(edu/gov)roam
let's move together!

Philippe Van Hecke - Senior Services/Network Engineer

Belnet
dedicated connectivity

.be

Agenda

- Welcome and practical informations
- How does eduroam / govroam work? (reminder)
- Security and Trust relations
- Pros/Cons of the actual infrastructure
- How to mitigate Cons?
- Tips and tricks to take care of
- New register interface and dashboard
- CAT and geteduroam (help your users onboarding)
- Onboarding and troubleshooting
- Q&A

Belnet
dedicated connectivity

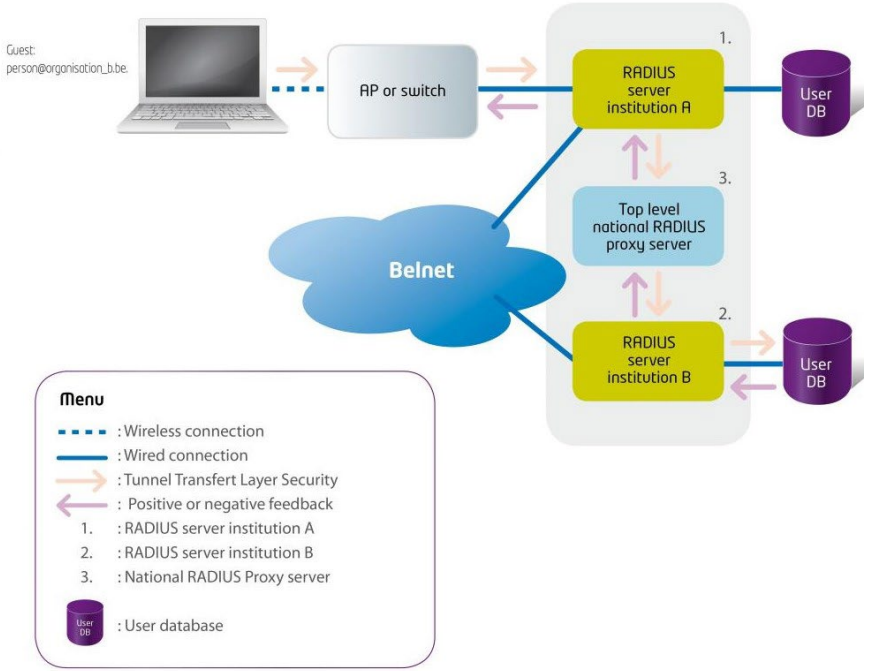
Welcome and practical informations

- The session will be **recorded**
- Please **mute your micro** if you don't need it
- **Who am I?**

Philippe Van Hecke
Senior Network and System Engineer
22 years at Belnet
Working on eduroam / govroam implementation for over 15 years

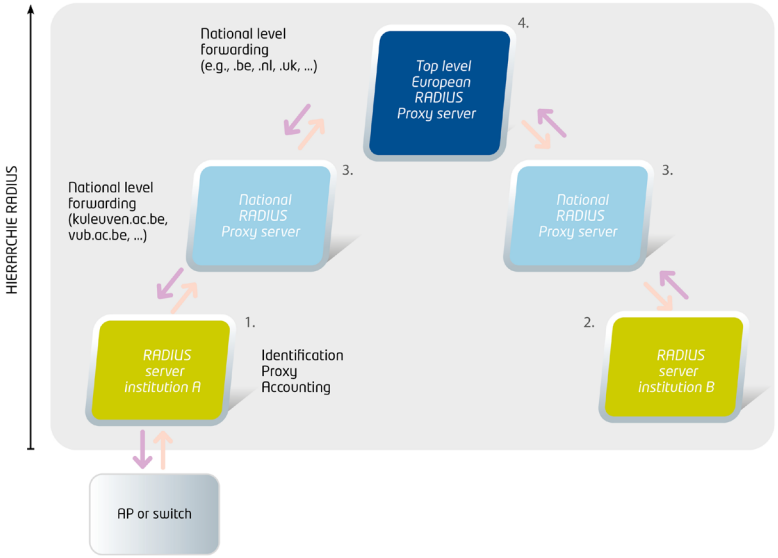
- If you have **questions**, please ask them **in the chat**. We will try to answer all questions at the end of the presentation. If we can not answer all questions during the session, we will send the answers by mail after the session.

How does eduroam / govroam work @ Belgian level?



Belnet
dedicated connectivity

How does eduroam / govroam work @ international level?



Belnet
dedicated connectivity

Security and Trust relations (Trust)

Based on **a common**:

- SSID
- Usage policy
- Hierarchy of trusted partners (Belnet / GÉANT)

Security and Trust relations (Security)

- Based on well known and robust **protocol** for the past decade **(EAP)**

- At any time, only **the end-user device** and **its own radius server** can see credentials

Belnet
dedicated connectivity

Pros and Cons of the actual infrastructure (Pros)

- The infrastructure is based on a well-known and robust protocol, **EAP**
- Implemented by **various radius system providers**
- **Secure**
- **Simplify** visiting user **network access** (and even more with **guestroam**)
- **Worldwide** implemented (eduroam, OpenRoaming)

Belnet
dedicated connectivity

Pros and Cons of the actual infrastructure (Cons)

- EAP protocol is **a connection-less stateful protocol** (load balancing can be complicated)
- Issue with **timeout response** due to the increase in the number of institutions and users
- It is difficult to have **coherent timeout parameters** across all involved radius servers (cumulative effect)
- **Certificate management for TLS tunnels** can be complicated on end-user devices. Even more with the current statement of the CAB forum regarding 90 days certificate validation.
- **UDP fragmentation**

Belnet
dedicated connectivity

How to mitigate Cons?
Timeout - UDP fragmentation (1)

Try to use a radius server that implements RFC-5997

- Status-Server (FreeRadius, Radiator, Aruba, Extreme Network)

Rely on TCP instead of UDP using radius 1.1 (D)TLS

- Radius 1.1 uses TCP/TLS connections between radius servers (rfc-6614 and RFC-7360)
- Trust change to a certificate based trust with certificate delivered by edupki infrastructure or others trusted PKI infrastructure
- Already implemented (radsecproxy, Radiator, freeradius, Cisco ISE, Aruba, Extreme Network)

Belnet
dedicated connectivity

How to mitigate Cons?
Timeout - UDP fragmentation (2)

Using rfc-7585 Radius Dynamic Peer Discovery protocol.

- Supported by Radiator, Radsecroxy (DNS based discovery)

If not supported by your radius, you can configure your DNS to let the Belnet radius server be directly contacted by other radius peer that support it.

- NAPTR 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.belnet.be.
- _radsec._tcp.belnet.be. IN SRV 0 0 2083 roaming1.belnet.be.
- _radsec._tcp.belnet.be. IN SRV 1 0 2083 roaming2.belnet.be.

Belnet
dedicated connectivity

Tips and tricks to take care of (1)

- **Belnet as a proxy doesn’t change any attributes**

  Try to send to the upstream radius; attributes that are only needed for authentication (avoid sending vlan related attributes Tunnel-{Type|Medium|Private Group}

- **Avoid filtering on incoming attributes that are not dedicated to authentication**

  Like Service-Type

Tips and tricks to take care of (2)

- **Assure that your radius server doesn’t send packets bigger than the MTU 1500**
  On most servers this can be done by setting Framed-MTU to a value lower than 1344 (check your radius configuration files).

- **Avoid sending requests for local users to Belnet proxy**
  - This can create a loop
  - We have a loop-free mechanism in place that will reject the request

New register interface and dashboard (register interface)

- Added support for rfc-5997
- Added check of user test and debug report of the check
- Added check for any user
- Hide passwords / and shared secret informations
- Multiple language support
- https://register.eduroam.be
- https://register.govroam.be

Belnet
dedicated connectivity

New register interface and dashboard (dashboard)

- The dashboard is helpful for troubleshooting
  - contains all statistical information regarding Acces-Accept and Access-Reject
  - you can filter by different parameters
  - first thing to look at after your log in case of a problem
  - you can access it from register interface or here: https://dashboard.belnet.be

Belnet
dedicated connectivity

CAT and geteduroam (1)
Help your users onboarding

- **Onboarding user can be challenging**
  - A radius certificate must be accepted by user devices
  - Recent devices refuse to ignore certificate validation
  - with CAB decision to push certificate validation to 90 days
- **CAT eduroam and geteduroam app to the rescue**
  - the duo cat and get eduroam should be seen as lightweight MDM
  - cat permit to eduroam admin to create profiles for different realms and devices
  - geteduroam permits to user to apply such profile to its own devices

Belnet
dedicated connectivity

CAT and geteduroam (2)

Conditions to have access to CAT administration

- You must be a **member of the Belnet federation** and your idp metadata must be published into **the eduGAIN federation**
- Your idp must release one of **the following attributes**
  - eduPersonTargetedID, Subject-id, Pairwise-id
- You must put **contact information** into the register interfaces
  - The e-mail address must be in the requested idp attribute
- When done, we will send you an **invitation to join CAT**

Belnet
dedicated connectivity

CAT and geteduroam (3)

Conditions to have access to CAT administration

- You can find **a guide to CAT** here: https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators

- You can access **the CAT admin interface** here: https://cat.eduroam.org/admin/

Belnet
dedicated connectivity

geteduroam (users app)

- User can get the geteduroam app on well-know **app store**:
  - Apple: https://apps.apple.com/no/app/geteduroam/id1504076137
  - Android: https://play.google.com/store/apps/details?id=app.eduroam.geteduroam
  - Windows: https://dl.eduroam.app/windows/x86_64/geteduroam.exe
  - Linux: coming soon (but user can directly use cat.eduroam.org to get profile)
- **End user usage** can be found here:
  - https://www.geteduroam.app/enduser/connecting/

Belnet
dedicated connectivity

Onboarding eduroam / govroam process (1)

- Contact your **Belnet account manager**
  - give the eduroam/govroam contact
  - send back signed copies of the eduroam/govroam technical policy (see Belnet website)
- **Configure** your Wi-Fi and radius infrastructure
  - the SSID must be eduroam/govroam
- **Connect** to the register interface
  - configure your radius servers, realms, contacts (we will validate all changes when done, with a max of 24 hours' delay)

Belnet
dedicated connectivity

Onboarding eduroam / govroam process (2)

- **Use the Belnet test user** to check that users visiting your institution get access to your local eduroam/govroam network
- On the register interface, give a test user and check that this user gets **Access-accept** from your radius servers (or use the verify link)
- If both tests above work, that means that eduroam/govroam **is well configured**

Troubleshooting / Help

- End users having **problems** must
  - → First contact the ICT department of the visited or/and home institution
- If the problem **is not on the end user's side**
  - → The following tool will help make the first diagnoses
    - register check and verify user
    - Belnet dashboard
    - https://monitor.eduroam.org/mon_direct.php (for eduroam)
- If the problem **involves a top level proxy** (Belnet, World level institution)
  - → Open a case with the Belnet service desk

Belnet
dedicated connectivity

Q&A


Thank you
for your attention
Belnet
dedicated connectivity