Session 3: What is eduroam and how it works

eduroam deployathon Workshop

Lagos, October 2024

LOCAL HOST

WITH SUPPORT FROM

Summary

1. Overview of eduroam
2. Components of the eduroam infrastructure
3. deploy eduroam at the national level
4. deploy eduroam at the Campus level
5. Test EAP and eduroam
6. Configuring Supplicants
7. Policies and strategy for the development and management of the National Federation eduroam

Eduroam Overview

acronym for **edu**cation **roam**ing, is a global wireless network infrastructure that aims to facilitate secure Internet access to users of participating academic institutions following the principle "***Start your laptop and get connected***".

based on the mechanisms of**Authentication**,**Authorisation**and of**Accounting/Statistics**implemented by the RADIUS server.

Collaboration between several of these RADIUS servers to realize Authn (by eduroam IdP) and Authz (by eduroam SP)

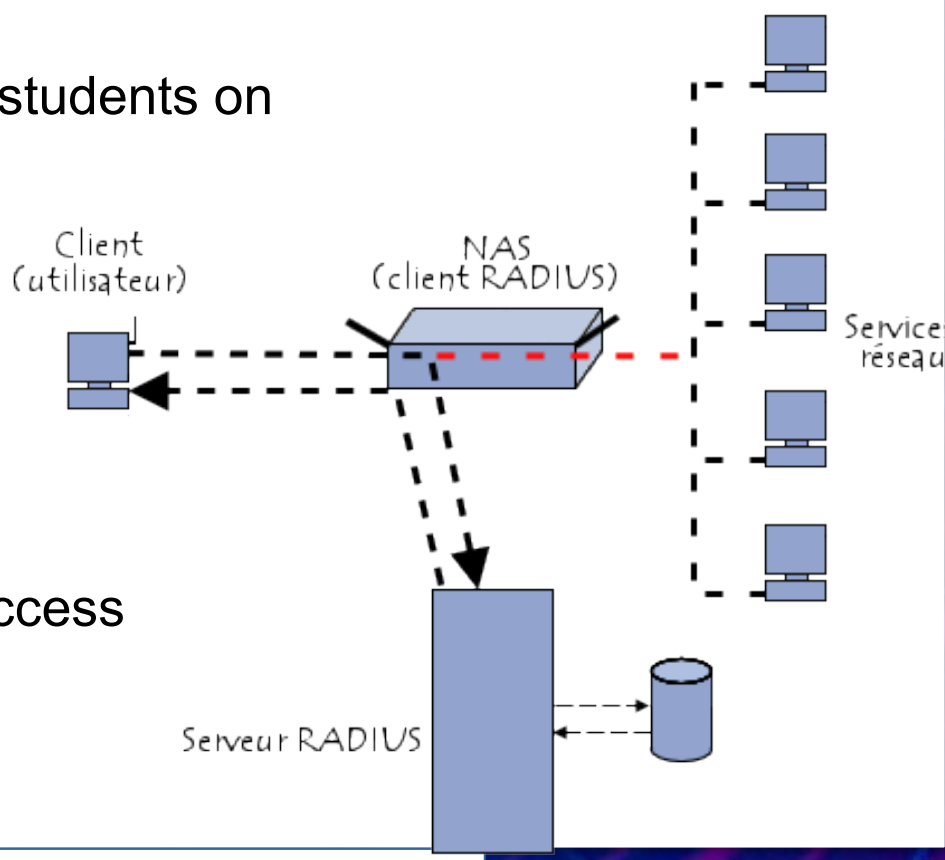
Eduroam Overview: The Benefits

Efficiency:
- No need to provide a visitor account to Teachers/Researchers or students on mobility

Security:
- No more need for an open or shared key guest network
- More precise access control and metrics collection

Better user experience:
- User login with a known and trusted identity for secure network access

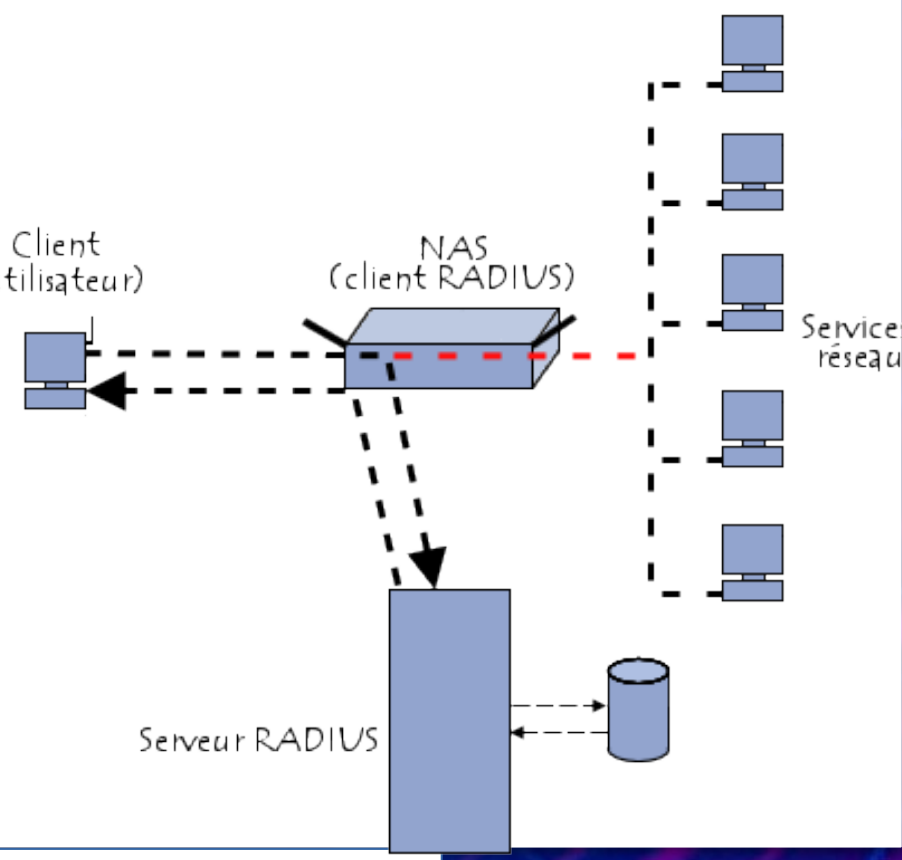
.



Eduroam Overview: Costs and Challenges

Beyond eduroam Infrastructure

IAM: good management of campus identities ie
Who remains an active user?
Who has left the institution and is therefore no longer active?
An infrastructure to disseminate the answers to the 2 questions



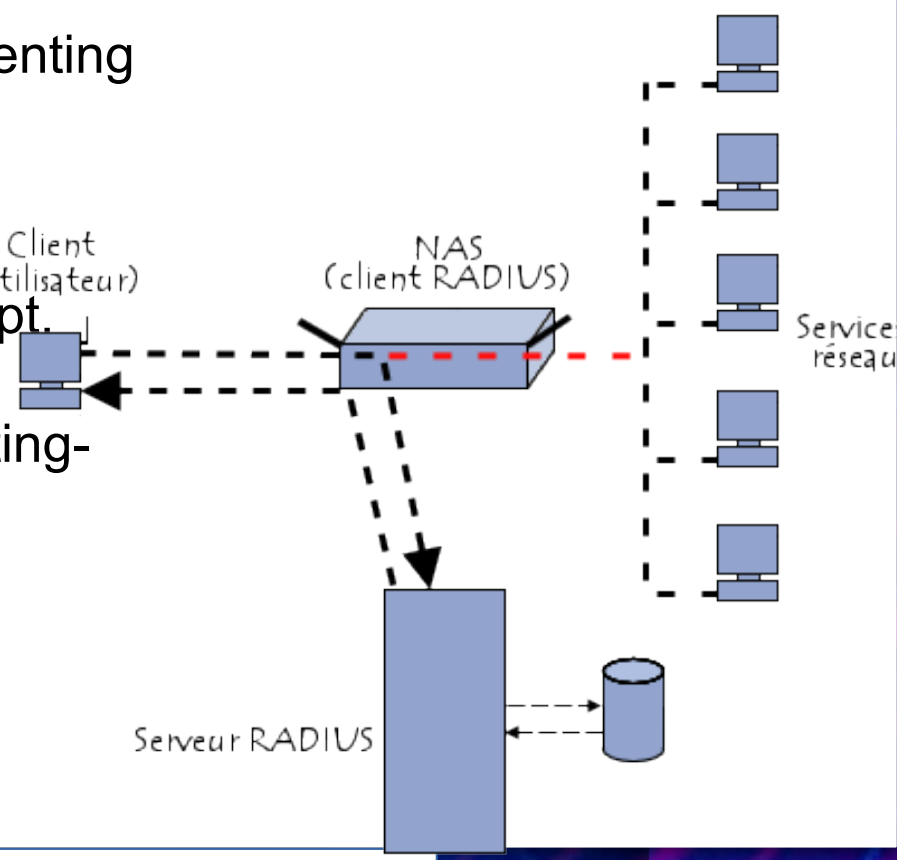
eduroam Overview: How RADIUS Works

RADIUS:**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice protocol implementing AAA processes to secure network access.

Server implementing the RADIUS protocol runs on:

1812: Authn+Authz(Access-Request, Access-Challenge, Access-Accept, Access-Reject)

1813: Traceability/Accounting/Statistics (Accounting-Request, Accounting-Response, Accounting-Status)



eduroam Overview: How RADIUS Works

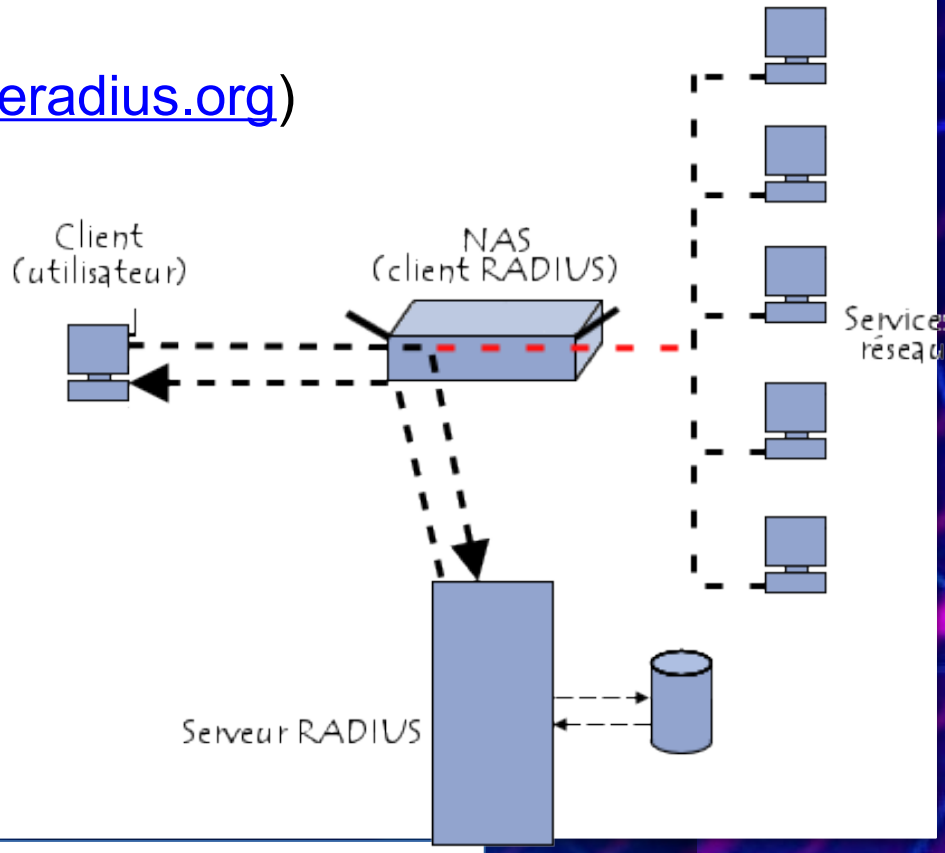
FreeRadius: Implementation of the RADIUS protocol (https://freeradius.org)

.

Originally developed by Alan Dekok & Miquel van Smoorenburg

Very active community

Debugging:
- freeradius -X ; radiusd -X
- https://networkradius.com/freeradius-debugging/



eduroam Overview: How RADIUS Works

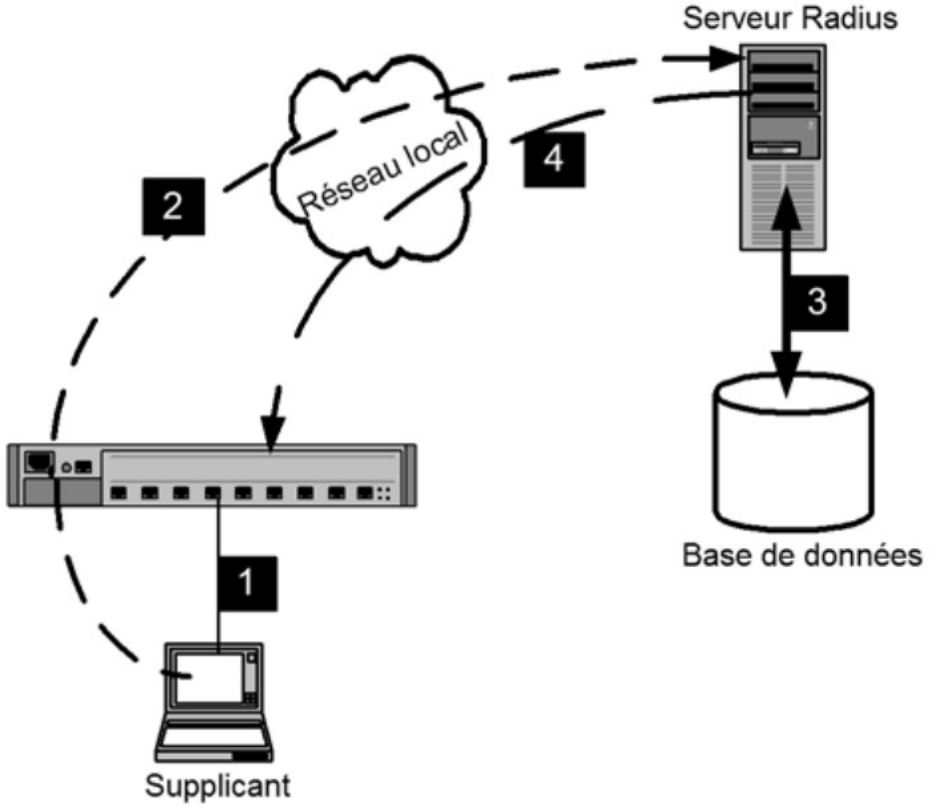
Connection diagram to a controlled access network

1-**Initialization**: NAS detects supplicant's connection attempt

2-**Identification**: identification request/identification response/access request

3-**Protocol negotiation**: Reception of challenge/Transmission of challenge/Acceptance or rejection of challenge by the supplicant

4-**Authentication**: Authentication Request/Response; Acceptance or Rejection of authentication by the server



eduroam Overview: How RADIUS Works

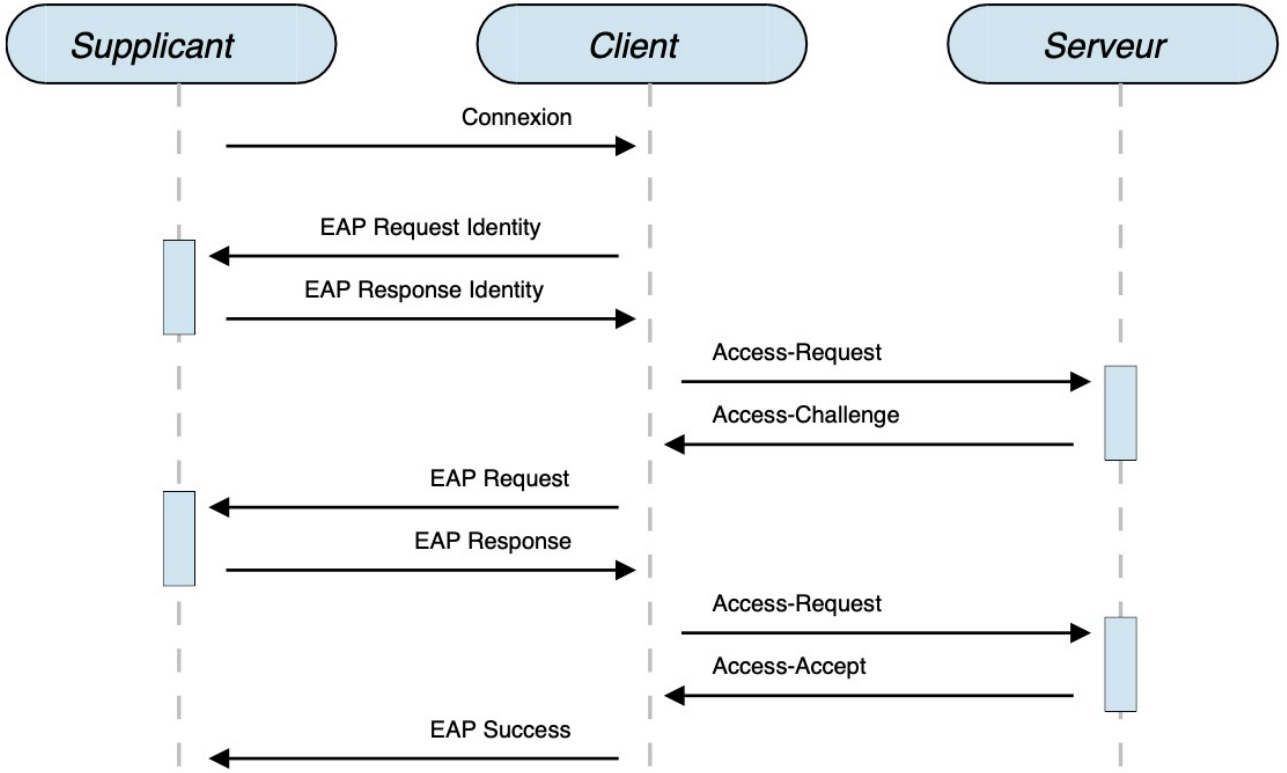
EAP:**E**xtensible Authentication **P**rotocol (802.1x or dot1.x) : authentication protocol transport protocol.

EAP packets: Request, Response, Success, Failure

Authentication protocols carried EAP methods:

MD5:EAP-MD5
TLS: Auth Server, Auth Client, Encryption
PEAP-MSCHAPv2: Auth Server, Auth Client(username/password)
TTLS: Server auth by the client
FAST:

eduroam Overview: How RADIUS Works



eduroam Overview: How RADIUS Works

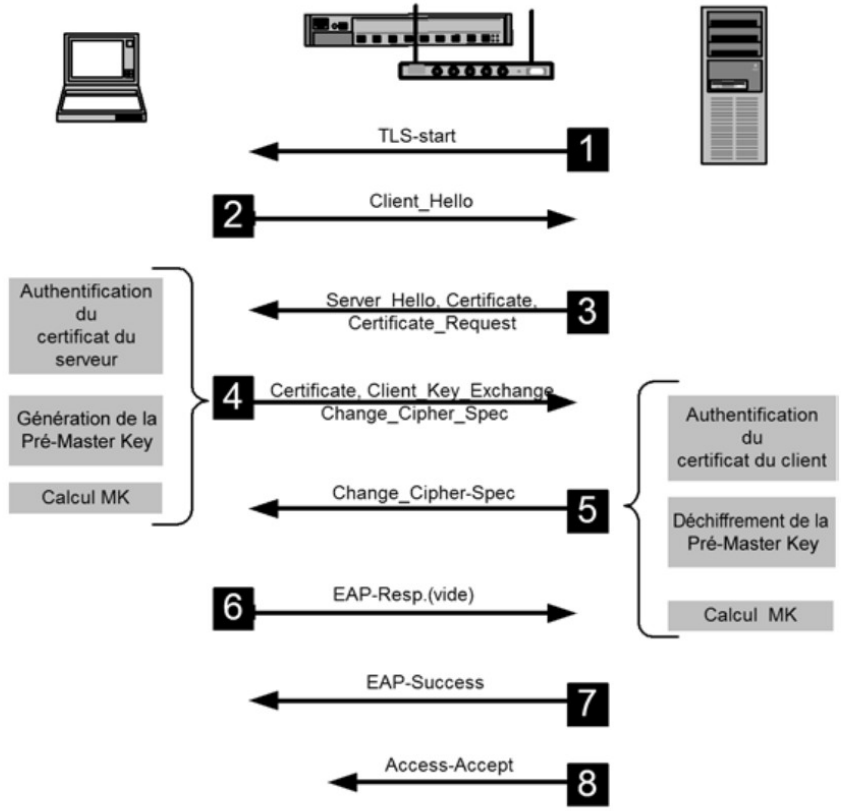
EAP-TLS inner-working

1- The server sends the supplicant a TLS start request
By means of an EAP-Request packet containingEAP-Type=TLS

2- The supplicant responds (Client_Hello) with the list of algorithms encryption it is capable of using.

3- The server responds (Server_Hello) by transmitting the algorithm it has ch among the list he received, and another challenge

4- The supplicant authenticates the server's certificate. Then it sends its cert with its public key (Client_Certificate)



5-The server authenticates the certificate sent by the supplicant. He deciphers the Pre-Master Key thanks to private key of own certificate

6-The supplicant sends a requestEAP-Responseempty for to indicate that the operations are completed on his side.

7-The server sends the supplicant a packetEAP-SuccessFor notify him that the authentication is accepted

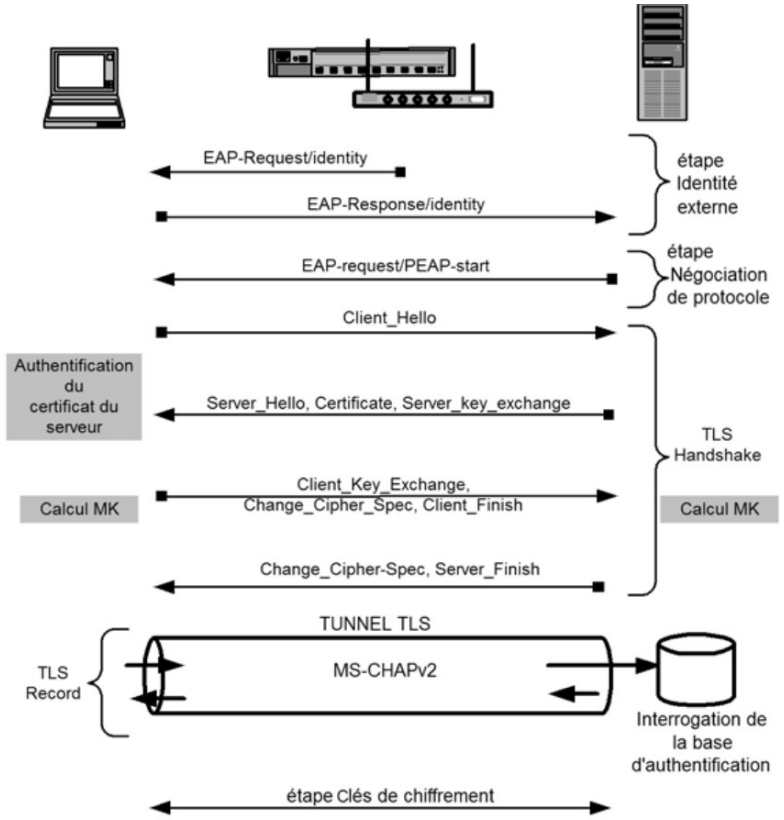
8-An Access Accept packet is sent to the NAS for it command to open the port.

LOCAL HOST

WITH SUPPORT FROM

eduroam Overview: How RADIUS Works

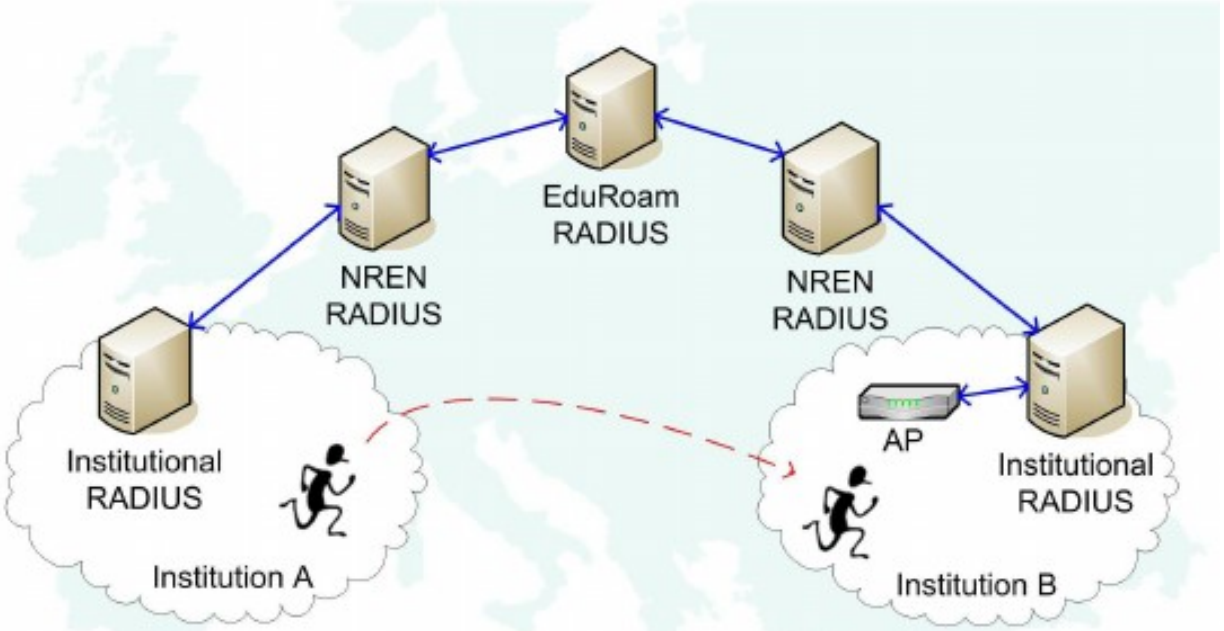
EAP-PEAP inner-working



Eduroam Overview: The components of eduroam

UPSTREAM: eduroam ROOT servers.

RPS: Regional Proxy Server, RADIUS server managing requests at the eduroam confederation level in Africa
FLR: Federation Level Radius
eduroam IdP: eduroam Identity Provider
eduroam SP:eduroam Service Provider
NAS/Authenticator/Client: Network Access System
Access-Points:
Supplicant:
Campus Identity:

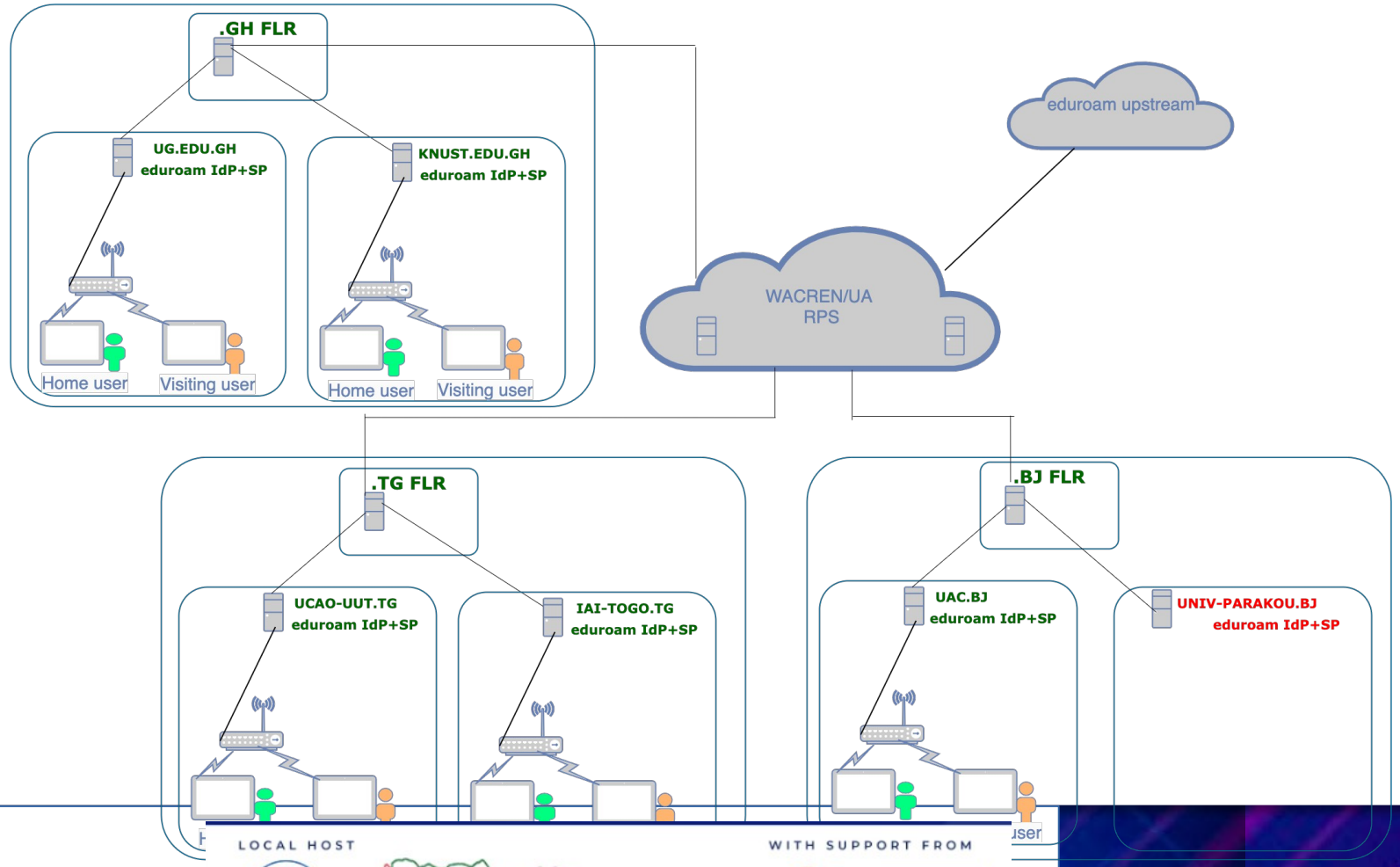


The components of the eduroam infrastructure: eduroam architecture

Operating principle

- Only the institution's eduroam IdP server the user originated from can process his authn request and authenticate him;

- Access authorization can only be granted
- by the eduroam SP server protecting the AP
- the user tried to connect to



LOCAL HOST

WITH SUPPORT FROM

Deploying eduroam at the national level

- **eduroam-FLR**

1- VM or physical machine (2GB RAM, 20GB disk, 2CPUs)

2- RADIUS implementation (Radiator, daloRadius, RadSecProxy,**FreeRadius**)

3- The FLR must be authoritative for a specific ctld e.g.: .bj, .bf, .gh, .ng, …
The ctld of which it is authoritative must be defined in its Upstream

4- the Upstream or TLR to which the FLR must forward the requests of the other ctlds must be defined

5- The eduroam-idp servers of the institutions must define

6- FLR must configure **F-Ticks** to send statistical data (number of connections for the **National Roaming** and the **Roaming International**) a eduroam OT.

Code available for eduroam-flr

https://gitlab.wacren.net/eduroam/eduroam-flr

Deploying eduroam at the national level

- **Test the communication between eduroam-FLR and its clients (up/down**

radtest, radclient

** From the client
sudo docker container exec <containerId> echo "Message-Authenticator = 42" |radclient <FLR-IP> status <Shared-Secret>

** From the FLR
sudo docker container exec <containerId> echo "Message-Authenticator = 42" |radclient <CLT-IP> status <Shared-Secret>

Deploying eduroam at campus level

- **eduroam-idp+sp**

Configuring the Freeradius service as an IdP requires:

1- The generation of **TLS certificate** for the operation of the**EAP methods** supported.

2- The**EAP methods** to support must be activated

3- The **eduroam-inner-tunnel virtual server** must be configured to do **Tunneled EAP Authentication**

4- The Freeradius server must be connected to a server **database** for the **user authentication**.

5- A **realm** must be defined and marked as a local domain known to the IdP server and therefore locally authenticated by it

6- the server must be configured to receive and process requests from the upstream (FLR)

Deploying eduroam at campus level

- **eduroam-idp+sp**

Configuring the Freeradius service as an IdP requires:

1- The generation of **TLS certificate** for the operation of the **EAP methods** supported.

2- The **EAP methods** to support must be enabled (most EAP methods require a certificate https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations)

3- The **eduroam-inner-tunnel virtual server** must be configured to do **Tunneled EAP Authentication**

4- The Freeradius server must be connected to a server Of **database** for the**user authentication**.

5- A **realm** must be defined and marked as local domain known to the IdP server and therefore locally authenticated by it

6- the server must be configured to receive and process requests from the upstream (FLR)

Deploying eduroam at campus level

- **eduroam-idp+sp**

Configuring the Freeradius service as an SP requires the following considerations:

1- The SP only forwards requests to other RADIUS servers

2- The SP does not perform authentication

3- The SP must be aware of the NAS

4- The SP must be configured to receive and process requests from upstream (FLR)

Codes available for IdP+SP

1-https://gitlab.wacren.net/Service/eduroam/eduroam-idp

2- Ansible:
https://gitlab.wacren.net/Service/eduroam/eduroam-ansible

Deploying eduroam at campus level

- **User Support**

Optimize user support through:

1- a dedicated helpdesk service(support@eduroam.tld| support@eduroam.realm).

2- Assisted configuration

Deploying eduroam at campus level

- **eduroam CAT (https://cat.eduroam.org)**

Configuration Assistant Tool(https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators)

1- help to generate a personalized supplicant for your Institution and different OS.

2- requires: idp name, location, logo, support contacts and eduroam IdP server settings

3- The NRO must feed the eduroam database

Deploying eduroam at campus level

- **eduroam CAT (https://cat.eduroam.org)**

Deploying eduroam at campus level

- **EAP Testing**

Test EAP with rad_eap_test (https://github.com/CESNET/rad_eap_test) :

Build rad_eap_test:https://wiki.geant.org/display/H2eduroam/Testing+wi

1- EAP-MSCHAPv2

```
eric@vm3:~/rad_eap_test$ ./rad_eap_test -t 60 -H 196.216.191.183 -P 181 -S testing123 -
utest.eduroam@uv.bf-p xxxx -m WPA-EAP -e PEAP -2MSCHAPV2-s eduroam
access-accept; 0.24 sec |rtt=244ms;;;0;60000 accept=1;0.5:;0:;0;1
```

2- EAP-TTLS

```
eric@vm51:~/rad_eap_test$ ./rad_eap_test -t 60 -H 196.216.191.183 -P 1812 -S testing123 -
utest.ujkz@ujkz.bf-p xxxx -m WPA-EAP -eTTLS-s eduroam
access-accept;0.23 sec |rtt=227ms;;;0;60000 accept=1;0.5:;0:;0;1
```


{:"(3742) Sent**Access-Accept**Id 10 from 172.30.0.2:1812 to**196.216.191.183**:54934 length 186\n","time":"2023-0
{:"(3742) MS-MPPE-Recv-Key = 0xf024a7……a1\n",,"time":"2023-06-17T12:38:37"}
{:"(3742) MS-MPPE-Send-Key = 0xc152….6\n",,"time":"2023-06-17T12:38:37.166156745Z"}
{:"(3742) EAP-Message = 0x03ba0004\n","time":"2023-06-17T12:38:37.166164397Z"}
{:"(3742) Message-Authenticator = 0x00000…..00000\n","stream":"stdout","time":"2023-06-17T12:38:37.166171767Z"}
{:"(3742)**User-Name = \" test.eduroam@uv.bf** \"\n","stream":"stdout","time":"2023-06-17T12:38:37.166213969Z"}

{:"(4842) Sent**Access-Accept**Id 21 from 192.168.128.2:1812 to**196.216.191.191**:52662 length 287\n","time":"2023-06
{:"(4842) MS-MPPE-Recv-Key = 0xf024a7……a1\n",,"time":"2023-06-20T10:30:37"}
{:"(4842) MS-MPPE-Send-Key = 0xc152….6\n","time":"2023-06-20T10:30:37.156256745Z"}
{:"(4842) EAP-Message = 0x03ca0004\n","time":"2023-06-20T10:30:37.156256745Z"}
{:"(4842) Message-Authenticator = 0x00000…..00000\n","stream":"stdout","time":"2023-06-20T10:30:37.156256745Z"}
{:"(4842)**User-Name = \" test.ujkz@ujkz.bf** \"\n","stream":"stdout","time":"2023-06-20T10:30:37.156256745Z"}

Deploying eduroam at campus level

- **Configuring NAS or access points**

The configuration of access points varies depending on the manufacturer (Cisco, Huaewi, Unify, etc.).
But in general it is necessary to:

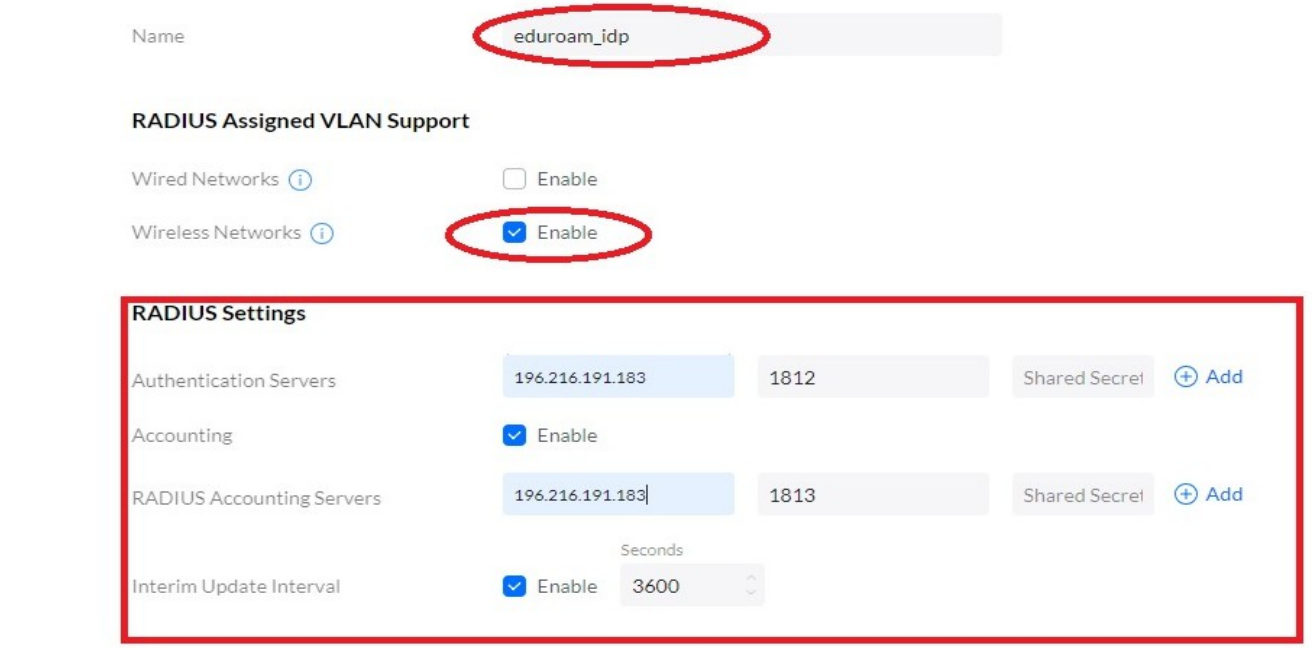
1- Define a security profile (which specifies the eduroam-idp+sp server and the shared secret)

2- create an ssid **eduroam** with WPA2-Enterprise support and associate the profile defined in 1

Deploying eduroam at campus level

- **Configuring NAS or access points**

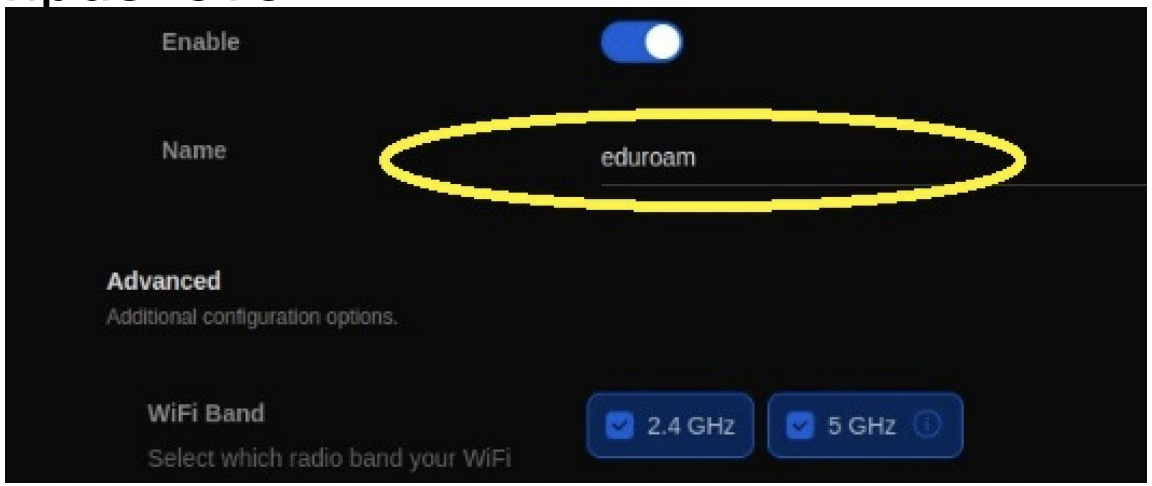
1- Create a radius profile on a controller Unify



Deploying eduroam at campus level

- **Configuring NAS or access points**

1- Create an eduroam ssid and assign the Security profile

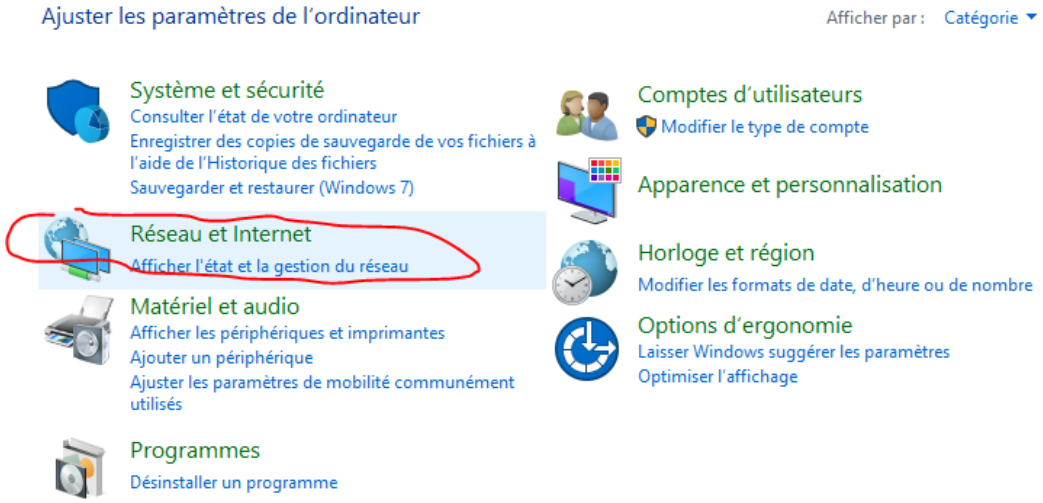


Deploying eduroam at campus level

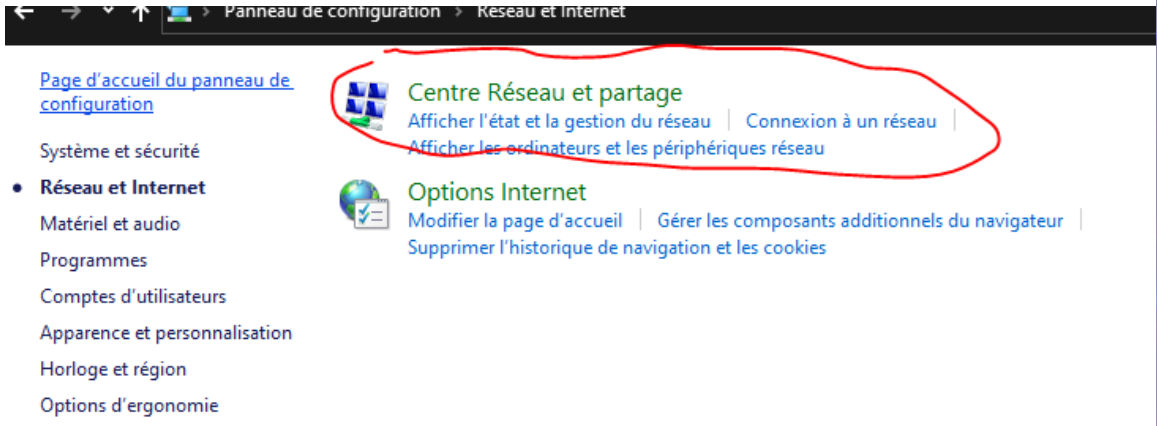
- **MacOS Client Configuration**

Deploying eduroam at campus level

- **Configuring Supplicant Windows**



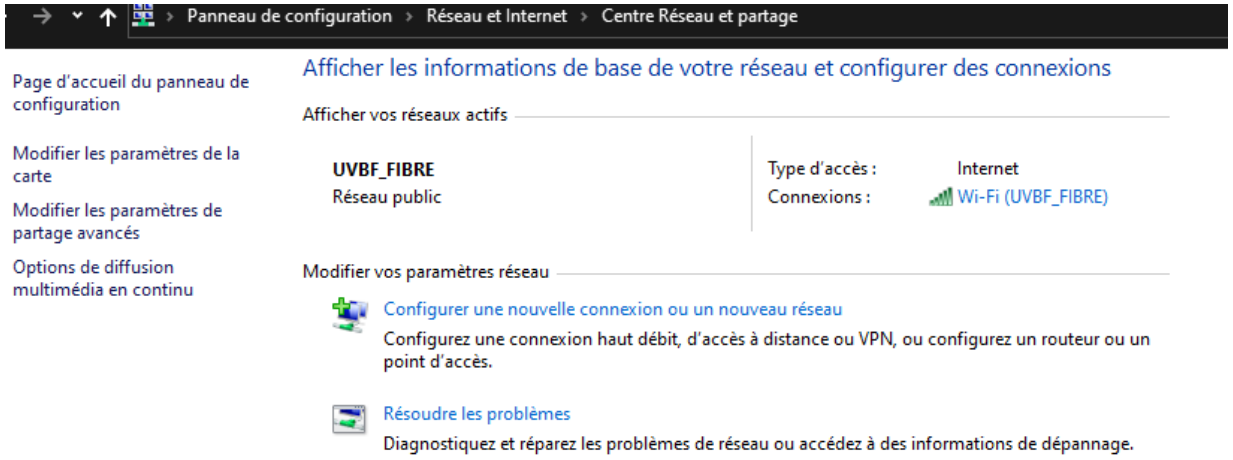
Step 1



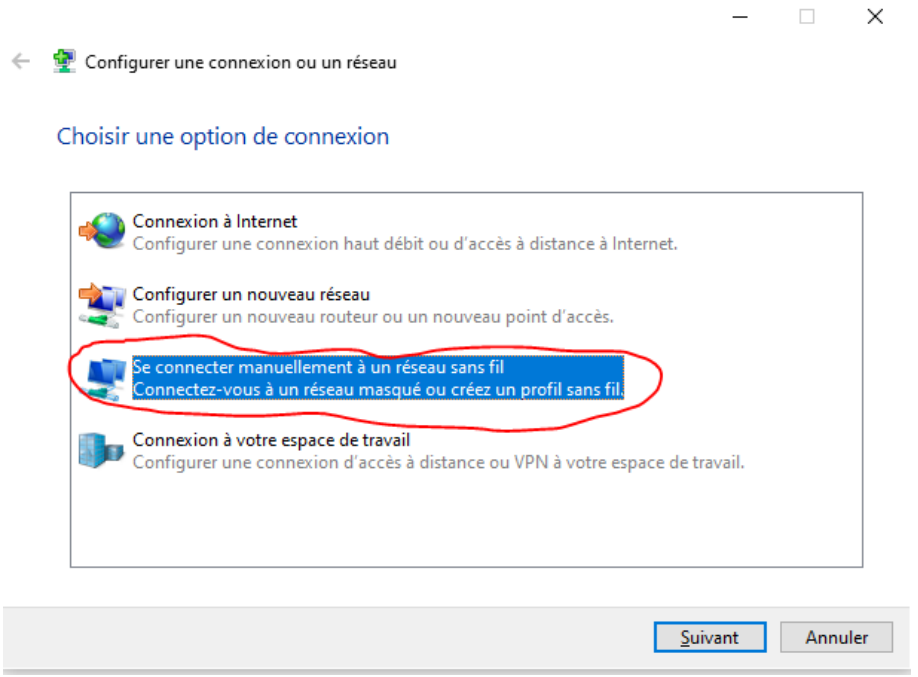
Step 2

Deploying eduroam at campus level

- **Configuring Supplicant Windows**



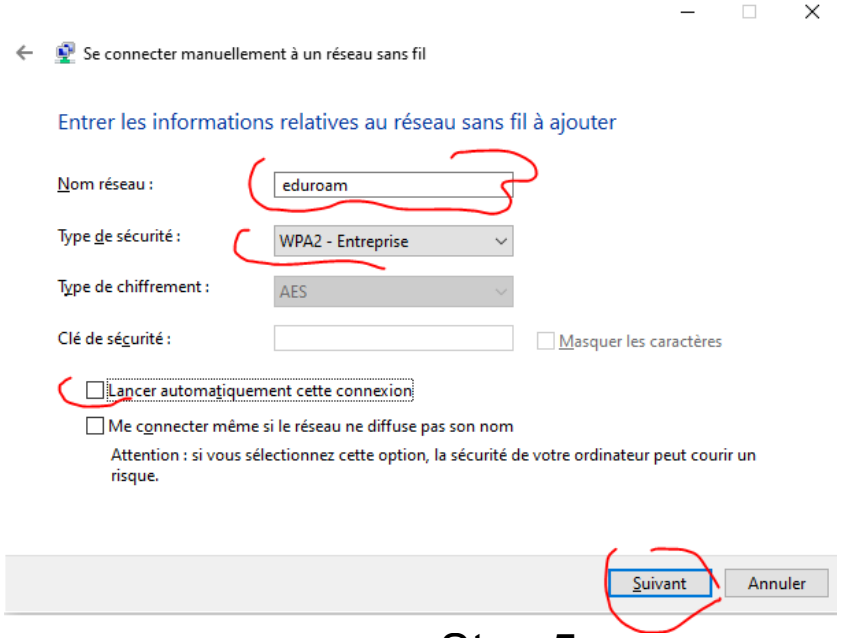
Step 3



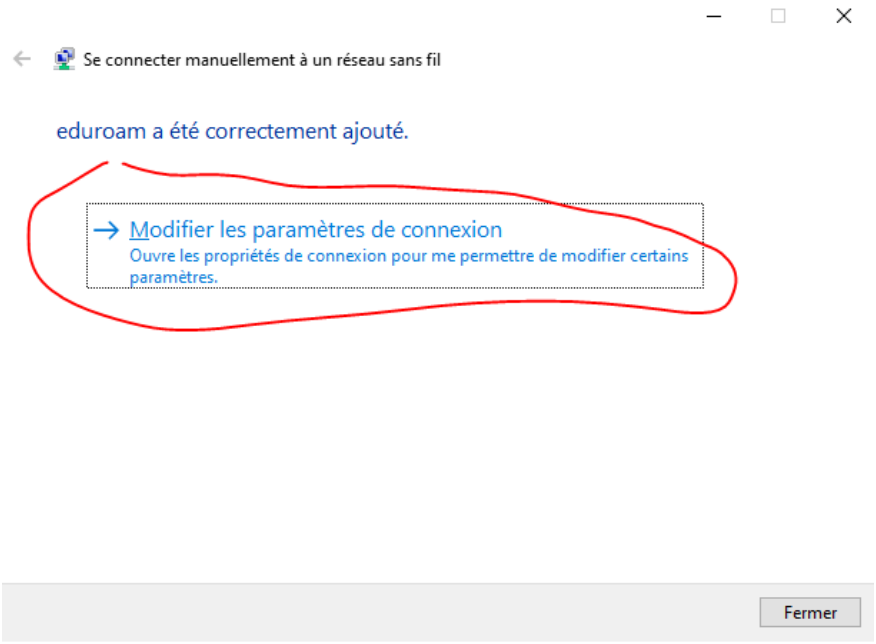
Step 4

Deploying eduroam at campus level

- **Configuring Supplicant Windows**



Step 5



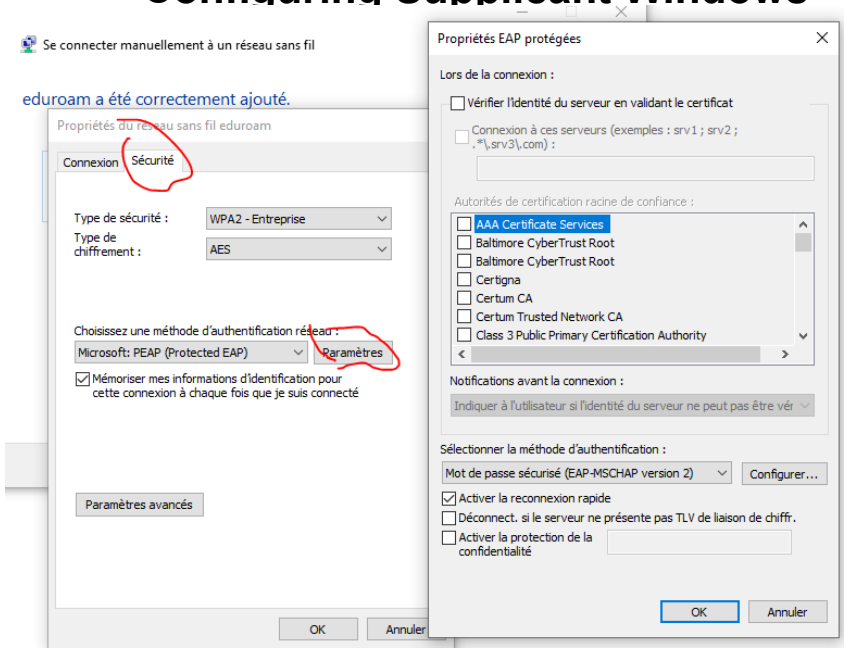
Step 6

LOCAL HOST

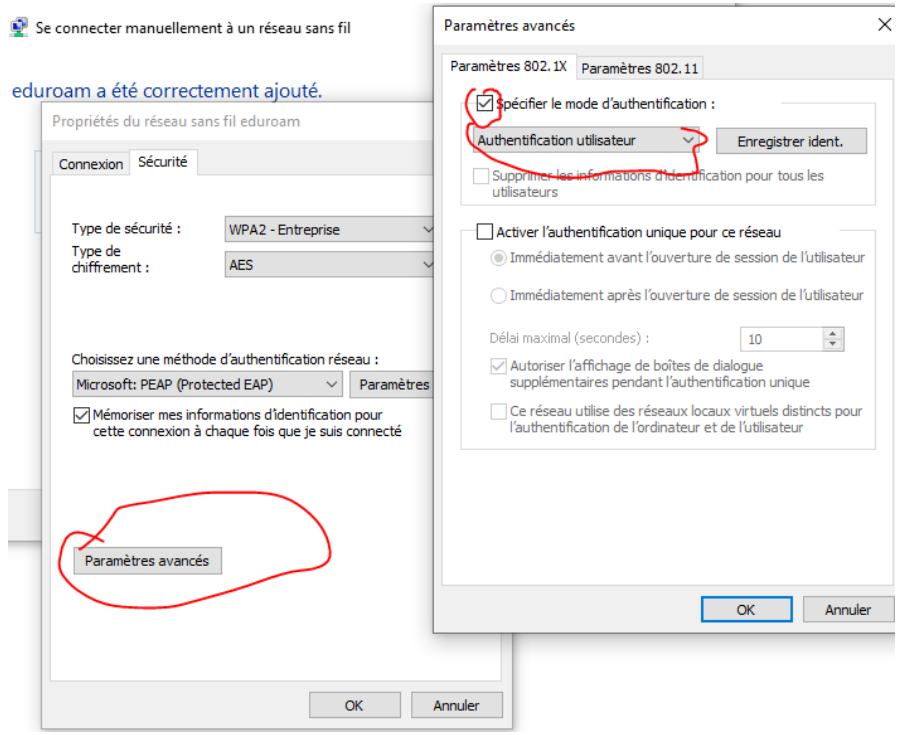
WITH SUPPORT FROM

Deploying eduroam at campus level

- **Configuring Supplicant Windows**



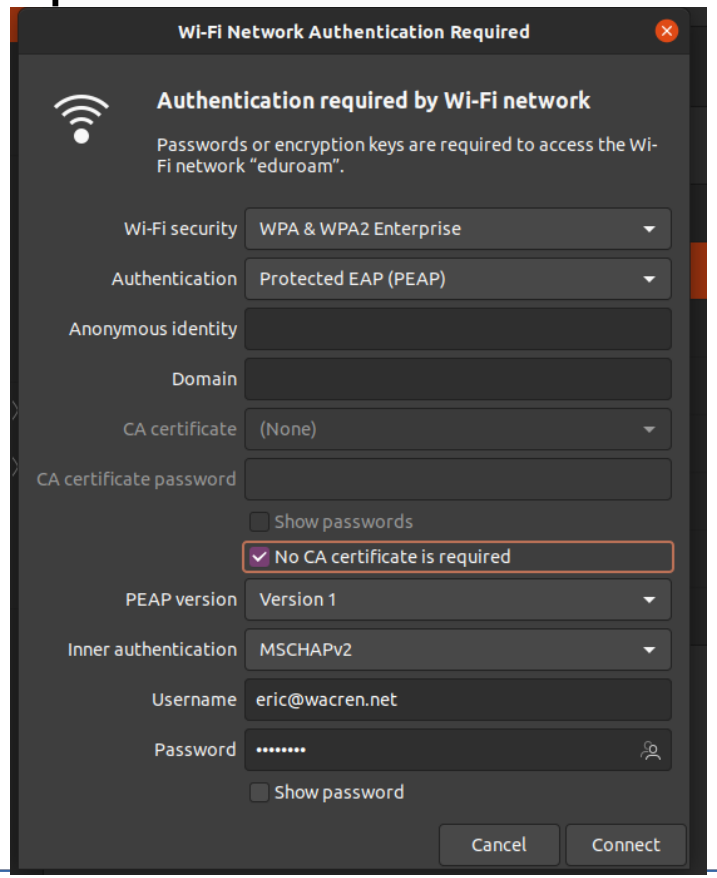
Step 7



Step 8

Deploying eduroam at campus level

- **Setup Supplicant Linux**



Deploying eduroam at campus level

- **Logging client connection**

```
e_idp |(10) Received Access-Request Id 23 from 102.180.19.51:37756 to 172.29.0.2:1
e_idp |(10) User-Name = " testuser@wacren.net "
e_idp |(10) NAS-IP-Address = 192.168.11.113
e_idp |(10) NAS-Identifier = "7ad79a18b48e"
e_idp |(10) Called-Station-Id = "7A-D7-9A-18-B4-8E:eduroam"
e_idp |(10) NAS-Port-Type = Wireless-802.11
e_idp |(10) Service-Type = Framed-User
e_idp |(10) Calling-Station-Id = "8E-32-29-7B-BD-63"
e_idp |(10) Connect-Info = "CONNECT 0Mbps 802.11b"
e_idp |(10) Acct-Session-Id = "82B6E62A96E3B9BC"
e_idp |(10) Acct-Multi-Session-Id = "D535140D9761B8C8"
e_idp |(10) WLAN-Pairwise-Cipher = 1027076
e_idp |(10) WLAN-Group-Cipher = 1027076
e_idp |(10) WLAN-AKM-Suite = 1027073
e_idp |(10) Framed-MTU = 1400
e_idp |(10) EAP-Message =
0x0282002e190017030300234b5a2059e391865d9bbca1e252f65d556e1eb38aa9930
e_idp |(10) State = 0xc0d366c9c9517ffbfb513e9673252cb4
e_idp |(10) Message-Authenticator = 0x857dcf391a55463a95ffdeab03033079
```

```
(10) Proxying request to home server 196.216.191.177 port 1812 timeout 20.000000
|(10) Sent Access-Request Id 140 from 0.0.0.0:60916 to 196.216.191.177:1812 length 179
 |(10) User-Name = " testuser@wacren.net "
 |(10) NAS-IP-Address = 192.168.11.113
|(10) NAS-Identifier = "7ad79a18b48e"
|(10) Calling-Station-Id = "8E-32-29-7B-BD-63"
|(10) EAP-Message =
0x0282002e190017030300234b5a2059e391865d9bbca1e252f65d556e1eb38aa99306de70fa542
|(10) State = 0xc0d366c9c9517ffbfb513e9673252cb4
|(10) Message-Authenticator = 0x857dcf391a55463a95ffdeab03033079
|(10) Operator-Name := "uvbf.bf"|(10) Proxy-State = 0x3233
```

Deploying eduroam at campus level

- **Logging client connection**

```
eduroam_idp | (10) Sent Access-Accept Id 23 from 172.29.0.2:1812 to 102.180.19.51:37756 length 166
eduroam_idp | (10) MS-MPPE-Recv-Key =0x68ee64fcb04e068cbcb1322f6332e95cf6b8a7735efb9f6059d68871e3c33e94
eduroam_idp |(10) MS-MPPE-Send-Key =0xed8862c92dd3d7b4b9ac68dfb33ff0a1e3ffcef158ed34df8bf3f33d623134a6
eduroam_idp |(10) EAP-Message = 0x03820004
eduroam_idp |(10) Message-Authenticator = 0x1ff2cb027a949095a289038c3f89c810
eduroam_idp |(10) Framed-MTU = 994
eduroam_idp |(10) Completed request
```

Deploy eduroam: monitoring

F_Ticks(Federated Ticker Systemc -https://monitor.eduroam.org/f_ticks_about.php-)
Tick: Event/Result of authentication with an eduroam SP

Configure and enable f_ticks
-activate the module**/opt/etc/raddb/mods-enabled/f_ticks**
-In the inner-tunnel (eduroam-inner-tunnel) section**post-auth**And subsection**Post-Auth-Type Reject**

```
    post-auth {
cook-inner
reply_log
f_ticks
...
 Post-Auth-Type Reject {
Cui-inner
reply_log
f_ticks
 }
}
```

Deploy eduroam: monitoring

F_Ticks Statistics logging format

F-TICKS/eduroam/1.0#REALM=uv.bf#VISCOUNTRY=BJ#VISINST=1sptic.uac.bj#CSI=47-bf-65-de-da-1f#RESULT=OK#

This shows a user from Université Virtuelle (Burkina-Faso – The REALM-), visiting Bénin (VISCOUNTRY – BJ -) and being granted access by an AP at Université d'Abomey-Calavi (VISINST – uac.bj -)

Deploy eduroam: monitoring

CUI(Chargeable-User-Identity)

Management policy and strategy of the National Federation eduroam

Become an eduroam Federation Operator (NRO)

Administrative Requirements

- the management and supervision of the FLR, eduroam Identity Providers, eduroam Service Providers;
- maintenance of authentication logs;
- a monitoring and diagnostic infrastructure;
- user support;
- compliance with requirements regarding availability times, etc.;
- good understanding of the service definition document as well as the roles and responsibilities of the federation members;
- join eduroam by signing the eduroam policy document;

Management policy and strategy of the National Federation eduroam

Become an eduroam Federation Operator (eduroam flr)

Technical Requirements

- Produce national eduroam statistics (https://www.eduroam.ctld/generate/ro.jsonor ro.xml, institution.json; institution.xml)

- Provide statistical data tohttps://monitor.eduroam.org/fact_eduroam_db.php

Management policy and strategy of the National Federation eduroam

Operate eduroam at campus level (eduroam idp+sp)

Administrative Requirements

- management and supervision of the institution's Identity/eduroam Service Providers;
- maintenance of authentication logs;
- a monitoring and diagnostic infrastructure;
- user support;
- compliance with requirements regarding availability times, etc.;
- good understanding of the service definition document as well as the roles and responsibilities of the federation members;
- join eduroam by signing the eduroam policy document;

Management policy and strategy of the National Federation eduroam

Operating eduroam at campus level (eduroam idp+sp)

Technical Requirements

- Campus WiFi infrastructure with IEEE 802.1x, WPA2/AES auth support;
- Open UDP ports 1812/1813 on firewalls;
- user support;
- If the institution supports EAP-TLS, manage the PKI infrastructure

Management policy and strategy of the National Federation eduroam

Become an eduroam Federation Operator
Managing a Federation Radius Server
Measuring the performance of the federation

References

https://confluence.terena.org/pages/viewpage.action?pageId=121346324

Managing a Federation Radius Server

Measuring the performance of the federation

Thank you!

THANKS!