Інструкція по впровадженню eduroam в науково-освітній установі на базі WiFi точок доступу Mikrotik

eduroam – сервіс WiFi-роумінгу між науково-освітніми організаціями. При відвіданні власним персоналом інших організацій (як в Україні, так і за кордоном) та при прийомі гостей подорожуючий буде автоматично підключений до Інтернет через найближчу WiFi eduroam точку доступу.

https://eduroam.uran.ua/ – український сайт послуги eduroam.

Точки доступу eduroam можна знайти по всьому світу:

https://eduroam.uran.ua/world – карта покриття eduroam із зазначенням точних місць розташування точок доступу.

https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus – технічна документація по eduroam (англійською).

Зручним пристроєм для побудови локальної мережі, що підтримує сервіс eduroam, є точка доступу **Mikrotik cAP ac**, яка виготовляється у вигляді модуля розміром близько 14 см, що кріпится на стелю або стіну. Має два гігабітних Ethernet-порти. Живиться через перший Ethernet-порт по PoE (*Power over Ethernet*). До другого Ethernet-порту можна підключати наступну точку доступу з Passive PoE.

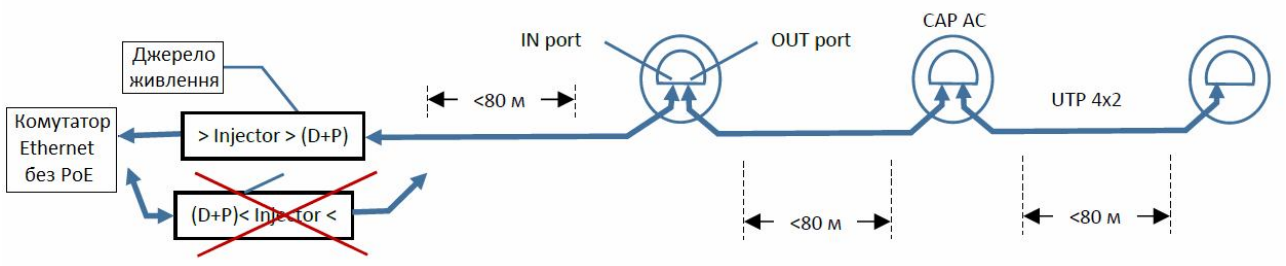
Детальніше див.: https://mikrotik.com/product/cap_ac ;
https://mikrotik.ua/product/mikrotik-cap-ac-rbcapgi-5acd2nd ;
https://lantorg.com/products/mikrotik-cap-ac-rbcapgi-5acd2nd ;
https://viva-telecom.org/13715/mikrotik/cap-ac/review/ .

Наявність точок доступу типу **Mikrotik cAP ac** або аналогічнних, підключених до локальної мережі організації, є мінімально необхідним для впровадження eduroam. При цьому одночасно можуть бути впроваджені й інші віртуальні WiFi мережі, оскільки cAP ac дозволяє активізувати декілька WiFi мереж (декілька SSID).

1. Створення сегменту локальної мережі в організації з WiFi точками доступу.

Фізично точки доступу повинні бути підключені до Ethernet комутатора (-ів) локальної мережі організації. Допустимі схеми сегментів мережі подані нижче.

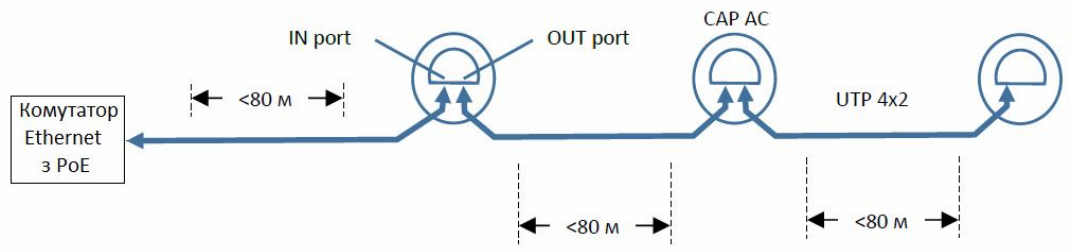
1.1. З комутатором Ethernet без PoE і додатковим джерелом живлення



Прим.[1]

[1] Недопустиме зворотнє включення

1.2. З комутатором Ethernet, обладнаним PoE



Може бути декілька сегментів з точками доступу, підключених до декількох комутаторів, у тому числі й до таких, що знаходяться в різних окремих IP-сегментах локальної мережі організації.

1.3. Практичні поради:

- Розміщувати точки доступу бажано на стелі: так досягається максимальна дистанція доступу та площа охоплення.
- При підключенні трьох точок доступу в ланцюжку треба уважно перевірити, щоб напруга живлення точки доступу була в межах від 12 В до 57 В. Також треба прийняти до уваги, що потужність одного джерела живлення, яке постачається разом з **MikroTik cAP ac** (24 В, 0,38 А, 9 Вт) може бути недостатньою для роботи навіть двох точок доступу в ланцюжку.
- Для підключення двох-трьох точок доступу в ланцюжку два джерела живлення можна з'єднати послідовно (вийде 48 В, 18 Вт), або придбати більш потужне джерело живлення **MikroTik MT48** (див. https://mikrotik.ua/product/mikrotik-mt48-480095-11dg) на 48 В, 0,8 А, 38 Вт.
- За можливості слід віддавати перевагу радіальному розведенню точок доступу. Такий варіант є більш доцільним з точки зору надійності живлення, незалежності точок доступу однієї від іншої, а також повної смуги доступу (до 1 Гбіт/с) для кожної з них.
- Точки доступу комплектуються кільцевими пластинами для зручного закріплення на підвісні стелі, що спрощує монтаж (див фото):

2. Налаштування (конфігурування) точки доступу

Перед встановленням точки доступу в місця експлуатації, де як правило, доступ до них може бути ускладненим, необхідно налаштувати точки доступу як мінімум так, щоб вони були доступні з локальної мережі через Ethernet-інтерфейс від комутатора та могли бути повністю налаштовані після встановлення.[2]

Адміністратори УРАН вводять такі параметри:

1) Режим *Bridge* для портів *IN port* та *OUT port,* що забезпечує підключення всіх точок доступу у ланцюжку до одного і того ж сегменту локальної мережі організації.
2) Встановлений режим *DHCP* для автоматичного отримання IP-адреси (а також маски та адреси шлюзу) та адреси DNS.
3) Початково точки доступу налаштовані на взаємодію з національним eduroam сервером URAN (212.111.203.54). [3]
4) Для WiFi інтерфейсів встановлений діапазон IP-адрес: **172.16.0.1/22**, що забезпечить до 1000 WiFi підключень одночасно до кожної точки доступу.[4]
5) В кожну точку доступу внесені два SSID: ***eduroam*** та ***mikrotik***. Для SSID ***mikrotik*** пароль доступу *MiKrOtIk*, такий самий, як і для користувача *mikrotik* через Ethernet-порти. SSID ***mikrotik*** може використовуватись для моніторингу та тестування роботи.
6) Для доступу адміністратора організації до точки доступу в режимі моніторингу (без можливості змін налаштувань) створений аккаунт: Name: *mikrotik* ; password *MiKrOtIk*.[5]
7) Потужність передачі сигналу від точки доступу виставлена відповідно до норм, дозволених в Україні.[6]

Після виконання вищезазначених дій з точками доступу їх можна змонтувати (закріпити) в місцях постійної експлуатації. Фізичне втручання в них вже не буде потрібним, за винятком можливих неполадок.

---

[2] Адміністратори УРАН налаштували точки доступу таким чином, що їх додаткове налаштування непотрібне.

[3] Через шлюз в локальній мережі забезпечується доступ до Інтернет. Також для роботи eduroam повинні бути пропущені порти: **Authentication Port UDP 1812** та **Accounting Port UDP 1813** на шляху до сервера 212.111.203.54 Також для можливості моніторингу всіх точок доступу з одного місця (зокрема, з робочого комп'ютера адміністратора) потрібно забезпечити доступ зао IP-адресою до інших точок доступу, в тому числі до тих, що встановлені в інших сегментах локальної мережі.

[4] Якщо цей діапазон перетинається з IP-адресами сегмента локальної мережі, до якого планується підключати точки доступу, то перед відправкою точок доступу зверніться до адміністрації УРАН для попереднього узгодження і зміни цього діапазону.

[5] Звертаємо увагу на незрозумілу несумісність cAP ac з мобільними пристроями фірми Apple, зокрема з **iPhone 8 (MX1E2J/A), iOS 13.5.1** та **iPAD Air (ME906J/A), iOS 12.4.4**. Для пароля довжиною 8 символів з'єднання не відбувалось. Збільшення довжини пароля до 11 символів усуває проблему.

[6] Якщо організація має необхідність встановити динамічне збільшення потужності випромінювання для віддалених абонентів, зверніться до адміністрації УРАН з відповідним запитом.

3. Моніторинг встановлених точок доступу

Після встановлення в місця експлуатації та підключення до локальної мережі організації всі точки доступу повинні стати доступними з локальної мережі для моніторингу та можливого подальшого налаштування або зміни налаштувань в процесі експлуатації.

Доступ до встановлених точок доступу здійснюється через локальну мережу організації по IP-адресі кожної з них. Ці IP-адреси призначаються динамічно через DHCP кожного локального сегменту, до якого підключена точка доступу, тому їх неможливо знати попередньо, а треба визначити після підключення точок доступу до локальної мережі організації.

3.1. Визначення IP-адрес точки доступу

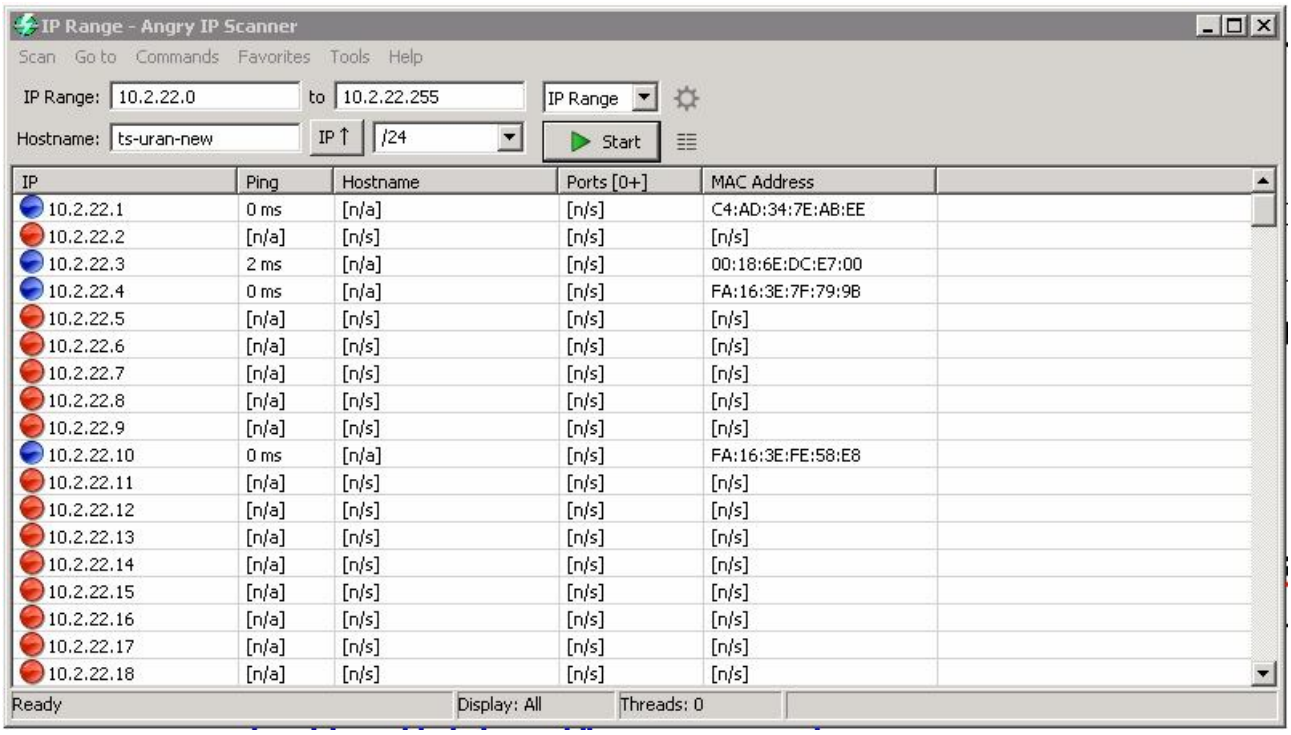
Визначення IP-адрес виконується шляхом сканування локальної мережі за допомогою програми ***Angry IP scanner*** з використанням Ethernet MAC-адрес, які нанесені на пакувальні коробки кожної точки доступу, а також прописані в актах передачі. Також треба знати блоки IP-адрес сегментів локальної мережі організації, до яких підключені точки доступу.

3.1.1. Встановлення та використання *Angry IP scanner*

Ця програма сканування IP-адрес надається по Freeware ліцензії, не потребує інсталяції та виконується одразу. Її можна завантажити за посиланням:

https://angryip.org/download/#windows

Існують версії для 32-розрядних та 64-розрядних процесорів.



Такий вигляд має інтерфейс програми після сканування сегмента. Потрібна нам інформація – це активні IP-адреси та їх MAC-адреси. Порівнюючи MAC-адреси з таблиці з MAC-адресами точок доступу, визначаємо їхні IP-адреси.

Якщо блок IP-адрес, що сканується, знаходиться за маршрутизатором, то результат нічим не відрізняється від локального сегмента, який тут показаний.

Існують й інші програми-сканери з аналогічними функціями.

3.2. Моніторинг точки доступу

Для моніторингу та, можливо, для конфігурування точки доступу ми пропонуємо дві можливості.

3.2.1. Моніторинг, вбудований у точку доступу

В точках доступу **Mikrotik cAP ac** доступний вбудований моніторинг. Доступ до нього через Ethernet-інтерфейс по http-протоколу за посиланням:

http://{IP}/graphs/, де {IP} – IP-адреса конкретної точки доступу, отримана, наприклад, за допомогою програми ***Angry IP scanner*** відповідно до п.3.1.

Вбудований моніторинг дозволяє отримати графіки (daily, weekly, monthly, yearly) трафіків на інтерфейсах, використання процесора, пам'яті та диску. Наприклад http://212.111.197.70/graphs показує моніторинг **Mikrotik cAP ac**, що встановлені в Київському палаці дітей на юнацтва.

Вбудований моніторинг можна отримати також через WiFi підключення до кожної точки доступу, наприклад: http://172.16.0.1/graphs/

3.2.2. Моніторинг та менеджмент через Winbox.

Можна використовувати програму ***Winbox***, яку потрібно встановити на Windows ПК, що буде використовуватись для менеджменту мережі:

https://mt.lv/winbox – інсталяція для 32-розрядного процессора;
https://mt.lv/winbox64 – інсталяція для 64-розрядного процесора

Winbox існує також і для інших операційних систем, зокрема для Android OS для мобільних гаджетів на Google PlayStore.

Маючи IP-адресу, отриману в результаті сканування, ви зможете підключитись до конкретної точки доступу для її моніторингу та менеджменту. При цьому вам зможе допомогти інструкція по ***Winbox***:

https://wiki.mikrotik.com/wiki/Manual:Winbox

Для **менеджменту** треба мати адміністративний аккаунт з правами запису. Якщо виникне потреба в такому доступі, зверніться до адміністрації УРАН із запитом.

4. Реєстрація користувачів eduroam.

Для тестування доступу до eduroam через встановлені WiFi точки доступу в зоні **uran.ua** створений тестовий обліковий запис:

guest@uran.ua з паролем: *guest*

Для авторизації користувачів при доступі до мережі SSID ***eduroam*** точка доступу повинна бути підключена до RADIUS-сервера мережі (RS). Локальна мережа та брандмауер мають пропускати **Authentication Port UDP 1812** та **Accounting Port UDP 1813** на шляху до RS. Початково клієнти RS точки доступу налаштовуються на RS URAN 212.111.203.54 для забезпечення роботи Managed IdP та авторизації користувачів, що вже мають обліковий запис та пароль для авторизації через ***eduroam***.

Організація може створити свій RS з базою користувачів і розмістити його або на фізичному сервері в локальній мережі організації, або у хмарі. УРАН може надати можливість розміщення RS в хмарі за окремим зверненням від організації.

Для кількості користувачів < 200 можна скористатись онлайн послугою *Managed IdP*. Це веб-портал, на якому створюється сторінка доступу для організації. На цій сторінці представник організації вводить дані про свою організацію і починає створювати базу даних своїх користувачів. Портал дозволяє реєструвати користувачів організації через веб-інтерфейс, а база даних і автентифікація користувачів буде знаходитись і виконуватись у хмарі. Для впровадження в організації *Managed IdP* зверніться до адміністрації УРАН.

5. Принципи надання послуги eduroam

Принципи, яких УРАН буде дотримуватись при впровадженні eduroam з постачанням точок доступу:

1) Принцип безпеки. Доступ до мережі надається тільки зареєстрованим користувачіам. Технологія eduroam це забезпечує. Також ми встановили на точки доступу лише один додатковий SSID ***mikrotik*** для технологічного використання, який захищено паролем.
2) Доступ до eduroam повинен бути забезпечений також для студентів. На звернення організації УРАН зможе надати безкоштовний інтернет-трафік для eduroam.

6. Особливості впровадження Mikrotik cAP ac з eduroam.

Для організацій, в яких вже є впроваджені **Mikrotik cAP ac**, можуть виникати варіанти впровадження точок доступу, отриманих від УРАН.

1) Мережа cAP ac впроваджена в організації з використанням ***CAPsMAN*** – програми групового керування cAP ac. В такому варіанті найкращим рішенням буде впровадження нових точок доступу від УРАН згідно з цією інструкцією, як ще однієї групи модулів. Підключення ж існуючої мережі **Mikrotik cAP ac** до eduroam зможе виконати адміністратор УРАН через віддалений доступ, наприклад з використанням програми ***TeamViewer***.
2) Якщо організація захоче мати свій власний RS замість використання *Managed IdP,* то його можна розмістити в одній з точок доступу. Для цього організація має повідомити дані інтерфейсу підключення цієї точки доступу до Інтернет із зовнішньою IP-адресою. УРАН встановить на неї RS та налаштує його.