TERENA Technical Report

TF-Mobility

Inter-NREN roaming

Final Report

James Sankar – UKERNA
Klaas Wierenga - SURFnet

This report summarises the work of the TERENA Mobility Task Force that has been working on roaming network access solutions from January 2003 to June 2004. The Task Force investigated the requirements and delivery of a unique network access solution that would allow guest users hassle free network access using their own credentials to authenticate through their home institution. A number of participants from European National Research and Education Networks have collaborated regularly in the TF-Mobility Task Force. Since January 2003, the Task Force has met five times in face-to-face and videoconference meetings. The Task Force was formally closed in July 2004, but TERENA is still running the mobility@terena.nl mailing list while the follow-up Task Force activity is defined and created.

The information in this document is supported by TF-Mobility's website:

http://www.terena.nl/tech/task-forces/tf-mobility/

For Further information please contact:

TERENA Secretariat
Singel 468 D
1017 AW Amsterdam
The Netherlands

Tel: +31 20 530 4488
Fax: +31 20 530 4499
E-mail: secretariat@terena.nl
www: http://ww.terena.nl

Production: TERENA Secretariat
Editor:
Layout and printing:

Contents

1. Introduction

The TF-Mobility Task Force held its first meeting as a workshop in March 2002 in Amsterdam to identify roaming development activities across Europe and to determine whether there were any commonalities of approach that could lead to the formation of a Terena taskforce in mobility/roaming. Klaas Wierenga took the initiative in organising a workshop and subsequent meetings in Limerick, Ireland (June 2002) and Amsterdam (October 2002) that led to the agreement of a scope of work and draft the Task Force charter with a list of deliverables and associated timescales. A mailing list "mobility@terena.nl" was also set up and a website was created at http://www.terena.nl/tech/task-forces/tf-mobility/.

The draft charter was submitted to the TERENA Technical Committee on the 16 December 2002 and was approved to formally start in January 2003. Two co-chairs were appointed for the Task Force. Carsten Bormann acted as technical chair, James Sankar acted as process chair.

The aims of the TERENA Mobility Task Force were

- To provide a forum for exchanging experiences and knowledge, and to make the results of the work of the Task Force available to the research networking community and promote the benefits of the technology;
- To identify requirements to address security aspects and regulatory issues;
- To define and test an inter-NREN roaming architecture by:
    - evaluating possible authentication and authorisation techniques in mobile environments (e.g. Web-based redirection, RADIUS+802.1x, VPN) for the research community in Europe;
    - identifying the most suitable techniques, which will be standards-based, platform independent and use whenever possible infrastructures currently deployed in the NRENs;
    - describing the elements for a possible inter-NREN WLAN architecture based on these selected technologies;
- To implement and test the proposed architecture amongst the participant NRENs; Quality of Service will also be considered;
- To evaluate mobile equipment and software;
- To evaluate next-generation mobile technology for handovers and roaming (Mobile-IP(v4 and v6)); in this area TF-Mobility will work closely with TF-NGN and the 6NET working group on IPv6 and Mobility.

The objectives of the Task Force were:

- To identify requirements to address security aspects as well as regulatory issues
- To define and test an inter-NREN roaming architecture

- To evaluate mobile equipment and software
- To evaluate next generation mobile technology for handovers and roaming

2. Summary of results

TF-Mobility has carried out the following activities

Information site on the TERENA server

A dedicated web page was established that contained information about the Task Force (charter, scope, mailing list, meetings and deliverables). It was useful for coordinating meetings and disseminating relevant information (agendas, presentations and meeting minutes) to ensure the activities were transparent. A private area was also created so that active Task Force members could review early drafts of the deliverables and provide comments prior to publication of a finalised version.

Glossary

A glossary was created as an early deliverable to ensure a common understanding of terms could be agreed amongst the various NREN representatives to ensure that subsequent deliverables were consistent in the use of terms to describe work undertaken. The glossary was initially based on technical terms but it soon was realised that non technical descriptions such as guest user, home institution etc. also needed to be defined to avoid misunderstanding in the production of deliverables. As a result, a second list of non-technical terms was duly written. Both technical and non-technical terms were agreed and merged into the later versions of the glossary deliverable.

Requirements definition

The Task Force members agreed and documented a requirements definition for inter-NREN roaming based on their experiences of developing and hosting national roaming solutions. A set of major and minor requirements were agreed. These requirements were pragmatic and agreed as achievable within the timeframe of the Task Force.

The major requirements were

The scalability of the proposed solution must be maintained and the administrative overhead must be minimised
The required security must be maintained for all partners in the process.

The minor requirements identified were

The usability must be good for all needed/used platforms
Accountability and logging functionality must be provided to track abuse.

It was also stated that where requirements were not possible a reasonable trade-off should be found. This deliverable then explored each requirement in more detail.

Inventory of web-based redirection network access to roaming requirements

An inventory was undertaken of a national roaming solution that was based on web-based redirection to an authenticating login page at FUNET. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming.

Inventory of 802.1X based network access to roaming requirements

An inventory was undertaken of a national roaming solution that was based on an 802.1X national roaming solution at SURFnet. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming.

Inventory of VPN based network access to roaming requirements

An inventory was undertaken of a national roaming solution that was based on a VPN national roaming solution at SWITCH and the University of Bremen. A description of the roaming solution was undertaken and details about the solution were compared with the major and minor requirements outlined in the requirements definition deliverable to ascertain how closely this national roaming solution met the requirements for inter-NREN roaming. This deliverable also proposed a scalable VPN solution for inter-NREN roaming called "Controlled Address Space for VPN gateways" and recommended that proof of concept tests be undertaken to determine its feasibility.

Preliminary selection for Inter-NREN roaming

This deliverable reviewed all three inventories and included a late submission from a fourth roaming solution "Roamnode" developed at the University of Bristol in the UK.

A detailed review and comparisons of all the national roaming solutions revealed that there was no single solution that met all the requirements identified by the Task Force, nor was any solution more dominant over others. The deliverable concluded that a solution be developed that could support a variety of national roaming solutions instead. The deliverable then considered in detail the design aspects for

A RADIUS proxy hierarchy,
A Controlled Address Space for VPN Gateways hierarchy
Software enhancements to the Roamnode.

Results of some early development test beds were also included in this deliverable.

Test bed and reference design for inter-NREN roaming

This deliverable considered the technical issues and work required at the NREN and organisational site level to create an interoperable environment where guest users from either a web redirection, 802.1X or VPN national roaming infrastructure environments could gain network access at any visited organisations regardless of the roaming solution preferred there.

This deliverable highlighted the following nine scenarios and additional work and .or equipment needed to support other guest users.

Site uses \ User with	802.1X	VPN	Web-based
802.1X	Okay	Work reqd	Work reqd
VPN	Work reqd	Okay	Work reqd
Web-based redirect	Work reqd	Work reqd	Okay

In addition a separate section detailed ongoing proof of concept tests and scaled trials of the Controlled Address for VPN gateways concept.

Roaming Policy - draft guidelines

As all national roaming solutions rely on fostering trust between participating organisations and given the take up in participation in the three tier (European (TERENA) - National - Organisational) RADIUS proxy hierarchy, there was a need to develop a policy and standards so that inter-NREN roaming solutions could scale and be managed easily. This deliverable provided guidelines for Inter-NREN roaming that NRENs needed to agree in order to join the TERENA level RADIUS server.

A web repository of tests on Wireless LAN devices

This deliverable was a comprehensive overview of wireless networking (WLAN Standards, the Workings of Wireless, Wireless and the Law, Wireless Security and known wireless problems) and also a detailed repository of wireless product tests and comparisons between different wireless products.

Impact of new technology and protocols such as IPv6 and MobileIPv6 on current roaming work.

This report (still to be finalised at the time of writing, as the last deliverable), describes the issues arising from availability of new protocols, in particular IPv6 and Mobile IPv6, for the roaming solution. Most NRENs now have a production IPv6 service on their backbones, as does GEANT. We can thus expect a slow but steady take-up of IPv6 support in campuses in the near future. This document describes how the proposed roaming solutions(s) work (or do not work) in an IPv6 environment, as well as new considerations for IPv6, especially MIPv6.

3. Dedicated website

The Task Force has created a public and private website and a mailing list with approximately 150 subscribers.
The web site is available at:
http://www.terena.nl/tech/task-forces/tf-mobility/ .

It contains information about meetings, deliverables and other related activities.

4. Glossary

- Written to ensure a mutual understanding of technical terms (such as standards) and terminology used by people
- To be a reference for deliverables and ensure a consistent use of terms.
- Revised on a regular basis to review descriptions and add new items.
- An online version is available at: http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelB/DelB_v1-3-5.pdf

The glossary is attached at the end of the end of this publication to help the readers.

5. Requirements definition

The requirements definition deliverable was necessary to define the scope of work. It also provided Task Force members with an opportunity to identify and agree on major and minor requirements.

Once the requirements had been defined, the Task Force used them to objectively assess each national roaming solution to determine its suitability as an inter-NREN roaming solution.

This deliverable provided a structure to document each national roaming solution and highlighted common issues such as security, scalability and policy matters for further consideration.

The requirements identified and agreed were as follows

Major requirements:

- The **scalability** of the proposed solution must be maintained.
- The **administrative overhead** must be minimised.
- The required **security** must be maintained for all participating institutions in the process.

Minor requirements:

- The **usability** must be good for all needed/used platforms.
- The **functionality** (service access) should be as complete as possible
- The **accountability and logging functionality** must be provided to track abuse.

A number of general and specific observations, vulnerabilities and limitations were also identified as follows.

1. If a visiting or local user's credentials (username and password) are stolen and another user is granted access using these credentials to authenticate with the victim's home institution, is the home institution or the "victim" liable for not informing the authorities promptly? Also, can the user who stole the credentials be traced?

2. An authentication method that relies on a chain of RADIUS referrals may suffer additional latency beyond one that is local. It is also subject to failure if any part of the chain is broken (an unavailable server, or a network failure, for example). It is also important to ensure that authentication packets passed between RADIUS serves are not transferred by the default "clear text". If the network can be trusted, a shared RADIUS secret could be used to improve security. If the network is cannot be trusted, use of IPSec can be considered.

3. A VPN-based solution where the visiting user establishes a VPN connection to their home institution implies that all VPN traffic is routed from the user's current location back to their home VPN en route to the real destination. This may cause additional latency and could place a significant bandwidth load on the VPN server, especially if a high volume of high capacity VPN links are being served.

4. While not all network traffic needs be routed via the users home VPN (just traffic destined for the home network may suffice) this may not be possible if the visited site only allows traffic out from its Wireless LAN when it is encapsulated in a tunnel to a "trusted" VPN gateway.

5. Some services are offered to institutions on the basis of observed source IP address. VPN users will have the benefit of appearing to come from their home institution, and thus be able to access such services as if at their home network.

6. VPN users may often be treated as internal to their home network. It is possible that while visiting "untrusted" WLANs that some virus or worm infections may be picked up that may then be relayed to the home network. Home site administrators should bear such risks in mind when setting site security policies.

7. Local authentication schemes should be able to differentiate between locally and remotely authenticating users, such that different levels of access to local

(or remote) resources can be offered based on whether the user is local or a guest.

8. There is an intention to migrate to IPv6 in the future, to take advantage of features including the larger address space. Most NREN's already have IPv6 deployed natively (dual-stack) on their backbone networks. It is expected that most universities will begin connecting natively in the near future; tunneled IPv6-in-IPv4 access may be used as an interim access measure. Roaming solutions should include IPv6 functionality from the earliest opportunity, e.g. IPv6 support in RADIUS servers.

6. Inventory of 802.1X network access to roaming requirements

This section provides a brief summary of the inventory produced by SURFnet on their 802.1X national roaming solution. 802.1X was ratified by the IEEE in September 2001[1] and is a layer 2 authentication solution between a mobile device and an access control device. Both wireless and wired networks are supported. 802.1X is used to control the network access at the edge of a network.

In 802.1X, the access control device can also detect the disruption of the connection and close the port if for example a cable is pulled out on a wired link or a wireless node leaves the coverage area of the wireless network. 802.1X authentication information is carried over the Extensible Authentication Protocol (EAP) for wireless or Extensible Authentication Protocol over LAN (EAPOL) for both wired and wireless access. Since there is no layer 3 access method, layer 2 needs to be encapsulated hence the use of EAP on LAN between the client and access control device, switch or authentication server.

This network access technology is different from other AAA schemes because authentication modules can be plugged in to cater for specific needs. If a RADIUS (Remote Access Dial In User Service) server is used, this server should support the Extensible Access Protocol (EAP). EAP can carry a number of authentication protocols, such as Transport Layer Security (EAP-TLS) or Tunnelled Transport Layer Security (EAP-TTLS). Since the ratification of 802.1X, there have been an increasing number of 802.1X client software solutions that have become publicly available. It is reasonable to expect that 802.1X implementations will continue to grow and harden in the next couple of years.

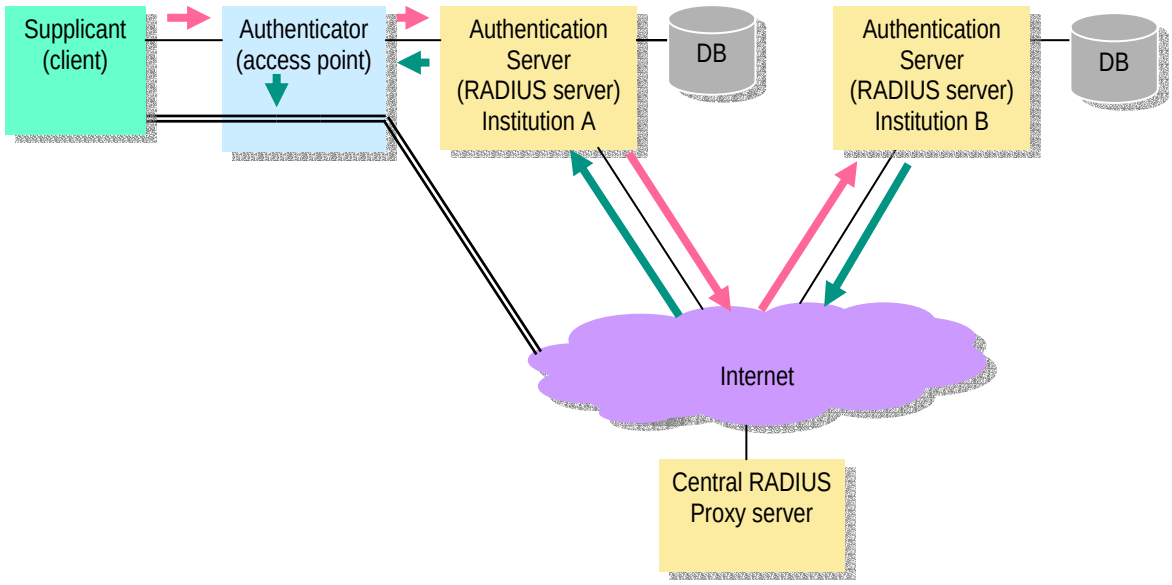


Figure 1: A diagram showing the 802.1X solution for roaming guest access.

[1] See http://standards.ieee.org/getieee802/download/802.1X-2001.pdf and http://www.ieee802.org/1/pages/802.1x.html contains pointers to more information (the MIB and the revisions to the standard).

Level of administrative overhead

Each Wireless LAN must have appropriate 802.1X client software installed; many newer operating systems now support 802.1X as standard, e.g. Mac OS/X. A table showing current support was included in the full deliverable.

When a new institution requests participation to roaming services, only its realm has to be entered into the National RADIUS Proxy Server, not into the servers of other institutions, because referrals to those institutions are relayed through the National Proxy. Therefore from the institution viewpoint, scalability is achieved without administrative overhead.

Level of user transparency

The visiting user will initially require 802.1X client software to be installed and/or configured onto the client device. When a visiting user wants to gain network access, the visiting user will be asked to enter their credentials (user@realm.topleveldomain)[2], and once authenticated at their home institution, the visiting user can move freely from one wireless network to another, while their mobile device remains connected to the 802.1X enabled networks without additional user or administrative efforts.

If a visiting user tries to connect to a visited institution network, the RADIUS server at that institution will not recognize the visiting user credentials, as the visiting user's realm is not recognised. When this happens, the RADIUS proxy mechanism ensures that the EAP encapsulated credentials get transported towards the home institution RADIUS server. The visited institution RADIUS server only has to know where to send unknown visiting user credentials and their requests to, in order to be authenticated.

Security

The IEEE 802.1X standard for port-based authentication is a layer 2 solution between a mobile device and an access control device. In the 802.1X framework, authentication information is carried over EAP; this enables the use of various authentication methods[3] that were mentioned earlier. Access control devices communicate with a RADIUS backend for visiting user verification; this is generally secure and scalable. After authentication, the communication between the mobile device and the access control device is encrypted using dynamic keys.

[2] The format of the credential needs to be defined, agreed and formalised in deliverable H.

[3] Username/password, certificates, OTP (One Time Password, f.i. via SMS) or credentials on a mobile operators' SIM-card. These mechanisms are implemented in the EAP types MD5, TLS, TTLS, MS-CHAPv2, PEAP, Mob@c and EAP-SIM.

As long as a strong EAP capable protocol like TLS is used, 802.1X provides a framework that gives a sufficient level of security for the intended purpose, i.e. access control to the home institution network. Tunnelling protocols such as PEAP and TLS and TTLS can be configured to prevent “Man in the Middle” attacks because both the server and the client can validate each other using certificates.

If a security incident occurs, RADIUS can quickly and flexibly block access to a particular user@realm or requests from the particular realm. Once the incident has been resolved, the realm can be unblocked just as easily.

Scalability

SURFnet has adopted a hierarchical RADIUS backend for user authentication. This solution only works if the mobile device, the access control device and the RADIUS server (in SURFnet’s case) support EAP.

7. Inventory of VPN based network access to roaming requirements

This section provides a brief summary of the inventory produced by SWITCH on their VPN national roaming solution called SWITCHmobile that interconnects 12 Universities and research institutions.

The University of Bremen has a similar roaming system called Wbone that has been deployed across 5 academic organisations. For clarity the following section summarises SWITCHmobile only.

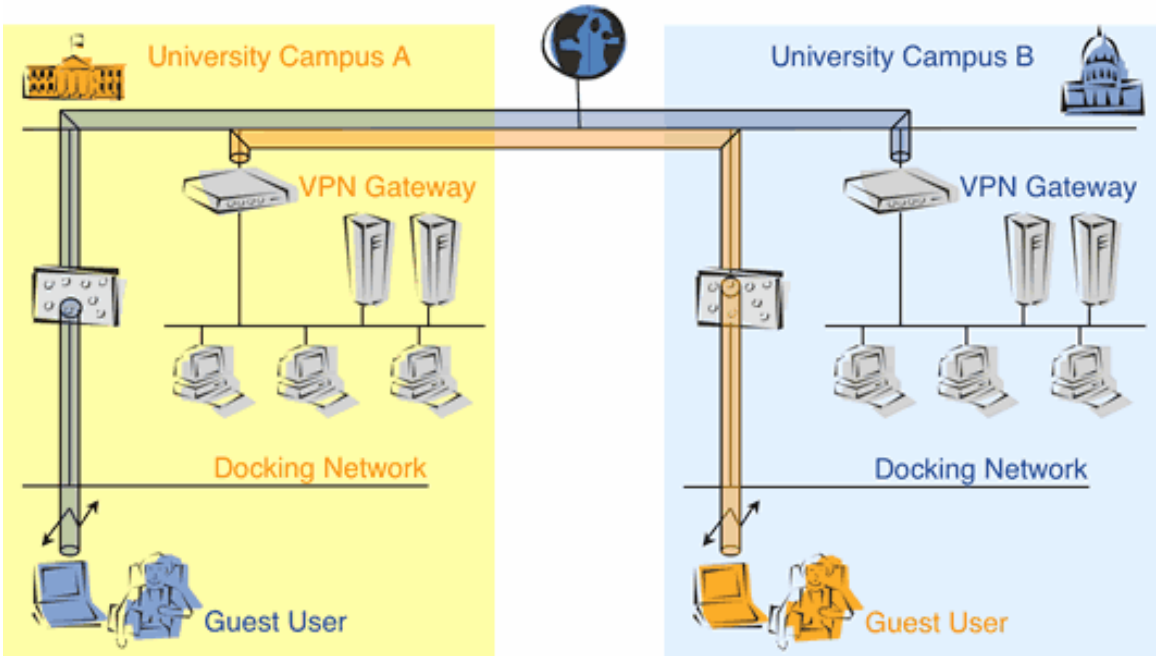


Figure 2: A diagram showing the VPN solution for roaming guest access.

Visiting users can connect to docking networks. These networks are “open“, i.e. users are not required to input any credentials in order to get basic connectivity. The networks are designed to make it as easy as possible for the users to connect to the network and receive an IP address.

However, at this stage users won't have access to anything interesting yet (like resources on the Internet or at the home organisation). Access is granted exclusively to a list of all the VPN gateways of the participating organisations (including the local organisation VPN server(s)). This restriction is implemented on access control lists at the docking network. They deny any traffic except from packets that go to one of the listed VPN gateways.

In order to proceed, users have to initiate a VPN tunnel to the VPN gateway of their home campus and get properly authenticated there. Once a VPN session has been established successfully, users can use the Internet (via the VPN gateway at their home organisation) as well as resources at their home campus.

Level of administrative overhead

The administrative overhead consists of updating the central list of trusted VPN gateways when a gateway is added or its address is changed. Whenever this happens, all the site administrators have to be notified about the change and they must adapt their local ACLs accordingly. The process of notification has been automated and adapting the ACLs might also be automated by the individual organisations.

Level of user transparency

Users use VPN connections wherever they go, thus the method is transparent wherever they are (assuming the visited site supports VPN access, and does not have NAT or other firewall restrictions – other participating sites in the roaming environment will offer such support).

Security

VPNs (at least those based on IPsec) are considered highly secure for data in transit. Devices will be considered inside their home network, and thus administrators should be aware of the risks of “infected” devices causing problems when connecting over a VPN.

Scalability

The solution presented here is suitable for a limited group of organisations (e.g. all universities in Switzerland) but not suitable for a European scale. In order to overcome this limitation, the Controlled Address Space for VPN Gateways (CASG) has been proposed (for details, see the proposed approach section of this document).

8. Inventory of web-based redirection network access to roaming requirements

This section provides a brief summary of the inventory produced by FUNET on their web-based redirection national roaming solution.

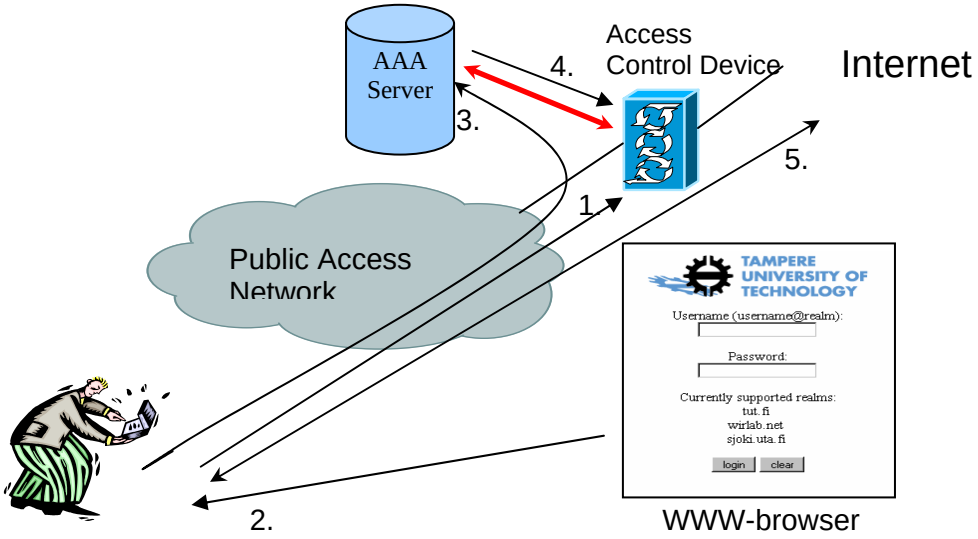


Figure 3: A diagram showing the web-based redirection solution for roaming guest access.

To gain access outside of the visited institution network, the visiting user must launch their web browser (we assume they have one) which will be automatically redirected to an authentication web page (1), the access control device manages this process by capturing the HTTP connection and redirects the user's web browser to an authentication page (2).

On the authentication page a web form appears where the visiting user must enter their user credentials (e.g. username and password[4]). This can be done over an SSL connection for password security. The access control device will then authenticate the visiting user at the user's home institution based on their credentials (3) e.g. using RADIUS. If the authentication succeeds (4) the access control device modifies the firewall rules (5) to enable the visiting user to gain access outside of the home institution network. If the authentication fails, an authentication error is returned to the visiting user and the credentials are asked for again. The amount of failed authentication attempts can be limited.

[4] In commercial deployments, "scratch cards" can offer a password valid for a period of time, or a valid password may be sent as an SMS text message to a visitor user.

Level of administrative overhead

Local Access Control Lists may need to be updated so that visiting users are forwarded to an authentication page to enter their credentials. These credentials are then forwarded to a RADIUS proxy server and transferred across a hierarchy of RADIUS proxy servers back to the visiting user's home institution to authentication with the home institution authentication server. Work may also be required at the national level RADIUS server to redirect credentials via another institution's RADIUS server or another NREN level RADIUS server.

Level of user transparency

User transparency will be high, as the user only requires an http(s)-based web browser. These are normally installed in all operating systems as standard. There is no additional client software or configuration required at the user end.

Security

This solution is less secure because it is based on using MAC-address and IP-address pairs where the attacker must be able to change a network interface card's MAC address to an authorised MAC address to gain access. Though not impossible, this solution does restrict security breaches to only skilled and/or serious hackers and not typical users.

Scalability

The Finnish web redirection solution is similar to 802.1X in terms of scalability in that it relies on a hierarchy of RADIUS Proxy servers behind a web proxy handler or the control device to forward authentication requests to a visiting user's home institution, thus solving any scaling issues. The web redirection authentication solution differs slightly from 802.1X in that it uses an http or (preferably) https web page interface for visiting users to input their credentials that are forwarded to their home institution server rather than at the access control device.

9. Roamnode Authentication solution

The Roamnode is an access control device developed at the University of Bristol to provide a low cost solution that fits into the existing network and authentication infrastructure, without complex requirements. The original intention was to only provide secure wired, wireless and remote access for local users; however, the architecture has developed to allow scalable and seamless roaming between trusting institutions.

The primary design goal of the Roamnode architecture is to de-couple the processes of establishing a physical network connection from the process of establishing a logical network connection. The reason for de-coupling is that each process is the responsibility of a different institution, and each has very different responsibilities. The first process - establishing a physical connection - is the responsibility of the visited institution. The second process - establishing a network connection - is the responsibility of home institution.

The second design goal of the Roamnode architecture is to use very simple interfaces between each component or layer of the protocol stack. This allows a protocol or a mechanism to be easily complemented or replaced with an alternative without disrupting the rest of the system. For example, the Roamnode currently uses the PPTP VPN protocol, but this could be changed to any other VPN protocol that is transported over IP.

The final design goal of the Roamnode architecture is to provide a vertical solution that allows higher layers to interact with lower layers; for example, to deliver location-aware applications, or to allow applications to disconnect users or to query and alter a user's bandwidth allocation.

Level of administrative overhead

An institution that deploys the Roamnode architecture and peers with the NREN’s national RADIUS proxy server can provide a seamless mobility service, either as a visited institution or as a home institution, without any additional administrative effort.

An overlay network has been created to avoid the need to allocate visitors with public IP addresses prior to establishing their VPN connections to their home institutions (these addresses would need to be public to allow Internet routers to make routing decisions for visiting users' VPN sessions). This is because these public IP addresses would need to be allocated from the visited institutions allocation, which would therefore violate the Roamnode architecture's primary design goal. It also allows institutions with limited or no available public IP address space to participate, without needing to use NAT (although allocation and use of such address space needs to be coordinated).

The mobile device can only connect to the visiting user's VPN gateway via the IP-in-IP tunnel that is built between a Localnode and Homenode when the RADIUS

ACCESS-ACCEPT packet is returned to the Localnode. This tunnel is built when a visiting user requires connectivity between the Roamnodes, and torn down when the visiting user no longer requires the tunnel. The process is entirely automatic, no management or configuration of the overlay network is required: it is built entirely on-demand.

Level of user transparency

The username and password needs to be entered to authenticate. This is the visiting user's home institution username and password and the username must be unique. Roamnode is designed to be entirely transparent to the visiting user as this user is allocated an IP address from their home institutions, so all applications would work as if that user was gaining network access physically at their home institution.

Security

A visiting user can connect to a visited institution's network only if the visiting user credentials are authenticated by the home institution that is trusted by the RADIUS back-end. This connection provides the minimum connectivity to establish a VPN session with the visiting user's home institution.

The Roamnode architecture has exact knowledge of every visiting user's name and home institution from the moment that the mobile device connects (this is because the home institution is explicit in the realm). Hence, visiting users are easily traced to their home institution. A central registry of realms and contacts could be maintained on a website to assist in liaising with other institutions. Another option would be to include a RADIUS attribute in the RADIUS transactions that describes a contact address for that institution.

The Localnode only allows the mobile device to send packets to the visiting user's Homenode, and only forward's packets to the mobile device that have originated from the visiting user's Homenode. This prevents a visiting user from using the service for any other purpose other than connecting to the visiting user's VPN gateway.

Only a cryptographic hash of the visiting user's password is passed to the Localnode, and not the password itself. Therefore, it is not possible to acquire credentials of a visiting user by sniffing the visited institution network, or by a malicious third party masquerading as a trusted authenticator. The Localnode also authenticates itself to the mobile device by passing it a second hash returned from the user's AAA server. The mobile device will not establish the connection to the Localnode unless the hash is correct. Thus trust is established in two directions.

Scalability

In the Roamnode architecture the visited institution does not need to provide any of its own address space to visiting users. This is because visiting users are simply allocated an RFC1918 address from the Localnode's allocation to allow them to connect to their home institution VPN gateway across the mesh network. The Roamnode can reside

behind a properly configured firewall performing NAT, enabling organisations that have a limited number of public IP addresses to participate.

The Roamnode architecture does not require edge hardware that can be quite expensive[5]. The Roamnode could be run on a redundant PC for example. A single Roamnode can handle several hundred simultaneous sessions. Roamnodes can also be clustered to create a "virtual" Roamnode, which can handle very many more.

If the volume of connections running through a given VPN becomes a problem, bandwidth limitations could be applied per connection.

[5] This is not exclusively so as HostAP (Linux free AP) supports 802.1X

10. Preliminary selection for Inter-NREN roaming

This deliverable provided an overview of each national solution and compared each against the defined requirements. The conclusions reached were as follows
The TF-Mobility group confirmed that there was no single national roaming solution that was suitable for inter-NREN roaming. Instead the Task Force agreed on the need to develop infrastructure to ensure interoperability between national solutions could be achieved bearing in mind the need to meet the majority of the requirements identified in earlier deliverables. As an aside, the Task Force decided not consider the following in their work

Local - VPN: VPN users will not be able to access a visited institution's VPN gateway because although it is technically possible to offer access to all VPN servers, this would not be practical as all participating institutions would have to purchase a VPN server for this single purpose
PKI: It would be good to have PKI when it is ready; currently it is not and would be complex to manage. Given the limited lifetime of TF-Mobility, PKI will not be considered. When PKI is ready, the group agrees it would consider the merits of migrating to such a solution.

This deliverable outlined in technical detail a design for interoperability between 802.1X, web-based redirection and VPN solutions. It highlighted nine scenarios and additional work and or equipment needed to support other guest users.

Site uses \ User with	802.1X	VPN	Web-based
802.1X	Okay	Work reqd	Work reqd
VPN	Work reqd	Okay	Work reqd
Web-based redirect	Work reqd	Work reqd	Okay

These designs were to be tested with results documented in a preceding deliverable. A phased development and testing programme was recommended and can be seen as follows: -

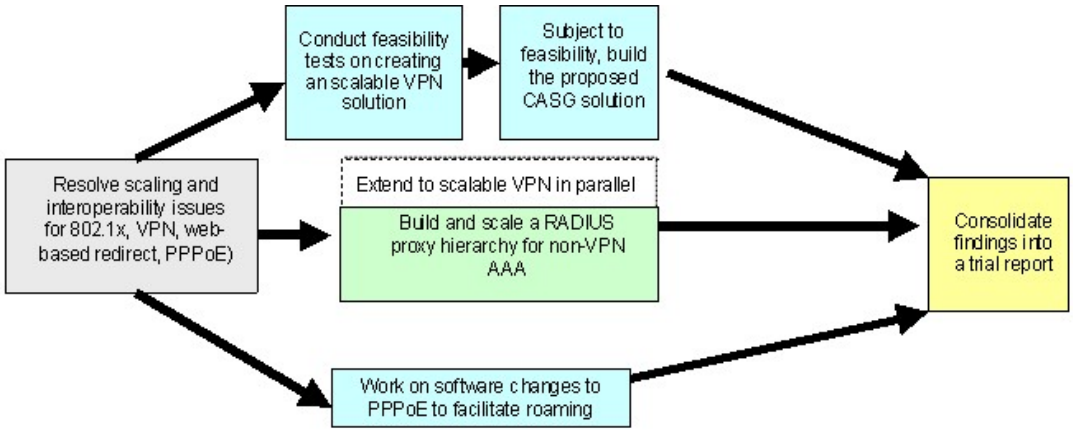


Figure 4: A diagram showing the recommended approach to develop interoperable roaming guest access.

The group's main aim is to bring each of the three streams of work as closely together as possible, ideally so that they can interoperate with each other.

TF-Mobility group members have successfully developed a RADIUS backend approach between a number of NRENs and SURFnet using a Radiator RADIUS proxy server hierarchy. In addition, deliverable H has successfully tested different network access methods over the RADIUS proxy hierarchy. In addition, a draft policy document has been created for deliverable I that includes an agreed user@realm format and a list of minimum requirements for protocols carried by EAP for NRENs and participating institutions.

The RADIUS Proxy hierarchy is currently in place and is growing in terms of NREN participants and institutions. The current status at the time of writing is as follows

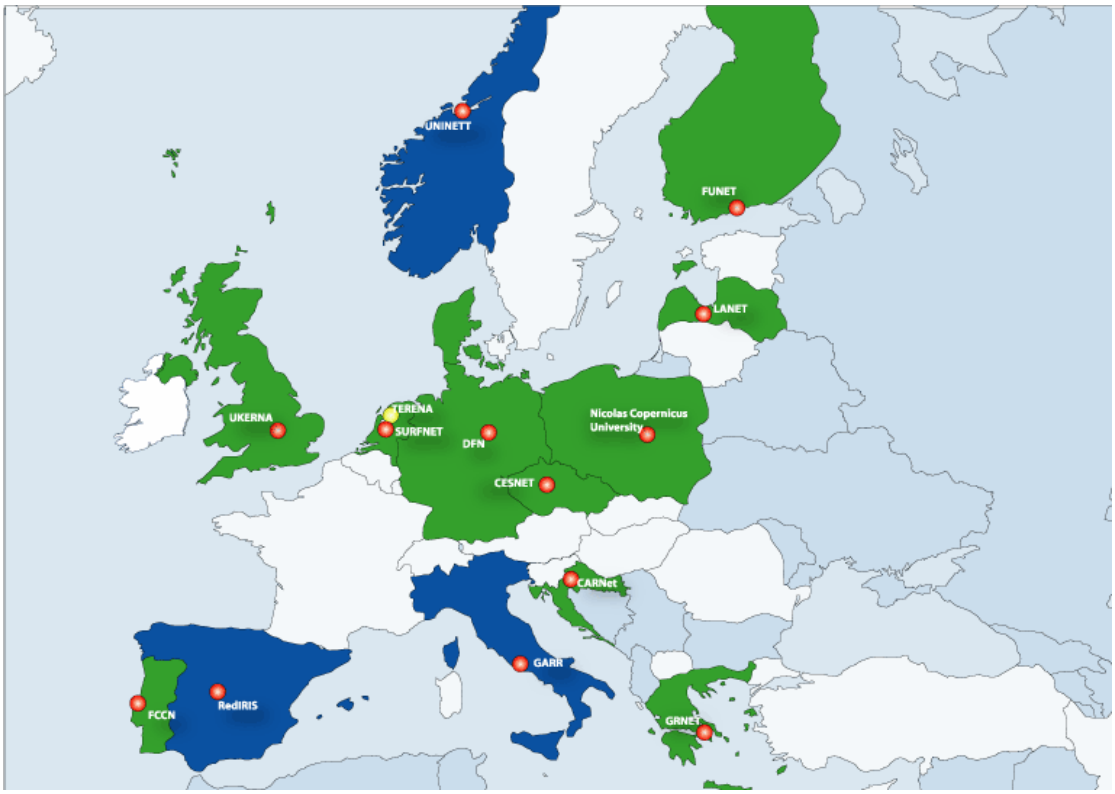


Figure 5: Current participants in the European RADIUS hierarchy (July 2004) (note: countries highlighted in blue are in the process of joining whilst those in green have already joined).

The Task Force has also recognised the need for policy guidelines to ensure the RADIUS proxy hierarchy is both manageable and scalable and also to protect and foster trust amongst participating institutions. This work has been completed in a later deliverable.

A proposed solution to solve the VPN scalability problem is to develop a new concept called Controlled Address Space for VPN Gateways. CASG are IP address ranges that each NREN has to obtain for themselves for their VPN gateways. In this way the

packet exchanging between the CASG network and the VPN gateway should be secure.

The diagram below describes the proposed architecture for a scalable wireless roaming VPN solution.

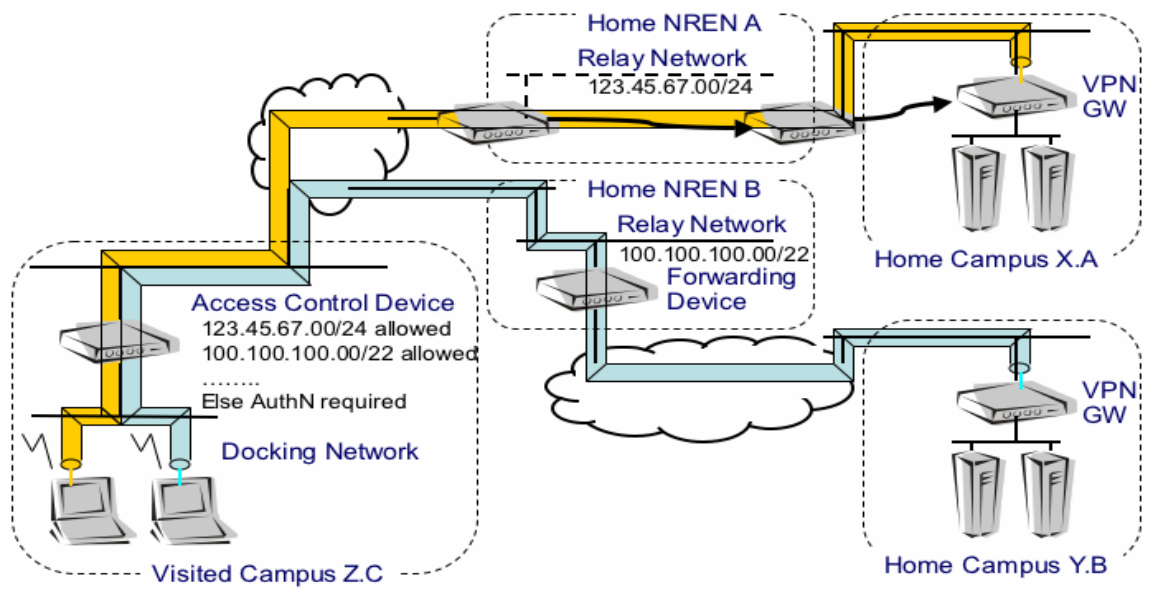


Figure 6: A diagram showing the scalable VPN solution for roaming guest access based on Controlled Address Space for VPN Gateways.

Development work in this area was undertaken in parallel to RADIUS interoperability testing. CASG pushes complexity away from the ACL lists in the site edge devices into the routing infrastructure of the NRENs; it is not clear how desirable or practical this solution is, on a larger scale.

The Roamnode (PPPoE over Linux) solution is an independent solution that has been developed at Bristol University. The Task Force recommended additional work to the Roamnode software to achieve interoperability with other national roaming solutions and tests thereafter.

11. Test bed and reference design for inter-NREN roaming

The original intention for this deliverable was to describe the architecture of the selected inter-NREN roaming solution. However, the “Preliminary selection for inter-NREN roaming” concluded that there will be no single national solution recommended as the European model. This is because no one solution outperforms all the others. Each solution has a number of strengths and weaknesses making such choices difficult. In addition there has been a considerable investment made to develop a variety of national solutions and there is a low likelihood that NREN’s will abandon their solutions in favour of a single, proscribed European model.
Therefore the deliverable has instead been focusing on ways to make the three main solutions (802.1X-, Web-redirect-, and VPN-based) interoperate. That is to say, to try to ensure that visiting users that use another solution can still authenticate at the visited institution, even though this solution is not offered to the home institution’s users.

The three major approaches have some characteristics that need to be taken into account when creating an interoperable solution. 802.1X based authentication is inherently different from Web based redirection and VPN-based authentication due to different demands on the wireless LAN networks. 802.1X enabled wireless networks require an encrypted channel (with dynamic WEP-keys), whilst the two other mechanisms are based on the concept of open, unencrypted access to the docking network. On the other hand the CASG approach for VPN-based access can not use a RADIUS backend whilst the other two solutions do require this. So the following situation exists:

Approach / Technology	802.1X	VPN	Web-based
encrypted radio	Yes	No	No
RADIUS backend	Yes	No	Yes

The result of these contradicting requirements is that in order to support both types of network authentication two logically separated networks on the radio layer need to be constructed. In the case of an access point it means that the access point must be capable of using multiple SSID’s and can support (multiple) VLAN assignment. An example can be seen from the following docking network configuration:

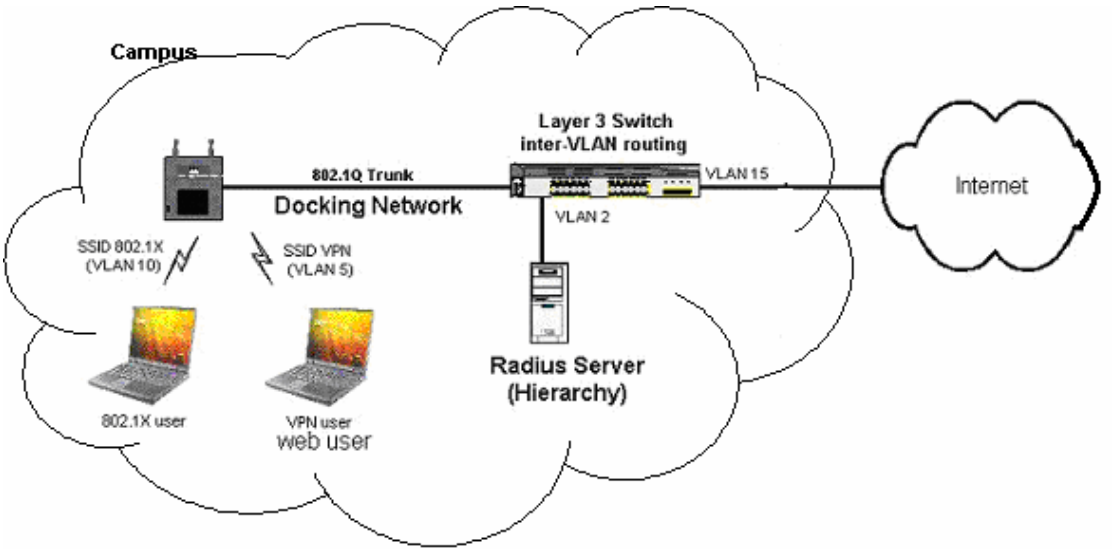


Figure 7: Network lay-out with multiple SSID's and VLAN assignment to support a number of roaming network access solutions.

If the access point is not capable of broadcasting multiple SSID's it may be necessary to create a physically (layer 1) separated architecture.

In addition to this, an institution that uses 802.1X or Web-based authentication needs to open up their switch for the CASG address-space while an institution that provides VPN-based access needs to set up a RADIUS server that connects to the eduroam RADIUS-hierarchy.

The deliverable describes the test beds that were created at the University of Tampere in Finland (Web-based), SWITCH (VPN-based) and SURFnet (802.1X-based). Each of these institutions have successfully created a setup that allows for guest use for all three approaches, using a different set of hard- and software. The document describes in detail these three setups and the user experience of visiting users.

Based on the three test beds a reference design has been produced that guides an institution that wants to provide guest access for visiting users in setting up the necessary infrastructure.

The deliverable clearly demonstrates that inter-NREN roaming is indeed possible. Time will show in how far these competing and co-existing solutions will continue to exist. However, building an infrastructure that is able to deal with users using the various access methods provides also for an easy migration for the home institution's users to one of the other two methods.

12. Roaming Policy guidelines

To facilitate the uptake of inter-NREN roaming in a manageable and scalable way and ensure the fostering and protection of trust amongst participants, roaming policy guidelines were needed to cater for roaming users, home and visited institutions, NRENs and the organisation responsible for the TERENA level RADIUS proxy server. This deliverable was created to draft policy guidelines to assist the scaling of the RADIUS proxy hierarchy and other roaming solutions as these emerge. The policy drafted by the group can be seen below as an abridged version:-

The vision

The vision of the TF-Mobility Task Force is to create a collaborative environment where academic guest users can visit other institutions either nationally or internationally and be offered an automated, authenticated network access service. The service should be recognizable as an academic roaming service and offer a minimum agreed level of security. Some institutions may make available a range of security options to the guest / roaming user, however it is the responsibility of the guest / roaming user to respect the acceptable use policy (AUP) of the *visited* institution as well as, of course, to follow the AUP of their *home* institution.

Once authenticated credentials have been sent to the guest /roaming user's home institution authentication server and have been successfully processed, the visited institution will "trust" the response from the guest / roaming user's home authentication server and grant a level of network access based on the visited institutions local site policy. All authentication sessions and network access sessions must be logged for auditing purposes to ensure that any breaches of the local acceptable use policy can be traced and appropriate remedial action can be taken in a timely manner that is acceptable to all participants.

Ideally the guest or roaming user should not have to do anything in addition to what he/she would normally do if physically located at their home institution. It will be necessary for home institutions to educate their own users participating in this service to ensure that they abide by the defined policies and contact the appropriate person(s) for technical support related matters.

Roaming Services - General Principles

- The obvious security requirement is that the roaming access must only be available to authorized users, which should include all users authorized for Internet access at the participating NRENs and their institutions.

- All roaming users are required to authenticate at their home institution in order to be granted network access at the visited institution.

- All roaming users are responsible for their own credentials (and transmission thereof) and must abide by the roaming AUP (see section 1.1 hereafter) that has been agreed on behalf of the user by their home institution.

- The visited institution must be able to prove that the network access service has access to the roaming service so that roaming users can recognise and take advantage of it.

- The visited institution must clearly state that the mechanism for the transmission of user credentials is secure. If not secure the visited institution must (if requested) be able to support a user-initiated solution typically from the guest user's client device so that a securer solution is possible.

- The visited institution has the right to block any roaming user, academic institution or NREN from accessing its local area network access provision.

- The visited institution will determine the authorisation of the network access provision.

- The home institution will be responsible for supporting their guest users including educating users on service support issues and abiding to relevant policies.

- Participants should provide feedback to their institutions on the roaming service and if necessary escalate any issues to their NREN who in turn on rare occasions may escalate a matter onto TERENA to either log or resolve.

Benefits of roaming services

- There will be a lower administrative burden supporting guest / roaming users.
- Users will ideally be able to gain reasonably secure transparent network access in a less complex and timelier manner without changes required to their client devices and ideally no need for additional user credentials.
- More pervasive transparent and secure guest or roaming access should result in greater opportunities for collaborative research and academic work groups between academic organisations both nationally and internationally.
- The use of authentication servers with logging facilities should provide a better system of traceability than the current solution of manually allocating guest access.
- Some roaming services can also be of local value for local users at the home institutions, i.e. user authentication services.

Policies

To facilitate the interest shown in roaming services it is important that policies are put in place at appropriate levels to ensure that benefits remain whilst threats and risks are minimized and managed within acceptable levels. The following sections will list policies that relate to different levels of control and responsibility within a hierarchy of trust.

Roaming Services – Intra-NREN roaming Policy

1. <u>TERENA level policy (agreements for participation between NRENs and TERENA)</u>

TERENA will adopt this document as the TERENA roaming policy. All participating NRENs connecting to or wishing to connect to the TERENA authentication servers (European top level RADIUS servers) to participate in inter-NREN roaming must abide by the following as a minimum

1.1. Participating NRENs must abide by this "roaming" service agreement contained herein.

1.2. NRENs are responsible for ensuring that their national authentication servers can provide a secure means of transferring user credentials to and from other proxy authentication servers as required.

1.3. NRENs must have signed agreements in place with their academic institutions to participate in the supply and receipt of national and inter-NREN roaming services.

1.4. NRENs must have the following procedures in place to handle

1.4.1. National authentication server support and maintenance.
1.4.2. Security issues. It is advisable that the NRENs keep their CERT groups informed of development work and have channels in place to work together on issues that affect both parties
1.4.3. Fraudulent use of the roaming service by users or groups of users.
1.4.4. A monitoring facility to show the status of the national authentication servers so that home institutions can use this information as part of any guest user fault reporting activity.
1.4.5. A mechanism for providing feedback on the roaming service so that guest or roaming users can identify participating institutions and their service offering.

1.5. Ideally, NRENs should have a minimum of two authentication servers at different locations on their core network for resilience and redundancy.

1.6. The NREN must mandate their participating institutions to notify guest users on the level of security offered for the transmission of user credentials.

1.7. The NREN must mandate their participating institutions to educate their users in the roaming service and ensure that any technical support issues are handled at the home institution only. If the home institution

determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

1.8. The NREN must mandate their participating institutions to log authentication sessions and network access sessions so that they can trace a user for both security and capacity planning purposes.

1.9. The NREN must mandate their participating institutions to report any security issues or fraudulent activities to their NREN and manage and resolve such matters accordingly and report these to TERENA.

1.10. NRENs are not expected to provide privacy against casual snoopers; it is therefore the responsibility of the home institution and the guest user to have appropriate end-to-end privacy solutions in place to secure communications.

1.11. NRENs should have written guidelines for participating institutions to assist them in drafting local site and user policies to ensure compliance with the roaming service agreements with their NREN.

2. NREN level policy (agreements for participation between NRENs and their institutions)

A national policy framework must be in place so that all participating institutions have signed acceptance to that agree to the following as a minimum

2.1. Participating academic institutions must abide by the “roaming” service agreement contained herein.

2.2. Participating academic institutions are responsible for educating their users to respect the local AUP of the visited institution that their users that have been granted network access to and are obliged to help resolve any issues that relate to their users.

2.3. Participating academic institutions must provide a secure authentication server that can securely process and forward user credentials as required.

2.4. Participating academic institutions should communicate to guest or roaming users on whether and how they offer the roaming service.

2.5. Participating academic institutions should inform guest users of the level(s) of security offered for the transmission of user credentials.

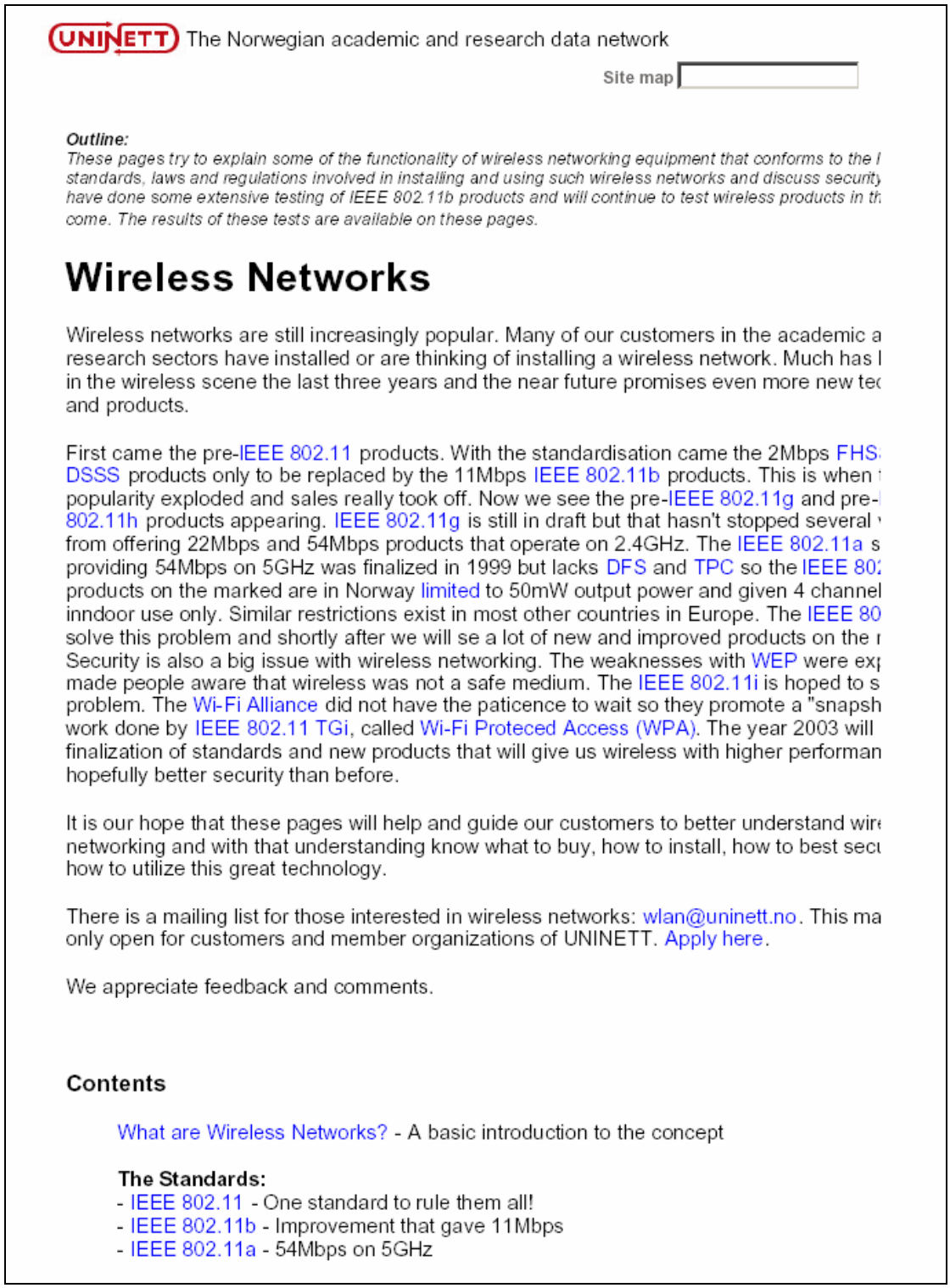
2.6. Participating academic institutions must educate their users in the roaming service and ensure that any technical support issues are handled at the home organisation only. If the home organisation determines the fault lies at the visited institution, only then should the issue be raised with the visited organisation technical support team.

2.7. Participating academic institutions must log authentication sessions and network access session and be able to trace a user for both security and capacity planning purposes.

2.8. Participating academic institutions must report any security issues or fraudulent activities to their NREN to manage and resolve accordingly.

13. A web repository of tests on Wireless LAN devices

This deliverable was a comprehensive review of wireless products to be sure that NRENs or institutions who were considering investing in a roaming solution were able to make informed decisions on the choice of equipment in today's marketplace. Detailed technical information was made available on the UNINETT website as follows



UNINETT The Norwegian academic and research data network

Site map

Outline:
These pages try to explain some of the functionality of wireless networking equipment that conforms to the I standards, laws and regulations involved in installing and using such wireless networks and discuss security have done some extensive testing of IEEE 802.11b products and will continue to test wireless products in th come. The results of these tests are available on these pages.

Wireless Networks

Wireless networks are still increasingly popular. Many of our customers in the academic a research sectors have installed or are thinking of installing a wireless network. Much has l in the wireless scene the last three years and the near future promises even more new tec and products.

First came the pre-IEEE 802.11 products. With the standardisation came the 2Mbps FHS DSSS products only to be replaced by the 11Mbps IEEE 802.11b products. This is when popularity exploded and sales really took off. Now we see the pre-IEEE 802.11g and pre- 802.11h products appearing. IEEE 802.11g is still in draft but that hasn't stopped several from offering 22Mbps and 54Mbps products that operate on 2.4GHz. The IEEE 802.11a s providing 54Mbps on 5GHz was finalized in 1999 but lacks DFS and TPC so the IEEE 80 products on the marked are in Norway limited to 50mW output power and given 4 channel inndoor use only. Similar restrictions exist in most other countries in Europe. The IEEE 80 solve this problem and shortly after we will se a lot of new and improved products on the Security is also a big issue with wireless networking. The weaknesses with WEP were exp made people aware that wireless was not a safe medium. The IEEE 802.11i is hoped to s problem. The Wi-Fi Alliance did not have the paticence to wait so they promote a "snapsh work done by IEEE 802.11 TGi, called Wi-Fi Proteced Access (WPA). The year 2003 will finalization of standards and new products that will give us wireless with higher performan hopefully better security than before.

It is our hope that these pages will help and guide our customers to better understand wir networking and with that understanding know what to buy, how to install, how to best secu how to utilize this great technology.

There is a mailing list for those interested in wireless networks: wlan@uninett.no. This ma only open for customers and member organizations of UNINETT. Apply here.

We appreciate feedback and comments.

Contents

What are Wireless Networks? - A basic introduction to the concept

The Standards:
- IEEE 802.11 - One standard to rule them all!
- IEEE 802.11b - Improvement that gave 11Mbps
- IEEE 802.11a - 54Mbps on 5GHz

- HiperLAN/2 - A rival to the IEEE 802.11a
- Others
- Wi-Fi Alliance - An organization to standardize the eh.. standard.
- Status of the IEEE 802.11 standards

The Workings of Wireless:
- Roaming and IAPP
- OFDM
- Signal Strengths and Link Budget, Antennas, Fresenels zone, DFS, TPC, Interfere

The Law:
- Laws and Regulations

Security on Wireless
- Wireless security threats
- Securing a wireless network
  - Web portal
    - Description of some web portals
  - 802.1x based systems
  - VPN

- How WEP works
- How TKIP and MIC works

Product testing
- Expected throughput
- Hardware vendors
- Testing procedures and requirements for documentation
- Feature lookup and compare products
- IEEE 802.11b Products
- IEEE 802.11a Products

WLAN access in Norway
- Public WLAN HotSpots

Known problems (& solutions?)
- Problems with Zyxel P316/B-2000 when using Lucent ORINOCO/Agere PCMCIA card on Win XP
- Zyxel B-2000 will not bridge between LAN/WLAN when using an IBM ThinkPad with built-in WLAN
- The Zyxel Prestige 316 hangs when using WEP.
- The Zyxel ZyAir B-2000 has approx 80% packet loss on network traffic

Links
- TERENA TF-Mobility

In addition, a repository of product data and a comparison tool was also produced.

14. Impact of new technology and protocols such as MobileIP on current roaming work.

The new IPv6 protocol has reached standards maturity in the IETF, and is now widely implemented by the major operating system and router vendors. Many open source software applications are now IPv6 capable. While there is not yet any pressing need for European academic sites to migrate to IPv6 due to a lack of IPv4 address space, a number of sites are making small, early IPv6 deployments alongside their IPv4 infrastructure, enabling a pilot or pre-production dual-stack service. In some cases (e.g. at Southampton), IPv6 is used in a production environment. Early deployment gives experience of the protocol, a basis for teaching IPv6 in CS departments, support for IPv6 in research projects, and availability of IPv6 in an environment where innovate students and researchers may create interesting new IPv6 applications.

IPv6 has a number of implications for WLAN access control and inter-NREN roaming. Firstly, all such systems should support an IPv6 mode of operation, in parallel with the IPv4 service. Thus a system should be able to authenticate to a WLAN over IPv6 transport, just as it can with IPv4 transport. Currently, commercial web-redirection systems do not support IPv6. If a client tries to access a web page over IPv6, the web-redirection gateway will not recognise the protocol, and will not redirect the request to an authentication page. Thus the user cannot authenticate to the WLAN. If their system is (most likely) dual-stack, they can authenticate by visiting an IPv4 web page, but even after doing so, and being admitted, the gateway will likely prevent any IPv6 access through it (natively, or via any attempt to tunnel through the gateway). There are no current plans by commercial companies (e.g. BlueSocket) to provide this functionality. It would be interesting to investigate the open source NoCatAuth system to add IPv6 capability.

The VPN access control method relies on IPv6 VPN capability, which is currently in its infancy (some early work has been done by UCL and UMU in the Euro6IX and 6NET projects). The 802.1x method does allow IPv6 systems to gain admittance, because it works at Layer 2. The 802.1x access request is relayed by the (dual-stack) access point to a RADIUS server for authentication. There has also been early work done by an ISP in the Netherlands and by other groups on 802.1x with IPv6 RADIUS lookup; here the Access Point is typically a modified HostAP system, using a RADIUS server that supports IPv6 transport (Radiator as of the latest version, or FreeRADIUS with a patch). Thus currently 802.1x is the only viable method for WLAN access control where IPv6 protocols are to be used.

The RADIUS referral hierarchy could in principle run over IPv4 or IPv6 transport. One option is for local RADIUS server to be dual-stack, and support lookups over IPv4 or IPv6 (as is possible with Radiator or FreeRADIUS), and then make referrals to higher hierarchy servers over IPv4. This would see IPv6 capability added at the edge first. This is the principle by which dual mode transport support is currently being deployed for the DNS; local dual-stack resolvers, with an IPv4 hierarchy. However, it would also be possible to introduce dual-stack capability in the central RADIUS referral servers (and by analogy IPv6 transport is now being added to some DNS root servers).

Another aspect of IPv6 of interest is the new Mobile IPv6 protocol, which has recently reached Proposed Standard status in the IETF (RFC3775). MIPv6 allows a node to be addressable by a fixed IPv6 address, taken from its Home network, such that the node is always reachable via one address (and thus no dynamic DNS updates are required for hosts that may appear in different networks). It also allows a node to maintain (TCP) IP connections as it moves between networks. When the Mobile Node is away from its Home network, the Home Agent on the Home network will forward traffic to the Mobile Node at its current (remote) care-of address. A new optimisation for mobility in MIPv6 allows the Mobile Node to inform the Corresponding Node of its new care-of address, such that this triangular routing is removed, and direct communication possible. This optimisation is very useful where two roaming mobile nodes are in the same room; rather than the traffic between them passing through two different remote Home Agents, the nodes exchange traffic locally, directly. This is particular beneficial in a WLAN environment where there is low uplink capacity (e.g. ADSL).

With MIPv6 now at the RFC status, there are emerging stable implementations available, e.g. from Cisco, Elmic Systems and, for open source, the MIPL project (MIPv6 for Linux).

We expect the potential of IPv6 to be realised in the next three years; thus it is important that early experiences are gathered, vendor support for access control methods introduced, and IPv6 capability added to deployed roaming services, at the earliest opportunity.

15. Summary of national roaming developments

15.1 Croatia: Current status in Croatia (CARNet network)

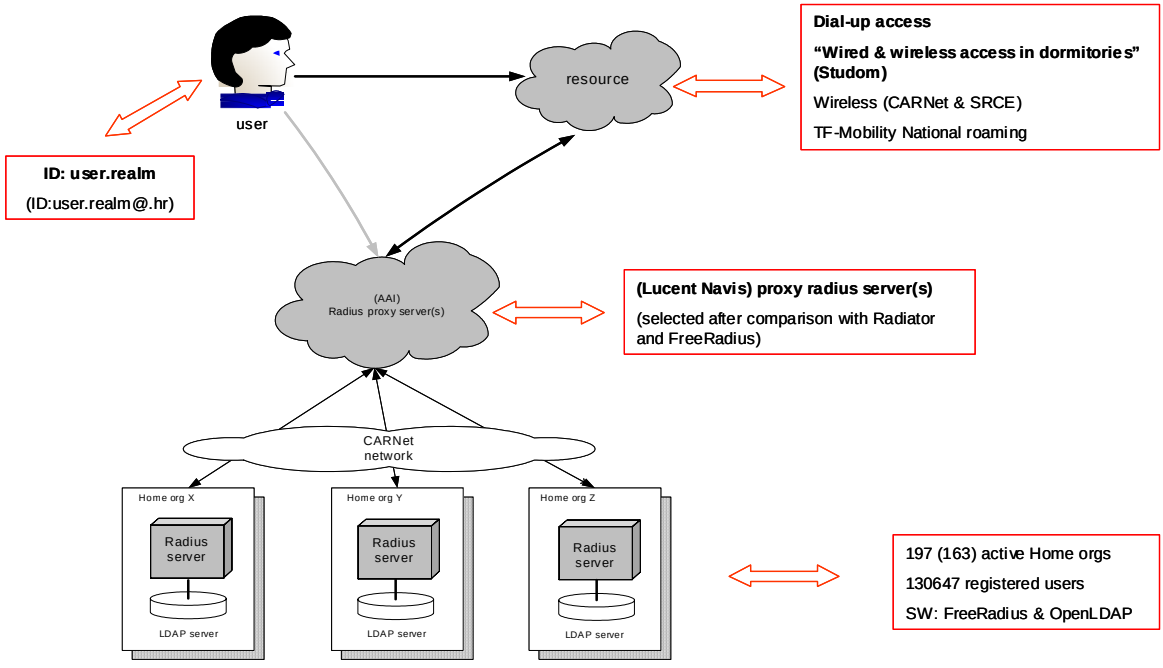
CARNet and University Computing Centre, University of Zagreb (Srce) have set up a national hierarchy of RADIUS servers tied up with LDAP directories. Their goal is to ensure that every institution connected to the CARNet network runs its own RADIUS server and LDAP directory. They see it as a basis for the AAI of A&R community in Croatia.

The national hierarchy was started in February 2003, originally as the basis for CARNet's dial-in service. Currently (June 2004) there are 197 institutions covered. Out of this number 163 run their own RADIUS and LDAP servers, while 34 are hosted by Srce. Total numbers of registered users is 130647 (June 2004). The national hierarchy has been connected (via a dedicated RADIUS proxy server) to the European Radius Hierarchy (as started by the TF-Mobility group).

Apart from dial-in access, the national RADIUS/LDAP hierarchy is also used for:

- wired and wireless (802.1x) access to the CARNet network from student dormitories (currently in operation only in Zagreb (selected dormitories only) and Osijek , the rest is under construction right now)
- wireless access at selected venues (e.g. CARNet and Srce building, selected faculties,).

The plan is to use the established RADIUS/LDAP hierarchy as the AAI for network access (dial-in, wireless, wired, cable, ...). Some organisational work is to be done, especially regarding the policies (for users and CARNet member institutions). The plan is to stay in the European Radius Hierarchy. The current status is illustrated with the next picture.



Miroslav Milinovic (30 June 2004)

15.2 Czech Republic: National status of “Eduroam” roaming services

CESNET are currently up and running with national RADIUS servers (radius1.eduroam.cz and radius2.eduroam.cz) which are ready to operate requests from organisation level RADIUS servers. The national RADIUS proxy servers are also connected to the Terena (Euro) level RADIUS servers. This means the RADIUS hierarchy is operational but it is still very much in a testing mode. The FreeRADIUS implementation (because of open source, cost, etc.) was selected, but it has not worked as well as had been expected. The operational stability of the FreeRADIUS isn't as good as had been expected. As a result, Radiator is being tested at the moment and there will probably be a change of RADIUS server software in the near future.

CESNET also has allocated the CASG IP address block for VPN gateways. CESNET wants to support all three authentication methods; however the priority is still 802.1x.

Discussions about roaming policy are currently in progress. A policy document is being reviewed by the NREN board of directors (representatives from universities, academy of science, etc.) and by an independent law company. The end result should be agreement to a national policy document by the end of September. Having the roaming policy and the RADIUS hierarchy in place is absolutely necessary in order to start the pilot project that is scheduled to take place during October 2004.

To date CESNET has received the "promise" of collaboration in this pilot project from five universities (TUL Liberec,CVUT Praha, VSCHT Praha, VSB Ostrava and ZCU Plzen) and it is hoped that many more institutions will join this project.

Other work activities include the testing some wireless devices (AP, client supplicants), tuning optimal network configuration, and work on the main “eduRoam” information portal for the Czech Republic (www.eduRoam.cz), the "final product" should be complete very soon.

Jan Furman (29 June 2004)

15.3 Denmark: National status of Eduroam-project in Denmark

Since Autumn 2003 the Danish NREN, Forksningsnettet, has closely followed the work of the TF-Mobility group. One large and one smaller meeting on roaming have been held with NREN-technical staff and network people at the connected institutions. Generally people are enthusiastic and eager to participate in Eduroam.

Forskningsnettet has in spring this year installed a redundant set of national RADIUS-servers (Radiator) which in turn has been connected to the top level server in Holland as of mid-June 2004. So far only the Danish Technical University is hooked up to the national server but other institutions will join in the coming months.

UNI-C, who runs the NREN, has now become national reseller of the Radiator software to academic institutions.

Denmark has offered to host a secondary top level RADIUS-server to the one in Holland, which is now being implemented. This sort of international redundancy will make sure that international roaming users will not be affected if a large power failure or other such event.

The Danish NREN newsletter announced the Danish participation and new possibilities for students and researchers in mid-June. Also articles will be printed in the campus papers of the larger institutions.

The RADIUS-hierarchy is now also paving the way for the Danish NREN's general offer to use a centralized iPass-service. Each institution can now sign up for the service and will be billed individually (at a lower price pr. minute, negotiated collectively by the NREN). As the authentication requests from iPass are RADIUS-packets these are received by the national roaming-server and redirected to a dedicated authentication iPass-server. Each iPass-user is provided with a unique NREN-ID which is matched to a name, institution etc. and which can hopefully later be used to provide the users with more services.

An administrative web interface has been developed, so that all participating institutions will administer their own users and thereby effectively be in control of their own phone bill. Other services are being considered as 'add on' to the RADIUS-based roaming service, i.e. distribution of IP-phone numbers based on approved authentication, roll based privileges etc.

David Simonsen (22 June 2004)

15.4 Finland

The original idea was to combine authentication databases so that people can go to different universities and get access without trying to find local administrators in order to get a guest account from them. Most of universities were already doing authentication, mostly by web redirection using the RADIUS protocol so the development of a RADIUS proxy hierarchy was a logical choice. Another reason for developing the RADIUS proxy hierarchy was the existing plan to support 802.1X in near future which also relies on a RADIUS proxy hierarchy.

CSC have been active participants in the TF-Mobility group and have contributed on many of the deliverables. CSC have also been the owner and author of Deliverable F: "Inventory of web-based solution for inter-NREN roaming".

The current status in Finland is that there are 20 realms registered with 12 academic and commercial organisations participating. The pilot will continue to run until June 2005 and there is a plan to expand organisational participation to the RADIUS hierarchy by developing a marketing campaign to generate awareness of roaming services to users. In addition CSC will be investigating RADIUS proxy server monitoring issues and hope to develop some solutions in this area during this year. Currently both failed and successful authentication requests can be identified but there is no other monitoring information available, for example it is not possible to monitor an organisation’s RADIUS server availability.

CSC will also create web pages for roaming services during this year.

Sami Keski-Kasari (30 June 2004)

15.5 Germany

Germany started a pilot project (DFNRoaming) on Internet roaming in January 2004 chiefly based on results/solutions taken from TERENA TF Mobility, but also from other sources. A test bed was installed at the DFN premises in Berlin.

At first, the aim was to set up an infrastructure based on IEEE 802.1X port authentication and a top down radius hierarchy was established. Two RADIUS servers (802.1X compatible) were set up at the DFN G-WiN backbone, one for direct use and another one as a backup server. Unfortunately the current status in Germany is that only a few research institutions and universities support 802.1X in their local environments. This problem cropped up mainly due to old access point technology and insufficient support of the 802.1X supplicants on the client side on the campus' wireless LAN.

Instead different VPN solutions are used locally. But 802.1X is a promising technology to make WLAN infrastructures more secure, so DFN introduced/offered a so called "Modular 802.1X migration solution (Mod8.X)" that supports a minimum demand web-based authentication immediately and 802.1X based authentication in the future, i.e. as soon as institutions will be able to set up access points that are capable of 802.1X and that are able to manage more than one “ESSID” for network identification.

Mod8.X can live together with VPN - based authentication and starts with a web-based authentication. Mod8.X comes with a debian Linux box, two LAN Ethernet cards and access points. The debian Linux box has to be configured with 802.1q and VLAN tagging should be enabled. Among other things a firewall script can be easily configured as well. As a web-based solution, tino from the University of Tampere in Finland is good. The tino system consists of some perl scripts and a cgi script and is very easy to handle. Naturally some commercial web-based solutions are also possible but these were not tried.

Because of the Mod8.X modular design, only the access points have to be changed and a second “ESSID” has to be established in the future if an upgrade to 802.1X in the WLAN infrastructure is required. Under DFNRoaming two “ESSID’s” are deployed: "802.1X" and "VPN/WEB". Institutions that want to be part of DFNRoaming are obliged to use these “ESSID’s”, but don't control it.

At the moment there are 15 large institutions registered at the DFN top level RADIUS with approximately 15,000 users. However, this does not mean that DFNRoaming is operational around these campus networks. There are still a lot of construction areas and DFN are working on a DFN-wide-map to configure out what is the status of the construction. There is an operational link from the DFN top level RADIUS to the TERENA top level RADIUS and vice versa. Future plans involve a native 802.1X authentication environment spanning DFN with about 500 research institutions and universities with 1.5 million users (most of them are students).

Ralf Paffrath, Juergen Rauschenbach (30 June 2004)

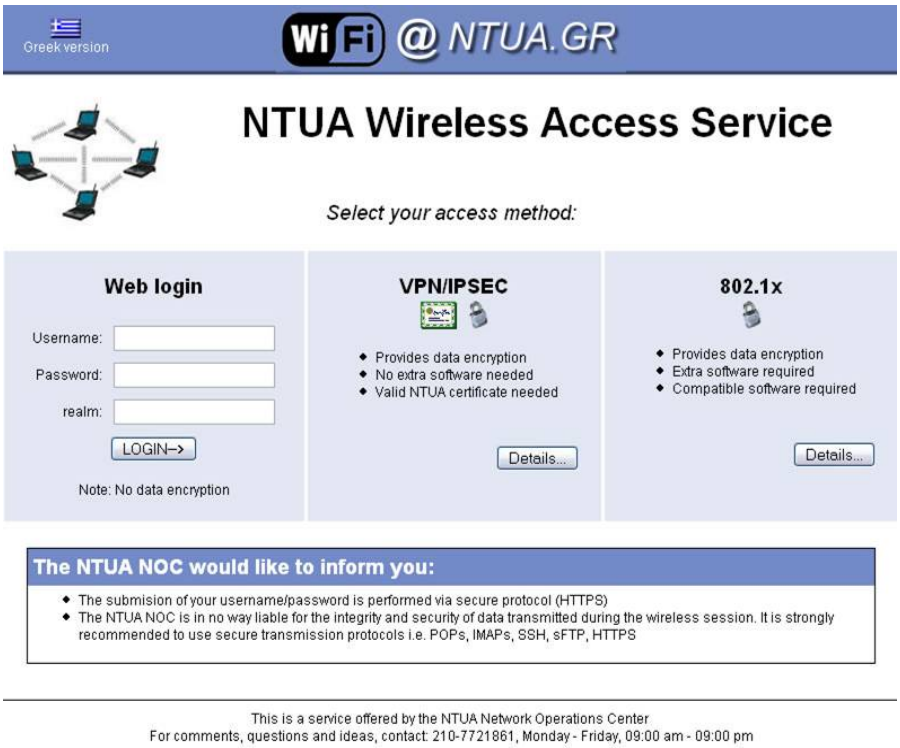
15.6 Greece: National roaming developments

National roaming activities in Greece started to take place when GRNET joined the European top level RADIUS hierarchy in June 2004. This has triggered a discussion between GRNET and VNOC[6] participants on how to promote roaming activities across the Greek universities. There has been much interest shown from all sides. Most of the university network infrastructures include a RADIUS server for authentication that is used for various services (e.g. Dialup, VPNs, VoIP, Wi-Fi etc). All these services are candidates for roaming by using GRNet's RADIUS hierarchy.

Among the proposals for roaming that were discussed were:

- Wireless access.
- L2TP VPNs. GRnet has investigated the possibility of providing a VPN server that may be used from any GRNET connected member, in order to terminate secure tunnels inside GRNET.
- VPDNs using MPLS L3-VPNS. Since GRNET is an MPLS based network, it can take advantage of L3 MPLS VPN in order to allow a remote user to connect to their home network.
- VoIP and H323 services may also benefit from a RADIUS roaming infrastructure.

Until now, only the National Technical University of Athens has joined the RADIUS hierarchy under GRNET, providing wireless access for visitors.



[6] VNOC: Virtual NOC is GRNET's Network operating Center that is distributed across many of the major academic institutes.

There were also thoughts of using GRNets roaming infrastructure for authenticating the wireless hotspots that were deployed by Information Society (Ministry of Economy and Finance) as a part of its activities on promoting broadband services in Greece.

Spiros Papageorgiou (16 July 2004)
NOC/GRNET

15.7 Netherlands

At the end of 2001 SURFnet, the Dutch NREN, started looking into methods for offering secure access to wireless LAN's. Early in 2002 it was decided to trial 802.1X with the University of Twente and the company Alfa&Ariss. As part of this trial Tom Rixom of Alfa&Ariss developed a freely available supplicant, now known as SecureW2. SURFnet made its RADIUS infrastructure available for use with this technology to provide for guest access.

Based on the success of this trial, the University of Twente decided to mandate 802.1X support in its European tender for a wireless campus. After an expert meeting in April 2002 a number of members of the SURFnet constituency decided to move to 802.1X for (wireless) network access too. In March of that same year SURFnet took the initiative to organize a workshop on network access at TERENA and later a meeting at TNC in Limerick to discuss setting up a Task Force on mobility. In 2003 SURFnet set up a European top level server for TERENA.

The roaming access service is launched under the name Eduroam, the website http://www.eduroam.nl will provide a portal for this service. Currently approximately 50 institutions take part in the RADIUS hierarchy whereas some 15 provide roaming wireless LAN access.

Current and future activities evolve around a number of themes:

Policy

Discussion about roaming policies has started. A draft policy has been produced to be included in the contracts with all SURFnets customers.

Supplicant software

A contract has been signed with Alfa&Ariss to further develop the SecureW2 software to include pre-built localised versions of the client.

Tracking and tracing

A group of universities have jointly developed a first version of a system for tracking and tracing of users in order to track abuse. This software is available at http://www.sourceforge.net/projects/usertracking

Basic infrastructure

Although the existing RADIUS-infrastructure that forms the basis of Eduroam performs its tasks satisfactory new developments will constantly monitored to see if any changes are useful or necessary. Emerging technologies like DIAMETER and DNSsec will be evaluated. Furthermore, the use of the existing basic infrastructure to provide other access to services will be investigated.

Integration with application access

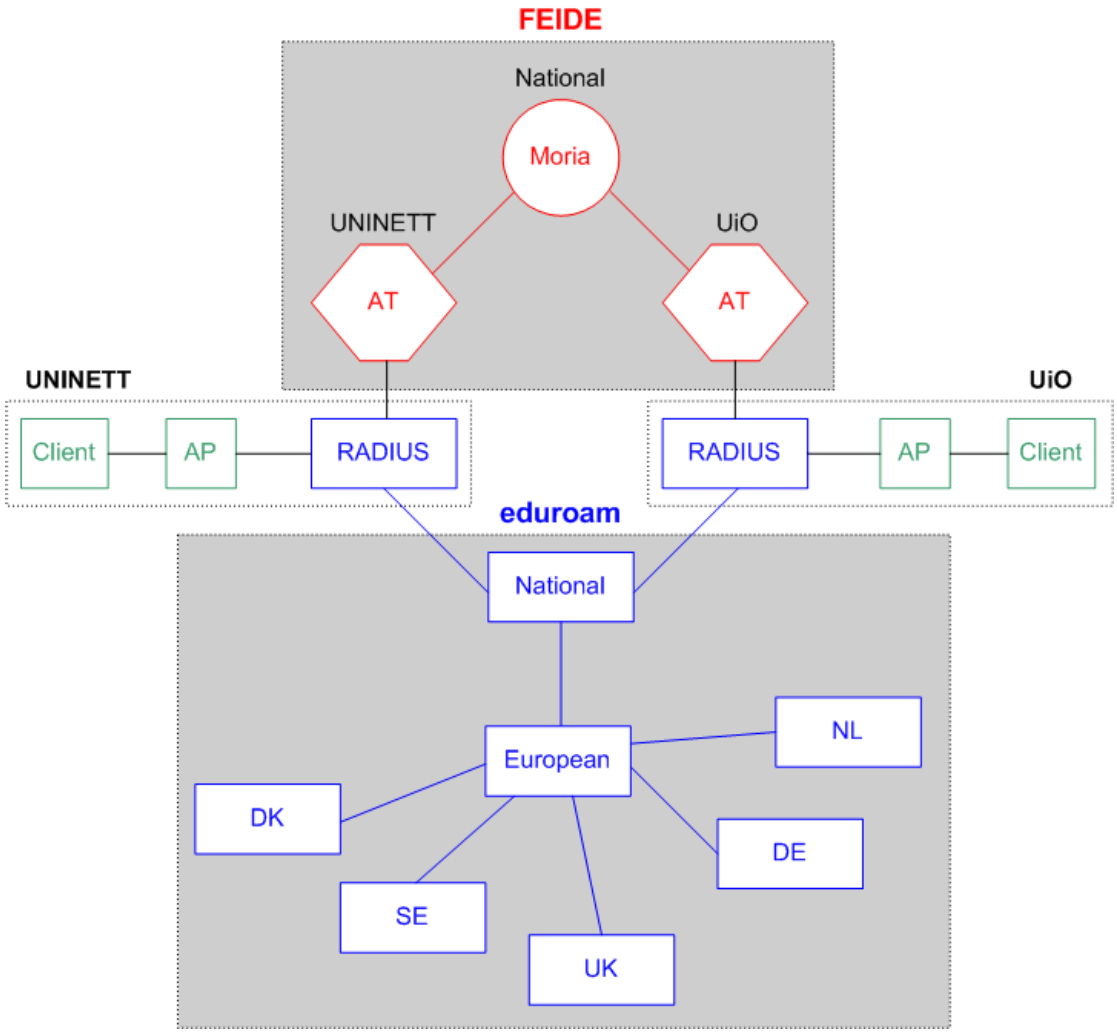
For (roaming) access to applications SURFnet uses an authentication system for web-based applications called A-Select (http://www.a-select.org). This tool allows for the use of various authentication means. SURFnet will investigate the integration of A-Select with the Eduroam service to make the use of various authentication means possible and to deliver a single sign on for both network and application access.

Klaas Wierenga (1 July 2004)

15.8 Norway: National status of “eduroam” in Norway

UNINETT is the NREN for Norway. Among its members are 4 universities and 40 colleges. Other members include miscellaneous research facilities. The daughter company UNINETT ABC aims at providing technological aid and expertise to schools at graduate and high-school and levels.

The future core of the UNINETT authentication system is FEIDE (http://www.feide.no) which is a "FEderated ID for Education". FEIDE will provide the user database and PKI. RADIUS servers are used at most organizations and it is one of the goals of FEIDE that they in the future only will function as a proxy for the back-end FEIDE. The FEIDE system will bind the organizations together and enable users to roam across organizations. FEIDE does not facilitate RADIUS by itself and therefore needs local RADIUS servers to handle requests from the various authentication systems. The RADIUS servers can be tied together in a national hierarchy in parallel to the FEIDE network. By connecting this to the European RADIUS hierarchy, it will be able to support roaming for visitors that are participants in "eduroam".



At this stage the various member organizations have employed various wireless security measures ranging from none at all to web portals, VPN and 802.1X.

UNINETT is advising its members on the use of 802.1X based security which is supported by FEIDE and also gives the organization a choice of authentication method and encryption in accordance with local security policy.

UNINETT has a FEIDE AA structure in development and 802.1X authentication on wireless networks in place. Several members have signalled their participation and together we have started a nation-wide deployment effort. The top level national RADIUS server is nearly ready for connection to the top level European RADIUS hierarchy so that we can take part in the "eduroam" cooperation.

Jardar Leira (29 June 2004)

15.9 Portugal: The Portuguese Roaming Project e-U

The Portuguese roaming initiative started within e-U virtual campus project (http://www.e-u.pt in Portuguese only). This project, partially funded by Portuguese government, will implement, among other things, wireless infrastructures on every higher education institution.

FCCN's role on this project it to study, produce documentation and provide the necessary help on the deployment of these infrastructures, so that they allow roaming for students and teachers in every campus. A pre-requisite to get funds on this project is that all built infrastructure supports roaming for its users.

To achieve these goals, FCCN started with eight pilot institutions that tested some hardware and several controlled access solutions like web-based login (nocat and nomadix), VPN access based on certificates and 802.1x. Based on these tests, 802.1x/EAP was adopted as the national roaming solution. Every campus will have at least two SSIDs (broadcasted 'guest-e-U' and 'e-U' that in most places will not be broadcasted). 'guest-e-U' is open with no WEP and e-U demands for 802.1x authentication. The first one gives only access to a local Web Server and the second provides access to Internet. So far there are 62 institutions (almost all public and private higher education) in the project in different stages of deployment, seven with roaming already in place and tested.

In the design of the hotspot some basic principles have been defined (in order to make the roaming experience 100% transparent for the end user):

Preferred EAP's: PEAP and TTLS (those are the ones that were tested on the hotspot but the institutions may choose among other ones)

Broadcasted open SSID: 'guest-e-U' with access to a web server with documentation; software; may not cover all the hotspots

802.1x SSID: 'e-U' with dynamic WEP keys (FCCN is avoiding using WPA/TKIP because of the not so mature drivers and support) with roaming; should cover all the hotspots

Radio Channels: from 1 to 11 for compatibility with US cards/centrinos – it is important to use non overlapping channels like 1, 6 and 11 but sites are free to make their wireless deployment with other channels.

IP assignment: the roamers are supposed to get a public IP address to avoid the problems that some software / VPN concentrators have with NAT.

The link for the e-U Project at FCCN is (English not supported):
http://www.fccn.pt/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=114&MMN_position=90:4
This section includes:
- Access Point tests results (3Com, Alcatel, Cisco, Enterasys, Gemtek, HP, Nortel, Colubris and SMC);
- Vendor cookbooks (Enterasys, Cisco, HP and Alcatel);
- Radius server cookbooks (Radiator, FreeRadius and IAS);
- Best-practices and other relevant documentation.

Luis Guido (30 June 2004)

15.10 Spain

This section explains the main objectives and the current state of a mobility initiative at a national level in Spain (MovIRIS).

MovIRIS is a national initiative that belongs to the Spanish Research Network. Its main objective is to coordinate Spanish research organizations with the aim of creating a unique mobile environment for their users. To do this, there is a national mobile use policy (currently only in Spanish) that is compatible with the European policy. Also, RedIRIS gives its organizations the necessary support to ensure their mobile infrastructure is compatible at technical level with the technical solutions supported by the TF-Mobility group.

The main objectives of MovIRIS are as follows:

1. To coordinate the starting of a national mobility infrastructure in the community, by being a single point of contact for common problems and solutions.
2. To develop a national mobility use policy compatible with the European mobility use policy.
3. To make sure that there is compatibility in the technological level solutions implemented in different national research organizations with those ones supported at European level.
4. To coordinate information, local to organizations, related with mobile access methods, mobile infrastructure, etc.
5. To support and promote national initiatives and solutions in the mobility area.

MovIRIS started in June 2004, and there are currently seven organizations involved. Two of them with a quite long experience: one of them uses VPN technology, and the other one has developed a version of NoCat with improved users and roles management.

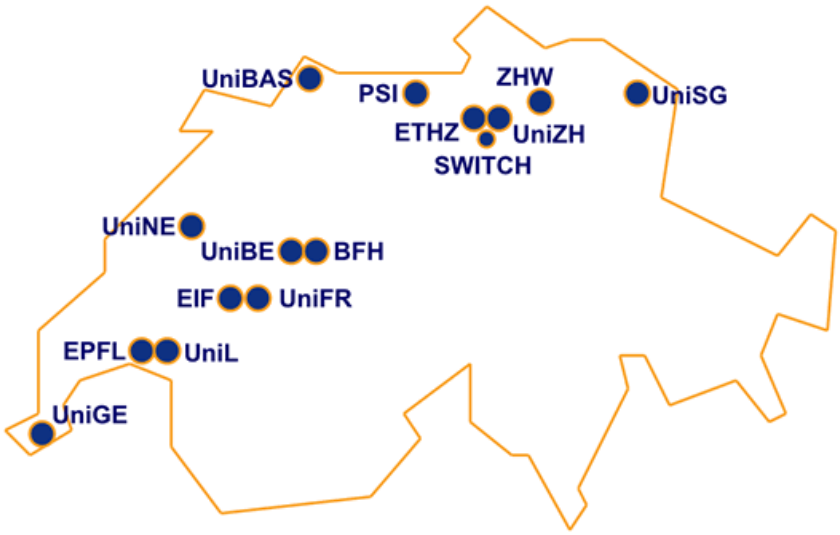
Rodrigo Castro (30 June 2004)

15.11 Switzerland: SWITCHmobile physical roaming services.

SWITCHmobile is the Swiss physical roaming service for Switzerland. The project was launched in Q4/2001, due to the increasing need to develop a solution that would enable physical roaming between campuses for researchers, professors, students and university staff. The first SWITCHmobile-workshop was held in June 2002, a number of potential solutions were investigated and presented. As a result of this workshop a working group with members from several universities and research institutes was formed and led by SWITCH to investigate whether a technical concept for a national roaming solution was feasible.

The working group agreed on a VPN solution as their preferred solution and published a first version of the technical concept in December 2002. Besides working on the technical concept a test bed with several pilot sites was also created. SWITCHmobile changed it status from trial to operational status in Q2/2003.

When TERENA launched TF Mobility in Q1 2003, SWITCH participated in an active role as representatives for the VPN approach. During the lifetime of TF Mobility, SWITCHmobile has mainly focused on the expanding the number of participating sites. Currently, SWITCHmobile has 15 active participating sites (universities and research institutes) with a few additional sites scheduled to join shortly. A map of participating SWITCHmobile sites can be seen below



Aside from the deployment activities, SWITCH is also organising regular working group meetings to facilitate discussions on general issues, problems and solutions. Besides the technical concept the working group has also created a concept for user and communication guidelines to define a common denominator across the SWITCHmobile participating organizations for communicating the SWITCHmobile concept and usage to the users. A small but substantial lab has been built at the SWITCH head office in order to be able to test new technologies and gain experience working towards a possible next-generation SWITCHmobile.

In the near future the stable and deployed VPN solution will still be the favoured solution. Working group meetings will be held three to four times a year, discussing further developments and other concerns. Test beds for emerging technologies including 802.11i, seamless roaming, Mobile IPv6, etc. will be run. SWITCH will also participate in the TF Mobility follow-up activity and in JRA5 of GEANT2 to help and contribute towards a European roaming solution that can cater for SWITCH's national needs and to expand the reach of roaming services across Europe and internationally.

Further information concerning SWITCHmobile can be found at http://www.switch.ch/mobile

Hansruedi Born (13 July 2004)

15.12 UK: National status of Location Independent Networking to facilitate "eduroam" in the UK

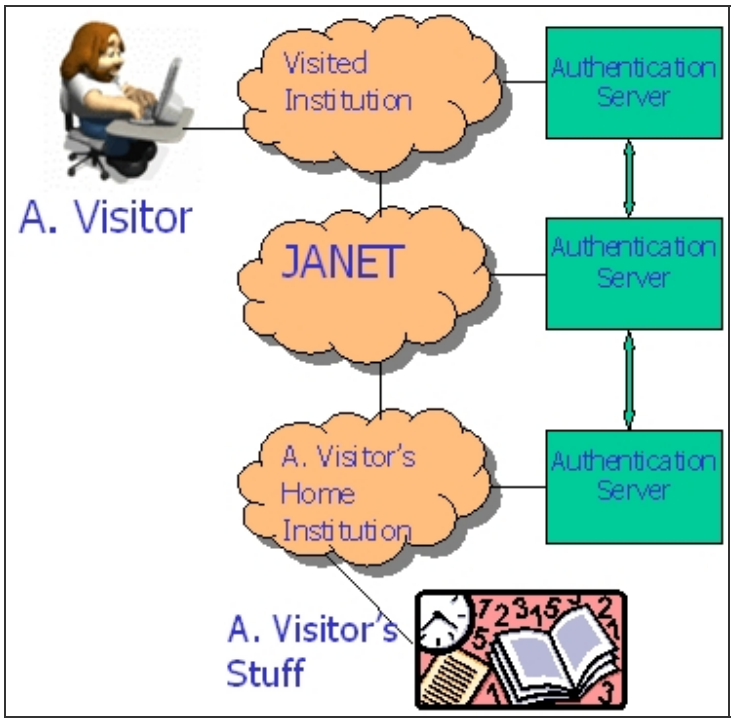
In the UK, UKERNA has been closely involved in the work of the TF-Mobility group. In parallel, UKERNA has established a JANET Wireless Advisory Group to look into the issues of wireless, mobility and the provision of guest access across the UK. The JANET Wireless Advisory Group has been responsible for the production of a variety of documents related to wireless networking that have been collated into an online repository of information at

http://www.ja.net/development/network_access/wireless/wag/wireless-info.html

The repository contains articles, white papers, case studies and in particular, three MAWAA reports from the University of Southampton that provide detailed information on wireless networking and issues related to the "eduroam" concept.

Over the past twelve months, UKERNA and the JANET Wireless Advisory group have been designing and developing the "eduroam" concept based on a RADIUS proxy server hierarchy to support web based redirect and 802.1X network access methods. UKERNA is also tracking support for VPN network access methods. The Roamnode solution, described earlier in this document, is under active development at the University of Bristol.

An architecture document was produced together with draft policy guidelines necessary to support and encourage participation. The work area has been titled "Location Independent Networking" and has been referred to as "hassle free" guest network access.



There has been significant interest in the development area so far. An example of how the concept has been promoted to the JANET community can be seen in the figure above.

The Location Independent Networking concept relies on a network of trust to be established between participating JANET organisations that have an authentication server that is configured to allow a guest user to enter and send their credentials onto their home organisation's authentication server. Once successfully authenticated, the visited organisation will then grant network access to the guest user according to the visited organisation's local policy.

UKERNA has initiated a development project to trial a two-tier national RADIUS proxy server hierarchy to test whether it can support the Location Independent Networking concept. The University of Bristol has been selected to manage two National RADIUS proxy servers. It has already built the National RADIUS proxy servers and technical support services in anticipation of proof of concept tests that are scheduled to commence in August 2004 with the following five participating organisations :-

- The University of Edinburgh,
- Lancaster University,
- The University of Manchester,
- The University of Southampton,
- The University of Strathclyde,

Once the National RADIUS proxy hierarchy has been successfully tested, the national servers will then be connected to a European level RADIUS proxy server to further test the concept with participating National Research and Education Networks and their organisations.

If the test phase is successful, UKERNA will issue an open Call for Participation to the JANET community in September 2004, with a view to seeking a number of JANET organisations to participate in the national trial service for a period of six months. For the trial service, the National RADIUS proxy service would be hosted at co-locations on the JANET backbone and managed remotely by the University of Bristol.

Three of the LIN test sites are also collaborating on a JISC-funded project called LICHEN (Location Independent Collaboration in Higher Education Networks), in which application and service-oriented support for roaming and virtual organisations will be explored, using the LIN infrastructure (or initially a clone of it) as the underlying technology. Synergies with Shibboleth will be explored. SURFnet has also expressed interest in this project.

More details will be made available at
http://www.ja.net/development/network_access/lin.html

James Sankar (29 June 2004)

16. Conclusions

The aims of the TF-Mobility group have been recognised as relevant and applicable in terms of benefits to academic researchers, staff and students that may have to work in more than one physical location. The work itself has been practical, technical and of sufficient scope and depth to be of use to many NRENs and Universities. The net result has been a significant interest in the mobility area and enthusiasm from the academic communities across Europe and beyond to participate in roaming activities.

The group has identified a key set of roaming requirements and has assessed these against a variety of roaming infrastructure deployments within NRENs. Their first conclusion reached was that no single solution meets all the key requirements listed. As a result an interoperable solution was recommended and substantial work was undertaken to design, build and test RADIUS proxy hierarchy and Controlled Address Space for VPN Gateway concepts. This integration approach also provided institutions with a realistic and easier upgrade path towards 802.1X.

As the group nears the end of its 18 month lifetime, it has been proven that it is possible to create a highly interoperable solution, and a cookbook has been written to ensure that the knowledge gained can be shared amongst the NRENs and their institutions.

Interest in participating in these activities has grown significantly with many NRENs developing their own roaming infrastructures to integrate into the interoperable solutions mentioned earlier. As a result, the Task Force has developed a set of policy guidelines to ensure the development service can scale and be manageable and also has the necessary foundations to move current work towards a service model.

Other work has been produced in the development of a product matrix on wireless Access Points and Wireless client cards. In addition a deliverable has been written to consider the impact of Mobile IP / IPv6 on the current roaming infrastructures. The Task Force has completed all of its original deliverables and added some new items along the way; further work has been considered and will be presented in the next section of this report.

17. Recommendations for future work

The Task Force considered future work items and whether to request the formation of a new group at meetings in Berlin, Amsterdam and Rhodes. These discussions led to an agreement to continue the work done but also to avoid any overlap from work going undertaken by DANTE in theJoint Research Activity "Ubiquity (Mobility) and Roaming Access to Services "(JRA5) in the Geant2 project.
A new charter was agreed at the final Task Force meeting in Rhodes in June 2004.

In summary the new charter foresees work to be undertaken to:
(1) Extend roaming service access beyond NRENs to other networks and
(2) Develop more secure, more flexible and more accountable roaming services by investigating and testing system integration with other Authentication, Authorisation and Accounting solutions.

A list of working items has been agreed as well.

Full details of the new terms of reference are available at:
http://www.terena.nl/tech/task-forces/tf-mobility/mobility2/TF-Mobility2ToFv2.0.pdf

18. References

Deliverables produced

Website
http://www.terena.nl/tech/task-forces/tf-mobility/

Glossary
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelB/DelB_v1-3-5.pdf

Requirements definition
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelC/DelC1-4.pdf

Inventory for an 802.1X national roaming solution
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelD/DelD_v1.2-f.pdf

Inventory for a VPN national roaming solution
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelE/DeliEv4.4-np.pdf

Inventory for a web-based redirection national roaming solution
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelF/DelF-f.pdf

Preliminary selection for Inter-NREN roaming
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelG/DelG-final.pdf

Test bed for Inter-NREN roaming
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelH/DelHv1.0.pdf

Inter-NREN roaming policy guidelines
http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelI/Roaming_policy_document_v.1.2.pdf

Inter-NREN roaming and MobileIP / IPv6 considerations
http://www.terena.nl/tech/task-forces/tf-mobility/DelAndDoc.html

Wireless product matrix
http://www.uninett.no/wlan/

Presentations by Task Force members

- Mobility Sessions presentations at TNC 2004 (7 – 10 June 2004)
  - "WLAN Roaming for the European Scientific Community: Lessons Learned" – Carsten Bormann
  - "A roaming Authentication Solution for Wifi using IPSec VPNs with client certificates" – Carlos Ribeiro
  - "Identity-Based Networking" – Eric Marin
  - Why Seamless? Towards Exploiting WLAN-based Intermittent Connectivity on the Road - Dirk Kutscher
  - Seamless Multimedia Communications in Heterogeneous Mobile Access Networks - Antonio Gómez-Skarmeta
  - An early adopter of full Wi-Fi coverage on campus - Philippe Hanset

- Tim Chown presented the work of TF-Mobility at Internet2 – Washington, USA (April 2004) http://events.internet2.edu/2004/spring-mm/sessionDetails.cfm?session=1378&event=203

- "Interconnecting heterogeneous wireless testbeds" EC workshop – Brussels (26 March 2003) http://www.surfnet.nl/innovatie/wlan/bijeenkomsten/ecworkshop25-3-3v2_wierenga.pdf

- Freeband Business Seminar – Utrecht (June 2003) http://www.surfnet.nl/innovatie/wlan/bijeenkomsten/FreebandTestbedBusSem20030506def.ppt

- NORDUnet conference - Reykjavik (September 2003 http://www.surfnet.nl/innovatie/wlan/bijeenkomsten/KlWi-WLANsecurity-Nordunet03.ppt - Klaas Wierenga

- UCISA "Short term network access workshop" - (30 October 2003) http://www.ja.net/conferences/short-term-access/James-Sankar.pdf

- Internet2 members meeting - Indianapolis (10 October 2003) http://international.internet2.edu/resources/events/2003/Fall03ITF1-Sankar.ppt

- Multi-service networks conference 2003 - (3 & 4 July 2003) http://www.acu.rl.ac.uk/msn2003/Talks/JamesSankar.pdf

- JANET Wireless Advisory Group meeting - (30 May 2003) http://www.ja.net/development/network_access/wireless/wag/Terena_Mobility_Group.pdf - James Sankar

- Mobility Sessions presentations at TNC 2003 (18-22 May, 2003)
  - "The Nomadic Network: Providing Secure, Scalable and Manageable Roaming, Remote and Wireless Data Services", Josh Howlett and Nick Skelton
  - "JANET Network Access and Last-mile Technologies", James Sankar
  - "The Wireless Campus Project", Elisa Marchioro
  - "Applying Radius-based Public Access Roaming in the Finnish University Network (FUNET)", Sami Keski-Kasari and Karri Huhtanen

- "Cross-organisational Roaming on Wireless LANs Based on the 802.1X Framework", Klaas Wierenga
- "Wbone: WLAN Roaming Based on Deep Security", Carsten Bormann

Acknowledgements

This report wishes to acknowledge the following people who have contributed to the work of the Task Force, both directly and indirectly.

TF-Mobility members who wrote the Task Force deliverables (in alphabetical order)

Carsten Bormann (University of Bremen)
Hansruedi Born (SWITCH)
Tim Chown (University of Southampton)
Paul Dekkers (SURFnet)
Erik Dobbelstijn (SURFnet)
Sami Keski-Kasari (Tampere University of Technology)
Ueli Kienholz (SWITCH)
Jardar Leira (UNINETT)
Niels Pollem (University of Bremen)
Juergen Rauschenbach (DFN)
James Sankar (UKERNA)
David Simonsen (UNI-C)
Roland Staring (SURFnet)
Klaas Wierenga (SURFnet)

TERENA

Licia Florio, Dick Visser

Thanks are also expressed to any other Task Force members not mentioned that have contributed at TF-Mobility meetings, and on the TF-Mobility mailing list.