Philippe Hanset, University of Tennessee Knoxville (phanset@utk.edu)

What is eduroam?

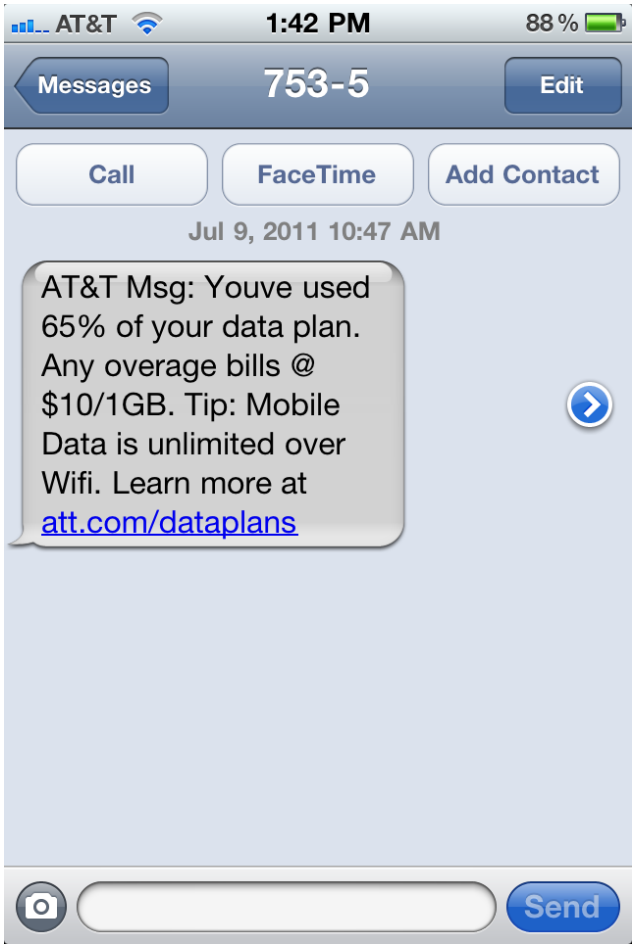
eduroam (**edu**cation **roam**ing**)** is the secure worldwide federated network access service developed for the international research and education community

eduroam relies on a worldwide federation of RADIUS servers to facilitate network access for roaming academic affiliates using IEEE 802.1x as the vehicle.

eduroam is standard based: 802.1x, EAP, RADIUS, SSL/TLS, and WPA2

Why eduroam? (the case for Wi-Fi)

Text Message received from at&t while walking peacefully to Sam's Sourdough Cafe, last Saturday.

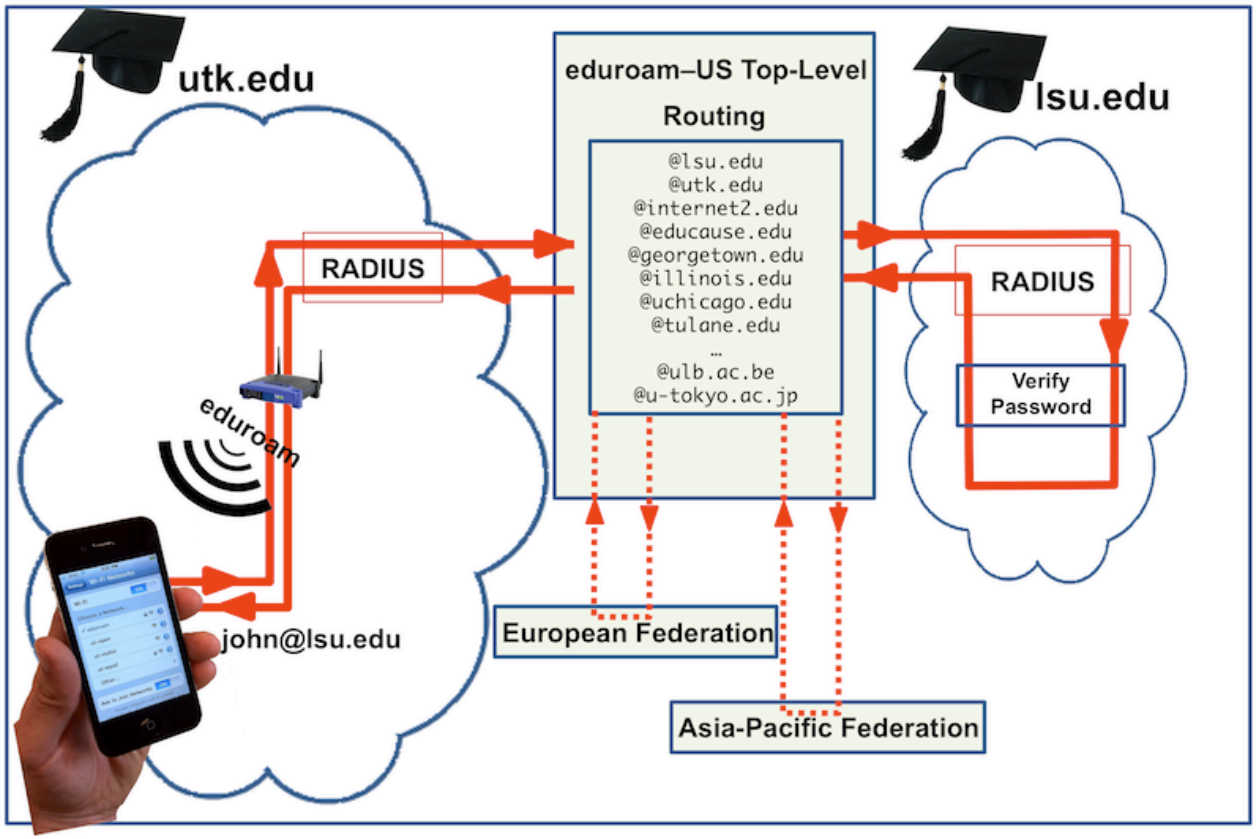


Why eduroam?

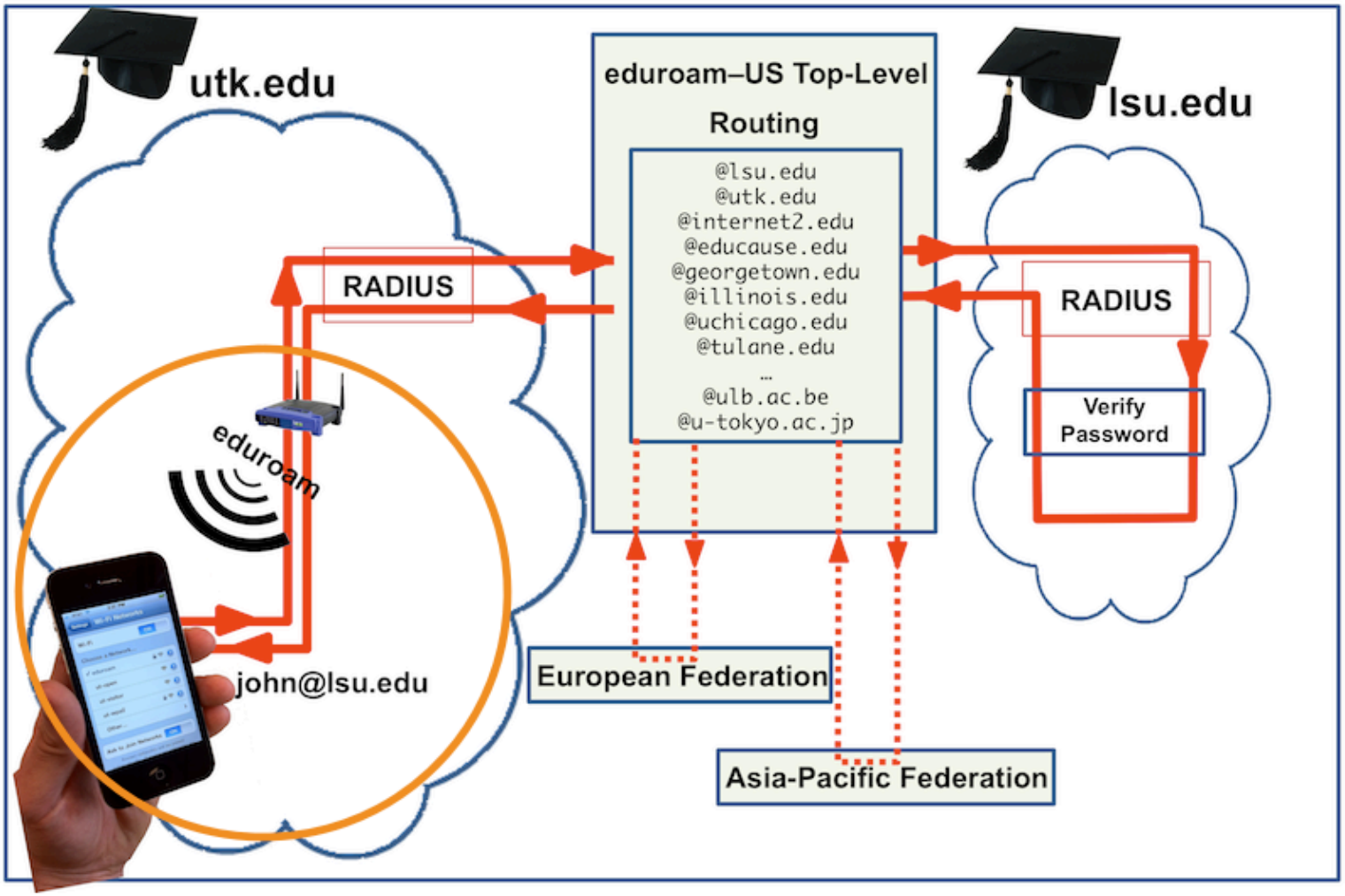
- When roaming:
  - Data over cellular wireless is limited by cost, Wi-Fi is generally not
  - Web portals are time consuming for users, eduroam is automatic and instantaneous
  - Authentication is useful to the user and to the service provider
  - Encryption over the air is not a bad idea
  - Compatibility across the world

How it works

John, from Louisiana State University (a participating eduroam school)
is visiting University of Tennessee Knoxville (another eduroam participating school).
To join UTK's network, John fires up his smartphone and the eduroam authentication process takes place

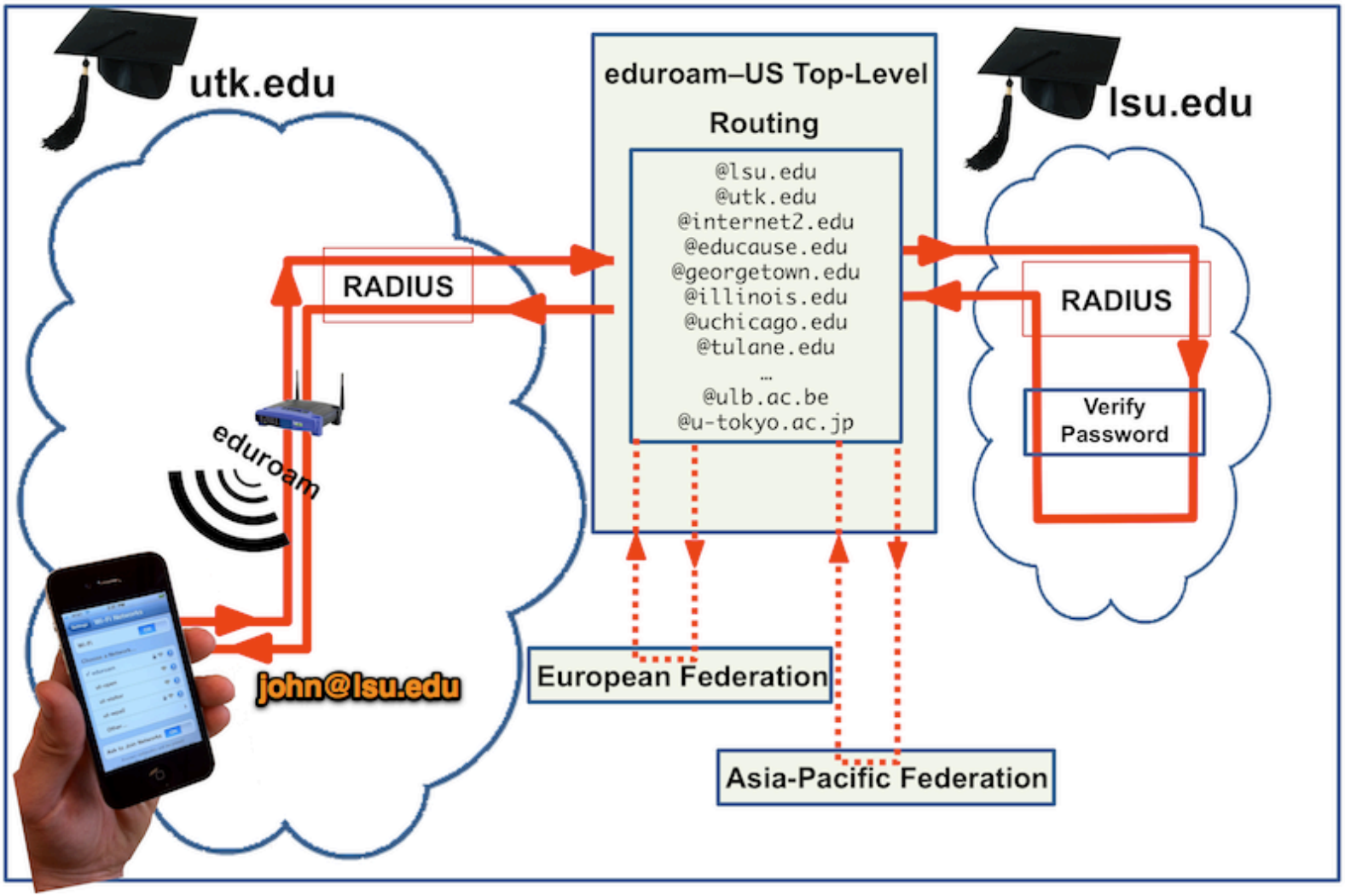


How it works



John's device joins the eduroam SSID
Image 1 of 10

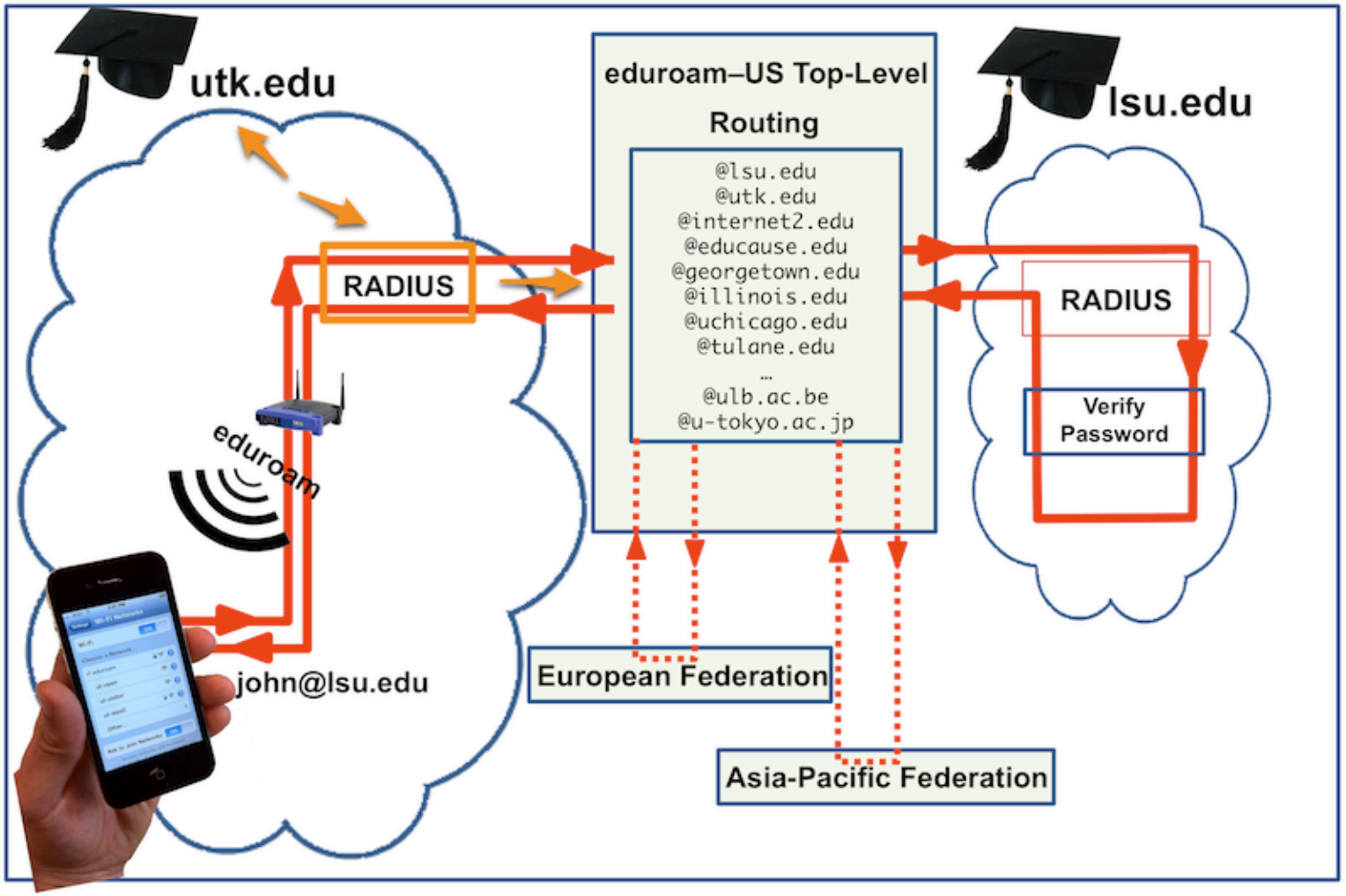
How it works



The client on John's device sends a request to connect to UTK's eduroam network as john@lsu.edu

Image 2 of 10

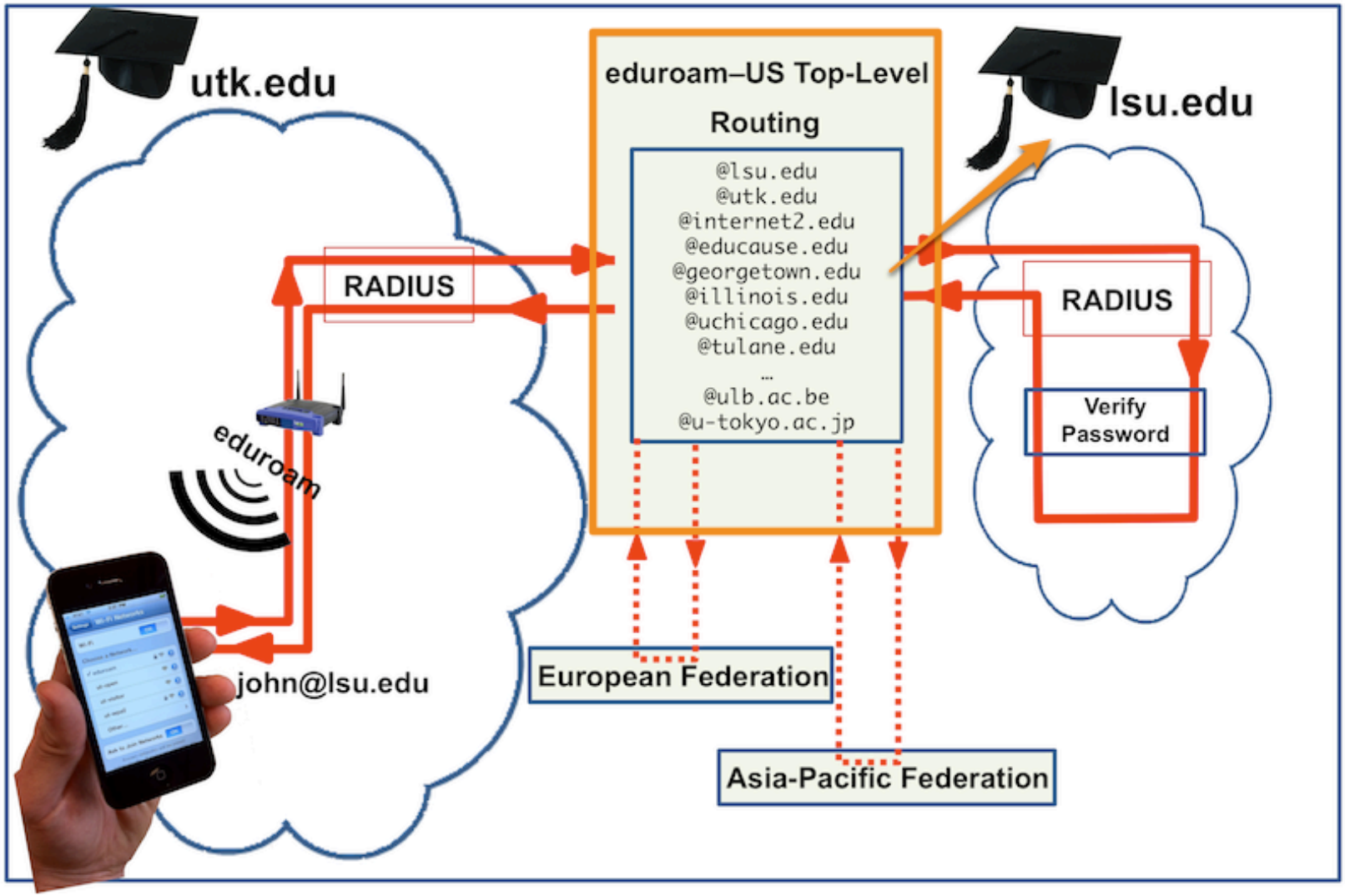
How it works



UTK's local RADIUS server (that is connected to UTK's Wireless Infrastructure) recognizes that John's realm (@lsu.edu) is not local and forwards the request to the national RADIUS server

Image 3 of 10

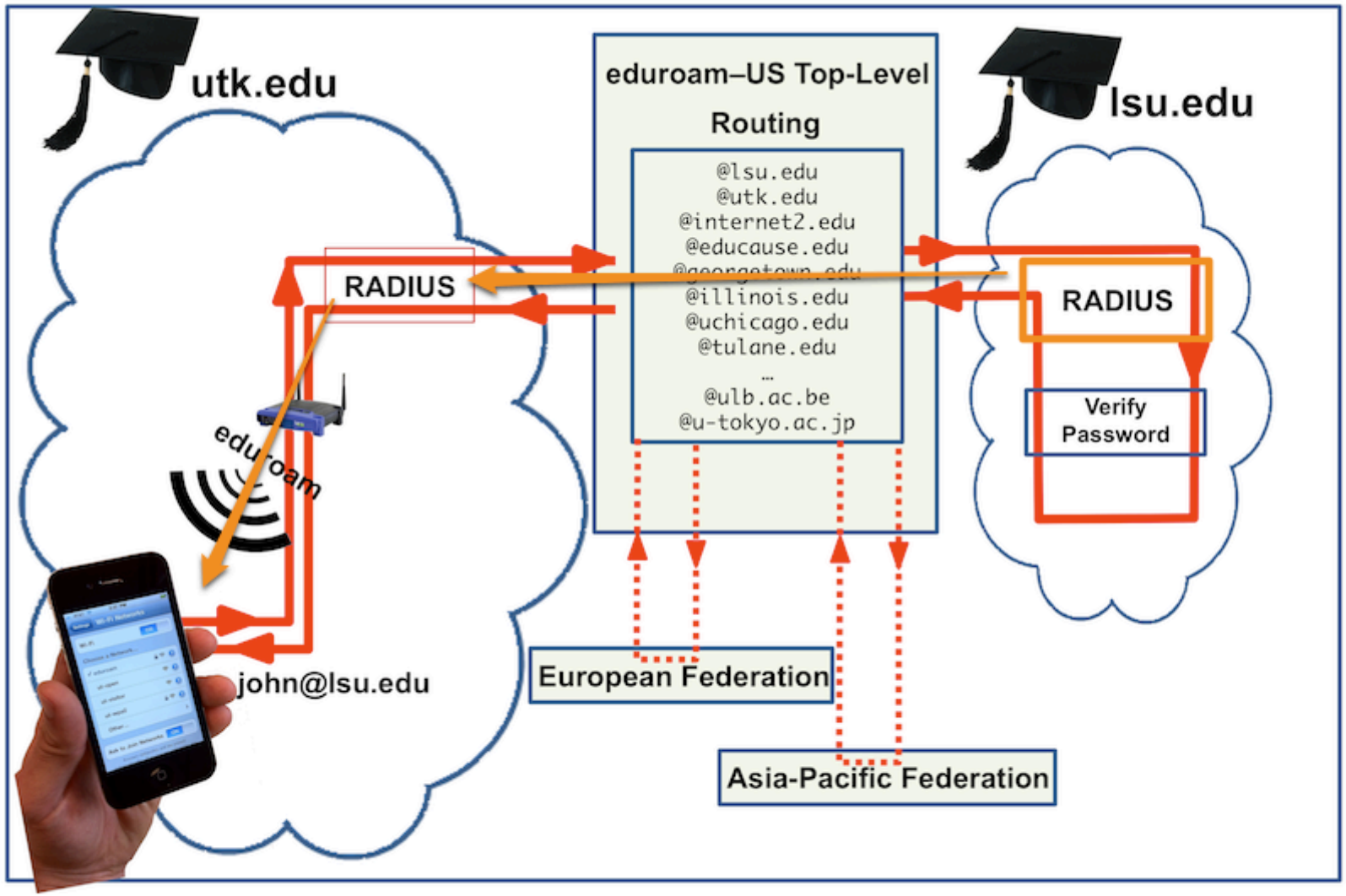
How it works



The national RADIUS server sends the request to the appropriate destination: lsu.edu

Image 4 of 10

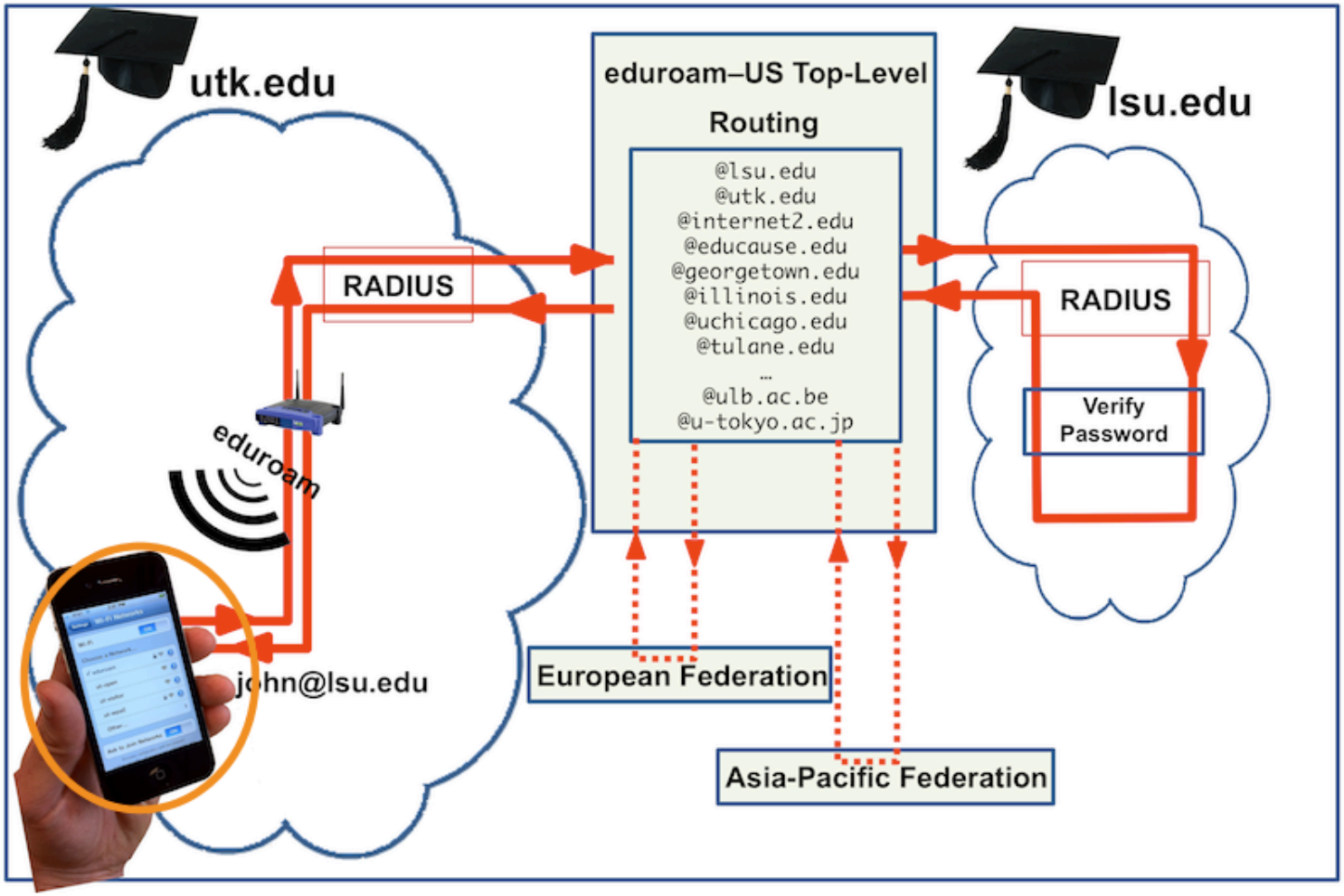
How it works



LSU's RADIUS server sends a certificate challenge back to John. This is the step that will allow John to make sure that UTK's eduroam SSID is a trusted member of the eduroam network.

Image 5 of 10

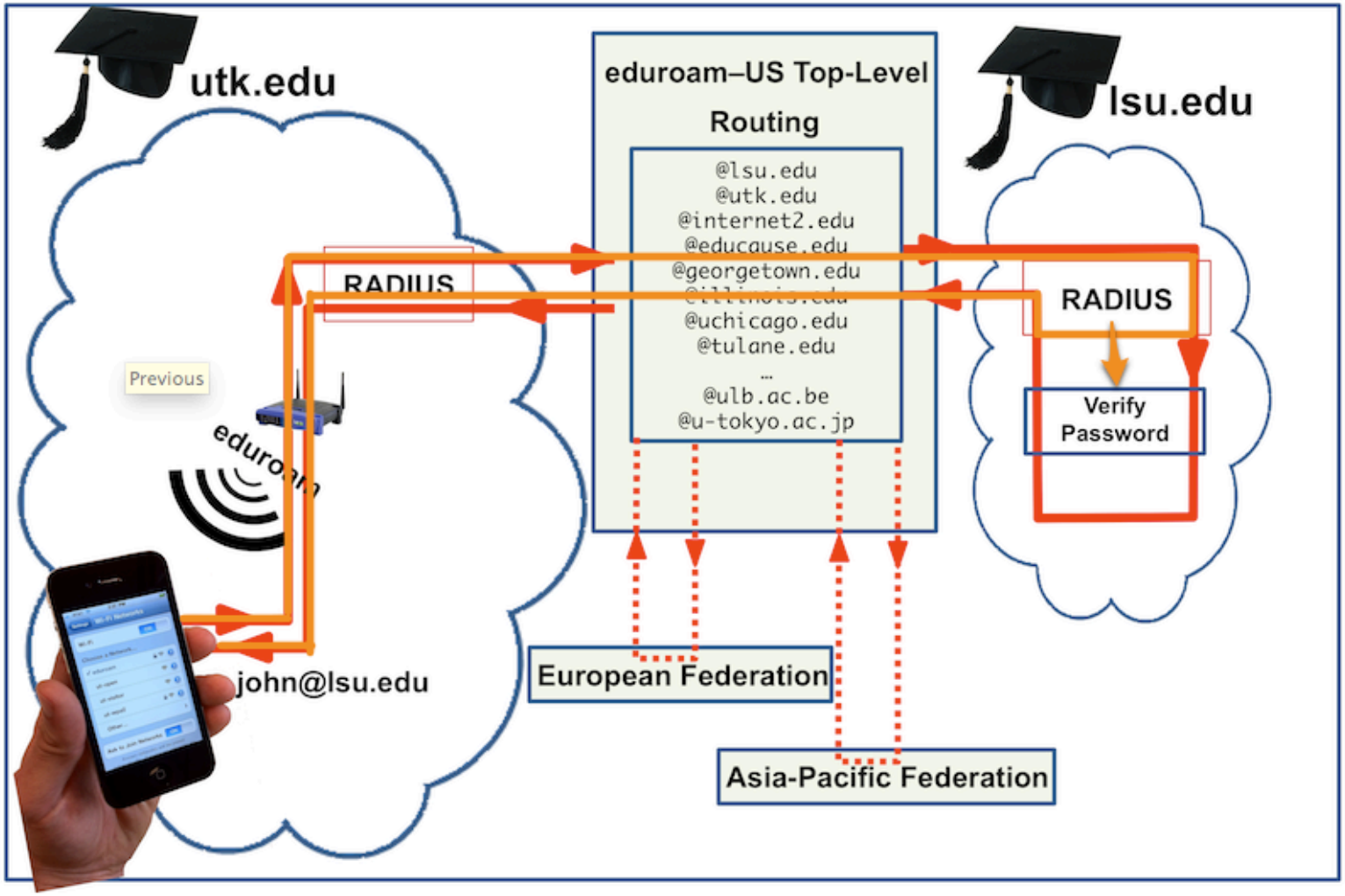
How it works



If the certificate was previously loaded on John's device (an important step in the eduroam process), the device will accept the certificate and establish an encrypted SSL/TLS tunnel between John's device and John's home institution RADIUS server. If John's device doesn't recognize the certificate, John will be prompted to either accept or reject the certificate. In all cases, the certificate will show the Common Name (e.g. eduroam-radius.lsu.edu). John shouldn't accept a Certificate with an unknown name (e.g. iwillownyou.com) as this indicates a Rogue Network.

Image 6 of 10

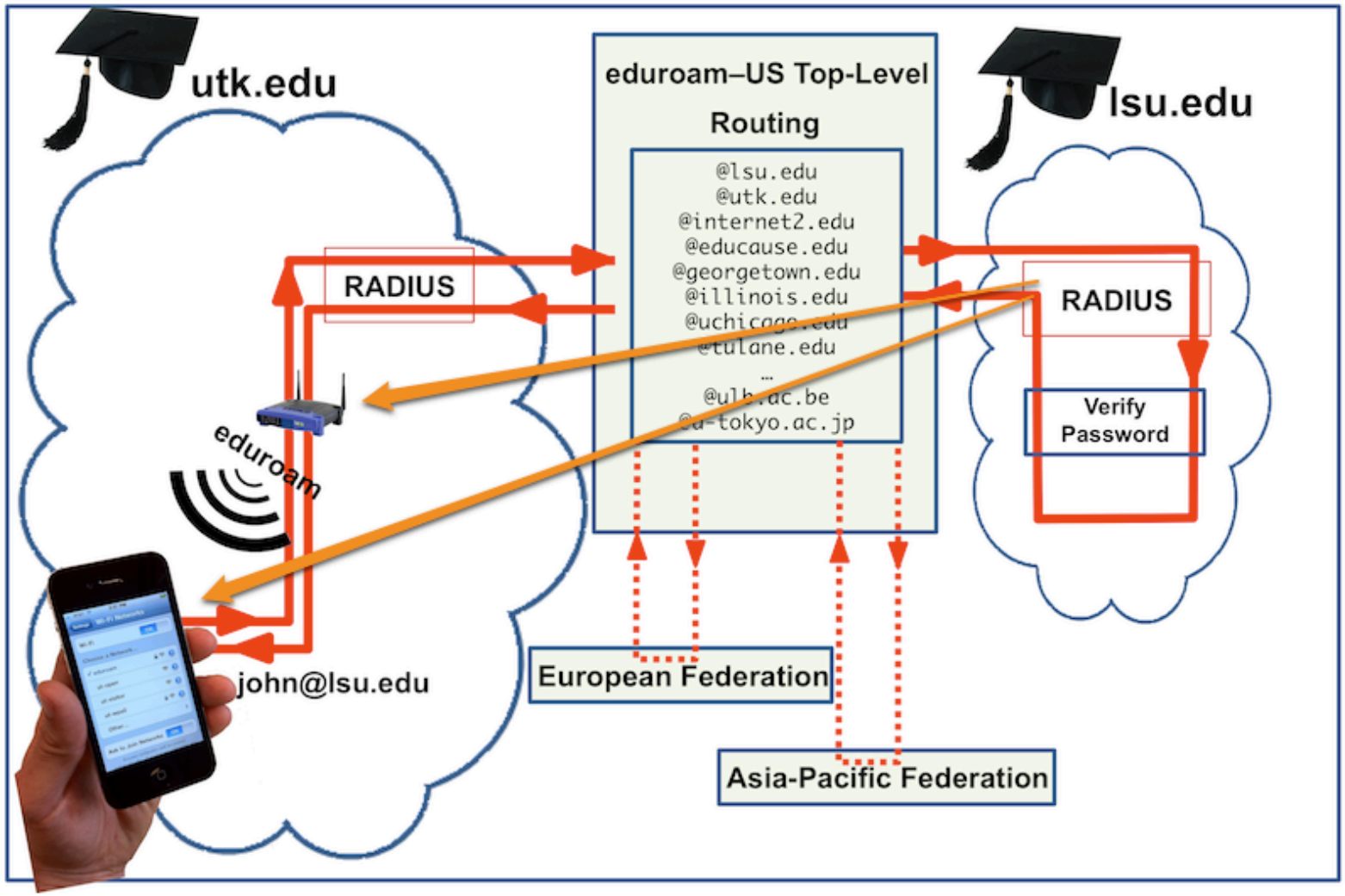
How it works



Now that the encrypted tunnel is established between John's device and LSU's RADIUS server, John's credentials are passed in the SSL/TLS encrypted tunnel between John's device and LSU's RADIUS server for verification. For this authentication step the RADIUS server is connected to the institution's Directory Service.

Image 7 of 10

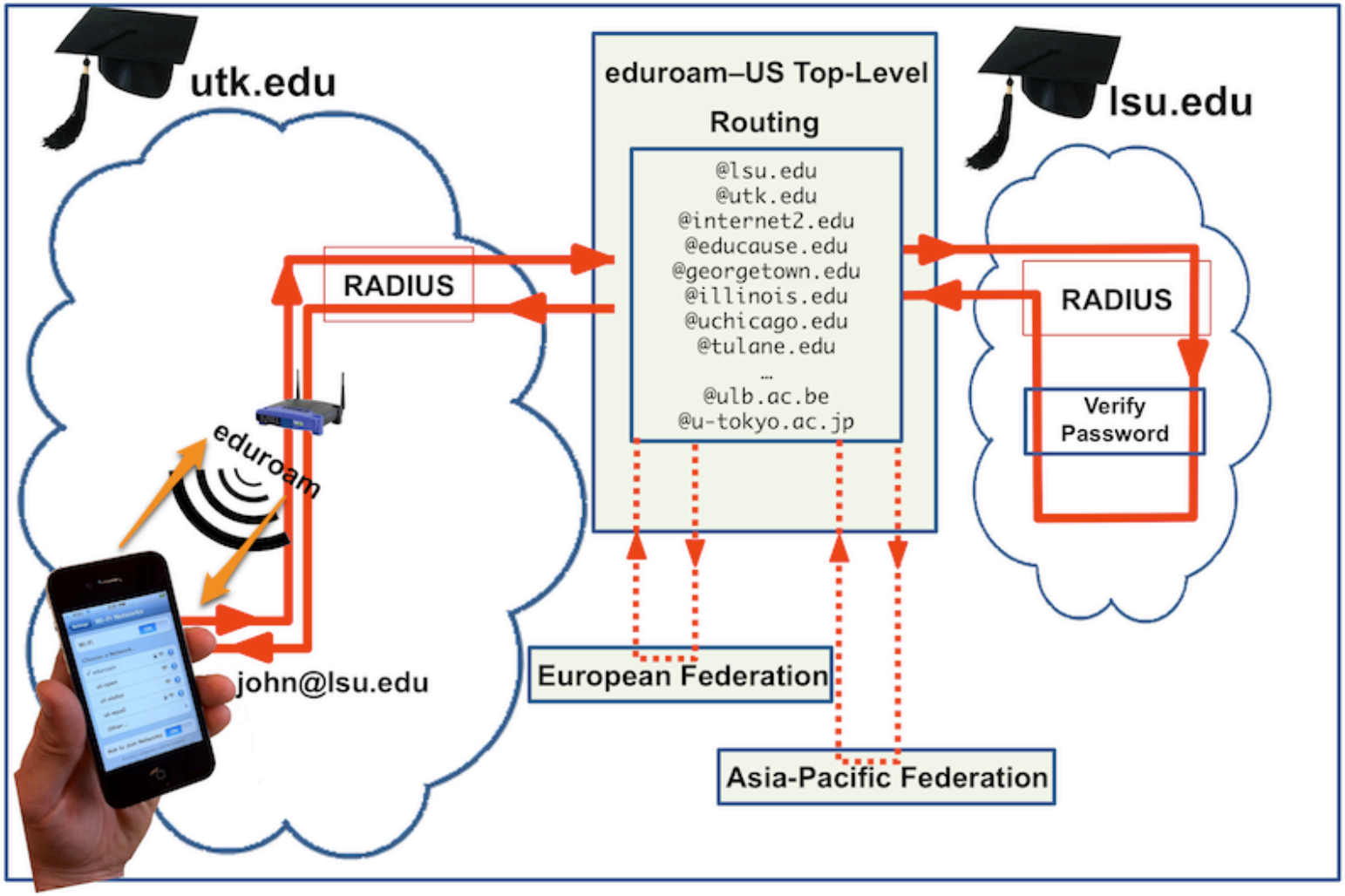
How it works



Upon successful authentication, LSU's RADIUS server sends an access-accept and some keying material to UTK's Infrastructure (outside the SSL tunnel) and some private keying material to John (inside the SSL tunnel).

Image 8 of 10

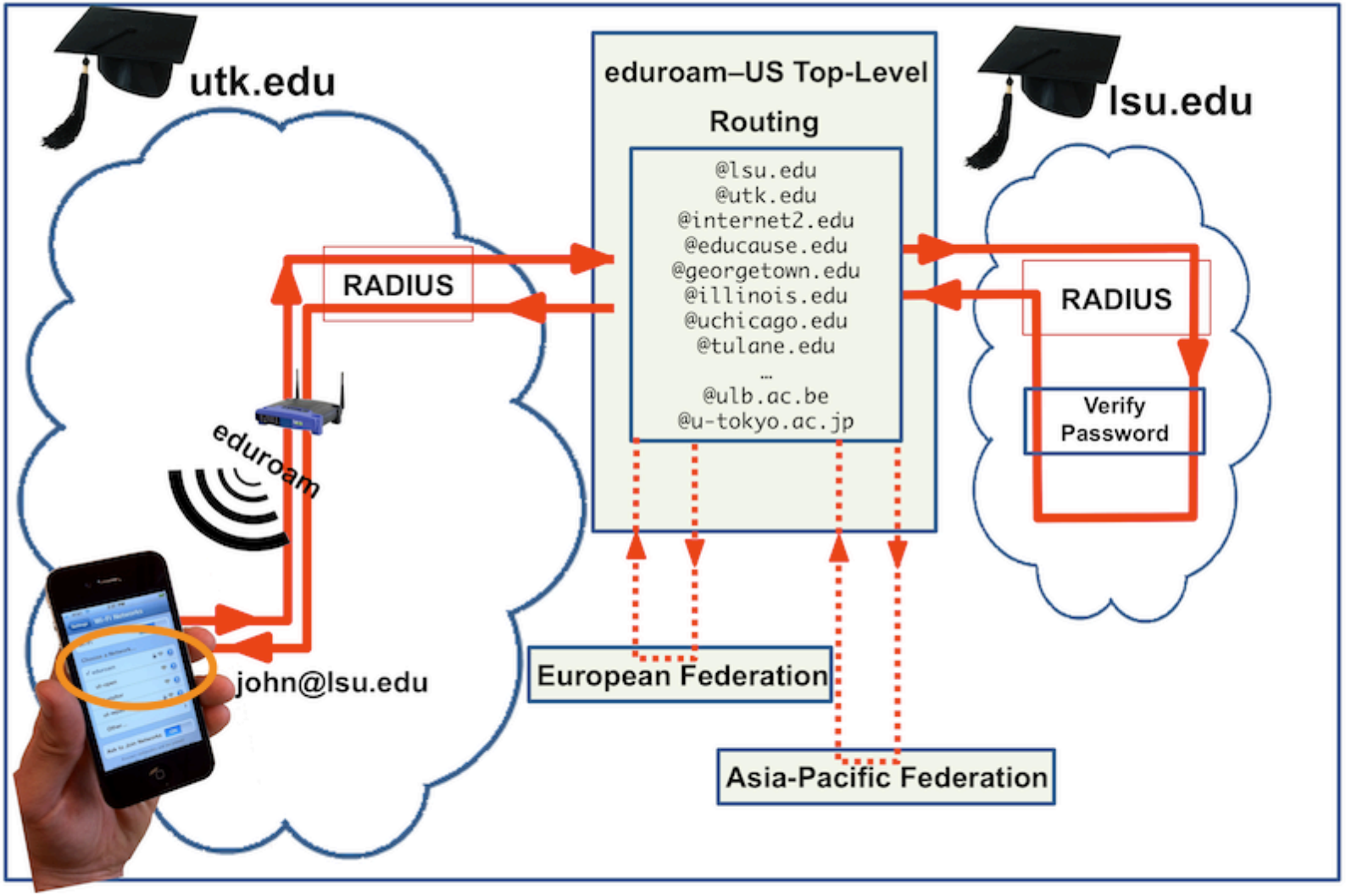
How it works



UTK's eduroam wireless infrastructure negotiates with John's device encryption key exchange to allow access on the network and enable encryption between John's device and UTK's wireless access-points.

Image 9 of 10

How it works



John can now connect to the eduroam SSID at UTK and enjoy authenticated and encrypted connectivity between his device and UTK's wireless network.

Image 10 of 10

eduroam: pros and cons

- Pros
  - Instant Access (no portals to deal with)
  - Authentication and encryption
  - Authenticated Infrastructure
  - Easy provisioning of access to network
  - EAP method independent
  - Layer2: works for IPv4 and IPv6
- Cons
  - No communication mechanism (inherent to 802.1x)
  - No solution “yet” for non R&E visitors
  - 802.1x (WPA2-enterprise) isn’t available on game consoles

eduroam in the US

Green = active (19)
Yellow = testing (16)

V = Service Provider only (1)
Blue = interested (24)

eduroam in the World

eduroam facts

- More regional than international
- Big savings on data roaming charges when abroad
- A few hours of work to peer with top level RADIUS server
- Setting up the eduroam network on campus takes more time
- Very few trouble calls (not HelpDesk intensive)

  (testimonies from UChicago, UCSD, LSU)

Resources

- eduroamus.org = eduroam.us
  - general documentation (maps, slideshow, …)
  - peering request form
  - documentation for various RADIUS flavors
  - Links to campus eduroam pages

- eduroam.org
  - new developments
  - Policies
  - and much more