High-quality Internet for higher education and research

Klaas Wierenga
SURFnet
klaas.wierenga@surfnet.nl

Stefan Winter
RESTENA
stefan.winter@restena.lu

Nicosia, Jan 15, 2007
Contents

• From 802.1X to eduroam
• Policy
• Status of eduroam
• Joining eduroam
From 802.1X to eduroam
Wireless LANs are unsafe

root@ibook:~# tcpdump -n -i eth1
19:52:08.995104 10.0.1.2 > 10.0.1.1: icmp: echo request
19:52:08.996412 10.0.1.1 > 10.0.1.2: icmp: echo reply
19:52:08.997961 10.0.1.2 > 10.0.1.1: icmp: echo request
19:52:08.999220 10.0.1.1 > 10.0.1.2: icmp: echo reply
19:52:08.999220 10.0.1.2 > 10.0.1.1: icmp: echo request
19:52:08.999220 10.0.1.1 > 10.0.1.2: icmp: echo reply ^C
Users are mobile

Internet backbone

University A
WLAN

University B
WLAN

Student Dormitory Access

Access Provider ADSL

Access Provider WLAN

Access Provider GPRS/UMTS

International connectivity

High-quality Internet for higher education and research
Requirements

• Identify users uniquely at the edge of the network
  – No session hijacking

• Enable guest usage

• Scalable
  – Local user administration and authentication

• Easy to install and use
  – At the most one-time installation by the user

• Open
eduroam architecture

- Security based on 802.1X
  - Protection of credentials
  - Provides basis for new wireless security standards WPA and 802.11i
  - Different authentication mechanisms possible by using EAP (Extensible Authentication protocol)
    - Username/password
    - X.509 certificates
    - SIM-cards
  - Integration with VLAN assignment

- Roaming based on RADIUS proxying
  - Remote Authentication Dial In User Service
  - Transport-protocol for authentication information

- Trust fabric based on:
  - Technical: RADIUS hierarchy
  - Policy: Documents/contracts that define the responsibilities of user, institution, NREN and the eduroam federation
Secure access to the network with 802.1X

Supplicant

Jan@student.university_a.nl

Authenticator (AP or switch)

RADIUS server
University A

User DB

Internet

- Employee VLAN
- Commercial VLAN
- Student VLAN

802.1X

(VLAN assignment)

High-quality Internet for higher education and research
High-quality Internet for higher education and research

Supplicant

Guest
piet@university_b.nl

Authenticator
(AP or switch)

RADIUS server
uni.lu

RADIUS server
university_b.nl

Internet

RADIUS proxy hierarchy

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

signalling
data
The RADIUS proxy hierarchy
The eduroam policy
The European eduroam policy

- Mutual access
- Home institutions are/remain responsible for their users abroad
- Members are NRENs
- Members guarantee required security levels by their participants
- Members promote eduroam in their countries
- European eduroam may peer with other regions
National policy

- Mutual access
- Members are connected institutions
- Home institution is/remains responsible for its users behaviour.
- Home institution is responsible for proper user management
- Home and visited institution must keep sufficient logdata
- Appropriate security levels
The status of eduroam
Status of eduroam

New members:
- Lithuania
- Romania
- Hungary
- China
- Hong Kong

Over 500 institutions in Europe, Australia and Taiwan

USA, Japan, Korea will follow shortly
eduroam

• Provides global network roaming

• Strong technical foundation:
  – RADIUS
  – 802.1X
  – Lingua Franca: EAP

• Needs ubiquity
Joining eduroam

High-quality Internet for higher education and research
Joining eduroam for an NREN

- Set up a server that proxies that:
  - Accept requests for *.cc-tld and forward to the right institution
  - Accept requests for non *.cc-tld and forward it to the European servers

- Send an (encrypted) e-mail to join@eduroam.org with:
  - FQDN of toplevel RADIUS-server(s)
  - IP-addresses of toplevel RADIUS-servers
  - Shared secret to use between European servers and national server(s).
  - URL of national eduroam website
  - Information about test-account
  - Contact details admin

- Sign the policy agreement
Joining eduroam for an institution

• Set-up your local 802.1X infrastructure
  – Accept requests for your-domain.cc-tld and process them
  – Proxy requests for non-local users to the national server

• Send an (encrypted) e-mail to your NREN with:
  – FQDN of toplevel RADIUS-server(s)
  – IP-addresses of toplevel RADIUS-servers
  – Shared secret to use between your and their server(s).
  – URL of your eduroam website
  – Information about test-account
  – Contact details admin

• Sign the policy document
Conclusions
Conclusions

- 802.1X provides secure, scalable access to the campus network
- Enabling eduroam is easy once 802.1X is in place
- Many have already joined, so
High-quality Internet for higher education and research
More information

- eduroam in SURFnet
  - [http://www.eduroam.nl](http://www.eduroam.nl)

- eduroam in Europe
  - [http://www.eduroam.org](http://www.eduroam.org)

- TERENA TF-Mobility
  - [http://www.terena.nl/mobility](http://www.terena.nl/mobility)

- The unofficial IEEE802.11 security page