Lietuvos mokslo ir studijų institucijų kompiuterių tinklas LITNET

Kauno technologijos universitetas

# Saugios belaidės prieigos (WiFi) paslauga

## Belaidės prieigos diegimo ir valdymo procedūra

Paslauga sukurta vykdant Europos socialinio fondo finansuojamą projektą „Mokslo ir studijų institucijoms LITNET teikiamų IT paslaugų plėtra“ Nr. 09.3.3-ESFA-V-711-01-0003

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Kaunas

2018 m.

# Belaidės prieigos diegimo ir valdymo procedūra

1. ***Esamos situacijos analizė***. **INSTITUCIJA** pateikia savo poreikius, t.y. kokie lūkesčiai iš WiFi tinklo (paslaugos, sparta, aprėptis).

1.1. **INSTITUCIJA** sudaro arba papildo LITNET paslaugų teikimo sutartį[1].

1.2. **INSTITUCIJA** pateikia pastatų planus, nurodydama erdves, kur reikalingas WiFi ryšys.

1.3. **INSTITUCIJA** pateikia planuojamų naudoti WiFi tinklo įrenginių tipus ir kiekius konkrečiuose vietose. Įrenginiai skirstomi į nešiojamus ir išmaniuosius. Nešiojamieji įrenginiai: nešiojami kompiuteriai, stacionarūs įrenginiai su WiFi plokštėmis. Išmanieji įrenginiai: išmanieji telefonai, planšetės ir kiti maži įrenginiai maitinami iš baterijų.

1.4. **INSTITUCIJA** ir LITNET susitaria dėl WiFi tinklų parametrų: SSID pavadinimų, saugumo ir autorizavimo metodų. Diegiamas eduroam SSID tinklas. **INSTITUCIJAI** pageidaujant sukuriami papildomi tinklai: papildomas 802.1x autorizaciją palaikantis tinklas su **INSTITUCIJOS** siūlomu SSID pavadinimu, rotuojamo bendrojo slaptažodžio (angl. *passphrase*) tinklas su **INSTITUCIJOS** siūlomu SSID pavadinimu. Bendras WiFi tinklų kiekis (SSID) negali viršyti keturių WiFi SSID tinklų vienam WiFi prieigos taškui. Esant poreikiui, papildomi SSID tinklai **INSTITUCIJOJE** gali būti keičiami. Rotuojamasis slaptažodis turi būti ne trumpesnis nei dešimties simbolių ilgio. Slaptažodį sudaro didžiosios ir mažosios lotyniškos raidės, skaičiai ir specialiųjų ASCII aibės ženklai. Papildomų SSID tinklų pavadinimai gali būti sudaromi iš lotyniškų didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų ASCII aibės ženklų. Papildomo SSID tinklo pavadinimo ilgis gali būti nuo vieno iki trisdešimties simbolių.

***2. Tinklo modeliavimas ir parametrų parinkimas.***

2.1. Jei pastate yra atviros erdvės per kelis aukštus, skirtingų aukščių lubos, esant netikslumams pastato planuose, pastatuose kurie sudaryti iš metalo ir stiklo konstrukcijų, atliekama patalpų apžiūra. Atlikus patalpų apžiūrą atliekami reikalingi pakeitimai WiFi tinklo modeliavime.

2.2. Siekiant nustatyti optimalų WiFi prieigos taškų kiekį, jų montavimo vietas ir užtikrinti optimalų signalo lygį naudotojo įrenginyje, atliekamas WiFi signalo galios modeliavimas. Modeliavimo metu įvertinami WiFi įrangos parametrai, pastato išplanavimas, konstrukcines medžiagos ir jų slopinimo įtaka WiFi signalui.

2.3. Remiantis atliktu WiFi tinklo modeliavimu, parenkami WiFi tinklo įrangos kiekiai. Pagal naudotojų įrenginių kiekio ir tipų analizę parenkamos WiFi prieigos taškų specifikacijos. WiFi prieigos taškai klasifikuojami pagal naudojimosi intensyvumą ir galimybes:

- „Mažo naudojimo“ - WiFi prieigos taškas diegiamas į vietas, kuriose naudotojų kiekiai neviršija dešimties naudotojų vienu metu, pavyzdžiui, praeinami koridoriai, mažos laukimo erdvės, mažos auditorijos. Šiose vietose pagrindinės naudojamos paslaugos: elektroninis paštas ir naršymas internete.
- „Didelio naudotojų kiekio“ - WiFi prieigos taškas, diegiamas į vietas, kuriose susiburia didelis išmaniųjų įrenginių naudotojų (10-50) kiekis, pavyzdžiui, laukimo salės, laisvalaikio zonos, vidutinio dydžio auditorijos, salės. Šiose vietose pagrindinės naudojamos paslaugos: elektroninis paštas, naršymas internete, mažų bylų persiuntimas (<30 MB), vaizdo transliacijos.
- „Didžiausių naudotojų apkrovų“ - WiFi prieigos taškas diegiamas į vietas, kur susirenka naudotojai su nešiojamais įrenginiais ir dirba, pavyzdžiui, kompiuterių auditorijose, bibliotekose, savarankiško darbo vietos. Šiose vietose pagrindinės paslaugos: elektroninis paštas, naršymas internete, didelių bylų perdavimas (>30 MB), vaizdo transliacijos.

Pirmoje lentelėje pateikiami kiekvienos klasifikacijos WiFi prieigos taško rekomenduojami parametrai. Dėl kitokios WiFi prieigos taškų įrangos rekomenduojama konsultuotis su LITNET.

[1] https://www.litnet.lt/lt/paslaugos/90-paslaugu-teikimo-tvarka

Antroje lentelėje pateikiami bendrieji WiFi prieigos taško reikalavimai saugios belaidės WiFi prieigos paslaugai.

1 lentelė. Saugaus belaidžio WiFi ryšio prieigos taškų specifikacijų rekomendacijos

| Parametras\tipas | „Mažo naudojimosi“ | „Didelio naudotojų kiekio“ | „Didžiausių naudotojų apkrovų“ |
|---|---|---|---|
| Palaikomi WiFi protokolai (IEEE 802.11) | g/n | a/g/n/ac | a/g/n/ac |
| Darbiniai dažnių ruožai | 2,4GHz | 2,4 GHz ir 5 GHz | 2,4 GHz ir 5 GHz |
| Antenų konfigūracija | 2x2 MIMO | 2x2 MIMO | 3x3 MIMO |
| Antenų stiprinimas | 3 dBi | 3 dBi | 3 dBi |
| Siuntimo galia (EIRP) | 20 dBm | 20 dBm | 20 dBm |
| Ethernet prievado sparta | 100 Mb/s | 1 Gb/s | 1 Gb/s |
| Elektros maitinimas | PoE 24 V pasyvus arba 802.3af /802.3at | PoE 24V pasyvus arba 802.3af /802.3at | PoE 802.3af /802.3at |

2 lentelė. Bendrieji reikalavimai saugaus belaidžio WiFi ryšio prieigos taškams

| Charakteristika | Charakteristikos aprašymas |
|---|---|
| Saugos protokolų palaikymas | WPA, WPA2 ir WPA + WPA2 palaikymas |
| | 802.11x palaikymas |
| Funkciniai reikalavimai | RFC 5905 (NTP) |
| | SSID ir VLAN susiejimas |
| | IEEE 802.1Q protokolo palaikymas |
| | Privalo naudoti išorinį RADIUS serverį ir palaikyti visas funkcijas vienu metu: klientų autentifikavimą, autorizavimą ir apskaitą |
| | Ne mažiau 4 transliuojamų belaidžio ryšio ID (SSID) palaikymas vienu metu vienam dažnių ruožui |
| Valdymas | Privaloma įrenginį konfigūruoti ir stebėti su valdymo kontroleriu |
| Kitos savybės | Privalomas suderinamumas su Europos (ETSI) radijo dažnių reguliavimo standartais |
| | WiFi prieigos taškas turi turėti gamyklinių parametrų atstatymo mygtuką |

2.4. **INSTITUCIJAI** pateikiami reikalavimai kabeliniam tinklui ir WiFi prieigos taškų montavimui. Užsakančioji **INSTITUCIJA** atsakinga už kabelinio tinklo įrengimą iki kiekvieno WiFi prieigos taško. Kabelis turi būti ne žemesnės nei CAT5E kategorijos. Maksimalus kabelio ilgis - 100 metrų. Abu kabelio galai turi būti užbaigti RJ45 tipo kištukiniais lizdais. WiFi prieigos taškas prijungiamas jungiamuoju (angl. *patch*) kabeliu. WiFi prieigos taškai, bus montuojami LITNET pateikto plano nurodytose vietose.

2.5. **INSTITUCIJAI** pateikiami reikalavimai tinklo maršrutizatoriui ir komutatoriams. Tinklo komutatoriai turi palaikyti 802.1q protokolą ir VLAN, turėti ne mažesnės nei 100 Mb/s (pageidautina 1 Gb/s) spartos prievadus ir aukštynkrypčio (angl. *uplink*) prievado spartą ne mažesnę nei 1 Gb/s. WiFi prieigos taškas turi būti prijungtas į tinklo komutatoriaus prievadą, kuris privalo perduoti WiFi prieigos taško valdymo VLAN be VLAN žymos. WiFi SSID srautas turi būti perduodamas naudojant VLAN žymą. Tinklo maršrutizatorius turi palaikyti VLAN ir keletą ne mažesnės nei 1 Gb/s spartos ethernet prievadus. Tinklo maršrutizatorius turi teikti šias paslaugas WiFi prieigos taškams ir WiFi tinklo naudotojams: tinklo adresų vertimo funkciją (NAT), DHCP ir ugniasienės paslaugą. Galėti kaupti ir siųsti sujungimo sesijų informaciją, DHCP paslaugos įrašus į nuotolinę tarnybinę stotį „*syslog*“ formatu.

Maršrutizatorius pralaidumas turi būti ne mažesnis nei 500 Mb/s, jei WiFi tinklu naudosis iki 200 naudotojų, ir ne mažesnio nei 1 Gb/s, jei naudosis daugiau. Jei **INSTITUCIJA** neturi tinkamo maršrutizatoriaus, jį gali suteikti LITNET.

2.6. **INSTITUCIJA** vykdo įrangos pirkimo procedūros. Pagal pateiktas rekomendacijas **INSTITUCIJA** įsigyja visą WiFi tinklui reikalingą įrangą.

***3. Autorizacijos sistemos.***

3.1. Autorizavimo sistema turi palaikyti RADIUS paslaugą. RADIUS turi palaikyti 802.1x reikalingus saugos protokolus: EAP, PEAP, PEAP-mschap2, PAP. **INSTITUCIJOS** teikiama RADIUS paslauga turi užtikrinti ne mažesnį nei 10 Mb/s tinklo pralaidumą, ne didesnį nei 2 % IP paketų praradimą ir ne didesnį nei 150 ms vėlinimą tinkle, jungiančiame WiFi prieigos taškus ir Lietuvos RADIUS tarnybines stotis. RADIUS privalo teikti paslaugą viešu IP interneto adresu ir turėti tapatybę patvirtinanti liudijimą.

3.1.1. Jei **INSTITUCIJA** neturi RADIUS paslaugos arba negali užtikrinti 3.1 punkte nurodytų reikalavimų, tada LITNET gali suteikti RADIUS paslaugą. LITNET RADIUS paslauga gali būti įdiegiama į organizacijos tarnybinę stotį arba į LITNET duomenų centre esančia tarnybinę stotį. Jei LITNET suteikia RADIUS paslaugą **INSTITUCIJA** privalo užtikrinti šiuos tinklo parametrus iki WiFi prieigos taško **INSTITUCIJOS** tinkle: ne didesnį nei 2 % IP paketų praradimą ir ne didesnį nei 150 ms vėlinimą. Jei **INSTITUCIJA** pageidauja turėti savo tinkle RADIUS tarnybinę stotį, **INSTITUCIJA** privalo užtikrinti 3.1 punkte nurodytus reikalavimus ir turi suteikti tokius tarnybinės stoties resursus:

- bent vieną procesorių;
- ne mažiau nei 512 MB darbinės atminties;
- ne mažiau nei 10 GB kietojo disko vietos;
- ne lėtesnį nei 100 Mb/s IP tinklo prievadą;

3.1.2. RADIUS paslaugos palaikomos šios duomenų bazių sistemos: LDAP, MYSQL, MSSQL, AD. Bet kurio tipo duomenų bazėje turi būti saugomi šie laukai:

- naudotojo prisijungimo vardas;
- naudotojo slaptažodis NThash formatu;
- leidimo prisijungti kintamasis.

Pagal naudotojo prisijungimo vardą, turi būti identifikuojamas konkretus paslaugos naudotojas. Gali būti panaudojamas papildomas duomenų laukas, leidžiantis identifikuoti konkretų paslaugos naudotoją pagal jo prisijungimo vardą. Duomenų bazė turi būti apsaugota nuo nesankcionuoto prisijungimo. **INSTITUCIJA** pilnai atsako už duomenų bazėje esančių duomenų teisingumą. Rekomenduojama naudoti perduodamų duomenų iš duomenų bazės šifravimą. **INSTITUCIJA** turi užtikrinti ne didesnį nei 10 ms IP tinklo ir duomenų bazės užklausos uždelsimą RADIUS paslaugai.

3.1.2.1. Jei **INSTITUCIJA** neturi tinkamos duomenų bazės, ji gali naudotis LITNET teikiama tapatybių valdymo paslauga. **INSTITUCIJAI** suteikiamos administravimo teisės naudotojų importavimui, eksportavimui, redagavimui ir naikinimui. Duomenų bazė valdoma naudojantis WWW valdymo skydu, o naudotojai aktyvuojasi per WWW registracijos portalą.

3.1.2.2. Į duomenų bazę sukeliami **INSTITUCIJOS** naudotojai. Į duomenų bazę **INSTITUCIJA** importuoja naudotojus naudodamasi WWW valdymo skydu. Kiekvienas **INSTITUCIJOS** naudotojas aprašomas prisijungimo vardu, el. pašto adresu, vardu pavarde, naudotojo prisijungimo prie **INSTITUCIJOS** metais. **INSTITUCIJA** pilnai atsako už duomenų teisingumą duomenų bazėje.

3.1.3. **INSTITUCIJA** ir LITNET susitariama dėl duomenų bazių sąsajų. Priklausomai nuo naudojamos duomenų bazės susitariama dėl prieigos:

- OpenLDAP bazės atveju: perduodami administruojančio naudotojo prisijungimo duomenys su teisėmis skaityti kitų naudotojų laukus (naudotojo vardas, prisijungimo

slaptažodis, leidimo prisijungti kintamasis), pateikiama duomenų bazės struktūra, duomenų bazei reikalingi prisijungimo duomenys ( IP adresas, prievadas, saugos protokolas).

- MSSQL bazės atveju: perduodami administruojančio naudotojo prisijungimo duomenys su teisėmis skaityti kitų naudotojų laukus (naudotojo vardas, prisijungimo slaptažodis, leidimo prisijungti kintamasis), pateikiama duomenų bazės struktūra, duomenų bazės pavadinimas, duomenų bazei reikalingi prisijungimo duomenys ( IP adresas, prievadas, duomenų bazės vardas, duomenų bazės versija).
- MYSQL bazės atveju: perduodami administruojančio naudotojo prisijungimo duomenys su teisėmis skaityti kitų naudotojų laukus (naudotojo vardas, prisijungimo slaptažodis, leidimo prisijungti kintamasis), pateikiama duomenų bazės struktūra, duomenų bazei reikalingi prisijungimo duomenys ( IP adresas, prievadas, duomenų bazės vardas).

3.2. Naudojant pateiktą duomenų bazės sąsają sukonfigūruojama RADIUS paslauga. Pagal suteiktus duomenų bazių duomenis sukuriama ir sukonfigūruojama duomenų bazės sąsaja.

3.3. Atliekami RADIUS paslaugos testavimo darbai. Duomenų bazėje sukuriamas bandomasis naudotojas ir išmėginamos sudarytos sąsajos veikimas.

3.4. Nauja autorizavimo sistema prijungiama prie eduroam autorizavimo sistemos. RADIUS paslaugos tarnybinei stočiai suteikiama prieiga prie nacionalinių Lietuvos RADIUS tarnybinių stočių, sugeneruojami saugos raktai ir jais apsikeičiama tarp **INSTITUCIJOS** RADIUS paslaugos tarnybinės stoties ir nacionalinių Lietuvos RADIUS tarnybinių stočių. Atliekamas **INSTITUCIJOS** RADIUS tarnybinės stoties ir nacionalinio Lietuvos RADIUS tarnybinių stočių komunikacijos bandymas. Nuo šio momento **INSTITUCIJA** yra oficialiu eduroam paslaugos nariu. **INSTITUCIJAI** suteikiama prieiga prie eduroam konfigūravimo įrankio CAT.

***4. Įrangos diegimas.***

4.1. Atliekamas WiFi įrangos konfigūravimas

4.1.1. Atliekamas maršrutizatorių konfigūravimas pagal **INSTITUCIJOS** sutiektus IP adresus ir VLAN numerius. Kiekvienam WiFi prieigos taškui reikalingas privatus nekintantis IP adresas, kuris suteikiamas naudojantis DHCP paslauga. WiFi prieigos taškui turi būti užtikrinimas komutuojamo tinklo ryšys su WiFi tinklo kontroleriu, IP tinklo ryšys su RADIUS paslauga ir NTP paslauga. **INSTITUCIJA** atlieka komutatorių ir maršrutizatorių konfigūravimą. LITNET gali padėti sukonfigūruoti tinklo komutatorius ir maršrutizatorius.

4.2. Atliekamas įrangos diegimas. Įrangos montavimo darbus atlieka **INSTITUCIJA**. Įranga montuojama remiantis sudarytais planais ir tik į suplanuotas vietas.

***5. Įdiegto tinklo analizė ir perdavimas naudoti.***

5.1. Nustatoma įdiegto tinklo aprėptis ir WiFi tinklo pralaidumas. Matavimai atliekami iš anksto sutartose vietose (vietos kuriose reikalingas WiFi ryšys), naudojant atvirojo kodo programinį paketą „iperf3“ serveris-klientas režimu. Kiekvieno matavimo trukmė yra 5 minutės. Tam, kad atmesti kitų perdavimo linijų įtaką matavimo rezultatams, naudojama **INSTITUCIJOJE** esanti tarnybinė stotis. Išmatuoti parametrai laikomi atraminiais.

5.2. Pateikiama įdiegto WiFi tinklo dokumentacija. Pateikiama dokumentacija su įdiegta tinklo įranga, jos konfigūracija. Pateikiama ataskaita su išmatuota tinklo sparta, pateikiant naudotos įrangos specifikaciją, matavimo metodiką, nurodant matuojamos vietos pavadinimą, matavimo metu dirbusio WiFi prieigos taško vardą arba MAC adresą.

5.3. Atlikus tikrinimo, matavimo darbus ir nesant papildomų pakeitimų, tinklas laikomas paruoštu teikti paslaugą. Tinklu gali pradėti naudotis **INSTITUCIJOS** naudotojai. Atliekamas tinklo parametrų stebėjimas. Esant tinklo sutrikimams registruojamos problemų kortelės. Naudotojams suteikiami prisijungimo duomenys, jie yra supažindinami su LITNET tinklo

naudojimo taisyklėmis[2]. Pirmojo prisijungimo metu **INSTITUCIJOS** naudotojai patvirtina sutikimą laikytis LITNET tinklo naudojimo taisyklių .

5.4. Tinklo priežiūra. LITNET atlieka WiFi įrangos ir suteikto tinklo maršrutizatoriaus gamintojo programinės įrangos atnaujinimo darbus. **INSTITUCIJA** privalo užtikrinti nepertraukiama elektros maitinimą, apsaugą nuo žalingo išorės veiksnių poveikio.

5.5. Esant WiFi tinklo parametrų nuokrypiams nuo atraminių išmatuotų parametrų, atliekama analizė ir nustatomos priežastys. Problemų korteles gali registruoti tinklo naudotojai ir **INSTITUCIJOS** IT administratoriai. Problemos, kurių priežastys yra naudotojo programinės, aparatinės įrangos gedimas arba naudotojo įrenginio konfigūracijos klaidos, turi būti sprendžiamos **INSTITUCIJOS**. Esant tinklo įrangos gedimui **INSTITUCIJA** rūpinasi įrangos keitimo darbais. **INSTITUCIJA** įsipareigoja atlikti LITNET jai paskirtas užduotis susijusias su tinklo veikimo užtikrinimu. LITNET įsipareigoja teikia konsultacijas, susijusias su WiFi tinklu ir jo priežiūra.

***6. WiFi paslaugos valdymas ir stebėjimas.***

6.1. **INSTITUCIJAI** pageidaujant LITNET suteikia prieiga prie WiFi tinklo kontrolerio, kur **INSTITUCIJA** galės keisti tokius WiFi tinklo parametrus: sukurti arba panaikinti WiFi tinklą (SSID), sukurti arba pakeisti WiFi tinklo pavadinimą (SSID), nustatyti WiFi tinklo saugos protokolą, WiFi tinklo bendrąjį slaptažodį, įdiegti į tinklą naują WiFi prieigos tašką.

6.2. **INSTITUCIJAI** LITNET suteiks prieigą prie WiFi tinklo srautų apskaitos, kurioje galės stebėti WiFi tinklu perduodamus duomenų kiekius.

[2] https://www.LITNET.lt/lt/tnt