IP-osoitteiksi niin, että lähiverkon osoitteilla pääsee internetiin. Tekniikka parantaa tietoturvaa verkoissa, joista ei ole tarvetta ajaa mitään palveluita ulkoverkkoon. (Jaakohuhta 2005, 196.)

Julkisen verkon osoitteiden puutteen ja myös tietoturvan parantamisen takia laboratorioverkossa käytetään monelta osin NAT-tekniikkaa.

4.6 DHCP-palvelu

DHCP-palvelu (Dynamic Host Configuration Protocol) jakaa verkon laitteille IP-osoitteet ennalta määritellystä IP-osoiteavaruudesta. Yleensä laitteille jaetaan samalla myös muita asetuksia, kuten oletusyhdyskäytävän ja nimipalvelimien tietoja. (DHCP 2014.)

4.7 MAC-osoite

Jokaisella verkkokortilla on oma uniikki MAC-osoite (Media Access Control). Osoitteet verkkorttien valmistajille määrittää ja antaa IEEE. MAC-osoite on 48-

bittinen numerosarja, jossa 24 bittiä määrittää valmistajan ja loput bitit on verkkokortin sarjanumero. MAC-osoite ilmoitetaan yleensä kuutena heksadesimaalilukuna joko väliviivalla tai kaksoispisteellä eroteltuina. (i&i Solutions 2006.), esimerkiksi 00:A0:24:AA:BB:CC tai 00-A0-24-AA-BB-CC

Tätä tietoa tarvitaan, kun määritetään kiinteitä ip-ohjauksia tietyille verkkokorteille DHCP-palvelun avulla.

4.8 Verkon seuranta

Monimutkaisen verkon seurannassa ja ylläpidossa pitää ottaa huomioon verkon seurannan työkalut. Lähtöhetkellä verkossa ei ollut käytössä mitään verkonseurantaohjelmaa. Tämän opinnäytetyön puitteissa verkkoon asennettiin Observium verkonseurantaohjelma, johon voidaan hakea SNMP-protokollaa hyväksi käyttäen tietoja verkkolaitteiden ja palvelinten reaaliaikaisesta tilanteesta sekä kuormituksesta. Observium voidaan konfiguroida ilmoittamaan esimerkiksi sähköpostitse, jos palvelin tai aktiivilaite lopettaa vastaamasta verkossa.

4.9 Verkon ylläpito ja huolto

Verkko elää ja kehittyy aina tarpeen mukaan. Teknologiat vanhentuvat ja laitteet vaihtuvat, mutta niiden on aina tarkoitus toimia lähes samalla lailla verkon käyttäjille.

Verkon käyttäjäkanta ja liikennemäärät muuttuvat jatkuvasti ja aina verkkoon varattu kapasiteetti ei riitä. Laboratorioverkon osalta päivityksen myötä kriittiset komponentit on siirretty 100 megabitin verkosta yhden gigabitin yhteyksiin, ja verkossa on valmius yhteyksien niputtamiseen (port-trunking) sen varalle, että kapasiteettia tarvittaisiin lisää.

Projektin aikana selvisi, että osa koneista voidaan erottaa kokonaan nykyisestä verkosta, joten näitä ei tarvinnut huomioida sen enempää lopullista verkkosuunnitelmaa tehtäessä.

Merkittävin kustannuksiin vaikuttava tekijä on kapasiteetti, jota voidaan hallita fyysisellä liitäntänopeudella ja liitäntänopeuden teknisillä rajoituksilla. Verkon kapasiteettia saadaan hallittua verkon palomuurilla ja solmukohtissa esimerkiksi tietynlaisten palveluiden kapasiteettirajoituksilla. Sähkönkulutuksessa voitaisiin säästää poistamalla konehuoneen vanhemmat palvelimet kokonaan ja niiden sisältö voitaisiin integroida pois fyysisiltä palvelimilta uusiin virtualisoiuihin alustoihin.

Verkon elinkaaren aikana varmistetaan aktiivilaitteiden käyttöiän aikana niiden toiminnan varmuus, sekä niiden käyttöiän päättyessä uudistetaan laitteet hallitusti.

Tietoverkon elinkaaren osalta tulee ottaa huomioon kustannukset sekä verkon ja toiminnan varmuuden tarve. Laboratorioverkon tapauksessa verkon ei tarvitse olla päällä yhtäjaksoisesti, koska tilassa ei ole montaa julkiseen verkkoon vastaavaa palvelinta. Laitteiden käyttöiän päättyessä voidaan laitteet korvata uusilla esimerkiksi iltaisin, kun koululla ei ole opetusta, joten tämän osalta ei kannata maksaa verkon komponenttien varmentamisesta sen hyötyyn nähden.

Laboratorioverkon yhteyskapasiteetiksi riitti tässä vaiheessa 100 megabittiä työasemilta kytkimiin ja kahdennettu yhden gigabin linkki kytkinten väliseen liikenteeseen. Jos kytkinten välinen liikenne saadaan tulevaisuudessa 10 gigabitin portteihin, voitaisiin myös työasemilla hyödyntää yhden gigabitin yhteyksiä.

5 YHTEENVETO JA JATKOKEHITYSKOhteet

Projektin alkaessa vain muutama edellä mainittu tietoverkon dokumentointiin liittyvä asiakirja oli saatavilla. Näiden jo osittain vanhentuneiden dokumenttien pohjalta oli lähdettävä suunnittelemaan uutta laboratorioverkkoa ja dokumentoida se mahdollisimman hyvin. Haastavin tilanne suunnittelussa tuli siitä, että dokumentti, jota käytettiin uuden verkon suunnitteluun, ei ollut ajan tasalla. Verkkoon oli kytketty myöhemmin keskeisessäkin roolissa verkon toimivuuden ja hallinnan kannalta olevia laitteita, joita ei ollut merkitty mihinkään. Ongelmana verkossa oli myös Stonesoft-palvelin, joka kuului oletuksena täysin eri verkkoon sitä hyödyntävän luokan kanssa. Opetuksen alussa piti määrittää asetukset erikseen luokan työpäätteille ja Stonesoft-palvelimeen ja tietoverkkoon yhdistäminen samanaikaisesti ei ollut mahdollista. Uudessa verkkoympäristössä tämä on otettu huomioon niin, että luokat ottavat DHCP:llä oikeanlaiset ip-osoitteet, jotka perustuvat luokkien VLANeihin, jotta esimerkiksi Stonesoft-palvelimen käyttö on mahdollista ilman verkkokorttien uudelleen konfigurointia.

Turun ammattikorkeakoulun Lemminkäisenkadun laboratorioverkko on irrallaan koulun muissa luokissa käytössä olevasta opetusverkosta. Laboratorioverkko keskittyy muutamaan yksittäiseen luokkaan ja palvelintilaan. Verkko on normaalin opetusverkon kanssa rinnan tietoturvan takia, jotta laboratorioverkon oikeuksia voidaan rajoittaa tiettyjen kurssien tarpeiden mukaisesti. Laboratorioverkosta poistettiin kaikki 32-bittiset vanhentuneet palvelimet ja tiivistettiin verkon palveluita vähemmälle laitemäärälle. Kaikki erilliset palvelut, joita olivat esimerkiksi DHCP, DNS ja VPN, yhdistettiin vain muutamaan palvelimeen.

Laboratorioverkko saatiin toteutettua lähes täysin uuden verkkosuunnitelman pohjalta ja verkosta saatiin poistettua useampia vanhentuneita aktiivilaitteita sekä satoja metrejä turhaa verkkokaapelia. Mahdollisia kehityshankkeita, jotka jäivät vielä toteuttamatta tämän opinnäytetyön puitteissa, ovat

- Varmistetaan aktiivilaitteiden käyttöään aikana niiden toiminta (Stacking)
- Asetetaan SNMP päälle kaikkiin kytkimiin ja palvelimiin ja niistä statistiikat keskitetyksi jollekin palvelimelle
- SAN-levypalvelimen hankinta, jotta kaikkien palvelimien data voitaisiin keskittää yhteen paikkaan, mikä mahdollistaisi myös reaaliaikaisesti virtuaaliapalvelimien siirron fyysisesti toiselle palvelimelle esimerkiksi huoltokatkosten tai versiopäivitysten ajaksi
- Otetaan käyttöön IPv6
- Verkkoliikenteen priorisointi ja rajoitukset.

LÄHTEET

DHCP. 2014. Wikipedia. Viitattu 26.01.2014

http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol.

Hakala, M. & Vainio, M. 2005. Tietoverkon rakentaminen. 1. painos. Helsinki: Docendo.

Huhtanen, K. 2008. Verkon suunnittelu. Viitattu 22.05.2013

<http://www.cs.tut.fi/~karrih/material/verkon-suunnittelu-muistiinpanoineen-current.pdf>.

i&i Solutions 2006. Lähiverkon tekniikka. Viitattu 22.5.2013

<http://www.esp.fi/attachments/filebank/19.pdf>.

Jaakohuhta, H. 2005. Lähiverkot – Ethernet. 4. uudistettu painos. Helsinki: Edita Publishing Oy.

Parikaapeli. 2013. Wikipedia. Viitattu 22.5.2013 <http://fi.wikipedia.org/wiki/Parikaapeli>.

Rantapere, J. 2012. Turun Ammattikorkeakoulun Lemminkäisenkadun toimipisteen laboratorioverkon dokumentointi. Opinnäytetyö. Turku: Turun ammattikorkeakoulu.