

eduroam

“Federation Light”

Identity Management & Federation 2019

Role players in eduroam

Identity Providers

- Where you come **from**
- Also known as an “IdP”, “home institution” or “home organisation”
- Responsible for authorisation – answers the question “is this person part of your organisation?”
- Operate a RADIUS[†] server

† Remote Access Dial-In User Service, used for network authentication

Service Providers

- Were you are **visiting**
- Also known as an “SP” or “visited institution”
- Responsible for providing the service – maintains a network and provides Internet access
- Usually operates a wireless network carrying the “eduroam” SSID‡

‡ Service Set Identifier = wireless network name

National Roaming Operators

- Coordinate eduroam within their country or territory
 - Own the trademark for eduroam® in their service area
 - Define national policy
 - Responsible for ensuring compliance with global policy
 - Operate a RADIUS proxy
- Generally one RO per country (NRO), but there are exceptions to this
- The NRO is the federation operator

Global eduroam Governance Committee

- GeGC is responsible for the overall technical standards for eduroam
- Also indirectly for the top level RADIUS proxies
- Chaired by a Canadian (Chris Phillips, CANARIE)
- Has three representatives from the African region:
 - Mohamed Aliouat, (ARN, Algeria)
 - Kennedy Aseda (KENET, Kenya)
 - Samuel Ouya (snRER, Senegal)

eduroam governance model

eduroam governance model

- eduroam relies on a tripartite trust relationship between an IdP, an SP, and the various ROs
- IdPs advertise the eduroam service to their users and trust that SPs will provide it
- SPs trust that the users asserted by an IdP are bona fide members of that organisation
- IdPs and SPs trust ROs to convey information

eduroam governance model

- eduroam policy exists at all levels to:
 - provide a basis for a mutual understanding of responsibilities;
 - make the boundaries of the **trust** relationship clear to all parties; and
 - reduce the risk that the relationship will break down as the result of inadvertent or malicious actions by a minority

<http://eduroam.ac.za/policy>

eduroam governance model

- eduroam policy exists

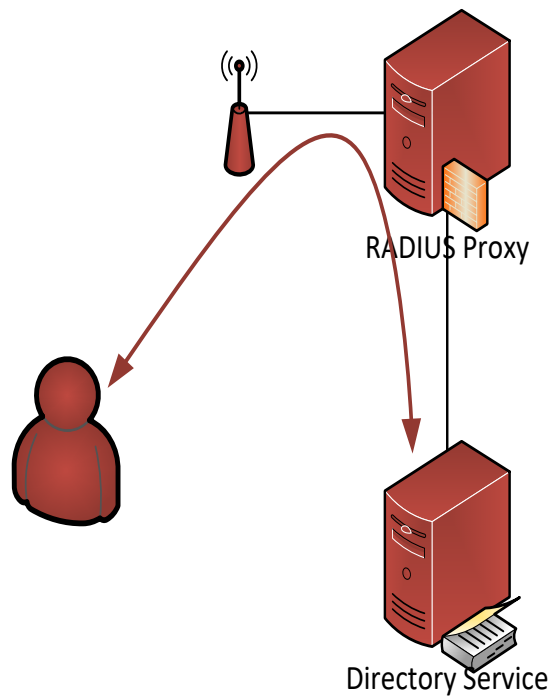
- provide a basis for decisions;
- make the boundaries clear between parties; and
- reduce the risk of disputes as a result of inadvertent or

Trust
is built in the
governance
layer

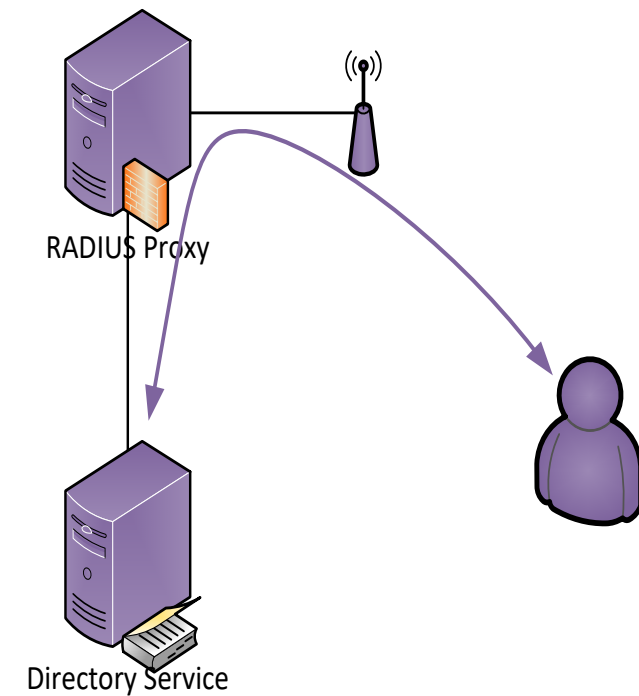
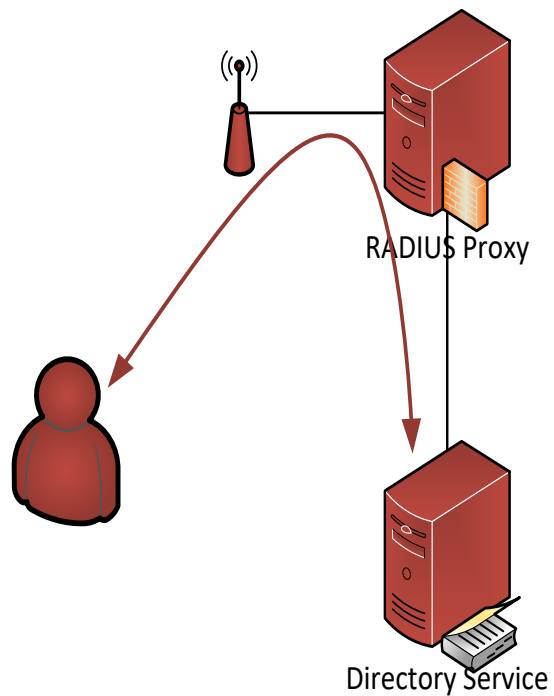
<http://eduroam.ac.za/policy>

How does eduroam work

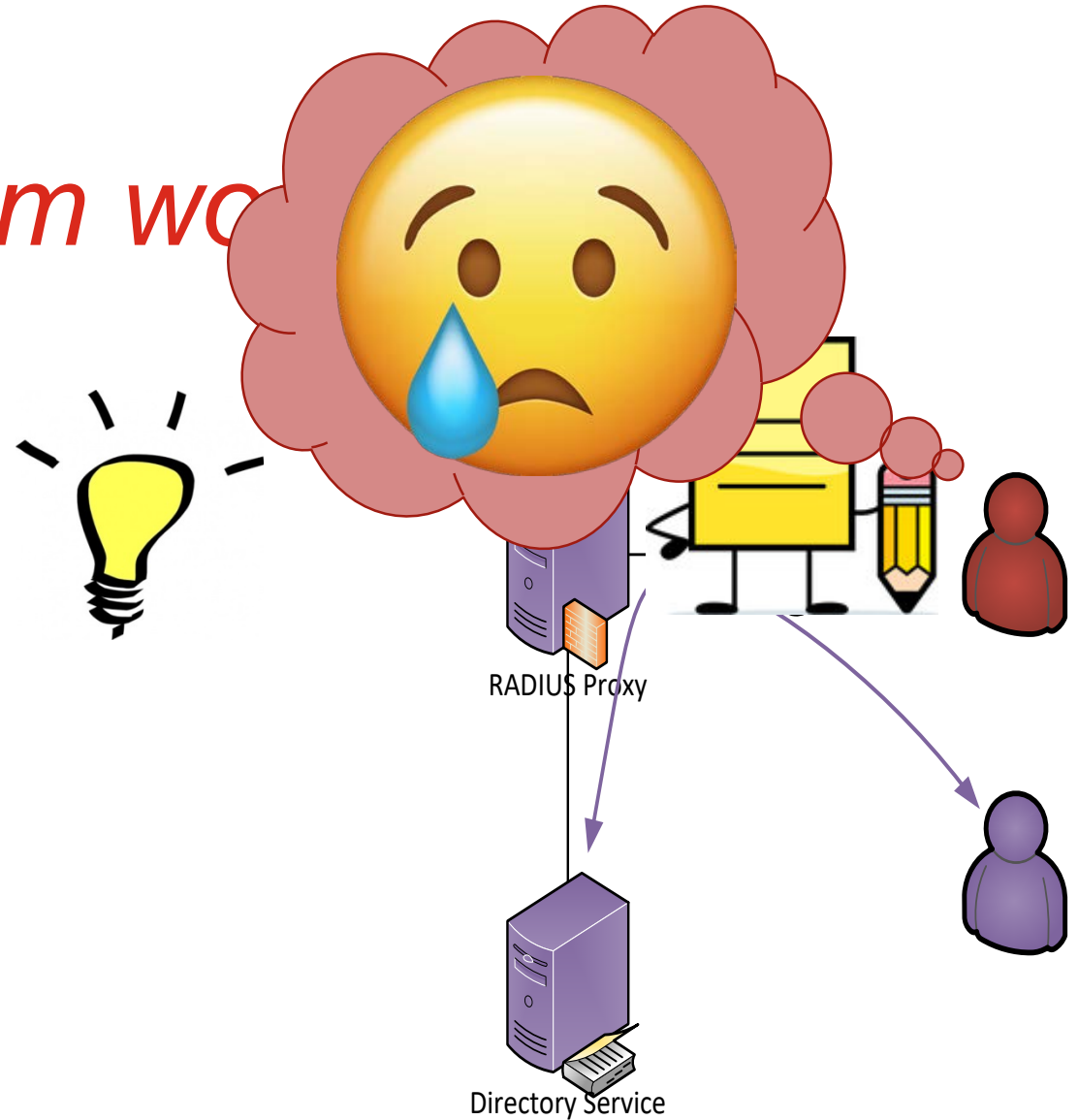
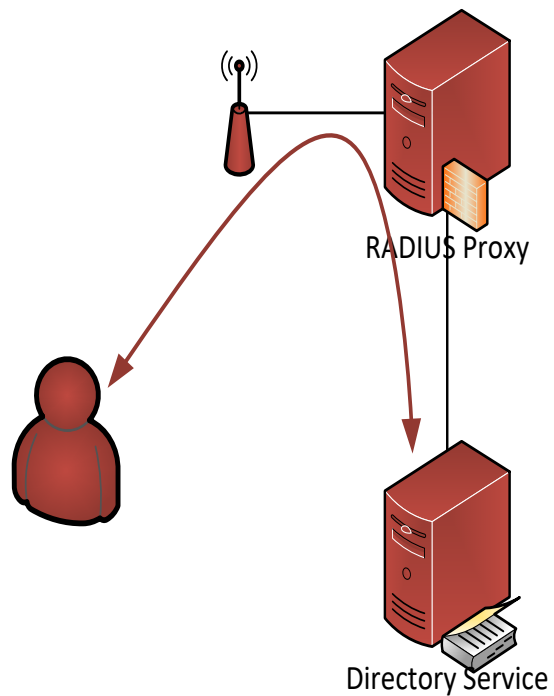
How does eduroam work



How does eduroam work



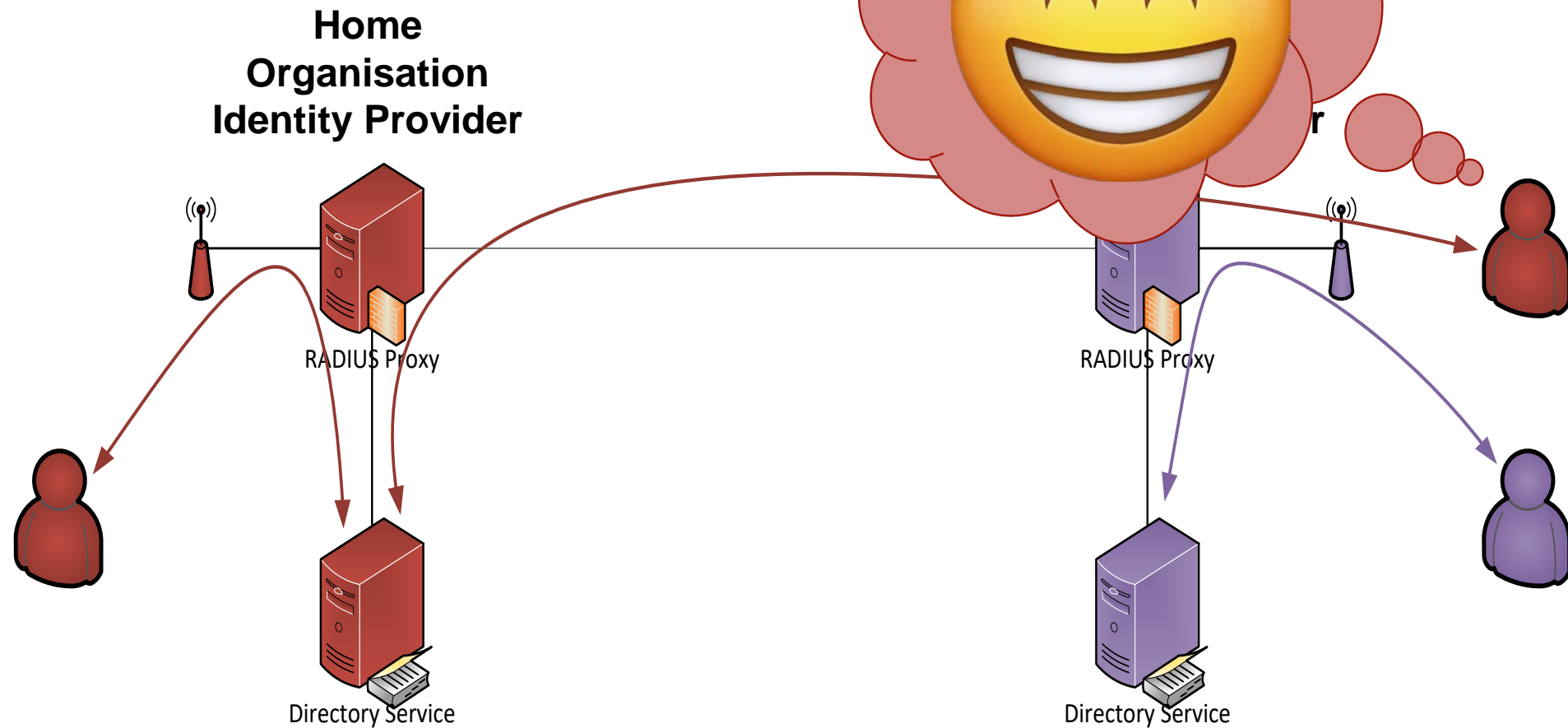
How does eduroam work



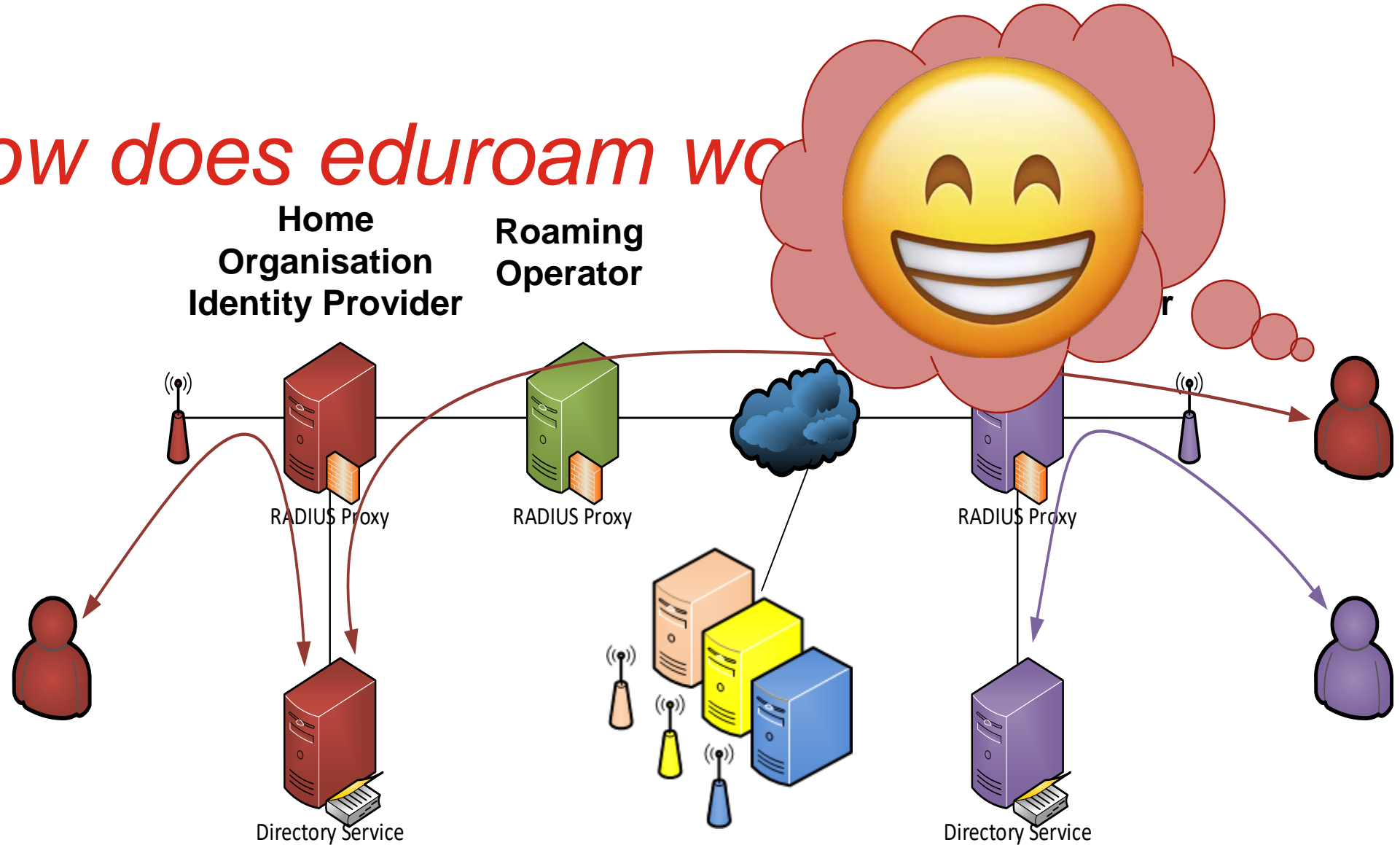
How does eduroam work



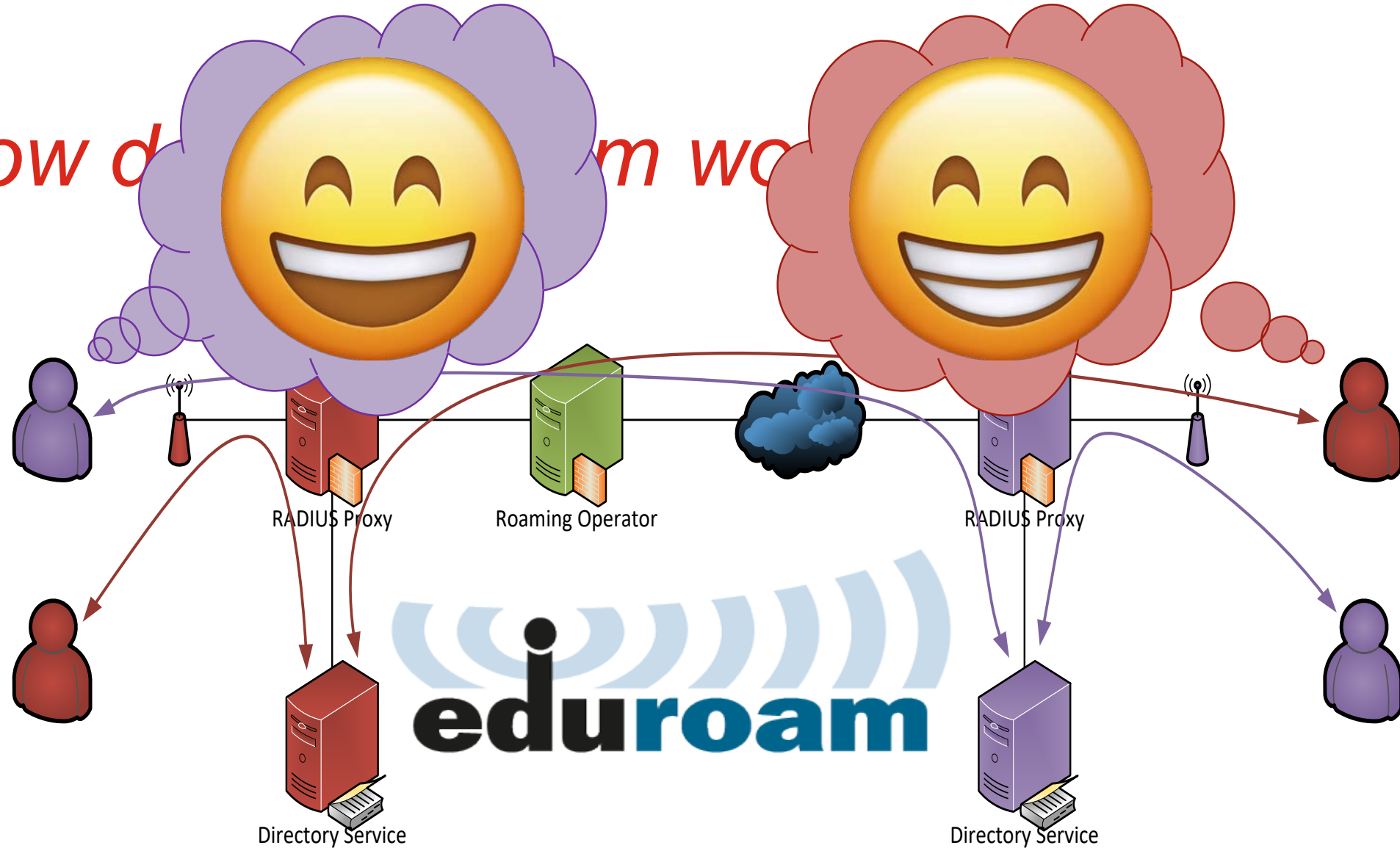
How does eduroam work



How does eduroam work



How do we do it?

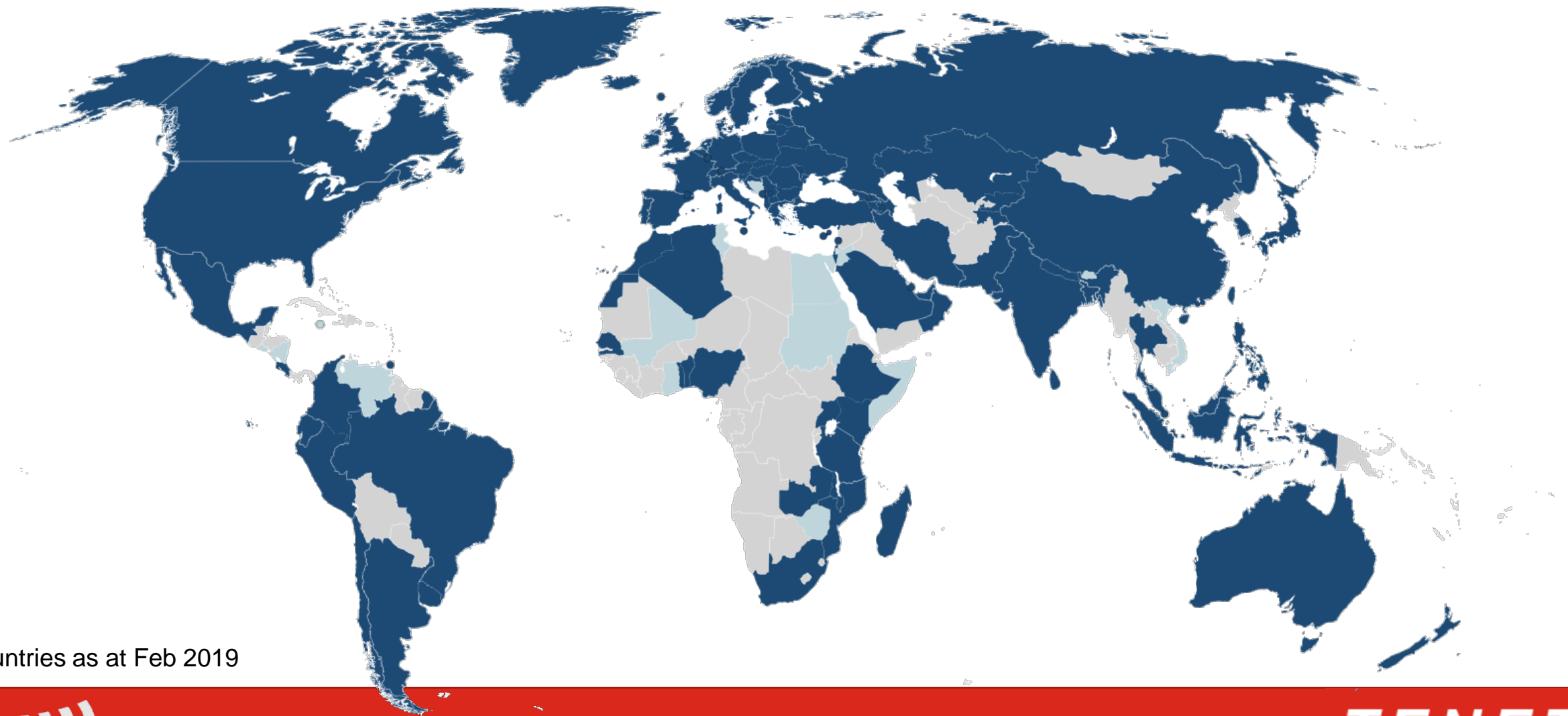


Inter-federation

eduroam confederations

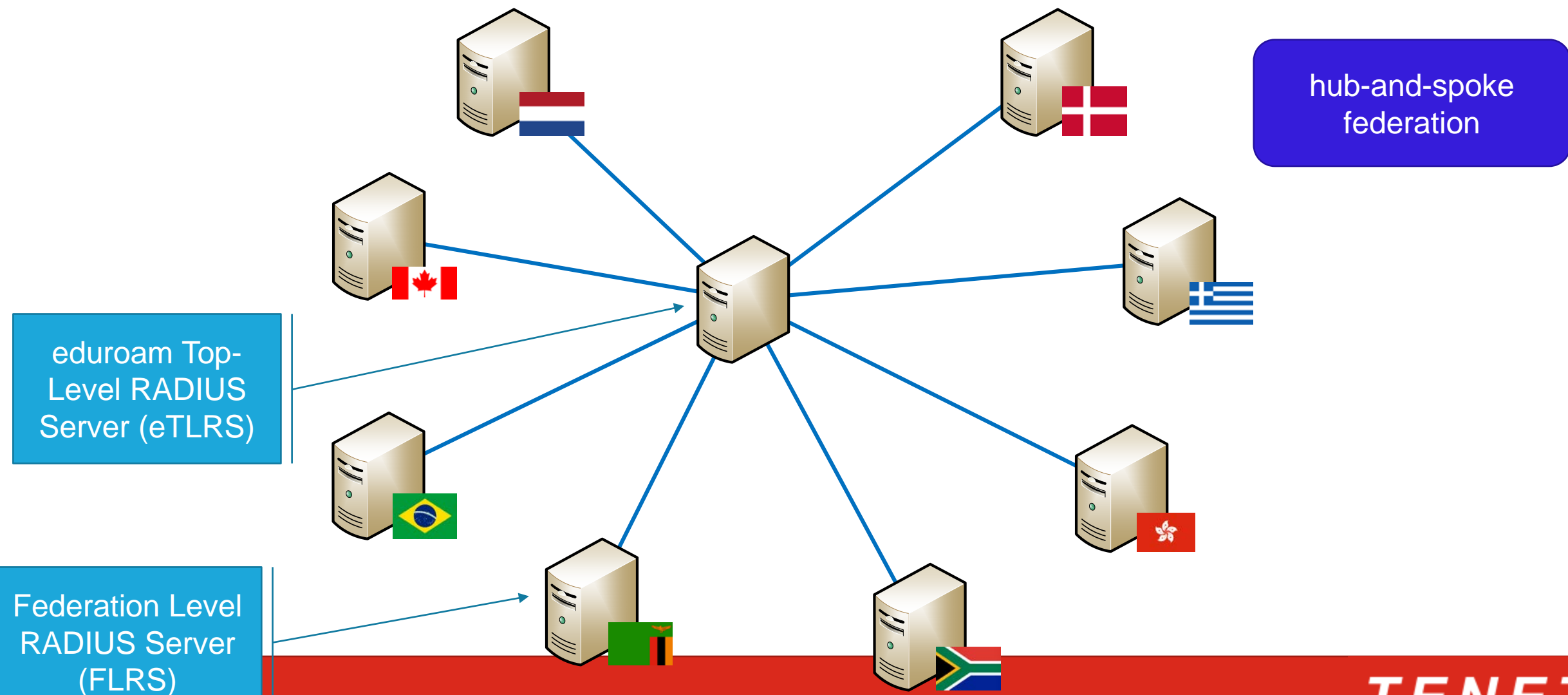


Where can we eduroam?

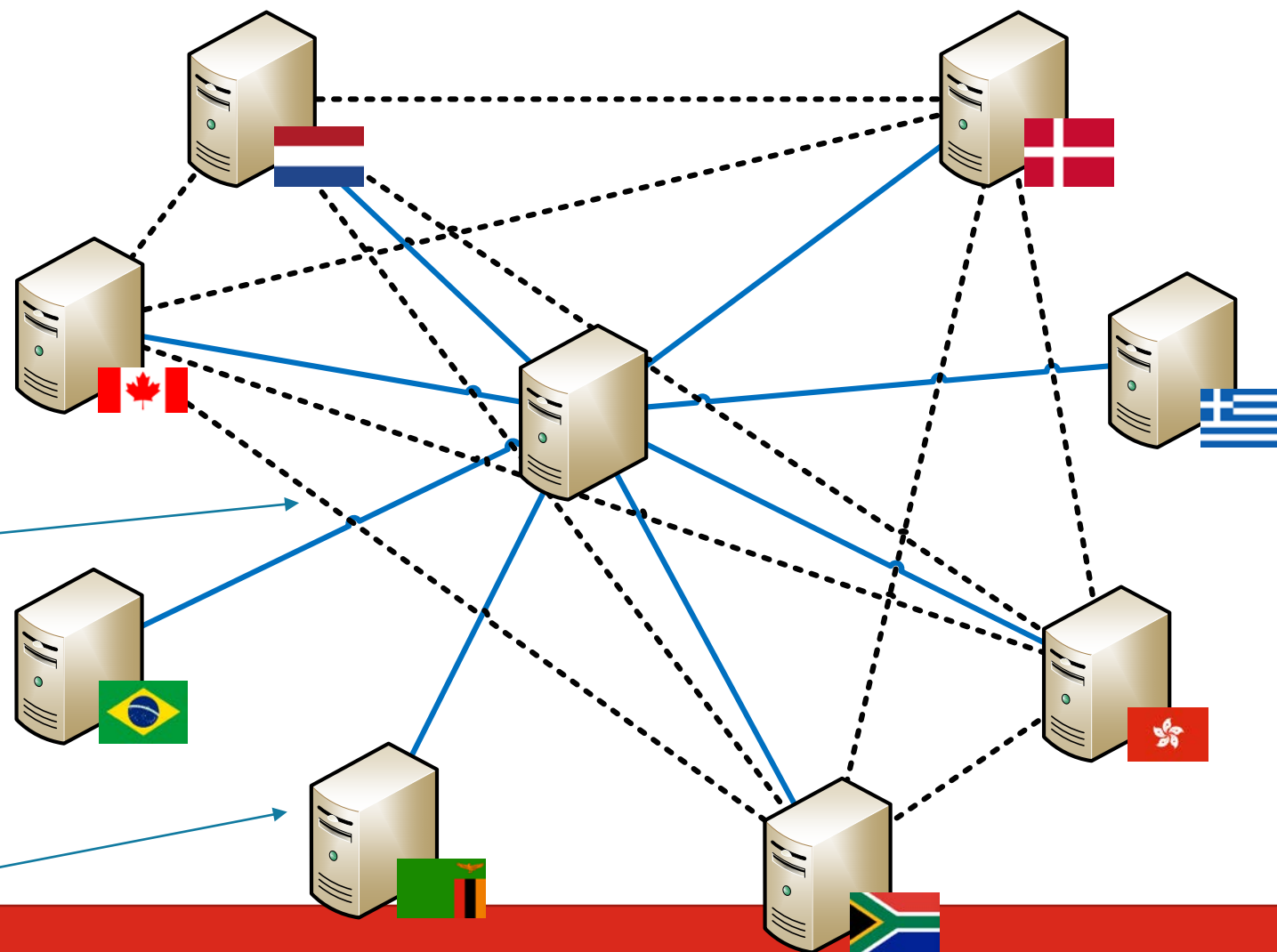


101 countries as at Feb 2019

eduroam inter-federation architecture



eduroam inter-federation architecture



hybrid federation

P2P RadSec via
NAPTR and SRV
DNS records

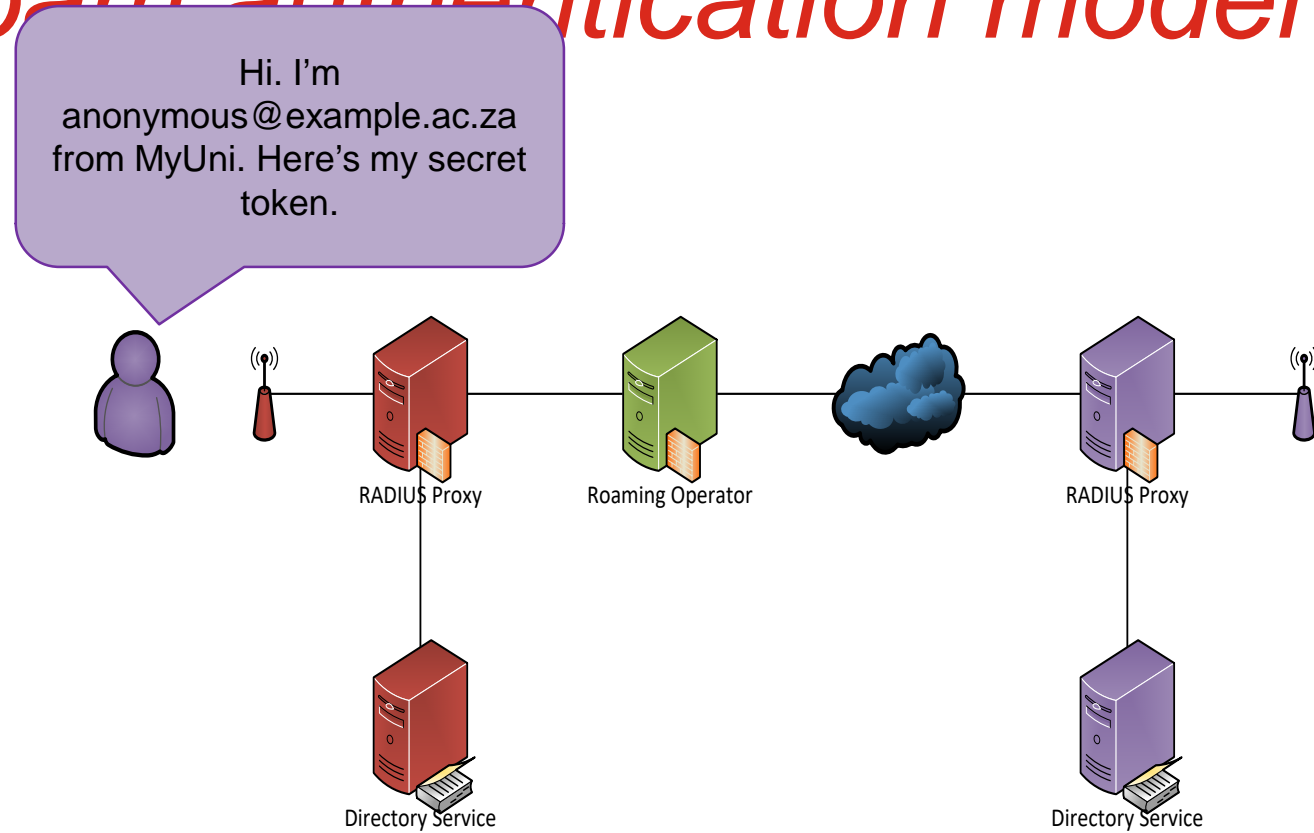
Still reach some
FLRS via eTLRS

eduroam authentication model

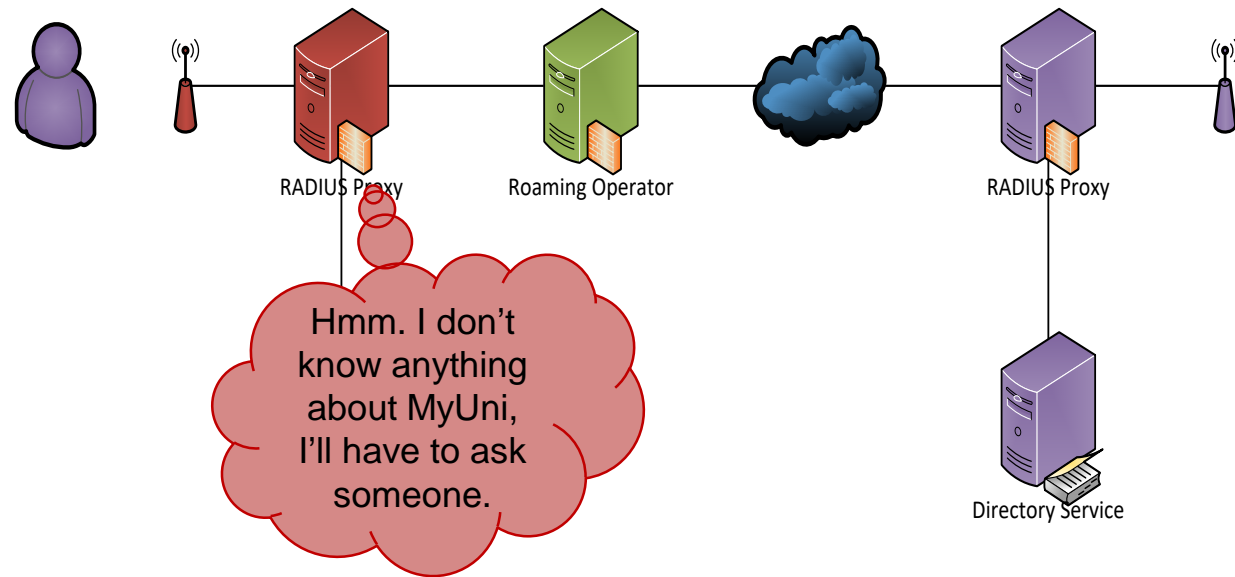
eduroam authentication model



eduroam authentication model

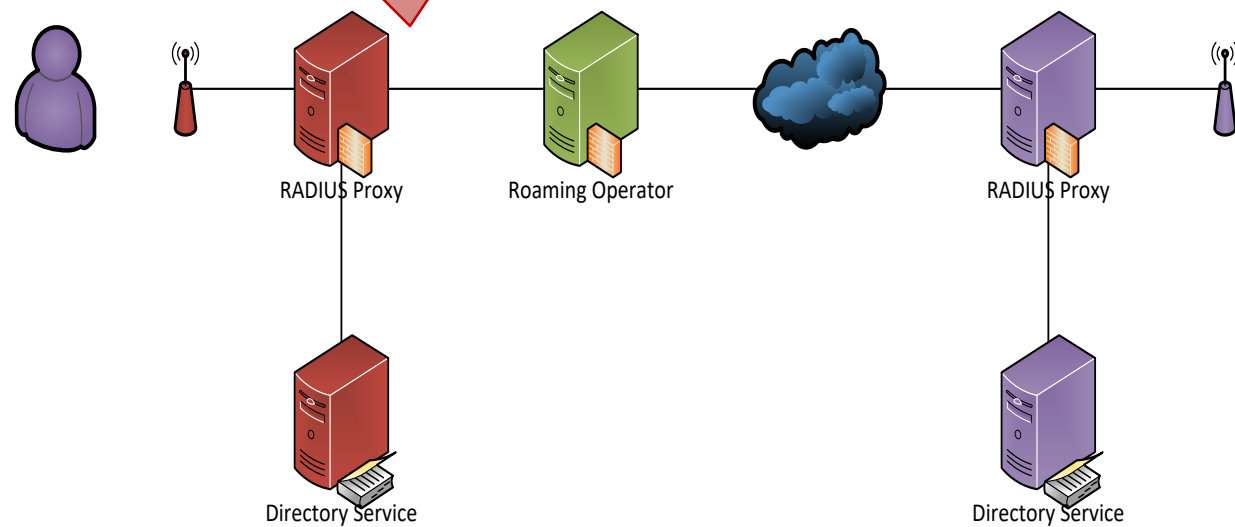


eduroam authentication model

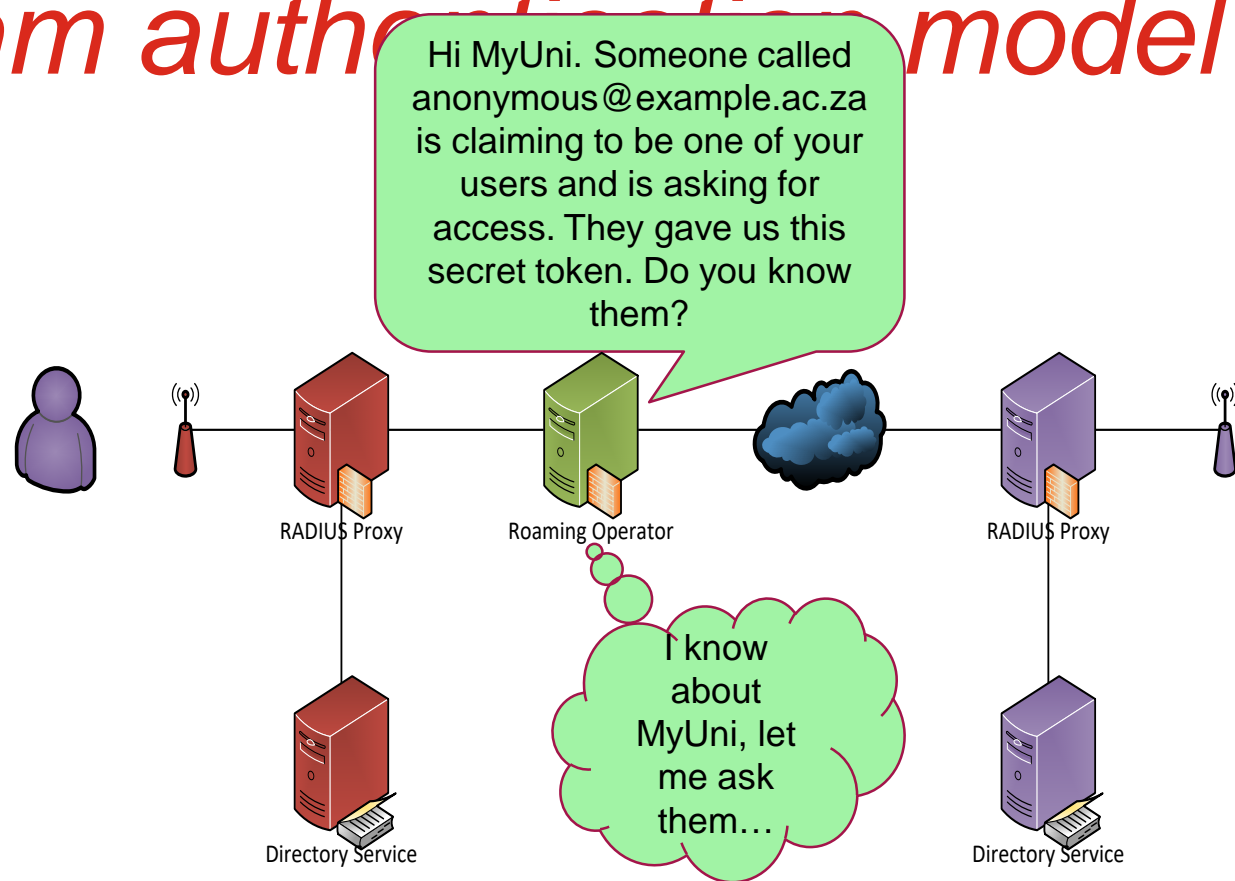


eduroam authentication model

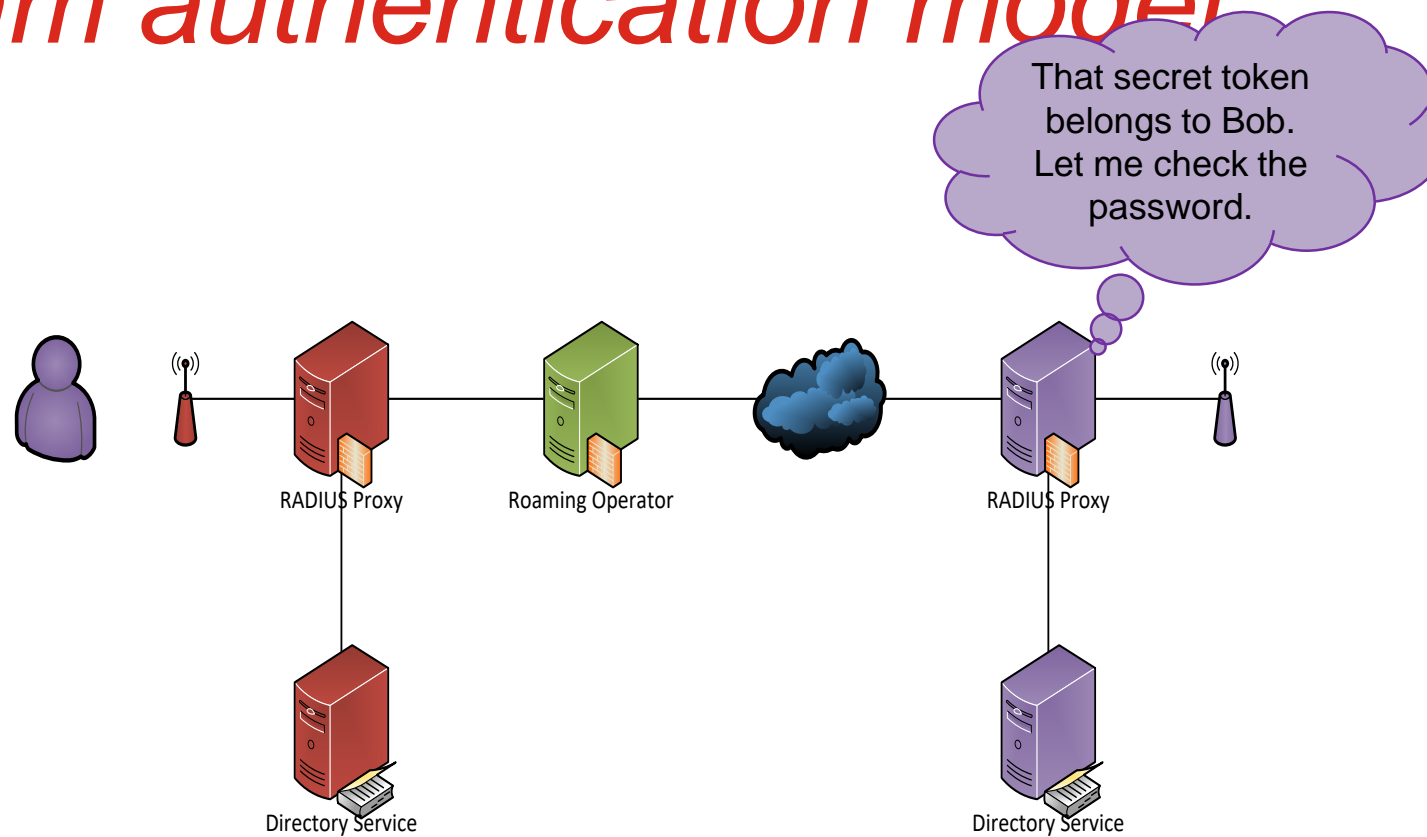
Hey, Roaming Operator, do you know anything about anonymous@example.ac.za from MyUni? They gave me this secret token.



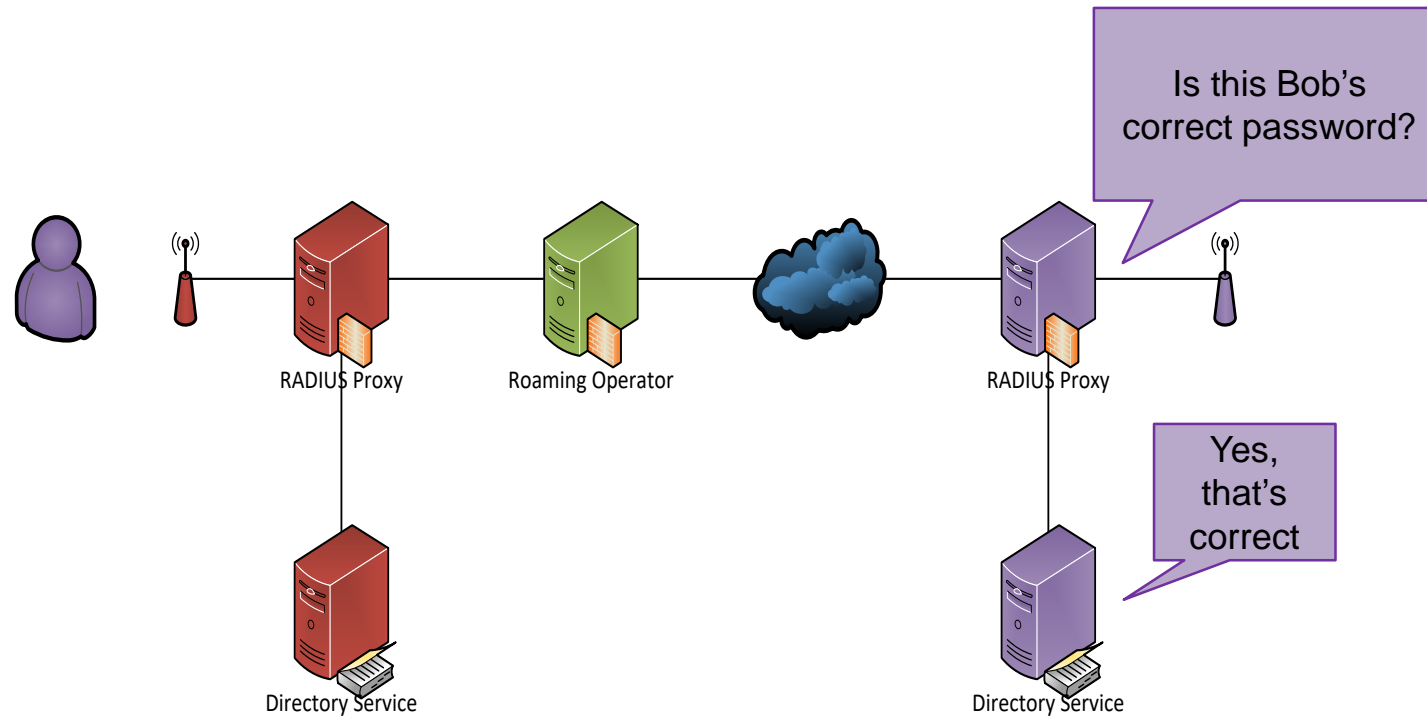
eduroam authentication model



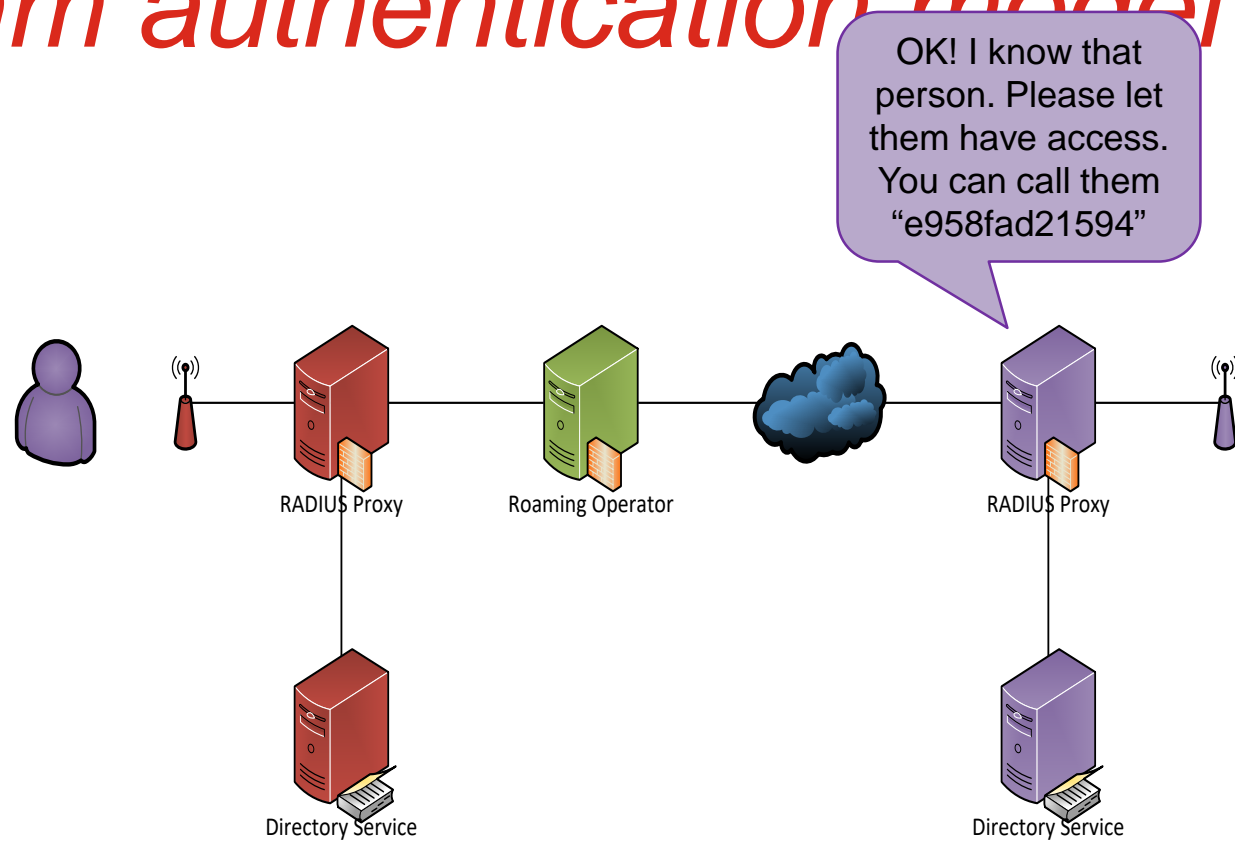
eduroam authentication model



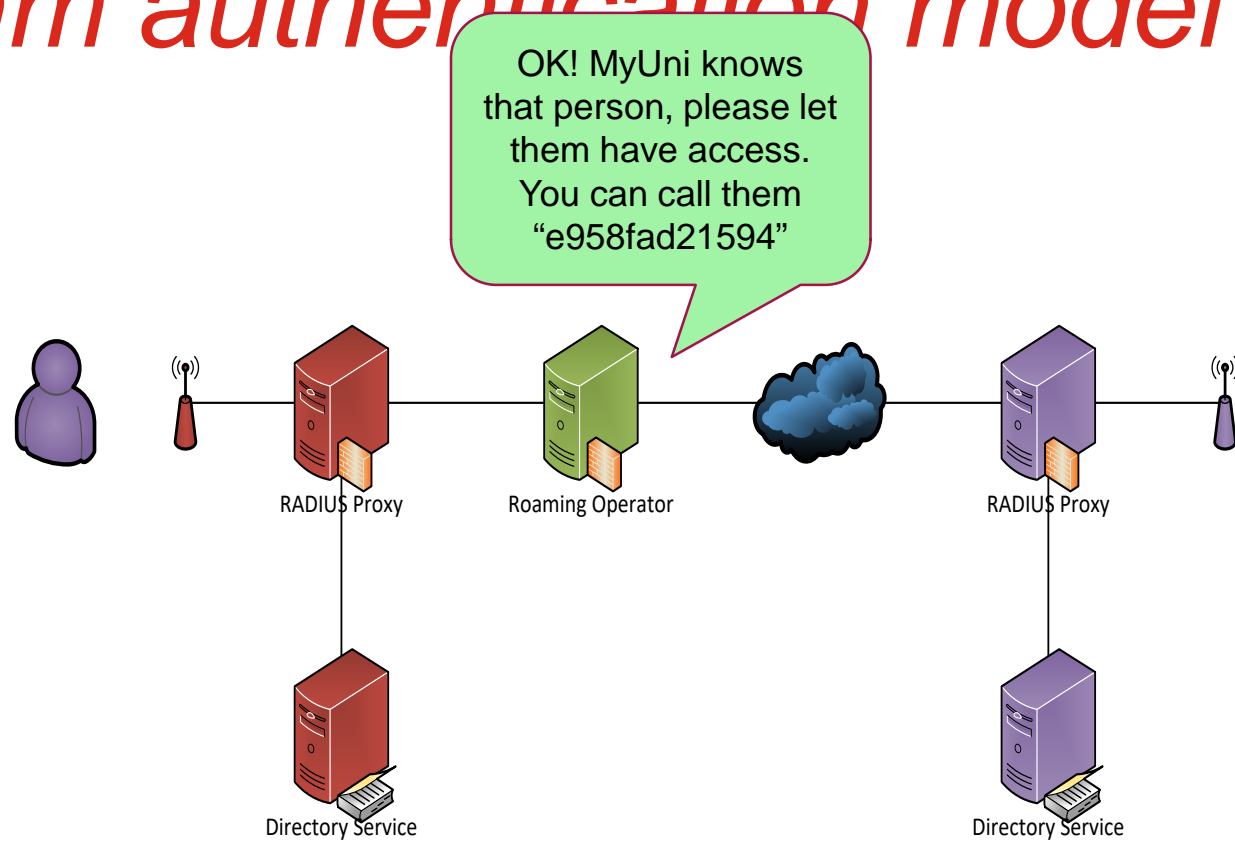
eduroam authentication model



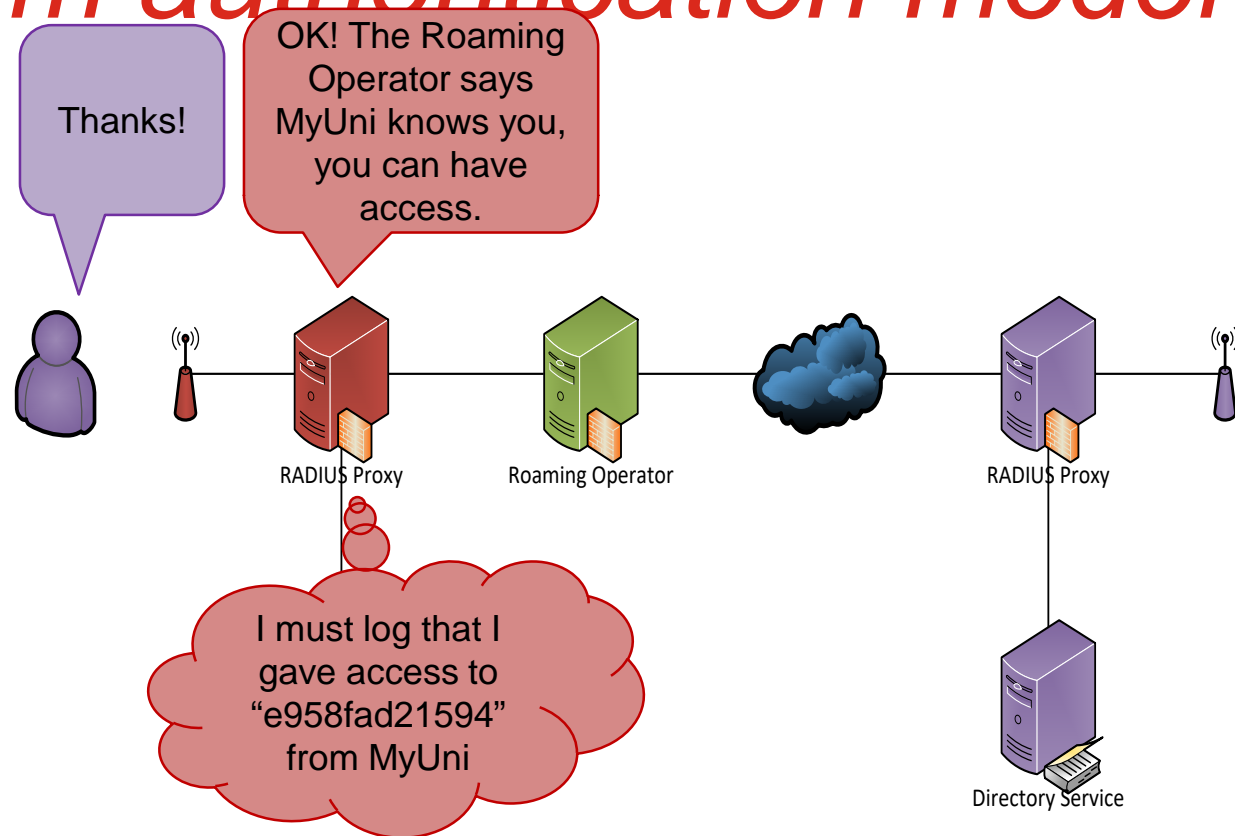
eduroam authentication model



eduroam authentication model



eduroam authentication model



eduroam authentication model

