jamk.fi

Kampusverkon suunnitelma

Harjoitustyö

Joni Korpihalkola
Joonas Mankinen
Niko Poutanen

Yritysverkot
4/2017
Tieto- ja Viestintätekniikka
Tekniikan ala

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Sisällysluettelo

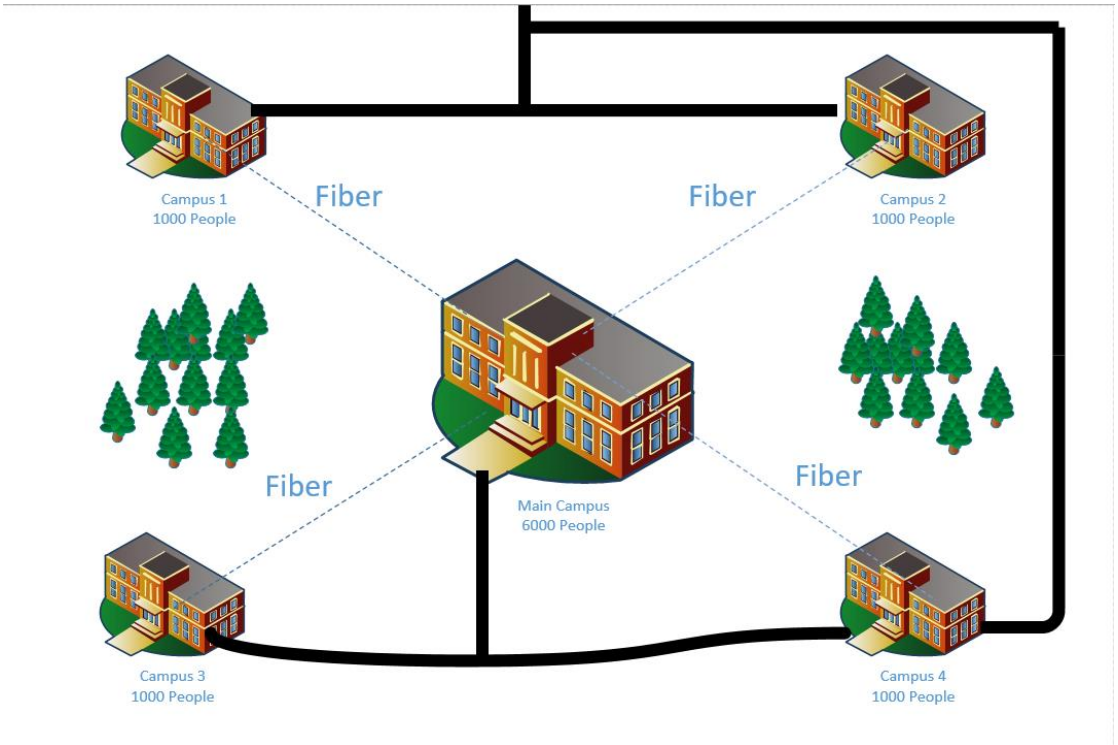
Kuviot

1 Johdanto

Työn tavoitteena on suunnitella korkeakoululle opetus- ja kampusverkko. Korkeakoulun toimipisteinä toimivat korkeakoulun pääkampus ja korkeakoulun neljä pienempää kampusta, jotka kaikki sijaitsevat samassa kaupungissa. Etäisyyttä kampuksien välillä on yli 10 kilometriä.

2 Kampus

Henkilökuntaa ja opiskelijoita pääkampuksella on yhteensä noin 6000 henkilöä. Pienimmillä kampuksilla henkilökuntaa ja opiskelijoita on yhteensä noin 1000 henkilöä jokaisessa. Eli koko verkossa pitäisi saada palvelut toimimaan sujuvasti noin 10000 henkilölle. Yhteytenä kampusten välillä käytetään kaupungilta vuokrattua kuituverkkoa (Kuvio 1).



Kuvio 1. Kampukset ja niiden väliset kuituyhteydet kuvitettuna

3 Palvelut

Kampuksen verkossa tulee olla seuraavat palvelut:

- Keskitetty käyttäjä- ja laitehallinta
- Langattomat verkkopalvelut
- Pilvipalvelut
- Etäyhteydet sisäverkkoon
- Sisäverkon perusinfrasktruktuuri eli DNS- ja DHCP-palvelut

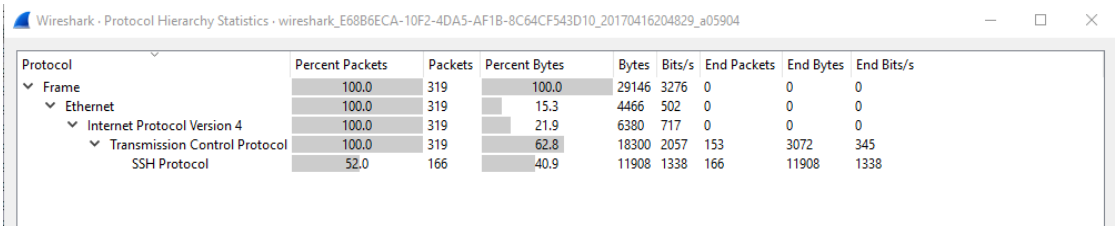
3.1 Palvelujen kaistankäyttö

Windows AD käyttää paljon resursseja aamulla ja luentojen alussa, kun kaikki käyttäjät saattavat kirjautua melkein yhtäaikaisesti sisään profiiliinsa, jolloin profiilin vienti palvelimelta vie kaistaa. Etäyhteydet VPN:n kautta, joka on salattu tunneli, joka aiheuttaa lisäkuormaa verkolle. Palomuuri päärouterin päässä lisää kuormaa.

Windows AD:n authentication packet koko vaihtelee 1-10 MB:n välillä. Windows AD:n asetuksista voisi muuttaa, että käyttäjien profiilien maksimikoko on 20 MB. Tällöin jos ajatellaan, että koneelle kirjautumisessa saisi kulua aikaa maksimissaan 120 sekuntia, ja koneen pitäisi ladata 30 MB:n edestä tietoa, niin jokaiselle sisäänkirjautuvalle koneelle varattaisiin kaistaa 250 KB/s.

Jokaiselle opiskelijalle voitaisiin varata pilvipalveluksi verkkolevy, jonka maksimikoko on 1 GB. Pilvipalveluiden käyttöä on vaikea ennustaa, mutta tiedonsiirron rajaksi voitaisiin määritellä 1 MB/s, jolloin opiskelijat saavat vähän isommatkin tiedostot kohtuullisen nopeasti siirrettyä verkkolevyltä.

SSH etäyhteyden sessiot käyttävät noin 3300 bittiä sekunnissa kaistaa. 10 000 henkilöstä arviolta 5% maksimissaan käyttäisi samaan aikaan etäyhteyden palveluita, joten sille varattaisiin kaistaa 1650 kb/s (Kuvio 2).



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	319	100.0	29146	3276	0	0	0
Ethernet	100.0	319	15.3	4466	502	0	0	0
Internet Protocol Version 4	100.0	319	21.9	6380	717	0	0	0
Transmission Control Protocol	100.0	319	62.8	18300	2057	153	3072	345
SSH Protocol	52.0	166	40.9	11908	1338	166	11908	1338

Kuvio 2. Testi SSH-etäyhteyden pakettien koosta

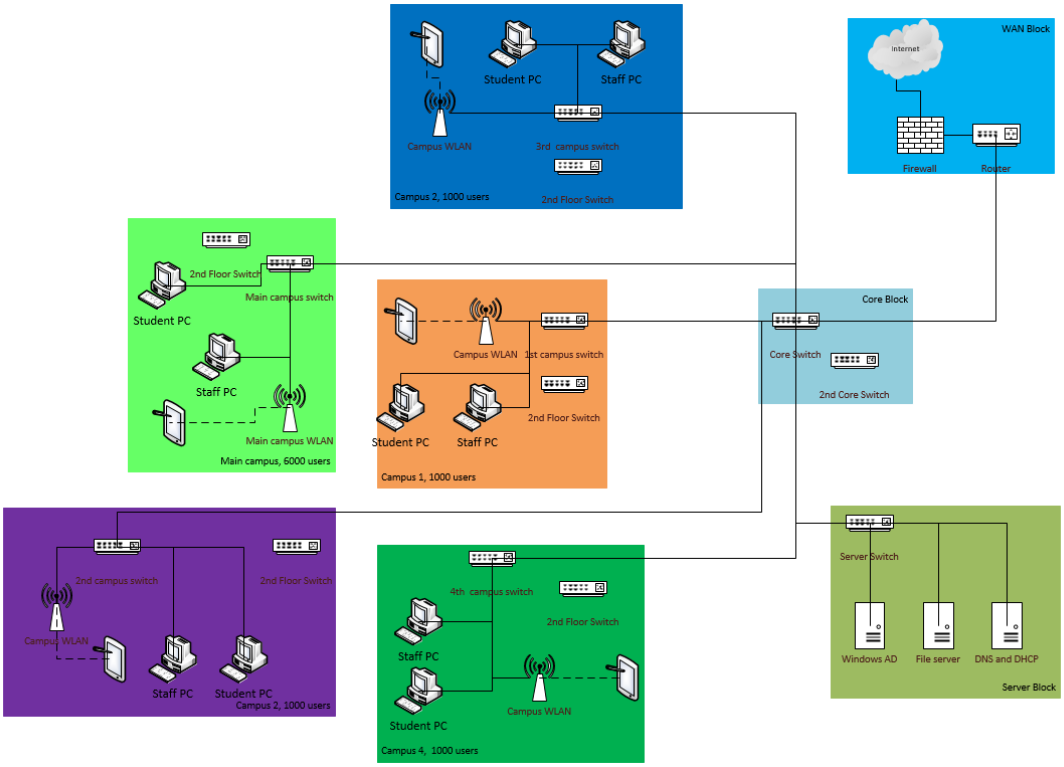
Jokaisella kampuksella on langaton reititin, joka tarjoaa langatonta verkkopalvelua kampuksen rakennukseen. Jotta langaton verkko ei ruuhkautuisi, siihen voisi myös asettaa 100 kB/s tiedonsiirtorajan laitetta kohden. Langaton verkko olisi myös salattu tietoturvan lisäämiseksi, sekä myös ruuhkautumisen estämiseksi. Vieraille voitaisiin jakaa väliaikaiset verkkotunnukset. Opiskelijoille jaetaan omat verkkotunnukset.

Kampuksen verkossa on myös DHCP-palvelin jakamassa IP-osoitteita ja DNS-palvelin. DHCP:ssä asiakkaan ja verkon välillä välitetään neljä pakettia, joiden koon maksimi on yleensä 576 tavua (B). DNS-paketin koko vaihtelee verkon mukaan, keskimääräinen voisi olla 100 tavua. DHCP:n lease ajaksi verkkoon voisi määritellä 30 päivää, jolloin koneet hakevat uuden IP:n noin kerran kuukaudessa. DHCP palvelimen ruuhkautumisen välttämiseksi jokaiselle kampukselle voitaisiin määrittää eri päivä, jona ne päivittävät IP-osoitetiedot DHCP-palvelimelta. Kampuksien sisällä voisi myös koneissa harjoittaa lease-aikojen hajontaa niin, että esimerkiksi puolet kampuksen koneista päivittäisivät IP-osoitteensa eri päivänä kuin toiset. Päivitykset voitaisiin myös ajoittaa viikonlopulle, jolloin ei olisi paljon muita verkon käyttäjiä. Jos DHCP pakettien kooksi sovitaan 576 tavua, niin pääkampuksella 6000 koneet vievät kaistaa IP-osoitteiden päivitykseen 567B*4*6000 = 13,6 MB. Pienemmillä kampuksilla 567B*4*1000= 2,268 MB.

DNS kyselyiden määrä riippuu siitä, käyvätkö opiskelijat sivuilla, joita ei ole tallennettu DNS Cacheen. DNS kyselyiden määräksi voisi arvioida koko kampuksen verkossa 500 per sekunti. Jos kysely ja vastauksen pakettikoko on sama noin 100 tavua, niin DNS kyselyille pitää varata kaistaa 100B*500=50 kB/s.

4 Kampusverkon toteutus

Alla olevassa kuvassa on suunnitelma verkkomme rakenteesta (Kuvio 3).



Kuvio 1. Verkon suunniteltu rakenne

Internetistä tullaan palomuurin läpi reitittimelle, joka ohjaa liikenteen verkon pääkytkimelle, joka jakaa tulevan datan määränpäähänsä. Pääkytkimen päässä on jokaisen muun kampuksen kytkimet, sekä palvelinten kytkin. Jokaisella kampuksella on kaksi kytkintä toimivuuden varmistamiseksi. Kampuksien kytkimen päässä on opiskelijoiden tietokoneet, henkilökunnan tietokoneet sekä langaton tukiasema, joka jakaa kampuksen WLAN verkon, jota opiskelijat, henkilökunta ja vierailijat saavat vapaasti käyttää. Palvelimia varten pääkampuksella on erillinen lukittu huone, jossa fyysiset laitteet sijaitsevat.

4.1 Lohkot

Kampukselle voitaisiin suunnitella ns. Core-lohko, joka koostuisi kahdesta Ciscon 6500 kytkimistä. Core-lohko toimisi kampuksen runkoverkkona, ja kaksi kytkintä lohkossa toisi verkolle vikasietokykyä, jos toinen kytkimistä lakkaisi toimimasta. Kytkimet jakaisivat myös kuormaa, ettei toinen niistä ylirasittuisi liikenteestä. Kaikki liikenne kampusten, palvelimien ja internetin välillä kulkisi Core-lohkon kautta. Core-lohkon tehtävänä on siis siirtää kampuksen tietoliikennettä käyttäen

mahdollisimman vähän prosessointitehoa, maksimoida verkon suoritusteho, tarjota 100% verkon käytettävyyttä ja tehdä verkon laajennuksesta helpompaa. Core-lohkossa multilayer kytkimet myös toimisivat reitittimen tavoin verkossa, jolloin lohkossa voitaisiin soveltaa esimerkiksi OSPF-reititysprotokollaa (Cisco Systems Overview of Campus Network Design).

Jokainen kampus olisi erillisenä Switch-lohkona, jotka ovat yhdistetty suoraan Core-lohkoon. Ne kytkimet, jotka ovat yhdistetty Core-lohkon kytkimiin, jakaisivat verkkoa eri kerrosten kytkimille, josta taas jaettaisiin verkkoa eteenpäin kerrosten tietokoneille. Kytkimien tulisi olla layer 3 kytkimiä.

Palvelimille olisi myös oma lohko, jossa olisi myös layer 3 kytkin, joka on yhdistetty Core-lohkon kytkimeen, kytkettynä kolmelle palvelimelle. Jos palveluja tarvitsisi saada lisää tai tarvitsisi uusia palvelimia ylläpitämään verkon palveluja, niin niitä olisi helppo lisätä.

Reititin, joka on yhdistetty internettiin ja siihen kytketty layer 3 kytkin, voitaisiin nimetä WAN-lohkoksi. Tässä lohkossa olisi myös palomuuri, joka monitoroisi ulosmenevää ja sisääntulevaa liikennettä.

4.2 Osoitteidenjako

Kuvassa verkkomme IP jakelutaulukko (Kuvio 4).

First address	Last Address	Description	Area
10.10.10.0	10.10.10.8	Servut	Server Block
192.168.15.0	192.168.39.255	Main campus	Main campus
192.168.45.0	192.168.49.255	Campus 1	Campus 1
192.168.55.0	192.168.59.255	Campus 2	Campus 2
192.168.65.0	192.168.69.255	Campus 3	Campus 3
192.168.75.0	192.168.79.255	Campus 4	Campus 4
192.168.80.0	192.168.104.255	Main campus WLAN	Main campus WLAN
192.168.110.0	192.168.114.255	Campus 1 WLAN	Campus 1 WLAN
192.168.120.0	192.168.124.255	Campus 2 WLAN	Campus 2 WLAN
192.168.130.0	192.168.134.255	Campus 3 WLAN	Campus 3 WLAN
192.168.140.0	192.168.144.255	Campus 4 WLAN	Campus 4 WLAN

Kuvio 4. Kampuksen osoitetaulu

Palvelimille on varattu osoitteet 10.10.10.0-10.10.10.8. Jokaiselle kampukselle on varattu tietty määrä osoitteita, jotka kattavat kampuksen henkilöstön tarpeet. Taulukosta (Kuvio 4) näkee mitkä IP-osoitteet ovat varattu millekin kampukselle.

Osoitteidenjaossa käytetään omalla palvelimella pyörivää DHCP:tä. Jokaiselle kampukselle ja palvelimille on määrätyt rajat joista saavat IP-osoitteen. Kampuksilla sijaitsevat WLAN verkot saavat myös omat IP-osoitteet DHCP:lta, jotka eivät tule samasta rangesta kun muiden koneiden IP-osoitteet.

4.3 Reititys

Reitityksen käytetään Enhanced Interior Gateway Routing Protocol (EIGRP) – protokollaa. EIGRP:ää käyttävät reitittimet tekevät naapuri- ja topologiataulun. Naapuritauluun on tallennettu IP-osoitteet kaikista reitittimistä, jotka on suoraan kytketty laitteeseen. Topologiataulussa löytyy EIGRP -protokollan määräämät reitit ja niille painoarvot. EIGRP on myös helppo konfiguroida, taulujen jakaminen on nopeaa ja reititys on luokaton. EIGRP reitityksestä on myös helppo päivittää esim. Ipv6-

protokollaan, koska reititys on siitä riippumaton. (Cisco System Deploying A Fully Routed Enterprise Campus Network)

4.4 Verkon vikasietokyky

Kytkimille, jotka ovat tärkeitä koko lohkon toiminnalle ja reitittimille tulisi olla saatavilla varavirtalähteet ja tuulettimet komponenttien hajoamisen varalta. Olisi hyvä pitää myös sellaisia komponentteja varalla, jotka voidaan liittää laitteisiin ilman, että niitä tarvitsee käynnistää uudelleen.

5 Tietoturvallisuus

Mahdollisia tietoturvauhkia, joita kampuksen verkko saattaa kohdata, ovat seuraavia (Design and Implementation of a Secure Campus Network):

- Virus sähköpostin kautta
    - Saattaa altistaa koko verkon leviämällä uhrikoneesta eteenpäin
- Virus, joka pääsee sisään verkkoon avoimien porttien kautta
- Sivustoilta tarttuvat virukset
- Palvelimiin kohdistuva hyökkäys
    - DoS hyökkäys
- Hyökkäys verkon sisältä
    - Esimerkiksi työntekijä
- ARP Spoofing
- Fyysinen murtautuminen palvelimelle
- WLANiin kohdistuvat hyökkäykset

5.1 Uhkien torjuminen

Palomuuri sijaitsee verkossa internetin ja reitittimen välissä, ja kaikki verkkoon tuleva ja siitä lähtevä liikenne kulkee palomuurin läpi. Lisäksi käyttöoikeuksilla rajataan eri henkilöiden pääsyä eri paikkoihin, esimerkiksi palvelimiin ei pääse käsiksi oppilaat. Poislukien jokaiselle käyttäjälle suunnattu oma osuus palvelimen levykapasiteetista, jota voi käyttää etänä. Oppilailla ei ole oikeuksia mennä opettajien, eikä muiden oppilaiden omiin kansioihin, vain omaan kansioon on jokaisella käyttöoikeus. Sama pätee myös opettajiin.

5.1.1 VLAN

Verkon turvallisuutta voidaan parantaa jakamalla verkko Virtual LANeilla pienimmiksi palasiksi riippuen, kuka paketin lähettää. Kampusverkkoon voisi toteuttaa seuraavat VLANit (Kuvio 5).

VLAN ID	VLAN Name
10	Server
50	Admin
150	Staff
200	Student
500	WLAN
600	SSH

Kuvio 5. Kampusverkon VLAN ID:t ja niiden nimet

5.1.2 Palomuuri

Palomuurilla voidaan tutkia sisääntulevaa ja ulosmenevää liikennettä. Palomuuriin voidaan asettaa sääntöjä, joilla estetään pääsy esimerkiksi sivuille, jotka on merkitty haitalliseksi ja estetään myös kampusverkosta tapahtuva muiden verkkojen häiriköinti. Paras palomuuri kampukselle olisi sellainen, joka päivittäisi itseänsä kokoajan uusimmilla uhkasivuilla, joille pääsemisen se sitten myös estäisi. Palomuuri tarvitsee myös säännöt ulkoatulevalle liikenteelle, joka yrittäisi selvittää, mitä portteja palomuurissa on auki ja joka yrittäisi hyökätä niiden kautta kampuksen verkkoon.

Lähteet

Cisco System Deploying A Fully Routed Enterprise Campus Network. 7.5.2005. Viitattu 17.4.2017 https://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns656/net_design_guidance0900aecd804ab689.pdf

Cisco Systems Overview of Campus Network Design. n.d. Viitattu 15.4.2017. https://ftp.utcluj.ro/pub/users/cemil/prc/campus_design_eng1.ppt

Louisiana State University Campus Network Report, 20.6.2013. Viitattu 14.4.2017. http://listserv.educause.edu/scripts/wa.exe?A3=ind13&L=NETMAN&E=base64&P=22557670&B=--_004_C9A89953BAE16C4ABE90F1578296D64D7089001ASN2PRD0610MB372_&T=application%2Foctet-stream;%20name=%22Campus%20Network%20Report%20JAN13-JUN13.pdf%22&N=Campus%20Network%20Report%20JAN13-JUN13.pdf&attachment=q&XSS=3

Mohammed Nadir Bin Ali, Mohamed Emran Hossain, Md. Masud Parvez. Implementation of a Secure Campus Network. 7/2015. Viitattu 18.4.2017.

https://www.researchgate.net/file.PostFileLoader.html?id=5712fea193553b52231b9d74&assetKey=AS%3A351697495969793%401460862625372