EduRoam: movilidad por Europa... y España

EduRoam: pan-European Mobility Service

Klaas Wierenga

Resumen

EduRoam es un servicio pan-europeo de acceso invitado a redes de instituciones académicas. En este artículo se pretende dar una vision panorámica del trasfondo técnico y organizativo de este servicio. Asimismo se mostrarán los planes de futuro respecto a la mejora del servicio y a su expansion a otras áreas tales como el acceso a aplicaciones.

Palabras clave: EduRoam, movilidad, redes de instituciones académicas.

Summary

EduRoam is a pan-European service for guest access to networks of educational institutions. This article will give an overview of the technical and organizational backgrounds of this service. Future plans with respect to improving the service as well as expanding towards other areas like access to applications will be presented.

Keywords: EduRoam, mobility, networks of educational institutions.

1.- Background

The amount of mobile devices has increased hugely over the last couple of years. The majority of laptops sold nowadays has wireless LAN capabilities built-in and users expect to be able to get connectivity everywhere, at home, on the road and at the educational institution. At the same time however, a number of exploits (like Kismet[1] and Airsnort[2]) have demonstrated that the classic security of wireless LANs based on Wireless Equivalent Privacy (WEP) is not effective at all.

EduRoam is a pan-European service for guest access to networks of educational institutions

Users are also increasingly mobile beyond their own organizational boundaries. It has become normal that students take classes at another faculty or institution. Stimulated by European initiatives like Erasmus-scholarships this has even expanded across national boundaries. Providing network access for these 'roaming' users involve complex administrative procedures.

These roaming needs of users have led to a number of national and international initiatives to provide network roaming for their constituencies. Within the TERENA taskforce on Mobility (TF-Mobility[3]) the requirements have been formulated as follows:

Enable NREN users to use the Internet (WLAN and wired) everywhere in Europe with:

- Minimal administrative overhead (per roaming user)
- Good usability
- Maintaining required security for all partners
- Scalable

TF-Mobility identified three possible approaches that were in use by the various participants within the taskforce: Web-based authentication[4] (Finland), VPN-based authentication[5] (Germany and Switzerland) and 802.1X-based authentication[6] (The Netherlands).

[1] http://www.kismetwireless.net/
[2] http://airsnort.shmoo.com/
[3] http://www.terena.nl/mobility/
[4] http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delF/DelF-f.pdf
[5] http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delE/DeliEv4.4-np.pdf
[6] http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delD/DelD_v1.2-f.pdf

1.1.- Web-based access

The basic idea is here that a user who tries to get online is automatically provided an IP-address and IP-connectivity. All browser sessions are however intercepted by a so-called captive portal that requires the user to authenticate himself and only then traffic is allowed to pass through. This captive portal verifies the user credentials against an authentication server, possibly a RADIUS-server.

To enable guest use the captive portal needs to be able to verify user credentials for users from abroad. This can be done relatively easy by using a RADIUS-backend. RADIUS is capable of proxying requests that are not destined for itself. This makes the web-based solution one with low administrative overhead, scalable and with good usability (Internet browsers are omnipresent). The difficulty in the web-based solution lies in the requirement to maintain the required security. First, since HTTP is a session-less protocol, after authentication there is no session that binds the computer of the authenticated user. This means that is is relatively easy for another user to hijack an IP-address from an authenticated user. Furthermore, it is important that entering user credentials can be done in a safe way. With a web-based solution this typically means by using an SSL-connection to the authenticating device. When the user is however visiting another institution there is no way for the home-institution of the user to enforce this. Lastly, typically the user credentials of a roaming user travel unencrypted over the Internet to the home-institution of the user.

The VPN-based approach is however hard to make scalable for guest use without much additional administrative overhead

1.2.- VPN-based access

Here the set-up is similar to that of the Web-based solution. Again the user gets automatically IP-connectivity for a network that is separated from the rest of the Internet by a device, in this case a VPN-concentrator. In order to get connectivity with the Internet the user is required to use a VPN-client to connect and authenticate to the VPN-concentrator.

This solution does provide the required security. Also the usability is high once a VPN-client is installed and configured. The VPN-based approach is however hard to make scalable for guest use without much additional administrative overhead. Basically there are only two options for guest usage: allowing VPN-traffic to connect to the home VPN-concentrator of the user or to authenticate the user at the VPN-concentrator of the visited institution. The first approach requires maintaining a long and changing list of ‘allowed IP-addresses’ or to number all VPN-concentrators from a well-known range of addresses that are allowed to pass-through (like the CASG-approach[7] proposed within TF-Mobility). The latter requires all participants to basically use the same type of VPN-solution.

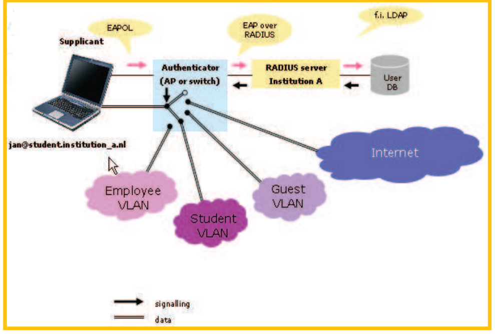
1.3.- 802.1X

The IEEE 802.1X standard for port-based authentication is a layer 2 (Ethernet layer) solution between client and the Access Control Device (either a wireless Access Point or a switch). In the 802.1X framework authentication information is carried over the Extensible Authentication Protocol (EAP) that enables the use of various authentication methods inside. Access control devices communicate with a RADIUS backend that carries the EAP-messages for user verification. After authentication, the communication between client and Wireless Access Point is encrypted using dynamic keys.

Figure 1 shows a typical 802.1X set-up. A student provides his credentials via the 802.1X EAPOL (EAP over LAN) protocol. These credentials are verified by the RADIUS-server against a user database and

[7] http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/delE/DeliEv4.4-np.pdf

FIGURE 1: 802.1X WITH VLAN ASSIGNMENT



upon proper authentication the user gets connected to the student VLAN.

This solution is both secure (when using the proper authentication methods) and scalable (by using the RADIUS-backend). Enabling roaming is very straightforward by proxying requests for unknown realms to another (higher-level) RADIUS-server.

In terms of usability there is however still room for improvement. 802.1X is relatively new, because of that the integration with the various operating systems is still not perfect, although Windows 2000, Windows XP and Mac OS-X support 802.1X natively. For other flavors the use of 3d party software is still needed.

This solution (802.1X) is both secure (when using the proper authentication methods) and scalable (by using the RADIUS-backend)

1.4.- Access method of choice

The characteristics in the previous paragraph, can be summarized as follows:

- Web: Scalable, Unsafe
- VPN: Not Scalable, Safe
- 802.1X: Scalable, Safe.... but new

These characteristics and the fact that upcoming security standards like WPA and 802.11i are all build on 802.1X, TF-Mobility has concluded that 802.1X authentication is the method of choice[8], even though not every institution is able to support it currently because of legacy equipment. The EduRoam service that was created as an 802.1X-based service, supports however also web-based authentication with RADIUS.

2.- EduRoam

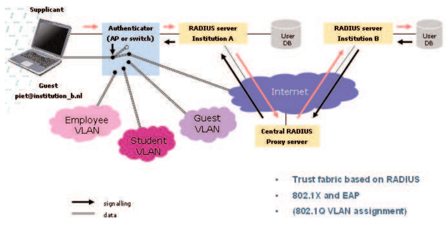
The EduRoam service builds on a hierarchical system of (currently) RADIUS-servers. TERENA deploys a European top level RADIUS-server to which all European NRENs that participate connect with their national RADIUS-server. Every institution that wants to participate in EduRoam connects its institutional RADIUS-server to the national server of their NREN.

FIGURE 2: THE EduRoam LOGO

Figure 3 shows the typical operation for a guest user at an EduRoam participant. The user provides his credentials, the RADIUS-server discovers that it is not responsible for the institution-b.nl realm and proxies it to the national RADIUS-proxy server (that in turn might proxy it to the European server in case the user is coming from another country), this national server forwards the credentials to the home-institution of the user where they are verified. The 'acknowledge' of a successful authentication travels back over the proxy-hierarchy to the visited institution and the user is granter access.

[8] http://www.terena.nl/tech/task-forces/tf-mobility/Deliverables/TF-MobilityfinalReport.pdf

FIGURE 3: EduRoam BASIC SET-UP



2.1.- Tunneled authentication

Because the user credentials travel via a number of intermediate servers, not under control by the home-institution of the user, it is important that the credentials are protected for privacy reasons. This requirement limits the types of authentication methods that can be used. Basically there are two categories of useful authentication methods, those that use credentials in the form of some public key mechanism with certificates (EAP-TLS, EAP-SIM) or those that use so-called tunneled authentication (EAP-TTLS, PEAP).

Authentication using both server and end-user certificates requires the roll-out of a public key infrastructure (PKI) with end-user certificates which has proven difficult in most NRENs

Authentication using both server and end-user certificates requires the roll-out of a public key infrastructure (PKI) with end-user certificates which has proven difficult in most NRENs. Most institutions therefore use a tunneled authentication method that only requires server-certificates.

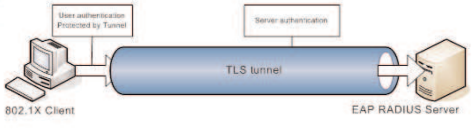
The idea here is that a secure (TLS) tunnel is established between the client and the RADIUS-server of the home-institution on top of RADIUS based on the verification of the server certificate of the home RADIUS-server. This set-up is comparable to that of a web store or an online banking system.

2.2.- Current Situation

At the moment (December 2004) more than 350 institutions in 13 countries participate in EduRoam (See figure 5 in green current participants, in blue countries in the process of joining).

In the United States of America the Internet2 working group SALSA-NetAuth[9] has started an initiative to create a RADIUS-hierarchy for higher education and to become EduRoam participants and also in the Australian-Pacific region an EduRoam initiative[10] has started. Most countries that participate in EduRoam are setting up a web page showing which institutes are participating in EduRoam, like for instance the Netherlands[11].

FIGURE 4: TUNNELED AUTHENTICATION (©ALFA&ARISS)



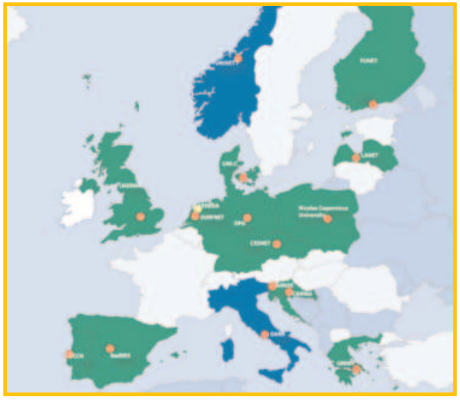
3.- Future of EduRoam

The current set-up of EduRoam works remarkably well, in fact its design based on authentication at the home-institution and authorization at the visited institution has proven to be so powerful that within the Géant2[12] project a full pan-European authentication and authorization infrastructure service will be built upon this architecture. This will take place in Joint Research Activity 5: Roaming and Authorization. The aim is not only to build an infrastructure for network roaming but also for access to applications and to provide single sign-on across applications and networks.

[9] http://security.internet2.edu/netauth/
[10] http://www.eduroam.edu.au/
[11] http://www.eduroam.nl

3.1.- Limitations

FIGURE 5: CURRENT EduRoam PARTICIPANTS



The trust establishment between the RADIUS entities in EduRoam is accomplished using a static shared secret for each peer, where authentication requests are passed on from one entity to the other until the request reaches the authenticating server. This mechanism has a number of disadvantages, namely:

- the traffic generated for authentication must travel through a chain of RADIUS proxies, while the authentication itself is only of interest to the RADIUS entities at the edges of the chain (the one that needs to authenticate a user and the one that checks the user credentials),
- intermediate proxies may inspect the RADIUS payload which places extra requirements on the type of authentication, in practice only EAP-TLS or tunneled EAP types can be used,
- having a fixed chain of proxies is quite error-prone, as failure of one of the servers in the chain can easily result in denial of service to roaming users,
- a shared secret must be agreed upon and exchanged out-of-band for secure communication between RADIUS peers, and
- it is not easy for participating entities in a roaming agreement to obtain an overview of all other partners in the agreement.

The fact that credentials travel through a chain of servers is for network access mainly of concern for performance and reliability reasons because safe authentication methods are used. A solution where the authentication servers (the RADIUS-servers) communicate directly is of particular importance when this infrastructure is used for communication between servers that provide guest access to applications or when more complex interactions between home and visited institution are necessary. These systems typically are not able to use tunneled authentication so protection of credentials and other attributes is of great importance. Setting up a direct secure connection is much easier than setting up a secure connection through a proxy-hierarchy.

Setting up a direct secure connection is much easier than setting up a secure connection through a proxy-hierarchy

In order to overcome these limitations three alternative solutions are investigated in Géant2: PKI, Diameter and DNSsec. The common denominator for all three solutions is that they decouple the (hierarchical) trust establishment with the actual transport of credentials and the fact that they aim at interoperability with the existing EduRoam architecture providing a gradual evolution path.

3.2.- RADIUS/PKI

In this approach the RADIUS-server of the visited institution sets up a direct secure connection with the RADIUS-server of the home institution (see figure 6 where numbers indicate the order in which the steps are carried out). The trust is established through a PKI to which both the home and the visited organization belong. The peers are for instance found through DNS SRV records. The advantage of this solution is that all components are well understood and proven.

The disadvantage of this solution is that it is to a large extent custom made out of the various components. It is also unclear how institutions can participate in more than one hierarchy.

[12] http://www.geant2.net

3.3.- DIAMETER

Diameter[13] is the succesor of RADIUS that has been designed to overcome the shortcomings of the RADIUS-protocol while maintaining backward compatibility (See figure 7 where numbers indicate the order in which the steps are carried out). It operates very similar to RADIUS but a Diameter server can also be set up as a redirector/broker, thus allowing for direct communication between two peers. The advantage of Diameter is that it includes all the necessary components within the protocol. The disadvantage is that, after a number of years since the first IETF-documents where published, there is still a very limited amount of implementations of Diameter and hardly any experience with it.

3.4.- RADIUS-DNSsec

A last possible approach is to use the new DNS-secure (DNSsec[14]) protocol (See figure 8 where numbers indicate the order in which the steps are carried out). This approach is in some respects similar to the PKI-approach, but the trust is established through a secure DNS-zone. Peers are discovered by resolving a DNS entry for the domain of the user. Authenticity and integrity is provided through using DNSsec.

The advantage of Diameter is that it includes all the necessary components within the protocol

Advantage of this solution is that an organization can participate in more than one hierarchy and that a DNS-approach is very versatile and scalable. Disadvantage is that DNSsec is relatively new and that there are not many implementations or experience yet.

FIGURE 6: RADIUS WITH PKI

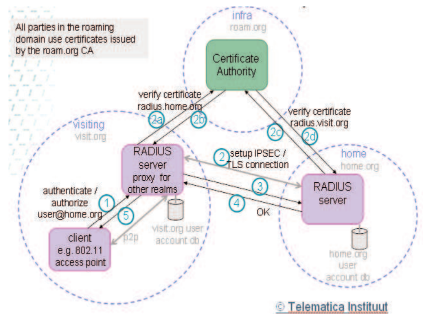
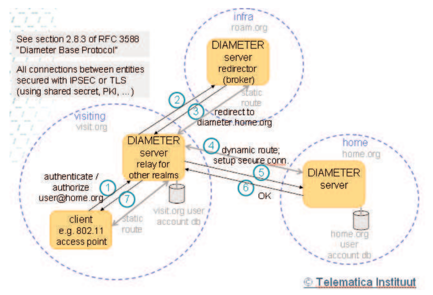

All parties in the roaming domain use certificates issued by the roam.org CA
infra
roam.org
Certificate Authority
verify certificate radius.home.org
2a
2b
verify certificate radius.visit.org
2c
2d
visiting
visit.org
RADIUS server proxy for other realms
2
setup IPSEC / TLS connection
home
home.org
RADIUS server
3
4
OK
authenticate / authorize user@home.org
1
5
p2p
client e.g. 802.11 access point
visit.org user account db
home.org user account db
© Telematica Instituut

FIGURE 7: DIAMETER


See section 2.8.3 of RFC 3588 "Diameter Base Protocol"
All connections between entities secured with IPSEC or TLS (using shared secret, PKI, ...)
infra
roam.org
DIAMETER server redirector (broker)
2
3
static route
redirect to diameter.home.org
visiting
visit.org
DIAMETER server relay for other realms
4
dynamic route; setup secure conn.
home
home.org
DIAMETER server
5
6
OK
authenticate / authorize user@home.org
1
7
static route
client e.g. 802.11 access point
visit.org user account db
home.org user account db
© Telematica Instituut

4.- Conclusion

EduRoam has proven itself as a scalable, secure and successful service. This is proven by the fact that more and more countries and institutions participate, also beyond Europe, thus making it more and more beneficial for the participants.

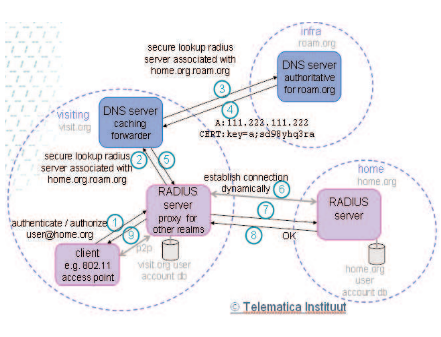
[13] http://www.ietf.org/rfc/rfc3588.txt

[14] http://www.ietf.org/internet-drafts/draft-ietf-dnsext-dnssec-intro-13.txt (work in progress)

Within Géant2 JRA5 the aim is to expand the existing service into a pan-European service for Roaming and Authentication/Authorization. This will result in a service that is more robust and suitable for new categories of use, in particular federated access to applications.

Foreseen improvements of the infrastructure concentrate on the 'backplane' of the service, while keeping intact the institutional set-up. This, and the fact that new security standards like WPA and 802.11i are build upon the 802.1X framework ensure that an investment in EduRoam participation is a well spent one.

FIGURE 8: RADIUS AND DNSsec


infra
roam.org
secure lookup radius server associated with home.org.roam.org
3
DNS server authoritative for roam.org
4
A:111.222.111.222
CERT:key=a;sd98yhq3ra
visiting
visit.org
DNS server caching forwarder
secure lookup radius server associated with home.org.roam.org
2
5
establish connection dynamically
6
home
home.org
RADIUS server proxy for other realms
7
RADIUS server
authenticate / authorize user@home.org
1
9
8
OK
client e.g. 802.11 access point
p2p
visit.org user account db
home.org user account db
© Telematica Instituut

More information

- http://www.eduroam.org/
- http://www.eduroam.nl/
- http://www.terena.nl/mobility/

Within Géant2 JRA5 the aim is to expand the existing service into a pan-European service for Roaming and Authentication/ Authorization

Klaas Wierenga
(Klaas.Wierenga@surfnet.nl)
SURFnet bv,
The Netherlands