Євгеній Преображенський
melkin@uran.ua
URAN

Мета тренінгу

Розуміння як діє Едюроам
Які він дає переваги
Як налаштувати Едюроам в вашому навчальному закладі

Відповіді на запитання

Загальні відомості

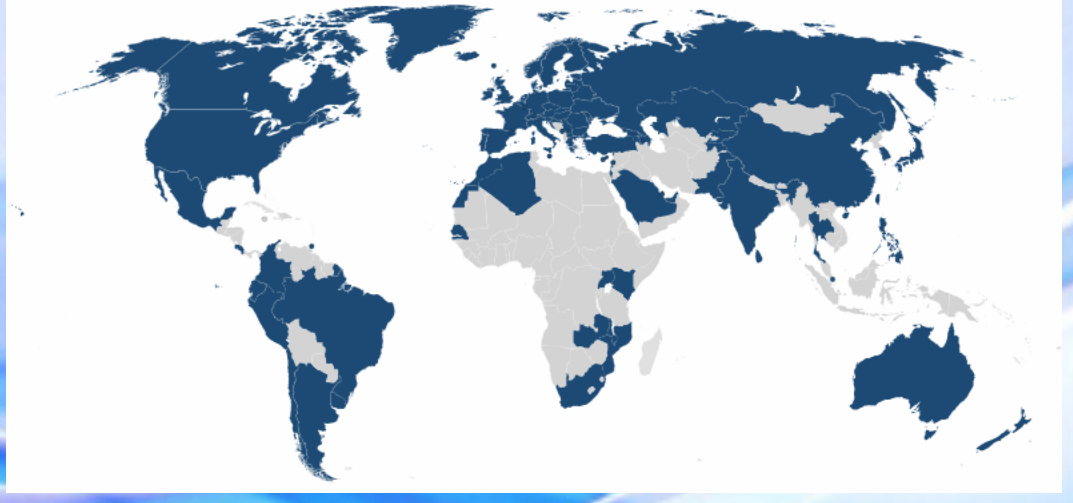
Огляд
Що це таке?
Як це працює?
Едюроам та NREN
Едюром та освітянський заклад
Вимоги
Впровадження

Огляд

Як багато NREN-ів приймають участь?
Як багато освітянських закладів приймають участь?

Що це таке?

Глобальна федерація організацій що надають доступ до Інтернет головним чином через WiFi



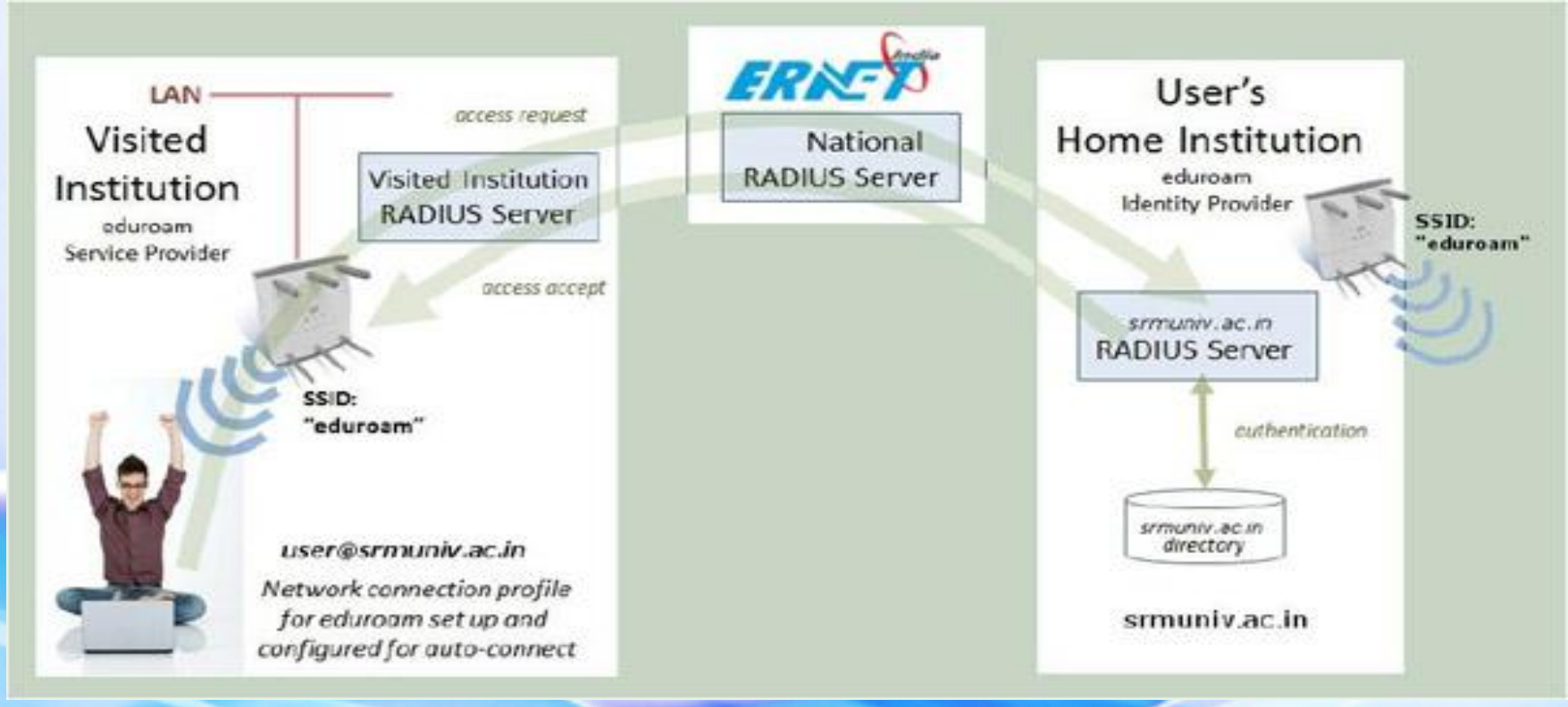
Переваги

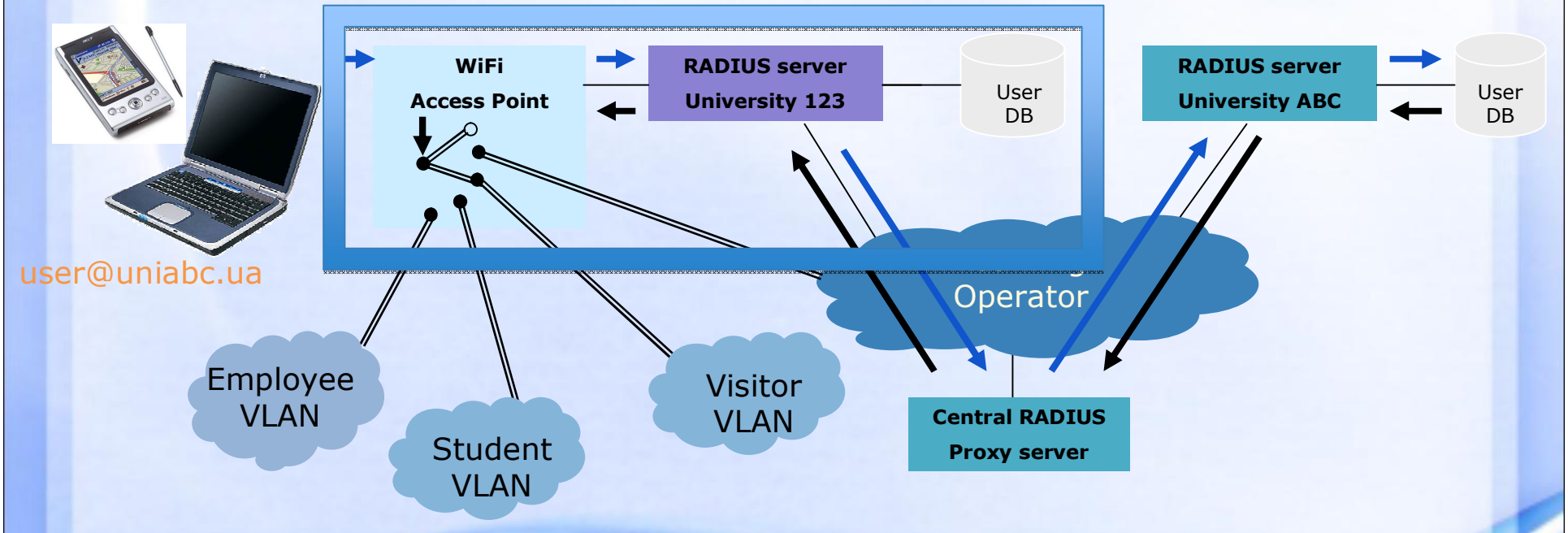
- Легкий роумінг
- Кожний користувач є ідентифікований
  - Можливо проведення аудіту та логірування
  - Допомагає в разі розслідування зловмисних інцидентів
- Канали WI-FI кожного користувача є шифрованими
  - Едюроам вимагає шифрованого спілкування меж клієнтом та AP

Відео

https://www.youtube.com/watch?v=TVCmcMZS3uA

Як це працює?


LAN
Visited Institution
eduroam Service Provider
access request
Visited Institution RADIUS Server
access accept
SSID: "eduroam"
user@srmuniv.ac.in
Network connection profile for eduroam set up and configured for auto-connect
ERNET India
National RADIUS Server
User's Home Institution
eduroam Identity Provider
SSID: "eduroam"
srmuniv.ac.in RADIUS Server
authentication
srmuniv.ac.in directory
srmuniv.ac.in


WiFi
Access Point
RADIUS server
University 123
User
DB
RADIUS server
University ABC
User
DB
user@uniabc.ua
Operator
Employee
VLAN
Student
VLAN
Visitor
VLAN
Central RADIUS
Proxy server
signaling
data

Терміни

RO – Roaming Operator
ETLRS – European Top-level RADIUS Servers
FLRS – Federation Level RADIUS Server
IdP – eduroam Identity Provider
SP – eduroam Service Provider
NAS – Network Access Element
F-Ticks – Federated Ticker System

Інфраструктура

Top level RADIUS server (ETLRS)
National RADIUS Proxy (FLRS)
Institutional RADIUS (IdP and/or SP)
Identity management system (IdM)
Access Points, switches (NAS)
Clients (Supplicant)
Monitoring (F-Ticks)

Протоколи та безпека

802.1x
  Supplicant to AP communication
RADIUS protocol
  NAS to IdP communication
EAP protocol
  Supplicant to IdP communication
  PAP, CHAP, TLS, TTLS, MS-CHAPv2, …
TLS protocol
  Securing FLRS to ETLRS as well as IdP to FLRS communication

EAP — Protocol Flow

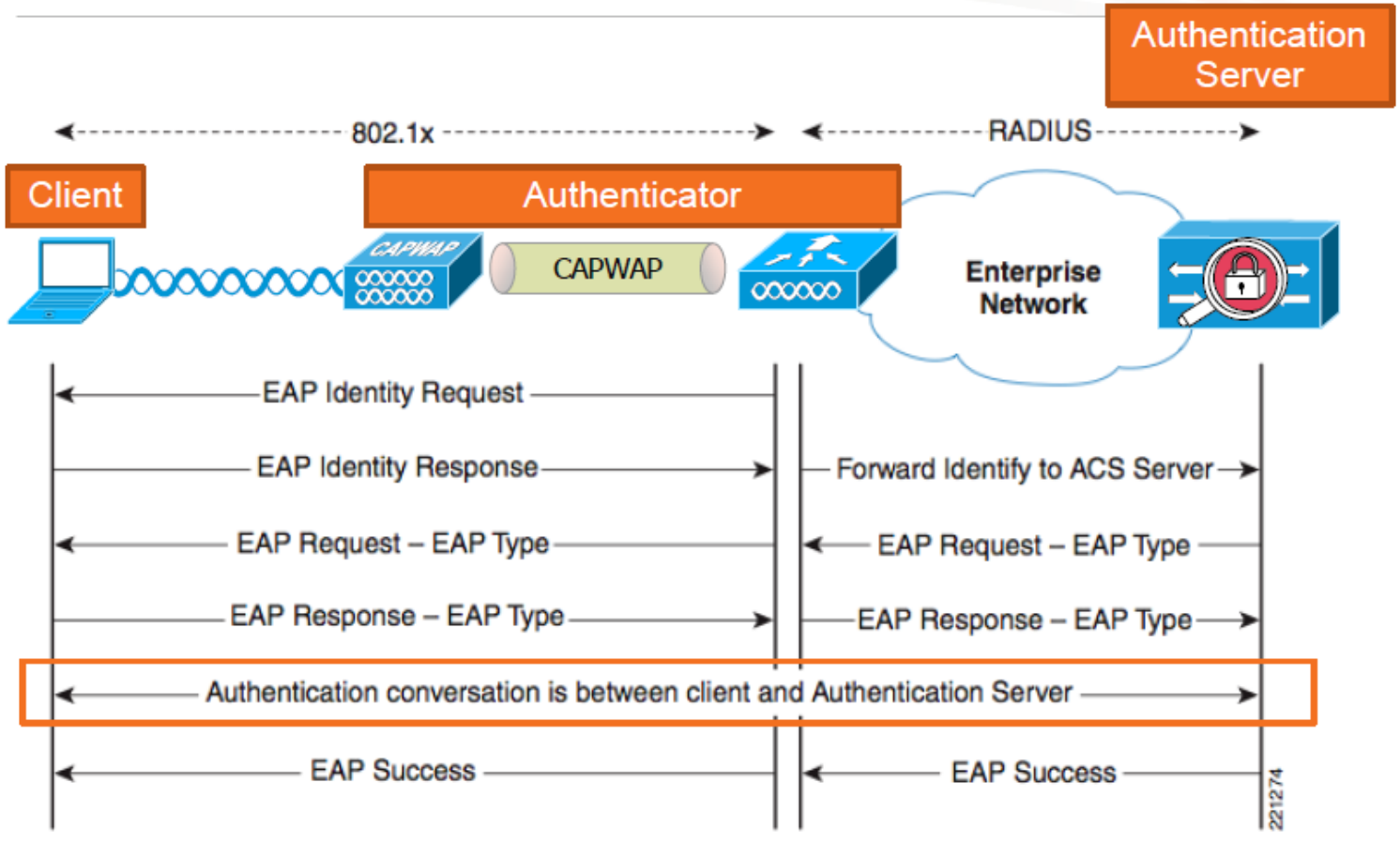


Diagram from http://mrncciew.com

Протоколи автентифікації

PAP – Password Authentication Protocol
CHAP – Challenge-response Authentication Protocol
TLS – Transport Layer Security – X.509 authN
TTLS – Tunneled TLS with e.g. PAP

Едюроам та NREN

Національна точка входу у глобальний Едюроам
Підтримує роботу FLRS
Проксює запити від SP до IdP та ETLRS
Моніторить інфраструктуру для IdP

Вимоги

Цифрові сертифікати що приймаються Едюроам PMA

Сервер з публічною IP адресою

Ідеально два сервери задля HA чи failover конфігурації.

Веб сервер.

Опціонально система поштових розсилок

Як це працює?

Вхідні запити маршрутизуються до національного IdP

далі пересилаються до ETLRS

FLRS не змінює RADIUS пакет

можлива тільки фільтрація певних атрибутів (наприклад видаленя номеру VLAN)

Інформаційні ресурси

Веб сторінки

Надають інформацію для користувачів та SP

https://eduroam.uran.ua

Список розсилки

Глобальний список розсилки Едюроам

Едюроам та освітянська організація

Автентифікація користувачів

Зв’язується з локальним IdM

Підтримка користувачів

Переважно за все працює як SP

Технічні терміни

IdP – автентіфікатор користувачів
NAS – Мережевий сервіс доступу
AP – Пункт доступу

Автентифікатор користувачів

Проводить автентифікацію користувачів за допомогою обраного метода
IdP selects authentication method
Проводить регистрацію користувачів
IdP повинен мати можливість точно ідентифікувати користувача персонально

Суплікант

Програмне забезпечення на боці клієнта яке забезпечує автентифікацію клієнта по протоколу EAP
Створює захищений тунель до IdP
Передає облікові данні користувача до IdP
Захищає передачу даних від комп'ютера користувача до AP
Присутній в Windows, Mac OS, Linux, Android, IOS, …

NAS

WiFi обладнання доступу
Повинно підтримувати 802.1x
Зв’язується з IdP по RADIUS протоколу
Має один пароль з IdP
WiFi захищеність: WPA2/AES
Відкриті порти

see 6.3.3 in eduroam Service Definition

Вимоги

Цифровий сертифікат який може бути прийнятий FLRS

Долучення до локальної бази користувачів

Сервер з «білими» IP адресами

В ідеалі два сервери для надійності

Опціонально (але дуже бажано) мати мережу пунктів доступу

Інформаційні ресурси

Вєб сторінка та контактна пошта для підтримки користувачів

Надає інформацію як доєднатися до Едюроам

Надає інформацію о локальних обмеженнях

Які порти закрити/відкрити

Діапазон NAT/IP

Джерела

https://www.eduroam.org
https://eduroam.uran.ua