

Wireless Authentication

Network Startup Resource Center
www.nsrc.org

Edit: 201610 RENU Uganda



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license
(<http://creativecommons.org/licenses/by-nc/4.0/>)

What is Authentication?

Definition:

- Authentication is the process of verifying the claim that an entity is allowed to act on behalf of a given known identity
- This sounds very complicated!
- More simply:
 - Is this person says who they say they claim to be ?
 - Can they prove it (for example, with password, signature)?
 - In our case, the entity is the software, acting on behalf of the user controlling the computer.

Why do we make it so complicated?

It is important to be aware of the differences:

- Just because I am on a certain computer, I am not necessarily its owner - the device is not the same as the person.
- Just because I am a certain person, I might not be in the right role to have access to a resource.

For example:

`user@private.place.net`

is not the same as

`user@at.work.com`

Some core concepts, 1

It is important to distinguish between the following concepts:

- confidentiality
- access control
- authentication
- authorization

Some core concepts, 2

- Confidentiality
 - Ensure that only those who should have access to information can indeed do so (usually through encryption, access control)
- Authorization & access control
 - Authorization defines what an entity (here: a user, a device) is authorized (allowed) to access or do
 - Which networks (ACLs/filters)?
 - Which systems, which files, apps, services ? (FS ACLs, permissions) (a remark just for this workshop: we have not really talked about linux permissions!)
 - When can they do that (time policies) ?

Authentication:

What we are trying to solve?

- We want to know

WHO, WHERE(*), WHEN, HOW

- NOT the same as using password based encryption (WPA2-PSK)! Keys can be **shared** between users
- We want to know:
 - Which user?
 - *What area of the wireless network (AP) did they associate with?
 - When did they log on?
 - What IP number did they have?

Solutions

- There are two recommended ways to do this:
 - Captive portal
 - **802.1X (EAPoL and EAP-TLS) – preferred solution**
- Your choice depends on
 - The size of your organization
 - The maturity of your IT systems
 - You will need user stores, databases (e.g. AD/LDAP)
 - Your human resources
 - system admin, helpdesk, support
 - And many other factors

Captive Portal, 1

- Plus
 - Popular (public areas, airports, hotels, ...)
 - Flexible
 - Self-explanatory (web page), can enforce AUP (Acceptable Use Policy) validation
 - Relatively easy to implement
- Minus
 - Depends on browser
 - Not standardized (different looks, different credentials, ...)
 - Requires regular re-authentication (disruptive)
 - Often unreliable and easy to break

Captive Portal, 2

To "redirect" you to a welcome page, any one of the following methods may be used:

- HTTP silent redirection
- HTTP 30x redirect
- IP hijacking
- DNS hijacking
- Certain URLs may be allowed
 - e.g Information page, help page, use policies

Captive Portal, 3

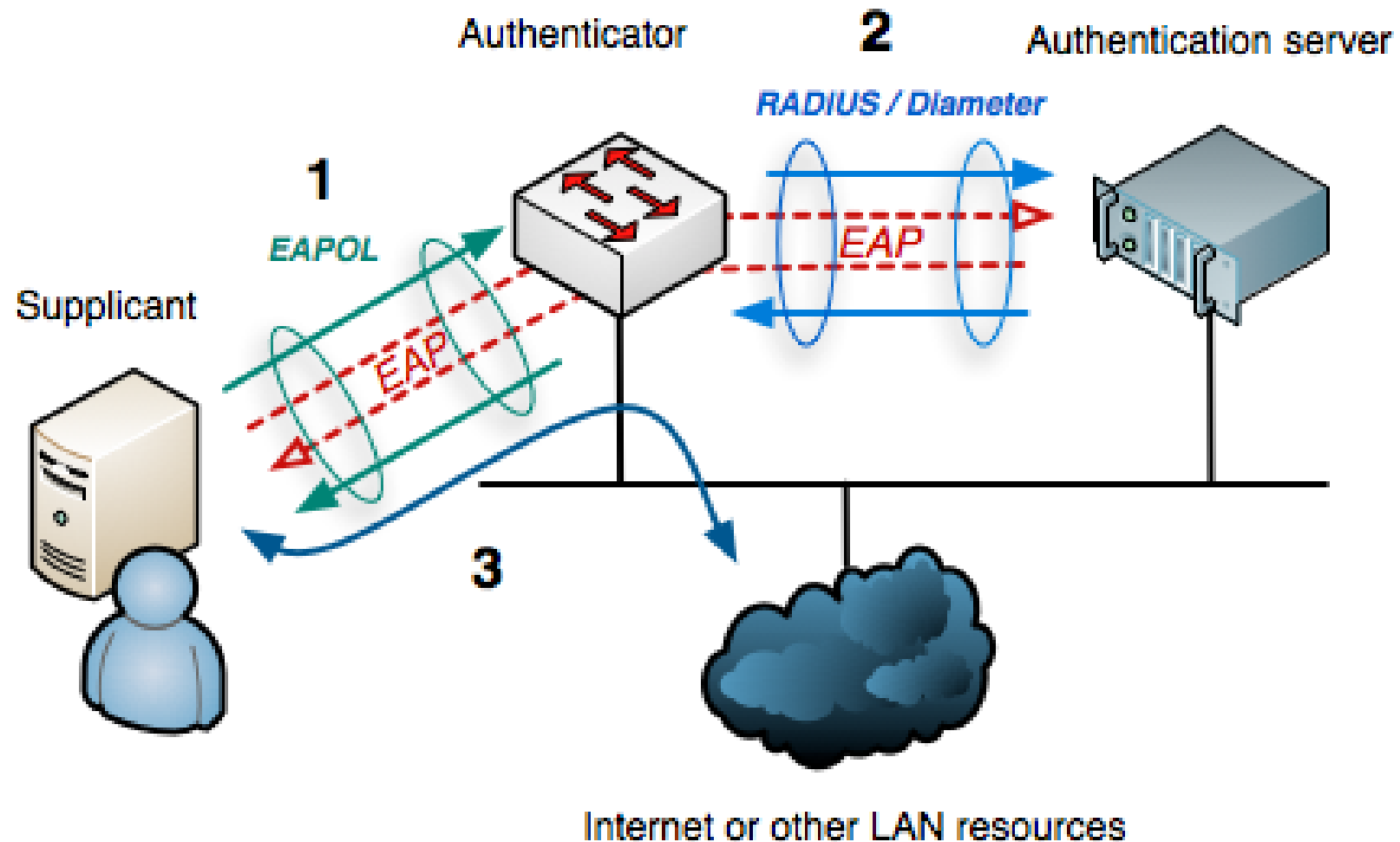
- Many vendors and open source projects
 - CoovaChilli, CoovaAP
 - WiFidog
 - M0n0wall, pfSense
 - zeroshell
- Many general networking vendors offer some form of integrated captive portals, e.g.
 - Mikrotik, HP, Cisco, Aruba, Atilo, Ubiquiti

802.1x/EAP

- Often called WPA2 Enterprise
- Originally designed for wired networks (EAPoL), but design accommodated for wireless networks
- RFC 5216 (2004), RFC 5247 (2008)
- Layer 2 protocol (but depends on SSL/TLS certificates!)
 - 4 states:
 1. initialization (all traffic blocked – no DHCP or anything)
 2. initiation (authenticator sends EAP-Requests, and client responds with EAP-Response-Identity)
 3. negotiation of a method of authentication
 4. authentication if negotiation succeeds

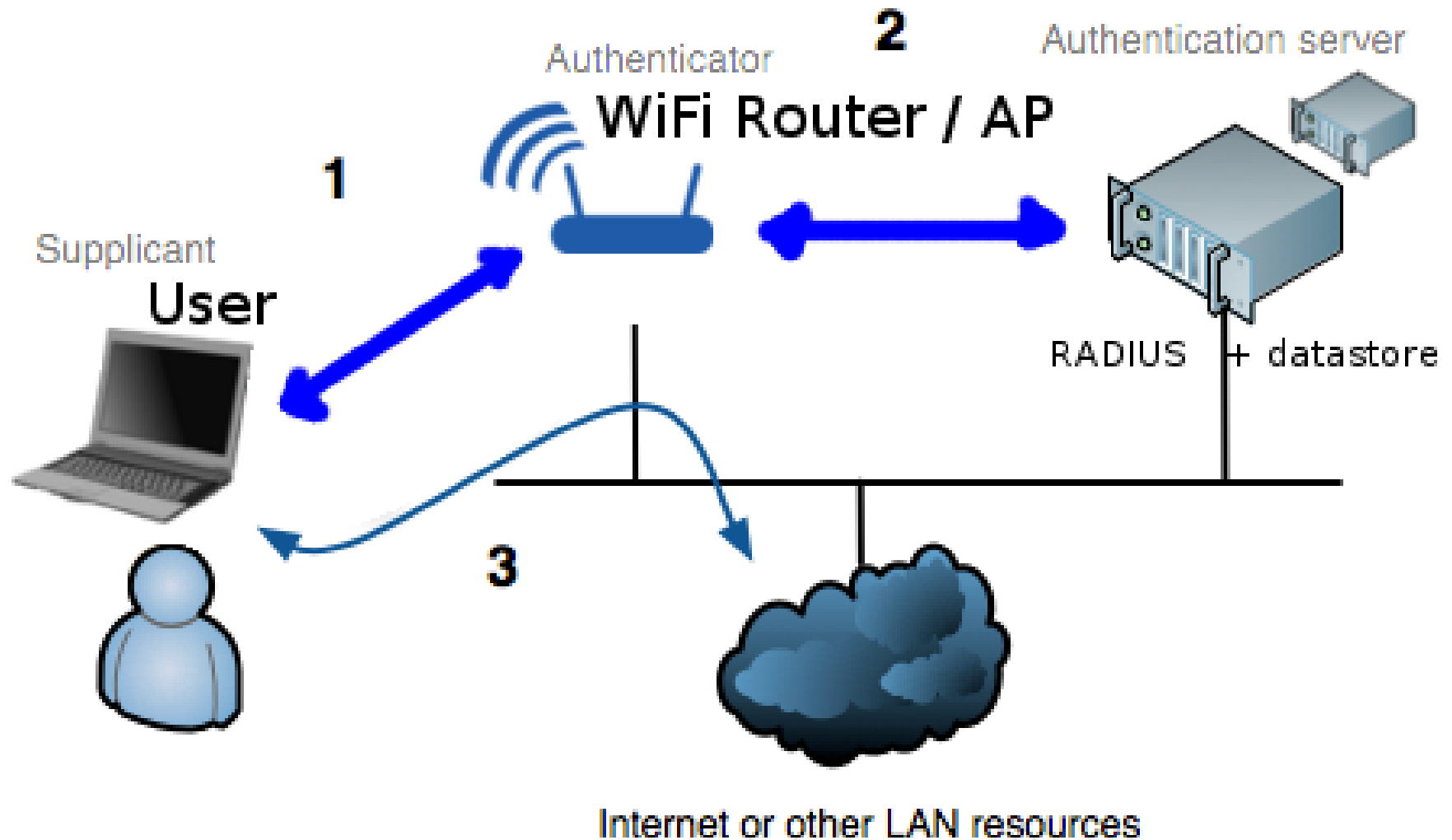
Traffic is allowed through

802.1x/EAP – How does it work



Source: Wikipedia

802.1x/EAP – How does it work

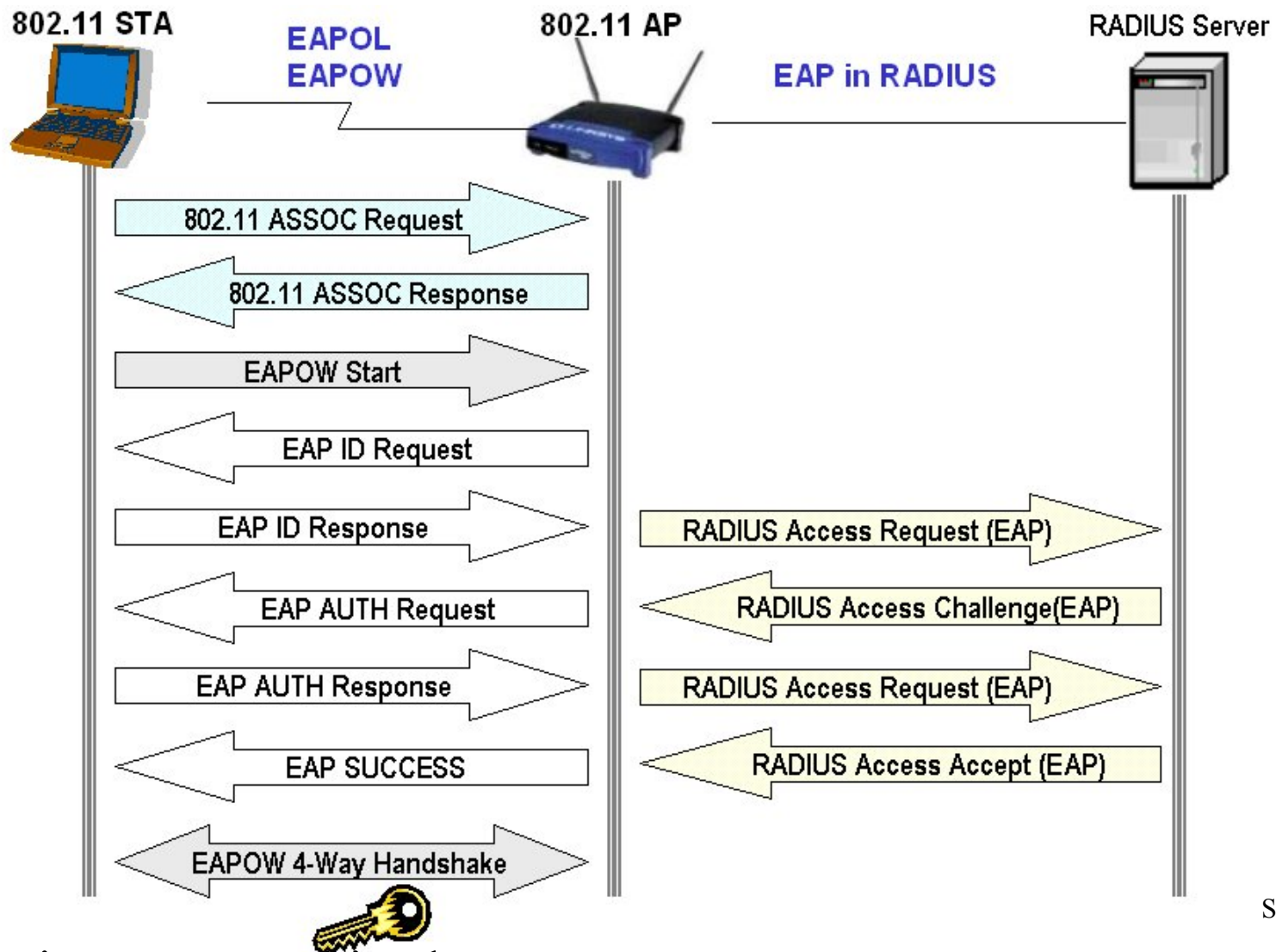


Source: Wikipedia, modded

In plain words

- The **client** (laptop, phone, ..) asks the **access point** (AP) for access
- The **AP** is set to contact a **RADIUS server** and pass on the user's credentials
- The **RADIUS server** looks up in the **datastore** (where the user information is kept) - which might be a SQL DB, an AD/ldap, or just a text file – and finds the user and its info.
- RADIUS server answers to AP
- AP answers to client

802.1x/EAP – detailed



Source: WiFi-Planet

On Linux: to see this, do

```
$ grep wpa /var/log/syslog
```

EAP dialogue

Trying to authenticate with 44:d9:e7:8d:11:e0 (SSID='NSRC_auth_secure' freq=2462 MHz)

Trying to associate with 44:d9:e7:8d:11:e0 (SSID='NSRC_auth_secure' freq=2462 MHz)

Associated with 44:d9:e7:8d:11:e0

CTRL-EVENT-EAP-STARTED EAP authentication started

CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25 -> NAK

CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21

CTRL-EVENT-EAP-METHOD EAP vendor 0 method 21 (TTLS) selected

CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/C=FR/ST=Radius/L=Somewhere/O=Example Inc./emailAddress=admin@example.org/CN=Example Certificate Authority'

CTRL-EVENT-EAP-PEER-CERT depth=1 subject='/C=FR/ST=Radius/L=Somewhere/O=Example Inc./emailAddress=admin@example.org/CN=Example Certificate Authority'

CTRL-EVENT-EAP-PEER-CERT depth=0 subject='/C=FR/ST=Radius/O=Example Inc./CN=Example Server Certificate/emailAddress=admin@example.org'

EAP-TTLS: Phase 2 MSCHAPV2 authentication succeeded

CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully

WPA: Key negotiation completed with 44:d9:e7:8d:11:e0 [PTK=CCMP GTK=CCMP]

CTRL-EVENT-CONNECTED - Connection to 44:d9:e7:8d:11:e0 completed (reauth) [id=0 id_str=]

802.1x/EAP

- Plus
 - transparent for Applications
 - "inline", layer 2 - doesn't require interaction with upper layers like DHCP, IP, HTTP to function (exc for certificates!)
 - standardized for both wired (!) and wireless LANs
 - Integrates with **eduroam** !!!
- Minus
 - More challenging in deployment
 - requires an external authentication server (Radius)
 - New to users (?)

802.1x & EAP vs captive portals, 1

- Captive portals may be preferable for networks, or parts of the network, where there are many non-regular guest users which you don't want in your AD or other datastore
- Captive portals can guide users, provide helpdesk contact information –
- 802.1x is more streamlined – and standardized – making it preferable for known users
- A combination of both may be useful:
 - 802.1x everywhere possible, on LAN/WLAN (dedicated SSID)
 - "Guest"-style captive portal for the rest

802.1x & EAP vs captive portals, 2

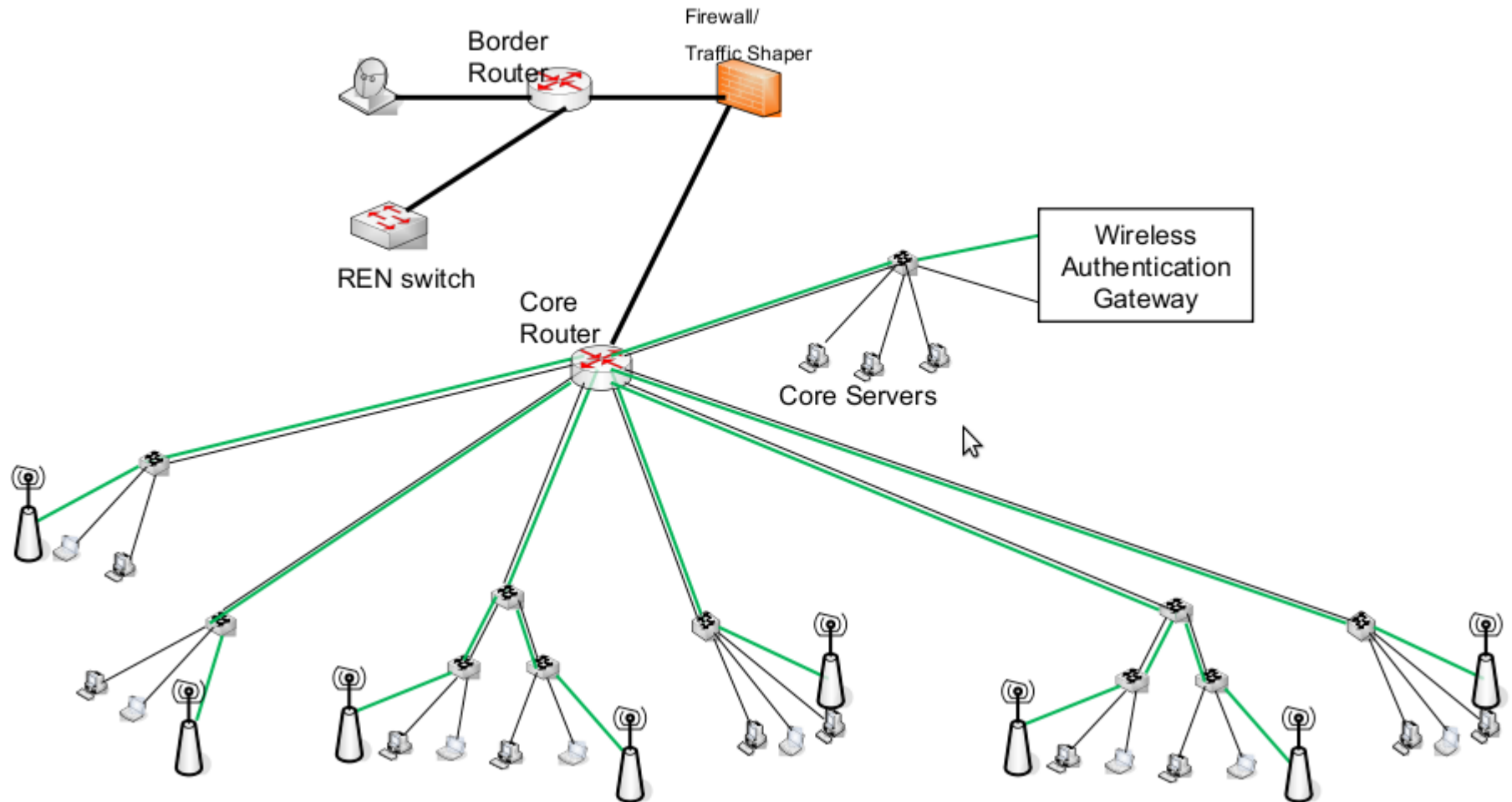
- 802.1x is layer 2,
Captive Portals use layers 3 - 7
- Both need authentication backends:
 - SQL or LDAP/Active Directory
 - Can be local flat text file (only advisable for small organizations, or as start/test)
 - Backends can be shared between technologies (captive portal + 802.1x)
- AAA server **Radius** - can work with any of the above solutions

Question

- Where in the network would you put ...
 - Your RADIUS server
 - Your user datastore (AD, ldap or such)

?

Central authentication backend on core network



Security issues of 802.1x

802.1x or WPA2/EAP is the recommended authentication option, but it has a security problem too:

- Its outer tunnel security relies on TTLS/SSL certificates
- These are **vulnerable to man-in-the-middle attacks** – if the client device does not **properly check the certificate**, then it will give its credentials to ANY AP, e.g. rogue APs
- Its inner tunnel encryption is MSCHAP2, which is known to be broken/crackable

Source and scope of the security problem

The problem is essentially a SSL/TTLS implementation problem

- Clients often do not even check CN (server name that the certificate belongs to), or they trust ANY certificate from a given root (CA) (android phones are major problem!)
- Nothing can protect us against client devices with bad certificate check implementations.
- Another part of the problem is the inner tunnel: MSCHAP2 is crackable.

Addressing security issues of 802.1x

- It is essentially a question of SSL certificate trust
- We can **enforce the best possible client configuration**, for example by using the **eduroam CAT tool**, see <https://cat.eduroam.org>
- Helpdesk, information, policies!
- See also security recommendations on GEANT wiki:
<https://wiki.geant.org/> e.g.
<https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations>

Addressing security issues of 802.1x

- If you take this very seriously (and follow eduroam best practice), you will
 - want to create your own SSL root CA, which only serves your 802.1x certificate
 - separate network credentials from any other access (so that a stolen network password does not open for other services)
- Discuss the risk management aspects!

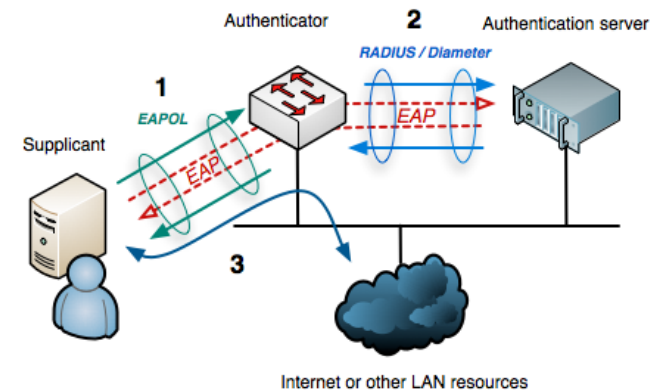
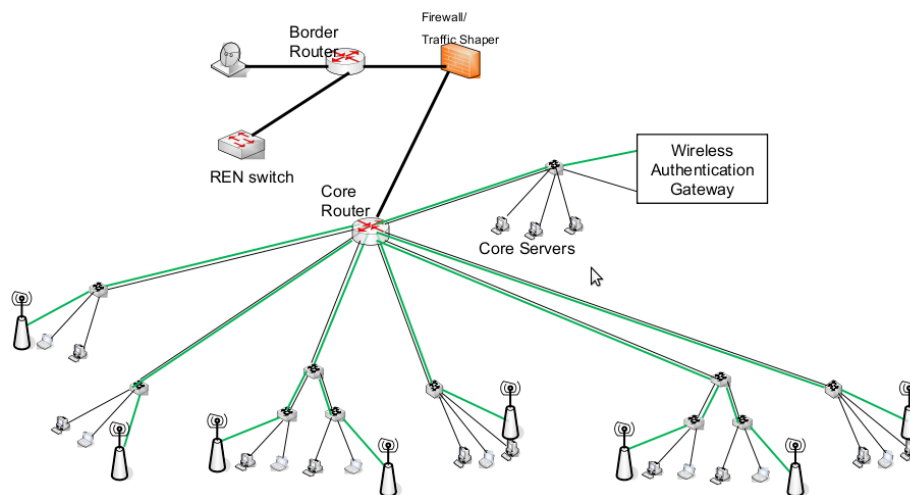
Demonstration of man-in-the-middle attacks on 802.1x

- Get user to associate to rogue AP and start handshake,
- Authentication process
- Packet dump everything
- Analyze the traffic, isolate the handshake
- The outer tunnel is easy – as the attacker owns certificate and keys
- The inner tunnel (typically MSCHAP2) can be cracked (via offline or online services)



NSRC recommendation for authentication

- User store in LDAP/AD, e.g. OpenLDAP
- RADIUS, e.g. freeradius
- Despite the security problems, **802.1x remains the best option** – with Captive Portal as a second option



How to deploy 802.1x, simplified

- You check if your organisation and infrastructure is ready!
- You have or build a user datastore (e.g. AD/ldap, SQL). For very small institutions, even a text file can do the job.
- You build a RADIUS server <https://freeradius.org>
 - best with eduroam configuration from the start
 - Eduroam guide is also great help for general RADIUS setup
- You configure your wireless APs to do 802.1x (WPA2 enterprise).
 - Of course your hardware needs to support this – all modern APs do
 - You inform and educate your users (!)

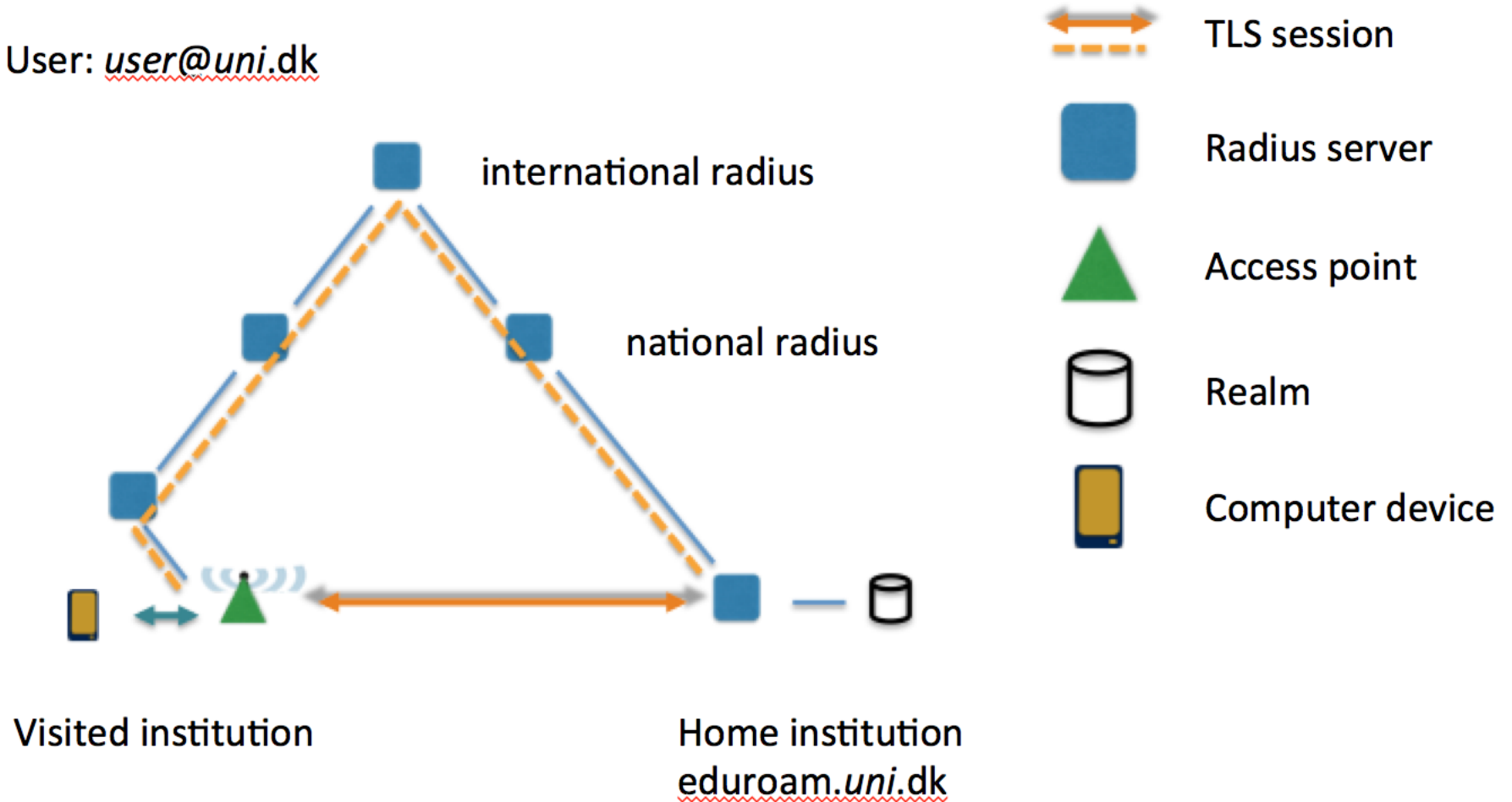
eduroam

- A recommended addition to your campus networks authentication is **eduroam**,

an international roaming service
for users in research,
higher education
and further education.

How eduroam works

User: user@uni.dk



eduroam

- Allows you to join network in any member place around the world, with your home credentials
- It can actually be the only network/SSID you offer at your place. Your datastore knows the local users and can give them access to local services (which your guests should not have, of course)
- **Put eduroam Uganda on the world map!**

eduroam



eduroam

- Learn more at:



EDUCation ROAMing

Purpose	International authentication infrastructure
Region served	Worldwide
Parent organization	TERENA
Website	www.eduroam.org 