# eduroam

Vieninga autentifikacijos sistema

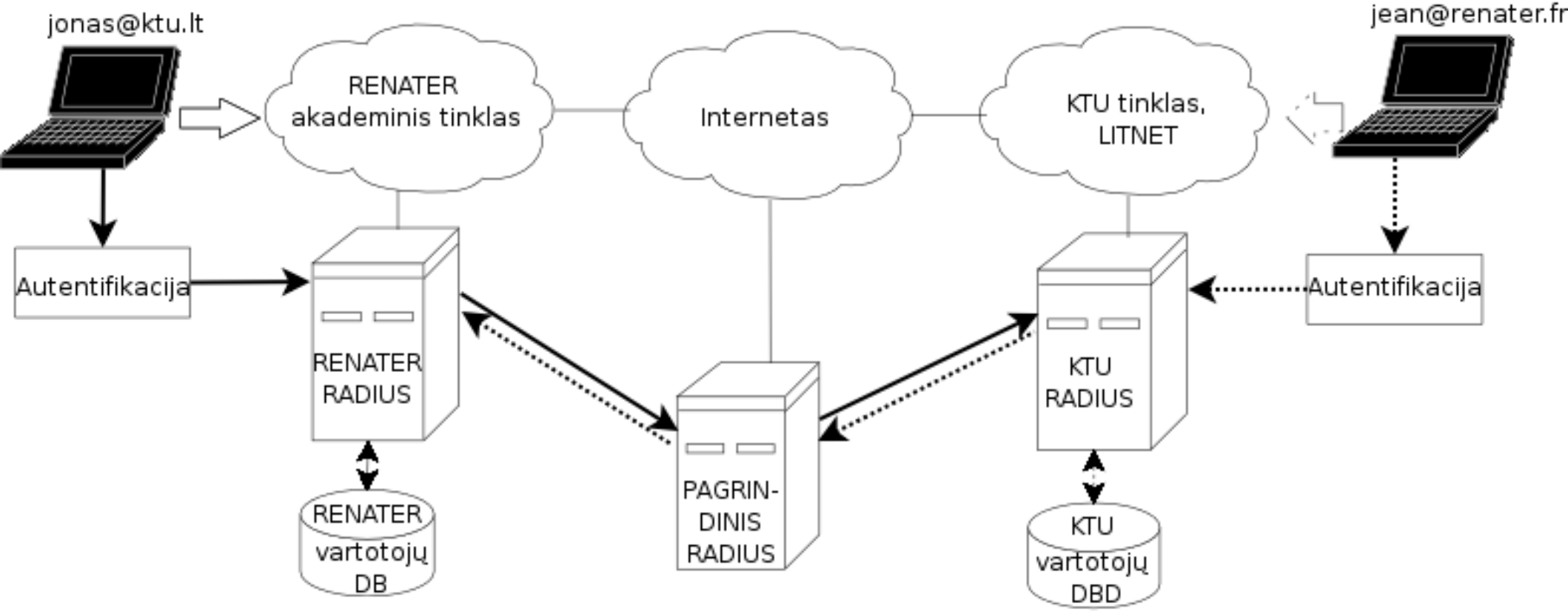
# Apžvelgiamos temos

- Kas yra eduroam? Pagrindiniai principai
- Saugumas
- Techniniai ir programiniai sprendimai
- Kaip prisijungti?

# Kas yra eduroam ?

- Eduroam (Education Roaming) – tarptinklinio ryšio paslauga, skirta akademinėms institucijoms, prisijungusioms prie eduroam infrastruktūros.
- Paslauga leidžia skirtingoms projekte dalyvaujančioms organizacijoms naudotis vieninga bevielio ryšio vartotojų autentifikavimo sistema.
- Autentifikavimo sistema yra pagrįsta
  - RADIUS serverių hierarchija
  - 802.1X technologija

# Vieninga autentifikacijos sistema



# Prisijungusios šalys

- http://www.eduroam.org

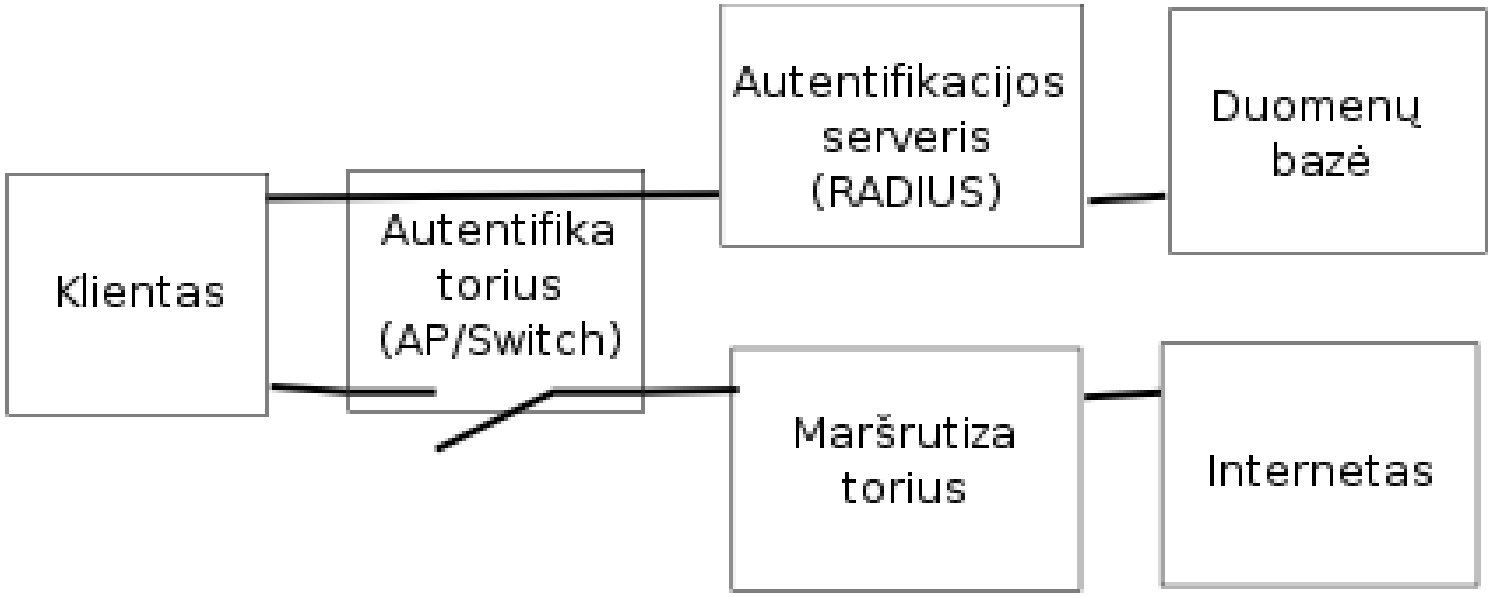
# Privalumai

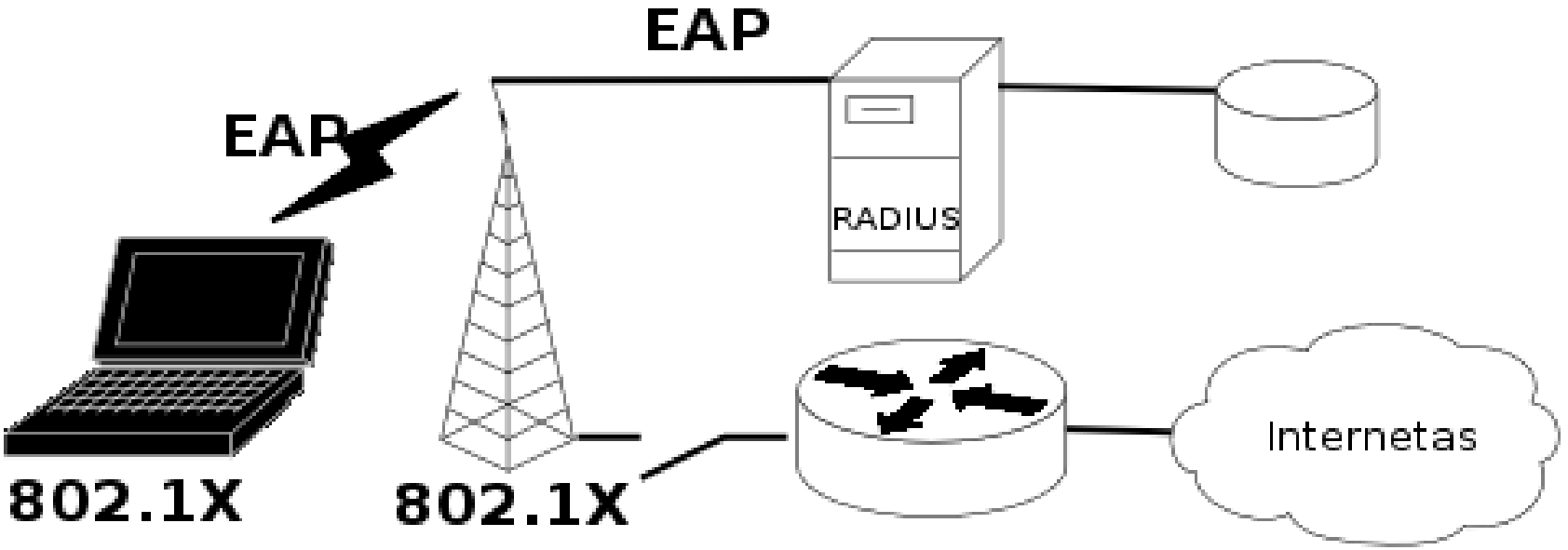
- Patogu vartotojui
- Patogu administratoriui
- Saugu
- Lankstu

# IEEE 802.1X

- Naudojamas autentifikacijai per RADIUS serverį
- Galimi keli autentifikavimo mechanizmai (EAP-MD5, **MS-CHAPv2**, EAP-SIM, EAP-TLS, EAP-TTLS, **PEAP**)
- Pasiekiamumas aprobotas ties portais
- Kiekvienam vartotojui ir kievienai sesijai suteikiamas atskiras raktas (dinamic keys)
- Dinaminių VLAN kūrimo galimybė
- Reikalinga klientinė programinė įranga
- Tinka ir LAN ir WLAN

# 802.1X ir EAP


Klientas
Autentifikatorius (AP/Switch)
Autentifikacijos serveris (RADIUS)
Duomenų bazė
Maršrutizatorius
Internetas


EAP
EAP
RADIUS
802.1X
802.1X
Internetas

# EAP tipai

- EAP – TTLS, PAP
  - žinute perduodamas slaptažodis
- EAP – TTLS, CHAP
  - žinute perduodama skaičių seka
- PEAP, MSCHAP
  - žinute perduodama skaičių seka
- Naudojant EAP – TTLS ir PEAP
  - sudaromas saugus TLS tunelis
  - tinka Cisco ir kitiems AP

# Slaptažodžių šifravimas

- **chap** (Challenge-Handshake Authentication Protocol):
  - serveris siunčia klientui “challenge” žinutę
  - klientas grąžina serveriui reikšmę, gautą “challenge” žinutei pritaikius vienos krypties hash funkciją (pvz.: MD5)
  - serveris patikrina ar gauta reikšmė sutampa su reikšme, kurios jis tikisi (pagal savo skaičiavimus)
- Slaptažodžius turi žinoti abi pusės (klientas ir serveris)
- Kadangi mschap leidžia naudoti slaptažodžių hash'us, duomenų bazėje slaptažodžiai gali būti saugomi ne atviru tekstu, o šifruoti.

# freeRADIUS konfigūracija

- *radiusd.conf*
- *users*
- *clients.conf*
- *proxy.conf*

# radiusd.conf

```
eap {
        default_eap_type = peap
        timer_expire     = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no

        tls {
                private_key_password = pkw3ef7o
                private_key_file = ${raddbdir}/certs/cert-srv.pem
                certificate_file = ${raddbdir}/certs/cert-srv.pem
                CA_file = ${raddbdir}/certs/demoCA/cacert.pem
                dh_file = ${raddbdir}/certs/dh
                random_file = ${raddbdir}/certs/random
                fragment_size = 1024
                include_length = yes
                check_crl = no
        }
        *** perkelta
```

*** tęsinys

```
        peap {
            default_eap_type = mschapv2
        }
        mschapv2 {
        }
    } # eap aprašo pabaiga

    mschap {
        authtype = MS-CHAP
        use_mppe = yes
        require_encryption = yes
        require_strong = yes
    }
```

# radiusd.conf

```
ldap ldap_staff {
        server = "freeradius.litnet.lt"
        identity = "cn=Administratorius,dc=litnet,dc=lt"
        password = “paslaptis"
        basedn = "ou=staff,dc=ktu,dc=lt"
        filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
        start_tls = yes
        access_attr = "dialupAccess"
        access_attr_used_for_allow = yes
        dictionary_mapping = ${raddbdir}/ldap.attrmap
        ldap_connections_number = 5
        password_attribute = radiusTunnelPassword
        timeout = 4
        timelimit = 3
        net_timeout = 1
}
```

# radiusd.conf

```
authorize {
        preprocess
        auth_log
        suffix
        files
        eap
        mschap
        Autz-Type LDAP_STAFF {
                ldap_staff
        }
}
```

```
authenticate {
        Auth-Type EAP {
                eap
        }
        Auth-Type MS-CHAP {
                mschap
        }
        Auth-Type PAP {
                pap
        }
}
```

# users

```
# LITNET darbuotoju Realm'as
DEFAULT Realm == NULL, Autz-Type := LDAP_STAFF
        Fall-Through = yes
# KTU Darbuotoju Realm'as
DEFAULT Realm == ktu.lt, Autz-Type := LDAP_STAFF
        Fall-Through = yes
# KTU Studentu Realm'as
DEFAULT Realm == stud.ktu.lt, Autz-Type := LDAP_STUD
        Fall-Through = yes
```

# clients.conf

```
client 192.168.0.50 {
        secret          = @cCe$5p0i#t
        shortname   = eduroam
}

client 193.219.1.22 {
        secret          = 0r&aNi2@cijA
        shortname   = mokykla
}
```

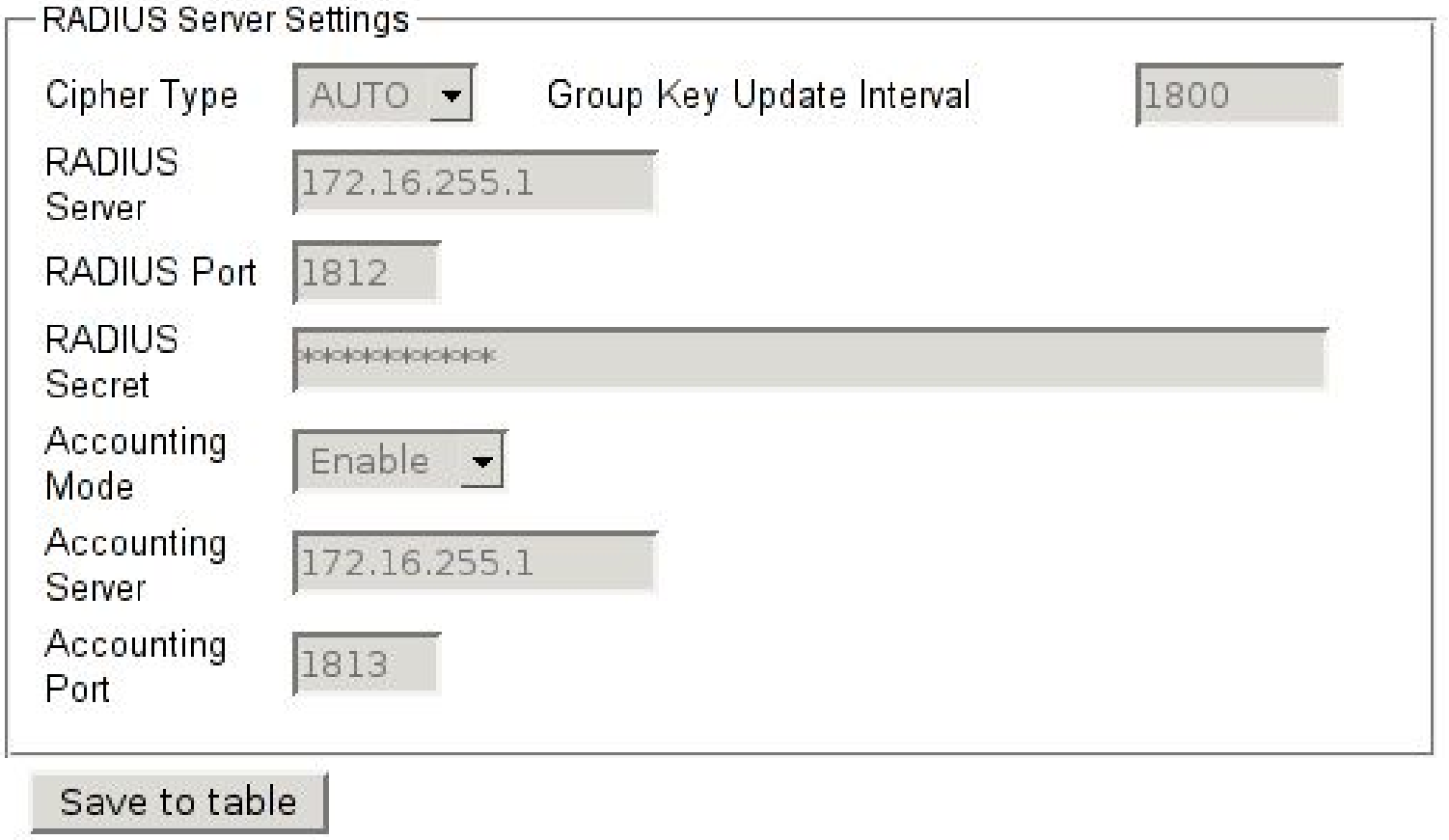
# proxy.conf

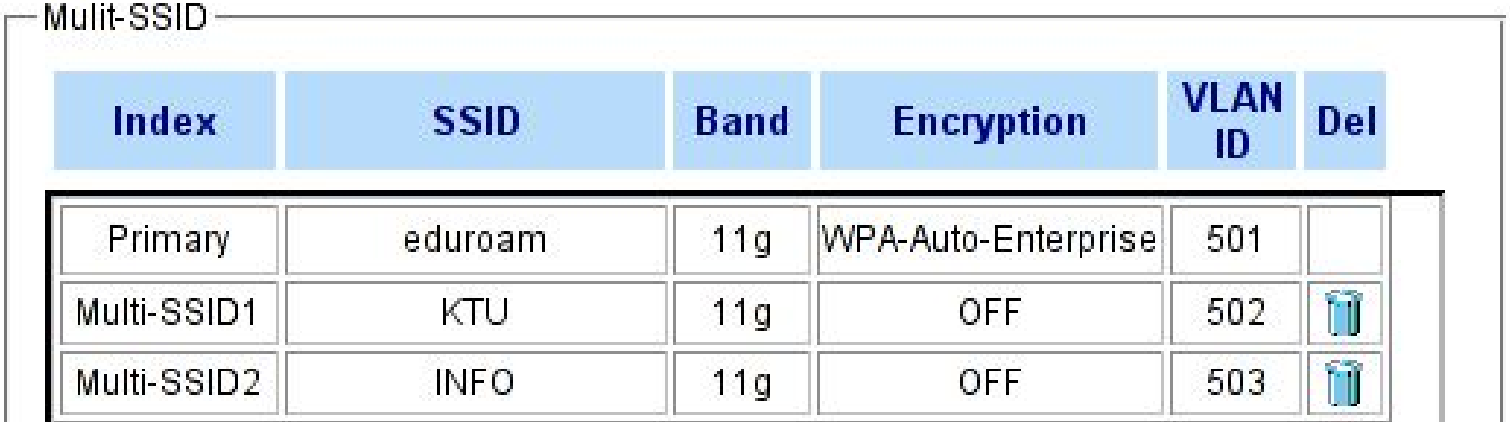
```
realm ktu.lt {
   type = radius
   authhost = 193.219.1.22:1812
   accthost = 193.219.1.22:1813
   secret = &3rA$
   nostrip
}

realm DEFAULT {
   type = radius
   authhost = 193.219.61.71:1812
   accthost = 193.219.61.71:1813
   secret = Pr0Xi#t*
   nostrip
}
```

# AP

- Turi palaikyti 802.11 a, b, g standartus, bet nebūtinai visus kartu
- Rekomenduojama naudoti AP, kuris teikia
  - multissid galimybę
  - log galimybę
- SSID: “eduroam” (būtinai!)
- WPA protokolas (ne WEP)

# Access Point konfigūravimo pavyzdys:



# KTU naudoja:

- Prieigos taškas – DWL-3200AP
- 3 SSID
  - Eduroam (WPA)
  - KTU (web, vpn)
  - info
- 4 VLAN
  - AP administravimui ( 1 VLAN )
  - Atskiras VLAN kiekvienam SSID ( 3 VLAN )
- Radius serveris – Freeradius 1.1.1
- Duomenų bazė – OpenLDAP
- Maršrutizatorius – Linux
- Visiems vartotojams bei įrenginiams suteikiami privatūs adresai ir audojamas NAT.

# Prisijungimo žingsniai

- Kontakto užmezgimas:
  - el. paštu: eduroam@litnet.lt
  - telefonu: 300645
  - gyvai: Studentų 48a- 101
- Pagrindinių reikalavimų patenkinimas:
  - Naudojamas 802.1X protokolas
  - Sukonfigūruotas RADIUS serveris
  - Serverių adresai: Radius nr.1, Radius nr. 2 (backup)
  - Testinis vartotojas
- Shared secret apsikeitimas
- Abipusis testavimas

# Informacija apie eduroam

- Tinklalapyje www.eduroam.lt
  - paslaugos aprašymas
  - paaiškinimai kaip naudotis
  - kurios akademinės organizacijos naudoja eduroam
- atskiras ssid infomacijai pasiekti
- logotipai