HITSA
Hariduse Infotehnoloogia Sihtasutus

Üldhariduskoolide digitaristu kaasajastamine

Koolide kohtvõrkude ja kohtvõrguseadmete üldised nõuded

15.04.2016

HITSA

Sisukord

Sissejuhatus

Koolide info- ja kommunikatsioonitehnoloogia (IKT) põhiste õppevaralahenduste kasutamiseks on vajalik, et koolide IKT-taristu oleks piisav. Kui suurendatakse koolide internetiühenduse kiirust, siis ei tohi ära unustada ka koolides oleva kohtvõrgu kaabelduse ja seadmete kaasajastamist. Iirimaa koolidele 100 Mbit/s Interneti ühenduse pakkumise projektist[1] on selgunud, et koos koolide Interneti ühenduse parandamisega on vaja korda teha ka kohtvõrgud, mille tehnoloogiline mahajäämus ja halb konfiguratsioon on põhjuseks, miks ei saa koolis kasutada 100 Mbit/s ühendust täiel määral.

Käesolevas dokumendis on välja toodud kooli kohtvõrgu kaasaegsete ja tulevikku vaatavate komponentide nõuded. Hetkel on loetletud nõuded üldised, ent täpsemad nõuded pannakse paika programmi hilisemates hankedokumentides. Koolide kohtvõrkude üldised nõuded põhinevad HITSA dokumendil „Soovitused koolide ja lasteaedade IKT taristu väljaehitamiseks või renoveerimiseks"[2]. Lisaks on kasutatud Sloveenia, Iiri ja Portugali akadeemiliste võrkude kogemusi. Ameerika Ühendriikide haridusministeerium on välja töötanud dokumendi *„Future Ready Schools: Building Technology Infrastructure for Learning*"[3], milles antakse üldised soovitused koolidele IKT-taristu kaasajastamiseks ning mis on hea ülevaade valdkonnast.

Põhimõtted

Käesoleva nõuete eesmärgiks on kasutada võimalikult palju tööstusstandardite (*industry standard*) parimatele tavadele põhinevaid IT taristu komponente ja metoodikaid. Kavandatavad tsentraalselt (kaug)hallatavad lahendused vähendavad lokaalse inimtööjõu vajadust, mis on kõige suurem kulukomponent võrguseadmete ekspluatatsioonil. Võrgutõrgete lahendamine peab olema operatiivne ja andma õpetajatele kindluse igapäevatöö tegemiseks.

Nõuete väljatöötamisel on silmas peetud seda, et kavandataval võrgulahendusel oleks valmidus kasutusele võtta VOSK („võta oma seade kaasa", ingl k BYOD ehk *Bring Your Own Device*), mis võimaldab õpilastel kasutada õppetööks enda isiklikku nutiseadet[4] .

Lõppseadmete ühendamine kohtvõrku

Töökohtades, kus asub lauaarvuti, millel puudub Wi-Fi tugi, tuleb kasutada kaabeldatud ühendust.

---

[1] „Schools 100 Mbit/s Project" http://www.heanet.ie/schools/schools-100-mbits-project
[2] „Soovitused koolide ja lasteaedade IKT taristu väljaehitamiseks või renoveerimiseks" https://www.innovatsioonikeskus.ee/sites/default/files/IT%20juhtimine/KoolideIKTtaristu_soovitused.pdf
[3] „Future Ready Schools: Building Technology Infrastructure for Learning" http://tech.ed.gov/wp-content/uploads/2014/11/Future-Ready-Schools-Building-Technology-Infrastructure-for-Learning-.pdf
[4] „Future Ready Schools: Building Technology Infrastructure for Learning"

Õpilaste kaasaskantavate arvutite ja nutiseadmete jaoks on ainetundides mõistlik kasutada traadita võrgu (Wi-Fi) ühendust, mis võimaldab õpetajal kasutada erinevaid digitaalõppe vorme. Lisaks on tõenäoline, et õpilase peamiseks töövahendiks ainetundides kujuneb nutiseade, millel puudub kohtvõrgu ühendus. Statsionaarne arvutiklass või muu konkreetse otstarbega, lauaarvuteid kasutav aineklass on mõistlik ühendada täies mahus füüsilise kaabliga. See tagab suure hulga seadmete puhul, stabiilsema ühenduse ja võimsusvaru mahukate multimeedia failide mängimisel.

Elektritoide

Suures mahus IKT vahendite soetamisel on oluline üle kontrollida hoone elektripaigaldiste olukord ning peakaitse võimsusvaru. Vanemates koolides, kus elektripaigaldised on üle paarikümne aasta vanad, ei ole tõenäoliselt arvestatud nii suurte koormustega ning see võib osutuda oluliseks takistuseks tehnoloogia laiaulatuslikul kasutamisel. Wi-Fi pääsupunktide puhul on vajalik PoE-tugi (*Power-over-Ethernet*), mille jaoks ei ole tarvis paigaldada eraldi elektritoidet. Võimaluse korral tuleb kasutada kesksetel võrguseadmetel UPS-toidet, mis silub ära lühiajalised elektrikõikumised.

Seadmete hankimisel on tähtis üldiste nõuete juures välja tuua, et kõik seadmed peavad töötama Eesti vooluvõrgus (230V), vältides hilisemaid ühilduvusprobleeme.

Võrguseadmed

Kommutaator (switch)

Kommutaator on arvutivõrgu aktiivseade, mille abil luuakse ühendused erinevate lõppseadmete (arvutid, server jne) ning internetiühendust pakkuva seadme vahel. Kommutaator peab olema hallatav ning võimaldama kohtvõrku segmenteerida erinevateks levipiirkondadeks, kasutades virtuaalseid kohtvõrke (VLAN). Segmenteerimine, koostöös marsruuteri/tulemüüriga, võimaldab võrgutopoloogias rakendada erinevaid turvapoliitikaid, muutes edastatava võrguliikluse paremini hallatavaks ning turvalisemaks.

Kommutaatori kõik liidesed peavad toetama 1 Gbit/s (1000 Mbit/s – *Gigabit Ethernet*) ühendusi ning vajadusel ka tagasiühilduvalt 100 Mbit/s ühendusi (10/100BASE-T). Kui on vaja kommutaatoreid omavahel ühendada, siis peaks vajadusel kasutama 10 Gbit/s liideseid (SFP+), luues seadmete vahelise magistraalvõrgu, mis suudaks teenindada kasvavat andmeside mahtu. Seadmete soetamisel tuleb arvestada portide arvu 15-25% liiasusega.

Wi-Fi ühenduse pääsupunkte (*access point*, AP) teenindavate kommutaatorite korral tuleb valida seadme mudelid, mis toetavad PoE (*Power-over-Ethernet*) tehnoloogiat. PoE on tehnoloogia, mille abil on võimalik lõppseadmete elektritoide saada läbi Ethernet kaabli ühenduse. Seda kasutatakse näiteks pääsupunktide, turvakaamerate, VoIP telefonide jne seadmete elektritoite lahendusena. PoE standardit peab toetama sel juhul nii kommutaator kui ka vastav lõppseade. Oluline on tähele panna, et turul on kahe erineva standardiga tooteid IEEE 802.3af (nn PoE) ja IEEE 802.3at (nn PoE+), mis pakuvad erinevaid võimsusi ning ei ole täies mahus omavahel ühilduvad. Enne ostmist on soovitav seda eelnevalt testida, et vältida hilisemaid ühilduvusprobleeme. Paljud IEEE 802.11ac (traadita võrgu standard) võimekusega tugijaamad nõuavad täisfunktsionaalsus töötamiseks tänapäeval 802.3at (PoE+) tuge, mis peab võimaldama kommutaatori ühest võrguliidesest edastada 25,5W võimsusega elektritoidet.

Voolutarbimise poole pealt soovitame valida kommutaatorite mudelid, mis võimaldavad luua ajalisi seadistusprofiile. Sellega on võimalik näiteks ööseks voolu tarbivad seadmed (Wi-Fi tugijaamad, VoIP telefonid jne) automaatselt välja lülitada või nende voolutarbimist piirata.

1. <u>Üldised nõuded</u>
   - 1.1. Allalink liideste arv vähemalt 24 x 10/100/1000BASE-T ehk *Gigabit Ethernet* (*full duplex*)
   - 1.2. Üleslink liideste arv vähemalt 2x 10G SFP+ (1G/10G *dual speed*)
   - 1.3. Seadmega peavad kaasas olema SFP+ moodulid (vähemalt 2tk) koos *single-mode* kiudoptiliste kaablitega, aktiivseadmete omavaheliseks ühendamiseks või optikapaneeliga (LX andmepesad) ühendamiseks
   - 1.4. Seadmega peavad kaasas olema seadmekappi kinnitamistarvikud (racki kinnitused)

1.5. Kommutaator, mille külge ühendatakse tugijaamad peab olema kas PoE või PoE+ võimekusega ning tagama tugijaamade, 802.11ac mudelite, täisfunktsionaalsuses töötamise
  1.5.1. PoE(IEEE 802.3af) liidestega kommutaator peab 15,4W võimsusega suutma varustada korraga kõiki kommutaatori allalink liideseid
  1.5.2. PoE+ (IEEE 802.3at) liidestega kommutaator peab 25,5W võimsusega suutma varustada korraga vähemalt pooli (50%) kommutaatori allalink liideseid
1.6. Kommutaatorite PoE või PoE+ toega seadmemudelid tuleb valida selliselt, mis võimaldaks vooluga varustada kõiki kooli ruumidesse paigaldatavaid tugijaamu korraga

2. Tehnilised nõuded

2.1. Toetatud STP (täispuu protokoll) režiimid: RSTP/MSTP/PVRST
2.2. QoS tugi
2.3. Edastamise ja kommuteerimise võimekuse parameetrid peavad vastama tabelis toodud andmetele, vastavalt pakutava kommutaatori mudelile:

Liideste arv	Kommuteerimise võimekus vähemalt (Gbps)	Edastamise võimekus vähemalt (Mpps)
24 GbE + 2 SFP+	88	65,5
48 GbE + 2 SFP+	136	101,2
24 GbE + 4 SFP+	128	95,2
48 GbE + 4 SFP+	176	130,9

2.4. IPv6 tugi
2.5. SNMPv3 ja SYSLOG tugi
2.6. LLDP ja LLDP-MED tugi

3. Liideste võimekus

3.1. VLAN(802.1q) tugi
3.2. Dünaamiline VLAN-i määramine
3.3. Liideste põhine VoIP teenuse VLAN-i (*Voice* VLAN) tugi
3.4. Portide ja VLAN liideste peegeldamisvõime võrguliikluse analüüsimiseks
3.5. Liideste agregeerimine (LACP)
3.6. Eraldi füüsiline haldusliides (RJ-45 - *Ethernet*) ehk *out-of-band management*

4. Turvalisus

4.1. RADIUS tugi
4.2. 802.1X tugi
4.3. Privaatsete VLAN-de tugi
4.4. Ligipääsu piiramine L2 ja L3 taseme pääsupiiramisloenditega (ACL)
4.5. Liidesepõhine turvalisus (*Port Security*)
4.6. DHCP *snooping*
4.7. Dünaamiline ARP kontroll

5. Lisa nõuded keskses seadmeruumis asuvatele kommutaatoritele

5.1. Topelt toiteplokk
5.2. Kuumvahetatav toiteplokk
5.3. Kuumvahetatav ventilaatormoodul
5.4. Pinu võimekus (*stacking*)

Tulemüür

Tulemüür (*firewall*) on oluline organisatsiooni IKT turvapoliitikate rakendamise objekt. Selle abil saab lubada ja keelata erinevaid tegevusi kooli sisevõrgu või erinevate sisevõrkude ning avaliku interneti vahel. Tulemüüris on võimalik jälgida liiklust, samuti on võimalik peatada erinevaid rünnakuid, kas automaatselt, erinevate tüüpreeglite kirjeldamise kaudu või käsitsi, reageerides tulemüüri kasutajaliidese kaudu konkreetsele olukorrale. Tulemüüri eesmärgiks on kasutajate kaitsmine nii kohtvõrgust, kui ka Internetist tulevate rünnete ja tarkvaraliste nõrkuste (*vulnerability*) eest.

Koolide võrkudes võib tulemüür olla ka osa marsruuterist (marsruuter ühendab omavahel kaht või enamat võrgusegmenti).

Soovituslik on kasutada rakenduste teadlikku tulemüüri (*application layer firewall*), mis võimaldab turvapoliitikate seadistamist ning võrguliikluse piiramist, vastavalt kasutatavatele rakendustele või seadmetele. Lisaks sellele peab olema toetatud ka standardne olekufiltriga tulemüüri võimekus (*stateful inspection firewall*), mis jälgib vahendatavate võrguühenduste olekut, tuvastades paketid, mis kuuluvad algatatud ühendusse ning avavad ja sulgevad selle liikluse jaoks vajalikke porte.

Tulemüürilahendus peab toetama täies mahus IPv4 protokolli ja seadmest läbikäivast liiklusest, IPv6 protokolli.

Seadme mudel tuleb valida selliselt, mis suudaks teatava varuga teenindada kõiki kasutajaid. Mudeli valikul on põhilisteks parameetriteks tulemüüri maksimaalne läbilaskevõime ehk andmeedastuskiirus, mis näitab kui suurt hulka andmeid suudab seade ühes ajaühikus teenindada ning maksimaalne ühenduste arv, mis näitab üheaegsete andmesideühenduste arvu (nt üks veebilehe külastus võib tekitada mitusada ühendust korraga). Osadel tootjatel on kodulehel välja toodud ka soovitatav kasutajate arv, mis hõlbustab seadmemudeli valikut. Tähtis on arvestada ka liideste arvu ja tüüpi, millesse ühenduvad kommutaatorid ja välisühendust pakkuv teenusepakkuja seade/kaabel.

Tulemüüri ligipääsureeglite ning marsruuteri funktsionaalsuse seadistamine ja haldamine nõuab väga spetsiifilist IT kompetentsi ning soovituslik on seda teenust hankida ettevõtetelt, kes on sellele valdkonnale spetsialiseerunud. Tagamaks terviklahenduse kvaliteeti on soovituslik valida lahenduse pakkuja selliselt, kes oleks seadmete tootjate kohalik ametlik partner ning omab vastavat tehnilist spetsialiseerumist pakutavatele toodetele.

1. <u>Üldised nõuded</u>
   - 1.1. Liideste arv vähemalt 6x 10/100/1000 ehk *Gigabit Ethernet*
     - 1.1.1. Seal hulgas vähemalt 2x SFP või SFP+ liidest
   - 1.2. SFP/SFP+ liideste puhul peavad olema seadmega kaasas vastavad moodulid ja kaablid, ühendamiseks
   - 1.3. Seadmega peavad kaasas olema seadmekappi kinnitamistarvikud (racki kinnitused)

1.4. Seadme mudelid jaotuvad kolme kategooriasse ning peavad olema valitud vastavalt kooli õpilaste arvule:

Mudel	Soovitatav kasutajate arv	Tulemüüri võrguliikluse läbilase (rakenduse teadlikkusega – L7)	Uute ühenduste arv ühes sekundis	Tulemüüri üheaegsete ühenduste arv
1	25 - 110	Vähemalt 300 Mbps	Vähemalt 8 000	Vähemalt 250 000
2	Vähemalt 500	Vähemalt 650 Mbps	Vähemalt 12 000	Vähemalt 500 000
3	Vähemalt 1500	Vähemalt 1 Gbps	Vähemalt 30 000	Vähemalt 750 000

1.5. Tagatud töökindlus vähemalt 35˚C temperatuuri juures

2. Tehnilised nõuded

2.1. Sisemine kõvaketas vähemalt 64GB
2.2. Paketisalvestus analüüsitarkvara (nt *Wireshark*) formaati
2.3. Võimalus luua virtuaalseid kohtvõrgu alamliideseid vähemalt 100
2.4. Sissehitatud DHCP server erinevatele võrkudele
2.5. NAT tugi (1:1 NAT, pordipõhine NAT)
2.6. QoS tugi
2.7. IPv6 tugi
2.8. Võrguliikluse sessioonide arvu piiramine või ribalaiuse piiramine (*traffic shaping*)

3. Turvalisus nõuded

3.1. IPSec VPN (AES) tunnelite arv vähemalt 100
3.2. Kliendipõhine VPN (*remote access* VPN)
3.3. Rakenduseteadlikus ning võimalus seadistada rakendusepõhiseid (*Facebook, Youtube*, jm.) ligipääsureegleid
3.4. Sisupõhine filtreerimine
3.5. URL-i mustrite ja kategooriate põhine filtreerimine
3.6. Grupipõhiste turvapoliitikate rakendamine
3.7. Võimalus tuvastada pahavara (teenuse aktiveerimine ja litsentseerimine ei ole nõutud)
3.8. Võimalus tuvastada ja ennetada ründeid (teenuse aktiveerimine ja litsentseerimine ei ole nõutud)

Traadita võrk (Wi-Fi)

Traadita võrk on viimase 5 aastaga kujunenud üheks peamiseks kasutatavaks teenuseks. Wi-Fi on muutunud õppetöös vajalikuks teenuseks, seda nii digitaalõppe populaarsemaks muutumise, kui ka informatsiooni kättesaadavuse seisukohast. Traadita andmeedastuskiirused on tehnoloogilise arenguga jõudnud ajajärku, kus Wi-Fi tugijaamad suudavad edastada kiirused üle 1 Gbit/s (IEEE 802.11ac). Selline olukord seab suuremat rõhku ka kogu andmeside võrgu baastaristule, mis peab kasvavat andmeside mahtu olema suuteline teenindada.

Planeerides uut Wi-Fi võrku on oluline arvestada lisaks levikattuvusele ka järjest kasvavat nutiseadmete ja kasutajate arvu ning teenustega, mida võrgus plaanitakse kasutada.

Koolide puhul on tegemist suure tihedusega kasutajate keskkonnaga, mis tähendab, et kasutajate arv klassiruumides või üldkasutatavates ruumides(koridorid, aulad) on keskmise kontori Wi-Fi lahendusega võrreldes suurem. Seda tuleb arvestada ka tugijaamade mudelite valikul, kuna seadmed peavad olema võimelised sellise kasutajate arvuga töötama.

Traadita võrgu turvalisus

Koolide traadita võrgus peavad kasutajad olema autenditud. Kooli õpilaste, õpetajate ja töötajate autentimiseks tuleb kasutada eduroam'i, mille korral on iga kasutaja nimeliselt autenditud. Kasutajatel on rollipõhised ligipääsuõigused ja edastuskiiruse piirangud, mis on seotud kasutaja identiteediga. eduroam'i rakendamisel on mõistlik rakendada kasutajate halduslahendust (*Active Directory*, LDAP, HarID). Kasutajate autentimiseks saab kohtvõrkudes kasutada prokokolli 802.1X, ehk kommutaatoritel peab olema kõigil portidel prokokolli 802.1X tugi. eduroam'i teenuse täpsemad tingimused on kirjeldatud eduroami kodulehel dokumendis „*eduroam Compliance Stanement*"[5].

Kooli külalistele on vaja pakkuda „külaliste võrku", et inimesed kellel ei ole *eduroam'i* kontot saaksid vajadusel kasutada Wi-Fi võrku. Sellisel võrgul on kooli sisesest võrgust rangemad piirangud: näiteks saavad nad vaadata ainult veebilehti, ent koolitöö ajal voogedastust kasutada ei saa, kuna selle edastamine tarbib liialt võrguressurssi. Kasutada võib ka soovitusi dokumendi „Avalik kohtvõrk ja Wi-Fi. Valdkonnakäsitlus, mõisted, nõuded ja soovitused"[6] punkti 2.1.1.2 järgi.

[5] „eduroam Compliance Statement" https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf
[6] „Avalik kohtvõrk ja WiFi. Valdkonnakäsitlus, mõisted, nõuded ja soovitused"
https://www.mkm.ee/sites/default/files/avaliku_kohtvorgu_soovituslik_juhend_0.pdf

Andmeside pesade paigaldus Wi-Fi tugijaamadele

Kohtvõrgu kaabeldus on planeeritud projekti esimesse tööde etappi ning peab toimuma enne Wi-Fi leviala kaardistust. See tekitab probleemi, kus tugijaamade jaoks vajalikud andmeside pesad tuleb paigaldada enne seda, kui on teada täpsed tugijaamade asukohad.

Lahendusena antud probleemile, võib planeerida lisa andmeside pesa(d) kõigisse klassiruumidesse, mis võimaldab pesasse ühendatud tugijaama, vahekaabli pikkuse võrra enda asukohas liigutada, leidmaks selle optimaalne asukoht. Lisaks sellele saab korruseplaanide järgi hinnata eeldatavat tugijaamade asukohta ka teistes üldkasutatavates ruumides (nt koridorid, aulad ja teised üldkasutatavad ruumid).

Selline lahendus ei tekita kaabeldustöödes märgatavaid lisakulutusi, kui plaanitakse traadita võrku 802.11ac kiiruste saavutamiseks suure tihedusega kasutajate keskkonda, kuna vajalik Wi-Fi leviala nõuab keskmiselt ühte tugijaama 1,2 klassiruumi kohta[7]. Täpsemalt on kaabeldustöödega seotud teemad kirjeldatud dokumendis „Koolide digitaristu kaasajastamine – Kohtvõrgu kaabeldustööd“, mis on kättesaadav HITSA kodulehelt.

Traadita võrgu planeerimine

Traaditavõrgu ehk Wi-Fi võrgu planeerimine on tegevus, mille raames teostatakse hoonepõhine mõõdistamine, selgitamaks välja tugijaamade arv, mida on vaja, et katta kogu hoone kvaliteetse Wi-Fi levialaga. Arvesse võetakse hoone ehitust ning ehituslikke eripärasid, mis võivad takistada leviala ulatust (vaheseinade materjal, ripplaed ja ruumide asetus).

Wi-Fi kaardistamisel võetakse aluseks koolide poolt edastatud hoonete korruseplaanid.

Wi-Fi kaardistamise väljundiks on põhjalik raport koos leviala kaartidega, mis on koostatud traadita võrgu mõõdistustele spetsialiseeritud tarkvaraliste vahenditega (nt *Ekahau Site-Survey and Planning Tool* tarkvaraga).

Selle põhjal saab teada tugijaamade arvu ning kommutaatorite arvu, mida läheb vaja tugijaamade vooluga varustamiseks (PoE toega kommutaatorid).

1. Tehnilised tingimused Wi-Fi planeermine
   - 1.1. Kaardistus teostatakse samade tugijaama mudelitega, mida hiljem paigaldatakse
   - 1.2. Teostatakse 802.11ac (5GHz) leviala kaardistus
   - 1.3. Kaardistus peab sisaldama ka 802.11b/g/n (2,4 GHz) mitte-kattuvate kanalite jaotust
   - 1.4. Klassiruumis peab olema tagatud Wi-Fi kohtvõrkvõrgu liikluse *half-duplex* läbilaskevõime, summeritult kasutajate peale, vähemalt 130 Mbps, ühe tugijaama piires
     - 1.4.1. Testitavad tugijaamad peavad töötama, testi tulemustele vastavalt, ka 60 üheaegselt tugijaama külge ühendatud kasutajaga
     - 1.4.2. Läbilaske test tehakse nii TCP kui UDP liiklusega
     - 1.4.3. Läbilaske test tehakse eraldi nii üles- kui allalaetava liiklusega (*download* ja *upload*)

[7] „Schools Wi-Fi Buyer’s Guide“ http://buyersguide.educationsuperhighway.org/learn/wireless/hardware

1.4.4. Läbilaske test tehakse, kasutades 5GHz sagedusvahemikus vähemalt ribalaiust 40MHz
1.4.5. Läbilaske test peab sisaldama ka 2,4GHz kliente ning näitama tugijaama *dual band (2,4GHz ja 5GHz samaaegne kasutamine)* võimekust

1.5. Tugijaamade arvu, mudeli ja asukohtade planeerimisel tuleb arvestada, et kasutajate arv suurematesüldkasutatavates ruumides (koridorid, aulad) võib olla üle 300 (kasutajakoormuse hajutamiseks tuleb paigaldada nendesse ruumidesse mitu tugijaama).
1.6. Kaardistamisel tuleb tugijaama asukohtade planeerimisel arvesse võtta, et traadita võrku hakatakse kasutama nutiseadmetega ning tavaliseks veebi liikluseks (*Data*) liikluseks.
1.7. Tugijaamade asukohad peavad olema valitud selliselt, mis ei takistaks Wi-Fi levi kiirgamist (nt. ei tohi olla paigaldatud veetorude vahele).
1.7.1. Tugijaamade arv peab olema minimaalne, et saavutada nõutud levikattuvus ja liikluse läbilaskevõime;
1.7.2. Tugijaamade asukoht ei tohi olla õpilaste või õpetaja töökohale lähemal, kui 3 meetrit
1.8. Tugijaamade asukohad märgitakse hoone korrusekaartidele
1.9. Tugijaamade asukohast tehakse foto, mis lisatakse raportisse, viitega tugijaama asukohale korrusekaardil.
1.10. Kaardistus ja testimine peab olema dokumenteeritud ning tulemused esitatud raportina
1.11. Raport peab olema koostatud Wi-Fi mõõdistustele spetsialiseeritud tarkvaraliste vahenditega (nt *Ekahau Site-Survey and Planning Tool*) ning sisaldama tugijaamade asukohti hoone korruste kaartidel, fotosid tugijaamade paigaldatavast asukohast, leviala kaarte.
1.12. Mõõdistustulemused (kiiruse läbilaske testid) peavad olema dokumenteeritud ning sisaldama mõõdetud TCP/UDP kiiruseid, mõõtmiseks kasutatud tugijaamade ja klientide loetelu
1.13. Raport koos mõõdistustulemustega esitatakse digitaalsel kujul (PDF ja originaal failid) tellijale.

Traadita tugijaamad (*access points*)

Traadita võrgu (Wi-Fi) pääsupunkt ehk tugijaam (*access Point*, AP) on seade, mis võimaldab juhtmevaba juurdepääsu kohtvõrgule ja seeläbi ka Internetile. Pääsupunktide valimisel on oluline IEEE 802.11 n/ac standardite tugi, sest siis on tagatud piisav edastuskiirus kasutajate rakendustele ja parem Wi-Fi võrgu katvus ning kvaliteet. Tugijaamad peavad toetama ka vanemate standarditele 802.11 a/b/g vastavaid seadmeid.

Oluline tehnoloogiline nõue pääsupunkti juures on 2.4 GHz ja 5 GHz sagedusala samaaegne kasutus. See tagab suurema kliendiseadmete arvu sama pääsupunkti levialas ning madalamal andmevahetuskiirusel (802.11 a/b/g) töötavad seadmed ei mõjuta nii palju uute, kiiremat andmeedastuse standardit (802.11 n/ac) kasutavate seadmete kiirust. Kuna kooli Wi-Fi kasutajate seadmepark on mitmekesine, annab selline lisavõimalus olulise eelise. Oluline on, et pääsupunktid suunaksid kliendiseadmed kasutama sagedusala (*band steering*) 5 GHz.

Suurema arvu pääsupunktide haldamiseks on soovituslik kasutada keskset halduslahendust (kontrolleri põhine lahendus). Keskne haldus võimaldab ühest kesksest kohast (mitte igast

tugijaamast eraldi) hallata tugijaamade seadistust, turvapoliitikaid, teostada veatuvastust ning tarkvara uuendusi. Osade tootjate tugijaamadesse on selline võimekus sisse ehitatud ning ei nõua lisa riistvaralist/tarkvaralist komponenti.

1. Üldised nõuded
   - 1.1. Seadmega peavad kaasas olema seinale ja lakke kinnitamiseks vajalikud tarvikud
   - 1.2. Tugijaam sobima paigaldavasse keskkonda, nii väljanägemiselt kui võimekuselt
   - 1.3. Riistvara garantii vähemalt 5 aastat

2. Tehnilised nõuded
   - 2.1. IPv6 tugi (kasutajate poolne)
   - 2.2. QoS WMM tugi
   - 2.3. Võimalus seadistada rakendusepõhiseid liiklusmahu piiranguid
   - 2.4. Rändlusprotokollide 802.11k ja 802.11r tugi
   - 2.5. PoE+ (IEEE 802.3at) või PoE (IEEE 802.3af) tugi
     - 2.5.1. PoE (IEEE 802.3af) toide ei tohi piirata tugijaamas 802.11ac võrgu funktsionaalsust ega andmeedastuskiiruseid
   - 2.6. 802.1Q VLAN tugi
   - 2.7. Vähemalt 5 SSID tugi
   - 2.8. Kliendi põhine koormuse hajutamine erinevate tugijaamade vahel (*Client/ AP load balancing*)
   - 2.9. Vähemalt 1x 10/100/1000 ehk *Gigabit Ethernet* liides
   - 2.10. Auto MDI/MDIX tugi
   - 2.11. Tugijaam on täielikult hallatav kesksest haldusplatvormist
   - 2.12. Võimekus jätkata töötamist haldusplatvormiga ühenduse katkemisel

3. Raadio nõuded
   - 3.1. 2,4 GHz 802.11 b/g/n tugi
   - 3.2. 5 GHz 802.11 a/n/ac tugi
   - 3.3. Klientide teenindamine korraga mõlemal sagedusvahemikul (2,4GHz ja 5 GHz - *dual band*)
   - 3.4. Vähemalt 802.11 ac wave 1 tugi
   - 3.5. 256-QAM digitaalne modulatsioon
   - 3.6. Vähemalt 2X2:2 MIMO (2 spacial streams)
   - 3.7. Signaalitee valik (*Band Steering* või samaväärne funktsionaalsus)
   - 3.8. Levisignaali kliendipõhine suunamine (*Beamforming* või samaväärne funktsionaalsus)
   - 3.9. EU raadiosageduste tugi
   - 3.10. Sisemiste antennidega mudel
   - 3.11. Dünaamiline saatevõimsuse kohandamine (RRM)
   - 3.12. Dünaamiline sagedusvahemiku valimine (DFS)
   - 3.13. MU-MIMO tugi tugijaamadel, mis paigaldatakse aulatesse või sarnastesse üldkasutatavatesse ruumidesse, kus üheaegsete kasutajate arv on kõrge
   - 3.14. Võimalus kasutada 20, 40 ja 80 MHz kanaleid 5GHz sagedusvahemikus
   - 3.15. Sisseehitatud spektrianalüsaator

4. Turvalisus nõuded
   - 4.1. Külaliskasutajate veebiportaali (*Captive portal*) loomise võimalus
   - 4.2. WPA2 AES tugi
   - 4.3. 802.1X tugi
   - 4.4. RADIUS tugi (eduroam isikutuvastusteenuse tugi)
     - 4.4.1. RADIUS funktsionaalsus peab vastama *eduroam Compliance Statement* dokumendis kirjeldatud tingimustele (https://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf)
   - 4.5. 802.1i tugi

4.6. Kliendi andmeside liikluse kiiruse piiramine
4.7. Rakendusepõhine andmeside liikluse piiramine
4.8. Integreeritud sissetungi vältimise süsteem (wIPS)
4.9. Võõraste tugijaamade tuvastus
4.10. Võimekus kasutada erinevaid autentimismeetodeid erinevatel SSID-l

Haldusmudel

IKT lahendused muutuvad järjest mitmekesisemaks ning keerukamaks. Asutuste IT meeskonnad seisavad keeruliste probleemide ees hallata kiiresti kasvavat kasutajate, seadmete, keskkondade ja teenuste hulka. Täna on suureks probleemiks asutustes väga erinev IT teadmiste kompetents ja piisava meeskonna puudumine. See ei pruugi tagada kooli kohtvõrkudes piisavat turvalisust, standardile vastavat kohtvõrgu topoloogilist ülesehitust ja seadmete hallatavust. Koolide digitaristu kaasajastamise projekti üheks eesmärgiks on viia kooli kohtvõrgud sellisele tasemele, mis vastaks tänapäeva turvalisuse standarditele, oleks jätkusuutlik ning kergesti laiendatav.

Halduskoormuse vähendamiseks on soovitatav kohtvõrgu haldus, teenusena väljast poolt hankida.

Juhendis kirjeldatud lahendus võimaldab rakendada keskset haldusmudelit, mis võimaldab koolidesse paigaldatavaid seadmeid hallata ühest kesksest punktist (väline andmekeskus). Selline mudel lihtsustab seadmete ning teenuste monitoorimist, teenuse kvaliteedi jälgimist ning loob võimaluse ühtlustada turvapoliitikate rakendamist. Haldusmudeli keskseks ideeks on võrgulahenduse standardiseerimine ning koolide digitaristus kõrgema teenuskvaliteedi tagamine.

Lahenduse haldust on võimalik teostada rollipõhiselt, mis võimaldab luua erinevate õigustega kasutajate ligipääse halduskeskkonnale kooli/piirkonna põhiselt.

Keskne haldusmudel ei nõua koolidelt võrgulahenduse haldamiseks lisa riistvaralisi kulutusi, vaid võimaldab seda kasutada välise teenusena, kus haldusplatvormi riistvara, tarkvara ja litsentsid sisalduvad digitaristu kaasajastamise projektis.

Projekti perioodi lõppedes tuleb arvestada lisakulutustega, mis kaasnevad haldusplatvormi ülalhoidmisega, või võimalusega loobuda kirjeldatud mudelist ning liikuda tagasi lokaalse halduse peale.

Keskne haldusplatvorm

1. <u>Üldised nõuded</u>
   - 1.1. Lahenduse seadmeid(tulemüürid, kommutaatorid ja tugijaamad) peab olema võimalik täielikult hallata maksimaalselt kahest kesksest halduskeskkonnast.
   - 1.2. Halduskeskkond võib koosneda maksimaalselt kahest eraldiseisvast veebiportaalist(haldusplatvormist), läbi mille toimub seadmete haldus.
   - 1.3. Kaks erinevat haldusplatvormi võivad olla kombineeritud haldama järgmisi seadmeid, seadmetüüpide järgi:

Valik	Platvorm 1	Platvorm 2
1	Kommutaatorid, tulemüürid	Wi-Fi tugijaamad/kontrollerid
2	Tulemüürid	Wi-Fi tugijaamad/kontrollerid, kommutaatorid
3	Wi-Fi tugijaamad/kontrollerid, kommutaatorid, tulemüürid	*Puudub*

1.4. Haldusplatvorm võib koosneda eraldiseisevatest füüsilistest seadetest või olla virtuaalne keskkond
1.5. Pakutav lahendus peab sisaldama vajalikku riist-, tarkvara ja litsentse haldusplatvormi töötamiseks
1.6. Haldusplatvormi erinevad komponendid peavad olema eelnevalt seadistatud ja omavahel liidestatud selliselt, mis võimaldaks lahendust pärast soetamist koheselt kasutada
1.7. Haldusplatvorm peab asuma kas pakkuja, tootja või kolmanda osapoole andmekeskuses ning peab vastama „Andmekeskuse nõuded“ alampunktis välja toodud tingimustele
1.8. Haldusplatvormid peavad vastama punktis 3 kirjeldatud turvanõuetele.
1.9. Haldusplatvormi andmekeskuse majutuskulud peavad olema kaetud projekti perioodi lõpuni, võimalusega seda teenust pärast projekti perioodi lõppemist, tellija poolt jätkata

2. Tehnilised nõuded

2.1. Võrguseadmete grupeerimine asukohapõhiselt
2.2. Seadmeid kuvamine asukohapõhistelt ja korruste kaartidel (tugijaamad)
2.3. Seadmete tööparameetrite kuvamine (*device monitoring*)
2.4. Seadmete sündmuslogi salvestamine ja kuvamine (*event log*)
2.5. Võrguliikluse statistika salvestamine ja kuvamine, mis peab võimaldama näha:
  2.5.1. Liideste põhist liiklusstatistikat
  2.5.2. Rakenduse põhist statistikat
  2.5.3. Kasutajapõhist statistikat
2.6. Hallatavate võrguseadmete seadistusmallide (*configuration template*) loomise ja rakendamise võimekus üksikule seadmele ning seadmete grupile
2.7. Sisse ehitatud veatuvastus tööriistad (k.a. *ping* ja *traceroute* utiliit)
2.8. Platvorm peab võimaldama teostada hallatavates võrguseadmetes paketivoo salvestust (*packet capture*) ning võimalust jäädvustada salvestatud fail võrguliikluse analüüsimistarkvarale (nt *Wireshark*) sobivasse formaati
2.9. Kohandatud raportite koostamine hallatavatest võrguseadmetest, võrguliiklusest ja turvaintsidentidest.
2.10. Raportite salvestamine ning edastamise võimalus nii käsitsi kui automaatselt (nt. Emaili)
2.11. Halduskeskkonnaga ühenduse katkemisel peavad lahenduse kõik seadmed edasi töötama täisfunktsionaalsuses

3. Turvalisusnõuded

3.1. Rollipõhine ligipääs administratiivsetele kasutajatele (seadmegruppide/asukoha põhiselt)
3.2. Seadmegruppide/asukoha põhiste lugemisõigustega kasutajate loomine
3.3. Seadistusmuudatuste logi
3.4. Haldusplatvormi sisse logitud kasutajate logi (k.a. ajas tagasiulatuvalt)
3.5. Kasutajate võrguliiklus ei tohi olla suunatud läbi halduskeskkondade
3.6. Haldusliiklus kohtvõrgu seadmetest halduskeskkonda peab olema krüpteeritud

4. Andmekeskuse nõuded
   - 4.1. Süsteemi ülalolekuaeg peab olema tagatud aastas 99,99% (*uptime* SLA)
   - 4.2. Andmekeskus peab vastama ISO 27001 sertifikaadile
   - 4.3. Andmekeskus peab asuma EU regioonis
   - 4.4. Andmekeskus peab olema kõrgkäideldav ning distributeeritud füüsiliselt erinevates asukohtades
   - 4.5. Andmekeskuse rikete korral automaatne halduskeskkonna andmekeskuste vaheline liigutamine ja tööfunktsionaalsuse taastamine

5. Lahenduse topoloogia