REPORT - Workshop on Implementing eduroam on a Campus Network

Introduction

Held from 09 October 2024 to 11 October 2024, the workshop on Implementing eduroam on a Campus Network, at the premises of at University of Lagos brought together participants from several institutions, including : Central University, TOGORER, Federal University of Health Sciences, zare, Michael Okpara University Of Agriculture, Umudike Abia State Nigeria, Nnamdi Azikiwe University, Federal University of Kashere, Joseph Sarwuan Tarka University, Intern, Ahmadu Bello University, Federal University of Health Sciences, Otukpo, Federal University of Technology, Akure (NgNOG), Eko-Konnect, University of Ibadan, Covenant University, Nigerian Research and Education Network (NgREN), University of Jos, University Of Benin, Benin City, Covenant University and University of Lagos (UNILAG).

The objectives of the workshop were to:

- Improve eduroam coverage in NGREN institutions
- Educate participants on eduroam's robust security features and best practices for maintaining secure, reliable network access for all users.
- Provide participants with hands-on experience in deploying and configuring Eduroam on campus networks.
- Train participants using the eduroam Switchboard and eduID to manage federations and user identities proficiently.
- To foster collaboration and knowledge sharing among network administrators within the WACREN community.
- Promote eduroam adoption and enhancement to ensure seamless global connectivity and support international academic collaboration.

The training covered three days, following the schedule below :

Day1: 9 oct. 2024

The training session commenced with a thorough introduction to Wi-Fi network security, offering a detailed exploration of the RADIUS protocol, with a focus on its implementation through FreeRadius. The trainer not only explained the technical components of RADIUS but also emphasized its vital role in securing Wi-Fi networks, especially in environments with mobile devices. This initial overview equipped participants with a strong foundation in the core concepts of the protocol, enabling them to understand how it integrates into the broader context of network security and mobility management.

After establishing this theoretical groundwork, the trainer shifted focus to the eduroam federation, a key component for educational institutions that require secure and seamless wireless access across campuses. The session covered the essential steps of configuring an eduroam setup, from the initial installation and configuration of services to the deployment and upkeep of a federation-level RADIUS (FLR) server. Participants were guided through the intricacies of setting up and maintaining an eduroam Service Provider (SP) and Identity Provider (IdP) within the context of a campus network. This hands-on section was designed to provide practical experience, ensuring that attendees not only understood the theoretical aspects but were also equipped to handle real-world deployment and management of the eduroam infrastructure.

By the end of the session, participants had gained both a comprehensive understanding of Wi-Fi security protocols and practical skills in implementing and maintaining a campus-wide eduroam system, positioning them to effectively manage such environments in their own institutions.

Day2: 10 oct. 2024

The day began with a deep dive into advanced RADIUS protocols, focusing on key components of the eduroam infrastructure. The session covered various elements, including the Regional Proxy Server (RPS), managed by WACREN, the Federation Level Radius (FLR) at the national level, which is overseen by a National Research and Education Network (NREN), as well as the Network Access Server (NAS), eduroam Service Provider (SP), Identity Provider (IdP), and the Supplicant. The Supplicant is a software (often embedded in the Operating System but also available as a standalone program) that leverages the 802.1X protocol to send authentication requests via EAP.

Next, the session delved into EAP protocols and their role within the eduroam federation. After a coffee break, the focus shifted to eduroam CAT, exploring how to set it up and use it to streamline eduroam management within a campus network, as well as how to monitor log statuses within the eduroam network.

The session concluded with a practical segment that included knowledge sharing through the presentation of Switchboard and eduroam exercises. This involved registering FLR, IdP, and SP, adding NAS (Access Points) to the Switchboard, and updating configuration files (clients.conf and proxy.conf) on the RPS, FLR, and IdP+SP. Finally, participants learned how to configure the NAS and test user authentication, both for local users and visitors.

Day3: 11 oct. 2024

The final day of the training focused on the eduroam deployathon held at the Unilag Campus. The day was dedicated to hands-on deployment and configuration activities, where participants applied the knowledge gained throughout the training.

Key tasks included:

- Setting up and configuring eduroam Service Provider (SP) and Identity Provider (IdP) services within the campus network.
- Registering and configuring Network Access Servers (NAS) on the eduroam Switchboard.
- Updating essential configuration files (clients.conf and proxy.conf) on the Federation Level RADIUS (FLR), RPS, and IdP/SP systems.
- Testing user authentication processes, including both local users and visitors, to ensure proper integration.
- Introduce eduroam CAT

Participants successfully deployed a functional eduroam IdP to demonstrate the skills acquired over the course of the training.

Perspectives

- Resolve backend database issue: UniLag deployment during the workshop uses the backend database on ngren.eduid.africa, another backend exists and the UniLag admins have to select one
- Update the eduroam instances manager for some institutions (eko-konnect, Nnamdi Azikiwe, ...)
- Get instances admin to update service locations based on the template spreadsheet
- Have NGREN NRO to invite instances admin to eduroam CAT
- improve logging and monitoring

Conclusion

The three-day eduroam deployathon at Unilag Campus was an intensive and highly productive learning experience for all participants. The training began with a solid theoretical foundation on Wi-Fi security and RADIUS protocols, followed by an in-depth exploration of the eduroam federation's core components such as the Regional Proxy Server (RPS), Federation Level Radius (FLR), eduroam Service Provider (SP), Identity Provider (IdP), and Network Access Server (NAS). Participants were able to grasp the importance of EAP protocols and how they function within the eduroam framework.

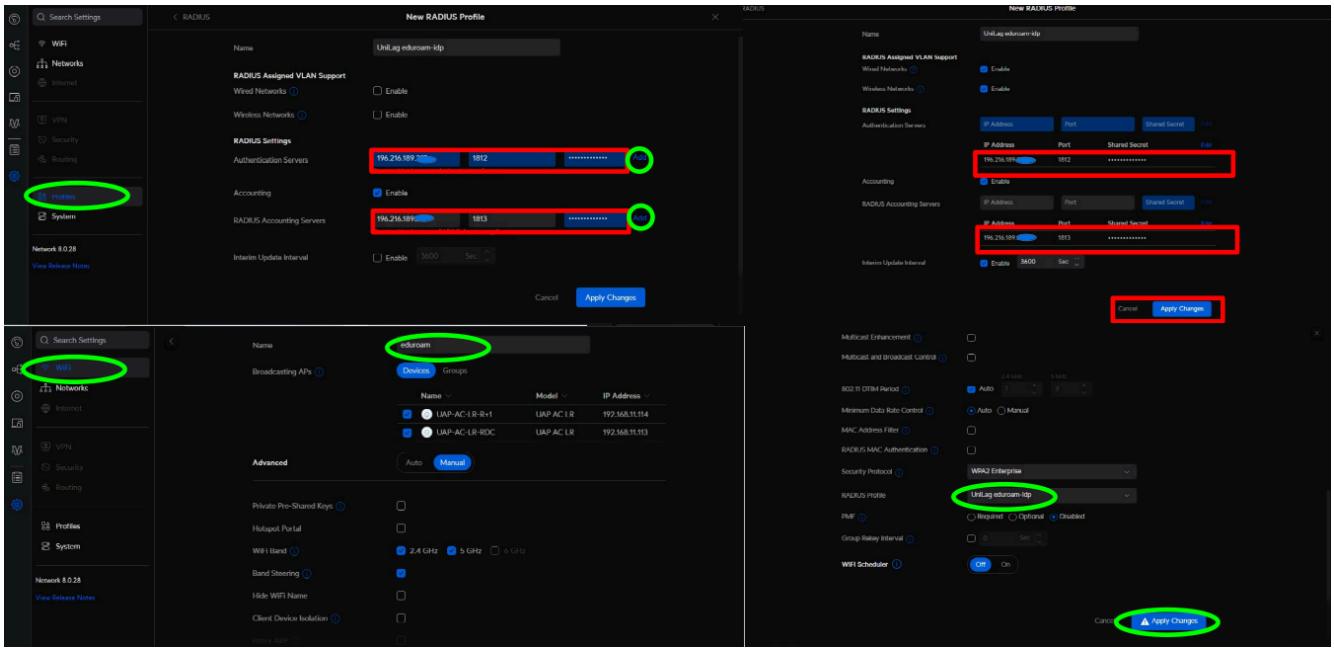
Hands-on sessions on eduroam CAT, log monitoring, and the use of the Switchboard provided participants with practical skills in configuring and managing eduroam services in a campus network. The final day's deployathon was particularly valuable, allowing attendees to apply their theoretical and practical knowledge to fully set up and test eduroam in a real-world scenario.

By the end of the training, participants were equipped with both the technical knowledge and practical experience needed to deploy and maintain a secure eduroam network at their own institutions. The event was successful in fostering a deeper understanding of eduroam deployment and enhancing the participants' confidence in managing network authentication and security protocols.

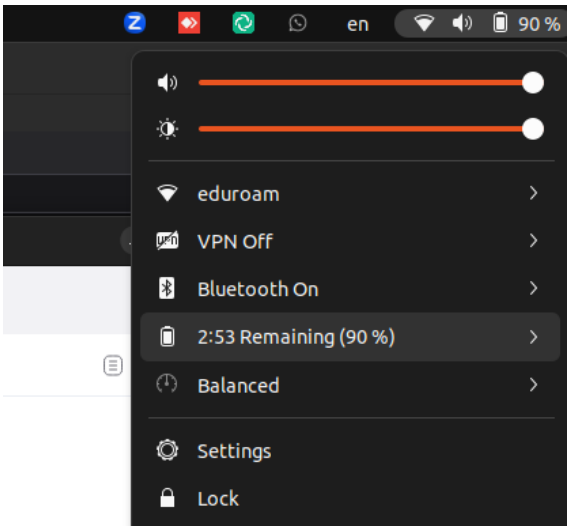
Annex

Annex 1

Group photo of Participants



NAS configuration, radius profil creation



Test connectivity to eduroam SSID