

**TF-Mobility Meeting
18 January 05
Zurich, Switzerland**

Attendees list

Hansruedi Born	SWITCH
Rodrigo Castro	RedIRIS
Licia Florio	TERENA
Jan Furman	CESNET
Adrian Gschwend	University of Applied Sciences, Biel
Luis Guido	FCCN
Josh Howlett	University of Bristol
Antonia Kujundzic	CARNet
Diego Lopez	RedIRIS
Miroslav Mllinovic	Srce/CARNet
Marcin Michalak	Telscom
Ralf Paffrath	DFN
Spiros Papageorgiou	GRNET
Juergen Rauschenback	DFN
James Sankar	UKERNA
Lino Santos	FCCN
David Simonsen	UNI-C
Milan Sova	CESNET
Torbjörn Wiberg	Umeå Universitet
Klaas Wierenga	SURFnet
Stefan Winter	Fondation RESTENA
Tomasz Wolniewicz	Torun University/PIONIER

1. Welcome

The meeting was open by James Sankar and Klaas Wierenga who welcomed the participants and thanked SWITCH.

James announced to the group that due to his plan to move to Australia he cannot act as co-chair any longer. It was asked for a volunteer to replace James. David Simonsen from UNI-C volunteered. It was agreed to send an email to the list to inform people who were not present and see whether someone else volunteered.

At the time this minutes are being written, no other people volunteered therefore David was appointed as co-chair.

a. Deliverable D1

The task force charter states that the group will produce a report about performances and results achieved every six months.

ACTION: all to comment James first draft of the six months summary document on line at: (<http://www.eduroam.org/wiki/ActivitySummary?v=xou>)

2. JRA5 Update – Juergen Raushenbach

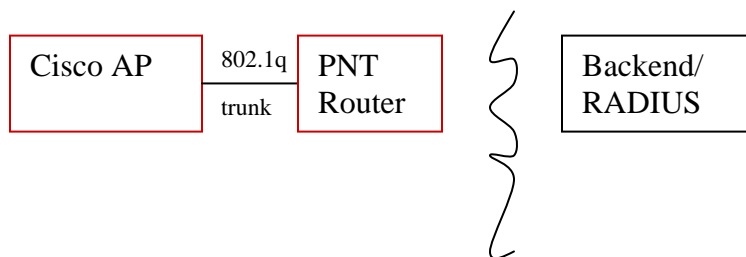
Juergen provided a summary about the JRA5 meeting which took place the day before.

JRA5, which started in September 2004 focuses on two areas: one exploring AA issues and the other exploring roaming issues.

Two deliverables have been produced: a glossary defining the AAI and roaming terms used by the group and a document which gathers the requirements for a roaming infrastructure.

The roaming part of JRA5 builds upon EduRoam to create an infrastructure that connects all the NRENs in Europe to EduRoam and adds AA features.

Ralf demonstrated what DFN are currently working on, which is a test based on Cisco router able to manage two SSIDs (one for VPN and another one for 802.1X). The Cisco access point is able to assign different WLAN to different users. The access point is connected to a PNT router, which redirects the connection to a WEB page in case the user gets connected using the VPN/WEB SSID or directly to a RADIUS server in case the users gets connected using 802.1X SSID. The picture below shows the components.



The mobility group is working to provide the elements that are in red in the picture above in one package. This solution called eduroam-in-a-box will reduce the configuration effort on the user side.

2. TF-Mobility update

An update about the activities of the group followed.

a. Feedback from the 1st VC/IM meeting

The group met in November 04 via videoconference. Minutes of this meeting are on-line at:

<http://www.terena.nl/tech/task-forces/tf-mobility/meetings/19-11-04/draftMinutesNov04v3.pdf>

A short discussion followed to understand whether the videoconference can be used again in the future. It was agreed that face-to-face are preferred, but when this is not possible videoconferences or phone conference can be arranged.

b. Eduroam and NREN participation

The SALSA FWG, operating under the umbrella of Internet2 have expressed interested in joining EduRoam. Klaas reported that he had some discussion with them and it seems likely that they will join the European top level Radius Server in June 2005.

Department of energy (DoE) in USA is using the RADIUS infrastructure to provide one-time password and would like to be able to use it for EduRoam as well. Some discussion is ongoing with them as well.

To date there are 15 NRENs that are part of EduRoam and AARNET which joined in December 2004.

Since December 2004 a EduRoam dedicated web site is available <http://www.eduroam.org/>. Klaas has set up a wiki server that is being used by the task force members to upload information.

It was suggested that all the NRENs that are part of the EduRoam to buy a domain eduroam.countrycode like Cesnet and Surfnet and other NRENs have already done. The idea is to provide as much information as possible on the EduRoam map available on the eduroam web site.

ACTION: April 1st all the countries that are in green on the map to set a local eduroam page. Namely: UNINET, Funet, Lanet, DFN, Carnet, Grnet, RedIRIS and GARR.

c. EduRoam Wiki (<http://www.eduroam.org/wiki/>)

Klaas showed the participants how to use the Wiki server. Wiki is being used by the group for a few months and since the beginning has proved to be a very handy tool to update documents. People who want to get an account should contact Klaas.

3. Update on work areas

Four working areas have been selected as core activity of the group. The updates about the results on each of the areas are available at:

<http://www.eduroam.org/wiki/HomePage>

a. Mobility Next Generation (Owner Miroslav Milinovic)

Two main tasks are part of this work package:

1. **Alternative approaches to RADIUS Hierarchy**, which tries to look into three main areas:

- a. *Information server* – to define procedures to retrieve the users' home institution.
- b. *Trust fabric* - to define how institutions can trust each other
- c. *Credential transport* - to define procedures to transport the users' credentials over the RADIUS hierarchy.

Possible alternative to RADIUS will also be explored. The reason to look for alternatives is due to way EduRoam currently works: the users' credentials are carried over the RADIUS hierarchy and there is at the moment no cache possibility, which means that all the time credentials have to travel along the all hierarchy. RADIUS servers share secrets with each other and it could be worth using some kind of PKI-based solution for this purpose.

- Possibility to use PKI to support RADIUS

In the current implementation of the eduroam hierarchy, trust is established along the RADIUS server chain. At the same time the credential are transported on the same hierarchy, which is to say that the hierarchy is used both to transport credentials and to establish trust.

Some possibility has been investigated to separate the trust from the credentials transport, in order to use the RADIUS hierarchy to establish trust (in a hierarchic way, which is more scalable) and to validate the credential in a peer-2-peer way.

The use of PKI to validate the credentials was discussed, which would imply to open some ports to allow for this.

ACTION: MS to rewrite the introduction for this work-package by 15 of March.

2. Operational issues, which tries to define policies about the use of the RADIUS infrastructure. The first step was to set up another the Top Level (European) RADIUS Server (*TLRPS*), maintained by UNI-C in Denmark, To date there is a TLRPS in the Netherlands and a backup in Denmark. The possibility of having a third top level server was discussed, but it was agreed that for the moment it is not necessary. The amount of traffic is not so high to require a third server.

Other two areas are part of this task, namely *LDAP* and *XML Configuration of RADIUS proxy servers*.

3. Managing and Monitoring use and abuse (Owner James Sankar)

It was agreed that Joshua Howlett will take responsibility for this working item, when James leaves.

The activity area focuses on a number of different issues identified as follows:

a. *RADIUS Monitoring*, which explores the *RADIUS availability, RADIUS authentication monitoring and ad hoc monitoring*.

Work has been undertaken to provide information about the National RADIUS Proxy Server (NRPS) availability status.

Miroslav showed what they use in Croatia to check for the status of various RADIUS servers.

ACTION: Miro to produce an English version of the site.

ACTION: Miro to provide a template to gather the same kind of information for the RADIUS server (end of February)

b. *RADIUS Management*, which explores *RADIUS configuration and accounting guidelines and RADIUS policy and procedure recommendations*.

Information about the tasks mentioned above are available on the wiki page (<http://www.eduroam.org/wiki/ManagingMonitoring?v=bv3>)

c. End Users Mobility (Owner **Klaas Wierenga**)

This area focuses on making it easier for end-users to access EduRoam and involves:

- *EduRoam web site* maintenance,
- *Access points phone book* (to know where to find the nearest EduRoam access point)
- *Location Based Service*
- *iPass* solution for NRENs.

SURFnet has prepared a proposal for an Access Point database that contains location information for the Access Points in EduRoam, available at:

<http://www.eduroam.org/wiki/AccessPointDB?v=rsl>

Marcin talked about the NOMAD project (<http://www.ist-nomad.net/index.php>) and a client on the PDA that is location-aware and using an ldap-server is able to locate services in the neighbourhood.

ACTION: everybody to provide comments about the database by end of February.

ACTION: Marcin to provide details for the phone book and template for the PDA.

David Simonsen gave an update about the use of iPass (<http://www.ipass.com>) and showed how it works. iPass, based on a propriety solution, is basically a phone book; a client needs to be installed on the user pc. There is no client for Linux yet.

Unfortunately the user-name length requested by iPass allows only for 32 characters, which are not enough to enter an email address or the realm used for EduRoam.

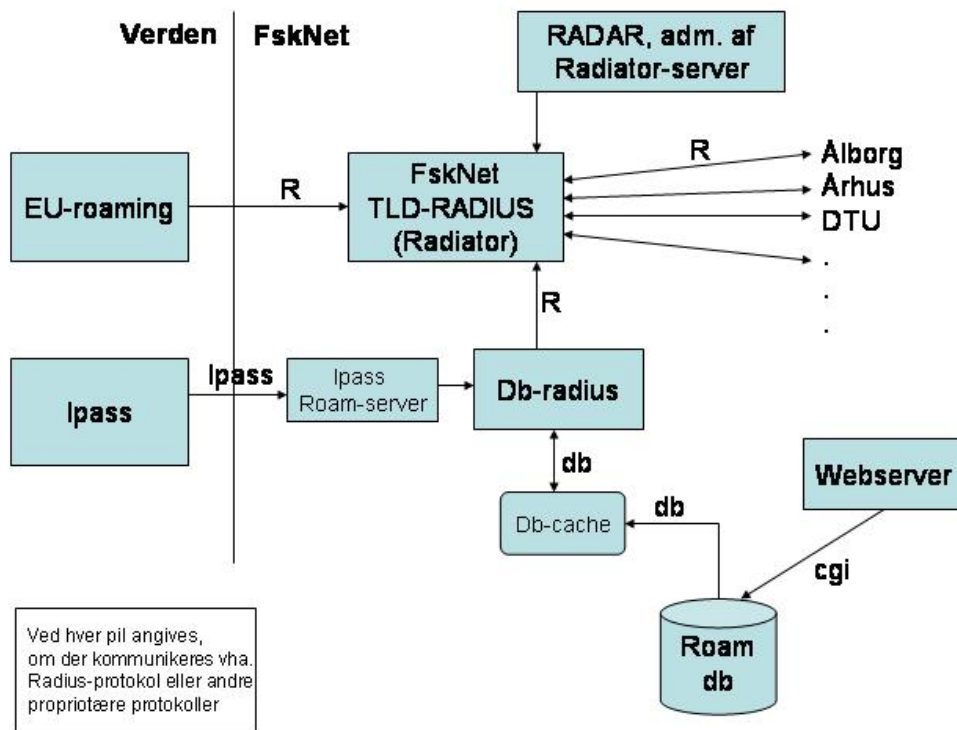
UNI-C (Denmark) has made a deal with iPass on behalf of the Danish institutions connected to the NREN. The research institutions will now be able to use iPass at a lower price and each institution will administer their own users using a web interface. UNI-C has bought one iPass client (with just one realm: '@fsknet.dk') for the whole NREN-community in Denmark. All users are registered with a special 'iPassID' in a database at UNI-C (administered by the institutions themselves).

The installed iPass-roam-server is connected to the RADIUS-hierarchy so that the users' passwords, normally used for roaming, is also used for iPass-authorization (a mapping from iPass-username to roaming-ID is performed). iPass would make their database available to the NRENs.

David's proposal is to create a client to integrate eduroam with iPass at European level, where Denmark would still be responsible for the bill at European scale.

The picture below depicts the way Denmark has combined the use of iPass with EduRoam.

ACTION: David to further investigate the proposal.



d. Deployment Issues (Owner Ralf Paffrath)

Hansruedi, currently the leader of this activity, will be leaving the group after the summer, so he sought for a replacement.

Ralf Paffrath has volunteered to take responsibility for this working area. Josh, Adrian and Marcin will contribute.

There two types of activities in this working area: EduRoam-in-a-box and EduRoam checklist for Eduroam compliance.

Hansruedi talked about eduroam-in-a-box. This proposal has some similarities with what Ralf from DFN presented. Two approaches are possible: a first approach would be to add the VPN/Web/802.1X capabilities in a box versus a second approach to look for a commercial solution.

Marcin circulated on the mailing list some days before the meeting the results of the work carried out by a student to do a similar thing.

The approaches proposed are listed below:

- Soekris, Linux-based box rather expensive, but easier to develop
- LINKSYS: SWITCH and UKERNA had some contacts with the company (which is a division of Cisco) that produce the box. In this case it could be possible to develop the product within the tf-mobility group as well as to ask the company to implement the specific functionalities.

It was agreed to provide first specifications in terms of what should be installed on the box, what kind of software should be used and so forth.

Klaas, Hans and James mentioned a meeting that had been organised to generate eduroam requirements. The list of what is needed is available on the wiki (<http://www.eduroam.org/wiki/DeploymentIssues?v=1910>)

After the requirements will be agreed and some test done, the type of box will be selected.

ACTION: all to comment and finalise these requirements (March 15th).

James demonstrated Linksys eduroam-in-a-box firmware.

SWITCH Update Hansruedi Born

Hansruedi gave an update about the SWITCH activities as far as roaming. SWITCHlan is the SWITCH backbone and all the universities are connected to. There is a commercial WLAN (PWLAN) provider that provides commercial hotspot. SWITCHmobile will try a pilot with 4 universities, in collaboration with PWLAN in order to provide bi-lateral access to both services. Students will be able to access the SWITCHmobile network as well as the PWLAN with no costs. When a user tries to access the system, he will have to choose if he is a commercial user or an academic user. In case of users not belonging to any university, they will access only the PWLAN network and they will be charged.

A.o.B

A final report to describe the results achieved by the group was prepared in July 2004. The report, available at:

<http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/TF-MobilityfinalReport.pdf>

The original idea was to have a hard copy of the original report to distribute. In a second moment it was thought that turning the report into a cookbook would have been more appropriate. To date nothing has been done yet.

Licia will produce a new version of the report by March 20th, which will be evaluated by Klaas, James, Juergen and David.

ACTION: Licia to produce a new version of the TF-Mobility final report (March 20th).

Next TF-Mobility meeting will be held in **Poznan** on **June 5th**.

