Title: Preliminary selection for inter-NREN roaming

Version: 1.0

Published date: 19th December 2003

Editors: James Sankar (UKERNA)
Tim Chown (University of Southampton)

Contributors: Klaas Wierenga (SURFnet)
Ueli Kienholz (SWITCH)
Sami Keski-Kasari (FUNET)
TF Mobility Group
Table of Contents

1.0 ABSTRACT ...................................................................................................................... 3
2.0 INTRODUCTION ........................................................................................................... 4
  2.1 INTER-NREN ROAMING REQUIREMENTS ................................................................. 6
  2.2 VULNERABILITIES & LIMITATIONS: ..................................................................... 6
3.0 REVIEW OF NATIONAL ROAMING SOLUTIONS ...................................................... 9
  3.1 802.1X AUTHENTICATION SOLUTION .................................................................... 9
    3.1.1 PRE-REQUISITES ............................................................................................... 10
    3.1.2 LEVEL OF ADMINISTRATIVE OVERHEAD ...................................................... 10
    3.1.3 LEVEL OF USER TRANSPARENCY ................................................................. 11
    3.1.4 FALLOUT FOR NON-802.1X CLIENTS ............................................................. 11
    3.1.5 SECURITY ........................................................................................................... 11
    3.1.6 USER ACCOUNTABILITY .................................................................................. 12
    3.1.7 IMPACT OF NAT ON 802.1X .......................................................................... 13
    3.1.8 IMPACT OF THIS SOLUTION ON USER THROUGHPUT RATES ...................... 13
    3.1.9 SCALABILITY .................................................................................................... 13
  3.2 VIRTUAL PRIVATE NETWORK (VPN) BASED AUTHENTICATION SOLUTION ........ 15
    3.2.1 PRE-REQUISITES ............................................................................................... 16
    3.2.2 LEVEL OF ADMINISTRATIVE OVERHEAD ...................................................... 16
    3.2.3 LEVEL OF USER TRANSPARENCY ................................................................. 16
    3.2.4 SECURITY ........................................................................................................... 16
    3.2.5 USER ACCOUNTABILITY .................................................................................. 17
    3.2.6 IMPACT OF NAT ON THE VPN SOLUTIONS ................................................... 17
    3.2.7 IMPACT OF THIS SOLUTION ON USER THROUGHPUT RATES ...................... 17
    3.2.8 SCALABILITY .................................................................................................... 17
    3.2.9 THE WBONE APPROACH .............................................................................. 17
    3.2.10 A PKI APPROACH ......................................................................................... 18
  3.3 WEB REDIRECTION AUTHENTICATION SOLUTION ............................................... 19
    3.3.1 PRE-REQUISITES ............................................................................................... 20
    3.3.2 LEVEL OF ADMINISTRATIVE OVERHEAD ...................................................... 20
    3.3.3 LEVEL OF USER TRANSPARENCY ................................................................. 20
    3.3.4 SECURITY ........................................................................................................... 20
    3.3.5 USER ACCOUNTABILITY .................................................................................. 21
    3.3.6 IMPACT OF NAT ON WEB REDIRECTION AUTHENTICATION SOLUTION .... 21
    3.3.7 IMPACT OF THIS SOLUTION ON USER THROUGHPUT RATES ...................... 21
    3.3.8 SCALABILITY .................................................................................................... 21
  3.4 UNIVERSITY OF BRISTOL – ROAMNODE AUTHENTICATION SOLUTION ............ 23
    3.4.1 PRE-REQUISITES ............................................................................................... 25
    3.4.2 LEVEL OF ADMINISTRATIVE OVERHEAD ...................................................... 25
    3.4.3 LEVEL OF USER TRANSPARENCY ................................................................. 25
    3.4.4 SECURITY ........................................................................................................... 26
    3.4.5 USER ACCOUNTABILITY .................................................................................. 26
    3.4.6 SCALABILITY .................................................................................................... 26
    3.4.7 IMPACT OF NAT ON ROAMNODE ................................................................. 27
    3.4.8 IMPACT OF THIS SOLUTION ON USER THROUGHPUT RATES ...................... 27
4.0 PRELIMINARY SELECTION ............................................................................................ 28
5.0 INTEROPERABILITY ISSUES .......................................................................................... 30
  5.1 802.1X – INTRODUCTORY NOTES ............................................................................. 30
  5.2 INTEROPERABILITY SCENARIOS .............................................................................. 32
  6.0 PROPOSED APPROACH .............................................................................................. 42
1.0 Abstract

Wireless LAN technology (WLAN, according to IEEE 802.11*) is already an important part of the network access infrastructure at universities and research institutions connected to National Research and Education Networks (NREN’s) in Europe.

The TERENA Task Force Mobility Group (TF-Mobility group) has assessed national solutions that enable transparent Wireless LAN access for nomadic wireless users at different locations on a national level and has identified the requirements and additional work required to scale each national solution to a European level.

This deliverable will not select a single national solution as the recommended European model. This is because considerable investment has already been made to develop a variety of national solutions and it is unlikely that NREN’s will abandon their solutions in favour of a recommended one. Instead, this deliverable will list the interoperability issues between the national solutions, it will attempt to address what additional work is required from each solution to scale to a European level and specify the design requirements needed to develop a solution that can support the national solutions mentioned in this document.

This is a TF-Mobility group document.

The TF-Mobility group Terms of Reference are available at http://www.terena.nl/tech/task-forces/tf-mobility.

A table of planned deliverables is available at: http://www.terena.nl/tech/task-forces/tf-mobility/docs/DelList.pdf

This document follows the guidelines of the TF-Mobility group glossary of non-technical terms as outlined in http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/DelB/DelB_v1-3-5.pdf
2.0 Introduction

The number of academic institutions in European NREN’s deploying Wireless LANs is growing and the number of wireless users in each of these institutions is also increasing. It is now common to have wireless network access from buildings and external areas. Wireless access is also being extended to public areas such as cafés, airports and city centre areas offering wireless users the opportunity to gain access to university networks through a variety of wireless service providers. This expansion in network access opportunities enables wider access for local and visiting users in the academic community. It also requires the implementation of access control devices and security measures on home and visited institution networks to ensure that only approved users gain access to the wireless media and resources, and that external access is accountable in the event of abuse via the home or visited institution networks.

The access control and security measures taken by academic institutions differ significantly and this can also be the case between different departments within the same institution. One of the reasons for such disparity is the variety of wireless LAN standards and deployments, which has led to incompatibilities in providing seamless wireless access and security control mechanisms. The result is that the scalability of institutional level access control mechanisms to the national and international level has been challenging, technically, administratively and politically. The problems of scaling Wireless LAN technology at the national level led to the development of the TERENA sponsored Mobility group. The group exchanged experiences and knowledge of setting up national authentication infrastructures for wireless LAN access and discussed a range of wireless issues. After a number of meetings, the group decided to focus its attention on how it could scale national wireless LAN solutions to create a European solution that would enable a visiting user to gain transparent network access from any location (whereby the home institution was participating in the national roaming network and the visiting user was within the coverage area of an access control device) to gain access either to the Internet (once authenticated) or to the visiting user’s home institution (to authenticate there and be given network access via the home institution).

Such a roaming solution would be of particular benefit to academic staff who travel across Europe on research activities and do not want to manually request guest network access from an administrator for each visit (which is a drain on resource for the visiting user and the visited institution administrator).

A charter and list of deliverables was agreed by the Mobility group to work on a European solution, and TF-Mobility group was established under the auspices of the TERENA Technical Programme. The remit of TF-Mobility group was to investigate roaming for mobile devices using wireless access technologies already deployed (or planned) in the NREN’s. The agreed action plan was as follows:

1. Defining the requirements for an inter-NREN roaming architecture.
2. Evaluating possible authentication and authorisation techniques in mobile environments (e.g. via Web-redirection, RADIUS (Remote Authentication Dial-In User Service)+802.1X, or restricted target VPNs) for the research community in Europe;
3. Identifying the most suitable techniques, which will be standards-based, platform independent and use whenever possible infrastructures currently deployed in the NREN’s;
4. Describing the elements (trial plan) for a possible inter-NREN WLAN architecture based on these selected technologies;
5. Implementing and testing the proposed architecture amongst the participant NREN’s;

Activity points 1 and 2 have been completed. This document focuses on activity points 3 and 4.

Before focusing the preliminary selection of an inter-NREN wireless roaming solution, it is worthwhile briefly revisiting the inter-NREN roaming requirements agreed by the TF-Mobility group and reviewing these against the characteristics of each national solution to better understand the issues that each national solution must resolve to enable each to facilitate inter-NREN roaming across Europe.
2.1 Inter-NREN roaming requirements

It became evident early in the TF-Mobility group discussions that wired and wireless access and security methods have a strong overlap, e.g., an access control method for Wireless LANs could also be applied to wired networks at student dormitories.

As a result, the objective of the TF-Mobility group effort was to enable nomadic users to gain both wired and wireless network access either to the Internet or via authentication at their home institution whilst attending a participating visited institution that may traverse another NREN. The group’s main focus is on wireless access as this is currently where the explosion in usage is occurring, and where specific interest in security lies. As this requirement is related to solutions on both the national and international level, the results of the project are of value for the NREN’s own national roaming solutions, too.

When a visiting user connects to a visited institution network by either wired or wireless means anywhere in the NREN community of participating institutions, the following requirements for a roaming solution should be met as closely as possible:

**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.

2.2 Vulnerabilities & Limitations:

There are also a number of general and specific vulnerabilities and limitations that have been identified that must also be considered and where appropriate, measures taken to reduce risk.

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 not trusted, trusted 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. It will also place a significant bandwidth load on the VPN server, especially if a high volume of high capacity VPN links are being served (this may imply per-connection bandwidth limits are required).

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 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.

Before discussing a proposed solution to meet the original requirements, it is worthwhile revisiting each national solution’s characteristics and issues in relation to the group’s requirements to better understand interoperability and scaling issues that will be discussed later.

The solutions that were assessed were (1) an 802.1X authentication solution, (2) a VPN authentication solution (whereby access may be granted from the visited network only to a restricted list of known participating institution home VPN servers), including a VPN solution with certificate based Public Key Infrastructure (PKI), (3) a web-redirect based authentication solution and (4) a Linux based authentication solution based on PPPoE. Each solution will now be presented.
There may be additional solutions, but this group did not consider these as none of the TF-Mobility members were working on other solutions at that time. For example in the IPv6 context, the introduction of Mobile IPv6 (which is being ratified as an IETF Proposed Standard at the time of writing) may provide part of the solution.
3.0 Review of national roaming solutions

3.1 802.1X authentication solution

SURFnet has deployed a national Wireless LAN authentication solution based on the IEEE 802.1X standard.

802.1X was ratified by 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. 802.1X provides the means to transport user credentials to the visited institution’s authentication server and from there onto the visiting user’s home institution authentication server.

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 grow and harden in the next couple of years.

3.1.1 Pre-requisites

The following equipment is required at the home institution
- Access control devices that support 802.1X.
- For additional security the Access Control Device should also support IPSec.
- Switches supporting Virtual LAN segmentation.
- 802.1X client availability for mobile devices and their associated operating system software.\(^2\)
- 802.1X client software to be installed on mobile devices.

The following equipment is required at the home institution, regional and national level
- RADIUS server(s) with EAP protocol support (and for example EAP/TLS or EAP/TTLS as appropriate).
- RADIUS proxy server(s) with similar EAP protocol support.
- For additional security RADIUS server should support IPSec.
- Commonalities of approach – e.g. best practice guidelines on supporting visiting users, Virtual LAN assignment etc.

3.1.2 Level of administrative overhead

Each Wireless LAN must have appropriate 802.1X client software installed. Microsoft Windows XP and Windows 2000 operating systems support EAP and TLS. MacOS/X supports 802.1X with EAP-TLS or TTLS as of version 10.3\(^3\). Some administrative work may be required for earlier Windows versions, to install 802.1X client software. Administrators may be required to configure client software on mobile devices and set up user accounts for all local and visiting users. SURFnet is working with a vendor that is developing free 802.1X client software for a number of operating systems.

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. Given widespread adoption of techniques requiring RADIUS referral lookups, some redundancy or load balancing may be required in that set of referral servers, at the national and European level.

---

\(^2\) A list of 802.1X client support / operating systems can be seen at [http://www.surfnet.nl/innovatie/wlan](http://www.surfnet.nl/innovatie/wlan)

3.1.3 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), 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.

3.1.4 Fallback for non-802.1X clients

If a visiting user’s mobile device does not have 802.1X client software and is only offered access to 802.1X supported access control devices, non-802.1X authentication will not work. To resolve this problem, SURFnet are planning to develop a web page giving users some explanation of how to obtain an 802.1X account with a link to downloadable 802.1X client software.

3.1.5 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 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.

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.

For data integrity or privacy issues a variety of standards based committees have been working on a number of wireless security extensions (WPA, TKIP, 802.11i, etc.). These extensions are also building on the 802.1X framework. However, the current mechanism of refreshing WEP keys on a regular basis delivers a very high level of

---

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

5 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.
confidence that the encryption is resilient to being cracked (in contrast to earlier non-dynamic implementations). To support “Greenfield” sites, it is recommended that as many bit keys as possible be used to reduce the likelihood of WEP security being compromised together with additional security for example solutions at layer 3. To support legacy systems, it is recommended that 64-bit keys be used to ensure backward compatibility with old network adapters (the installed base of such adapters is significantly large that excluding them would be problematic from a usability perspective), however additional security measures should also be introduced.

Security in the RADIUS infrastructure is provided by the use of shared keys between RADIUS servers and by installing these servers in carefully designed secure parts of the national and international network. Every RADIUS peering must have its own shared key. However, some messages might be altered along the way, so in addition IPSec tunnels can be set up to protect the paths between RADIUS servers. This has been achieved successfully in the Netherlands and Finland.

When an 802.1X/RADIUS authenticates local and visiting users, these users can be differentiated by being assigned different VLANs with different access restrictions configured in each VLAN. This requires that the hardware used can place devices into multiple VLANs. More recent access points (e.g. Cisco 1200 series) have such functionality.

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.

3.1.6 User Accountability

It is hard to detect abuse in any authentication process when an abuser has the set of credentials of someone else. RADIUS enables detailed logging of both local and visiting user sessions, so complaints of a victim whose name was abused can be conducted with details of the actual sessions that the abuser has initiated.

Loss of credentials by a local or visiting user can be reported to the home or visited institution help desk. When the help desk disables the account (in either the user database or the organizational RADIUS server), no further abuse can take place.

Detection and prevention of abuse of bandwidth on layer 2 is a problem. Action can be taken to shape the traffic based on Virtual LAN parameters or limit up/downlink capacity in VPN concentrators or web-gateways, but this does not prevent users from flooding the air with big packets. When using 802.1X, the user sending these packets can be traced. On Layer 1, the administrator is helpless. Jamming the 2.4 GHz with a microwave or radio signal simply prevents access to the wireless medium. Studies of methods to counter denial of service attacks are being undertaken by the TERENA TF-CSIRT group.

Any “content” abuse can be traced back to a user account. At the moment, visiting user activity logging is related to IP-address assignment in the visited institution network. Any suspicious accounts or even entire realms can be blocked on any level in the architecture, thus preventing the suspicious visiting user or institution from logging on to the network at all.
3.1.7 Impact of NAT on 802.1X

802.1X is responsible for layer 2 access, after which layer 3 is transparently transported. Since NAT is in layer 3, it is supported like any other layer three protocol (like multicast or VPN for instance). SURFnet discourages the use of NAT amongst its customers because it causes too many restrictions. In general we discourage the use of NAT in any of the roaming solutions in this document.

3.1.8 Impact of this solution on user throughput rates

Encryption is done on the access control device, which is dimensioned to do encryption at wire (less) speed. No encryption bottleneck is introduced this way.

3.1.9 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. Two scenarios for 802.1X are;

a. A local user wants to get authenticated at their home institution. In this case the RADIUS server at the home institution authenticates the local user. The picture shows the elements that are needed for the authentication and authorisation. After this process, users can be connected to the Internet, the campus network or a faculties' LAN (by VLAN-assignment).

b. A visiting user wants to get authenticated at a visited institution. In this case the RADIUS server at the visited institution doesn’t recognise the user’s credentials, so these are forwarded to the national and possibly then the European RADIUS server and from there down to the RADIUS server at the user’s home institution where the authentication takes place. If a successful response is sent back to the access control device at the visited institution, the visited user mobile device is granted access to a Virtual LAN (VLAN).
The example below shows that guest access to a VLAN can be restricted; in this case the user is not allowed access protected UTwente resources, but is only given access to the SURFnet backbone. If Alfa&Ariss uses certificates (TLS) to authenticate its users, the UTwente does not have to configure this mechanism separately, even if the UTwente would only use Username/Password (TTLS). Because the authentication request is transparently forwarded to the users' home RADIUS server, this RADIUS server handles the complete authentication process.
3.2 Virtual Private Network (VPN) based authentication solution

SWITCH has deployed a roaming system for Switzerland based on VPNs. This system (called SWITCHmobile) interconnects 12 Universities and research institutions at this the time of writing. At the state of Bremen a roaming system (called Wbone) has been deployed that comprises 5 academic organisations. These two systems are conceptually almost identical. For clarity the following section summarises SWITCHmobile only. Differences to Wbone are outlined at the end of the section.

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. 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.
3.2.1 Pre-requisites

The following equipment is required at each home institution:

- One or more VPN gateways. Alternatively, a gateway based on SSL may be installed that allows remote access to the most relevant services with just a web browser.
- “Open” docking networks (no layer 2 authentication or encryption methods imposed).
- Protection of these docking networks by an ACL in order to prevent anonymous users from using the infrastructure.
- VPN client software to be installed on the mobile devices (this is not required, if there is a gateway that allows remote access via web browsers).

The following equipment is required on regional or national level:

- A managed list of the organisations and their trusted VPN gateways.

3.2.2 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.

3.2.3 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).

3.2.4 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.
3.2.5 User Accountability

At visited institutions, a visiting user always appears to originate from their home institution, because they authenticate and obtain their IP address from there\(^6\). Any remote hacking will seem to come from the home institution, wherever the visiting user actually is physically located. Therefore it is the responsibility of the home institution to be able to trace the VPN source back to their user. In this situation, the visited institution is not concerned about by the visiting user abuse.

3.2.6 Impact of NAT on the VPN solutions

The SWITCHmobile-approach has nothing to do with NAT.

However, if a docking network is behind a NAT-box (which is optional) then only those users equipped with a NAT-traversable VPN software will be able to use it.

3.2.7 Impact of this solution on user throughput rates

All VPN traffic is tunnelled to the home institution – thus some network paths will be longer than required, i.e. general web browsing will go via the VPN gateway at the home institution. The VPN server will have to cope with potentially very high bandwidth demands by high volumes of high capacity remote VPN users. As a result, bandwidth limitations per connection may be required.

3.2.8 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).

3.2.9 The Wbone Approach

As mentioned earlier, the Wbone approach at Bremen is conceptually almost identical to SWITCHmobile with the following exception: a specific address space is used for all docking networks and VPN gateways. At Bremen it is private space - but it could be global space instead with no implications on the concept. The implemented routing makes sure that this address space only can be left via one of the VPN-gateways. This replaces the ACL-concept of SWITCHmobile by introducing a specific address space and specific routing across all organizations involved.

---

\(^6\) This scenario assumes that the user is not permitted any form of network access other than to establish a VPN and therefore hacking should not occur prior to authentication at home.
3.2.10 A PKI Approach

A completely different approach has been tested at the Technical University of Lisbon. This approach assumes that visiting users establish a standard IPSec connection to an IPSec gateway at the visited institution (in contrast to the SWITCHmobile/Wbone approach, where a connection is established right through to the home institution's gateway). Authentication takes place at the IPSec gateway of the visited organisation and is performed by verifying the user's client certificate using a certificate chain. Scalability certainly is not an issue here.

A method is proposed that greatly simplifies the generation of keys and downloading certificates for the user. This approach hides almost all the complexity of certificates from the user - while accepting that the private key of a user is stored on a server of his home organisation.
3.3 Web redirection authentication solution

When visiting users attach to a visited institution network that uses a web redirection authentication solution, they get an initial docking IP address (and associated local network configuration) via DHCP, but are initially unable to receive and send traffic outside the visited institution network.

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\(^7\)). 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.

Detaching the visiting user from the visited institution network may be initiated by the visiting user or by the visited institution network. When the visiting user wants to log out, there may be some kind of form or popup windows for sending the logout message. The pop-up window and regular re-registrations via HTTP may be used for ensuring the visiting user's mobile device does not remain connected and can be automatically logged out. Another method requires the access control device to frequently poll the visiting user mobile device with ARP or ICMP requests to detect if the mobile device has left the visited institution’s network. If the visiting user’s mobile device does not reply within a specific number of requests, the mobile device

\(^7\) 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.
is considered detached from the visited institution network and the access control
device closes the firewall rules to prevent session hijacking.

Commercial WLAN hotspots such as those from BT Openzone and Telia Homerun
both use the web-redirection based authentication method.

3.3.1 Pre-requisites

The following equipment is required at the home institution
- Any device that has a Web browser that supports HTTP, HTTPS with
  TLS/SSL capability, network interface card and DHCP client.
- For additional security the Access Control Device should also support IPSec.

The following equipment is required at the home institution, regional and national
level
- RADIUS server(s).
  - For additional security RADIUS server should support IPSec.
  - For better performance the authenticating RADIUS server should use
    an SQL database or LDAP for storing credentials.
- RADIUS proxy server(s).
- Commonalities of approach – e.g. best practice guidelines on supporting guests
  users, Virtual LAN assignment etc.

3.3.2 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.

3.3.3 Level of user transparency

User transparency will be high, as the user only requires an http-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.

3.3.4 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. Unrestricted access requires a determined deliberate act rather than one
where the user unwittingly stumbles into gaining access. Security can be tightened by
using SSL for authentication to prevent unauthorised users from accessing the access
control devices. Also, signed certificates from a trusted authority would overcome
“man-in-the-middle” attacks, however this has not been implemented as yet.
It should also be noted that DHCP is rarely (if ever) deployed with any authentication extensions (as per RFC3118). It may thus be possible for example for a rogue DHCP server to provide bogus address and other configuration information. This is a generic issue with any DHCP-based network.

3.3.5 User Accountability

From an access control device, the visiting user inserts their credentials to a web form. The access control device sends authentication credentials as RADIUS requests via a RADIUS hierarchy to the user's home institution's authentication server. Once authenticated, the visiting user is given Internet Access on an appropriate VLAN. There is no VPN connection established via the user's home institution for access to the Internet. This solution may assign IP addresses either statically or (more likely) dynamically using DHCP to authorized visiting users. The facility to log visiting user activity to resolve any user accountability related queries is achieved via RADIUS accounting, where the access control device logs accounting messages including the IP address supplied to the visiting user's IP-address, amount of transferred data, etc.

The authentication is performed at the home institution’s RADIUS server and logged there. The forwarding of the request may also be logged at the visited institution, and tied to the IP address assigned to the visited user’s mobile device.

3.3.6 Impact of NAT on web redirection authentication solution

The local user device could be assigned a NATed address and NAT can be used for outbound connections. This solution does work with NAT but it is strongly recommended that the use of NAT is restricted because of the many highlighted issues with NAT that have been identified by various technical and user groups. If NAT is used, only the access control device should be without NAT because it is a part of RADIUS hierarchy.

3.3.7 Impact of this solution on user throughput rates

The current processing power of today’s computers mean that the speed of network access control is not a problem. For example Linux boxes can IP filter at wire speeds in Gigabit Ethernet. The bottleneck is the access control device's uplink speed. There can also be traffic prioritisation methods applied that restrict certain traffic over others in particular states, for example Voice over IP traffic can be in a higher class or priority than http traffic. If congestion occurs, lower priority traffic can be dropped.

3.3.8 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.
This solution uses RADIUS but it doesn’t have to, however, it is recommended, as this is the best way to interoperate with other national solutions.
3.4 University of Bristol – 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.

Below is an example of the Roamnode solution at Bristol University.

A user visits another institution that has a local node installed. The visiting users mobile device connects to the docking network by attaching to a fixed network point or associating with an access control device.

The mobile device initiates a PPPoE session with the Localnode. The mobile device attempts to authenticate by passing a user name of the format “user@realm” with a secure hash of the user's password to the Localnode. The Localnode generates a RADIUS ACCESS-REQUEST packet that is passed to an internal RADIUS proxy...
daemon. The request also contains the NAS-IDENTIFIER attribute, which uniquely identifies the Localnode and the RFC1918 address space associated with the docking network. A local user's realm is known on this Roamnode and the request is passed to the home institution’s authentication server that is associated with the VPN gateway.

If the visiting user’s realm is recognised as being associated with a VPN gateway on another known Roamnode then the request is proxied to that Roamnode. Finally, if the daemon does not recognise the realm the request is passed to a “default” RADIUS proxy server with the expectation that the request will be passed through a RADIUS hierarchy until it eventually reaches the visiting user's Homenode residing at that user’s home institution.

If the AAA server associated with the Homenode authenticates the request it returns a RADIUS ACCESS-ACCEPT reply to the Localnode via the Homenode. The Homenode builds an IP-in-IP tunnel to the Localnode indicated in the NAS-IDENTIFIER attribute, and adds a route to the docking network via the tunnel. When the Localnode receives the reply it builds an IP-in-IP tunnel to the Homenode and adds a route to the VPN gateway via the tunnel. The Localnode also adds a firewall rule allowing packets to flow between the mobile device and the Homenode.
Finally, the mobile device connects to the VPN gateway using a VPN client. The VPN gateway provides the mobile device with an IP address from network associated with the VPN gateway, and hence an address from the home institution. The visiting user's traffic is forwarded between the VPN gateway and the mobile device via the Homenode and the Localnode using the IP-in-IP tunnel.

3.4.1 Pre-requisites

An institution that deploys the Roamnode architecture and peers with the NREN’s national RADIUS proxy server does not require any additional infrastructure to act either as a visited institution or as a home institution. An institution that wishes to be a visited institution can install a Roamnode on their network, acquire an allocation of RFC1918 address space for the docking network, and arrange a trust relationship with the national RADIUS proxy server. An institution that wishes to be a home institution can install a Roamnode on their network, configure as many VPN gateways as required, and arrange a RADIUS trust relationship with the national RADIUS proxy server.

3.4.2 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.

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.

3.4.3 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.
3.4.4 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.

3.4.5 User Accountability

User accountability would be found in both the visited and home institution’s RADIUS server accounting logs. If a user is found to be either unauthorized or has breached an acceptable use policy, the home institution can block abusive users, although measures could be enforced at any point along the RADIUS hierarchy to block RADIUS packets relating to that user.

3.4.6 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. The Roamnode could be run on a redundant PC for example.

---

8 This is not exclusively so as HostAP (Linux free AP supports 802.1X)
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.

Windows XP requires no additional software or patching. Windows 2000 requires a PPPoE client. Windows 95/98/Me require DUN patches to update the encryption and a PPPoE client. There are many freeware PPPoE clients, such as RASPPPoE. MacOS 10.2 requires no additional client software. Linux support varies according to distribution. However, client software is freely available.

No PDA Operating Systems currently support PPPoE, though support for PPPoE is likely to become more widespread in the next operating system iteration. Most North American and many European ISPs and Wireless ISPs are using PPPoE in preference to bridged Ethernet and DHCP. Experience at the University of Bristol is that approximately 95% of users are able to connect first time to the service without support by following the documentation provided.

3.4.7 Impact of NAT on Roamnode

This does not require NAT. The mesh network removes the requirement for NAT because the visited institution does not provide any of its own address space to visiting users.

3.4.8 Impact of this solution on user throughput rates

The encryption is handled in the Homendoe, this relieves the access control device from the encryption processing, thus increasing throughput over the wireless network. Roamnodes can also be clustered to allow load sharing.
4.0 Preliminary selection

The original aim of this deliverable was to agree on one national roaming solution and design a scalable and interoperable architecture based on that recommendation across Europe. From investigations and discussions so far, it is clear that there is no single solution that meets all the requirements, or can address the vulnerabilities and limitations identified. It is also impractical to expect NREN’s to abandon their existing national solutions in favour of another approach, but they might be willing to modify existing deployments to support interoperability.

This paper recommends the development of a European solution that can support the variety of national solutions, that can meet as many of the requirements outlined, that can address most of the identified vulnerabilities and limitations and can support as much interoperability between each national solution as possible. Ideally, the longer-term aim remains to move towards a single solution, but this is unlikely to be practical for some time.

Whilst considering interoperability issues between the national solutions, the TF-Mobility group identified a "multidimensional problem" that needs to be resolved in order to develop a scalable European solution that can support the range of national solutions previously described. The “problem needs to be carefully considered in deliverable H to be able to design and test a pragmatic, yet flexible solution and this should be reflected as policy or guidelines for those who wish to participate in the development, testing and operation of mobility solutions.

**Dimension 1 = Visiting User Access to the Visited Institution network**

802.1X, VPN (in IPSec), web-redirection-based, mesh overlay network

There are differences in terms of the client software loaded onto the mobile device and the access control device, see the table below

<table>
<thead>
<tr>
<th>National Solution</th>
<th>Client</th>
<th>Access Control Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>802.1X capable Access control devices</td>
<td>Access control device</td>
</tr>
<tr>
<td>VPN</td>
<td>Needs VPN capability</td>
<td>One access control device between docking network and CASG (which does not do any AAA itself, just limits access to the CASG)</td>
</tr>
<tr>
<td>VPN &amp; PKI (IPSec)</td>
<td>Needs VPN capability to find the most useful local VPN gateway.</td>
<td>VPN gateway in the visited institution as the access control device</td>
</tr>
<tr>
<td>Web-based</td>
<td>Web browser with TLS/SSL capability</td>
<td>Access control device between the docking network and the Internet, but often not (never?) in the AP</td>
</tr>
<tr>
<td>“Roamnode”</td>
<td>A client capable of</td>
<td>RADIUS or VPN Gateway at</td>
</tr>
</tbody>
</table>
Supporting PPPoE to the home institution (and HomeNode?)

**Dimension 2 = Visiting User Access to the Home Institution Network – (the mechanics are in place for AAA validation)**

RADIUS, Certificates, CASG

<table>
<thead>
<tr>
<th>Solutions</th>
<th>RADIUS</th>
<th>Security Certificates</th>
<th>CASG</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>VPN</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
</tr>
<tr>
<td>VPN &amp; PKI (IPSec)</td>
<td>NO</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>Web based</td>
<td>YES</td>
<td>NO</td>
<td>NO</td>
</tr>
<tr>
<td>Roamnode</td>
<td>YES</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>
5.0 Interoperability issues

The three main authentication solutions (802.1X, VPN and web-based redirection) will now be assessed in terms of their interoperability with each other. Roamnode will not be assessed, as it is an independent system that requires software enhancements to achieve interoperability with the other solutions.

5.1 802.1X – Introductory notes

802.1X based authentication on the one side and Web- and VPN-based authentication on the other side pose different demands on the wireless LAN networks. Where 802.1X enabled wireless networks require an encrypted channel (with dynamic WEP-keys), the two other mechanisms are based on the concept of open, unencrypted access to the docking network. The result of these two 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 that is capable of using multiple SSID’s and that supports VLAN assignment his leads to the following site configuration:

It should be noted that in the current generation of access points it is impossible to broadcast both configured SSID’s at the same time.
When it is imperative that all SSID’s are visible or when the access points are not capable of assigning VLAN’s, it may be imperative to create an infrastructure that is separated on layer 1, leading to the following site configuration:

For the remainder of this chapter the first setup will be assumed when using 802.1X based authentication in combination with one of the other methods.
5.2 Interoperability Scenarios

The following table shows that how the nine scenarios are related with each other:

<table>
<thead>
<tr>
<th>User@</th>
<th>802.1X</th>
<th>VPN</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>(1)</td>
<td>(2)</td>
<td>(3)</td>
</tr>
<tr>
<td>802.1X</td>
<td>(4)</td>
<td>(5)</td>
<td>(6)</td>
</tr>
<tr>
<td>VPN</td>
<td>(7)</td>
<td>(8)</td>
<td>(9)</td>
</tr>
</tbody>
</table>

5.2.1 Guest Access at a “802.1X” visited institution network

5.2.1.1 802.1X User at Remote 802.1X Site

Site Configuration

Docking network with DHCP, WEP and 802.1X authentication: Access points are connected to a layer 3 switch, which is responsible for inter-VLAN routing. Depending on the 802.1X authentication credentials users are placed in a particular (employee, student, guest etc.) VLAN.

User Experience / Logon Procedure

Depending on the operating system and the used 802.1X client the following procedure may be slightly different. In general an 802.1X user who wants to connect on a remote 802.1X site has to

- Connect their device to the docking network (by wire or wirelessly),
- Logon to the 802.1X network (-> 802.1X client sends credentials, after successful authentication the device receives IP configuration via DHCP).
5.2.1.2 VPN User at Remote 802.1X Site

Site Configuration

<table>
<thead>
<tr>
<th>SSID (e.g.)</th>
<th>VLAN-ID (e.g.)</th>
<th>Purpose</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>5</td>
<td>VPN and web user</td>
<td>Open, no WEP, DHCP</td>
</tr>
<tr>
<td>802.1X</td>
<td>10</td>
<td>802.1X user</td>
<td>802.1X, WEP, DHCP</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

Docking network containing access points capable of handling multiple SSIDs: SSIDs are mapped to VLANs (Table 1). Access points are connected to a layer 3 switch, which is responsible for inter-VLAN routing. VPN users connected to SSID “VPN” are granted (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E) implemented with an ACL on the layer 3 switch. 802.1X users connected to the SSID “802.1X” are granted access to the Internet upon successful authentication over RADIUS-hierarchy.

User Experience / Logon Procedure

A VPN user who wants to connect on a remote 802.1X site has to

- Connect their device to the docking network (SSID VPN, automatically receives IP configuration via DHCP),
Start their VPN client and login at the home site (access is granted to resources at the home site as well as to the Internet (via home site)).

5.2.1.3 Web User at Remote 802.1X Site

Site Configuration

![Diagram](image)

**Figure 3: Web roaming at 802.1X site**

<table>
<thead>
<tr>
<th>SSID (e.g.)</th>
<th>VLAN-ID (e.g.)</th>
<th>Purpose</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>2</td>
<td>VLAN for access points, RADIUS server</td>
<td>Open, no WEP, DHCP</td>
</tr>
<tr>
<td>802.1X</td>
<td>5</td>
<td>VPN and web user</td>
<td>802.1X, WEP, DHCP</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>802.1X user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2: VLAN configuration**

Docking network containing access points capable to handle multiple SSIDs: SSIDs are mapped to VLANs (Table 2). Access points are connected to a layer 3 switch, which is responsible for inter-VLAN routing. Web users connected to SSID “VPN” are granted (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E) implemented with an ACL on the layer 3 switch. 802.1X users connected to the SSID “802.1X” are granted access to the Internet upon successful authentication over RADIUS-hierarchy.
User Experience / Logon Procedure

A web user who wants to connect to the Internet on an 802.1X site has to

- Connect their device to the docking network (SSID VPN, automatically
  receives IP configuration via DHCP),
- Start a web browser, access any web page (-> automatic redirection to a login
  web page with additional information about the roaming system takes place),
- Enter credentials at the web page (-> access to the Internet is granted either for
  a limited amount of time or until a timeout occurs).
5.2.2 Guest Access at a “VPN” visited institution network

5.2.2.1 802.1X User at Remote VPN Site

Site Configuration

<table>
<thead>
<tr>
<th>SSID (e.g.)</th>
<th>VLAN-ID (e.g.)</th>
<th>Purpose</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>5</td>
<td>VPN and web user</td>
<td>Open, no WEP, DHCP</td>
</tr>
<tr>
<td>802.1X</td>
<td>10</td>
<td>802.1X user</td>
<td>802.1X, WEP, DHCP</td>
</tr>
<tr>
<td>Internet</td>
<td>15</td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: VLAN configuration

Docking network containing access points capable to handle multiple SSIDs: SSIDs are mapped to VLANs (Table 3). Access points are connected to a layer 3 switch, which is responsible for inter-VLAN routing. VPN users connected to SSID “VPN” are granted (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E) implemented with an ACL on the layer 3 switch. 802.1X users connected to the SSID “802.1X” are granted access to the Internet upon successful authentication over RADIUS-hierarchy.

User Experience / Logon Procedure

Depending on the operating system and the used 802.1X client the following procedure may be slightly different. In general a 802.1X user who wants to connect on a remote VPN site has to

- Connect their device to the docking network (SSID 802.1X),
- Logon to the 802.1X network (-> 802.1X client sends credentials, after successful authentication notebook receives IP configuration via DHCP).
5.2.2.2 VPN User at Remote VPN Site

Site Configuration

Docking network with DHCP, no WEP, which terminates at an access control device: Access control list on this device grants (unauthenticated) access to a list of address ranges (one address range per NREN). This list of address ranges is called CASG (for details see Deliverable E).

User Experience / Logon Procedure

A VPN user who wants to connect on a remote VPN site has to

- Connect their device to the docking network (automatically receives IP configuration via DHCP),
- Start their VPN client and login at the home site (-> access is granted to resources at the home site as well as to the Internet (via home site)).
5.2.2.3 Web User at Remote VPN Site

Site Configuration

Docking network with DHCP, no WEP, which terminates at an access control device, such as a captive portal: The access control device grants (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E). Access to all other addresses by so far unauthenticated users is redirected to a login web page and credentials are verified via RADIUS-hierarchy.

User Experience / Logon Procedure

A web user who wants to connect to the Internet on a VPN site has to

- Connect their device to the docking network (automatically receives IP configuration via DHCP),
- Start a web browser, access any web page (-> automatic redirection to a login web page with additional information about the roaming system takes place),
- Enter credentials at the web page (-> access to the Internet is granted either for a limited amount of time or until a timeout occurs).
5.2.3 Guest Access at a “web-based redirection” visited institution network

5.2.3.1 802.1X User at Remote Web-based redirection site

Site Configuration

![Figure 7: Web roaming at 802.1X site](image)

<table>
<thead>
<tr>
<th>SSID (e.g.)</th>
<th>VLAN-ID (e.g.)</th>
<th>Purpose</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>2</td>
<td>VLAN for access points, RADIUS server</td>
<td>Open, no WEP, DHCP</td>
</tr>
<tr>
<td>802.1X</td>
<td>5</td>
<td>VPN and web user</td>
<td>802.1X, WEP, DHCP</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>802.1X user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

Table 4: VLAN configuration

Docking network containing access points capable to handle multiple SSIDs: SSIDs are mapped to VLANs (Table 4). Access points are connected to a layer 3 switch, which is responsible for inter-VLAN routing. Web users connected to SSID “VPN” are granted (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E) implemented with an ACL on the layer 3 switch. 802.1X users connected to the SSID “802.1X” are granted access to the Internet upon successful authentication over RADIUS-hierarchy.

Switches now support functionality allowing a port to be in one VLAN in “open mode” and the client then starts 802.1X authentication. After successful authentication the client will be connected to an appropriate VLAN. The same port can be used for 802.1X, VPN and web users. If or when access points support this kind of functionality, the same SSID can be used for all three authentication methods.
User Experience / Logon Procedure

An 802.1X user who wants to connect to the Internet or a web site has to

- Connect their device to the docking network (SSID 802.1X),
- Logon to the 802.1X network (→ 802.1X client sends credentials, after successful authentication the device receives IP configuration via DHCP).

5.2.3.2 VPN User at Remote Web-based redirection site

Site Configuration

Docking network with DHCP, no WEP, that terminates at an access control device, such as a captive portal: The access control device grants (unauthenticated) access to a list of address ranges (CASG, for details see Deliverable E). Access to all other addresses by as-yet unauthenticated users is redirected to a login web page and credentials are verified via the RADIUS hierarchy.

User Experience / Logon Procedure

A VPN user who wants to connect on a remote web site has to

- Connect their device to the docking network (automatically receives IP configuration via DHCP),
- Start their VPN client and login at the home site (→ access is granted to resources at the home site as well as to the Internet (via home site)).
5.2.3.3 Web User at Remote Web-based redirection site

Site Configuration

Docking network with DHCP, no WEP, which terminates at an access control device, such as a captive portal: Unauthenticated users are redirected to a login web page and credentials are verified via RADIUS-hierarchy. There should be a European wide CA hierarchy to ensure that the captive portal is really for authentication to the network instead of capturing usernames and password. Or at least there must be some trusted place where users can get the roaming organisation’s CA certificate.

User Experience / Logon Procedure

A web user who wants to connect to the Internet on a web site has to

- Connect their device to the docking network (automatically receives IP configuration via DHCP),
- Start a web browser, access any web page (-> automatic redirection to a login web page with additional information about the roaming system takes place),
- Enter credentials at the web page (-> access to the Internet is granted either for a limited amount of time or until a timeout occurs).
6.0 Proposed Approach

The TF-Mobility group will 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.

A phased development and testing programme is recommended. The proposed phased plan is described below:

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. The first task, to resolve scaling and interoperability issues for each national solution, should be complete and captured within this Deliverable G document. Each stream of work will now be described.
6.1 Build & Scale a RADIUS Proxy hierarchy for non-VPN AAA networks (and test interoperability with VPN networks)

To scale SURFnet’s 802.1X national roaming solution and FUNET’s web redirection based authentication solution requires the national RADIUS proxy hierarchies in both countries to be extended. In order to make this work, the RADIUS servers need to know where to route the RADIUS requests based on the realm provided by the visiting user. The most scalable approach is a three-step RADIUS architecture where there exists a top level RADIUS server (provided by TERENA or some “neutral” organisation), where this top-level server establishes a trust relationship with all participating NREN level RADIUS servers. These NREN level RADIUS servers establish a trust relationship with all their participating subordinate RADIUS servers in that NREN. A subordinate server checks the realm to see whether it is local, if not the request gets forwarded to NREN level RADIUS server, if the request is not nationally recognised, it is forwarded onto the top-level server that in turn forwards the requests to the appropriate NREN and subordinate RADIUS server that in turn checks the authentication information and grants authorisation at the home institution.

This means that the realm should include institution information, requests that could for instance be in the form `user@institution`. There would also need to be some form of central co-ordination, the TF-Mobility group and their existing mailing list could manage this.

Alternatively, it would be possible for each RADIUS at the NREN level to trust the other NREN RADIUS servers at the same level, but the three-tier system simplifies the trust configuration at the expense of one extra redirection. Ideally the Top level and National RADIUS Proxy Servers should be duplicated for resilience. The TF-Mobility group recommended the three-tier approach because it would be more manageable and scalable and ensure all NREN’s have a single point of contact for RADIUS administration issues.

SURFnet has proposed to build and configure a top tier RADIUS server that NREN level RADIUS servers could direct visiting users to, to authenticate at their home institution for the purpose of an initial trial. This server would be housed at SURFnet but could be moved to TERENA (so long as there are resilient links to this server).
This has in fact already been successfully tested at a very small scale by a number of TF Mobility members with SURFnet, using a site-national-European RADIUS hierarchy, a Radiator RADIUS server and EAP-TTLS.

To overcome the limitations of a hierarchical network, a mesh network could be designed to address latency and single points of failure, however it is more likely that the architecture will be more costly and complex with additional management overheads at all levels from the campus/site level to the NREN level. Indeed, a mesh between all participating sites would simply not be scalable or manageable. A compromise solution is to (1) duplicate RADIUS servers at the national and top-level and (2) if institutions within a national country do have a significant number of nomadic users or reasonable resilience concerns, that they can be permitted to establish another link from their institution RADIUS server to another institution dependent of the hierarchy. This would add resilience and reduce latency in passing authentication requests via the national and possibly top-level RADIUS server.

If a NREN with a group of institutions wishes to participate in a European level 802.1X wireless roaming service, participation guidelines and an AUP must be accepted\(^9\) and then the Top level RADIUS Proxy Server must be updated with the new high-level domain for that NREN (for instance “.nl”), after which the forwarding mechanism works for each institution in that constellation thereafter.

In deploying a RADIUS hierarchy, there is an added benefit that sites running a web-redirect challenge authentication can share the same back-end authentication mechanism, thus supporting nomadic users at sites running either (or both) methods.

To give a good indication of the effort that is necessary to set up a proxy infrastructure, the configuration items of each element in the architecture are depicted below.

A) Organisational RADIUS Proxy Servers (ORPS) must

- Handle requests for its own realm
- Forward requests for other realms to the National RADIUS Proxy Server
- All RADIUS attributes must be forwarded transparently to ensure EAP-transparency
- Accept requests coming from National RADIUS Proxy Servers. Therefore, the IP addresses of the RADIUS servers must be exchanged and a RADIUS Secret must be determined for use between each National RADIUS Proxy Server and the European Top level RADIUS Proxy Server (one for each direction). The port number will be 1812
- Forward accounting messages transparently on port 1813
- Prevent looping by not forwarding requests to the server where they came from
- Be implemented in pairs (a primary and a secondary), each Organizational RADIUS Proxy Server sending requests to a secondary server when the primary is down. After a timeout, it should try to reach the primary again. Timeouts and fallback rules must be in line with the optimal performance parameters of the underlying access infrastructure (the Access control devices and switches)

\(^9\) This documentation would be part of deliverable H.
TF-Mobility Group  Deliverable G

- Log at least time, date, username and realm, accept/deny of each request and preferably the IP address that was assigned to the user
- (Optional) the communication with a National RADIUS Proxy Server can be encrypted with SSL or IPSEC for additional security
- May strip optional RADIUS attributes of incoming Accept-Accept messages that are only relevant in the context of the home institution RADIUS domain of the guest (e.g. VLAN assignment)
- A test account within the realm of the ORPS is necessary for testing purposes

In the organizational RADIUS infrastructure, existing RADIUS servers can carry out EAP handling in addition to existing authentication services such as dial-in services. RADIUS servers may also refer to local authentication schemes, e.g. the Radiator package can refer requests to local NIS authentication.

The guidelines as described here are only relevant for the EAP-handling and forwarding. It is possible to directly connect certain Organizational RADIUS Proxy servers when they are already closely related and they are likely to exchange a lot of requests. This can be the case when a couple of organizations reside on a single home institution, with many of their local users gaining network access at each other’s buildings.

B) The National RADIUS Proxy Servers (NRPS) must

- Forward requests based on second-level realm (utwente.nl, ukerna.ac.uk etc)
- All RADIUS attributes must be forwarded transparently to ensure EAP-transparency
- Accept requests coming from trusted top level RADIUS Proxy Servers and Organizational RADIUS Proxy Servers. Therefore, the IP addresses of the RADIUS servers must be exchanged and a RADIUS Secret must be determined for use between each National RADIUS Proxy Server and the European Top level RADIUS Proxy Server (one for each direction). The port number will be 1812
- Forward accounting messages transparently on port 1813
- Prevent looping by not forwarding requests to the server where they came from
- Be implemented in pairs (a primary and a secondary), each Organizational RADIUS Proxy Server sending requests to a secondary server when the primary is down. Timeouts, retries and fall-back to the primary when it is up again must be tuned to achieve optimal performance in combination with the values of these parameters at organizational level.
- Log at least time, date, username and realm, accept/deny of each request
- (Optional) the communication to and from the National level RADIUS Proxy Server can be encrypted with SSL or IPSEC for additional security
- A test account within the realm of the NRPS is necessary for testing purposes.

A choice can be made to let the National RADIUS Proxy Server handle subrealms as well, for instance the .uk NRPS can also process the ac.uk. It is also possible to insert any number of sublevels with corresponding RADIUS servers for that level in a country (for instance state-level servers or even regional level servers).
TF-Mobility Group

Deliverable G

It is possible that parallel proxy-infrastructures will arise for the same national level domain, for instance a commercial RADIUS clearing house. The exchange of subrealms that each proxy handles can be handled in an administrative process.

C) The Top level RADIUS Proxy Server (TRPS) must

- Forward requests based on top-level realm (.nl, .ch, ac.uk, .be, etcetera)
- All RADIUS attributes must be forwarded transparently to ensure EAP-transparency
- Accept requests coming from National RADIUS Proxy Servers Therefore, the IP addresses of the RADIUS servers must be exchanged and a RADIUS Secret must be determined to be used between each National RADIUS Proxy Server and the (European) Top level RADIUS Proxy Server (one for each direction). The port number will be 1812
- Forward accounting messages transparently on port 1813
- Prevent looping by not forwarding requests to the server where they came from
- Be implemented in pairs (a primary and a secondary), each National RADIUS Proxy Server sending requests to a secondary server when the primary is down. Timeouts and retries must be tuned.
- Log at least time, date, username and realm, accept/deny of each request

The communication links between a National RADIUS Proxy Server and the European Top level RADIUS Proxy Server to pass authentication requests can be encrypted with SSL or IPSEC for additional security.

TF-Mobility group members have successfully demonstrated this RADIUS backend approach between the UK, Portugal, Croatia, Germany and the Netherlands using 802.1X with EAP/TTLS, and a Radiator RADIUS server\(^\text{10}\) at all participating institutions for this demonstration. Finland has also recently confirmed a link to this hierarchy at the TF-Mobility meeting in September 2003. It is envisaged that Deliverable H will test the RADIUS proxy hierarchy and result in an agreed user@realm standard and a defined list of minimum requirements for protocols carried by EAP, and / or considerations of those protocols themselves to form guidelines for NRENs and possibly institutions too.

The RADIUS Proxy hierarchy is currently in place and the participation of other NRENs should be encouraged to enable the TF-Mobility group to gain as much practical experience as is possible. Participation guidelines, AUP, best practice for national and campus level implementations, and standard naming conventions need to be documented to ensure a manageable growth of this hierarchy.

Where possible, tests should be undertaken between the RADIUS hierarchy and the VPN networks to attempt some form of interoperability to support VPN users visiting non-VPN networks and non-VPN users visiting VPN networks.
6.2 Document and build an overlay network based on a Controlled Address Space for VPN Gateways (CASG)\textsuperscript{11} design.

A proposed solution to solve the VPN scalability problem is to use CASG, which are IP address ranges, one that each NREN has obtained for themselves. In this way the packet exchanging between the CASG network and the VPN gateway should be secure.

Participation guidelines, AUP, and best practice for VPN gateway implementations would need to be documented to ensure a manageable growth of the CASG.

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

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{diagram.png}
\caption{Proposed Architecture for Scalable Wireless Roaming VPN Solution}
\end{figure}

If one assumes that there are 640 million people at European Union level, the TF Mobility group assumes 16,000 public IP addresses need to be reserved. The calculations are based on the University of Bremen’s experience of developing a national VPN solution and has been extended and based on the total European population.

These numbers do not consider public hot spots, and the Netherlands and Finland do not have VPN concentrators, so it would be difficult for these to participate unless additional VPN equipment is bought. This solution is complex and finite, as one has to determine how much address space to allocate. Extending the address range in the future may be too complex and time consuming to be achieved.

\textsuperscript{11} An option to extend the list of all VPN gateways to resolve VPN scaling issues was considered and was not practical as access control lists containing several thousand entries would need to be kept up to date at thousands of access control devices throughout Europe. This method incurs too much administrative overhead resulting in an unresponsive solution. The access control list would be in the public domain and would need to be password protected, further complicating the management / administrative process.
This work can be done in parallel to RADIUS interoperability testing. The first activity would be to document the technical specifications, proposed implementation plan and highlight any possible security considerations. One documented and agreed by the TF-Mobility group, the CASG can then be build and tested. Tests should be undertaken to (1) attempt to automate the updating of Access Control Lists and (2) extend the CASG to possibly integrate with the RADIUS Proxy hierarchy mentioned earlier.

6.3 Software enhancements to Roamnode

The Roamnode (PPPoE over Linux) solution is an independent solution that has been developed at Bristol University. The approach recommended is as follows

1. Document the additional work needed to the software to achieve interoperability, including details of resources and timescales and the information and assistance required from SURFnet (802.12X), SWITCH (VPN) and FUNET (web-based redirection).

2. Work on any architecture and software enhancements and test.

3. Document results and test Roamnode interoperability in the following scenarios
   a. Roamnode user accessing another Roamnode network.
   b. Roamnode user accessing via a VPN network.
   c. Roamnode user accessing via an 802.1X network.
   d. Roamnode user accessing via a web-based redirection network.
   e. A VPN user accessing via a Roamnode network.
   f. An 802.1X user accessing via a Roamnode network.
   g. A web-based redirection user accessing via a Roamnode network.

6.4 Consolidation of findings from test activities

This phase will concentrate on the production of a report based on the results of these trial phases. The report should concentrate on technical aspects of the trial in meeting the original requirements. It should recommend a solution and conduct a risk assessment on the recommendation to identify any new risks and any further development areas.