TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Madis Võrklaev 175872IDAR

Kohtvõrgu lahendus põhikooli näitel

Diplomitöö

Juhendaja: Edmund Laugasson
MSc

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Madis Võrklaev

15. mai 2021

Annotatsioon

Käesoleva bakalaureusetöö eesmärgiks on ehitada töökindel, turvaline ja lihtsasti hallatav kohtvõrk äsjavalminud koolimajja.

Diplomitöös uuritakse valdkonna parimaid praktikaid ja lahendusi avalikus asutuses kohtvõrgu ehitamiseks. Vaadeldakse nii seadmeid ja nende omadusi kui vajalikke seadistusi, loomaks töökindlat ja turvalist lahendust.

Töö annab ülevaate asutuse vajadustest, omavalitsuse nõuetest ning erinevate praktikute soovitustest. Töö analüüsiosas vaadeldakse organisatsiooni ja hoone vajadusi ning neist tulenevalt valdkonna praktikaid ja lahendusi. Praktilises osas kirjeldatakse analüüsi tulemuste põhjal valminud kohtvõrgu lahendust. Põgusalt vaadatakse ka tulevikusuundasid, pannakse kirja märksõnad, millele toetuda järgmistes samalaadsetes projektides.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 40 leheküljel, 5 peatükki, 7 joonist, 8 tabelit.

Abstract

Solution of a Local Area Network on the Example of a Basic School

This thesis investigates the best practices for buiding a secure and reliable local area network in a 16,000m^2 school building. The author analyzes basic needs for the building and the organisation, defines parameters which the network equipment must meet. For this, documents from ISKE, RIA, HARNO, CISCO, etc are analyzed, as well as some resellers are interviewed. In the practical part the author describes the process and outcome of building the actual network. Also, documenting and logging are brielfy discussed. Some keywords and thoughts are brought out to take into consideration for next projects alike. This document will be further complemented by the author and his team, so this could be a standard for buildng and renewing the networks in other buildings that the municipality manages.

The thesis is in estonian and contains 40 pages of text, 5 chapters, 7 figures, 8 tables.

Lühendite ja mõistete sõnastik

DAC	*Direct attach copper, andmesidekaabel*
DHCP	*Dynamic host configuration protocol*, dünaamiline hostikonfiguratsiooni protokoll
E-ITS	Eesti infoturbestandard
Gbit/s	*Gigabit per second*, gigabitti sekundis
HARNO	Haridus- ja Noorteamet
IDS	*Intrusion detection system*, sissetungi avastamise süsteem
IPS	*Intrusion prevention sysetm*, sissetungi ennetamise süsteem
ISKE	infosüsteemide kolmeastmeline etalonturbe süsteem
ISO OSI	*International organization of Standardization Open System Interconnection*, avatud süsteemide sidumise arhitektuur
MU-MIMO	*Multi-user, multiple input, multiple output*, Wi-Fi tehnoloogia, mis võimaldab teenindada samaaegselt mitme klientseadet
NGFW	*Next generation firewall*, järgmise põlvkonna tulemüür
PIN	*Personal identification code*, isiklik tuvastamisnumber
PoE	*Power over ethernet*, toide üle arvutivõrgu
PXE	*Preboot execution environment*, käivituseelne täitmiskeskkond
RIA	Riigi Infosüsteemi Amet
RRM	*Radio resource management*, dünaamiline saatevõimsuse kohandamine
SFP	*Small form-factor pluggable*,võrguliidese moodul
SNMP	*Simple network management protocol*, lihtne võrguhalduse protokoll
SSID	*Service set identifier*, võrgu nimi Wi-Fi võrgus
U/UTP	*Unshielded twisted pairs*, varjestamata keerdpaarid
UPS	*Uninterruptable power supply*, katkematu toite allikas
VLAN	*Virtual local area network*, virtuaalne kohtvõrk
VOSK	Võta oma seade kaasa
WPA	*Wi-Fi Protected Access*, andmeturbe protokoll
VPN	*Virtual private network*, virtuaalne privaatvõrk

Sisukord

Autorideklaratsioon 2
Annotatsioon 3
Abstract Solution of a Local Area Network on the Example of a Basic School 4
Lühendite ja mõistete sõnastik 5
Sisukord 6
Jooniste loetelu 8
Tabelite loetelu 9
1 Sissejuhatus 10
1.1 Taust ja probleem 11
1.2 Ülesande püstitus 11
1.3 Metoodika 12
1.4 Ülevaade tööst 12
2 Vajadused 13
2.1 Sidelahenduse projekt 13
2.2 Portide kogus ja liiasus 15
2.3 Wi-Fi võrgud 16
2.4 Virtuaalsed kohtvõrgud 17
2.5 VPN 18
2.6 VOSK põhimõtted 18
3 Nõuded 20
3.1 Süsteemi suund 20
3.2 Omavalitsuse nõuded 20
3.3 Nõuded võrgutaristule 21
3.4 Nõuded välisühendusele 23
3.5 Nõuded tulemüürile 23
3.5.1 Tulemüüri kontseptsioon 23
3.5.2 Tulemüüri valikukriteeriumid 26
3.6 Nõuded kommutaatoritele 26

3.7 Nõuded traadita side pääsupunktidele 27
4 Teostus 29
4.1 Wi-Fi signaali modelleerimine 29
4.2 Hangitud seadmed 29
4.3 Võrgu topograafia ja topoloogia 30
4.4 Tulemüüri seadistused 31
4.5 Wi-Fi seadistused 32
4.6 Kaugindikatsioon ja logimine 32
4.7 Dokumenteerimine ja varundamine 33
4.8 Teostuse analüüs 34
5 Kokkuvõte 37
Kasutatud kirjandus 38
Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks 40

Jooniste loetelu

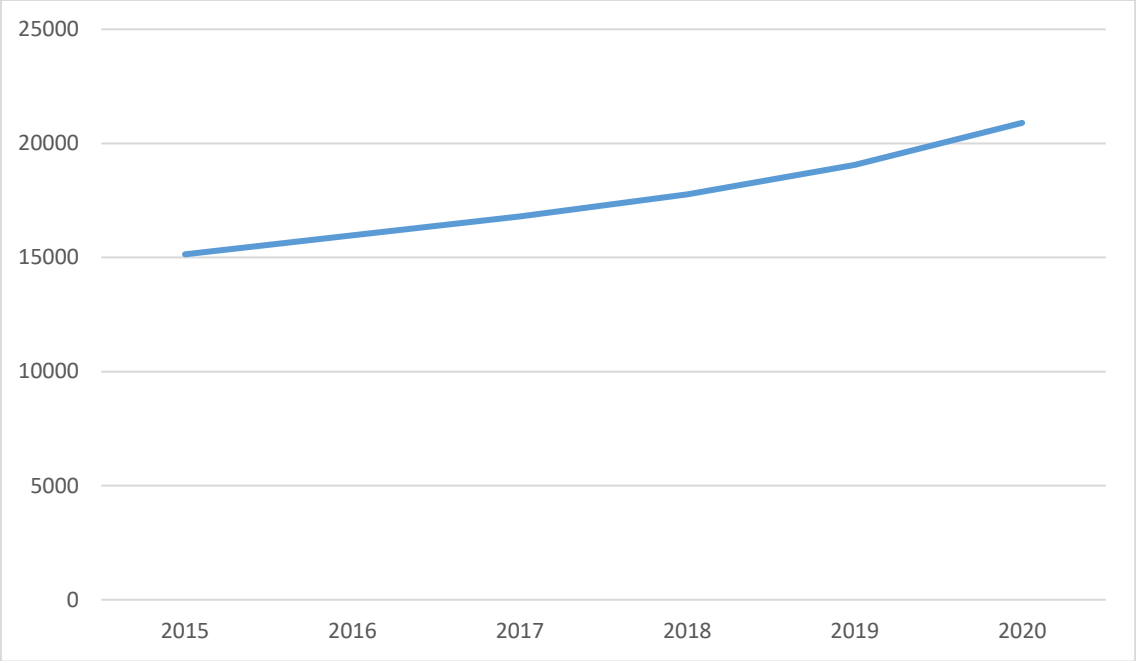
Joonis 1. Rahvastiku juurdekasv Rae vallas [1]. 10
Joonis 2. 2-kihiline mudel pinudena. 14
Joonis 3. Autodesk AutoCAD-iga projektist eksporditud andmed. 14
Joonis 4. Seadmekapp harjastega kaablihoidjatega. 22
Joonis 5. Valminud võrgu topograafia. 30
Joonis 6. W-Fi signaali katvus ühe korruse lõikes. 32
Joonis 7. Protsessi diagramm. 35

Tabelite loetelu

Tabel 1. Kommutaatoriportide vajadus jaotlate lõikes. 15
Tabel 2. Planeeritav kommutaatoriportide arv jaotlale lõikes. 16
Tabel 3. Kasutajatüüpide jagunemine traadita võrkude vahel. 16
Tabel 4. Sophos XG-seeria tulemüüri dimensioneerimine. 25
Tabel 5. Tulemüüri jõudluse parameetrid vastavalt kasutajate arvule [4]. 25
Tabel 6. Wi-Fi 5 ja Wi-Fi 6 pääsupunktide hinnavõrdlus. 28
Tabel 7. Riigihankega soetatud võrguseadmed. 29
Tabel 8. VLAN-ide jaotus 31

1 Sissejuhatus

Rahvastiku juurdevoolust tingituna rajavad suuremad omavalitsused uusi koole ning lasteaedu, samuti kaasajastatakse vanemaid õppehooneid. Näiteks on Rae vald ehitanud viimase viie aastaga kaks kooli, kaks lasteaeda, 2021. aastal lõpetatakse ühe põhikooli ehitus ja rajatakse veel üks täiendav lasteaed. Joonis 1 kujutab rahvastiku juurdekasvu viimastel aastatel Rae vallas.



Joonis 1. Rahvastiku juurdekasv Rae vallas [1].

Infotehnoloogia on muutunud vältimatuks osaks igapäevasest tööst ja õppetegevusest ning peab seda igati toetama, olema sealjuures nähtamatu, töökindel, turvaline. Haridusasutustes on igapäevaselt kasutusel keskkonnad nagu *Google Workspace*, e-Koolikott, Stuudium jms. Seega võib katkestus arvutivõrgus suuresti halvata kooli töö.

CERT-EE Twitteri leht võimaldab operatiivselt kursis püsida Eestis aktuaalsete rünnete ja ohtudega, samuti edastavad nad igal hommikul uudiskirja, kuhu on koondatud möödunud päeva aktuaalsemad küberintsidentidega seotud teemad kogu maailmast. Autori hinnangul on tegemist väärt lugemisvaraga, mis ei lase unustada, et küberturvalisus on miski, millega tuleb järjepidevalt tegeleda.

Käesolev töö uurib valdkonna parimaid praktikaid, mille abil luua töökindel, paindlik, lihtsasti hallatav ja turvaline kohtvõrgu lahendus ehitatavas 1000 õpilasega põhikoolis. Uuritakse ka teiste ümbruskonna koolide lahendusi, et leida, mida üle võtta ja mida parendada.

1.1 Taust ja probleem

Ehitatav hoone on üle 16000m^2 pindalaga kool koos spordihalliga. Planeeritav õpilaste arv on tuhande ringis. Õppetööga kaasas käivateks märksõnadeks on valikuvabadus, innovaatilisus, ettevõtlikkus.

Omavalitsuse IT-juhi hinnangul on varasemalt samas piirkonnas ehitatud koolides ja lasteaedades arvutivõrk ehitatud paljuski planeerimatult: võrgu füüsilises osas on lähtutud projekteerija nägemusest, mille tagajärjeks on kohati ebapraktiliselt asetsevad võrgupesad ja ebaühtlane traadita side katvus. Seadmete hankimise ja seadistamise seisukohalt puudub asutuste vahel ühtne nägemus, mistõttu on kasutusel mitmeid erinevaid lahendusi, seadmed on enamasti tarnija poolt seadistatud ja vastutaval IT-juhil puudub sellest lõplik teadmine ning ligipääs seadistustele. Lahenduste standardiseerimine, ühtlustamine võimaldaks optimeerida ka tööjõukulusid ning tööaega selliselt, et IT-juht ning haridustehnoloog võiksid olla samas isikus või oleks kooli IT-juhil võimalik hallata ka sama piirkonna laseteadu või muid allasutusi.

Töö tulemusena luuakse näidislahendus ja -dokumentatsioon, millest lähtuda ka teiste samalaadsete asutuste puhul seda pidevalt meeskonnana parendades ja täiustades.

1.2 Ülesande püstitus

Diplomitöö peamisteks eesmärkideks on:

- Selgitada välja nõuded ja soovitused loomaks turvalist ja töökindlat kohtvõrgu lahendust
- Defineerida vastavalt nõuetele, parimatele praktikatele ja asutuse vajadustele seadmete kogused, parameetrid, peamised pidepunktid konfigureerimiseks
- Luua eelmainitud punktide alusel töötav lahendus

Kevadel 2021 avaldas RIA ka esimese versiooni Eesti infoturbestandardist E-ITS, aga kuna antud töö oli sel hetkel juba lõppjärgus, siis selle nõudeid töös ei analüüsita.

1.3 Metoodika

Diplomitöö metoodika hõlmab nii vajaduste analüüsi, nõuete ja parimate praktikate uuringut kui praktilise lahenduse loomist ja selle analüüsi.

Nii seadmete tehniliste tingimuste kui võimaliku konfiguratsiooni välja selgitamiseks vaatleb autor soovitusi ja nõudeid, konsulteerib valdkonna ekspertidega ja kõrvutab saadud informatsiooni maja ning organisatsiooni vajadustega.

Ehituse valmides rakendatakse analüüsi tulemust töötava lahenduse loomiseks ja tagasiside saamiseks.

1.4 Ülevaade tööst

Töö esimeses osas defineeritakse hoone ja organisatsiooni vajadused. Ühelt poolt võetakse arvesse maja projekti, saamaks teada vajalike seadmete kogust, teisalt pannakse kirja olulisemad funktsionaalsed pidepunktid seadmete valikuks. Teises osas analüüsitakse erinevaid praktikaid ja nõudeid, mille alusel luua võrgu arhitektuur ja konfiguratsioon. Kolmandas osas kirjeldatakse lahenduse rakendamist praktikas. Töö neljas osa võtab kokku tehtu ja kirjeldab võimalikke arengusuundasid.

2 Vajadused

Kaasaegses (kooli)majas on arvutivõrgul suur roll: lisaks inimestele vajavad sidet ka erinevad tehnosüsteemid. Esialgsed lähtetingimused on:

- Ühtlane ja võimalikult kiire traadita side kogu majas
- Juhtmega võrguühendus igal statsionaarsel töökohal
- Igas klassiruumis saab olema kasutusel interaktiivne projektor
- Koridorides saavad olema infoekraanid
- Kasutama hakatakse nii üldkasutatavaid kui lokaalseid printereid
- Koolisöögi üle arvepidamiseks hakatakse kasutama õpilaspiletiga autentimist
- Maja tehnosüsteemide haldus ja monitooring peab olema võimalik ka väljastpoolt maja
- Rike mingis maja osas või võrguseadmes ei tohiks häirida teiste osade tööd

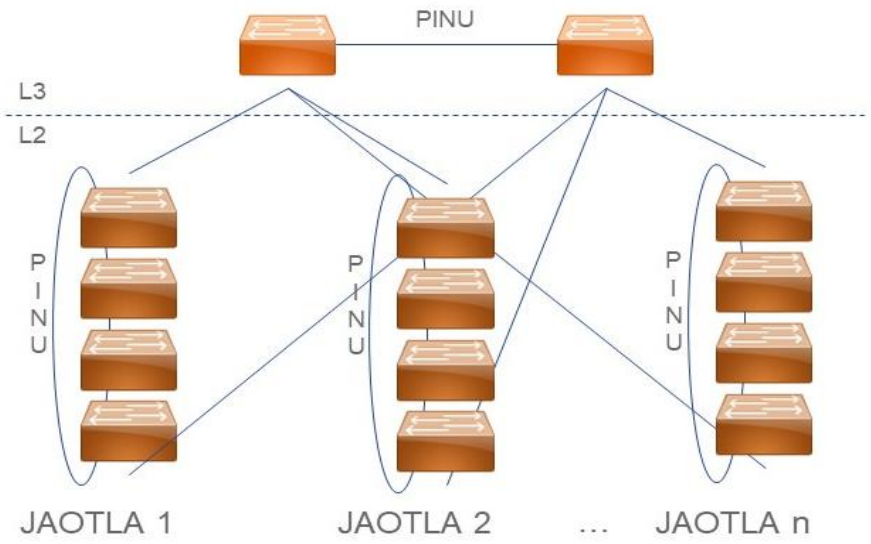
2.1 Sidelahenduse projekt

Saamaks aimu ehitatavast majast, tuleb esmalt tutvuda projektiga, seda analüüsida ja võimalusel ning vajadusel teha muudatusettepanekuid. Autor ei keskendu muudatusettepanekute osas tehnosüsteemide (kliimasüsteem, videovalve, lukustussüsteemid jms) lahendustele, vaatluse all on lõppkasutajale suunatud seadmed ja lahendused.

Välisühendus teostatakse optilise sideliiniga. Kõnealuses omavalitsuses on asutustele sideteenuse pakkujaks Riigi Infosüsteemi Amet (RIA).

Majja on planeeritud 6 andmesidejaotlat, millevahelised ühendused teostatakse optilise kaabliga. Kuigi täna laialt levinud 10Gbit/s ühendust saaks lahendada ka vaskkaabliliiniga, on optilise kaabli läbilaskevõime kuni 10 korda suurem [2], mis tagab tulevikukindluse. Joonis 2 kujutab üldkasutatavat ühendusviisi mitme jaotla korral (nn. linnaku võrk, ing. k *campus*

network), mis on 2-kihiline mudel ning koosneb jaotus- ja ligipääsukihist [3]. Kommutaatorid seadistatakse võimaluse korral pinuna (ing. k *stack*). Pinusse kuuluvad seadmed töötavad ja on hallatavad kui üks suur seade, kuid liikmete arv pinus on piiratud. Täpsem piirang sõltub konkreetsest mudelist. Jaotlatevahelised optilised magistraalid peavad sellist ühendusviisi võimaldama.



Joonis 2. 2-kihiline mudel pinudena.

Saamaks infot igasse jaotlasse planeeritud ühenduste arvu kohta, on mugav kasutada *Autodesk AutoCAD*-i olemasolul `DATAEXTRACTION`-käsku, mille abil saab luua tabeli soovitud infoga. Joonis 3 kujutab sel viisil loodud tabelit, mida saab hiljem kasutada kommuteerimise planeerimiseks ja dokumenteerimiseks, samuti on selle abil hõlbus tuvastada projekteerija vigu duplikaatide või puuduva info osas.

	'Name	'E_REMARKS	'E_SYMBTXT1	'E_SYMBTXT2	'RUUM	'SERVERIRUUM
41	LAN_P1_x	RL taga	Wifi	1FD5 .1.4	1043	1FD5
42	LAN_P1_x	RL taga	Wifi	1FD1_1.2.18	1040	1FD1_1
43	LAN_P1_x	RL taga	Wifi	1FD1_1.2.11	1041	1FD1_1
44	LAN_P1_x	RL taga	Wifi	1FD1_2.3.2	1085	1FD1_2
45	LAN_P1_x	RL taga	Wifi	1FD1_2.1.16	1108	1FD1_2
46	LAN_P1_x	RL taga	Wifi	1FD1_2.1.15	1109	1FD1_2
47	LAN_P1_x	RL taga	Wifi	1FD1_2.2.7	1096	1FD1_2
48	LAN_P1_x	RL taga	Wifi	1FD1_2.1.21	1105	1FD1_2
49	LAN_P1_x	RL taga	Wifi	1FD1_2.3.8	1083	1FD1_2
50	LAN_P1_x	RL taga	Wifi	1FD1_2.3.5	1084	1FD1_2
51	LAN_P1_x	RL taga	Wifi	1FD1_2.1.10	1110	1FD1_2
52	LAN_P1_x	RL taga	Wifi	1FD1_2.3.11	1082	1FD1_2
53	LAN_DKOMPLEKTX		IT.1T	1FD2_1.3.17	2018	1FD2_1
54	LAN_DKOMPLEKTX		IT.1S	1FD2_1.3.18	2018	1FD2_1
55	LAN_DKOMPLEKTX		IT.1T	1FD2_1.3.14	2017	1FD2_1

Joonis 3. Autodesk AutoCAD-iga projektist eksporditud andmed.

Projektist saadud info kohaselt on majja projekteeritud kokku 318 võrgupesa, millest 93tk on Wi-Fi pääsupunktidele. Tulenevalt loetletud vajadustest, nagu interaktiivsed projektorid,

infoekraanid ja printerid, aga ka erinevad ajutised töökohad, nagu näiteks kohtunike lauad spordivõistluste ajal jms, tuleb veenuda, et kõik vajalikud võrguühendused (aga ka muud nõrkvooluühendused ja toited) oleksid õige koha peal ja teha projekteerijale vastavasisulised muudatusettepanekud.

2.2 Portide kogus ja liiasus

Liiasus ehk reserv on kompromiss eelarve ja käideldavuse ning laiendatavuse vahel. Olles analüüsinud planeeritavaid töökohti, seadmeid ja Wi-Fi pääsupunktide vajadust, jõuame vajalike kommutaatorite portide arvuni. Vabu porte võiks olla 15%-25% [4]. Kui kasutatakse kombineeritult nii toitevõimekusega (ing. k *power over ethernet*, *PoE*) kui tavalisi kommutaatoreid, tuleb silmas pidada ka vabade *PoE*-võimekusega portide olemasolu. Seda nii võimalike Wi-Fi pääsupunktide lisamiseks kui ka muude seadmete tarvis (miniarvutid, *HDBaseT*, *Dante* jms protokollide muundurid jne). Erineva suurusega kommutaatorite vahel valides tuleks arvestada liiasuse nõuet, kommutaatorite hinnavahet ja maksimaalset seadmete arvu piirangut pinus: näiteks kasutades 24-pordist kommutaatorit võib liialt väikese liiasuse puhul tekkida hiljem vajadus täiendava kommutaatori lisamiseks, mis aga osutub võimatuks, kuna pinu on "täis" ning 24-pordine seade tuleb vahetada välja 48-pordise vastu.

Tabel 1 esitab ehitusprojekti ning vajaduste analüüsi tulemusel välja selgitatud portide vajaduse ja Tabel 2 planeeritava portide arvu koos liiasusega.

Tabel 1. Kommutaatoriportide vajadus jaotlate lõikes.

Jaotla	**Porte kokku**	**Neist PoE-porte**
FD1	57	21
FD2	63	19
FD3	83	13
FD4	78	23
FD5	42	10
FD6	45	9

Tabel 2. Planeeritav kommutaatoriportide arv jaotlale lõikes.

Jaotla	**PoE porte**	**Harilikke porte**	**Liiasus**
FD1	48	24	26%
FD2	48	48	52%
FD3	48	48	16%
FD4	48	48	23%
FD5	48	0	14%
FD6	48	0	7%

2.3 Wi-Fi võrgud

Koolis juhtmevaba võrguressurssi tarbivad inimesed võib jagada kolmeks: personal, õpilased ja külalised. Seega on vaja teenindada kolme tüüpi seadmeid: töö-, õppe-, ja isiklikud vahendid. Tabel 3 kirjeldab kasutajate jagunemist erinevate traadita võrkude vahel.

Tabel 3. Kasutajatüüpide jagunemine traadita võrkude vahel.

Seadme-tüüp / SSID	**Tööseade (arvuti)**	**Õppeseade (arvuti, tahvelarvuti)**	**Isiklik seade**
Personal	x		
Arvutiklass		x	
Avalik			x
Haldus	x*		

* peidetud SSID-ga võrk

Tabel 3 põhjal järeldub, et ka töötajate isiklikud seadmed saavad asuma avalikus võrgus. Sel viisil on personali võrgu kasutajate ring maksimaalselt kontrollitud. Halduse võrgu nimi (*SSID,* ing. k *service set identifier*) saab olema peidetud ja võrk kättesaadav ainult administraatoritele,

samuti ei edasta seda kõik pääsupunktid. Mainitud võrk on mõeldud ligipääsuks seadmete (tulemüür, kommutaatorid) ja serverite haldusliidestele.

Arvestama peab ka majas tegutsevate allüksuste vajadustega, nagu näiteks spordikeskus või huvialakool. Sellistel puhkudel võib tekkida vajadus avaliku võrgu nimi kas vastavalt muuta või lisada täiendavaid võrke.

2.4 Virtuaalsed kohtvõrgud

Virtuaalne kohtvõrk (ing. k *virtual LAN*, *VLAN*) on ISO OSI (ing. k *Open Systems Interconnection*) mudeli teises kihis töötav loogiline grupp seadmetest (tööjaamad, serverid, võrguseadmed), mis on näiliselt samas kohtvõrgus vaatamata nende geograafilisele asukohale. Kokkuvõtlikult on võimalik ühes VLAN-is oleva riistvara vahel andmeid liigutada eraldatult ja turvalisemalt [5]. Samuti tekib võimalus moodustada dünaamiliselt ja ajakohaselt uusi rühmi või neid ümber rühmitada, ilma et oleks vaja muuta füüsilist võrku [6].

Üldiselt tasub eraldi võrgud teha kõikidele seadmetele nagu serverid, tööjaamad, võrguseadmed, külaliste seadmed jne [6], [7]. Juhtmevaba võrgu segmenteerimisel kinnistatakse enamasti SSID kindlasse VLAN-i [8]. Seega moodustab Tabel 3 toodud võrkudest neli VLAN-i. Lisaks juhtmeta võrkudele võib loetleda veel järgnevad loogilised segmendid:

- Multimeedia (enamik statsionaarseid seadmeid nagu töökohad, projektorid, printerid)
- Partnerite seadmed (hooneautomaatika, sööjate registreerimise terminalid)
- Valveseadmed (valvekeskus(ed), videovalve)
- IP-telefonid
- VPN
- Allüksused (spordikeskus, huvialakool)

2.5 VPN

Kuna õppetööks kasutatakse *Google Workspace* keskkonda, nähakse VPN-i kasutust kooli puhul eelkõige personali vajadusena. Võimalikud kasutusjuhud oleksid:

- IT-süsteemide kaughaldus
- infoekraanide teenindamine
- haldussüsteemide kaughaldus
- (video)valve rakendused
- (3D) printimine
- võimalus kasutada turvalist ühendust avalikus võrgus viibides
- interaktiivsetele tahvlitele eemalt pildi kuvamine

Vajalik on kasutaja rolli tuvastamine, tagamaks üle VPN-i samade (ja ainult nende) ressursside kasutamisvõimalust, mis on talle võimaldatud maja sisevõrgus (näiteks ei tohiks VPN-i kasutav õpetaja pääseda halduse või hooneautomaatika võrkudesse). Võimalikud võrguühenduse kiiruse ja viitega seotud vajadused tuleb välja selgitada kasutamise käigus. Otseseid ajakriitilisi rakendusi ette ei nähta, testida tuleb näiteks projektoritele pildi edastamise võimalikkust.

2.6 VOSK põhimõtted

Töö aluseks olevas koolis on igale töötajale ette nähtud sülearvuti, kui see vähegi põhjendatud on (näiteks hakkab ühena vähestest lauaarvutit kasutama administraator, kuna tema töö ei eelda mobiilsust). Sülearvutite kasutamine ahendab isiklike seadmete ringi, milleks jäävad enamasti mobiiltelefonid.

Enamik kaasaegseid mobiiltelefone on vaikimisi krüpteeritud [9]. Töötajatel soovitatakse seadme lukustamiseks kasutada PIN-koodi ja teisi operatsioonisüsteemi poolt pakutavaid vahendeid, kuid kuna need seadmed on isiklikud, siis soovituse rakendamist kontrollida ega sundida ei saa. Telefonis hoitavad tööalased andmed on enamasti e-kirjades ja pilverakenduses (*Google Workspace*, *MS OneDrive*). Isiklikud seadmed ühendatakse asutuse avalikku võrku.

Vajadusel saab üksikutele kasutajatele teha erandeid või lubada näiteks avalikust võrgust printimist, kuid neid juhte vaadatakse vajaduspõhiselt.

3 Nõuded

Lahendusele esitatavate nõuete defineerimisel lähtub autor nii omavalitsuses välja kujunenud tavadest kui erinevate organisatsioonide ja raamistike (RIA, HARNO, ISKE) juhenditest.

3.1 Süsteemi suund

Selleks, et esitatavad nõuded oleksid asjakohased, tuleb võrku planeerides teha valik kolme peamise arhitektuuri vahel: pilv, hübriid, kohapealne [10]. Pilveteenuse puhul on kogu serveripargi osa majutatud pilveteenust pakkuva ettevõtte juures. Kohapeal on ainult töökohad, võrgujagajad, tulemüür, printerid. Hübriidlahenduse korral asub osa serveritest kohapeal, osa pilves. Kui kõik lokaalvõrgu serverid asuvad asutuse kontrolli all olevas serveriruumis, on tegemist kohaliku süsteemiga.

Planeeritav lahendus saab olema hübriid: pilveteenustest võetakse kasutusele *Google Workspace* ning *Microsoft 365*, mille poolt pakutavat kasutajate haldust dubleeritakse kohapeal asuvas domeenikontrolleris. Samuti saab majas asuma infotabloode sisu halduse server ning failiserver varunduse tarvis. Kasutajate arvutid hakkavad põhinema *Microsoft Windows* operatsioonisüsteemil.

3.2 Omavalitsuse nõuded

Kõik hangitavad seadmed peavad olema kaasaegsed ja omama võimalikult pikka tootja tuge. Tänane praktika Rae vallavalitsuses on, et haldus- ja tugilitsentsid, tulemüüri teenused jms ostetakse 5 aastaks ning tootjapoolne garantii hangitavatele seadmete peab olema võimalikult pikk, kuid mitte lühem kui 3 aastat. Mõned võrguseadmete tootjad pakuvad oma toodetele eluaegset garantiid – selle tingimused on küll tootjate ja seadmete lõikes erinevad ja vajavad põhjalikku tutvumist, kuid sellise võimalusega seadmed on kindlasti eelistatud. Ühelgi hangitaval seadmel ei tohiks olla välja kuulutatud eluea lõpu (ing.k *end of life*) tähtaega.

Püsimaks vallaüleselt mingites piirides ja tagamaks töötajate vahetumise korral süsteemi halduse jätkusuutlikkust, eelistatakse seadmeid ja lahendusi, mis on laialt kasutuses, nn "tööstuse standard". Erinevates omavalitsuse allasutustes kasutatavate seadmete ühtlustamine võimaldab hoida ka kriitilist laovaru või tagada kiiret tarnet koostööpartneritelt varuseadmete näol võimalike rikete kiireks kõrvaldamiseks. Seega on võetud üheks põhimõtteks, et

võimalusel ei kasutata nišitooteid ning hangitavad seadmed ja lahendused peaksid olema märgitud Gartneri "*Magic Quadrant for …*" viimase 2 aasta aruandes, soovitavalt liidrite sektsioonis. Mainitud kriteeriumit võiks pidada ka üheks usaldusväärse tootja/toote märgiks.

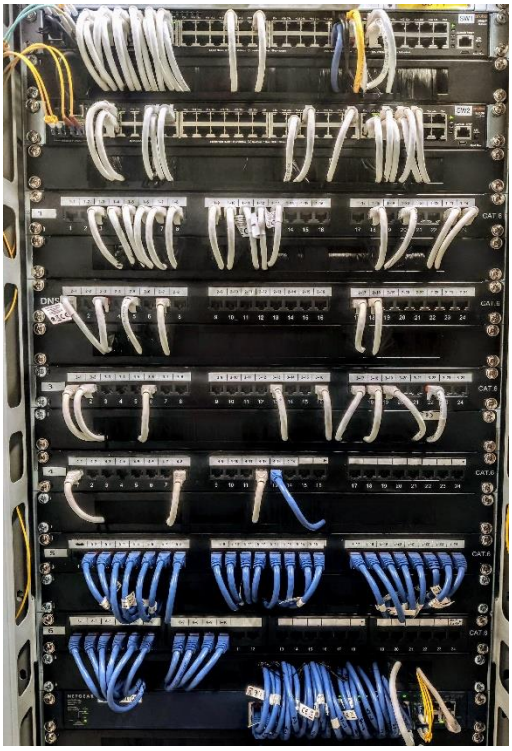
Infosüsteemide turvameetmete süsteemi ISKE nõuded peaksid olema täidetud vähemalt vastavalt turbeastmele M. Meetmeid rakendades lähtutakse etalonlahendusena vallavalitsuse ISKE auditist.

3.3 Nõuded võrgutaristule

Projektijärgselt peab ehitatava andmesidevõrgu kaabeldus võimaldama andmeedastust minimaalselt kiirusega 1 Gbit/s. Kaabelduse teostamiseks tuleb kasutada kaablit U/UTP 4x2x0,5 Cat.6 või paremat. Kaablid tuleb markeerida mõlemas otsas kulumis- ja veekindlate märgistega ning kogu võrk tuleb testida üldtunnustatud taadeldud testriga. Andmesidevõrgu testimise kohta koostatakse testraport [11].

Tagamaks manipuleerimisest vaba võrgu tööd, tuleb aktiivseadmed ja kommuteerimispaneelid paigaldada lukustatavatesse seadmekappidesse [12]. IT-süsteemid, mida hooldavad mittekoosseisulised töötajad (näiteks ventilatsioon, küte, taastuvenergia lahendused), peaks olema paigutatud eraldi ruumidesse. Peale selle oleks otstarbekohane paigaldada erineva kaitsetarbega või erinevate valdkondade IT-süsteemid eraldi ruumidesse, et sissepääsuõigusega isikute arvu väiksena hoida [13].

Seadmekapp peab olema komplekteeritud selliselt, et iga kommuteerimispaneeli kohta paigaldatakse üks kaablihoidja. Tagamaks kapi korrektset välimust, on autori soovitus kasutada harjastega kaablihoidjaid, mille puhul jooksevad kommuteerimiskaablid kapis sees. Selline lahendus (Joonis 4) väldib üleliigse kaabli kuhjumist ning aitab tagada kaablile lubatud maksimaalse painutusraadiuse piirides püsimist [14]. Kui seadmekapil on avatavad küljepaneelid, tagab mainitud lahendus vajadusel äärmiselt lihtsa kaablite tuvastamise ja ümberkommuteerimise võimaluse.



Joonis 4. Seadmekapp harjastega kaablihoidjatega.

Iga seadmekapi toide peab olema tagatud piisavat võimsusvaru pakkuva puhvertoiteallikaga (ing. k *uninterruptable power supply, UPS*). Puhvertoiteallika valikul tuleb silmas pidada eelkõige kolme kriteeriumit:

- Kasutatav tehnoloogia (*offline, line interactive, online*): IT-süsteemide korral on soovituslik kasutada *online*-tehnoloogial töötavat *UPS*-i, kuna sel juhul on toite väljund sisendist täielikult isoleeritud ning sõltumatu. ISKE kohaselt kujutab *UPS*, mis on liigitatud DIN IEC 62040-3 järgi VFI-SS-111 ehk *online*, endast IT-toite kõige optimaalsemat varianti [15].

- Jõudlus: Paljud *UPS*-ide tootjad märgivad lubatud väljundvõimsuse näivvõimsusena (ühik VA), seadmete vajadus on aga enamasti toodud aktiivvõimsusena vattides (W). Tuleb silmas pidada, et võimsustegurist (cos φ, ka PF, ing. k *power factor*) tulenevalt ei pruugi näivvõimsus olla võrdne aktiivvõimsusega.

- Toetusaeg: ISKE soovitus on, et toetuseaeg peaks olema võrdne ooteaja ja kahekordse väljalülitusaja summaga, sealjuures soovitatav ooteaeg on 15min [15].

Puhvertoiteallikas peab olema varustatud võrgumooduliga, et kasutada kaugindikatsiooni pakutavaid võimalusi.

3.4 Nõuded välisühendusele

Hoone välisühendus teostatakse projektijärgselt optilise kaabliga. RIA pakutav Riigivõrk võimaldab kuni 10 Gbit/s sümmeetrilist ühendust, tüüpiline lõppkliendi lahendus on täna siiski 1 Gbit/s [16]. Eeldusel, et infotehnoloogia on igapäevaste tööprotsesside osa, peaks 50 ja enama kasutaja puhul välisühendus olema minimaalselt 1Gbit/s [10].

Kool on asutus, kus töötajatest hoopis suurem kasutajaskond võivad olla õpilased. Sellegipoolest ei arvesta autor siinkohal märkimisväärse õpilastest tuleneva koormuse kasvuga välisühendusele, kuna:

- Kõik isiklikud seadmed saavad töötama vaid avalikus võrgus, mille kiirust saab vajadusel piirata
- Võib eeldada, et suur osa isiklikest mobiilsetest seadmetest kasutavad andmesideks telekomioperaatori võrku, mistõttu ei ole avaliku võrgu kasutamine kasutaja jaoks primaarne. Antud eeldust kinnitab ka senine kogemus teistes piirkonna koolides
- Paljud koolid on sätestanud sisekorraeeskirjades olulised piirangud mobiilsete seadmete kasutamise osas õppetöö ajal [17], [18]

Kui välisühenduse kiiruse tõstmine peaks siiski vajalikuks osutuma, peab füüsiline meedium seda võimaldama.

3.5 Nõuded tulemüürile

Tulemüür kui seade või tarkvara on üsna laiapõhjaline ja võimekas kontseptsioon, millel kasutusvõimalusi mitmeid. Selle edukaks rakendamiseks tuleks välja töötada nägemus, milliseid turvaeesmärke seade täitma peaks [19].

3.5.1 Tulemüüri kontseptsioon

ISKE kataloog toob välja mitmed turvalüüsi turvaeesmärkide näited. Neist tulenevalt võib öelda, et nii kohalikke servereid kui pilveteenuseid kasutava kooli, lasteaia jms asutuse kontekstis tuleks tulemüüri peamiseks ülesandeks lugeda sisevõrgu kaitsmise laivõrgust pärinevate volitamata juurdepääsukatsete eest [19]. Sellise ülesandepüstituse alla mahuvad ka kitsamad alad nagu kaitse võimalike tarkvaraliste turvaaukude, *IP-spoofingul* jms põhinevate rünnete ja lokaalsel tasandil esitatud ja salvestatud andmete terviklus- või konfidentsiaalsuskao

vastu. Teine suund ja eesmärk võiks olla ebasoovitava sisu filtreerimine: vajadusel keelata vägivaldse jm ebasündsa sisuga veebilehtede laadumine. Selle rakendamine sõltub suuresti asutuse vajadusest ja reeglitest ning kujuneb välja aja jooksul. Algseadistuseks küsitles autor ümberkaudsete asutuste IT-juhte ja valdav trend on, et sisu filtreerimist kasutatakse külalistele ja õpilastele mõeldud võrkudes (Arvutiklass, Avalik).

ISKE sõnastab ka mitmed eeldused, tagamaks, et turvalüüs suudaks edukalt täita oma ülesannet ja kaitsta võrku väljast tulevate rünnete eest. Üheks selliseks on, et turvalüüsi tohib kasutada eranditult vaid kui sisemist võrku kaitsvat üleminekut. Seetõttu tohivad turvalüüsis endas saadaval olla vaid hädavajalikud teenused ning täiendavate teenuste (nt veebiserveri) pakkumisest tuleb loobuda [19]. Sellegipoolest sisaldavad kaasaegsed tulemüürid võimalusi rakendada neid ka marsruuterina. Omavalitsusasutuse eelarve on piiratud ning maksumaksjalt kogutud raha kasutamine peab olema vastutustundlik. Seetõttu uuriti töö käigus nii tulemüüride andmelehti kui küsitleti ka edasimüüjaid, saamaks infot võimalike puuduste kohta tulemüüri rollide laiendamise osas. Vastavalt planeeritavale kasutusele tuleks vaadata maksimaalset üheaegset ühenduste arvu, samaaegsete võimalike VPN-tunnelite arvu, sissetungi takistamise süsteemi (ing. k *intrusion prevention system, IPS)* võimekust jms. Kasutajate arvu ja jõudluse kohta info leidmiseks tasub otsida märksõnu nagu "*sizing guide*" ja "*product matrix*". Soovitatav on ka tooteeksperdiga konsulteerimine, kuna kaasaegsed tulemüürid võimaldavad kasutada paljusid erinevaid teenuseid ja seetõttu võib ostetava seadme lihtsasti üledimensioneerida, kuna reaalsuses ei kasutata kõiki mooduleid - kas siis vajaduse puudumise või litsentsitasude tõttu. Tabel 4 esitab näidisarvutuskäigu Sophos XG-seeria tulemüüride dimensioneerimiseks eeldatava kasutajate arvu järgi [20]. Selles toodud kasutajate tasemete loomisel on arvesse võetud võimalikke kasutatavaid teenuseid.

Tabel 4. Sophos XG-seeria tulemüüri dimensioneerimine.

	Kasutajate arv	Tegur	Kaalutud kasutajaid
Tavakasutajaid	150	1	150
Edasijõudnud kasutajaid	10	1,2	12
Power-kasutajaid	0	1,5	0
Kokku kasutajaid	160	Kaalutud kasutajaid	162
		Süsteemi koormustegur	1,2
		Kaalutud kasutajaid	**195**

Edasimüüjatest intervjueeris autor Vendomar AS ja Econet Systems OÜ eksperte ning nende hinnangul võiksid käesolevas töös käsiteldava suurusega kooli puhul olla sobivateks näidistoodeteks *Fortigate* 100 või *Sophos* XG210. Mõlemad oskasid tuua praktikast palju näiteid, kus mainitud seadmed täidavad edukalt ISO OSI mudeli kolmanda kihi funktsioone.

Kooli puhul võib varasema kogemuseta olla keeruline ennustada samaaegsete kasutajate arvu. Tabel 5 väljendab HITSA (praegune HARNO) poolt avaldatud miinimumnõudeid tulemüüri jõudlusele, mille vastu saab hangitava seadme parameetreid võrrelda.

Tabel 5. Tulemüüri jõudluse parameetrid vastavalt kasutajate arvule [4].

Soovitatav kasutajate arv	Tulemüüri võrguliikluse läbilase (rakenduse teadlikkusega – L7)	Uute ühenduste arv sekundis	Üheaegsete ühenduste arv
25-110	Vähemalt 300Mbps	Vähemalt 8000	Vähemalt 250000
Vähemalt 500	Vähemalt 650Mbps	Vähemalt 12000	Vähemalt 500000
Vähemalt 1500	Vähemalt 1Gbit/s	Vähemalt 30000	Vähemalt 750000

3.5.2 Tulemüüri valikukriteeriumid

Kontseptsioonist, eelmainitud muudest nõuetest ja kaasaegsetest näidistoodetest tulenevalt saab sõnastada tulemüürile esitatavad nõuded. Alustades üldisematest, võiks need kirjeldada järgnevalt:

- Tootjat on mainitud viimase 2 aasta jooksul Gartneri "*Magic Quadrant for …*" aruande liidrite sektsioonis
- Hangitav tulemüür on rakenduste teadlik, kolmanda põlvkonna (ing. k *next generation firewall, NGFW*) seade
- Seade peab olema kasutatav lüüsi ja marsruuterina, sh võimalus luua virtuaalseid kohtvõrgu alamliideseid vähemalt 100tk [4]
- Seade peab töötama DHCP-serverina
- Liikluskoormuse dünaamiline taluvus vähemalt 135 000 uut seanssi sekundis
- Maksimaalne üheaegsete seansside arv vähemalt 8,25 mln
- VPN-režiimis läbilaskevõime vähemalt 1,3 Gbit/s
- Kasutajate arvul ei tohi olla tootjapoolset litsentsiga määratud ülempiiri
- *Active Directory* teenusega integreerimise võimalus

3.6 Nõuded kommutaatoritele

Ligipääsukihi kommutaatoreid ei tohiks kunagi kasutada võrgu laiendamiseks [21]. Seetõttu planeeritakse kasutatav lahendus kahekihilise mudeli baasil, nagu kirjeldatud peatükis 2.1.

Kommutaatori esimesteks valikukriteeriumiteks võib pidada hallatavust ning võimlaust kohtvõrku segmenteerida erinevateks levipiirkondadeks, kasutades virtuaalseid kohtvõrke [4]. Olukorras, kus konkreetne VLAN ei ole piiratud ühe andmesidejaotlaga, vaid seda kasutatakse üle maja või linnaku, on *Cisco* andmeil parim lahendus kasutada ligipääsukihis ISO OSI mudeli kanalikihis (2. kiht) ning jaotuskihis võrgukihis (3. kiht) töötavaid kommutaatoreid [21]. Siinkohal tuleb seadmeid hankides tähele panna, et mitte kõik kanalikihis töötavad

kommutaatorid ei ole pinuna seadistatavad, nagu vajaduste peatükis sätestatud, mistõttu võib osutuda maksumuse poolest otstarbekamaks hankida kolmandas ehk võrgukihis töötavad seadmed. Kommutaatorite omavahelised ühendused peavad võimaldama vähemalt 10Gbit/s andmeedastuskiirust ja tuleks võimalusel lahendada *DAC*- (ing. k *direct attach copper*) või optiliste kaablitega. *DAC*-kaablite ja *SFP*-moodulite valikul tuleb kindlasti kontrollida nende sobivust kasutatava riistvaraga.

Kommutaatorid, mille külge ühenduvad traadita side pääsupunktid, peavad varustama neid toitega (*ing. k power over ethernet, PoE*). Sealjuures tuleb silmas pidada, kas plaanitakse kasutada suurema võimsustarbega seadmeid kui 15,4W. Sellisel juhul peab kommutaator vastama IEEE802.3at ehk *PoE+* standardile, mis tagab kuni 30W võimsusvaru [22]. Sellisteks seadmeteks võivad olla näiteks motoriseeritud valvekaamerad, arvutid või suure väljundvõimsusega traadita side pääsupunktid. Tähelepanuta ei tohi jätta ka maksimaalset lubatavat koguvõimsust.

Ligipääsukihis kasutatavad kommutaatorid peavad omama vähemalt 10Gbit/s allalülitusliideseid, et tagada vajaduste peatükis 2.1 defineeritud andmesidekiirus. Kuna tegemist on nö keskse sõlmega, millest sõltub mitmete teiste sõlmede töö, peaks seadme toiteplokid ja ventilaatorimoodulid olema dubleeritud ja kuumvahetatavad.

3.7 Nõuded traadita side pääsupunktidele

Allikale tuginedes peaks tänapäevane pääsupunkt töötama sagedusel 2,4GHz ja 5GHz ning toetama ühendusstandardit vähemalt IEEE 802.11ac *Wave 2* [8]. Kaasaegset lahendust luues tuleks eelmist lauset parandada, lisades IEEE 802.11ax standardi (Wi-Fi 6) ja 6GHz sagedusriba. Tulenevalt Wi-Fi 6 standardi uudsusest ning sellest tulenevast seadmete kõrgemast hinnast (Tabel 6) ja tõsiasjast, et paljud täna müüdavad klientseadmed veel Wi-Fi 6 ei toeta, võib osutuda otstarbekaks ehitada traadita side võrk nn. Wi-Fi 5 ehk IEEE 802.11ac *Wave 2* seadmete põhiselt.

Tabel 6. Wi-Fi 5 ja Wi-Fi 6 pääsupunktide hinnavõrdlus.

WiFi pääsupunkt	**Kasutatav tehnoloogia**	**Orienteeruv hind**
HPE Aruba AP-305	802.11ac Wave 2	280€
HPE Aruba AP-505	802.11ax	580€
Ruckus R320	802.11ac Wave 2	300€
Ruckus R550	802.11ax	620€

Kaasaegne IEEE 802.11ac *Wave 2* tehnoloogial töötav pääsupunkt peab töötama samaaegselt 2,4GHz ja 5GHz sagedusalades, kasutama raadioeetrit võimalikult efektiivselt (*MU-MIMO*, vähemalt 3x3:3 ruumiliste voogude (ing. k *spatial stream*) tugi, dünaamiline saatevõimsuse kohandamine mõlemas sagedusalas (ing. k *radio resource management*, RRM), signaalitee (ing. k *band steering*) ja levisignaali kliendipõhine suunamine (ing. k *beamforming*), dünaamiline sagedusvahemiku valimine ja kiirgusvõimsuse piiramise võimekus jne). Turvalisuse kohapealt peavad olema toetatud tehnoloogiad nagu *WPA3*, 802.1X, võimekus kasutada erinevaid autentimismeetodeid erinevatel *SSID*-võrgunimede profiilidel, kasutajatevahelise liikluse blokeerimine (ing. k *client isolation*). Oluliste protokollidena olgu nimetatud veel ka IEEE 802.11r (*Fast BBS transition standard* ehk *fast roaming*), IEEE 802.11k (*radio resource management*) ja IEEE 802.11v (*BSS transition management*) [8]. Nõutav on ka lokaalse ja välise hõiveportaali tugi ning võimalus võrkudele ajaprofiile seadistada. Pääsupunkt peab säilitama funktsionaalsuse ka haldusplatvormiga ühenduse kaotamisel.

4 Teostus

Töö kirjutamise hetkel on paigaldatud ja seadistatud vaid üks osa majast (algkool), kuna ülejäänud osa valmib ehituse teises järgus ja võetakse kasutusele sügisel 2021.

4.1 Wi-Fi signaali modelleerimine

Projekteerija on kogu maja peale näinud ette 88 siseruumidesse mõeldud ja 5 välist traadita side pääsupunkti. Maja siseseintes on kasutatud nii raudbetooni kui kergplokki. Wi-Fi pääsupunktide tegeliku vajaduse väljaselgitamiseks paigaldati need kolme kõrvuti asetsevasse klassiruumi ja koridori (kokku 4 seadet). Testseadmeteks kasutati Aruba IAP-305 pääsupunkte ja signaalitugevuse analüüsiks programme *inSSIDer* ja *Aruba AirWave*. Ülejäänud maja osas modelleeriti pääsupunkte *AirWave* keskkonnas.

Võttes arvesse nii mõõtmistulemusi kui ka asjaolu, et klassidesse planeeritavad interaktiivsed projektorid võimaldavad üle õhu pildiedastust *Miracast*-tehnoloogiaga, mille rakendamise teeb igas klassis asuv pääsupunkt lihtsamaks, jäädi pääsupunktide asukoha ja arvu osas projekteerijaga samale seisukohale.

4.2 Hangitud seadmed

Tabel 7 kirjeldab käesoleva töö analüüsi tulemusel valminud tehniliste nõuete alusel hangitud võrguseadmeid.

Tabel 7. Riigihankega soetatud võrguseadmed.

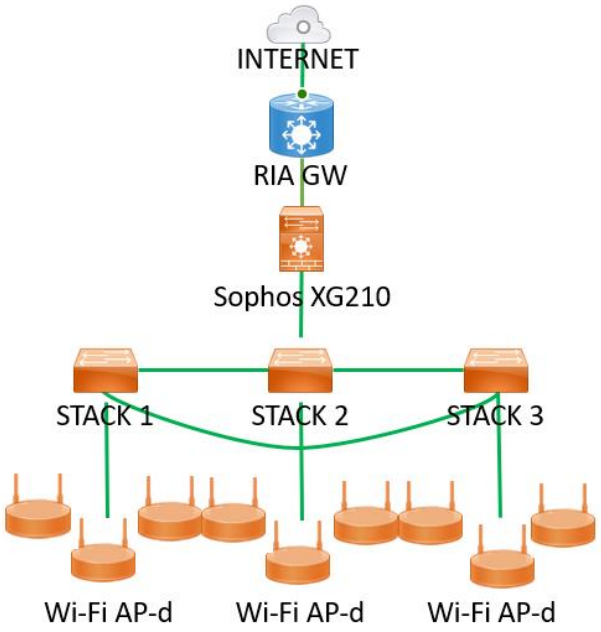
Seadme tüüp	Tootja	Mudel	Kogus
Tulemüür	Sophos	XG210	1
Kommutaator	HPE Aruba	JL256A	6
Kommutaator	HPE Aruba	JL254A	4
Wi-Fi pääsupunkt	HPE Aruba	IAP-305	88

Traadita side pääsupunktide valikul realiseerus peatükis 3.7 kirjeldatud olukord, kus eelarvelistest vahenditest lähtuvalt tuli Wi-Fi 6-st loobuda ja valida IEEE 802.11ac *Wave 2*

tehnoloogiat kasutavad seadmed. Samal põhjusel tuli hetkel loobuda ka jaotuskihi kommutaatorist, mille soetamine on planeeritud järgmisesse eelarveperioodi.

4.3 Võrgu topograafia ja topoloogia

Joonis 5 kujutab hetkel teostatud võrgu topograafiat.



Joonis 5. Valminud võrgu topograafia.

VLAN-ide ja alamvõrkude (ing. k *subnet*) planeerimisel lähtuti lihtsuse ja töökindluse huvides põhimõttest, et iga VLAN on ka eraldi alamvõrk. Võrgu segmenteerimisel on arvesse võetud töös viidatud erinevate allikate (ISKE, RIA, HITSA) nõudeid ja soovitusi ning sellest tulenevalt otsused tehtud. Erinevate alamvõrkude suuruse valimisel on lähtutud potentsiaalsete klientide arvust: näiteks on arvestatud, et avalikus võrgus võib ühel kliendil võib olla kuni 3 seadet (arvuti, telefon, tahvelarvuti). Seega 2046 aadressi puhul jätkuks IP-aadresse 682 kliendile. Tabel 8 on toodud VLAN-ide jaotus.

VLAN-i number võiks hallatavuse ja läbipaistvuse huvides peegeldada alamvõrku, millesse ta kuulub. Näiteks on alltoodud tabel koostatud selliselt, et VLAN-i number moodustub alamvõrgu aadressi teisest ja kolmandast oktetist (VLAN 160 võrgu aadress on 172.16.0.0, VLAN 1682 võrgu aadress on 192.168.2.0 jne).

Tabel 8. VLAN-ide jaotus

VLAN	Nimi	Aadresse	Kirjeldus	Ligipääs
160	Haldus	254	Haldusliidesed	WPA3, tulemüüri reeglid
161	Serverid	254	DC, NAS, ...	Tulemüüri reeglid
162	Personal	254	Töötajate WiFi	WPA3
163	Arvutiklassid	254	Õpilaste kasutuses olevad seadmed	WPA3
164	VoIP (reserv)	254	IP-telefonid	
165	VPN	254	VPN kliendid	SophosConnect
166	Multimeedium	510	Juhtmega töökohad, projektorid, infoekraanid, printerid, helisüsteemid	
168	Avalik	2046	Avalik Wi-Fi	WPA3
170	Automaatika	254	Välised partnerid	
171	Valvesüsteemid	254	Välisühenduseta	Juurdepääs ainult üle VPN ja sisevõrgust MAC-filtriga

4.4 Tulemüüri seadistused

Tulemüür on seadistatud selliselt, et see täidab ka marsruuteri ning DHCP serveri ülesandeid. Tavakasutajaile loodud VLAN-id on koondatud ühte, nn „LAN“-tsooni, millele rakendatakse IPS- ja sisu filtreerimise reegleid. Kasutusel on ka DoS-rünnaku kaitse, mis on seadistatud vaikimisi tulemüüri tootja pakutud väärtustega 12000 paketti minutis. DDoS-rünnaku vastased

meetmed ei ole XG210 mudelil toetatud [23], kuid vastavat kaitset pakub teenusepakkuja RIA. Reaalse ründe korral on võimalik kasutada varuühendusena ka mobiilsideoperaatori ühendust, mille tarvis on seadistatud üks tulemüüri portidest.

4.5 Wi-Fi seadistused

Kõik kasutusel olevad Wi-Fi võrgud on turvatud WPA3 protokolliga. Avalikus võrgus on lülitatud sisse tagasiühilduvuse tugi, mis võimaldab võrku kasutada ka vanemate, WPA2 protokolli toetavate seadmetega. Kuna teistes võrkudes kasutatakse vaid piiratud hulka seadmeid, millede võimekus on kontrollitud, puudub neis tagasiühilduvuse vajadus. Sisse on lülitatud IEEE 802.11r, IEEE 802.11k, IEEE 802.11v. Segmenti Wi-Fi signaali katvusest kujutab Joonis 6.

Joonis 6. W-Fi signaali katvus ühe korruse lõikes.

Avalikus võrgus rakendatakse kasutajatevahelise liikluse blokeerimist. Wi-Fi võrkudele on seatud ajalised piirangud: kõik võrgud, välja arvatud Personal, on saadaval tööpäevadel kella 7-20. Personali võrk on saadaval ka nädalavahetuseti, kuid lülitub samuti ööseks välja: selliselt vähendatakse võrku sissemurdmise tõenäosust ning vähendatakse eetri reostust. Kellaajalisi piiranguid võib vastavalt kasutajate tagasisidele muuta või üldse tühistada.

Võrguühendused on arvutites eelseadistatud ja kasutajatele on saadaval ainult avaliku võrgu parool.

4.6 Kaugindikatsioon ja logimine

Võimalike rikete ja anomaaliate avastamiseks kasutatakse eelistatult SNMPv3 (ing. k *Simple Network Management Protocol*) või kui seade seda ei võimalda, siis SNMPv2 protokolli.

Võrguseiretarkvarana kasutatakse esialgu *Paessler PRTG Network Monitor* tasuta versiooni, mis on piiratud 100 anduriga. Monitooritakse järgnevat:

- Välisühenduse olemasolu (*ping*)
- Tulemüüris seadistatud SNMP hoiatusi ning *syslog*-teateid
- Kommutaatorite üleslülitusporte (*ping*)
- Kommutaatorite SNMP hoiatusi
- Wi-Fi pääsupunktide olemasolu (andurite arvu piirangutest tulenevalt valikuliselt)
- UPS-ide SNMP hoiatusi

Kuivõrd *PRTG Network Monitor* on tasuline tarkvara ja selle juurutamine erinevates asutustes võib kujuneda üsna kulukaks, tuleb esmalt testida selle kasutegurit ning ka alternatiivlahendusi, nagu *Zabbix*.

4.7 Dokumenteerimine ja varundamine

IT-kasutuse planeerimine, juhtimine, kontrollimine ja hädaolukorraks valmisoleku plaan toetuvad kõik ühisele alustalale – olemasoleva IT-süsteemi dokumentatsiooni ajakohasusele. Ainult värskele informatsioonile toetudes on võimalik hädaolukorras IT-süsteemi uuesti vajalikul moel töökorda seada [24].

Töö autori hinnangul on parim dokumenteerimist alustada süsteemi loomise hetkest alates, ning paralleelselt tehtud tööga täiustada ka dokumentatsiooni. Kirjapandu tuleb kindlasti hiljem korrektselt vormistada, et see oleks vajadusel arusaadav kolmandatele isikutele. Kui mingis osas kaasatakse väliseid partnereid (sideühenduse teenusepakkuja, rendil olevad seadmed jms), peavad kirjas olema ka vastavad kontaktisikud.

Vajalik on dokumenteerida nii võrgu topograafia (füüsiline ülesehitus) kui topoloogia (loogiline struktuur) [25]. Kui vastav dokumentatsioon on ajakohane, näiteks uusehitiste puhul, on topograafia lihtsasti talletatav side teostusjooniste kujul. Punktis 2.1 kirjeldatud ühenduste tabel (Joonis 3) tuleb viia vastavusse teostusjoonistega, seejärel on suvaline ühendus kahe

punkti vahel lihtsasti tuvastatav ja leitav. Lisades siia veel ka peatükis 0 toodud Tabel 8, saab kogu võrgust hea ülevaate.

Mitte kõik muudatused ei ole pikalt planeeritud ja võib juhtuda, et kiiruga ja ajutiselt tehtud muudatus saab püsivaks ning ununeb dokumenteerimata. Selliste olukordade vältimiseks füüsiliste ühenduste korral on autor sisse viinud korra, kus igas seadmekapis on paberkandjal tabel, kuhu kõik muutused kirja panna ning seejärel hiljem korrektselt dokumenteerida.

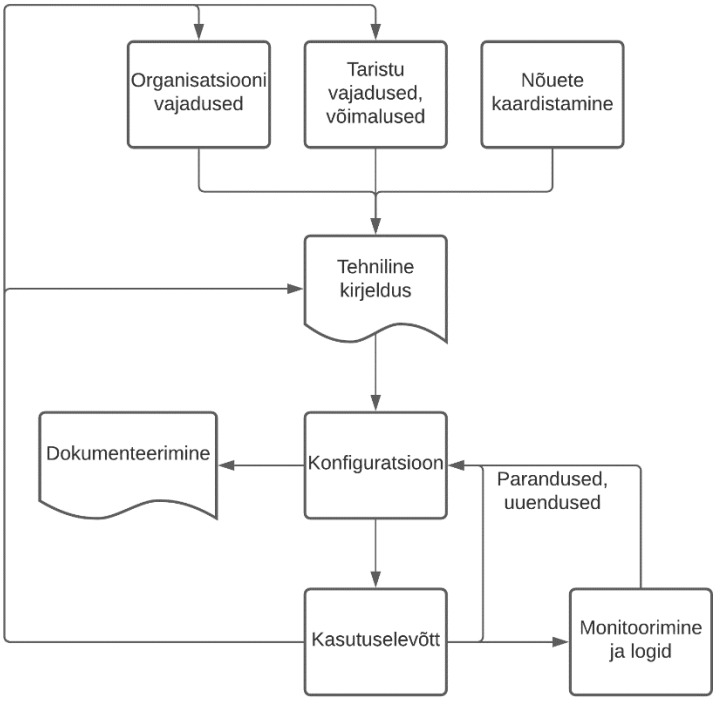
Vältimaks erinevaid versioone erinevatel andmekandjatel ja seega prinditud või salvestatud dokumentatsiooni aegumist, on autor kasutanud paberkandja ja välise mäluseadme asemel krüpteeritud pilve: *pCloud*, *MEGA*, *Personal Vault OneDrive*'s vms. Juurdepääs dokumentatsioonile peaks kindlasti olema mõnel teisel administraatoril või haridustehnoloogil ning asutuse või osakonna juhil - sedasi välditakse töötaja rivist välja langemise korral olulise info kaotamist. Kindlasti tuleb pidada ka versioonilogi – lihtsaimal juhul kasvõi muudatuste kuupäeva kirjeldusega iga dokumendi lõpus.

Tagamaks riknenud seadme võimalikult kiiret asendamist, tuleb talletada ja kaasaegsena hoida ka varukoopiat kõikide seadmete seadistustest. Võimalusel peaks see protsess olema automatiseeritud. Varukoopiad salvestatakse vaid administraatoritele ligipääsetavale võrgukettale.

4.8 Teostuse analüüs

Diplomitöö aluseks olev koolimaja valmib kahes etapis ning töö kirjutamise ajal on kasutuses vaid algkooli osa, mis moodustab umbes 1/3 kogu koolist. Sellest ja ka COVID-19 piirangutest tulenevalt ei ole võimalik analüüsida näiteks tulemüüri tegelikku koormust ja jõudlust, samuti leiavad tulevikus suure tõenäosusega täiendust sisu filtreerimise ja võrguliikluse piiramise reeglid. Eelarvest tulenevalt on hankimata ka jaotuskihi kommutaator(id) ja selle sõlme lisamine ning seadistus jääb järgmisesse eelarveperioodi.

Kogu protsessi võib kokku võtta, näitlikustada selliselt, nagu kujutatud Joonis 7. Läbi soovide, vajaduste ja nõuete jõuti võimalike lahenduste kirjeldamiseni, lahenduse väljaehitamiseni ning aja jooksul, kasutamise käigus toimub pidev parandamine, täiustamine ja ka lähteülesannete uuendamine, et neid saaks vajadusel taaskasutada juba paremas versioonis.



Joonis 7. Protsessi diagramm.

Kõik võrguseadmed on paigutatud nõuetekohaselt lukustatavates andmesidejaotlates asuvaisse lukustatavaisse seadmekappidesse, nende toited on tagatud puhvertoiteallikatega. Tehnosüsteemide juhtseadmed asuvad maja võrguseadmetest eraldi ruumides, samuti on nende võrguühendused eraldi VLAN-is, IP-aadressid antakse neile staatilised ja dokumenteeritakse. Kui vähegi võimalik, ühendatakse seade võrku kaabliga, vältides üksikuid, ühe süsteemi jaoks loodud Wi-Fi võrke.

Portide liiasus ja seega võrgu skaleeritavus jäi planeeritud piiresse, mõnevõrra kasvades, kuna suure tõenäosusega ei leia kõik projekteeritud ja ehitatud võrgupesad kasutust. Skaleeritavust suurendab ka hangitav jaotuskihi kommutaator.

Kommutaatorid on jaotatud kolme pinusse: vastavalt põhikool, algkool ja spordikeskus. Esialgne plaan seadistada pinud jaotlate kaupa oleks olnud vähem ülevaatlik, kuna igas jaotlas on 1-2 kommutaatorit, seega oleks pinude arv kasvanud ja lisanud haldusele keerukust. ISO OSI mudeli kolmandas kihis töötavad kommutaatorid annavad võimaluse teha tulevikus osa marsruutimisotsuseid enne tulemüüri (mis töötab ka marsruuterina) kui see peaks vajalikuks osutuma. Üks võimalik stsenaarium võiks olla seotud arvutiklassi võrgus liigutatava suuremahulise meediaga, olgu selleks siis virtuaal-reaalsuse lahendused või muu säärane paljusid kasutajaid ja suuri andmemahtusid hõlmav väljund.

Autori hinnangul tõstab võrgu jagamine VLAN-ideks oluliselt võrgu turvalisust ja aitab isoleerida neid ohtusid, mis on kas tulemüürist läbi pääsenud või asuvad perimeetris seespool. Võimalike haavatavate süsteemide arv viiakse selliselt miinimumini, samuti aitab segmenteerimine luua lihtsamaid ja täpsemaid reegleid ning vähendada haldamise keerukust.

Tulemüür kui turvalisuse ennetav osa on rakenduseteadlik, selles on aktiveeritud põhilised kaitsemehhanismid: DoS ja IPS. Samuti toimub elementaarne sisu filtreerimine: keelatud on vägivaldse ja ebasündsa sisuga veebilehtede ning ohtliku sisuga rakenduste laadimine. Nimetatud filtrites kasutatakse tootja vaikimisi määranguid, mida on võimalik aja jooksul täiustada – näiteks tuleb veenduda, et mainitud filtrid töötavad ka eestikeelse sisu korral. Kasutataval tulemüüril puudub sissetungi avastamise süsteem (ing. k *intrusion detection system, IDS*), mistõttu on kavas lisameetmena rakendada RIA pakutavat automatiseeritud seirelahendust *Suricata-4-all* [26]. VLAN-ide, nendevahelise liikluse ja DHCP serveri haldamine tulemüürist on mugav ja ülevaatlik. Tulemüüri reeglite ja marsruutimise seadistamisel tuleb veenduda, et töötaksid ka esialgu võib-olla tagaplaanile jäävad teenused nagu näiteks PXE-käivitus (ing. k *preboot execution environment, PXE boot*).

Wi-Fi signaal on kogu majas ühtlane, koridorides paiknevate pääsupunktide asukohtade muutmisega saab seda veelgi optimeerida, nagu näha ka Joonis 6-l. Paraku ei tööta valitud lahenduse puhul ideaalselt rändlus: probleem on nähtav reaalajaliste rakenduste puhul nagu näiteks (video)koosolekute ajal ringi liikudes. Lahenduseks oleks eraldi Wi-Fi kontrolleri lisamine, mis rändlust koordineeriks, kuid esmalt tuleb kasutuse käigus välja selgitada, kas see on probleem, mis segaks igapäevast kasutust.

Kasutajate lisandudes tuleb jälgida ka võimalikke MAC-aadresside juhuslikustamisest tulenevaid probleeme [27]. Ühelt poolt võiks eeldada, et peatükis 3.4 kirjeldatud põhjustel ei kasva klientseadmete hulk kuigi suureks, teisalt ei saa seda välistada.

Monitoorimislahendusena kasutatava PRTG tasuta versioon võimaldab kasutada kuni 100 andurit. Kasutades tarkvara pakutavaid seadmepõhiseid malle tundub see piirang esialgu väga kitsendav, kuid kui hoolega kaaluda, milliseid parameetreid iga seadme puhul jälgida soovitakse ja seega võib säärane piir aidata vältida infomüra teket ja hoida ülevaatlikkust.

Kõikide seadmete kellaaeg on sünkroniseeritud majasisese ajaserveriga, mis omakorda saab aja RIA ajaserverist.

5 Kokkuvõte

Infotehnoloogia on kiirest arenev valdkond, mistõttu tuleb selle ala inimestel end järjepidevalt uuenduste ja muutustega kursis hoida. Küberturvalisuse tagamine hõlmab endas tervikut: kasutajast, viirusetõrjest võrguseadmete ja teenusepakkujateni. Käesolevas töös on mainitud uusi tehnoloogiaid nagu WPA3 ja Wi-Fi 6, mis ei ole töö kirjutamise hetkel paljude kliendiseadmete poolt veel toetatud ja mille juurutamise kulud võivad olla ebamõistlikult suured (Tabel 6). Töö on koostatud dokumendina, mida autor koos meeskonnaga tulevikus täiustab, et iga järgmise projekti puhul oleks võrgu alustalad ühesugused, kuid kasutatav tehnoloogia ja lahendused ajakohased. Väga oluline on viia töö kooskõlasse äsja avaldatud Eesti infoturbestandardiga (E-ITS), mis on seni kasutusel olnud ISKE-st selgem, õhem ja Eesti digiriigi omadustele vastav ning vahetab 2024. aastaks ISKE täielikult välja [28].

Diplomitöö eesmärk oli defineerida konkreetse kooli vajadused, selgitada välja nõuded ja head tavad, millele kaasaegne arvutivõrk vastama peab ja vastavalt kogutud infole lahendus realiseerida. Töö kirjutamise hetkel on aktiives kasutuses vaid osa majast, kuid seni kogetu põhjal võib järeldada, et langetatud otsused nii VLAN-ide, Wi-Fi seadistuste, dokumenteerimise kui ka seadmete valiku osas on olnud asjakohased ning suuri probleeme ega intsidente tuvastatud ei ole.

Kasutatud kirjandus

[1] Rae vallavalitsus, "Rahvastik - Rae vald," 2020. [Online]. Available: https://www.rae.ee/rahvastik.

[2] S. Bhaumik and A. McGrath, "Differences between OM1, OM2, OM3, OM4, OS1, OS2 fiber optic cable nomenclatures," 2013. [Online]. Available: https://www.stl.tech/optical-interconnect-products/optical-fibre/pdf/Differences_between_OM1__OM2__OM3__OM4_.pdf.

[3] ARRIS Enterprises LLC, "Ruckus Enterprise Campus NetworkDesign Guide," 2019. [Online]. Available: https://webresources.ruckuswireless.com/pdf/other/campus-design-guide.pdf.

[4] HITSA, "Koolide kohtvõrkude ja kohtvõrguseadmete üldised," 2016. [Online]. Available: https://media.voog.com/0000/0034/3577/files/Seadmete_Dokumentatsioon_koolidele_HITSA_15042016.pdf.

[5] Cisco, "VLAN Best Practices and Security Tips for Cisco Business Routers," 2020. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1778-tz-VLAN-Best-Practices-and-Security-Tips-for-Cisco-Business-Routers.html.

[6] BSI, "M 5.62z Sobiv loogiline segmenteerimine," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M5/M_5.62.

[7] BALTIC COMPUTER SYSTEMS AS, "Windowsi-põhiste kohtvõrkude turbe juhend," 2019. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/windowsi_pohiste_kohtvorkude_turbe_juhend_0.pdf.

[8] OIXIO AS, "Avalik kohtvõrk ja WiFi," [Online]. Available: https://www.ria.ee/sites/default/files/avalikkohtvorkjawifi_avalikuks.pdf.

[9] B. Donohue, "Full Disk Encryption by Default in Android Lollipop - more secure than ever. | Kaspersky Official blog," 2014. [Online]. Available: https://www.kaspersky.com/blog/full-disk-encryption-android-5/6423/.

[10] H. Pook and N. Paju, "Eesti kohaliku omavalitsuse IKT taristu miinimumnõuded," 2017. [Online]. Available: http://kov.riik.ee/wp-content/uploads/2017/08/Eesti-kohaliku-omavalitsuse-IKT-taristu-miinimumn%C3%B5uded-vers-5.pdf.

[11] T. Kangru, "Kindluse Kool Objekt 01. Koolimaja Elektripaigaldis. Album 03. Nõrkvool. Tööprojekt," 2020.

[12] BSI, "M 1.43 Võrgu aktiivkomponentide turvaline paigutus," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M1/M_1.43.

[13] BSI, "M 1.58 Tehnilised ja organisatsioonilised nõuded serveriruumidele," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M1/M_1.58.

[14] nVent, "BEND RADIUS OVERVIEW REFERENCE SHEET," [Online]. Available: https://www.erico.com/catalog/literature/F1275W-NAEN.pdf.

[15] BSI, "M 1.28 Puhvertoiteallikas," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M1/M_1.28.

[16] Riigi Infosüsteemi Amet, "RIA aastaraamat 2020," 2020. [Online]. Available: https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb_0.pdf.

[17] "Kindluse kooli kodukord," [Online]. Available: https://kindlusekool.ee/wp-content/uploads/2021/03/KINDLUSE-KOOLI-KODUKORD-kehtiv-versioon-05.03.2021.pdf.

[18] "Järveküla kooli kodukord," [Online]. Available: https://jarvekyla.edu.ee/wp-content/uploads/2018/09/JK_kodukord_6.09.2018-4.pdf.

[19] BSI, "M 2.70 Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M2/M_2.70.

[20] "Sizing Guidelines Sophos XG Firewall - XG Series Appliances," [Online]. Available: https://www.enterpriseav.com/datasheets/sophos_xg_series_sizing_guide_sgna.pdf.

[21] Cisco, "High Availability Campus Network Design--Routed Access Layer using EIGRP or OSPF," 2008. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/routed-ex.html.

[22] M. Eisen, "Introduction to PoE and the IEEE802.3af and 802.3at Standards," 2009. [Online]. Available: https://www.ieee.li/pdf/viewgraphs/introduction_to_poe_802.3af_802.3at.pdf.

[23] Sophos, "Sophos XG Firewall: How to prevent DoS and DDoS attacks," 2020. [Online]. Available: https://support.sophos.com/support/s/article/KB-000035754?language=en_US.

[24] BSI, "M 2.25 Süsteemi konfiguratsiooni dokumenteerimine," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M2/M_2.25.

[25] BSI, "M 2.139 Olemasoleva võrgukeskkonna läbivaatus," [Online]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M2/M_2.139.

[26] RIA, "RIA tegevused küberturvalisuse parandamisel," 2019. [Online]. Available: https://www.ria.ee/et/kuberturvalisus/kuberturvalisus-2019/ria-tegevused-kuberturvalisuse-parandamisel.html.

[27] S. D. Wes Purvis, "Get to know MAC Address Randomization in 2020," [Online]. Available: https://www.mist.com/get-to-know-mac-address-randomization-in-2020/.

[28] RIA, "RIS infokiri märts 2021," 2021. [Online]. Available: https://www.ria.ee/et/riigi-infosusteem/infokiri/ris-infokiri-marts-2021.html.

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Madis Võrklaev

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Kohtvõrgu lahendus põhikooli näitel“, mille juhendaja on Edmund Laugasson
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

15.05.2021

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.