Supported by the
Walloon Region

Using tunnels and three party authentication to improve roaming security

Damien LEROY

UCLouvain - Belgium

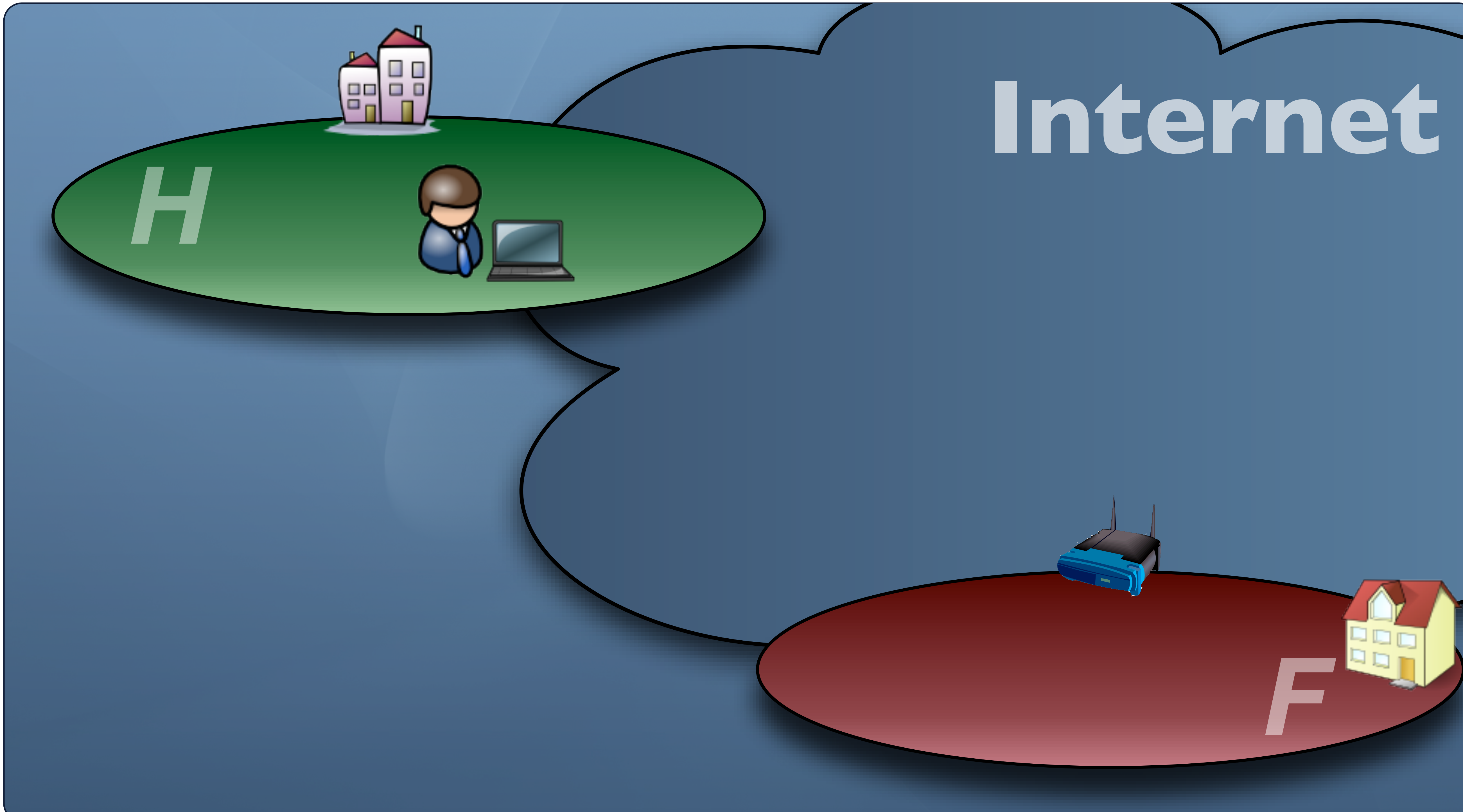
IP Networking Lab - http://inl.info.ucl.ac.be

BELNET Security Conference - April 30th, 2009

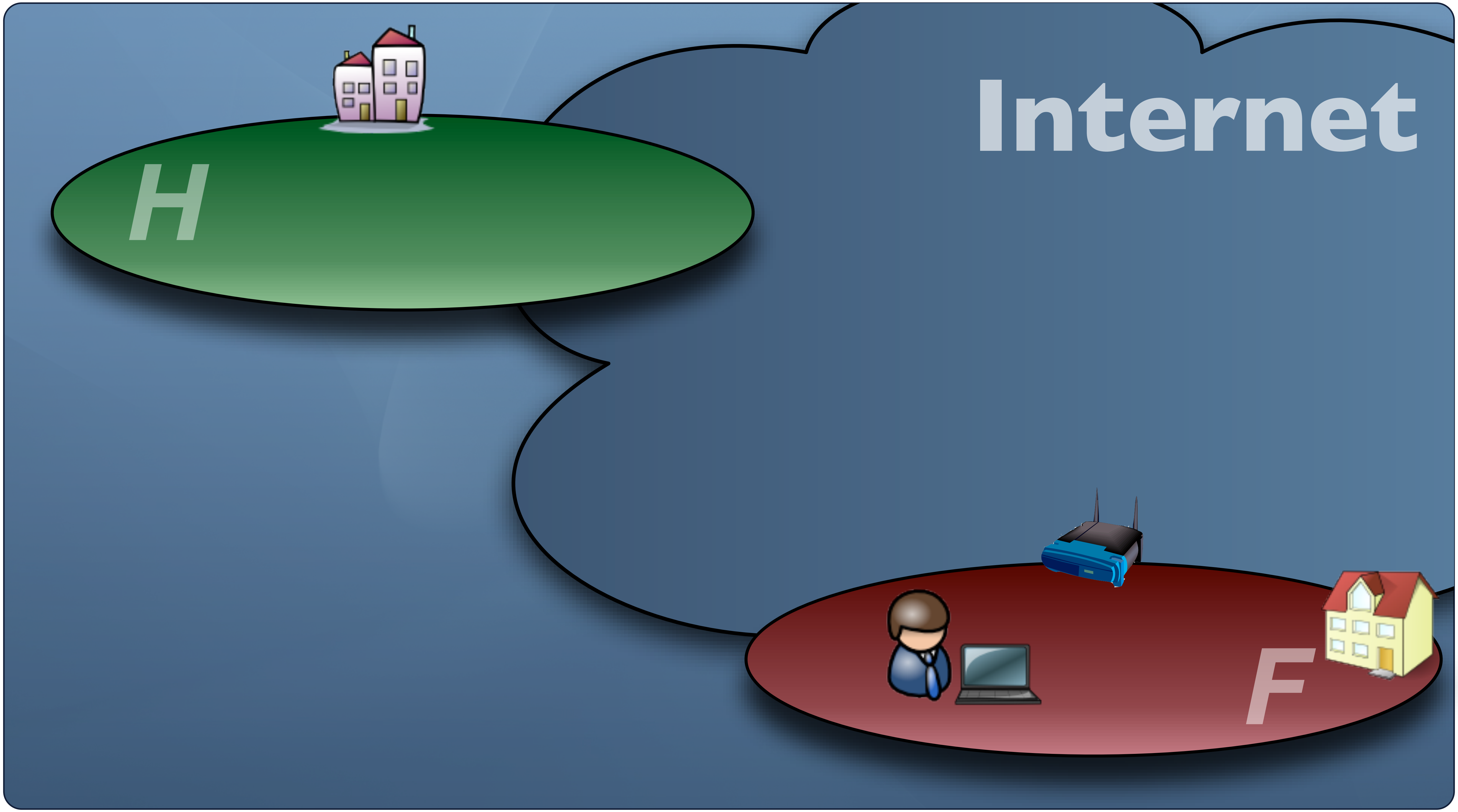
Content

Content

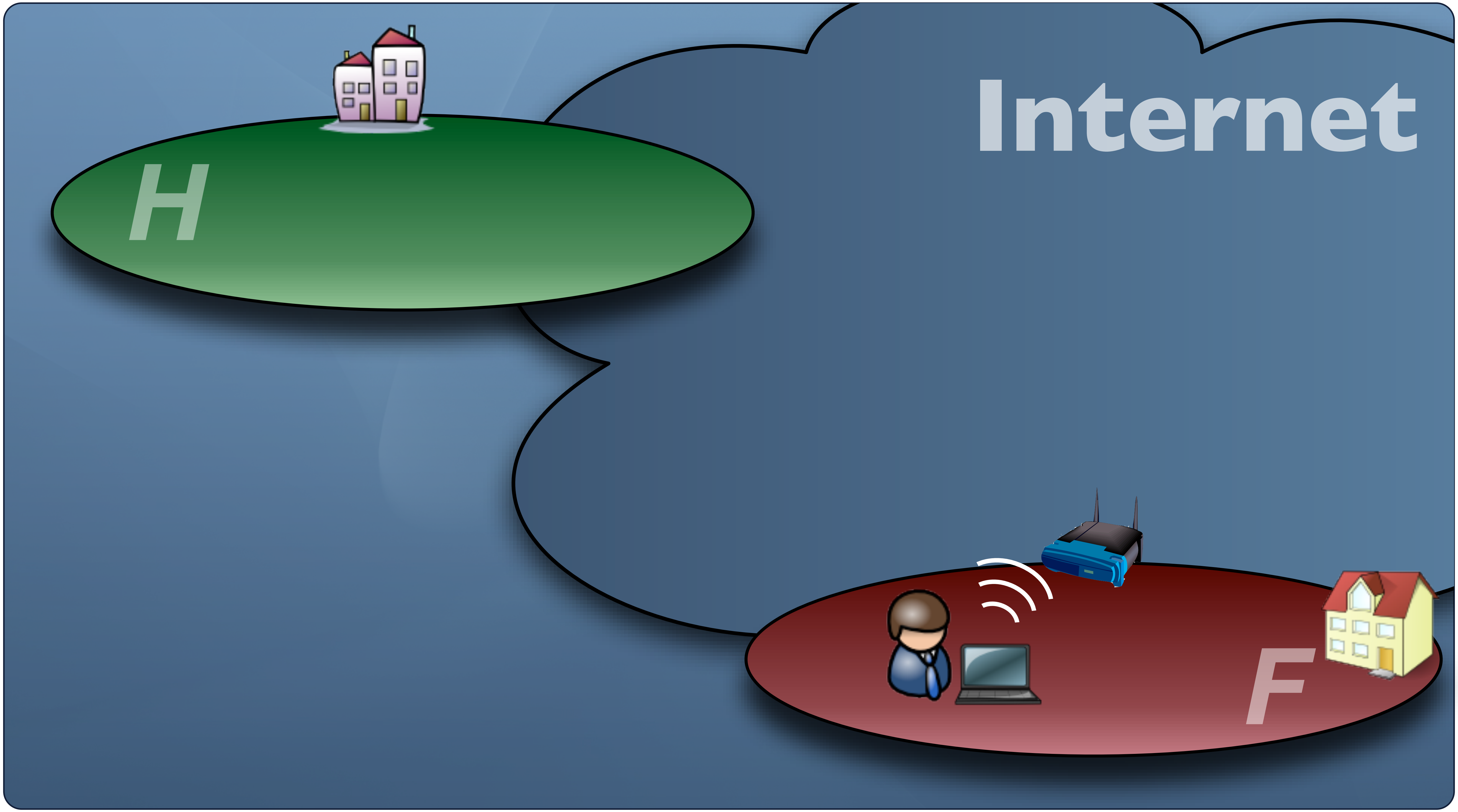
“WiFi Roaming”



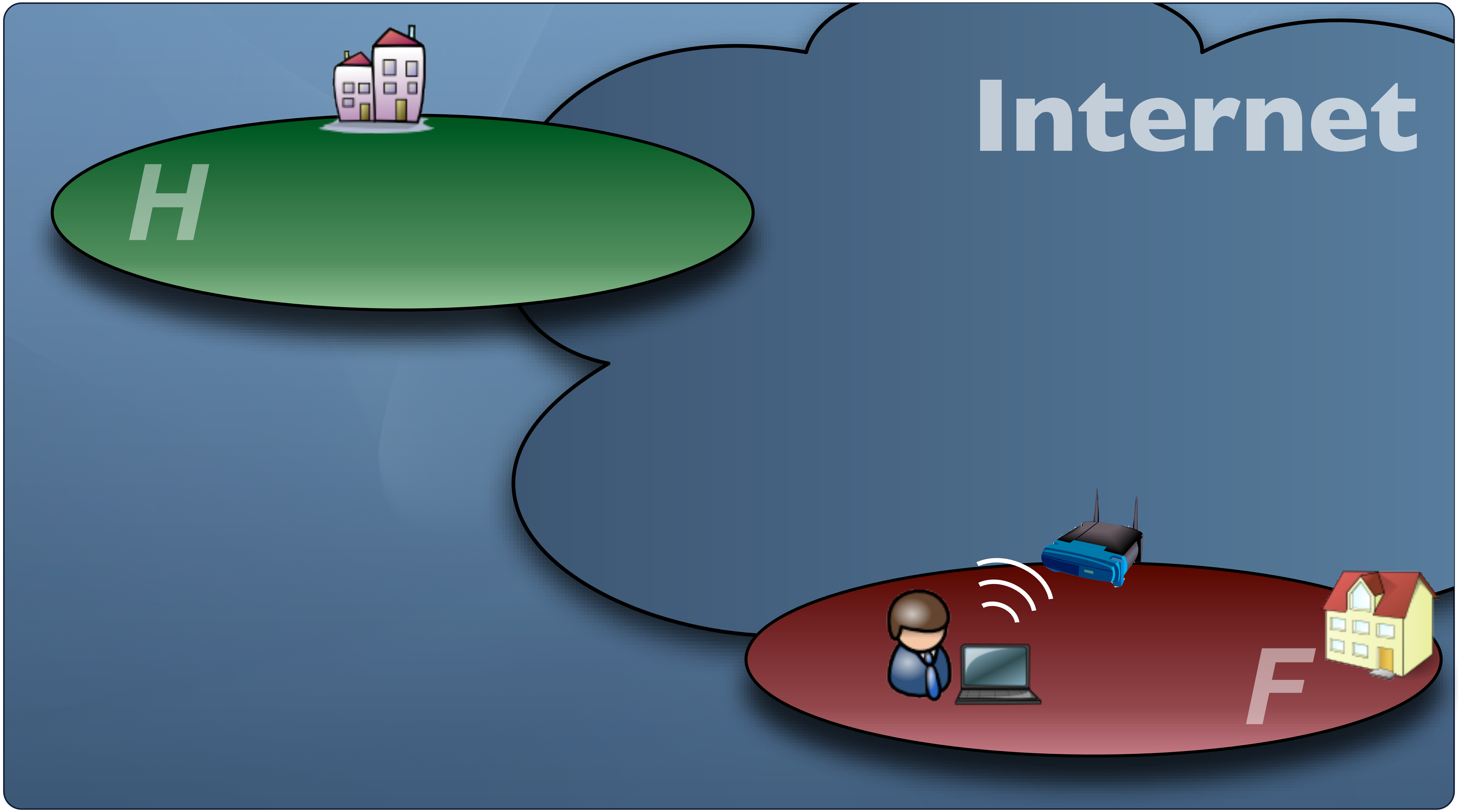
“WiFi Roaming”



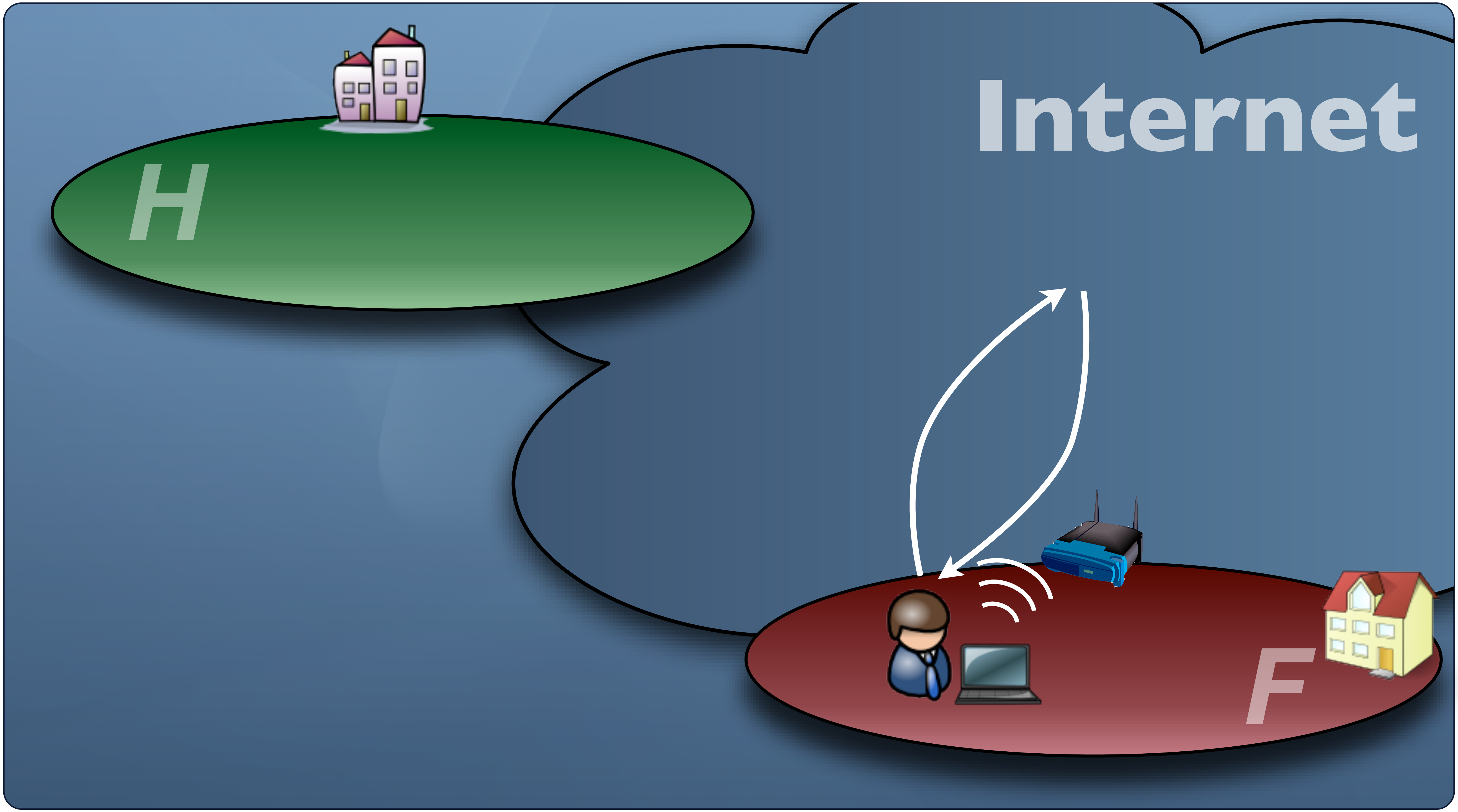
"WiFi Roaming"



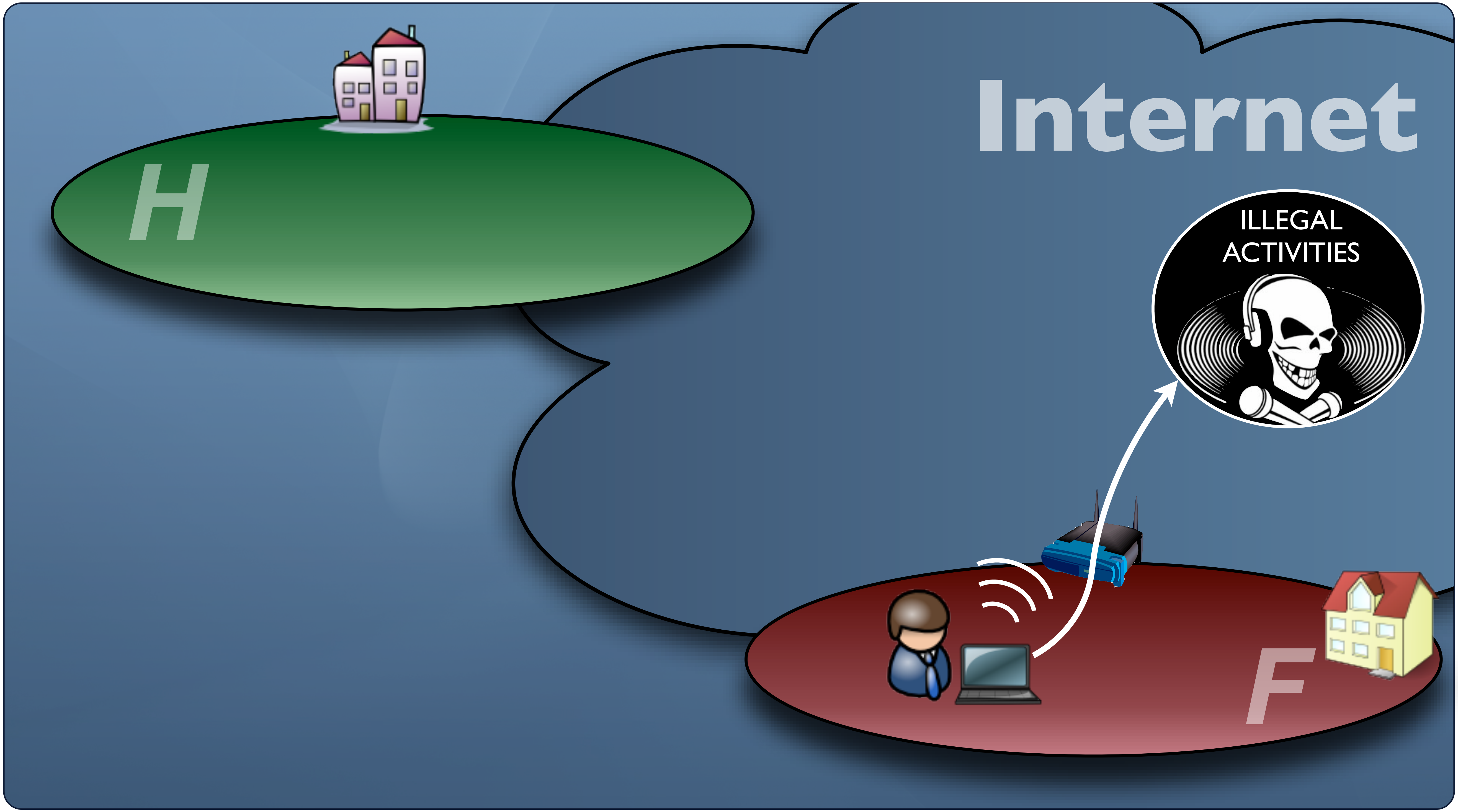
Scenario 1 : Open WiFi Access



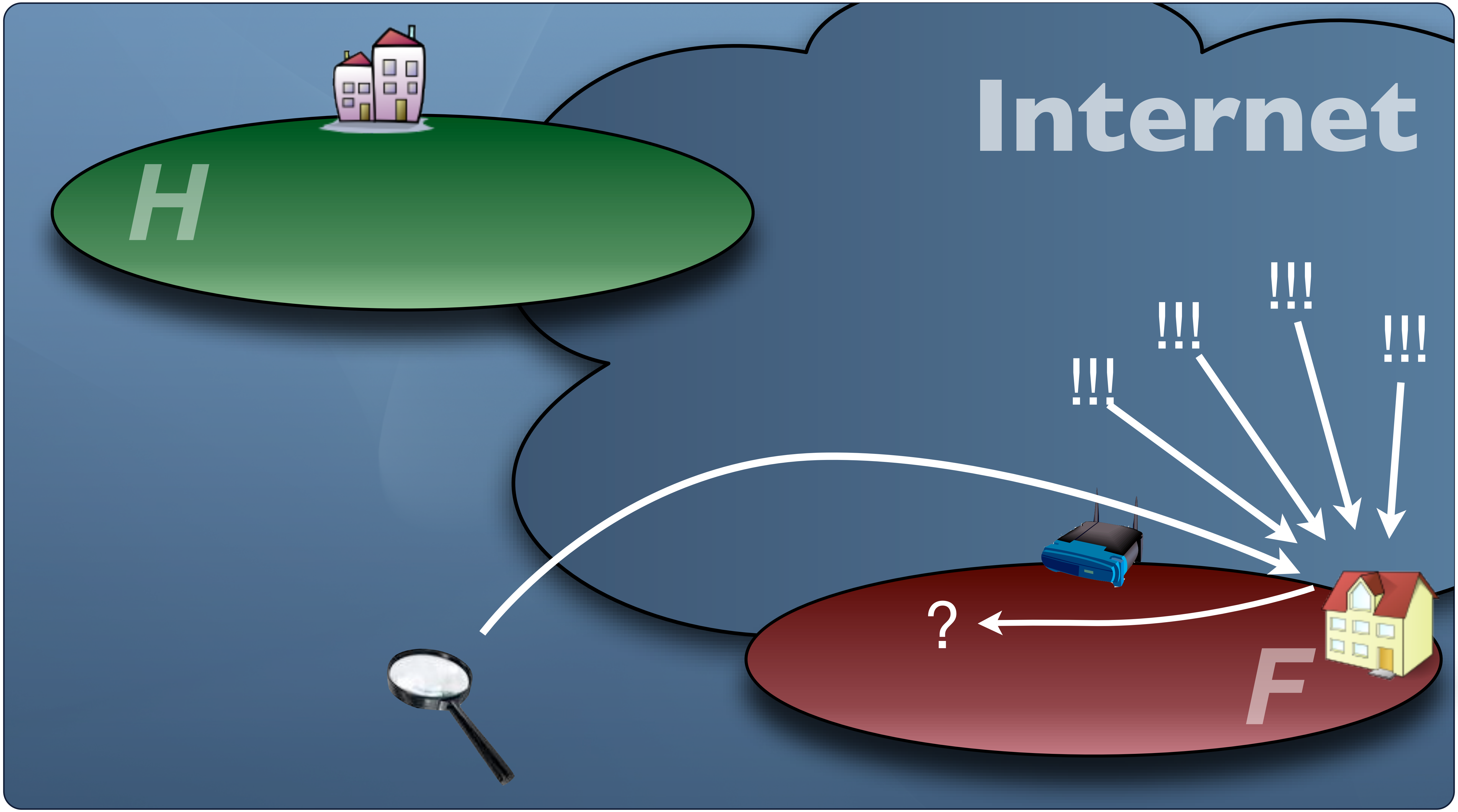
Scenario 1 : Open WiFi Access



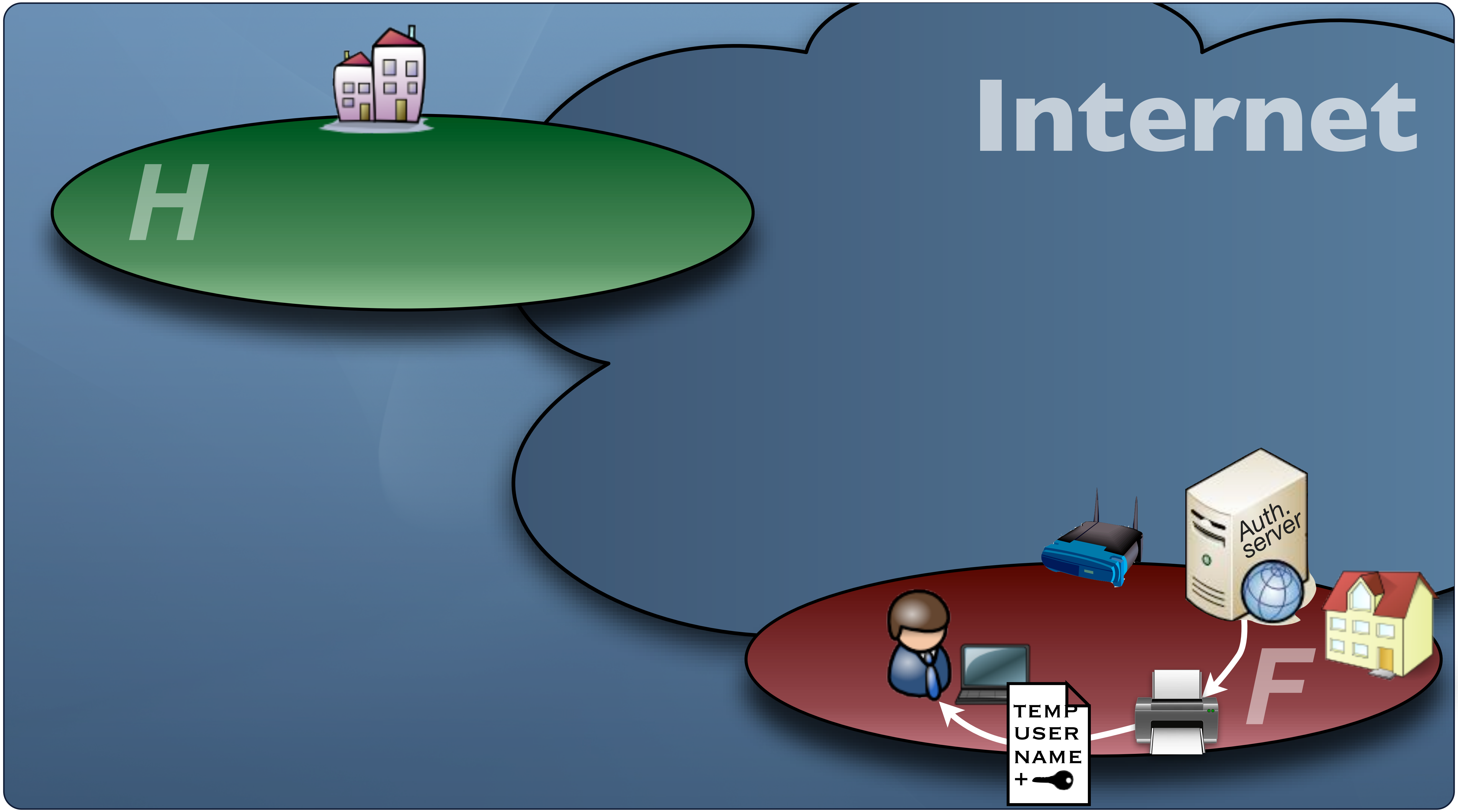
Scenario 1 : Open WiFi Access



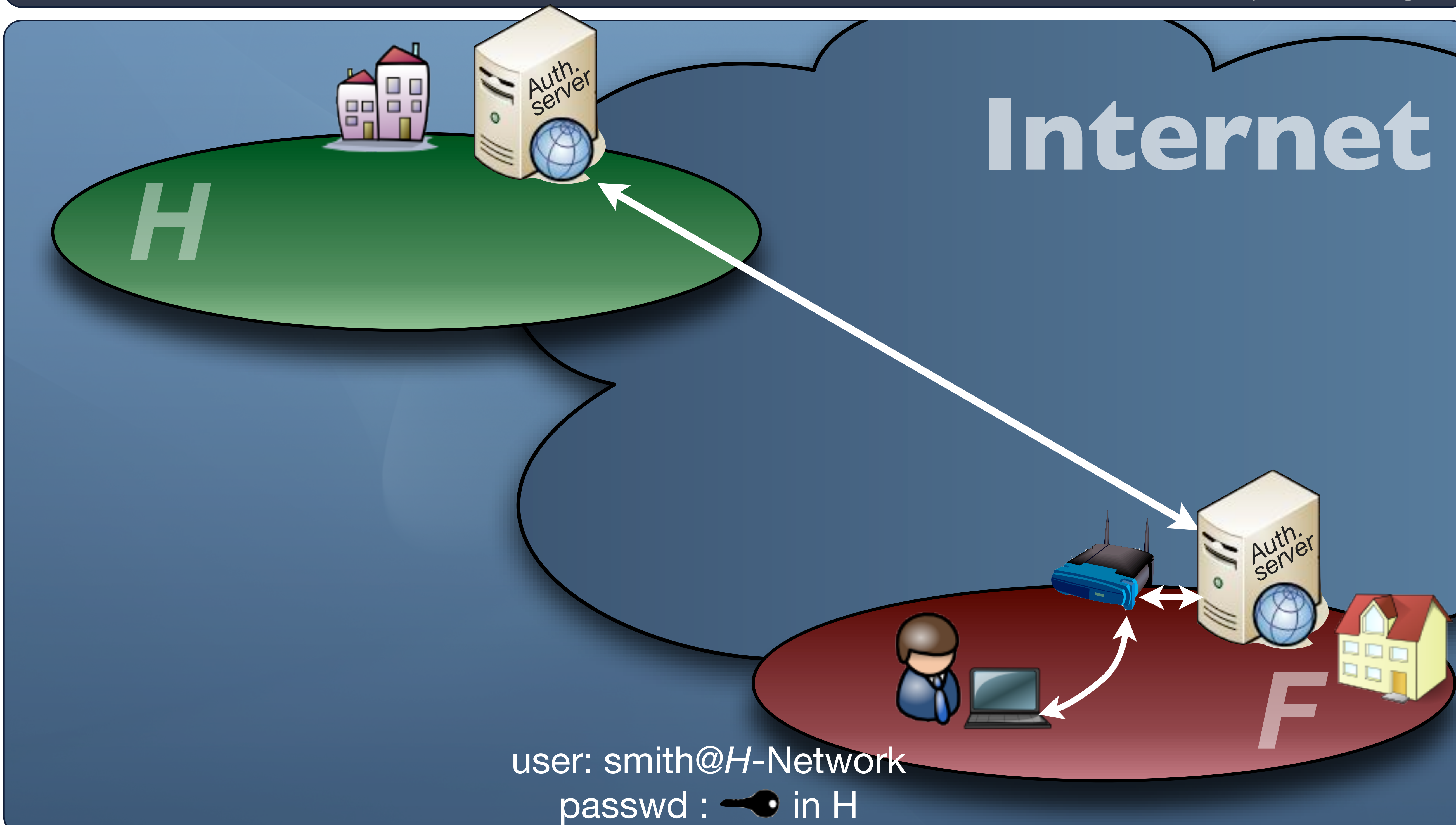
Scenario 1 : Open WiFi Access



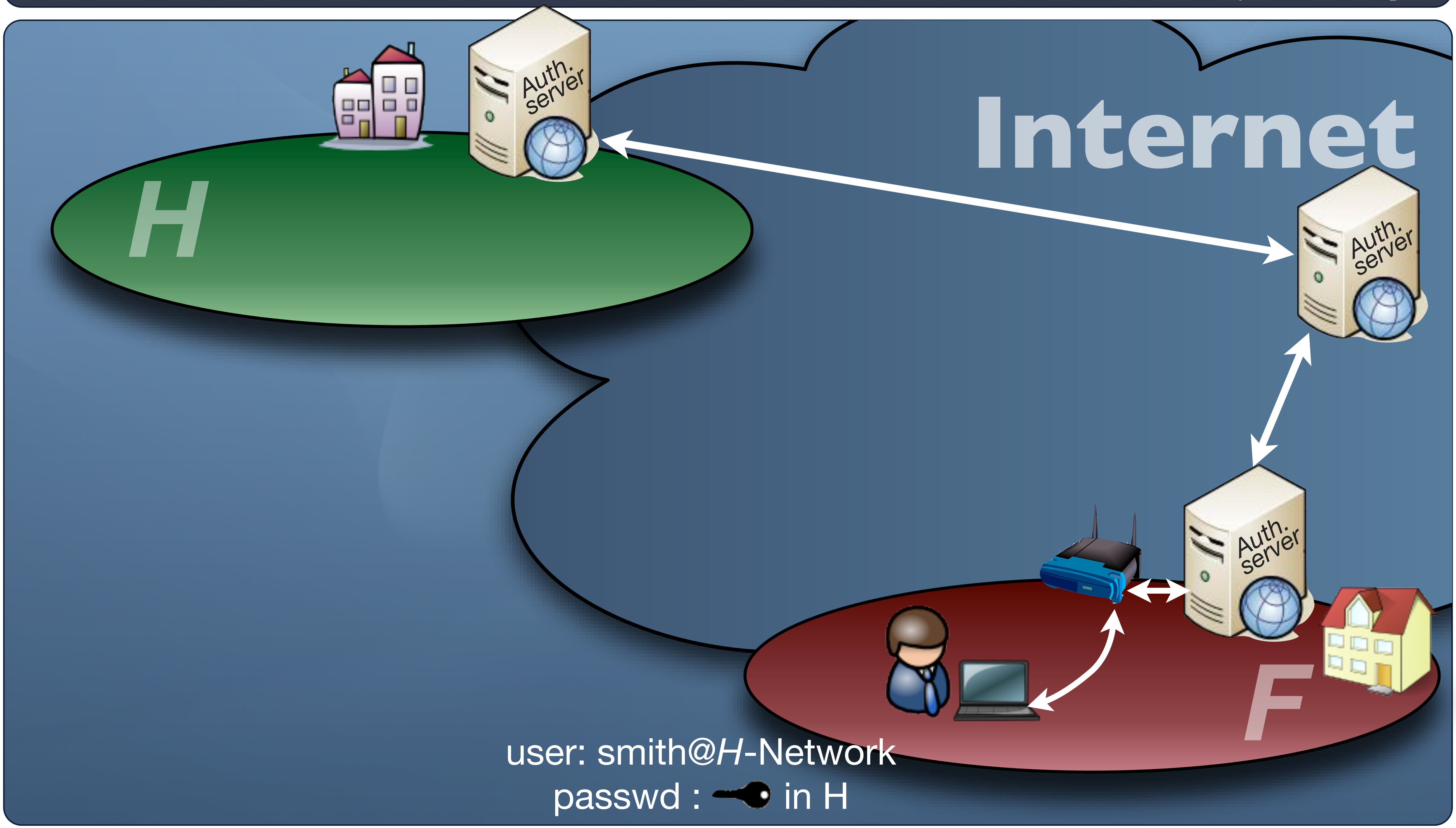
Scenario 2 : Temporary credentials



Scenario 3 : Remote authentication



Scenario 3 : Remote authentication



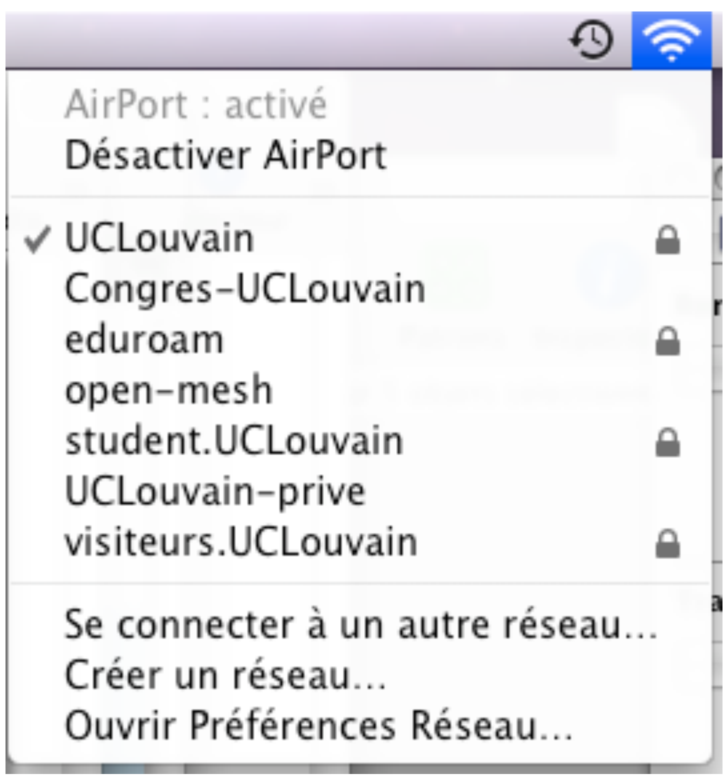
Content

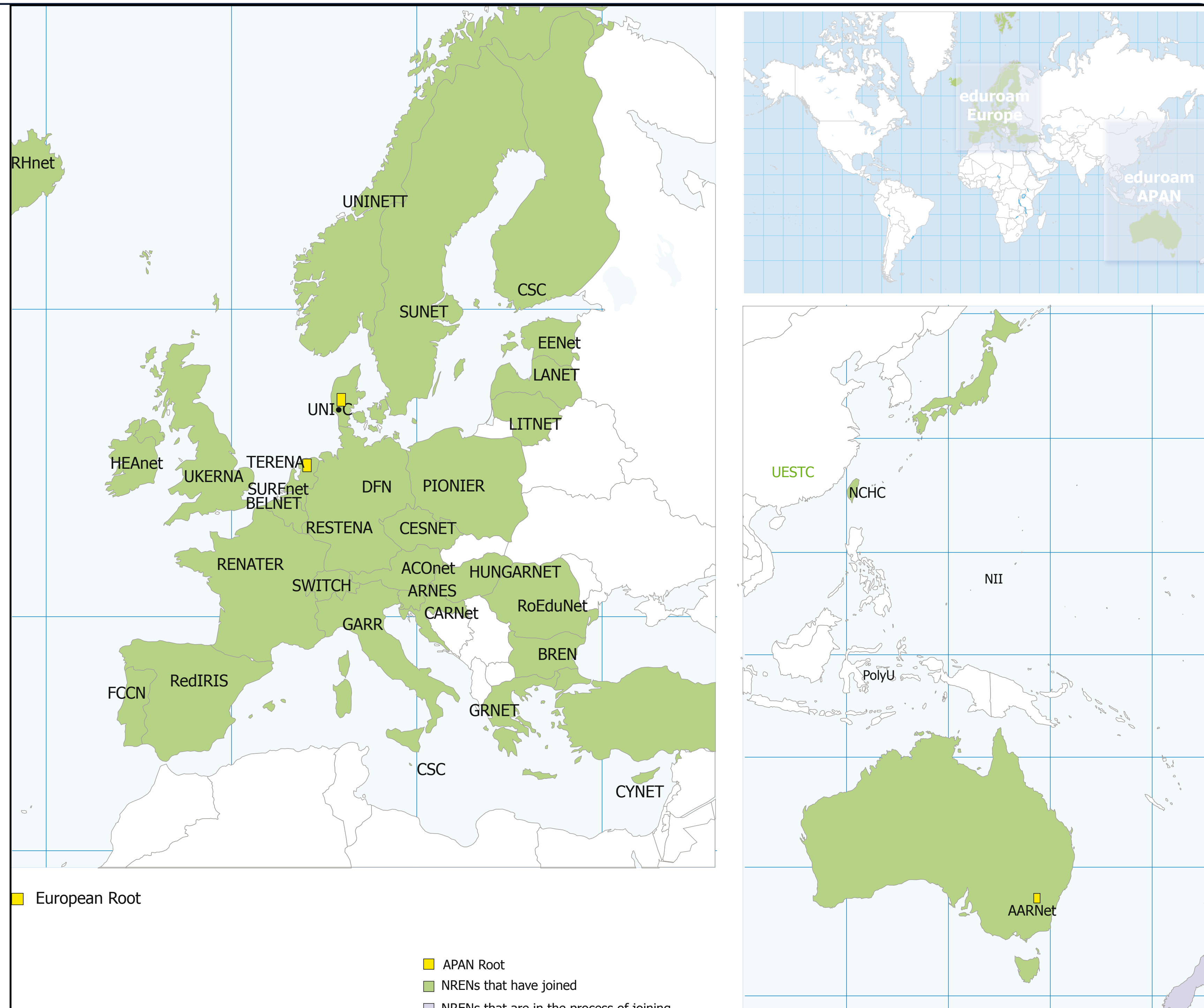
ip networking lab

The Eduroam Project

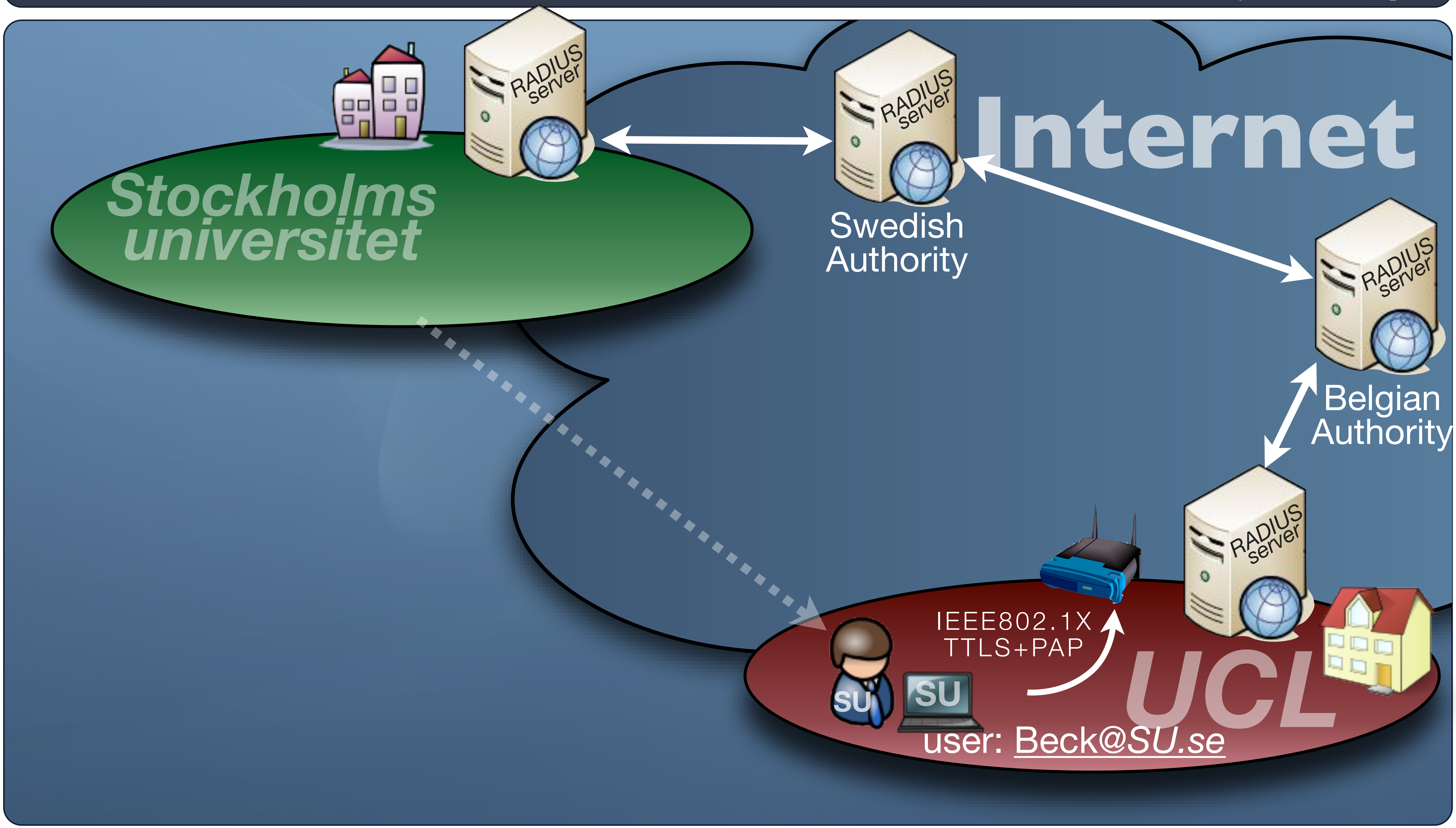
ip networking lab

eduroam

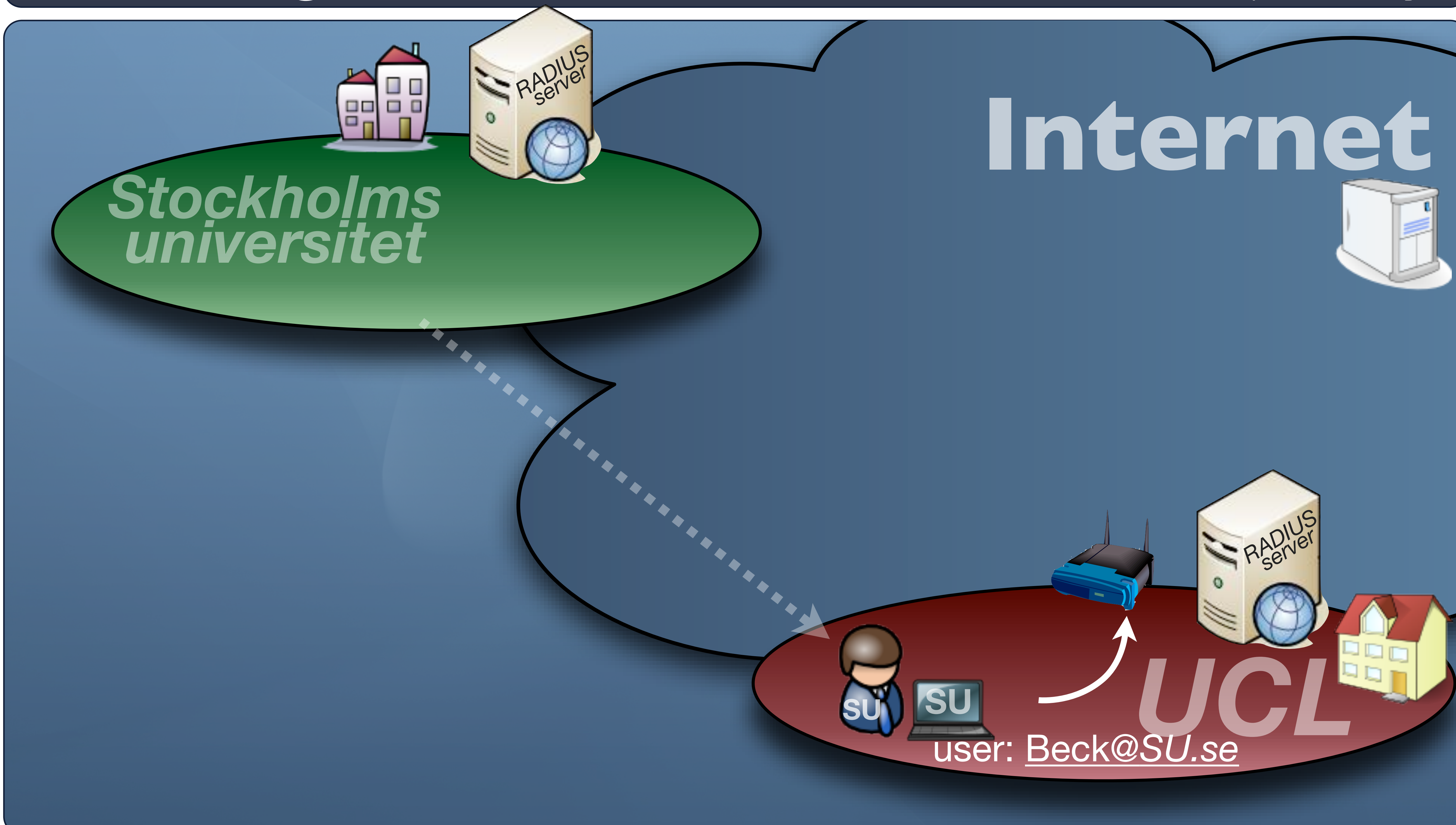




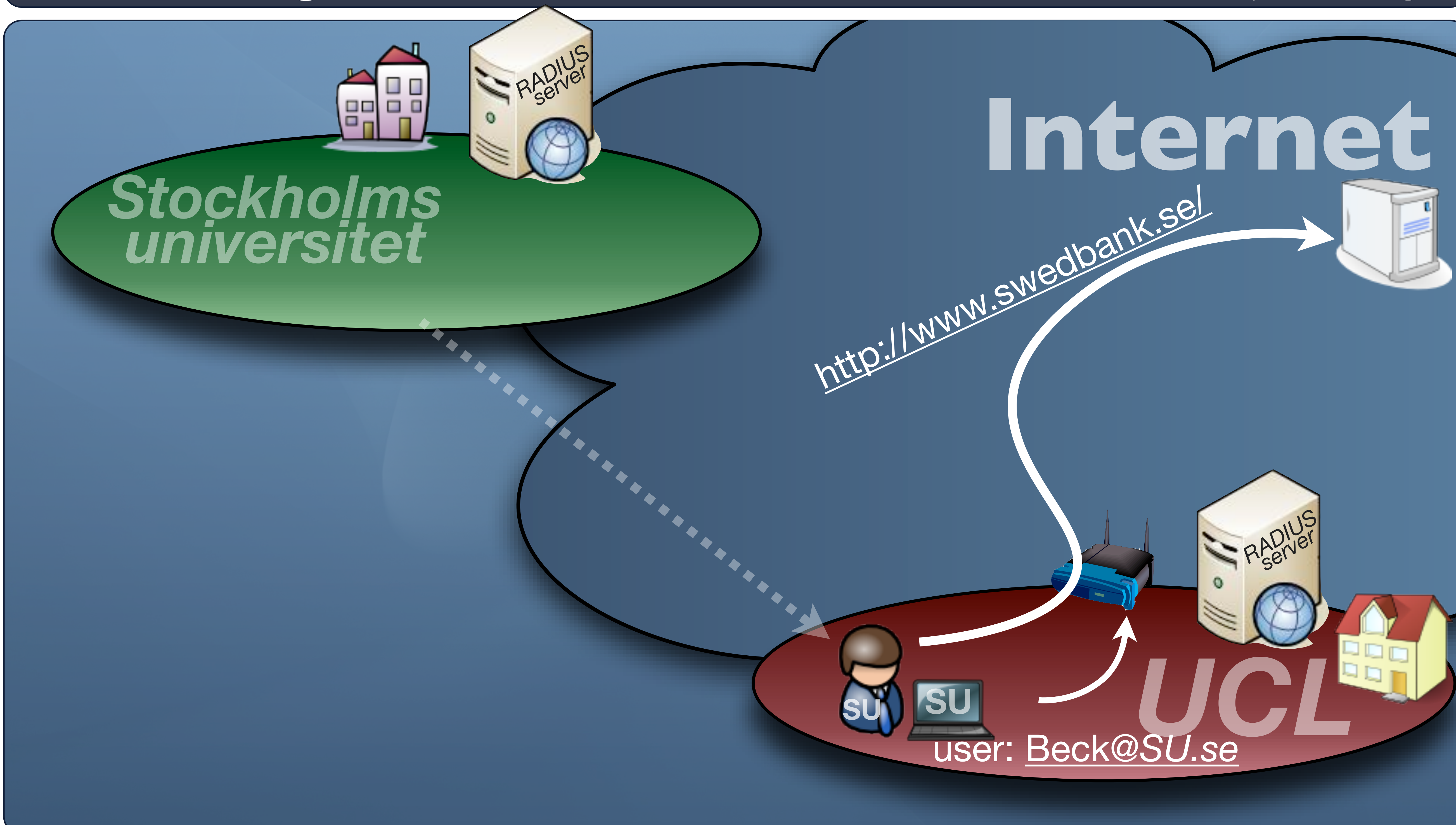
Authentication within Eduroam



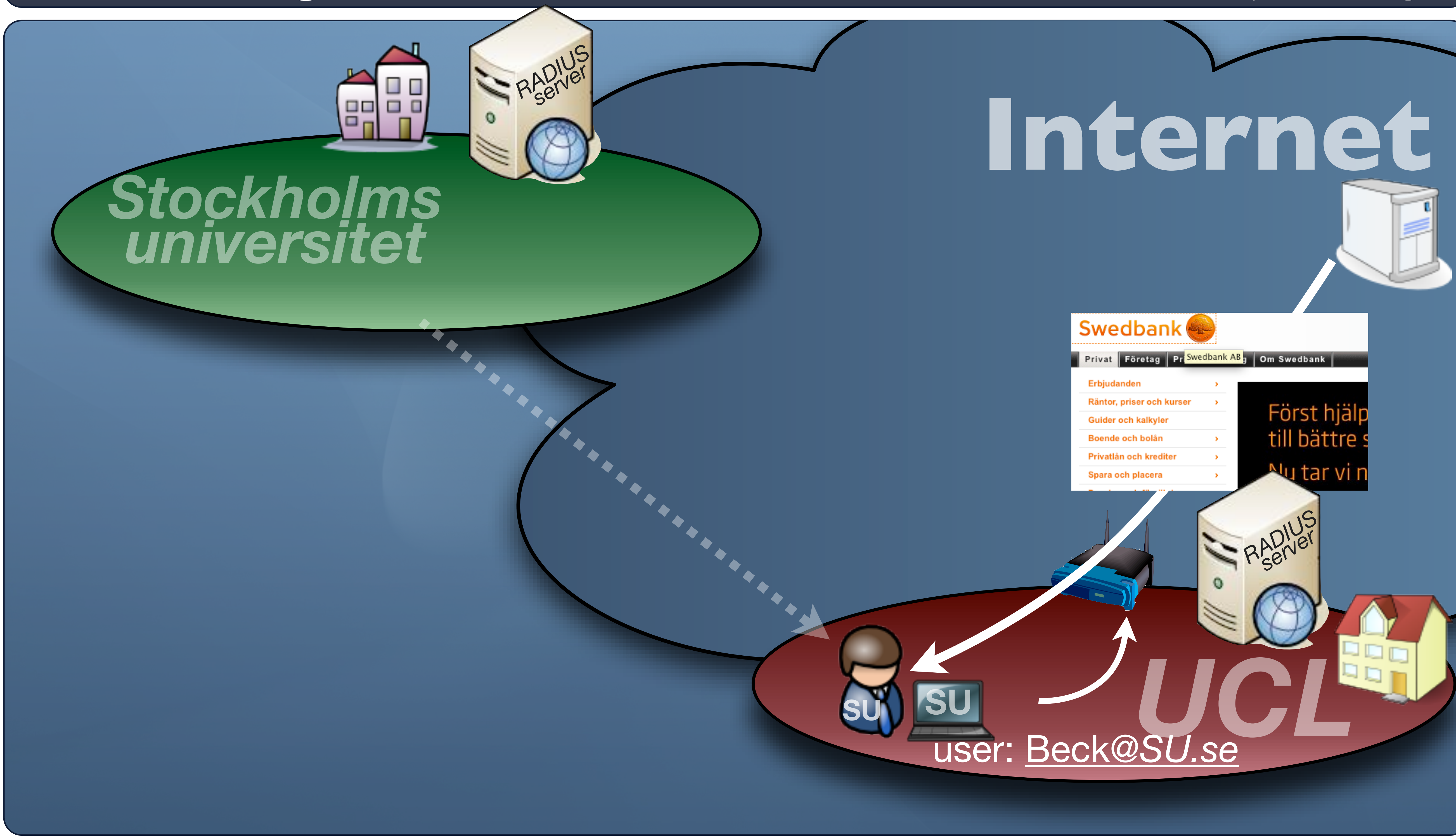
Roaming with Eduroam



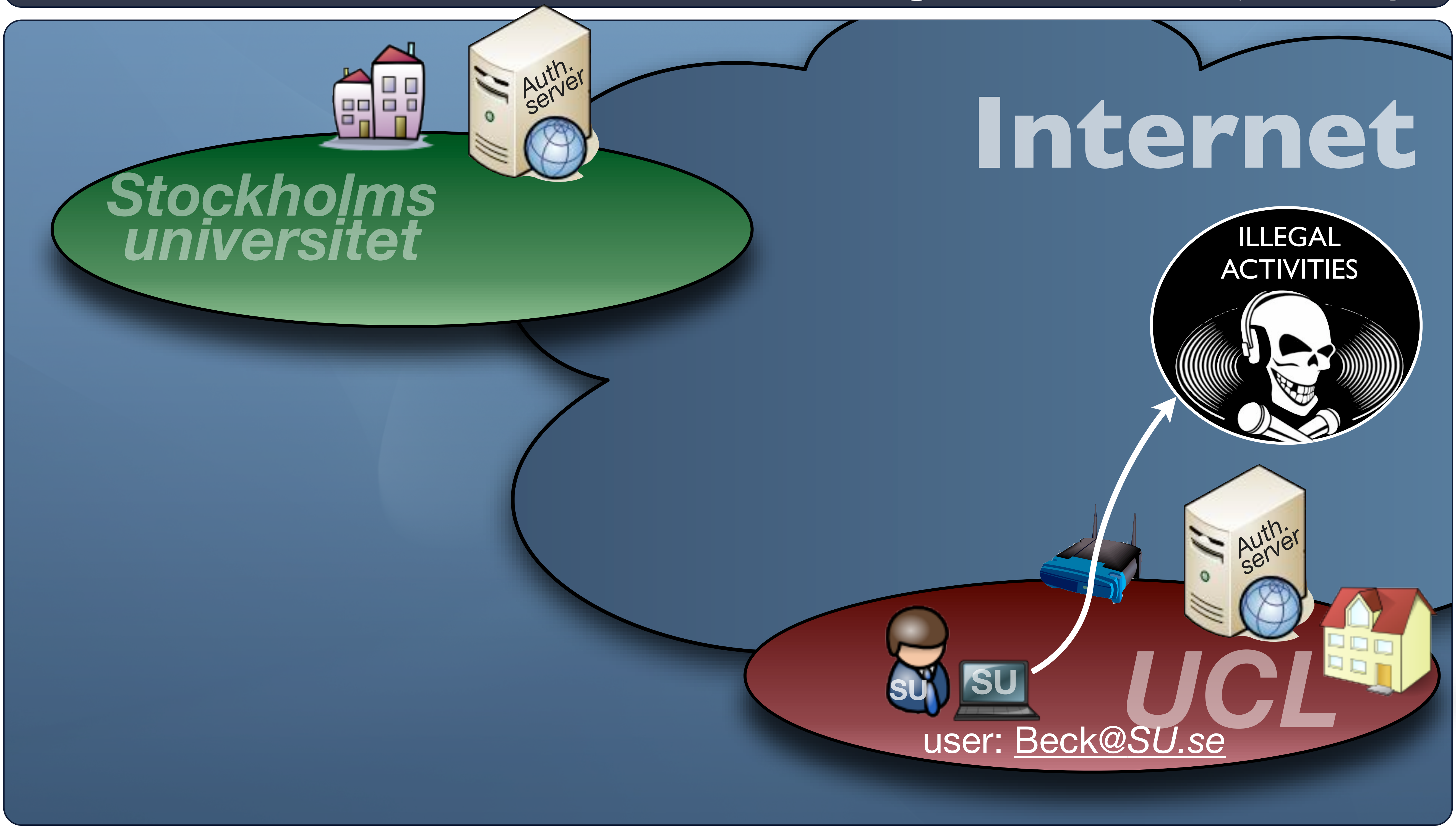
Roaming with Eduroam



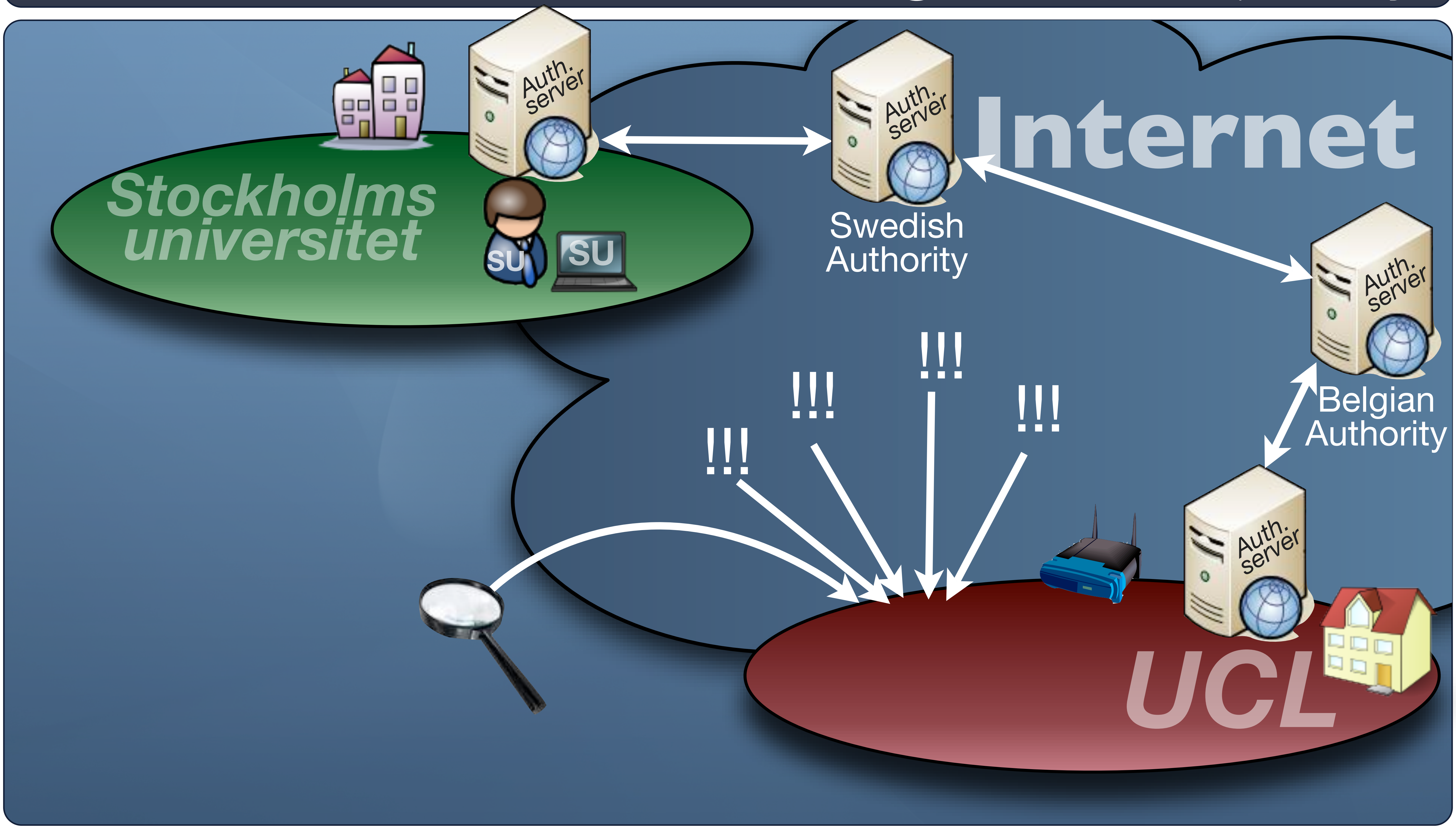
Roaming with Eduroam



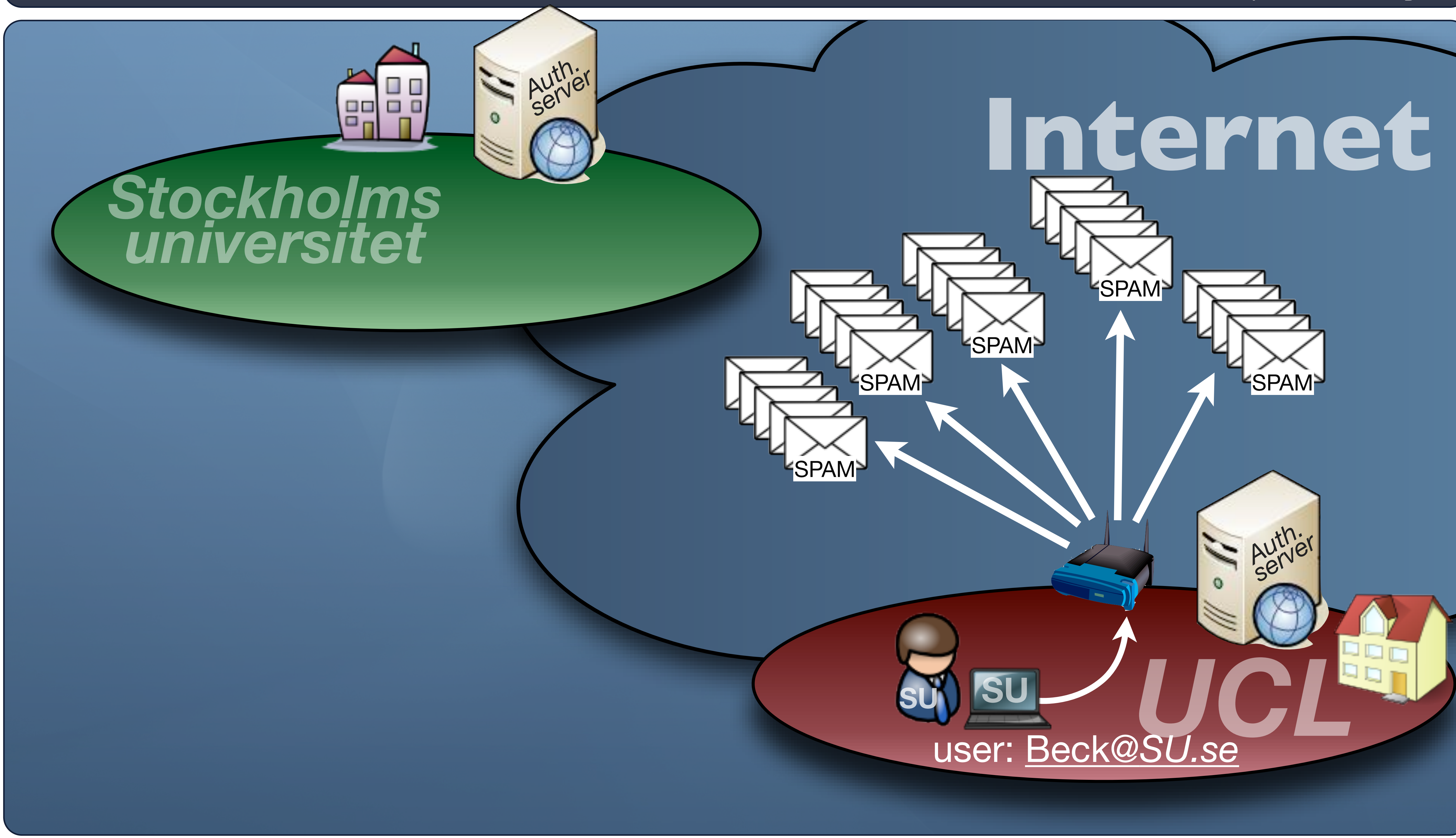
User abuse : Access to illegal data



User abuse : Access to illegal data



User abuse : Attack on the Internet



How do spam filters work ?

Score each mail based on :

- Content :
  "viagra", "diploma", "free videos", ...
- "Packaging" :
  Large images, lots of receivers, ...
- Well known spam-sender (often attacked hosts)
  Based on shared databases

How do spam filters work ?

ip networking lab

Score each mail based on :

- Content :
  "viagra", "diploma", "free videos", ...
- "Packaging" :
  Large images, lots of receivers, ...
- Well known spam-sender (often attacked hosts)
  Based on shared databases

high score -> mark as spam

How do spam filters work ?

Score each mail based on :

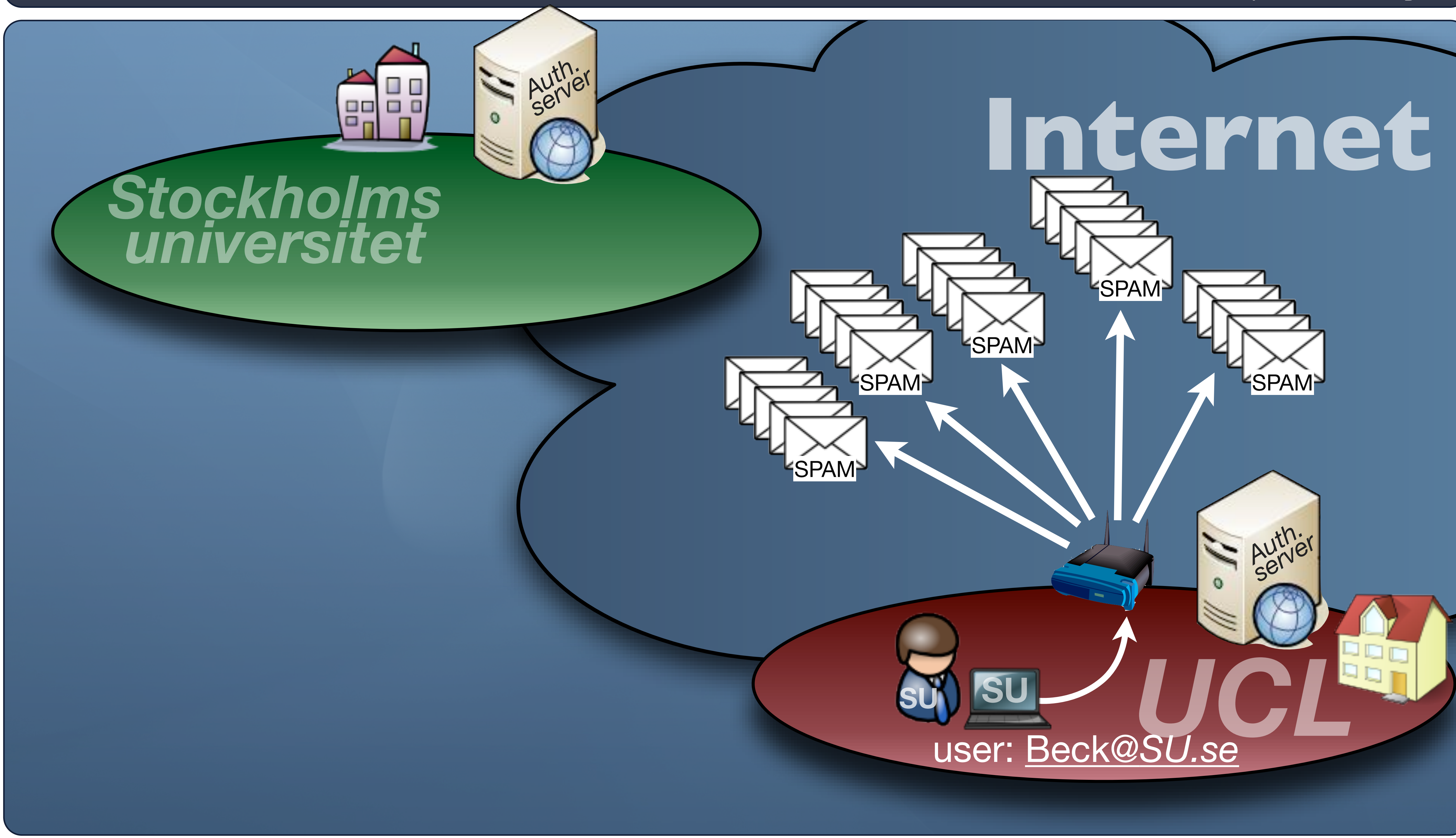
- Content :
  "viagra", "diploma", "free videos", ...
- "Packaging" :
  Large images, lots of receivers, ...
- Well known spam-sender (often attacked hosts)
  Based on shared databases

high score -> mark as spam

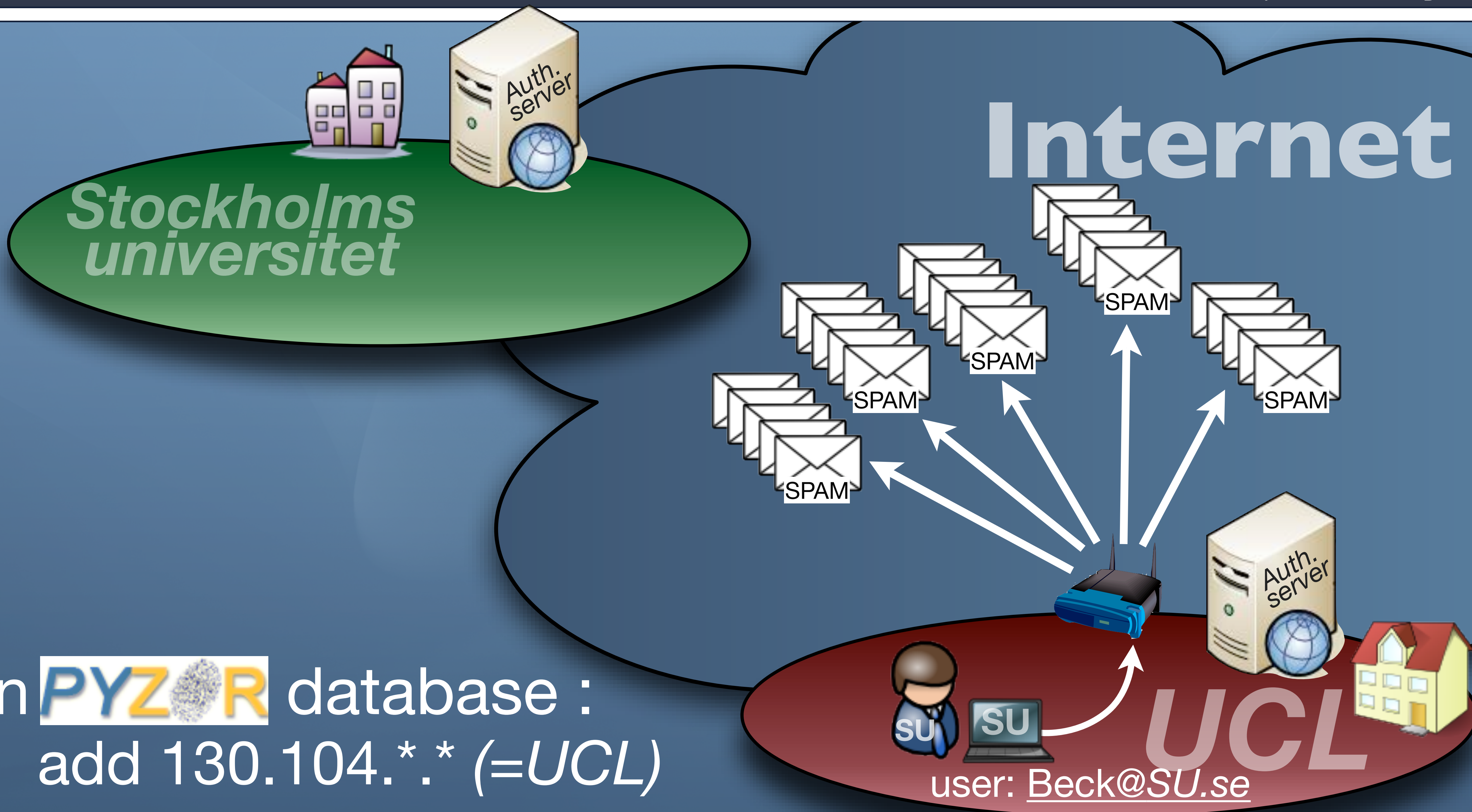
How are these databases built up?

- Based on previous “mass spam” activities
- Based on IP addresses of senders
- Open databases

User abuse : Attack on the Internet

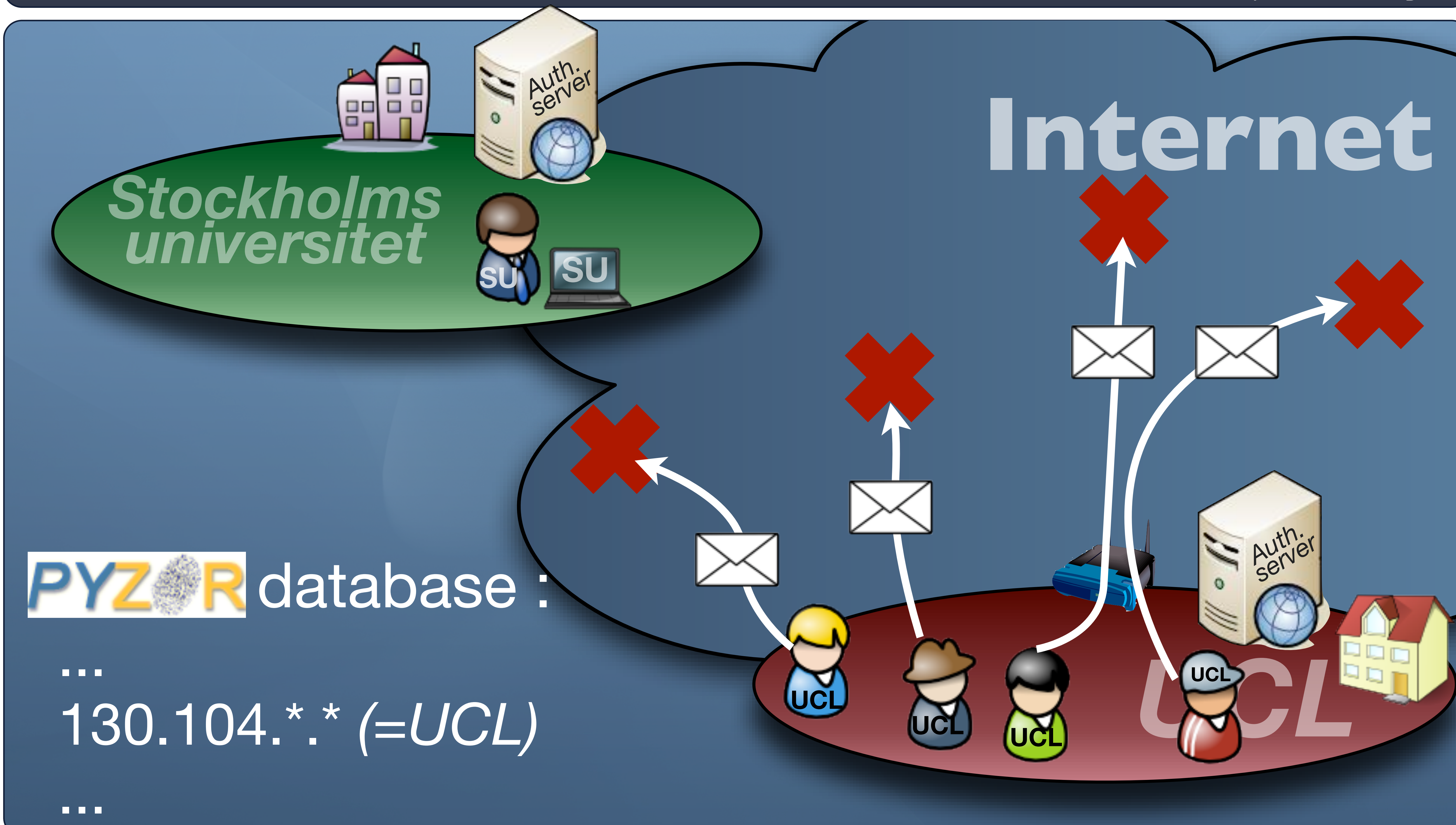


User abuse : Attack on the Internet



In PYZOR database :
add 130.104.*.* *(=UCL)*

User abuse : Attack on the Internet



PYZOR database :

...

130.104.*.* *(=UCL)*

...

Access control based on IP

- Some services (e.g., website) have their access control based on source IP.
  - Digital libraries
  - Intranet
  - ...
- The mobile user will have access to these services ! (more complex filtering could be added)

Security risks for visited network

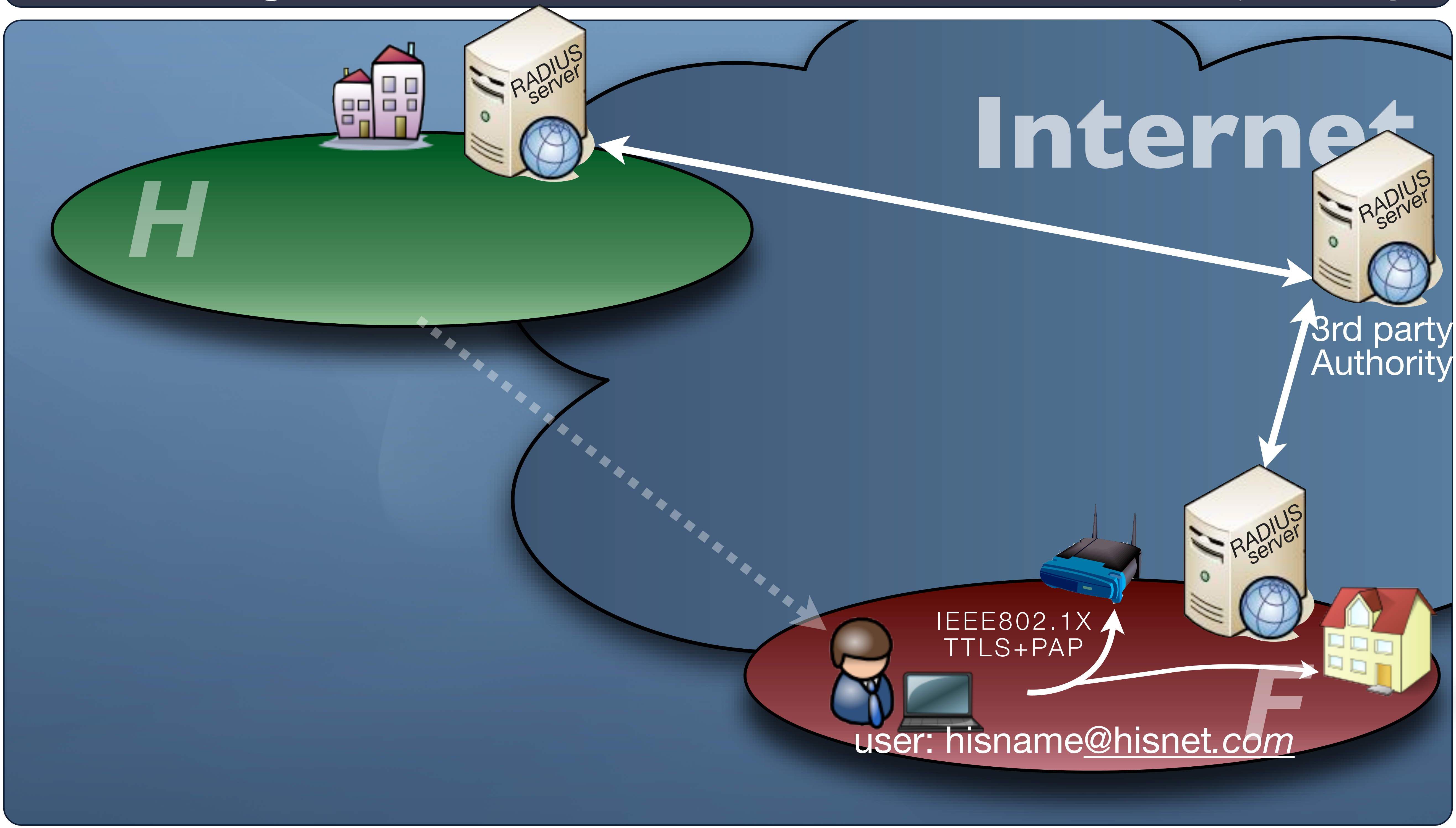
ip networking lab

Summary

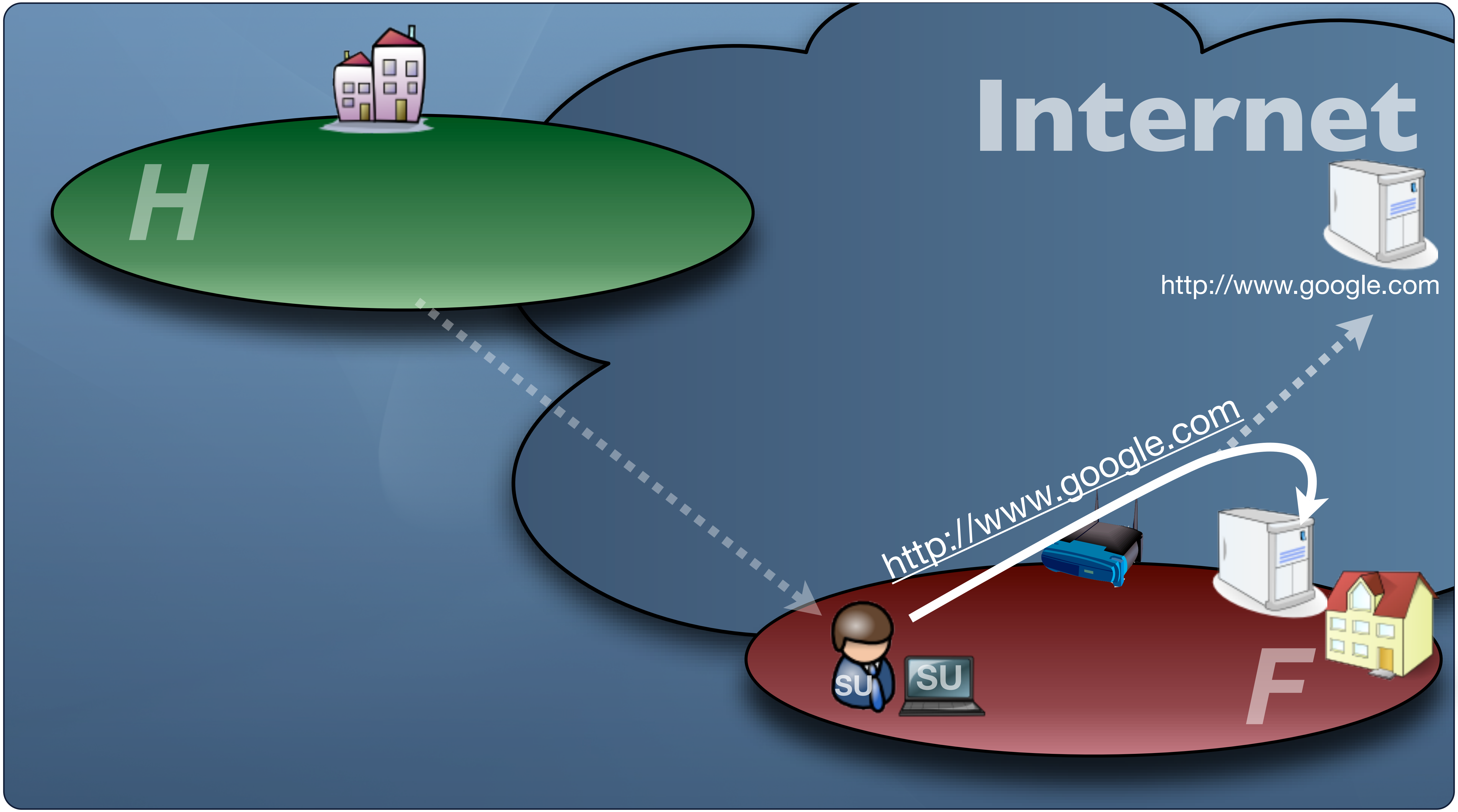
	Open WiFi	Temp. cred.	Remote auth.
User authentication	✗	⚠	✓
Administrative cost	✓	✗	✓
Ease of use (for user)	✓	✗	✓
Blacklisting based on IP	✗	✗	✗
Access based on IP	✗	✗	✗
Attack on the infrastruct.	✗	✗	✗

Content

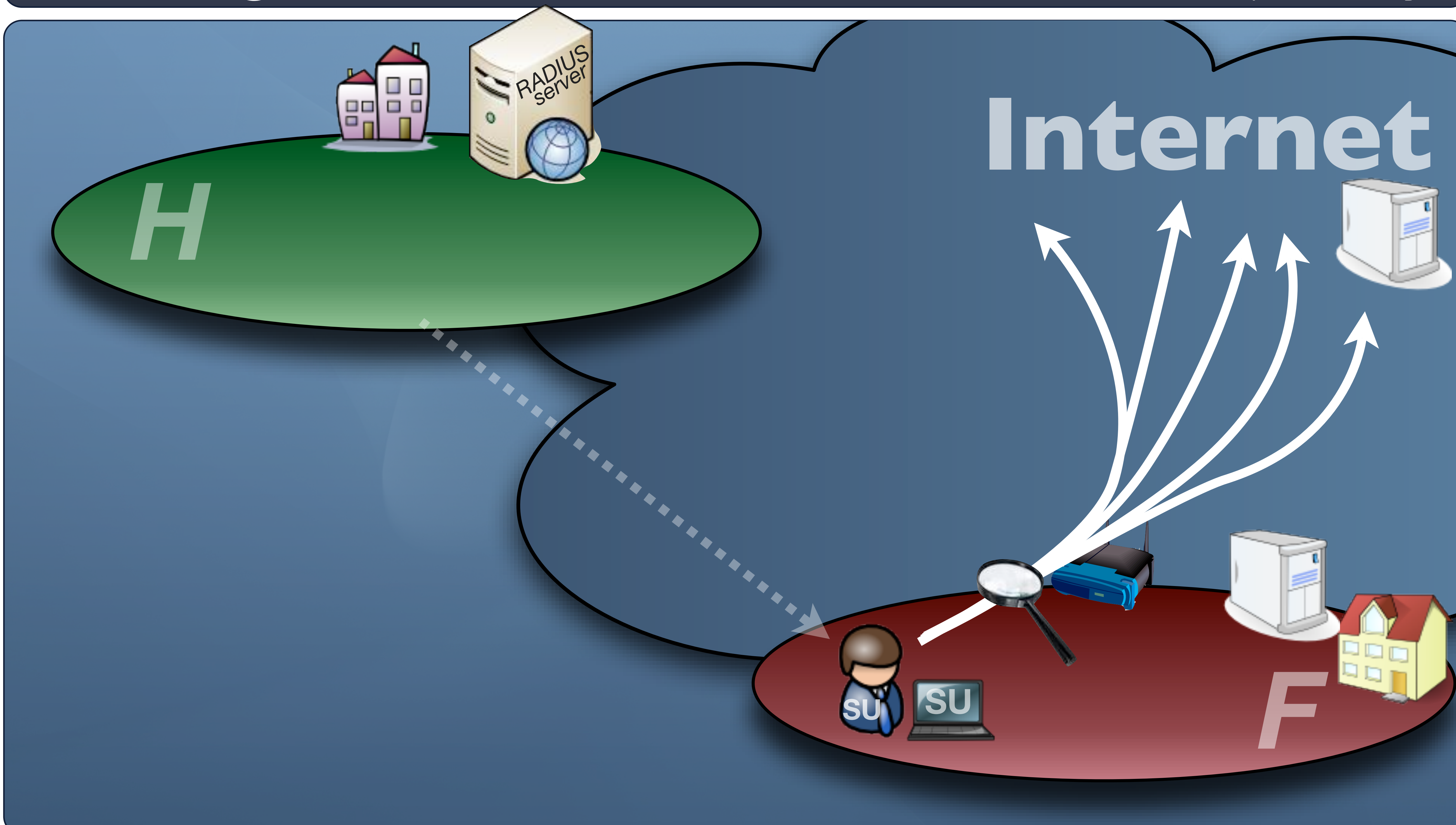
Stealing credentials



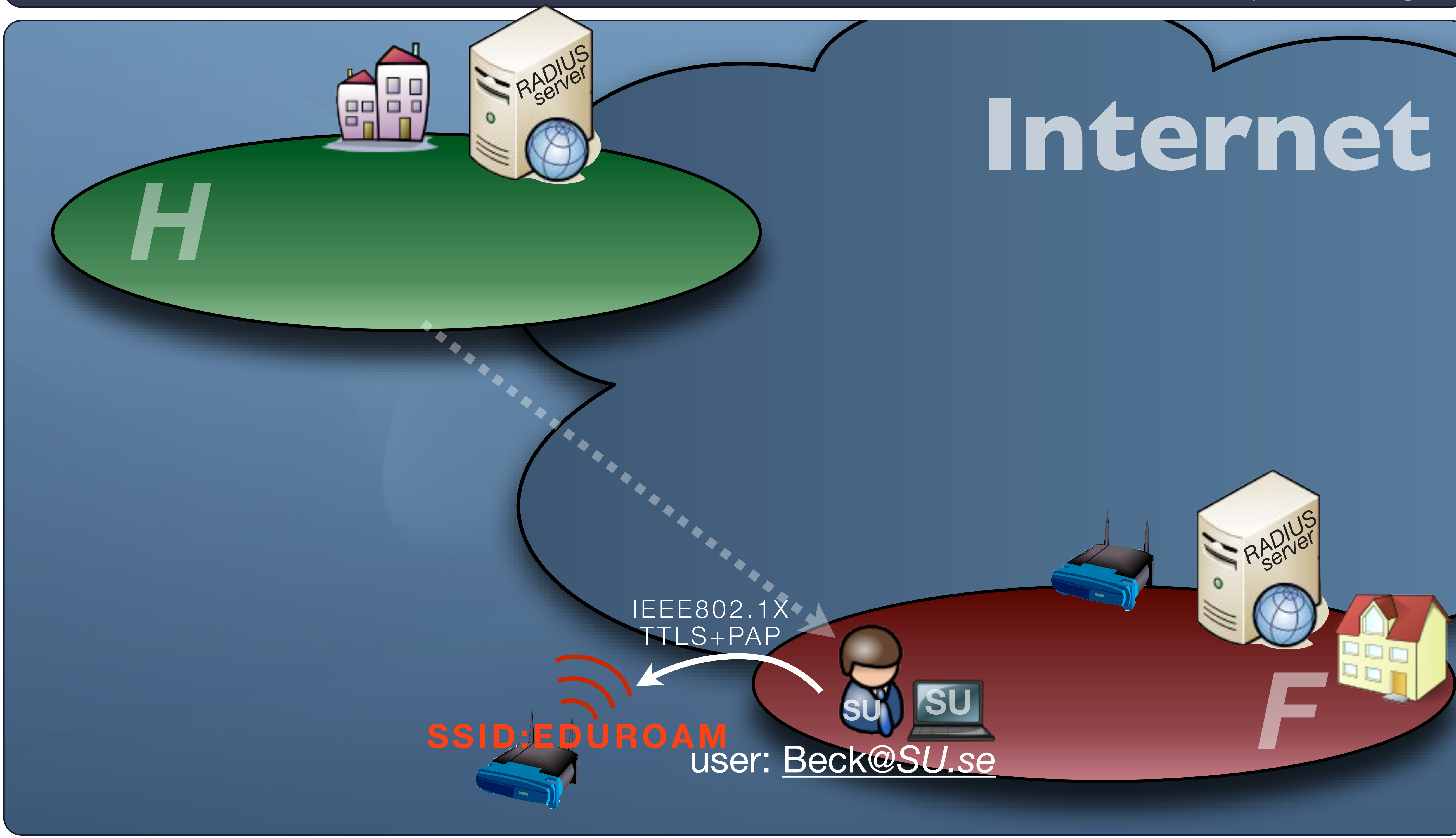
Pharming



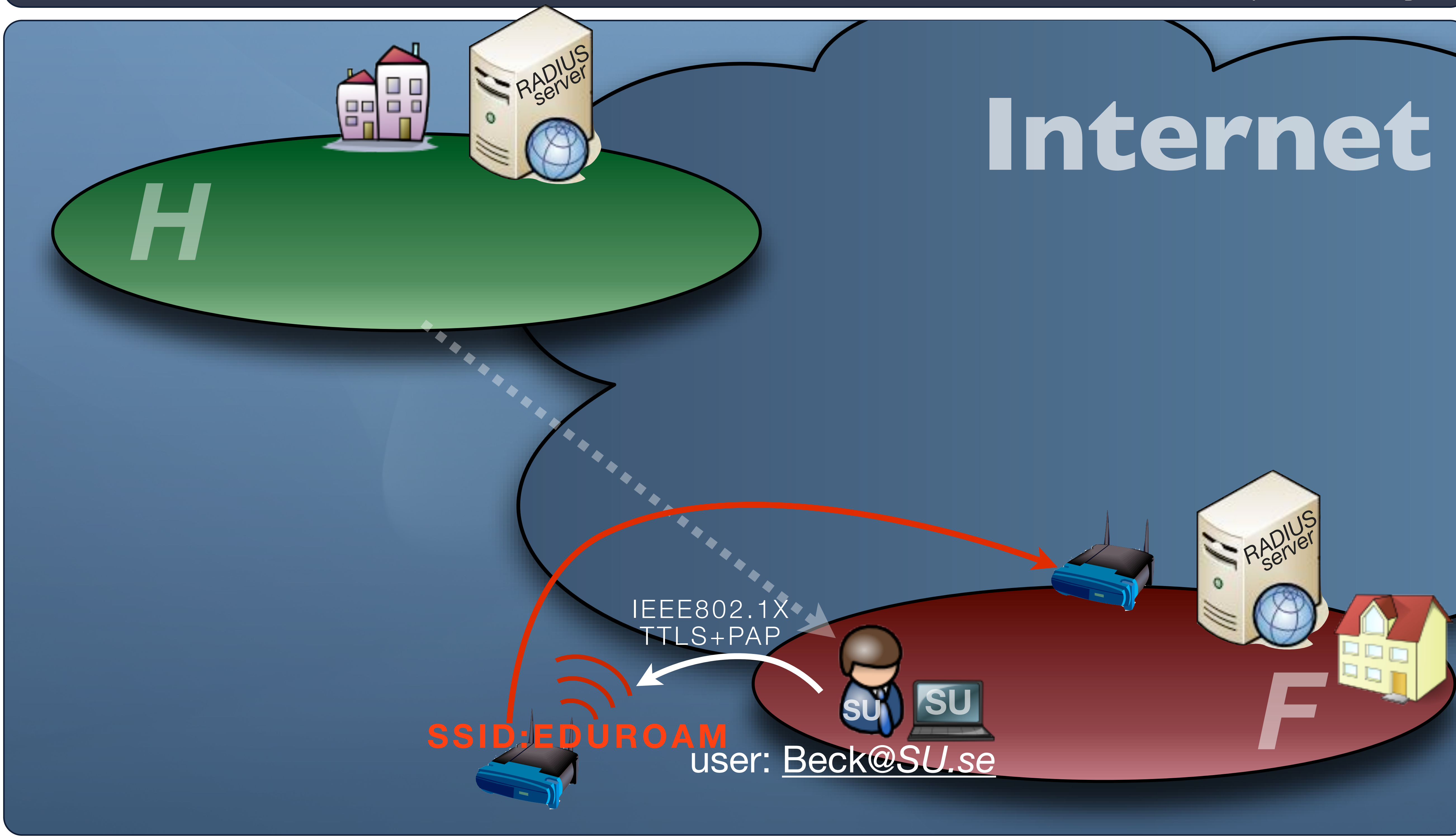
Sniffing



Fake Access Point

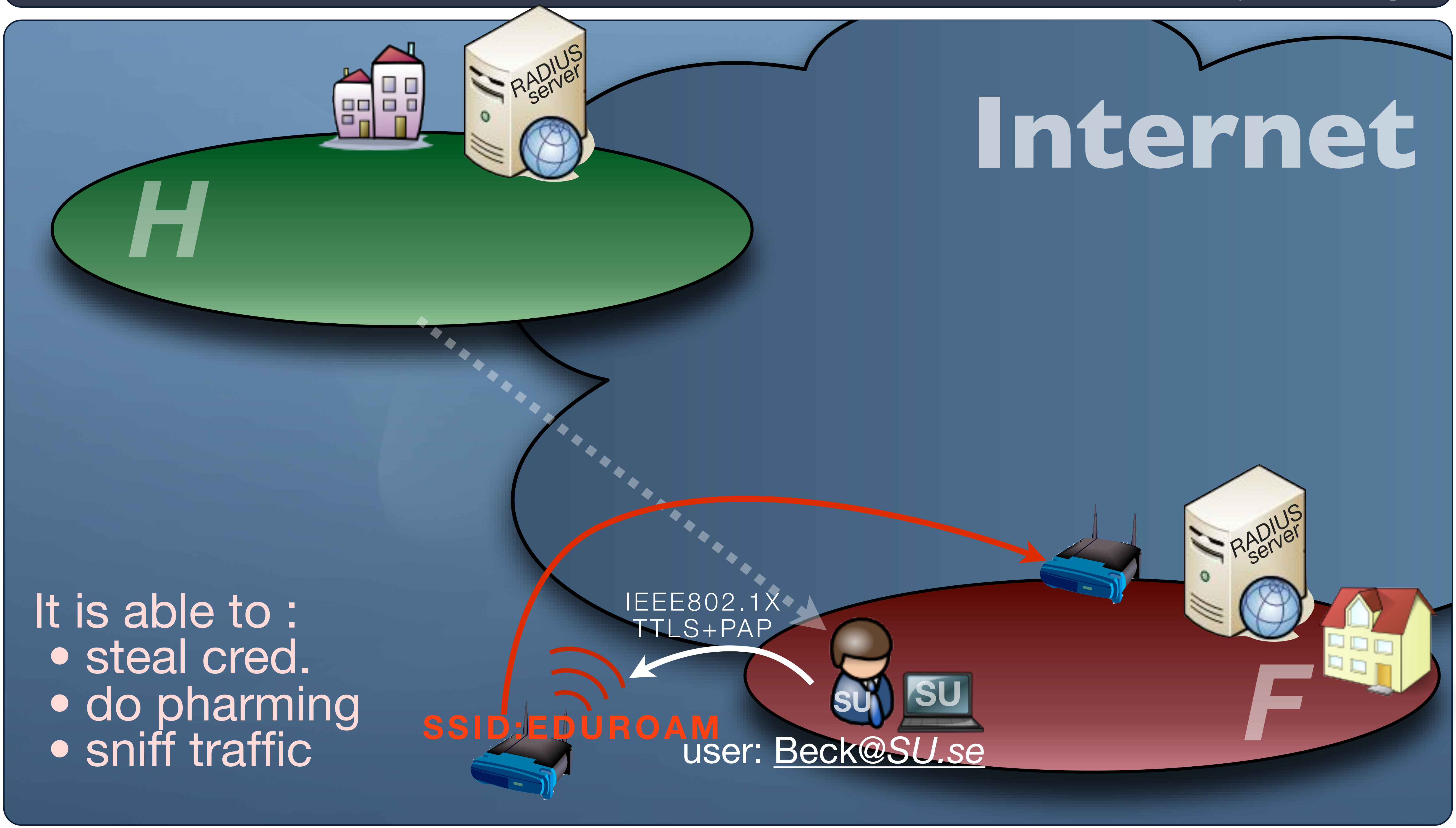


Fake Access Point



Fake Access Point

ip networking lab



It is able to :
- steal cred.
- do pharming
- sniff traffic

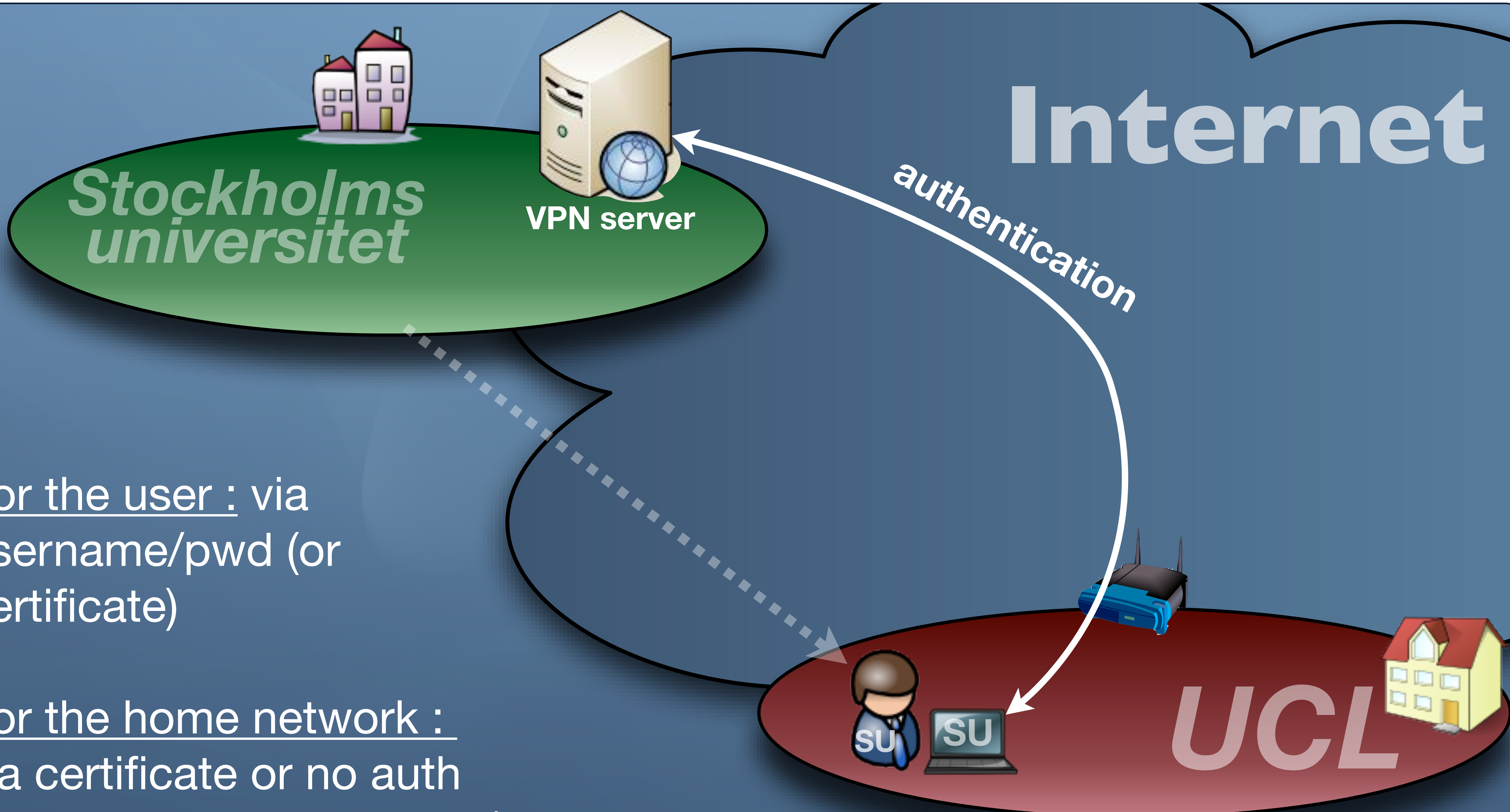
Security risks for F and M

ip networking lab

	Open WiFi	Temp. cred.	Remote auth.
User authentication	✗	⚠	✓
Administrative cost for F	✓	✗	✓
Ease of use (for user)	✓	✗	✓
Blacklisting based on IP	✗	✗	✗
Access based on IP	✗	✗	✗
Attack on the infrastruct.	✗	✗	✗
F malicious	✗	✗	✗
Fake access point	✗	✗	⚠

Content

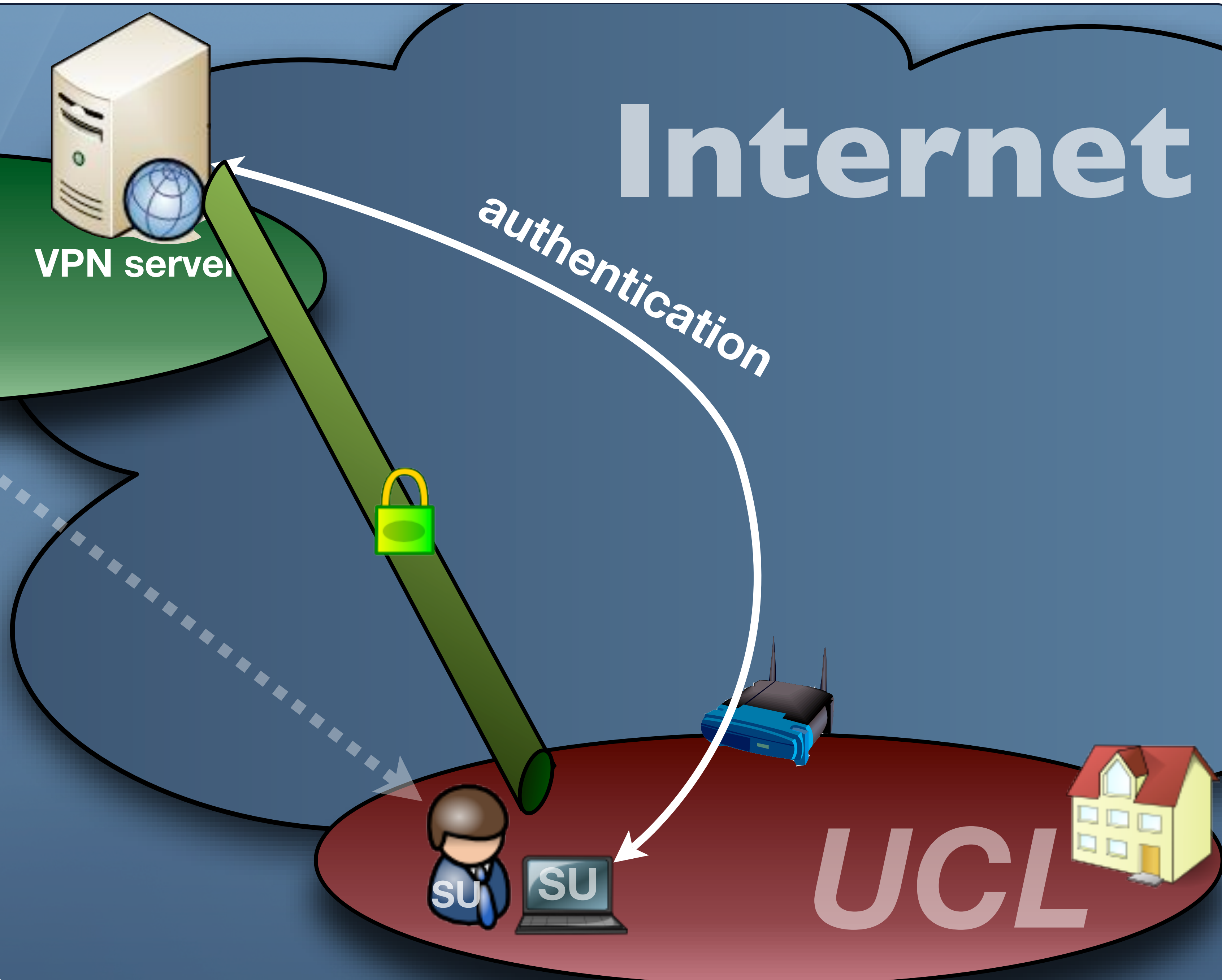
VPN



<ins>For the user :</ins> via username/pwd (or certificate)

<ins>For the home network :</ins> via certificate or no auth (cert must be distributed !)

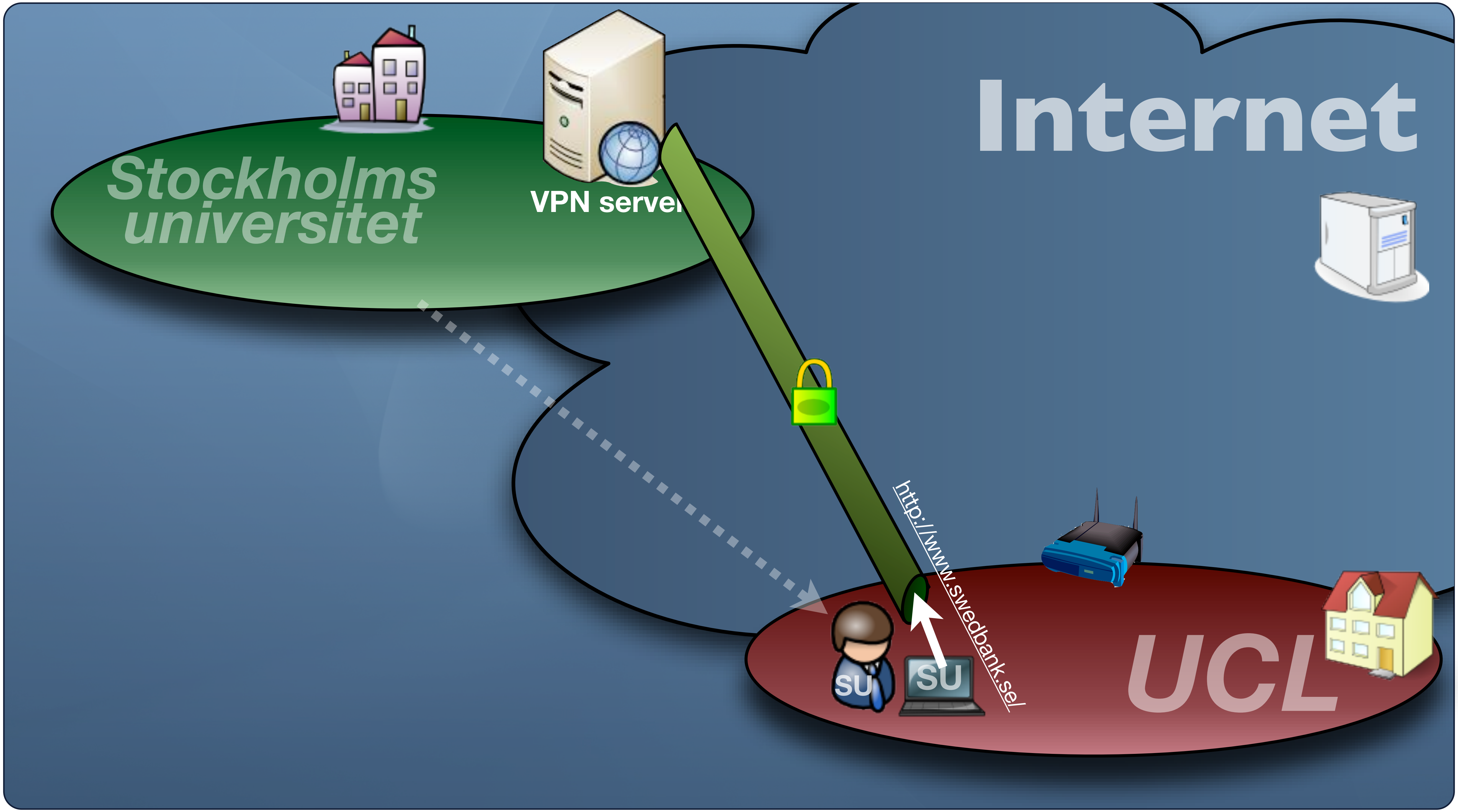
VPN



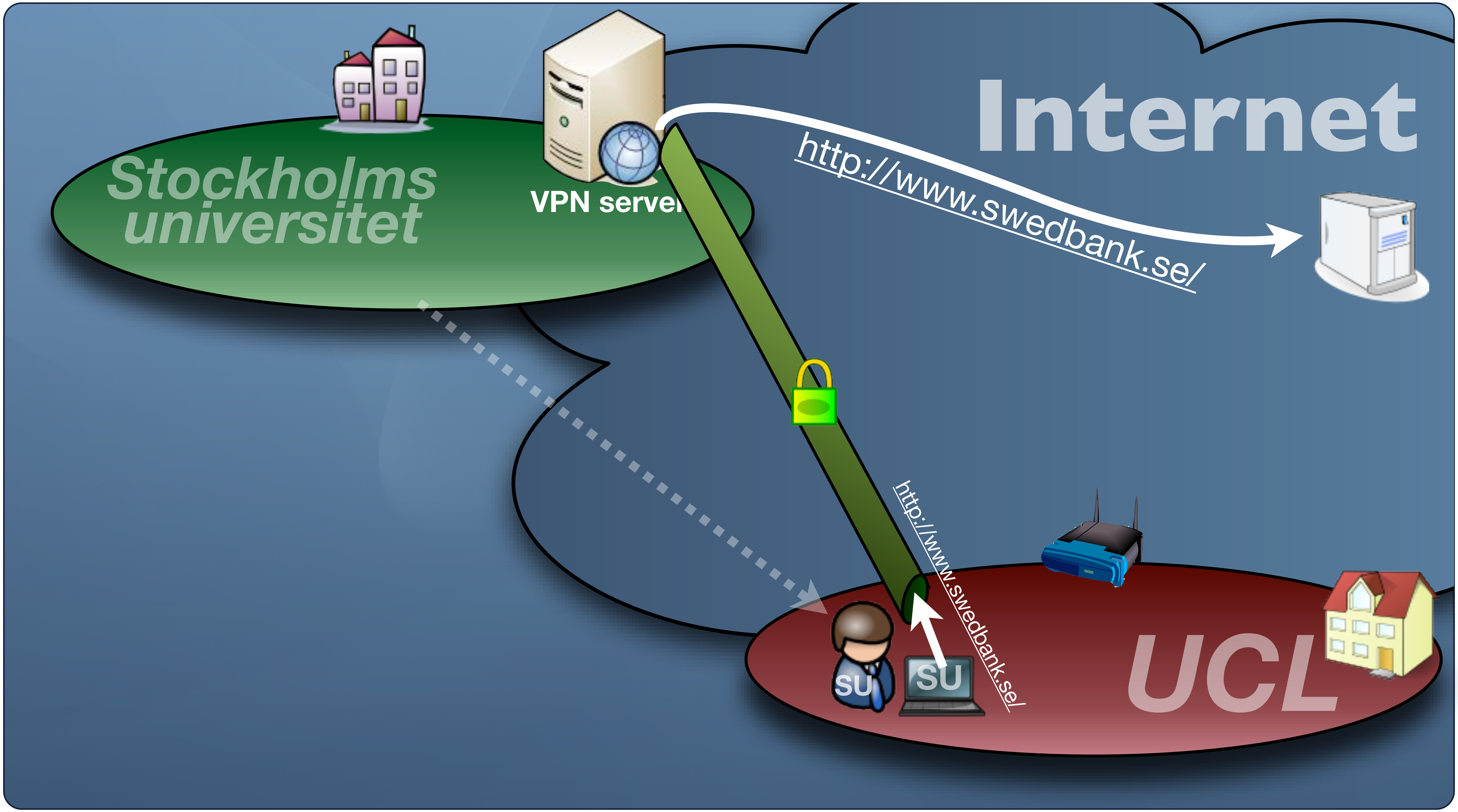
For the user : via username/pwd (or certificate)

For the home network : via certificate or no auth (cert must be distributed !)

VPN


Internet
Stockholms universitet
VPN server
http://www.swedbank.se/
SU
SU
UCL

VPN



Internet
Stockholms universitet
VPN server
http://www.swedbank.se/
http://www.swedbank.se/
SU
SU
UCL

VPN, a solution for previous issues ?

ip networking lab

Yes because :

- The requests are sent with the IP address of the home network
- If M sends spam over the Internet, only his home network is blamed
- It protects the user from a malicious visited network

VPN, a solution for previous issues ?

ip networking lab

Yes but :

- Only authentication between H and M :
  - F does not authenticate / know M and H
  - M does not always check H auth (F can do pharming)
- On user's demand
  - If M wants to meet some security goals
  - F cannot force M to create VPN to H

VPN, a solution for previous issues ?

The previous table, updated

	Remote auth.	VPN
User authentication (by F)	✓	✗
Administrative cost for F	✓	✓
Ease of use (for user)	✓	⚠
Blacklisting based on IP	✗	✓
Access based on IP	✗	✓
Attack on the infrastruct.	✗	✗
F malicious	✗	✓
Fake access point	⚠	✓

Combining IEEE802.1X and VPN

How ?

- Firewall of F blocks everything
- User connects with his credentials for IEEE802.1X
- F opens the VPN port as destination port, only from this user, and to its home network (inferred from IEEE802.1X)

Combining IEEE802.1X and VPN

Using both IEEE802.1X and VPN to reach security goals is possible. But :

- Need both infrastructures
- Once the user is authenticated, how the tunnel is forced to H ?
  - Filtering based on IEEE8021.X decision ?
- Two init phases can take some time (few seconds) to succeed

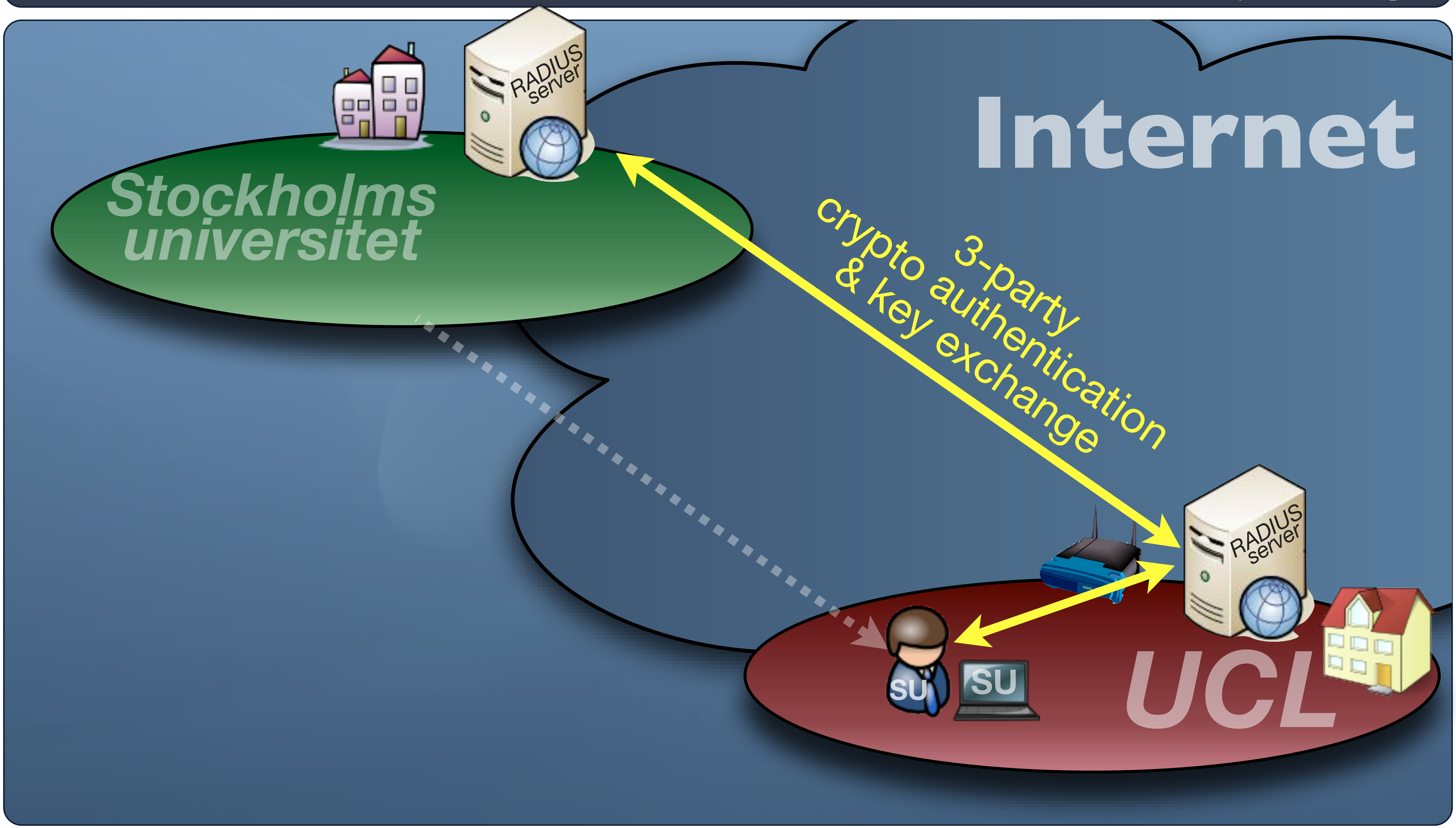
Content

The ALAWN project

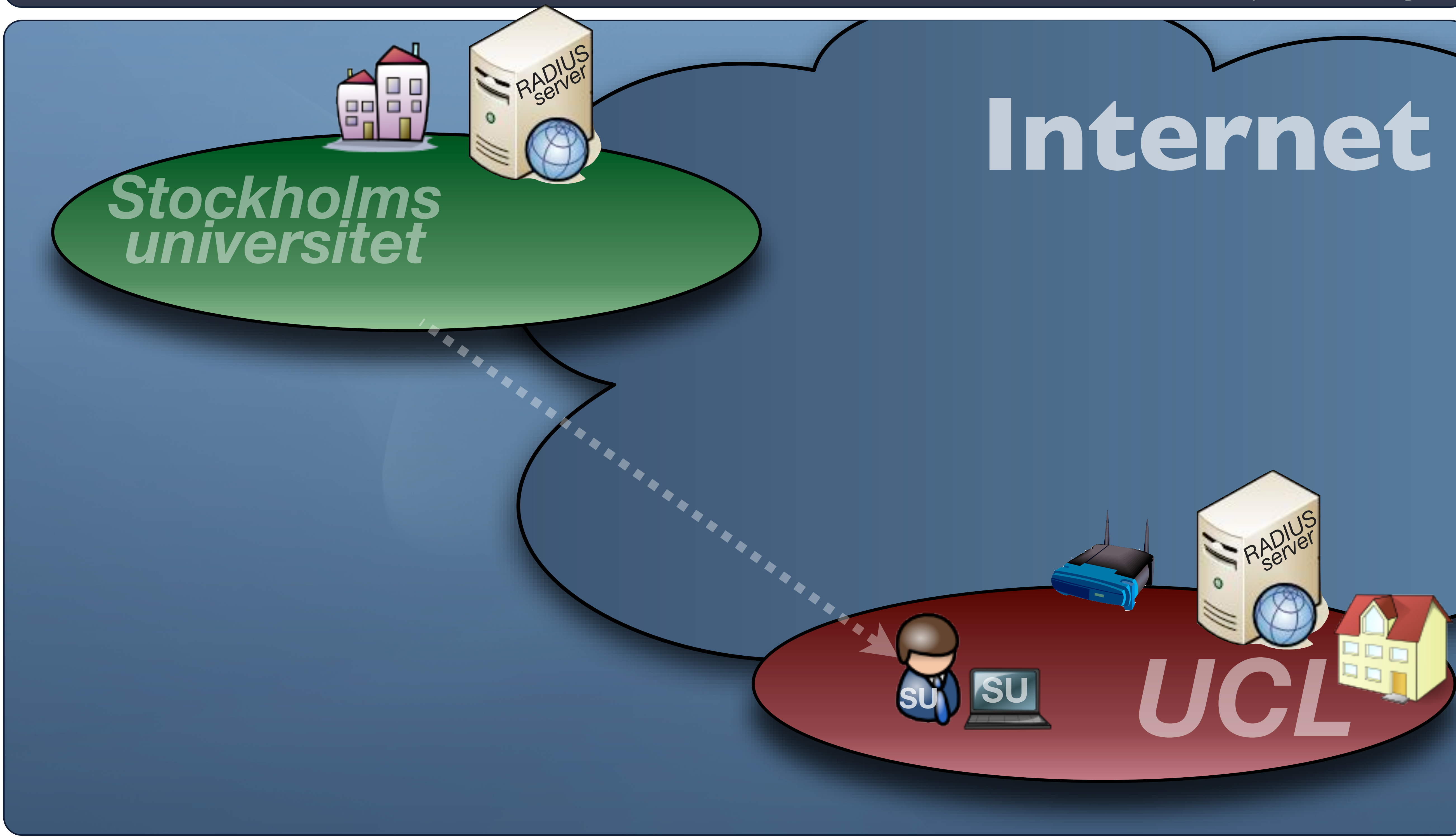
Some words about the project

- A Walloon Region project
- In collaboration with :
  - CRID (Research Centre on IT and Law - FUNDP - Namur)
  - Crypto Group - UCL
  - IP Networking Lab - UCL

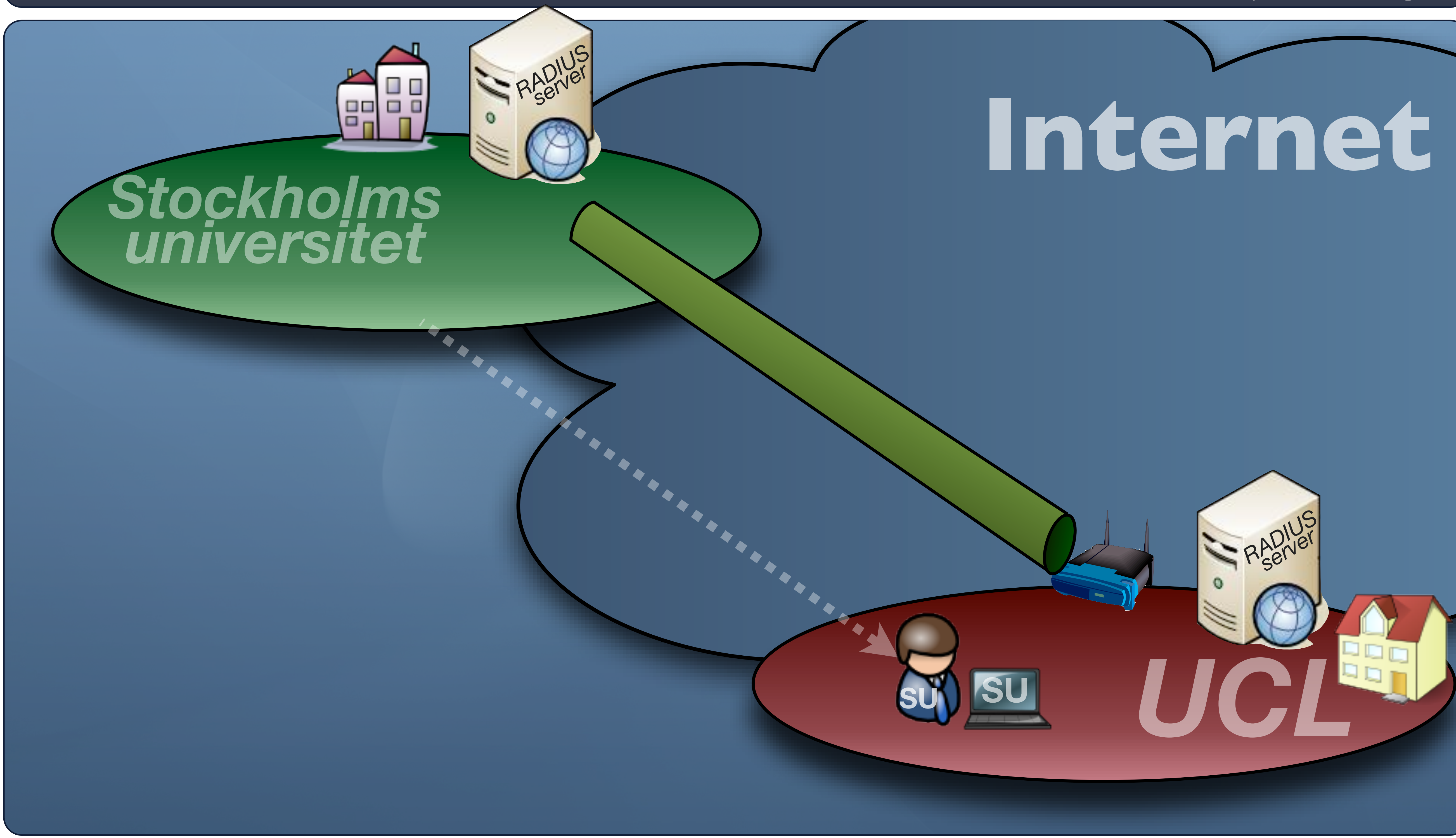
The proposal - Step 1



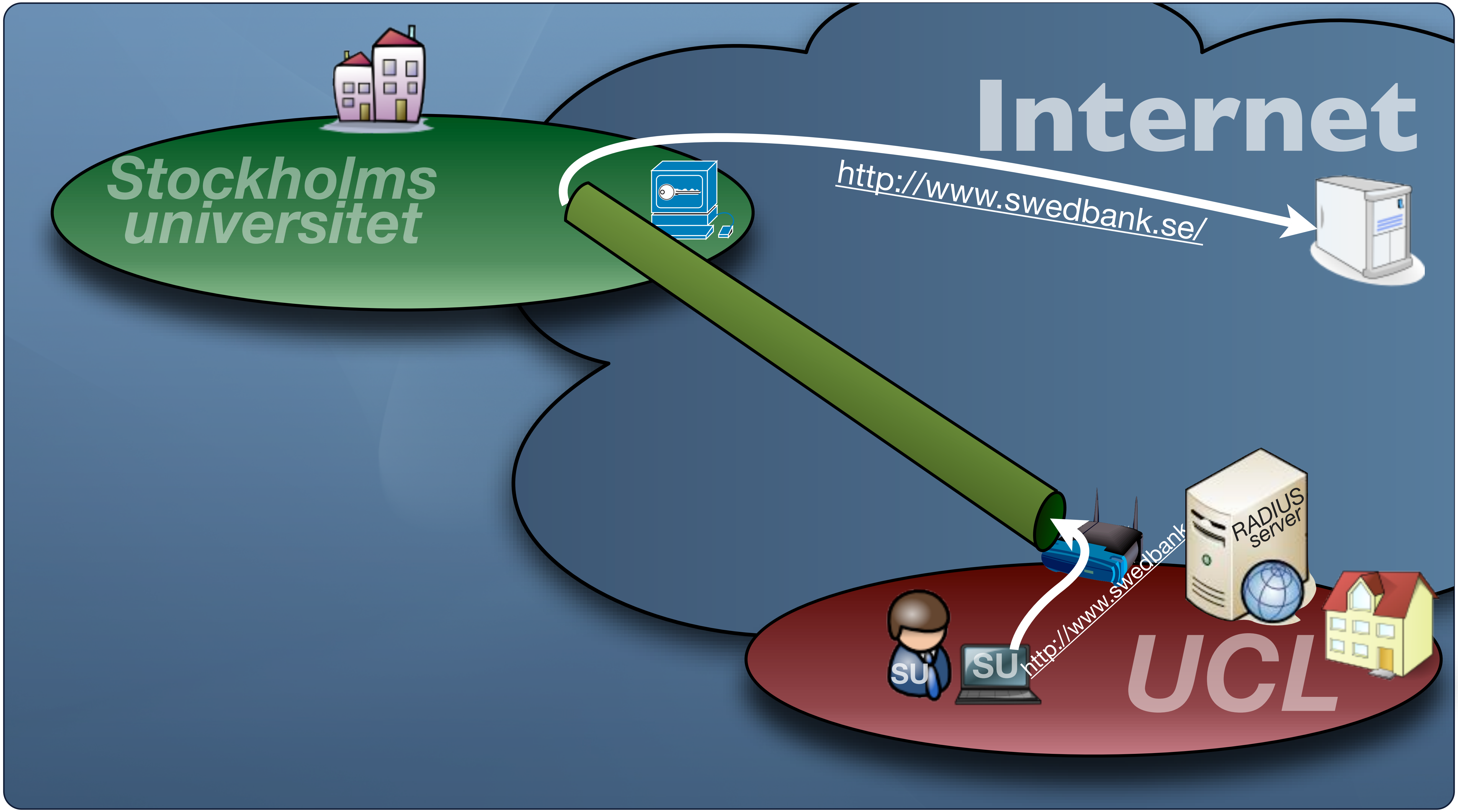
The proposal - Step 2



The proposal - Step 2



The proposal



Remote Auth. and Key Exchange (RAKE)

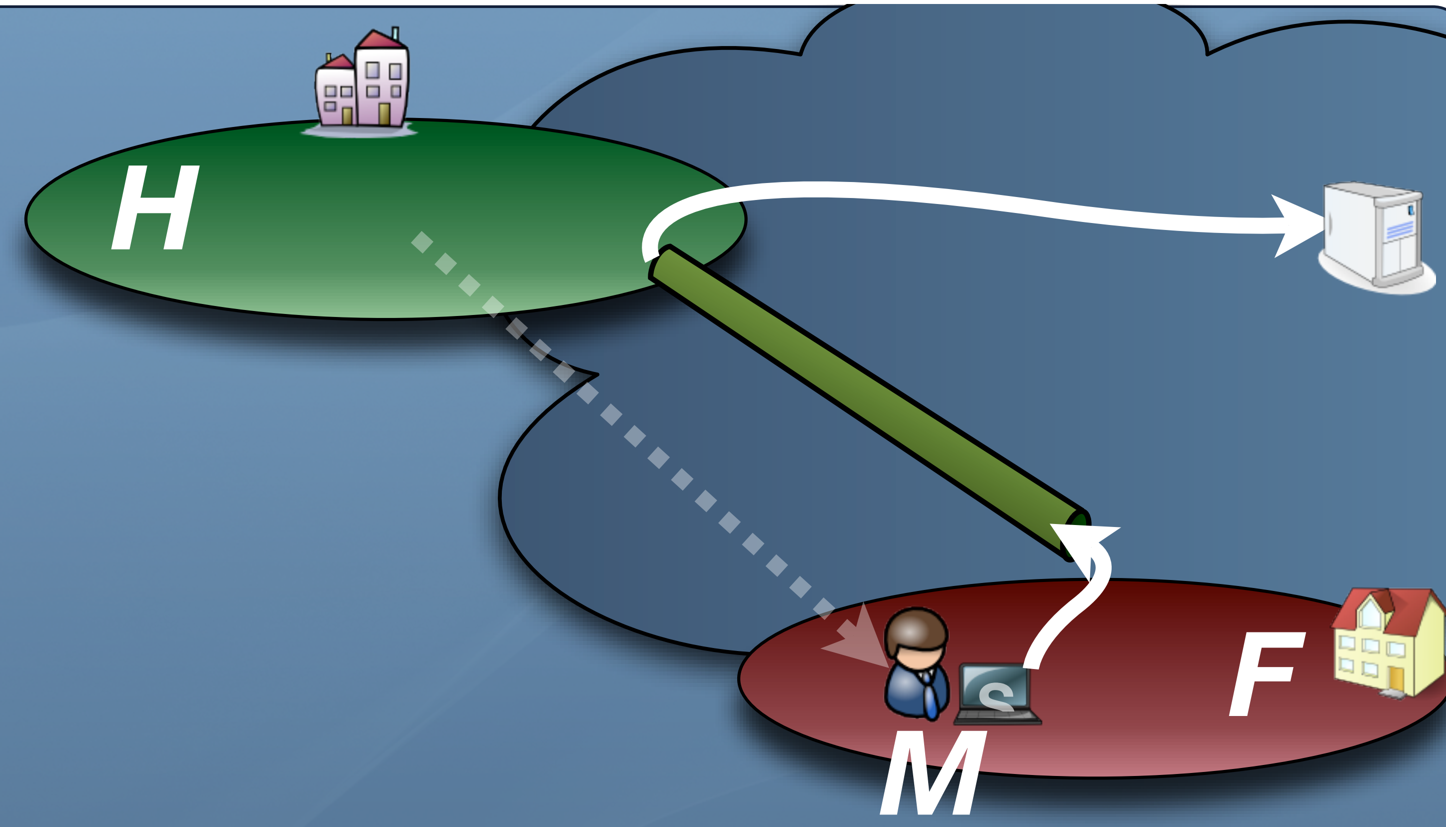
Goals for the protocol

- Authentication between M, H and F
- Key exchange
- (Negotiation of session parameters)

Security Goals

ip networking lab

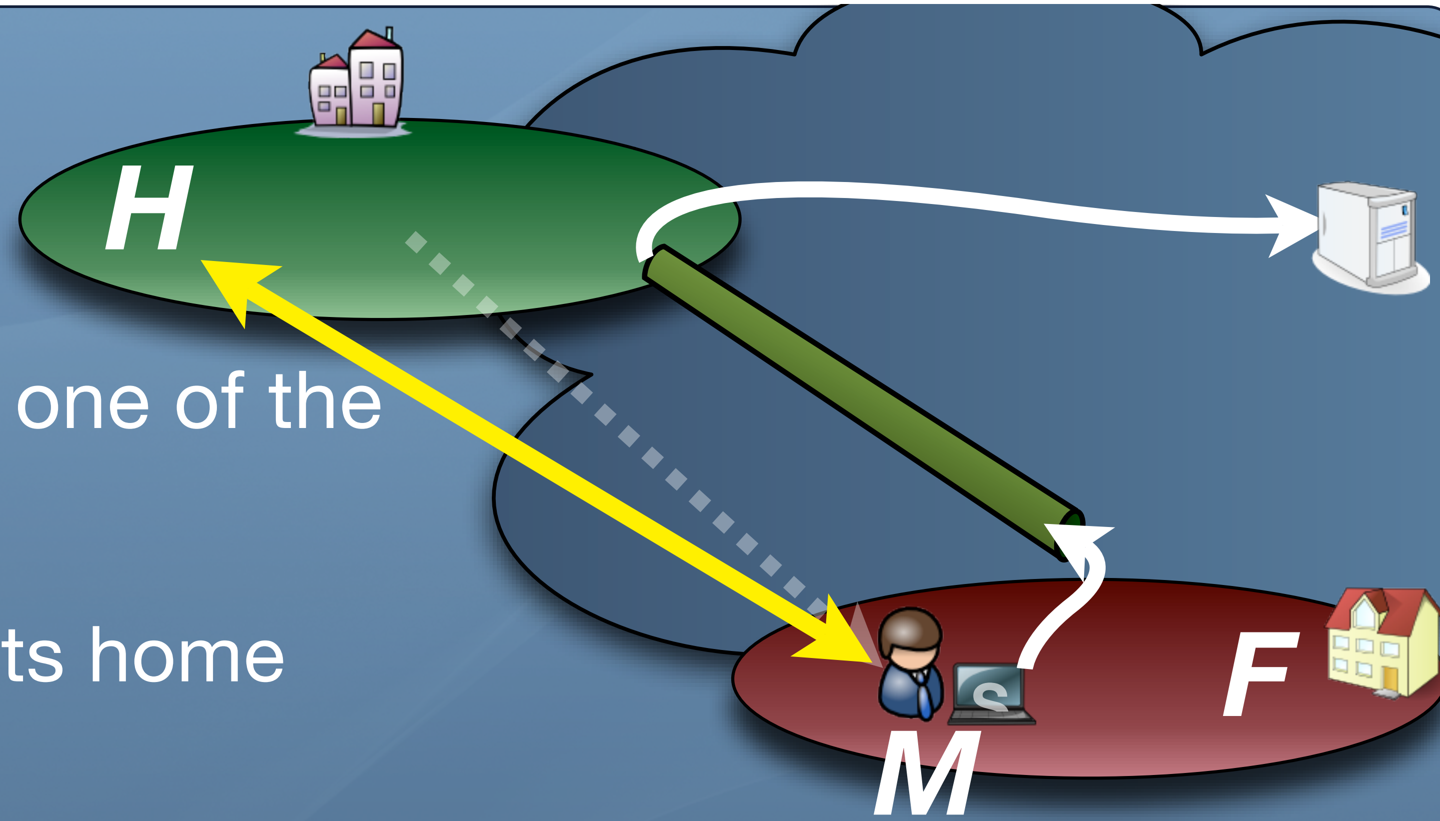
Authentication



Security Goals

ip networking lab

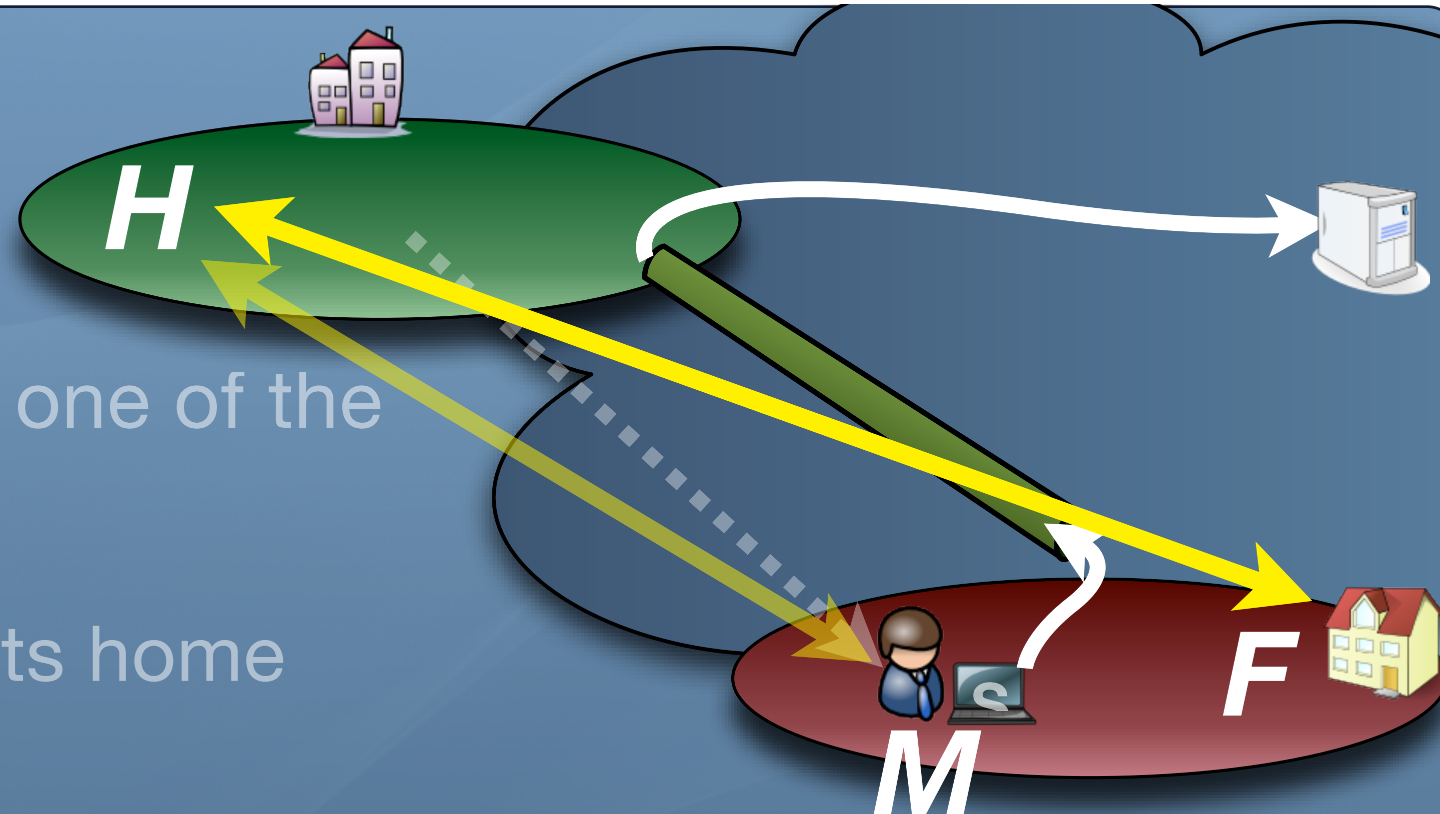
Authentication



- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network

Security Goals

Authentication

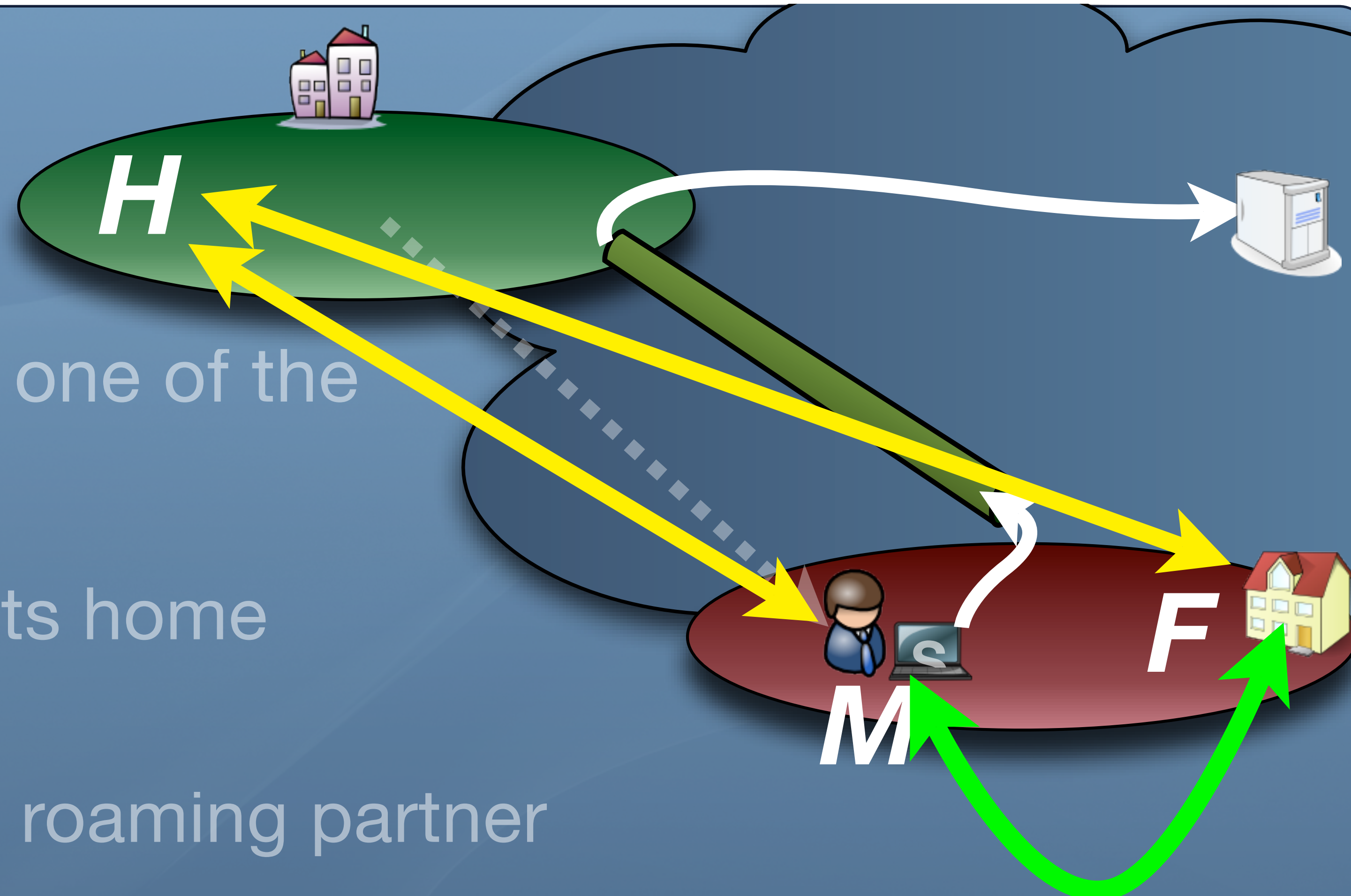


- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming partner

Security Goals

ip networking lab

Authentication

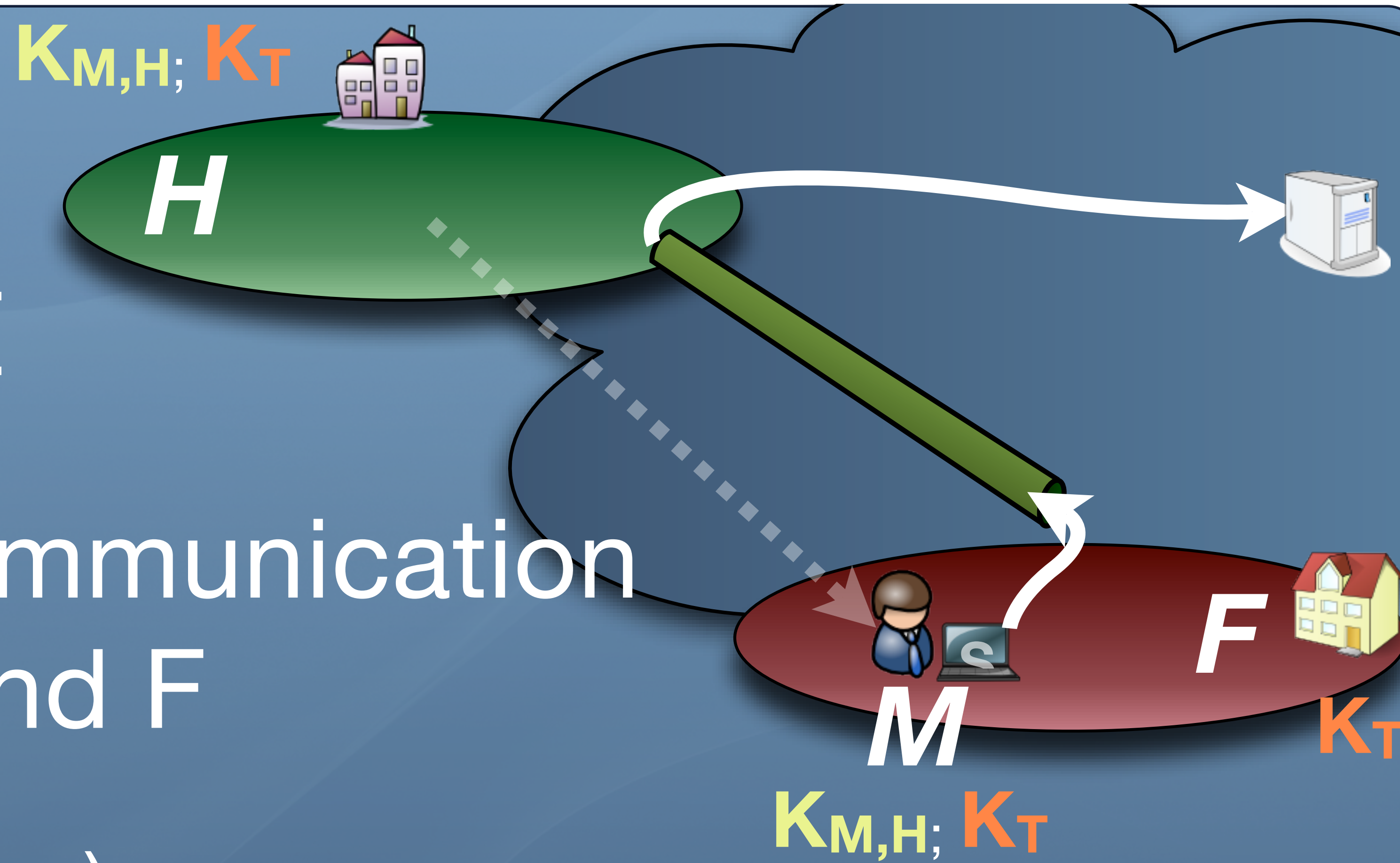


- H must authenticate M as one of the registered mobile devices
- M must authenticate H as its home network
- F must authenticate H as a roaming partner
- H must authenticate F as a roaming partner
- F trusts H to correctly authenticate M
- M trusts H to correctly authenticate F

Security Goals

Key establishment

- Protection of communication between M, H and F
  - ➡ K_T (tunnel key)
- End-to-end protection
  - ➡ $K_{M,H}$ (end-to-end key)



What are the keys used for ?

$K_{T,}$ the key shared between H-F-M

- To infer the key used for “wireless” communication
- To negotiate connection parameters (when it stops, accounting, mobility, ...)

What are the keys used for ?

$K_{M,H}$, the key shared between H and M

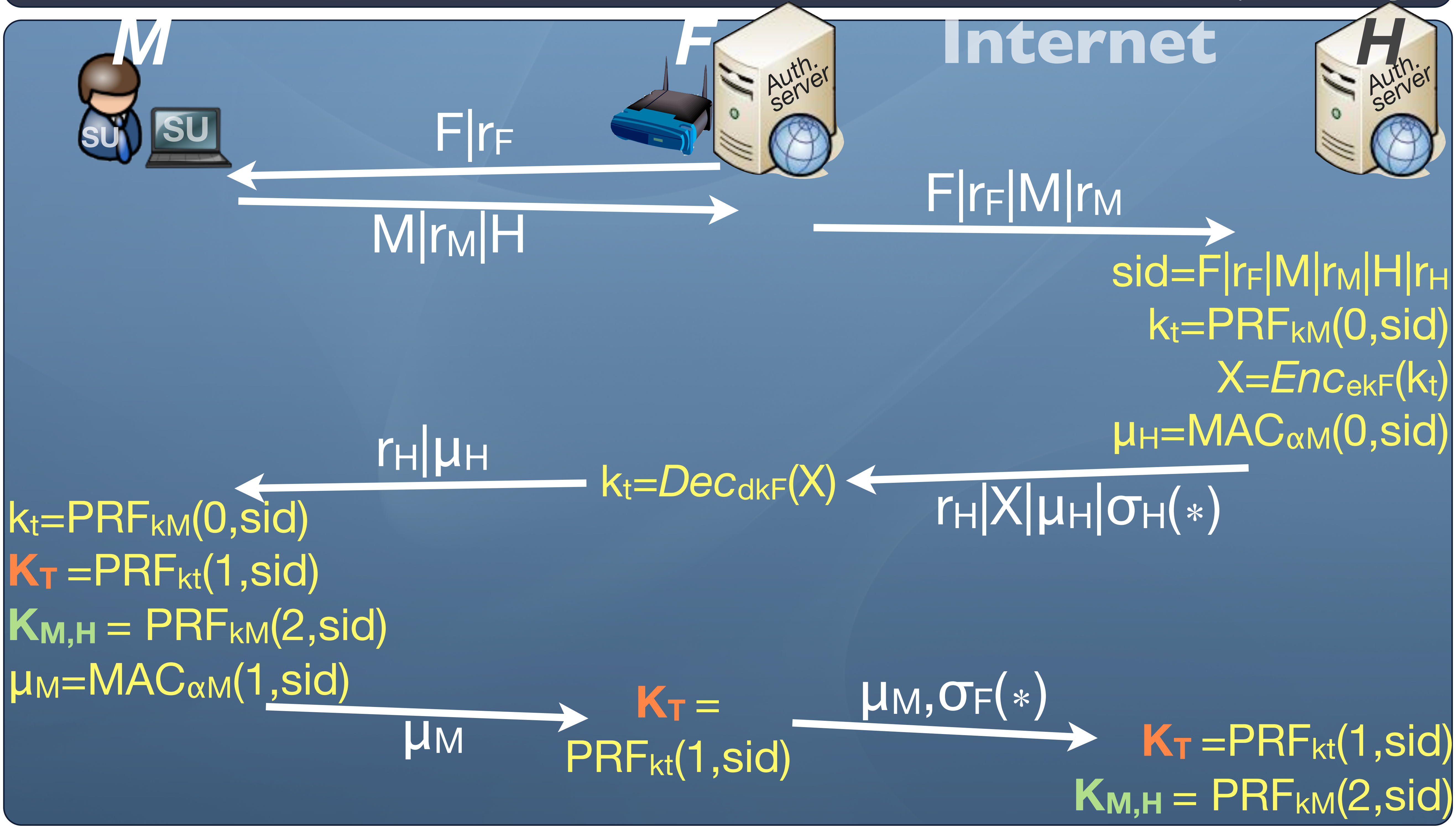
- For fully-encrypting the communication between M and H
- To negotiate connection parameters that should not be known/modified by F, shared between H and M

ip networking lab

Additional constraints

- RTT should be as low as possible
- The mobile device should not do “hard computation”

The protocol in itself (simplified)



The protocol in itself

- A full security model has be defined
- Protocol has been proved
- For the ones interested in details :

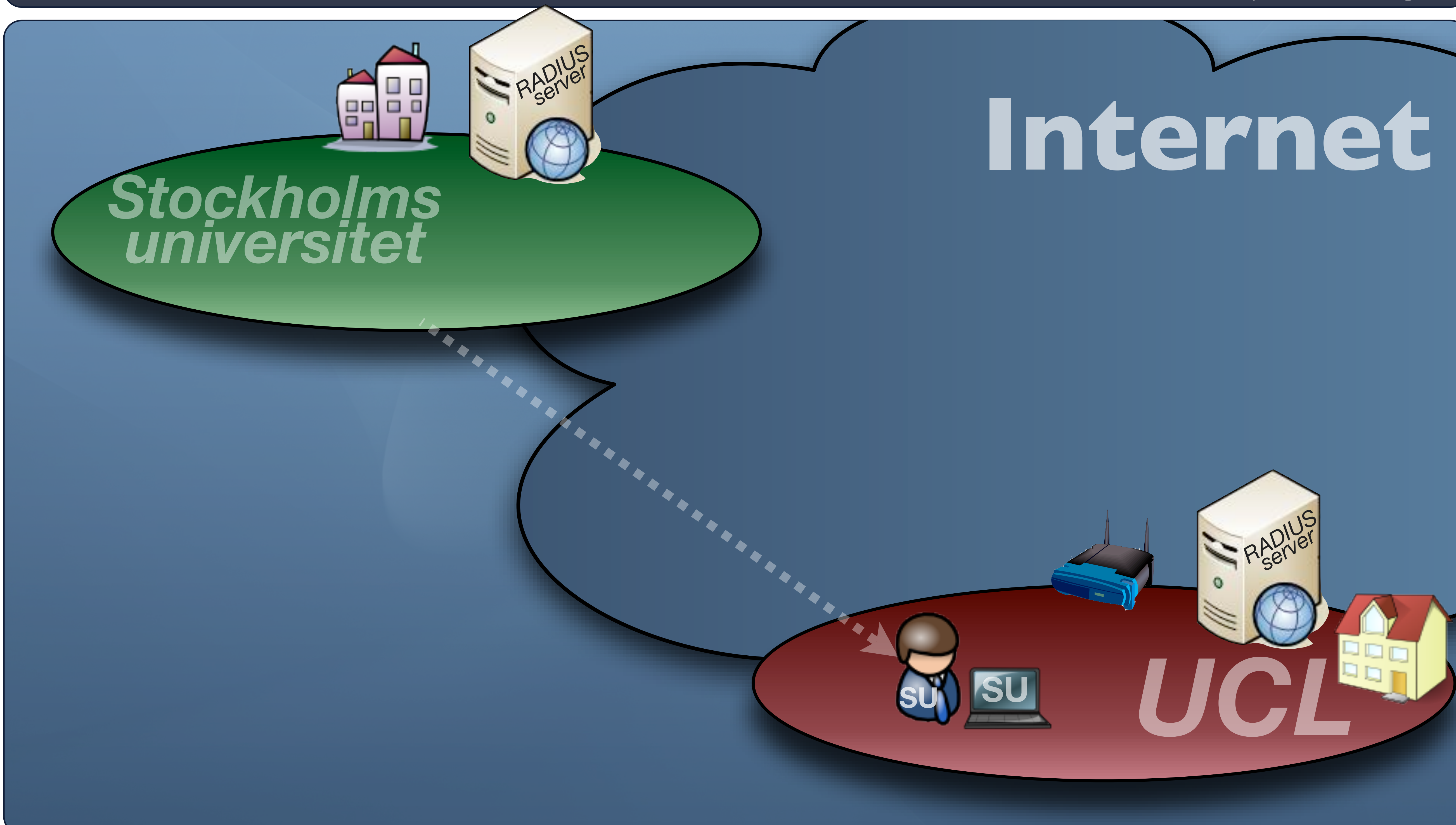
  M. Manulis, D. Leroy, F. Koeune, O. Bonaventure and J.-J. Quisquater, **Authenticated Wireless Roaming via Tunnels: Making Mobile Guests Feel at Home**, *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS 2009), Sydney, Australia, March 2009*

RAKE protocol

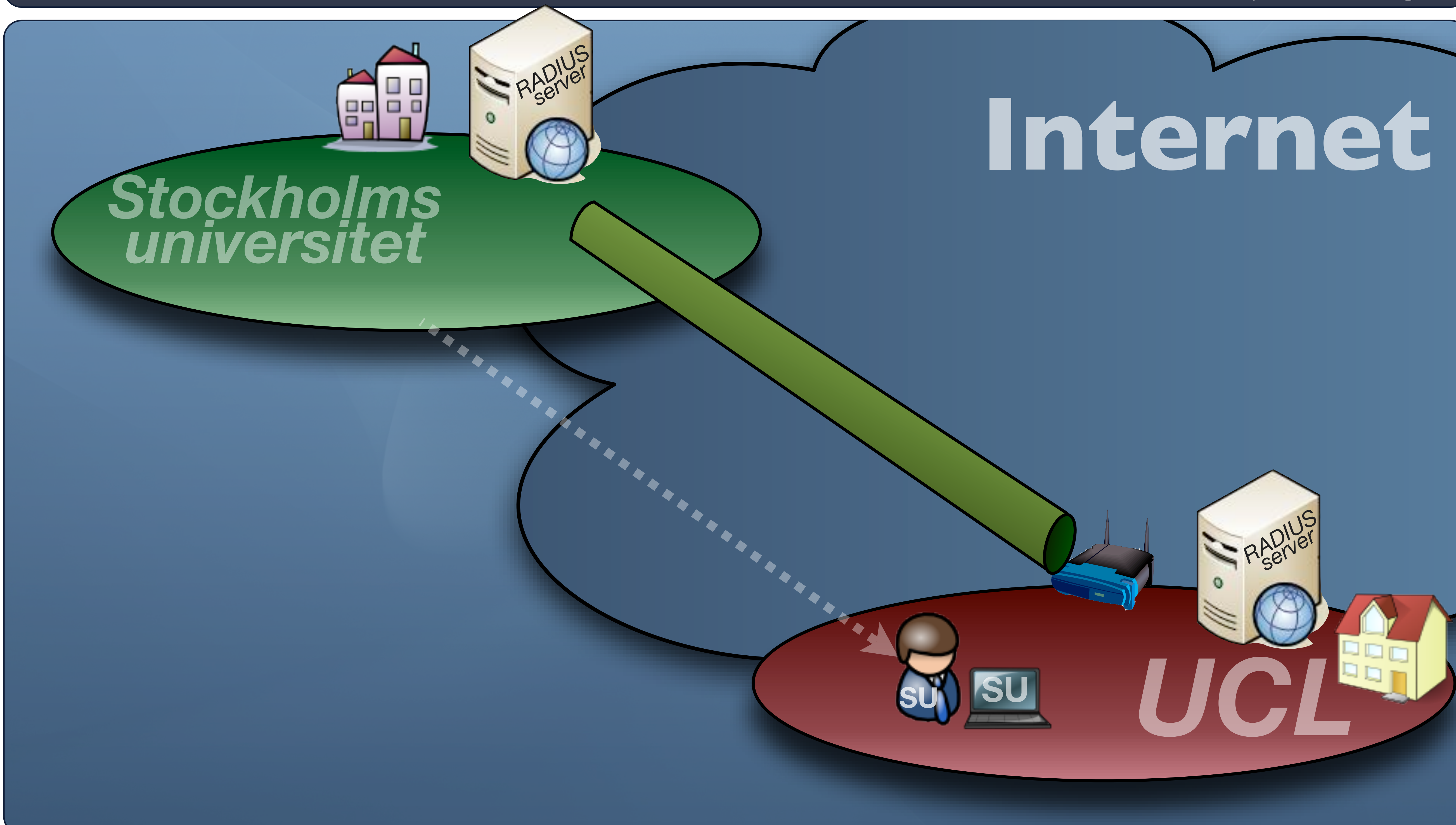
Additional constraints, results

- RTT should be as low as possible
- The mobile device should not do “hard computation”

The proposal



The proposal



Why using a tunnel ?

- Tunnel from F to H is not encrypted, it is only used to permit M to send packet to his home network
- Technical interests have been shown at the beginning of the presentation
- We showed with CRID that it also has legal advantages :

R. Robert, M. Manulis, F. De Villenfagne, D. Leroy, J. Jost, F. Koeune, C. Ker, J.-M. Dinant, Y. Poullet, O. Bonaventure, and J.-J. Quisquater, **WiFi Roaming: Legal Implications and Security Constraints**, *Int. J. of Law and Information Technology 2008 16: 205-241*

Technical choices

- The RAKE protocol :
  - Extending IEEE802.1X (EAP)
- The tunnel :
  - Use a L2TP tunnel
- Encryption between H and M :
  - Optional
  - Using IPSec (ESP)

Extending 802.1X for RAKE

- IEEE802.1X is now widely used
- It uses EAP (the Extensible Authentication Protocol) for authentication
- EAP can be easily extended

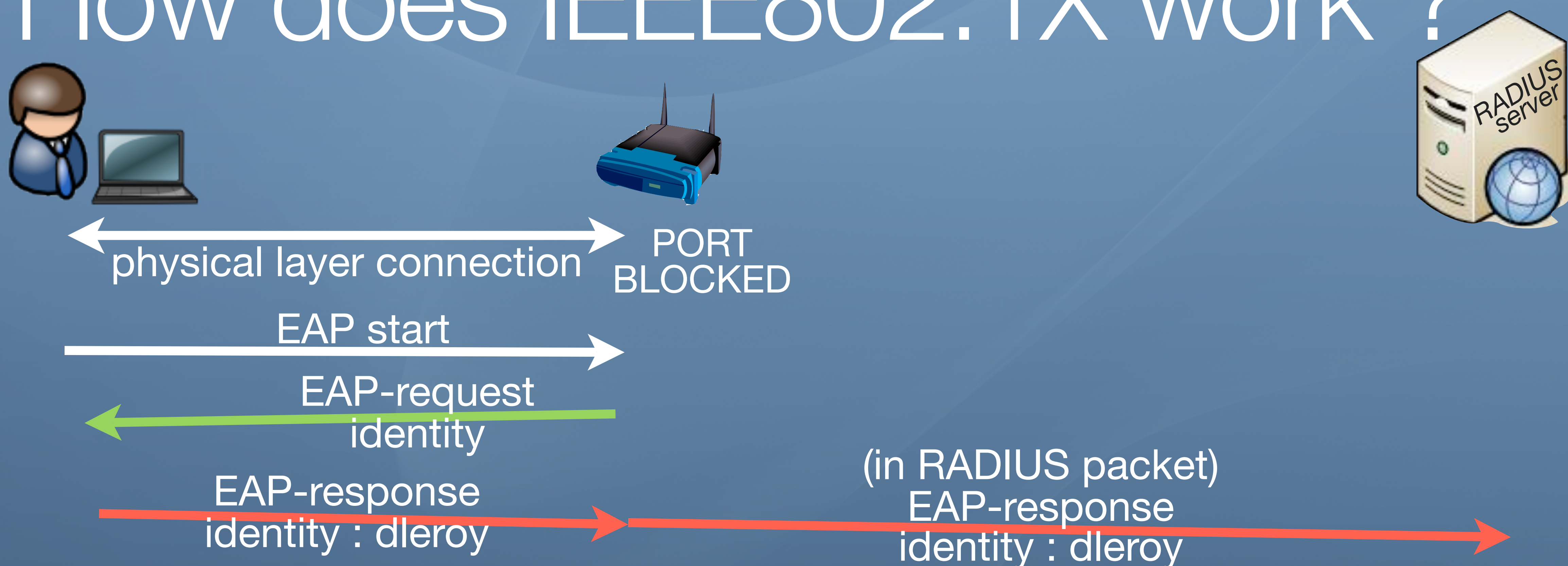
Extending 802.1X for RAKE

How does IEEE802.1X work ?

Extending 802.1X for RAKE

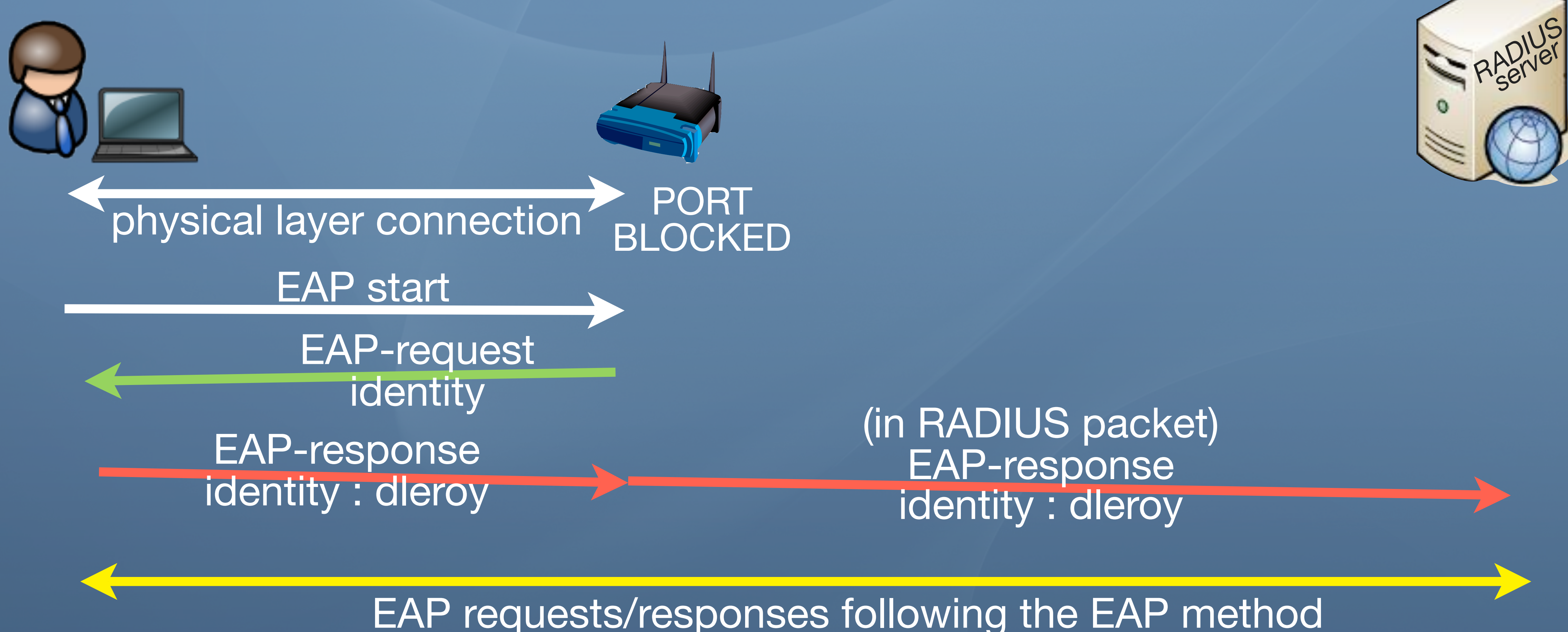
ip networking lab

How does IEEE802.1X work ?



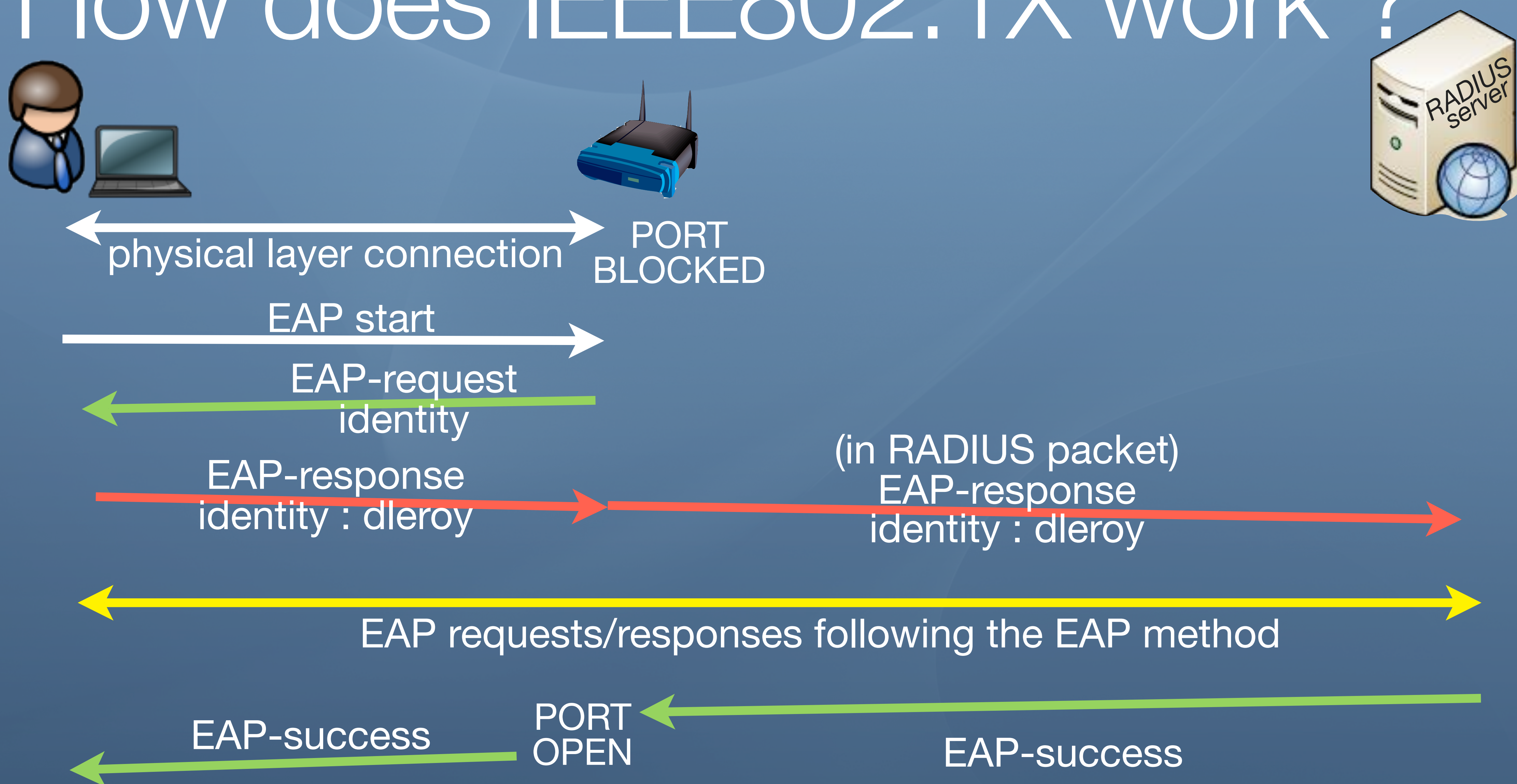
Extending 802.1X for RAKE

How does IEEE802.1X work ?



Extending 802.1X for RAKE

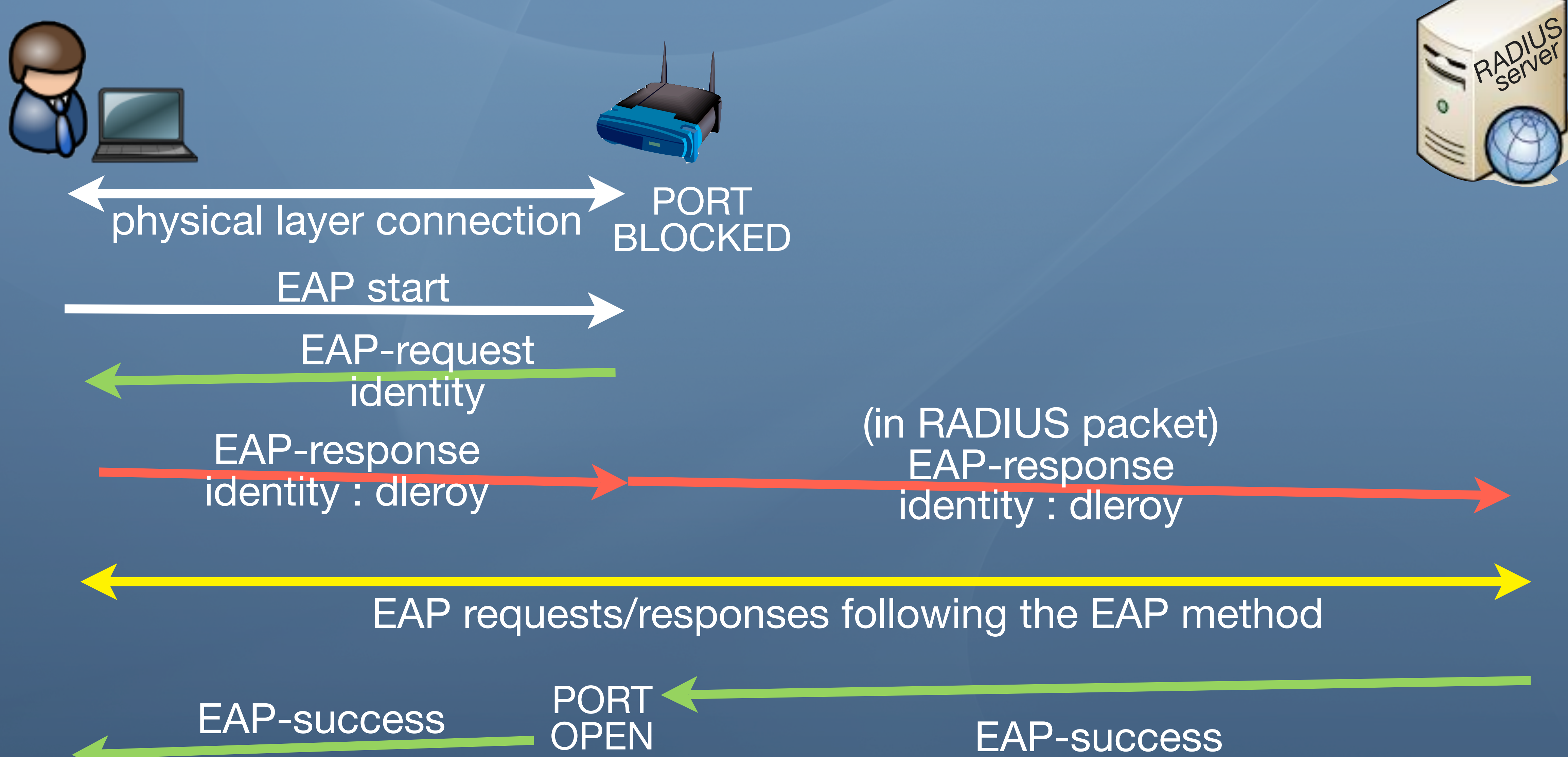
How does IEEE802.1X work ?



Extending 802.1X for RAKE

ip networking lab

How does IEEE802.1X work ?



Ethernet or WiFi (keys derived from previous negotiations)

Extending 802.1X for RAKE

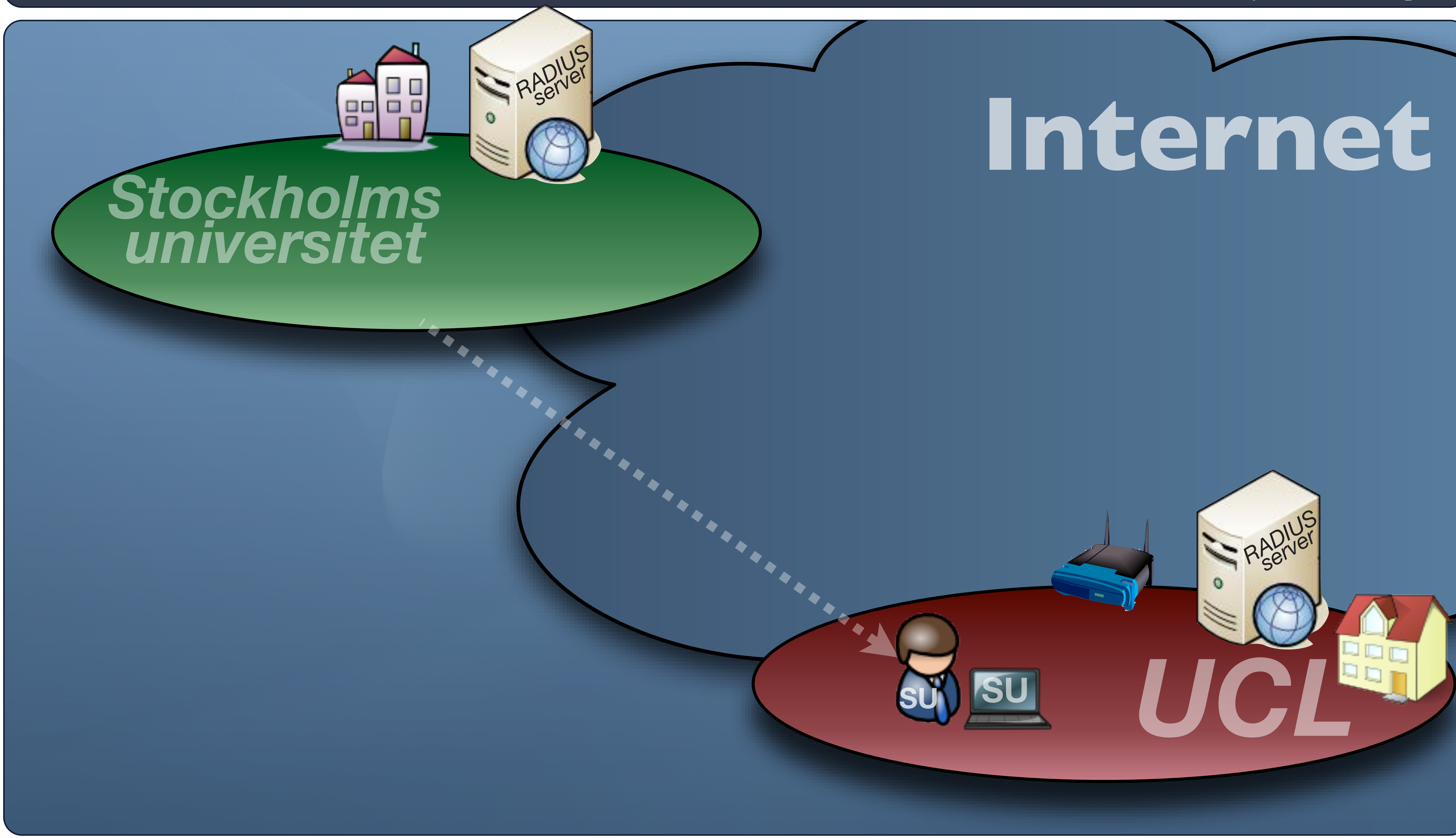
We have implemented it

- In “Host AP” project (hostapd & wpa_supplicant)
- An open-source implementation
- *hostapd* works with most Linux & BSD drivers
- *wpa_supplicant* works with most Linux, BSD & Windows drivers

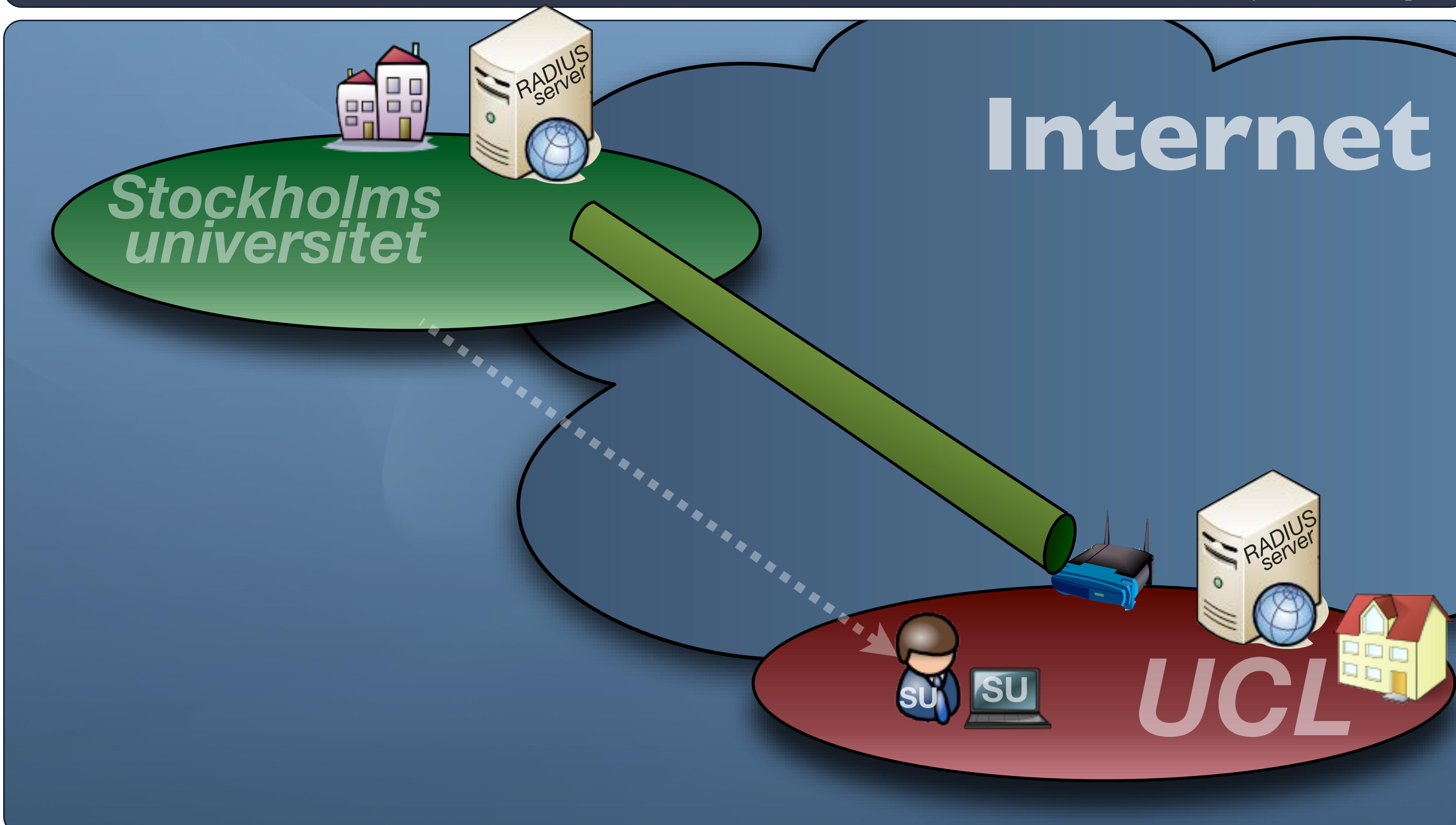
Extending 802.1X for RAKE

- In next months, we would like to test it in real situations
- With *hostap* :
  - On laptop and mobile devices
  - On access point (on OpenWRT OS)
  - On basic Linux server
- If you want to test the protocol in your network in a few months... please ask us

Tunnel between F and H



Tunnel between F and H



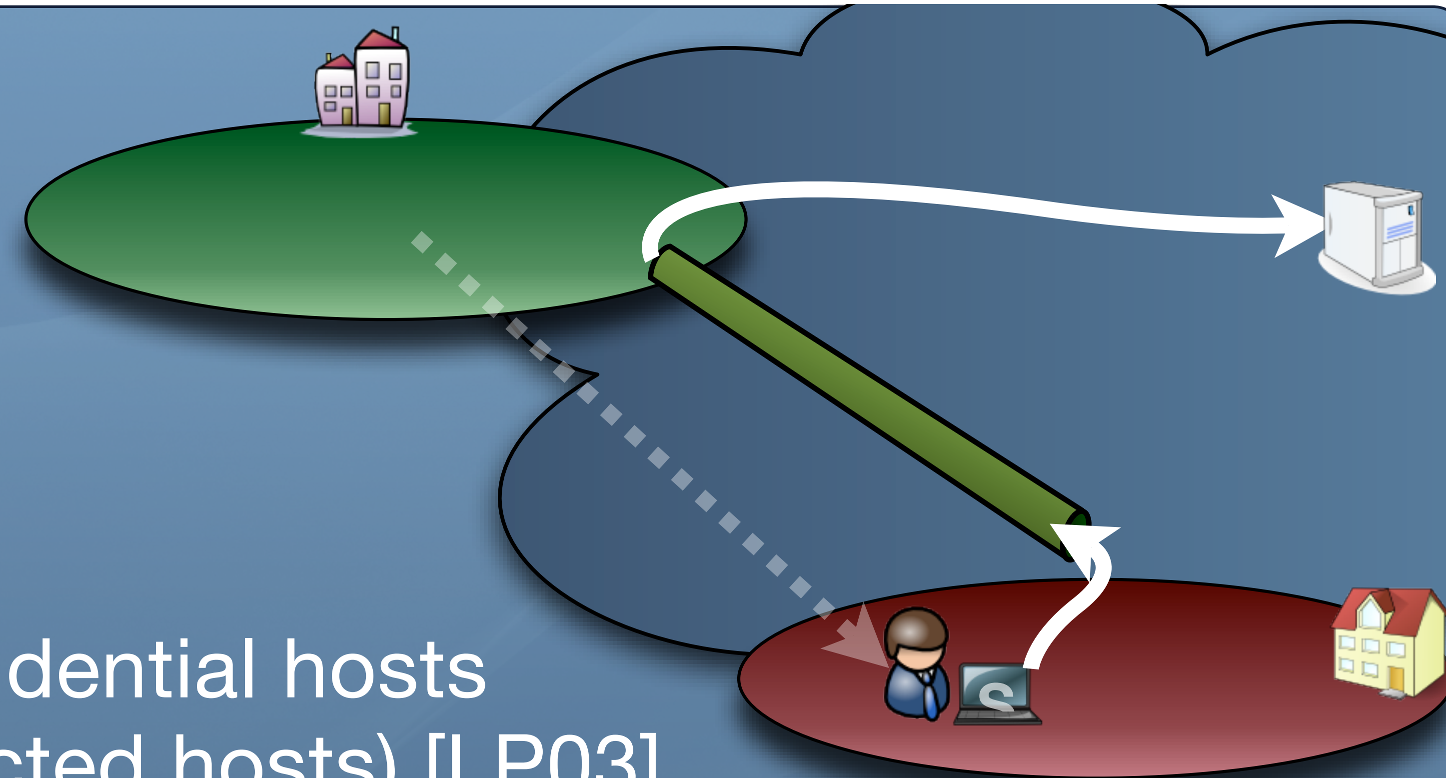
Tunnel between F and H

ip networking lab

A L2TP tunnel

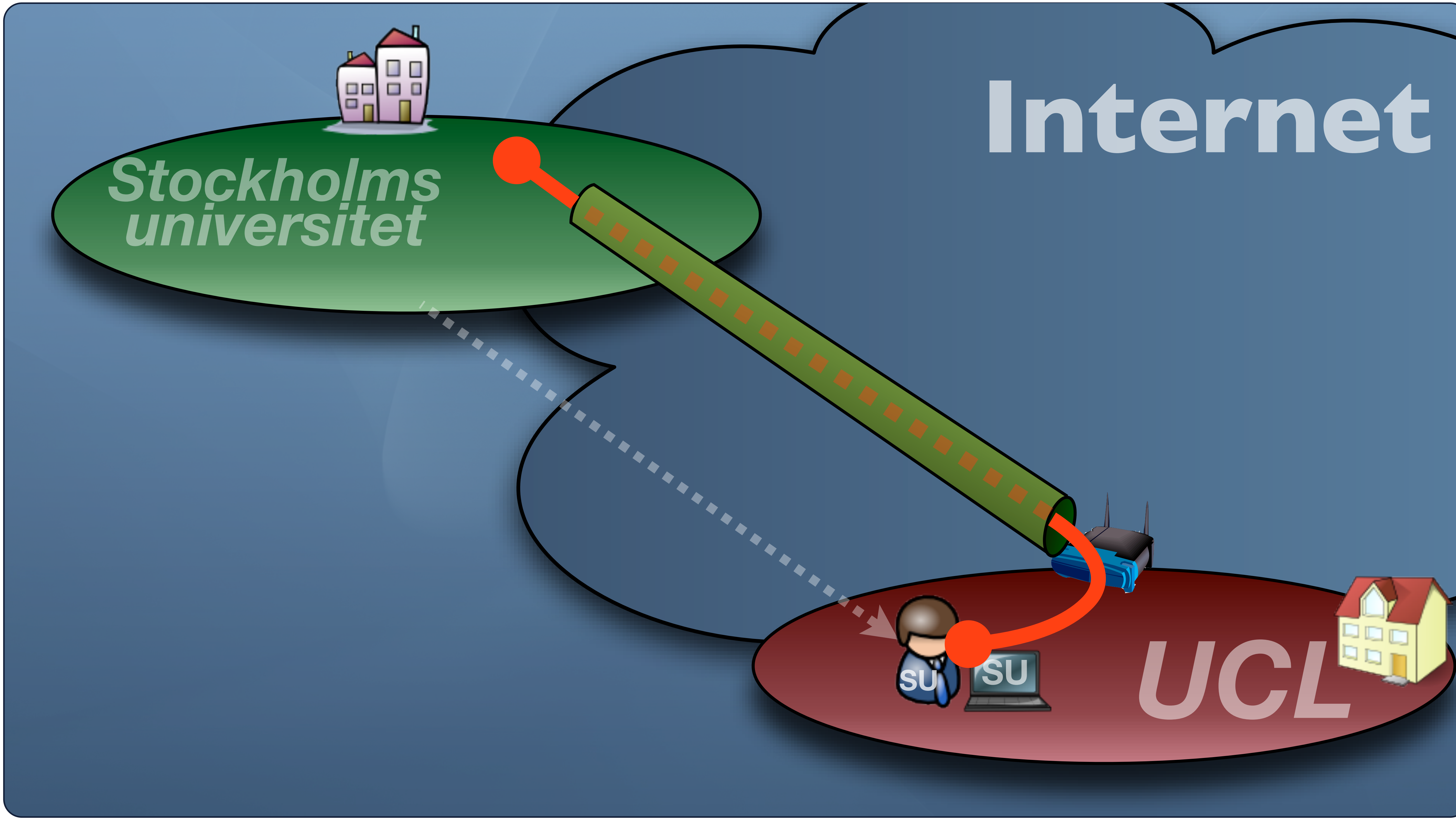
- The AP acts as layer 2 bridge
- Advantages:
  - Even the IP address is allocated by H
  - Do not have to rely on F technical config (e.g., IPv4/v6)
  - Less security risks for F
  - Transparent for M (the host and the user)

On Expected Increase of Latencies



- For each request, a RTT "H-F" is added
  - City : 30-60ms for residential hosts (3-4ms for well-connected hosts) [LP03]
  - Country (USA): <150ms [LP03]
  - Intercontinental : <250ms for 90% residential [DHGS07]
- ITU-T recommendations: one-way latency <400ms may be acceptable (e.g., VoIP)

Encryption between M and H



Encryption between M and H

- Kept optional (negotiated)
- Using $K_{M,H}$ (only known by M and H)
- Encryption method negotiated
  - more suitable : IPSec ESP in tunnel mode

Comparison with previous solutions

	Remote auth.	VPN	RAKE
User authentication (by F)	✓	✗	✓
Administrative cost for F	✓	✓	✓
Ease of use (for user)	✓	⚠	✓
Blacklisting based on IP	✗	✓	✓
Access based on IP	✗	✓	✓
Attack on the infrastruct.	✗	✗	✓
F malicious	✗	✓	✓
Fake access point	⚠	✓	✓

Summary on our proposal

ip networking lab

Constraints

- ✓ The tunnel increases the latency for some destinations
- ✓ The partnership has to be decided earlier
- ✓ Need (light) modifications of host, AP or the egress router, and authentication server.

Summary on our proposal

ip networking lab

Advantages

- ✓ If the user sends spam, the user's home network is blamed (and blacklisted), not the visited network
- ✓ Visited network does not care about the user activities
- ✓ Traffic can be encrypted

Summary on our proposal

ip networking lab

Advantages

- ✓ Tunnel is initiated (and forced) by F and H, not by the user
- ✓ H does verify F authentication (>< TTLS)
- ✓ Same services as “at home”

Questions ?

Damien Leroy
damien.leroy@uclouvain.be

ip networking lab
http://inl.info.ucl.ac.be