

EduRoam

EuroCAMP, 4 march 2005

Klaas.Wierenga@surfnet.nl

Contents

- Why EduRoam?
- Implementation
 - Requirements
 - Technology
 - Policy
- Status EduRoam
- The future

Why EduRoam?

Wireless LAN is unsafe

```

Network List (Autofit)
Name          T M Ch Packts Flags IP Range
! <stealthy>  A Y 01  9615      0,0,0,0

Info
Ntwrks      1
Pckets     9615
Cryptd     8996
Weak        1
Noise       0
Discrd      0
Pkts/s     376
Elapspd    000104

Status

Found SSID "stealthy" for cloaked network BSSID 00:02:2D:27:D9:22
Connected to Kismet server version 2.8.1 build 20030126205324 on localhost:2
Battery: AC 100% 0h0m0s
    
```

```
root@ibook:~# tcpdump -n -i eth1
```

```
19:52:08.995104 10.0.1.2 > 10.0.1.1: icmp: echo request
```

```
19:52:08.996412 10.0.1.1 > 10.0.1.2: icmp: echo reply
```

```
19:52:08.997961 10.0.1.2 > 10.0.1.1: icmp: echo request
```

```
19:52:08.999220 10.0.1.1 > 10.0.1.2: icmp: echo reply
```

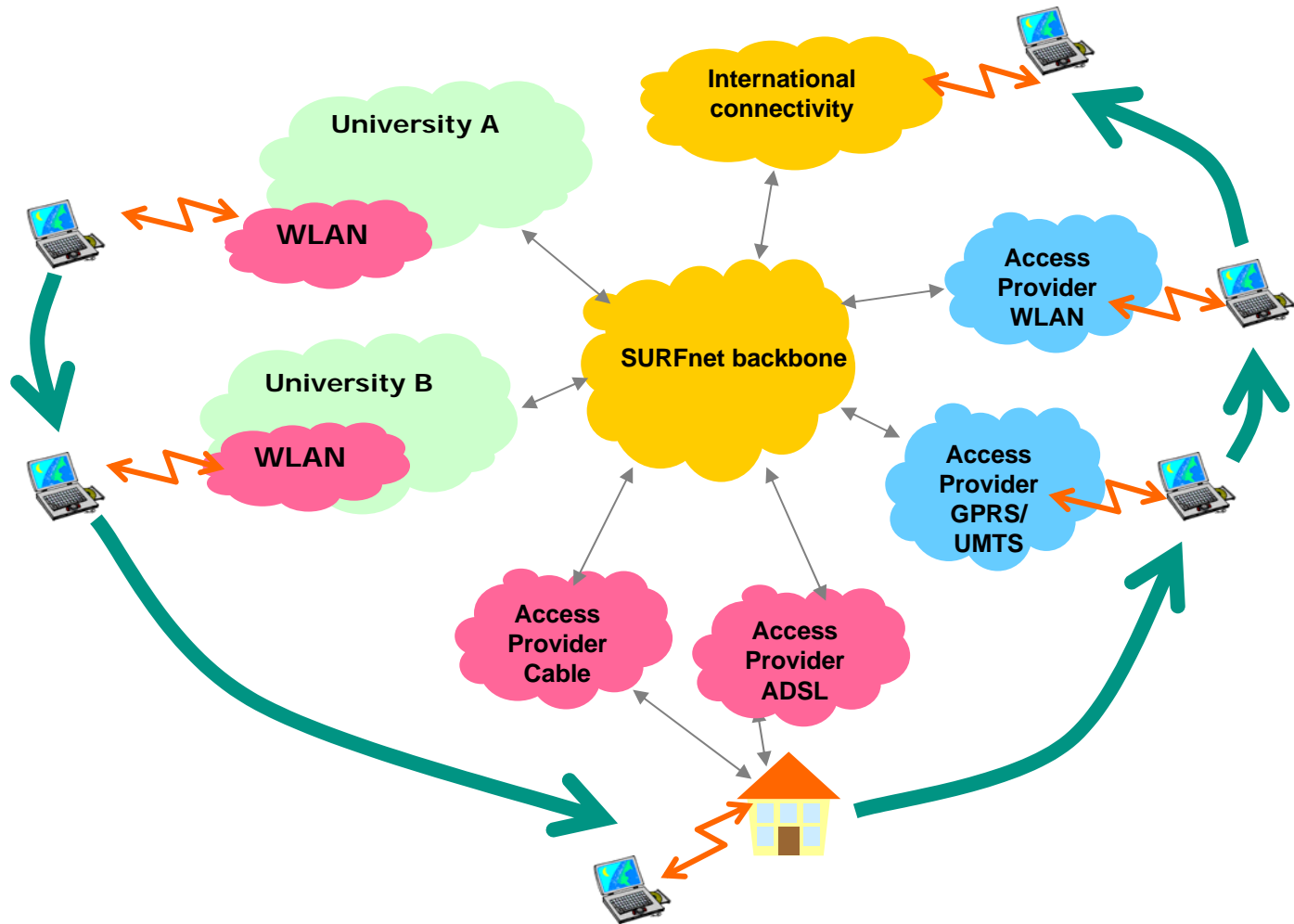
```
19:52:09.000581 10.0.1.2 > 10.0.1.1: icmp: echo request
```

```
19:52:09.003162 10.0.1.1 > 10.0.1.2: icmp: echo reply ^C
```

The screenshot shows the Aircrack-ng application window. At the top, there are menu options: File, Edit, Settings, Help. Below the menu is a control panel with buttons for '^ scan' and 'channel 6'. There are input fields for 'Network device' (set to eth1), 'Card type' (set to Other), '40 bit crack breadth' (set to 4), and '128 bit crack breadth' (set to 2). Below the control panel is a table with columns: C, BSSID, Name, WEP, Last IV, Chan, Packets, Encrypted, Interesting, PW: Hex, and PW: ASCII. The table contains one entry: X 00:02:2D:27:D9:22 stealthy Y D8:4A:1D 1 3430654 3379593 2294 74:38:24:47:63 t8\$Gc. At the bottom of the window are buttons for 'Start', 'Stop', and 'Clear'.

C	BSSID	Name	WEP	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASCII
X	00:02:2D:27:D9:22	stealthy	Y	D8:4A:1D	1	3430654	3379593	2294	74:38:24:47:63	t8\$Gc

Users are mobile



Requirements

- Identify users uniquely at the edge of the network
 - No session hijacking
- Enable guest usage
- Scalable
 - Local user administration and authentication
 - No exponential administrative load
- Easy to install and use
 - At the most one-time installation by the user
- Open
 - Support for all common operating systems
 - Non-proprietary
- Safe

Possible solutions

- Open access: scalable, unsafe
- MAC-address: not scalable, unsafe
- WEP: not scalable, unsafe

European research networks:

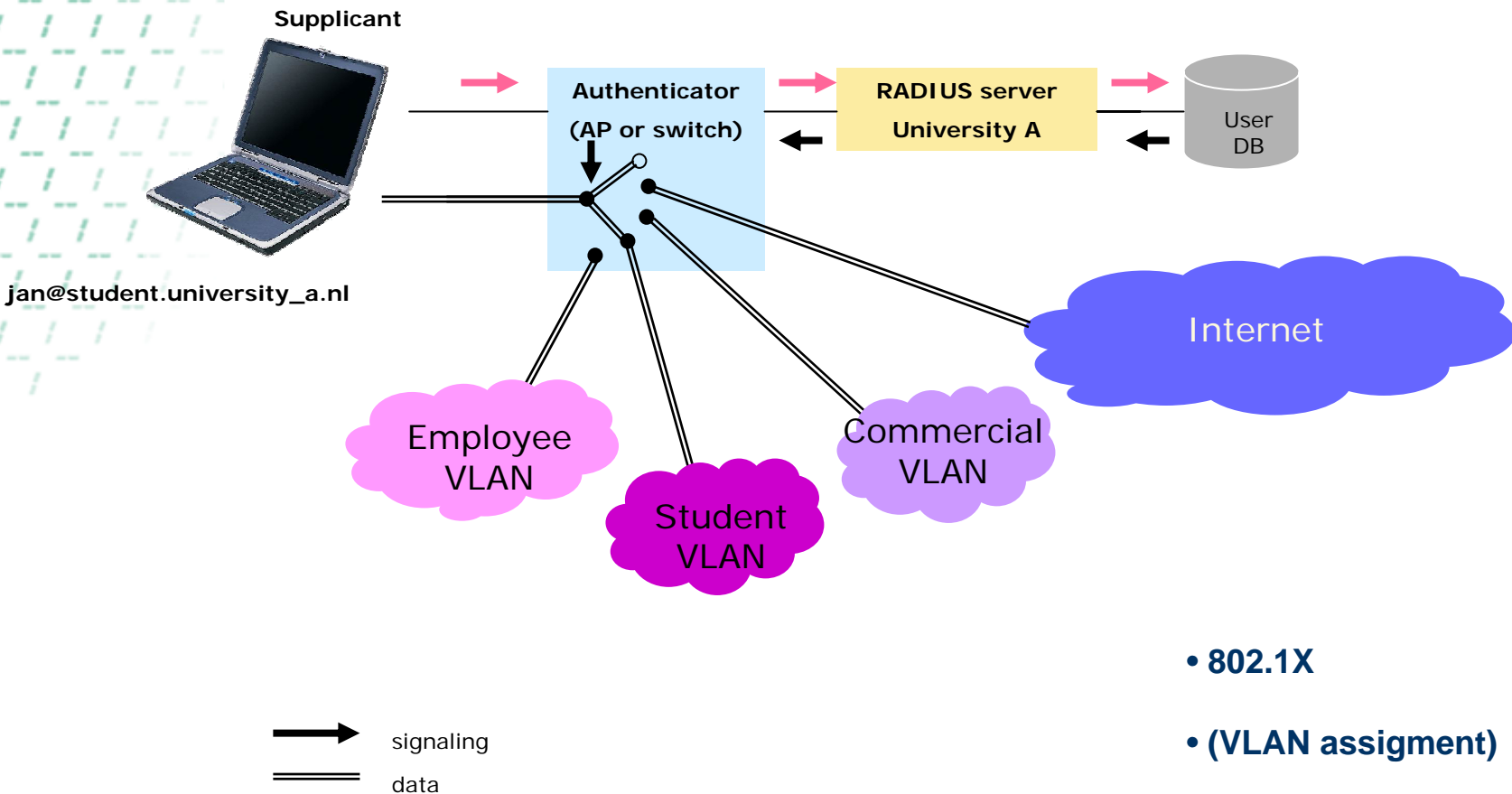
- Web-gateway+RADIUS: scalable, unsafe?
- VPN-gateway: not scalable?, safe
- 802.1X+RADIUS: scalable, safe, the future, but (at the time).... new

Implementation

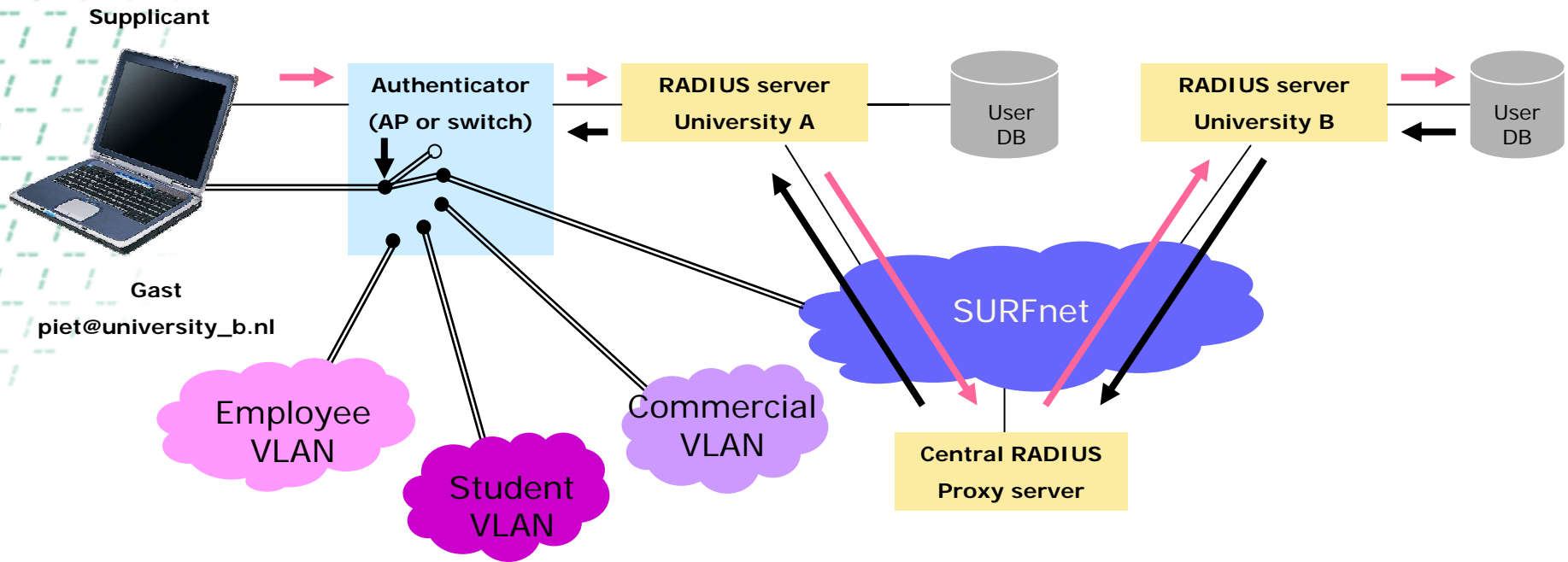
EduRoam architecture

- Security based on 802.1X (or web-based redirect)
 - Different authentication mechanisms possible
 - Identity-based networking
 - Mutual authentication possible (by using the right EAP-types: PEAP, TTLS, TLS)
 - Protection of credentials
 - Integration with VLAN assignment
 - Provides basis for new wireless security standards WPA and 802.11i
- Roaming based on RADIUS proxying
 - Remote Authentication Dial In User Service
 - Transport-protocol for authentication information
- Trust fabric based on:
 - Technical: RADIUS hierarchy
 - Policy: Documents/contracts that define the responsibilities of user, institution, NREN and the EduRoam federation

Secure access to the institution network with 802.1X



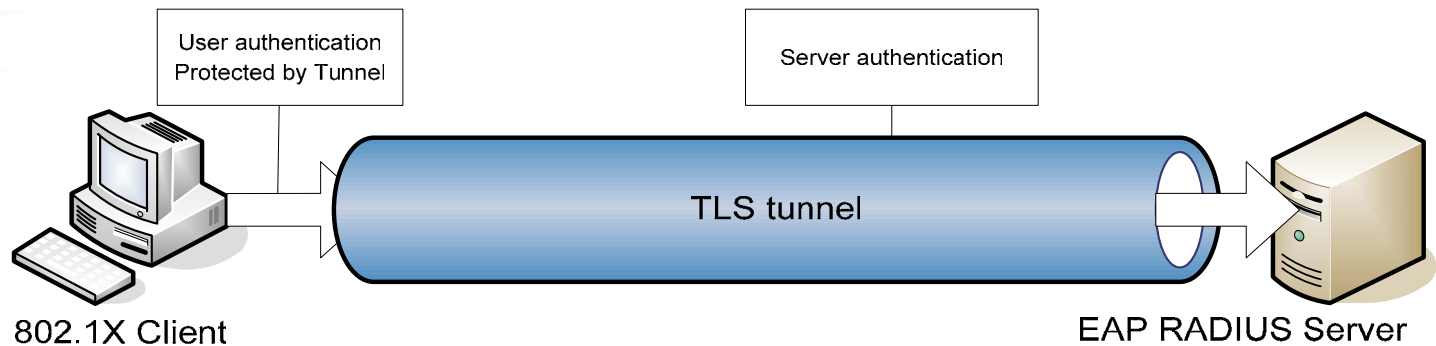
EduRoam



- Trust based on RADIUS plus policy documents
- 802.1X
- (VLAN assignment)

Tunneled authentication (PEAP/TTLS)

- Uses TLS/SSL tunnel to protect data
 - The TLS tunnel is set up using the server certificate, thus authenticating the server and preventing man-in-the-middle attacks
 - The user sends his credentials through the secure tunnel to the server, thus authenticating the user



- Can use dynamic session keys for 'in the air' encryption

Status

Future

Work done in the Géant2 project and TERENA TF-Mobility

Monitoring: usertracking & weathermap

UserTracking / - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

UT http://usertracking.surfnet.nl/php/radiuslist.php?setnum=1

SURF net UserTracking

Radius Log

Search

Time	User	Port	NAS IP	Type	Client
10:42:14 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Start	00001234abcd
10:40:57 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Start	0011223344ab
10:40:57 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Stop	0011223344ab
10:40:51 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Start	00001234abcd
10:40:51 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Stop	00001234abcd
10:40:35 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Stop	
10:35:02 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
10:32:42 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
10:29:50 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
10:28:25 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
10:10:53 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
10:09:36 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Start	
09:53:19 PM Aug 18th	fred@dutchie.org	123	1.2.3.4	Stop	
09:52:25 PM Aug 18th	fred@dutchie.org	0	1.2.3.4	Start	
09:52:05 PM Aug 18th	fred@dutchie.org	0	1.2.3.4	Stop	
09:49:01 PM Aug 18th	fred@dutchie.org			Stop	
06:48:10 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Start	0011223344ab
06:48:10 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Stop	0011223344ab
06:48:03 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Start	00001234abcd
06:48:03 PM Aug 18th	fred@dutchie.org	1234	192.87.116.250	Stop	00001234abcd

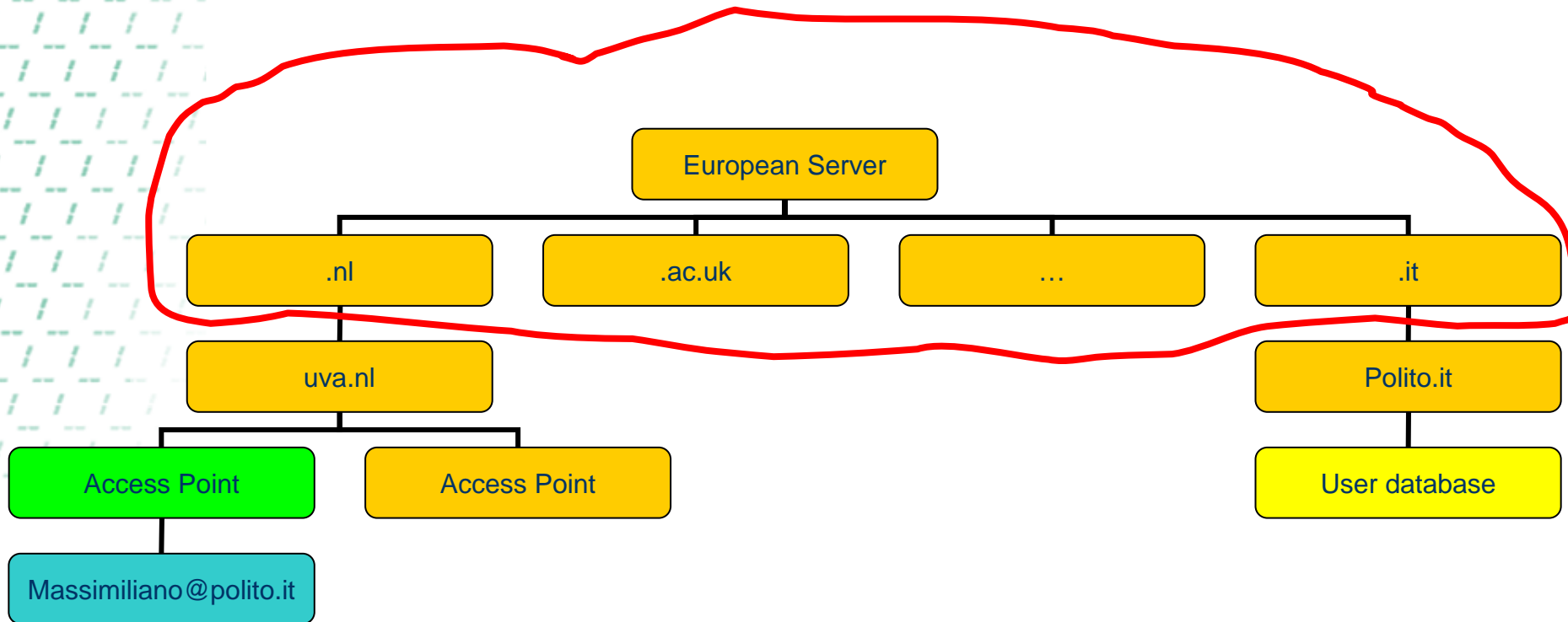
Home Menu Events Current MAC Historic MAC Radiator Online Admin Reports Help

http://usertracking.surfnet.nl/php/radiuslist.php?setnum=1&tableindex=MAC&sortBy=00001234abcd

Bereikbaarheid RADIUS-servers aangesloten instellingen

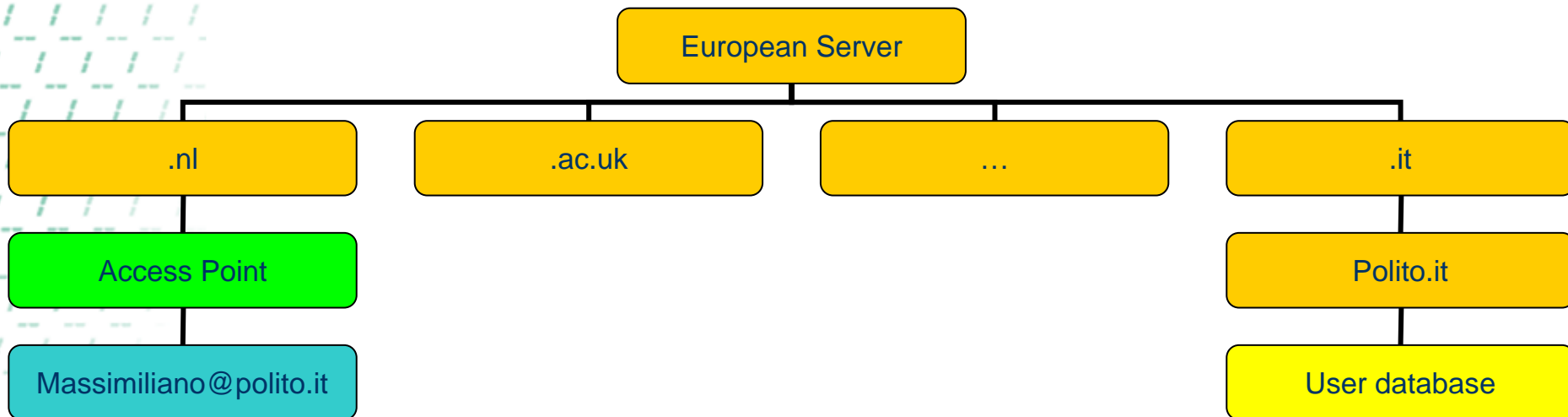
RADIUS	Via proxy: bobbiee.a3.surf.net		Via proxy: knifje.a3.surf.net	
	Status	Since	Status	Since
anon.nl	Requested Request Denied	01 Mar 2005 13:20:06	Requested Request Denied	01 Mar 2005 14:19:32
bagijn.nl	Requested Request Denied	21 Dec 2004 10:24:04	Requested Request Denied	21 Dec 2004 10:19:36
cheer.nl	No reply	21 Dec 2004 10:24:23	No reply	21 Dec 2004 10:19:56
eph.nl	OK	17 Dec 2004 14:03:31	OK	28 Dec 2004 10:20:28
ham.nl	No reply	21 Dec 2004 10:26:43	No reply	21 Dec 2004 10:20:35
hem.nl	Requested Request Denied	11 Jan 2005 14:16:06	Requested Request Denied	11 Jan 2005 14:20:38
hennard.nl	Requested Request Denied	21 Dec 2004 10:27:08	Requested Request Denied	21 Dec 2004 18:21:20
hkon.nl	Requested Request Denied	21 Dec 2004 10:27:16	Requested Request Denied	21 Dec 2004 10:21:22
hros.nl	OK	01 Feb 2005 14:16:25	OK	01 Feb 2005 18:20:57
huhrahand.nl	OK	18 Jan 2005 02:16:25	OK	19 Jan 2005 14:21:07
hvdvrouder.nl	No reply	21 Dec 2004 18:16:54	Requested Request Denied	01 Mar 2005 18:21:10
huy.nl	Requested Request Denied	22 Dec 2004 18:17:01	Requested Request Denied	22 Dec 2004 18:22:14
hys.nl	Requested Request Denied	21 Dec 2004 10:27:46	Requested Request Denied	21 Dec 2004 10:22:31
hys.nl	OK	17 Dec 2004 14:04:01	OK	23 Dec 2004 14:22:32
huzeland.nl	OK	01 Mar 2005 13:22:27	OK	01 Mar 2005 14:21:39
ichim-ke.nl	Requested Request Denied	21 Dec 2004 10:28:04	Requested Request Denied	21 Dec 2004 10:23:05
id.nl	Requested Request Denied	21 Dec 2004 10:28:13	Requested Request Denied	21 Dec 2004 10:23:14
idm.nl	Requested Request Denied	21 Dec 2004 10:28:22	Requested Request Denied	11 Jan 2005 18:22:59
idm.nl	OK	17 Dec 2004 14:04:12	OK	20 Dec 2004 18:24:22
hkon.nl	OK	17 Dec 2004 14:04:15	OK	20 Dec 2004 18:24:25
hvdvrouder.nl	Requested Request Denied	21 Dec 2004 10:28:36	Requested Request Denied	21 Dec 2004 10:23:47
is.nl	Requested Request Denied	25 Feb 2005 10:17:48	Requested Request Denied	25 Jan 2005 06:22:33
isoc-on.nl	No reply	29 Dec 2004 18:18:16	No reply	21 Dec 2004 10:24:26
isros.nl	Requested Request Denied	21 Dec 2004 10:28:58	Requested Request Denied	11 Jan 2005 18:23:40
istvan.nl	No reply	21 Dec 2004 10:29:17	Requested Request Denied	21 Dec 2004 10:24:55
isurf.nl	OK	17 Dec 2004 14:04:38	No reply	21 Dec 2004 10:25:16
isurfnet.nl	OK	23 Dec 2004 13:54:04	OK	05 Jan 2005 14:24:41
itn.nl	OK	26 Feb 2005 14:18:41	OK	26 Feb 2005 14:23:18
itn.nl	OK	02 Mar 2005 09:09:41	OK	02 Mar 2005 09:05:17
itn.nl	Requested Request Denied	11 Jan 2005 10:19:26	Requested Request Denied	11 Jan 2005 18:24:48
itn.nl	OK	15 Feb 2005 02:19:03	OK	15 Feb 2005 02:24:02
itn.nl	OK	11 Jan 2005 10:19:31	OK	21 Dec 2004 06:27:23
itn.nl	Requested Request Denied	15 Feb 2005 22:19:20	Requested Request Denied	15 Feb 2005 22:24:19

Bypassing the hierarchy overhead?



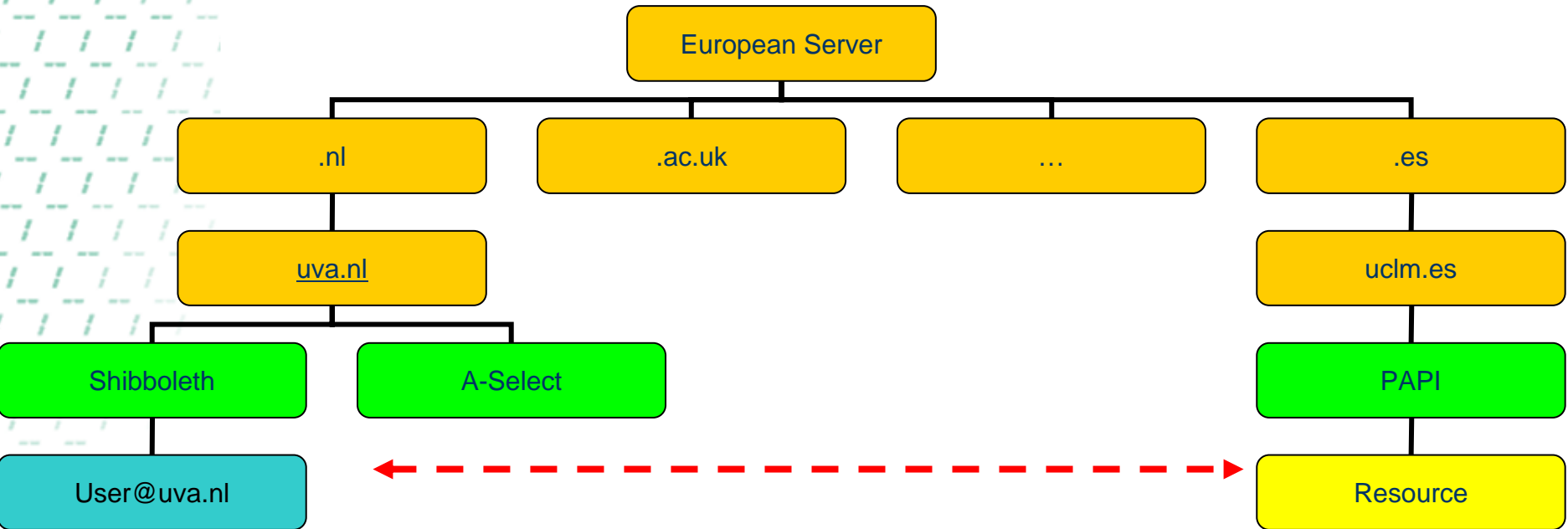
- AA traffic goes through all intermediate entries
- All links are peer-to-peer agreements / static routes
- DIAMETER? DNSsec? Shib?

Authorisation?



- Is Polito a university? How do you know?
- In general: How to pass attributes back and forth (SAML?)

Universal single sign-on?



- How do all these applications communicate? (SAML?)
- How can you protect credentials? Tunneled authentication?
- Should we want this?

Conclusions

- 802.1X plus RADIUS provide a secure and future proof solution for access to the institutional network
- But you might want to implement web-based or VPN-based too...
- Infra structure not perfect but...
 - It works TM
 - It is ready for the future
- Joining EduRoam is a small step for administrator-kind but a giant leap for the users, so.....

Time to join.....

The logo for eduroam features the word "eduroam" in a bold, sans-serif font. The "edu" is in black, and "roam" is in blue. Behind the text are several light blue, curved, overlapping shapes that resemble a stylized signal or a series of arches. The background on the left side of the slide has a light blue grid pattern.

eduroam

More information

- EduRoam in SURFnet
 - <http://www.eduroam.nl>
- EduRoam in Europa
 - <http://www.eduroam.org>
- TERENA TF-Mobility
 - <http://www.terena.nl/mobility>
- Géant2 Joint Research Activity 5 (authorisation and roaming)
 - <http://www.geant2.net/> (click on research)
- The unofficial IEEE802.11 security page
 - <http://www.drizzle.com/~aboba/IEEE>