freeRADIUS

Freeradius @ Uii

EDUROAM WORKSHOP 2017

FREERADIUS @ UII - EDUROAM WORKSHOP 2017

Whoami

WHOAMI

ARRAN CUDBARD-BELL

- Arran Cudbard-Bell (@arr2036)
- Principal architect for the FreeRADIUS project
- Mercenary at Network RADIUS
- Director RM-RF LTD
- IETF Note Taker (RADEXT - Soon to be defunct, boo)
- Janet 802.1X SIG member

…OK, BUT DAY TO DAY

- I write lots of code. Mainly C. Now mainly async C.
  - Core architecture
  - API design/rework
  - Lots of modules, eap methods, drivers
- I design highly scalable fault tolerant AAA solutions for Universities, Enterprises, Telcos and Medium/Large ISPS.
- Community/social outreach for the FreeRADIUS project.

freeRADIUS

FREERADIUS @ UII - EDUROAM WORKSHOP 2017

Whatis Eduroam

THE INTERNATIONAL CONFEDERATION

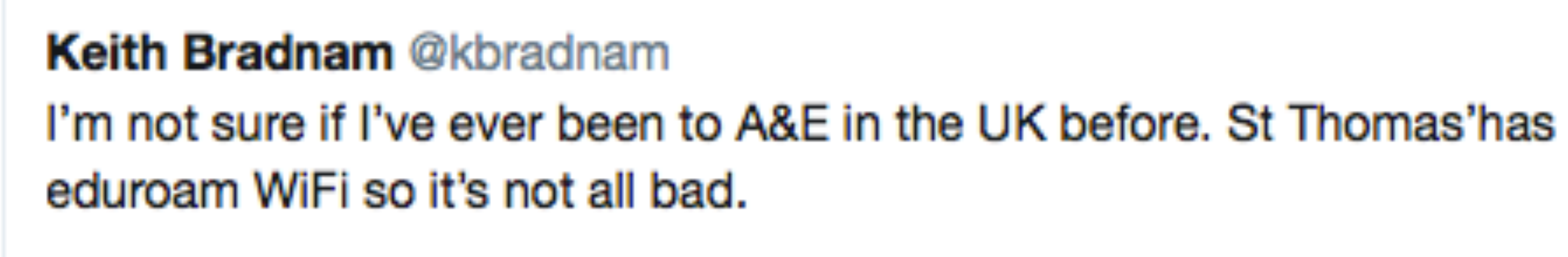
- Eduroam is an international confederation of Universities and other entities wanting to:
  - Remove barriers to/foster inter-institutional collaboration.
  - Ease technological burdens on their students and staff.
  - Provide resources for others in the academic community.
- Eduroam is made up of thousands of members, across 85 different countries.
- ...with just four organisations operating TLRS (Top level RADIUS servers)

THE HISTORY

- Started in 2003 as a pilot under TERENA TF-Mobility.
- Since Sept 2004: ops&dev of European eduroam funded by GEANT.
- 2006 - APAN eduroam Project Group commenced.
- 2007 European eduroam confederation policy agreed, & Operation Team (OT) formed.
- 2008 - EMEA Production service commenced.
- 2008 - Eduroam AU (incl. NZ) Pilot Service commenced.
- 2011 - APAN Eduroam production service commenced.
- 2016 - ITB becomes the Idnonesian NRO.

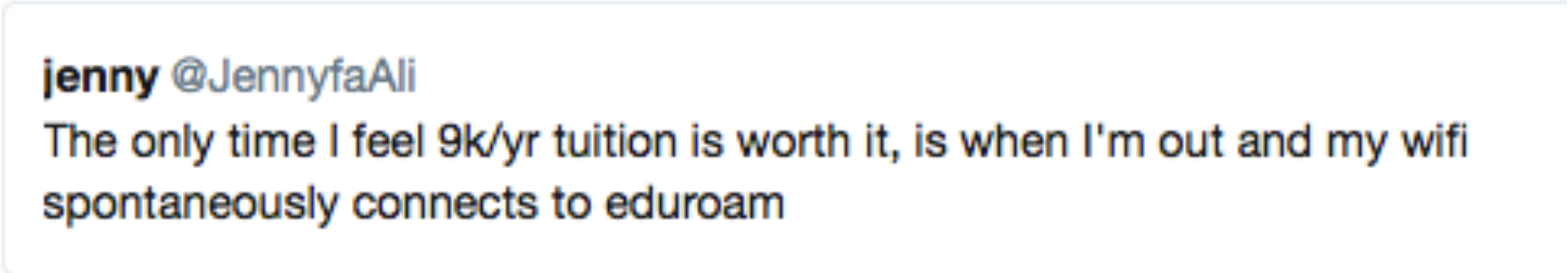
BENEFITS

- Students feel more welcome at other institutions (home is where the WiFi connects automatically).
- Convenience - It’s not just for University campuses.
- Removes barriers to collaboration. Show up, get online, no help desk required.
- Significantly increased security over WPA2-PSK (Pre-shared key).
- Bootstraps transition to policy driven networking.



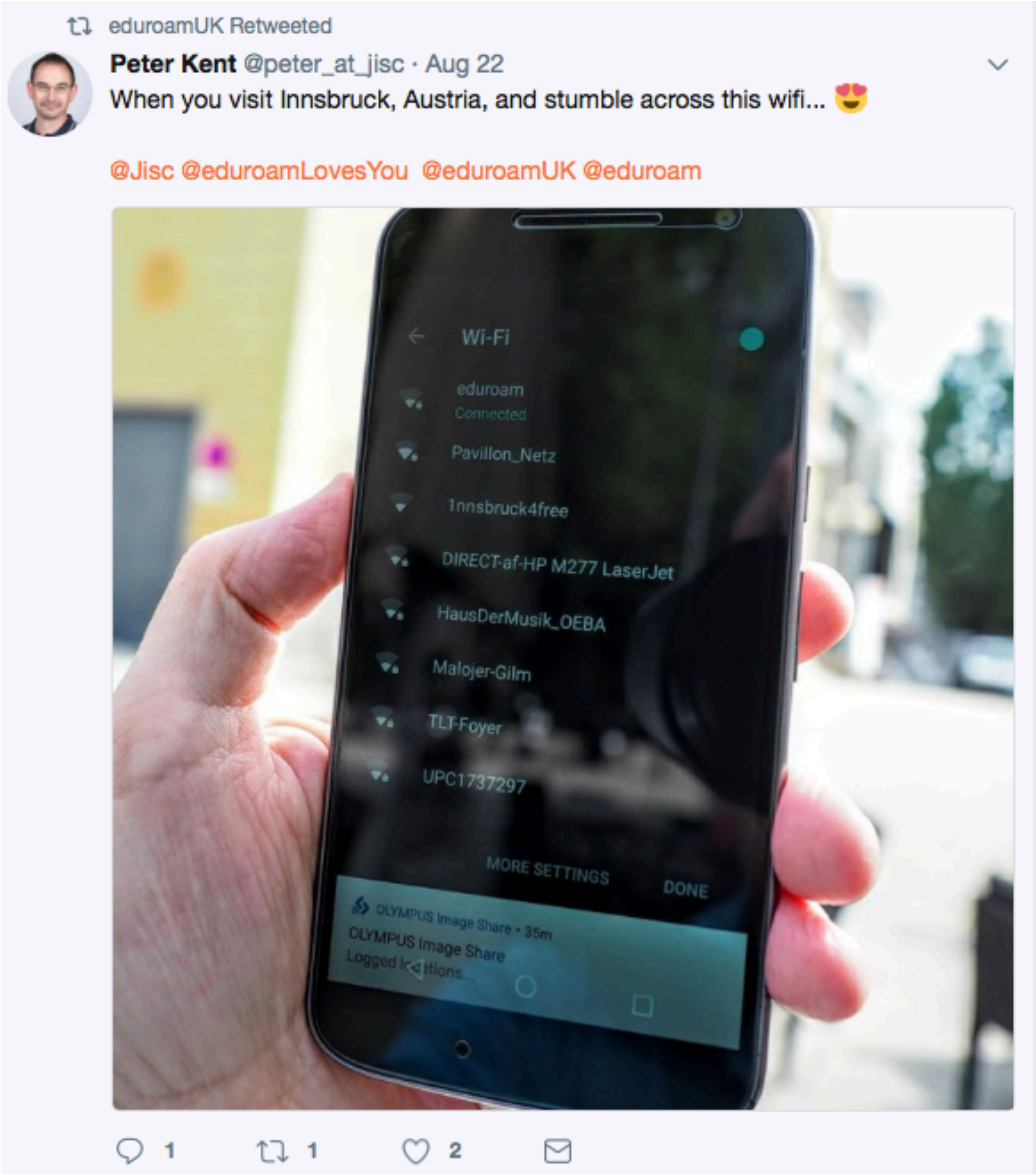
Keith Bradnam @kbradnam

I'm not sure if I've ever been to A&E in the UK before. St Thomas'has eduroam WiFi so it's not all bad.



jenny @JennyfaAli

The only time I feel 9k/yr tuition is worth it, is when I'm out and my wifi spontaneously connects to eduroam



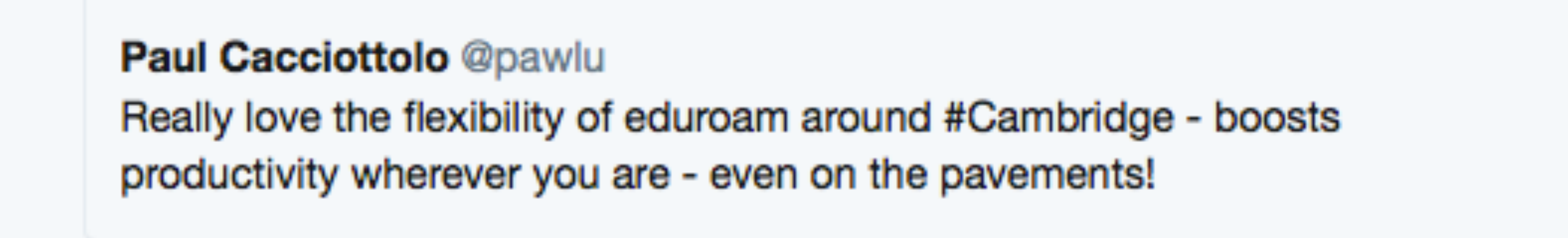
eduroamUK Retweeted

Peter Kent @peter_at_jisc · Aug 22

When you visit Innsbruck, Austria, and stumble across this wifi... 😍

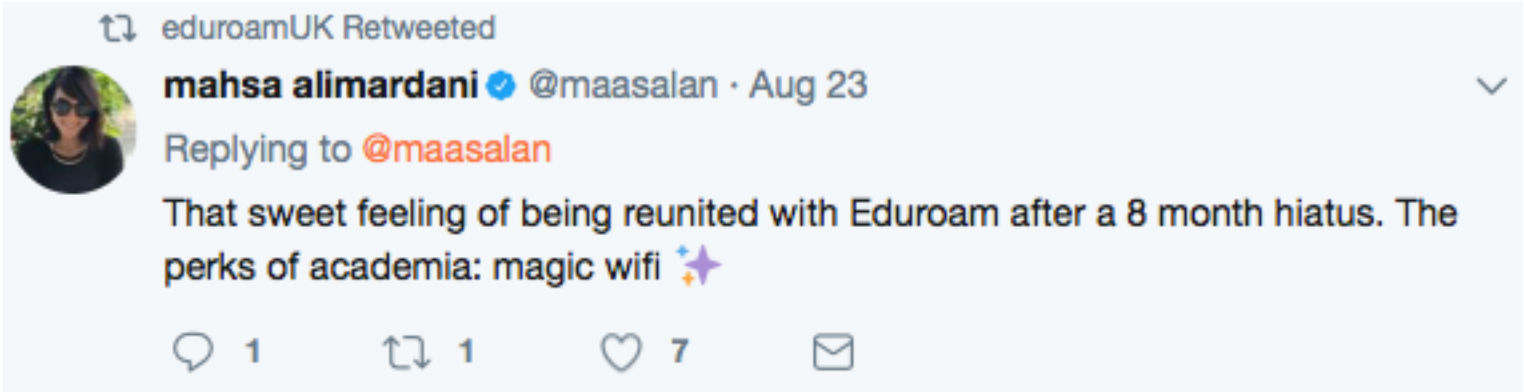
@Jisc @eduroamLovesYou @eduroamUK @eduroam

💬 1 🔁 1 ♡ 2 ✉



Paul Cacciottolo @pawlu

Really love the flexibility of eduroam around #Cambridge - boosts productivity wherever you are - even on the pavements!



eduroamUK Retweeted

mahsa alimardani @maasalan · Aug 23

Replying to @maasalan

That sweet feeling of being reunited with Eduroam after a 8 month hiatus. The perks of academia: magic wifi ✨

💬 1 🔁 1 ♡ 7 ✉

THE SSID

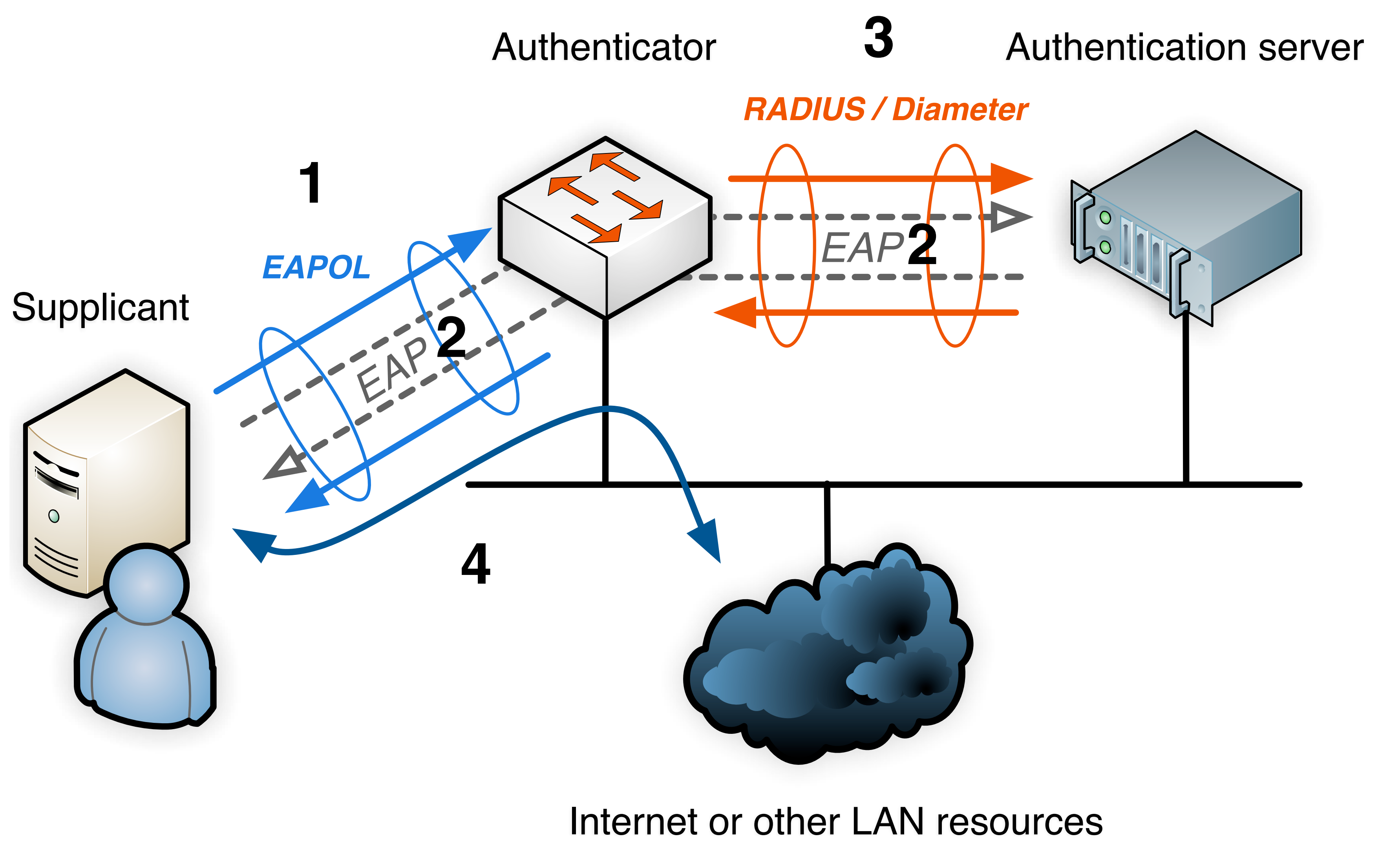
- Primary exposure of Students/Staff is via the “eduroam” SSID.
- The same SSID is broadcast by every (SP) institution.
- 802.11i parameters for the SSID are identical (on purpose) - all use:
    - WPA2-Enterprise
    - AES (CCMP)
    - WPA1/TKIP expressly forbidden.
- Once a device “remembers” the eduroam network, it’ll automatically connect anywhere (which is half the magic).
- The other half is routing the credentials provided for WPA2-Enterprise (username/password or X509 cert), back to the user’s home institution for validation.

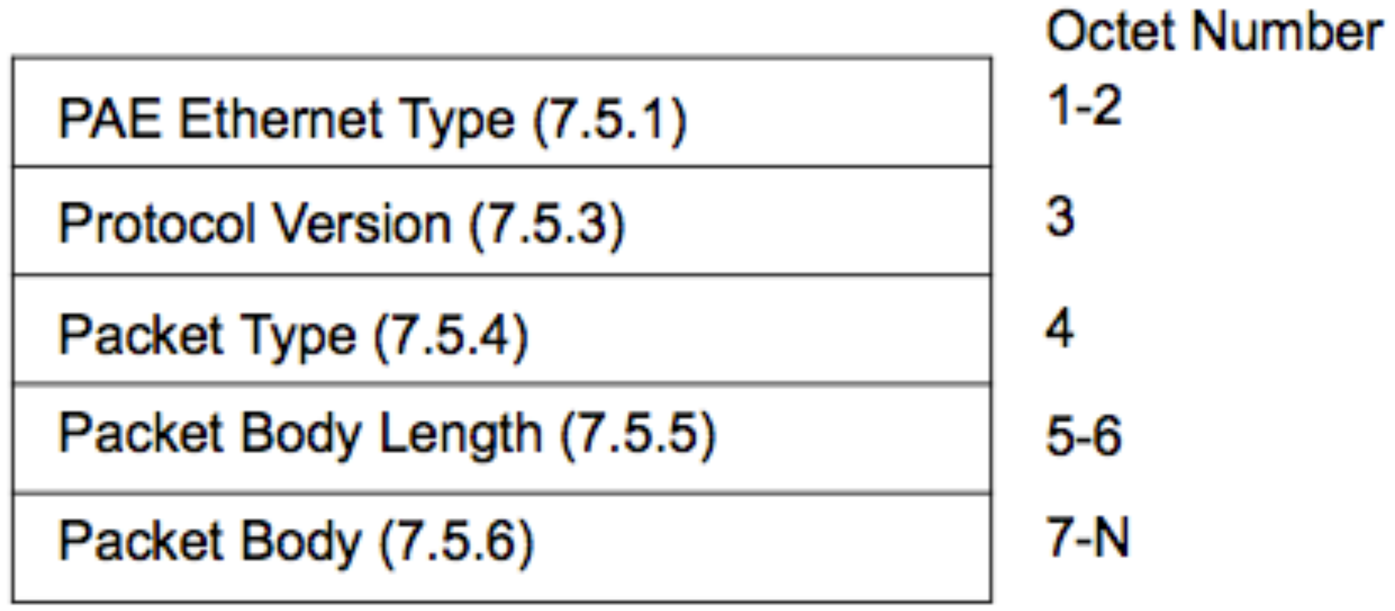
THE TECHNOLOGY

- Three key protocols:
  - IEEE 802.1X-2001/2004
  - EAP (Extensible Authentication Protocol) - IETF RFC 3748
  - RADIUS (Remote Authentication Dial In User Service) - IETF RFC 2865, 2866 and many others...

1 - IEEE 802.1X

- The gatekeeper protocol. Installs a PAE (Port Access Entity). To protect ports and SSIDs. Analogous to passport control.
- Mainly runs on switches an access points.
- Initially blocks **ALL** traffic on a port or 802.11 association, other than certain control frames and EAPOL (a very simple L2 encapsulation protocol).
- Interrogates any new connecting device with an EAP-Identity-Request.
- Device may respond with an identity response - i.e. anonymous@uii.ac.id.
- If it does, authentication begins. If it doesn't it stays blocked (usually).



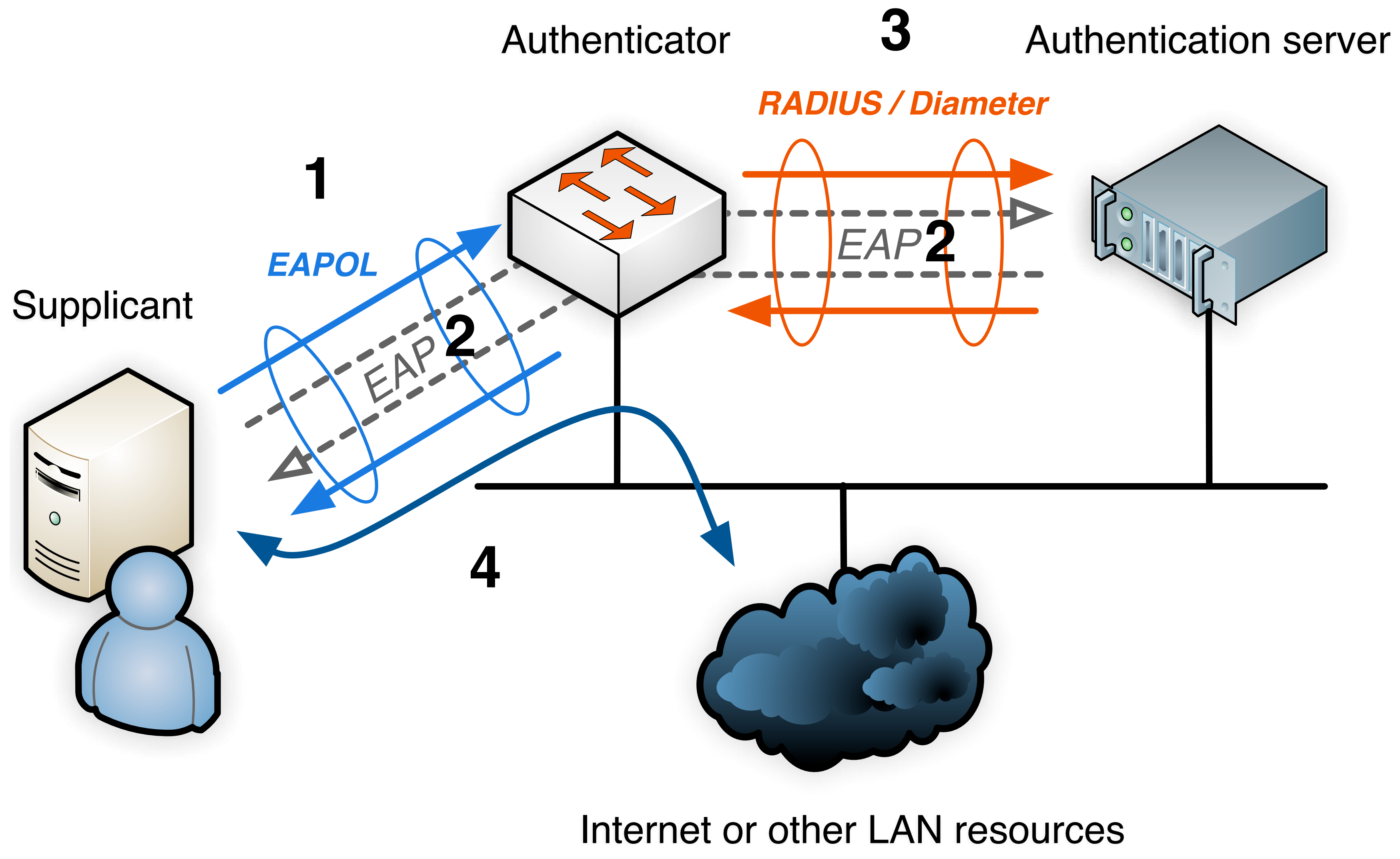


	Octet Number
PAE Ethernet Type (7.5.1)	1-2
Protocol Version (7.5.3)	3
Packet Type (7.5.4)	4
Packet Body Length (7.5.5)	5-6
Packet Body (7.5.6)	7-N

Figure 7-1—EAPOL frame format for 802.3/Ethernet

2 - EAP

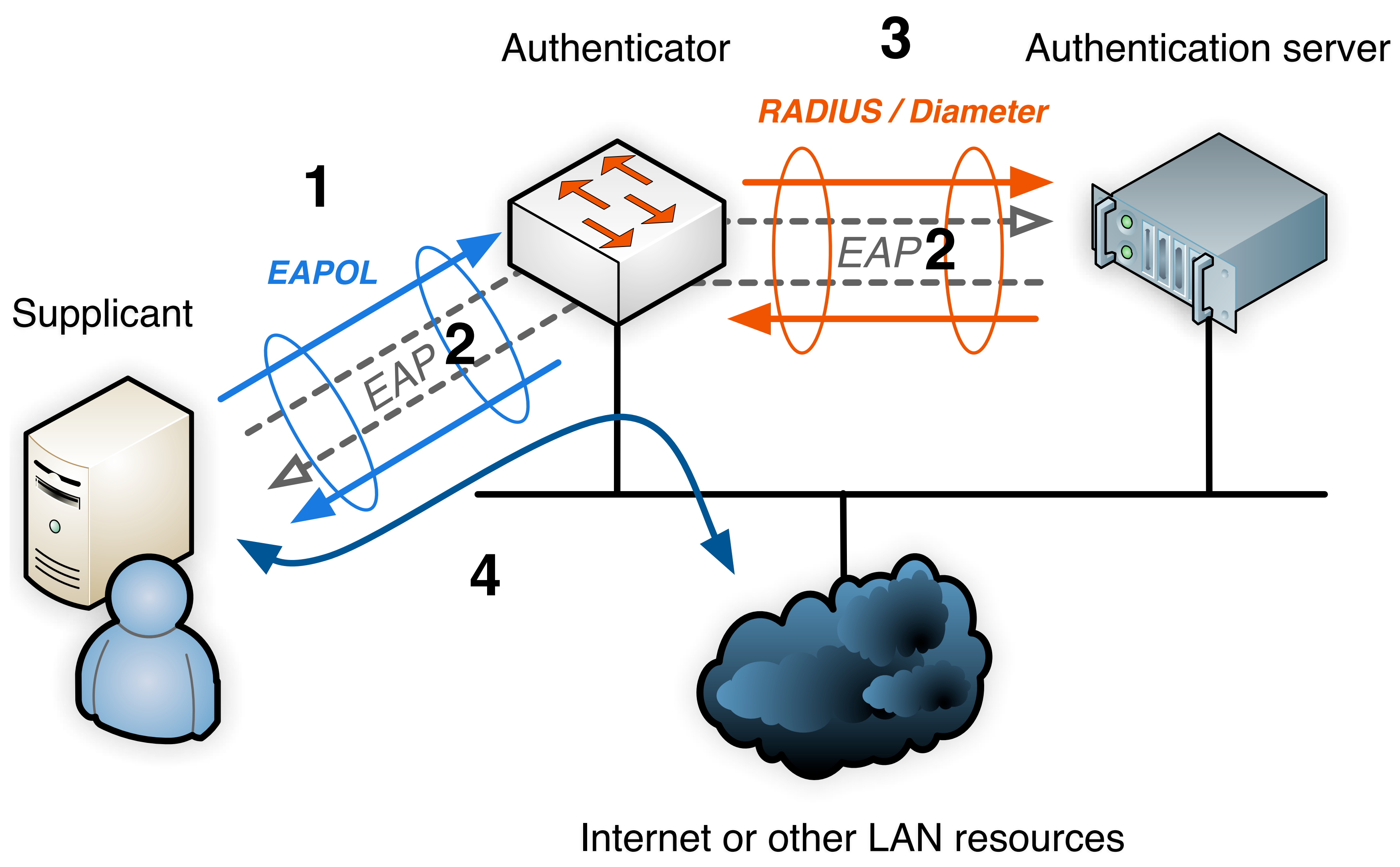
- The primary transport protocol.
- Tunnelled between the supplicant (software running on the users device) and the authentication server.
- Transports user’s identity and credentials, and sometimes posture information.
- EAP methods can be trivially simple (EAP-MD5), or very complex PEAPv0-MSCHAPv2-SoH.
- Common EAP methods on Eduroam are:
  - EAP-TTLS
  - PEAPv0
  - EAP-TLS



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Type-Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

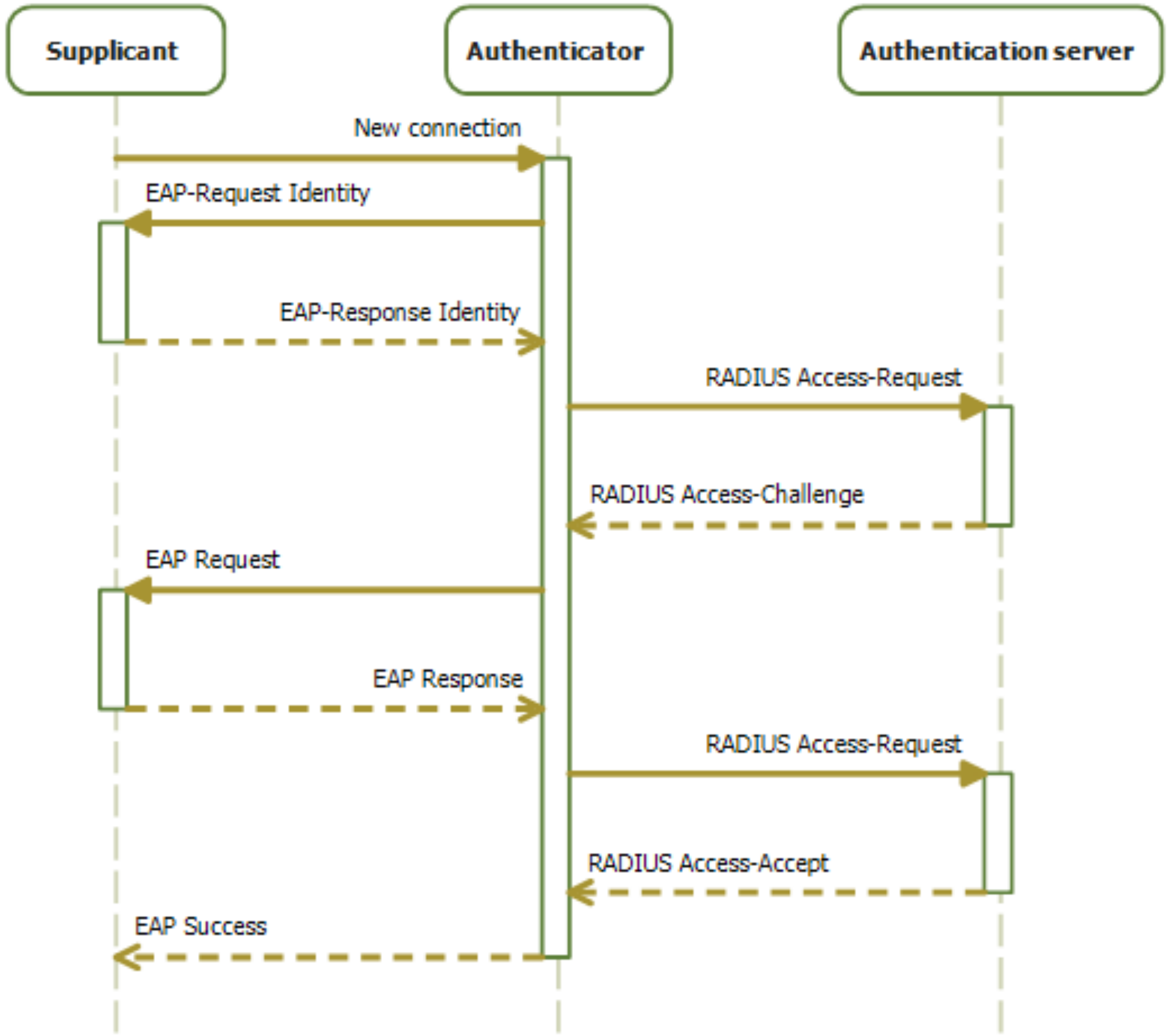
3 - RADIUS

- RADIUS transports EAP data from the Authenticator (PAE) to the Authentication server.
- Each packet contains multiple AVP (Attribute Value Pair) tuples.
- Carries EAP data to support authentication/authorization.
- Is routable (proxyable). User-Name AVP used for Eduroam routing.
- Provides authorizational data to the Authenticator.
  - Yes/No (allow or deny access).
  - VLAN assignment.
  - Firewall rules.
  - Session timeout (when the device needs to reauth).
- Distributes keys (PMKs) to the authenticator.



```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                     Request Authenticator                     |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Attributes ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

BASIC PROGRESSION



Supplicant

Authenticator

Authentication server

New connection

EAP-Request Identity

EAP-Response Identity

RADIUS Access-Request

RADIUS Access-Challenge

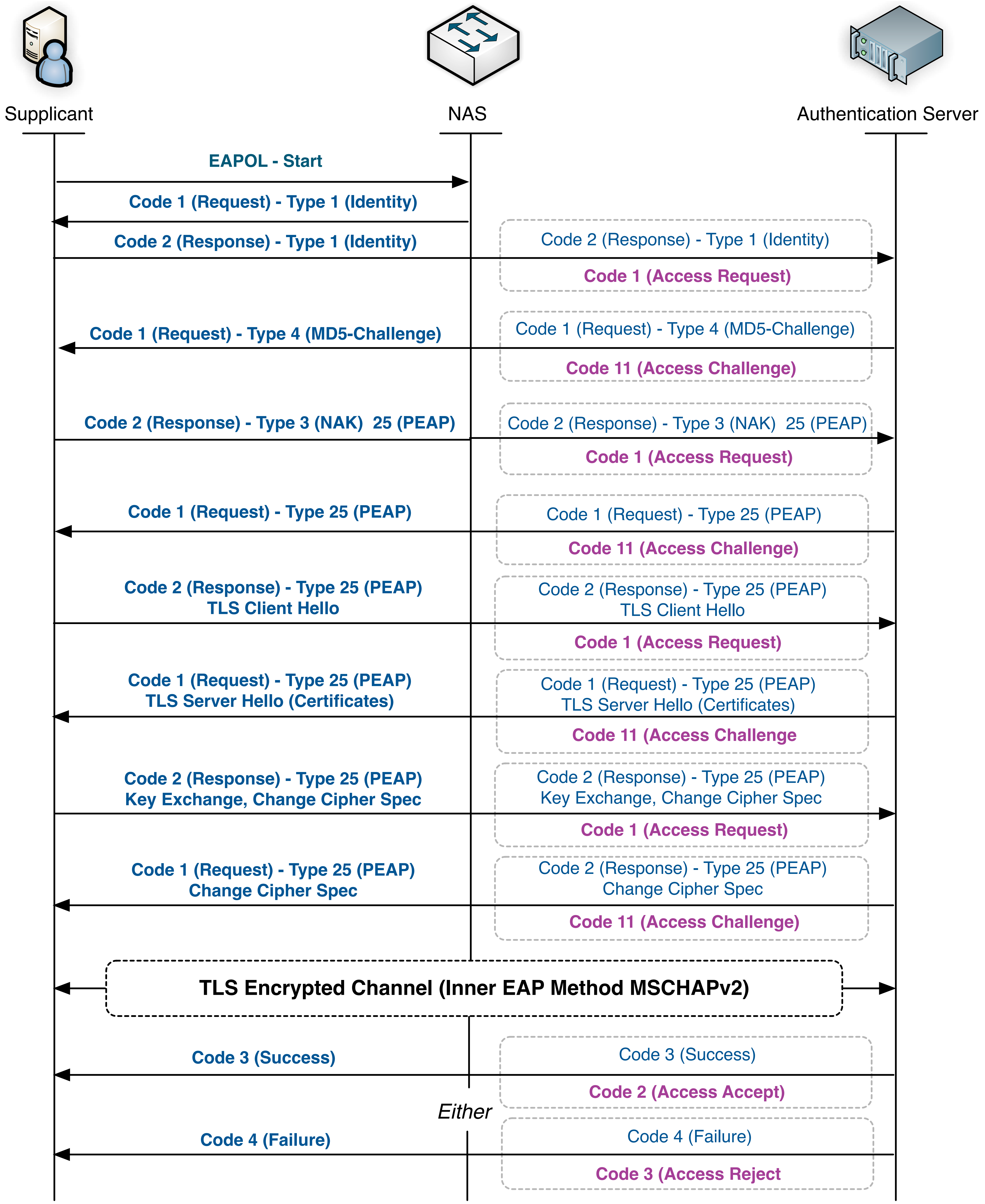
EAP Request

EAP Response

RADIUS Access-Request

RADIUS Access-Accept

EAP Success



Supplicant

NAS

Authentication Server

EAPOL - Start

Code 1 (Request) - Type 1 (Identity)

Code 2 (Response) - Type 1 (Identity)

Code 2 (Response) - Type 1 (Identity)

Code 1 (Access Request)

Code 1 (Request) - Type 4 (MD5-Challenge)

Code 1 (Request) - Type 4 (MD5-Challenge)

Code 11 (Access Challenge)

Code 2 (Response) - Type 3 (NAK) 25 (PEAP)

Code 2 (Response) - Type 3 (NAK) 25 (PEAP)

Code 1 (Access Request)

Code 1 (Request) - Type 25 (PEAP)

Code 1 (Request) - Type 25 (PEAP)

Code 11 (Access Challenge)

Code 2 (Response) - Type 25 (PEAP)
TLS Client Hello

Code 2 (Response) - Type 25 (PEAP)
TLS Client Hello

Code 1 (Access Request)

Code 1 (Request) - Type 25 (PEAP)
TLS Server Hello (Certificates)

Code 1 (Request) - Type 25 (PEAP)
TLS Server Hello (Certificates)

Code 11 (Access Challenge

Code 2 (Response) - Type 25 (PEAP)
Key Exchange, Change Cipher Spec

Code 2 (Response) - Type 25 (PEAP)
Key Exchange, Change Cipher Spec

Code 1 (Access Request)

Code 1 (Request) - Type 25 (PEAP)
Change Cipher Spec

Code 2 (Response) - Type 25 (PEAP)
Change Cipher Spec

Code 11 (Access Challenge)

TLS Encrypted Channel (Inner EAP Method MSCHAPv2)

Code 3 (Success)

Code 3 (Success)

Code 2 (Access Accept)

Either

Code 4 (Failure)

Code 4 (Failure)

Code 3 (Access Reject

FREERADIUS @ UII - EDUROAM WORKSHOP 2017

Routing In Eduroam

THE NAI - NETWORK ACCESS IDENTIFIER

- IETF RFC 7542 defines a standard format for identifying a user.
- The basic format is UTF8 strings in the format <user>@<domain>.
- <user> MUST BE ignored for all routing decisions.
- Domain generally matches the institution’s DNS domain.
- Domain components provide routing information at different levels of the confederation.
    - Complete domain at FLR level
    - Top level domain at TLR level

ROUTING IN EDUROAM

Forskningsnettet - TLR (EMEA)
Janet - FLR (UK)
sussex.ac.uk - IdP
Surfnet
- TLR (EMEA)
Hong Kong Polytechnic - TLR (APAC)
ITB - FLR (ID West)
UII - FLR (ID East)
UII - SP (ID East)
ARRNet - TLR (APAC)

FLR - Route via domain
- ox.ac.uk - University of Oxford
- cam.ac.uk - University of Cambridge
- sussex.ac.uk -> University of Sussex
- …
- * -> EMEA TLR

TLR - Route via tld
- *.ac.id -> APAC TLR
- *.ac.uk -> Janet FLR
- *.ac.au -> APAC TLR
- …
- * -> Drop

TLR - Route via tld
- *.ac.id -> UII/ITB FLR
- *.ac.uk -> EMEA TLR
- *.ac.au -> ARRNet TLR
- …
- * -> Drop

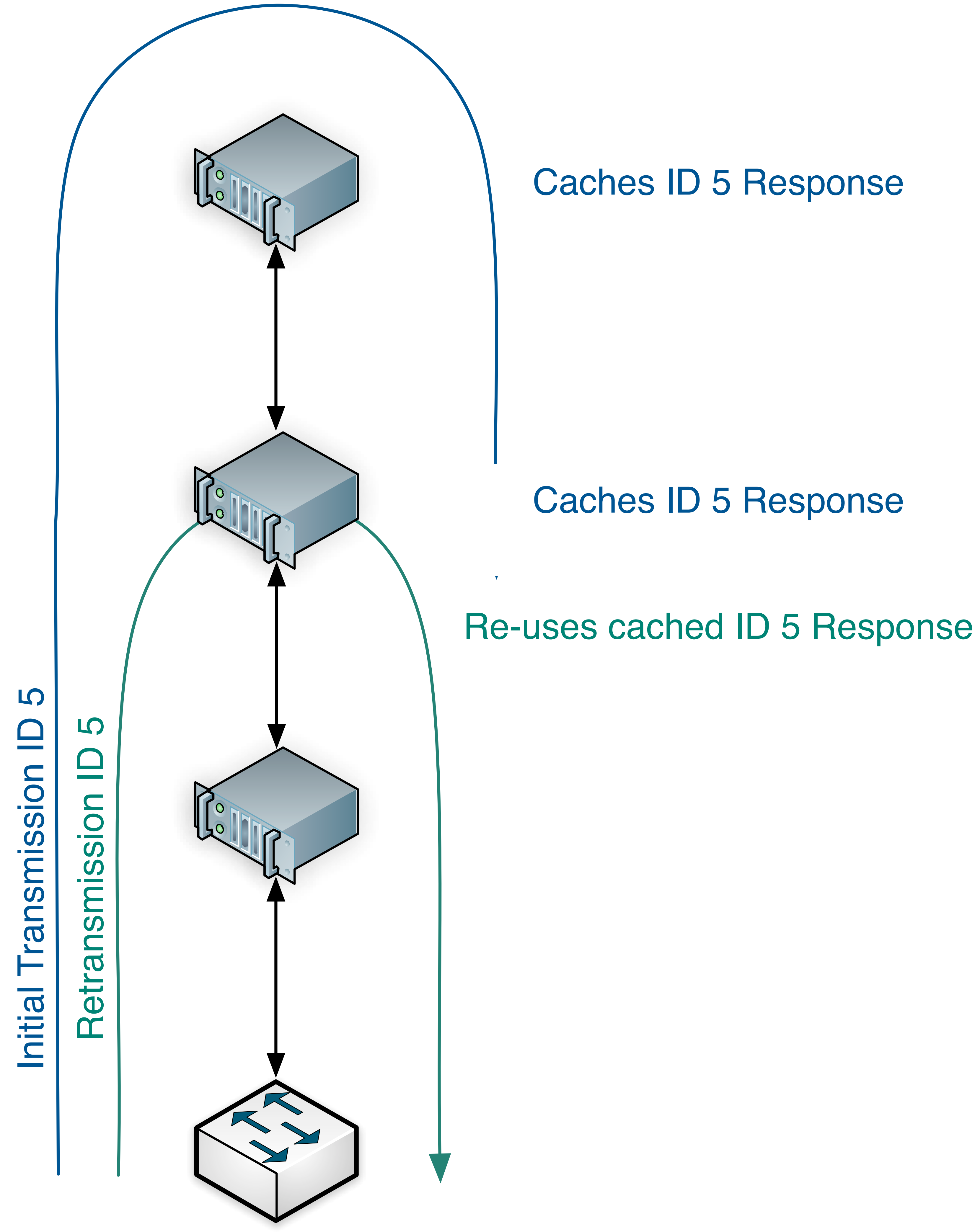
FLR - Route via domain
- ugm.ac.id - Universitas Gadjah Mada
- uii.ac.id - Universitas Islam Indonesia
- itb.ac.id - Institut Teknologi Bandung
- * -> TLR

REDUNDANCY

- Each level in the hierarchy has at least one level of redundancy
- Multiple TLR (Top Level RADIUS) clusters per region.
- Multiple servers for each FLR (Federation level RADIUS) cluster
- Multiple servers for each institution (both IdP and SP).
- Proxying fails over between upstream servers.
- Failover may not be seamless, and there may be temporary disruption.

RADIUS PROXYING

- Defined by RFC 2865
- Runs over UDP (optional DTLS), or TCP (optional RADSEC).
- Monitoring methods:
  - Tracking responses
  - Status-Server
  - Test Requests
- Only 256 outstanding requests per connection due to 8bit request/ response identifier.
- May be minor disruption on failover as timeouts are course (seconds).
- Status-server helps with this, but RFC 2865 forbids proactive monitoring.
- All FreeRADIUS proxy instances are implicitly caching proxy servers which helps with reliability.



FREERADIUS @ UII - EDUROAM WORKSHOP 2017

Tomorrow…

TOMORROW…

- Future technologies in eduroam
- Whatis FreeRADIUS
- FreeRADIUSv4