

Eduroam in a box (take 3)

Rok Papež,
ARNES,
Barcelona, 06.09.2005

ARNES EduRoam 1/2

- WPA/WPA2 Wireless network
 - WPA Enterprise (+ WPA2 where available)
 - Dynamic VLANs
 - Support for legacy networks (multiple SSID)
- RADIUS tree hierarchy
 - Non-automatic auth (forced EAP-TTLS + PAP)
 - Send real user-name with Access-Accept
 - Monitor users (full log + IP, close stale connections)
 - FreeRADIUS problems (threads, libs, Alan DeKok)

ARNES EduRoam 2/2

- OpenLDAP
 - Very unintuitive software
 - Reliability vs. Performance (bdb/hdb vs. Lmdb)
 - Phpldapadmin = administrator tool
 - siEduPerson schema
 - Bad documentation about schemas
- Specification updates
- L2 security is complex (Catalyst 3750, L2/L3 fw)

EduRoam administrators

- 50% use trial and error learning
 - Low understanding of Wireless security
 - Low understanding of Ethernet security
 - Radius servers are misconfigured
 - Extensive, manual one-time network inspections
 - Why use LDAP and not MySQL/text files ?
- Time consuming EduRoam deployment
- With time - small AAI misconfigurations

EduRoam in a box – why ?

- Speed up deployment
- For less technically experienced
- Deployment of a proven solution
- Less errors
- Automated configuration with easier deployment
- Easier reporting of data
 - Statistics
 - AP database

ARNES Eduroams

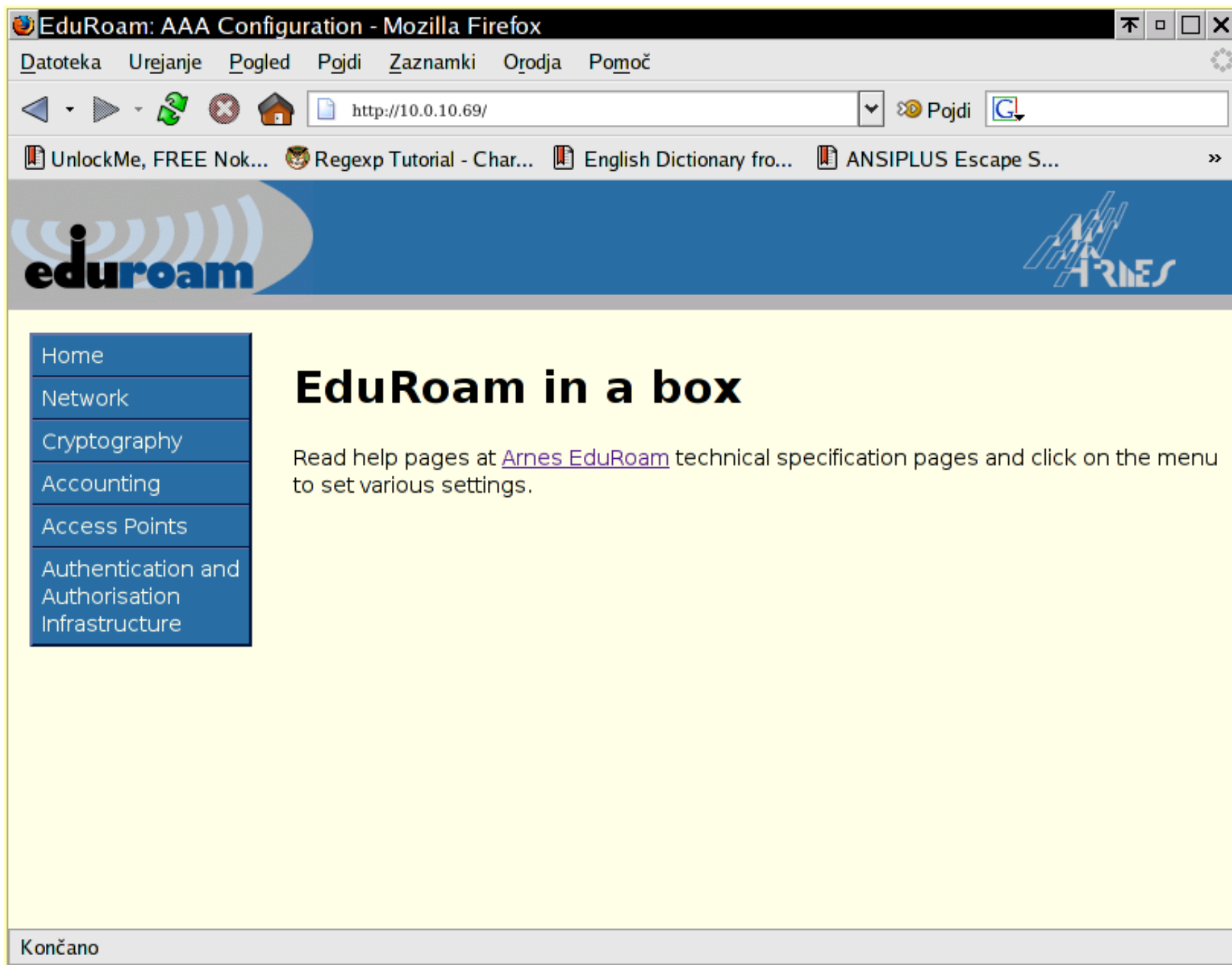
- Big EduRoam

- WPA(2) Enterprise
- FreeRADIUS
- OpenLDAP
- ISC DHCPd
- MySQL (accounting)
- EduRoam monitor
- L2/L3 security via switch

- Small EduRoam

- WPA(2) Enterprise
- FreeRADIUS
- OpenLDAP
- ISC DHCPd
- MySQL (accounting)
- EduRoam monitor
- L2/L3 security via Linux firewall

EduRoam in a box „Home“



The screenshot shows a Mozilla Firefox browser window titled "EduRoam: AAA Configuration - Mozilla Firefox". The address bar contains "http://10.0.10.69/". The browser interface is in Slovenian, with menu items like "Datoteka", "Urejanje", "Pogled", "Pojdi", "Zaznamki", "Orodja", and "Pomoč". The page content features a blue header with the "eduroam" logo and the "ARNES" logo. A navigation menu on the left lists: Home, Network, Cryptography, Accounting, Access Points, and Authentication and Authorisation Infrastructure. The main content area has the heading "EduRoam in a box" and a paragraph: "Read help pages at [Arnes EduRoam](#) technical specification pages and click on the menu to set various settings." The footer of the browser window displays "Končano".

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/ Pojdi

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

eduroam ARNES

Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure

EduRoam in a box

Read help pages at [Arnes EduRoam](#) technical specification pages and click on the menu to set various settings.

Končano

Eduroam in a box „Network“ 1/2

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/net

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

eduroam ARNES

Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure

Network configuration

Please select your WAN (uplink) interface:

- eth0
- eth1
- eth2

WAN address in IP/CIDR format:

Default gateway address:

Addresses of DNS servers (enter one per line):

Hostname (optional):

Domain name (optional):

http://10.0.10.69/cgi-bin/net

Eduroam in a box „Network“ 2/2

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/net

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

Hostname (optional):

Domain name (optional):

Select the type of WAN connection:

Bridge
 NAT

Management LAN interface address in IP/CIDR format
(specify when using NAT type of connection):

User VLAN number:

User VLAN interface address in IP/CIDR format:

Networks and hosts in CIDR format with management access to the server
(enter one per line, examples: 192.168.1.34, 10.0.133.0/24):

Končano

Eduroam in a box „Crypto“ 1/2

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/crypto

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure

SSL tool

Certificate Authority certificate information:

- Issuer: C=SI, ST=Slovenia, L=Ljubljana, O=ARNES/emailAddress=rok.papez@arnes.si, CN=ARNES EduRoam CA
- Valid From: Aug 26 13:57:32 2005 GMT
- Valid To: Aug 17 13:57:32 2006 GMT
- Fingerprint: BA:AE:42:45:09:A2:01:2E:45:05:6C:17:E9:AB:DD:EA:68:D9:1B:06

[Download CA Cert](#)

Current server certificates:

```
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=Eduroam server 1/emailAddress=rok.papez@arnes.si
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=pingo/emailAddress=rok.papez@arnes.si
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=*.pingo.org/emailAddress=rok.papez@arnes.si
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=xx/emailAddress=rok.papez@arnes.si
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=rrr/emailAddress=rok.papez@arnes.si
C=SI, ST=Slovenia, L=Ljubljana, O=ARNES, CN=rrx/emailAddress=rok.papez@arnes.si
C=SI, ST=RR, L=RR, O=ARNES, CN=rrxy/emailAddress=rok.papez@arnes.si
C=SI, ST=a, L=a, O=a, CN=sfd/emailAddress=a
C=aa, ST=aa, L=aa, O=aa, CN=aa/emailAddress=aa
C=SI, ST=Slovenia, L=lajbah, O=ARNES, CN=dd/emailAddress=dd
```

- Issuer: /C=SI/ST=Slovenia/L=Ljubljana/O=ARNES/CN=Eduroam server 1/emailAddress=rok.papez@arnes.si
- Valid From: Aug 26 13:58:21 2005 GMT
- Valid To: Aug 26 13:58:21 2009 GMT
- Fingerprint: 05:3D:A3:EB:EB:EB:5A:21:59:8D:B2:2D:81:6D:E4:F1

http://10.0.10.69/cgi-bin/crypto

EduRoam in a box „Crypto“ 2/2

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/crypto

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

- Valid To: Aug 26 13:58:21 2009 GMT
- Fingerprint: 05:3D:A3:EB:EB:EB:5A:21:59:8D:B2:2D:81:6D:E4:F1

Use Certificate for EduRoam

Download Certificate

Download Private Key

Create new certificate:
Common name (for server certificate usually a hostname):

Email address:

Days to be valid:

Organisation:

Locality (city):

State:

Country (2 letter country code):

Certificate type:
 Server
 Certificate Authority (*)

* **Warning!** If you regenerate CA certificate,
all the existing certificates will be rendered unusable!

Generate Certificate

Končano

Eduroam in a box „Accounting“

EduRoam Accounting system

Database is **online**

Create DB

Delete DB

Last connections:

User-Name	Calling-Station-Id	Client-IP-Address	Called-Station-Id	NAS-Port	Timestamp Start	Timestamp Dhcp
rok@domainX.tld	000c.f138.a2ba	10.0.12.109	000f.248a.95d1	259	2005-08-31 15:44:33	2005-08-31 15:57:09
rok@domainX.tld	000c.f138.a2ba	10.0.12.109	000f.248a.95d1	258	2005-08-31 12:14:56	2005-08-31 15:43:08
rok@domainX.tld	000c.f138.a2ba	10.0.12.109	000f.248a.95d1	257	2005-08-31 10:01:24	2005-08-31 10:46:01
rok@domainX.tld	000c.f138.a2ba		000f.248a.95d1	267	2005-08-29 16:04:42	1970-01-01 01:00:00
ksenija@domain.tld	0004.236e.8d12	10.0.12.74	000f.248a.95d1	257	2005-07-26 12:56:08	2005-07-26 14:36:34
ksenija@domain.tld	0004.236e.8d12	10.0.12.108	000f.248a.95d1	281	2005-07-25 12:36:41	2005-07-25 12:41:44
arnes_test@domain.tld	000c.f138.a2ba		000f.248a.95d1	272	2005-07-22 12:55:19	2005-07-22 15:25:24
burek_test@domain.tld	000e.35a2.7839		000f.248a.95d0	268	2005-07-22 11:18:12	1970-01-01 01:00:00
burek_test@domain.tld	000e.35a2.7839		000f.248a.95d0	265	2005-07-22	1970-01-01

Eduroam in a box „Access Points“

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/ap

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure

Configuration of Access Points

Access Point List:

10.0.1.66 (pass: heslo, snmp:snmp123snmp321, rad_sec:skritogeslo)

Delete AP Show MACs

Create or Modify Access Point:
Note: Before adding the Access Point make sure:

- AP has a valid IP address from the WLAN management subnet
- There is admin SSH access with a username 'root' from this server
- Read only SNMP access from this server is enabled
- That the Access Point is **powered on and reachable**

Access Point IP address:

Password for user 'root':

SNMP RO Community string:

Radius shared secret:

Add or Modify AP

http://10.0.10.69/cgi-bin/ap

Eduroam in a box „AAI“ 1/3

The screenshot shows a web browser window titled "EduRoam: AAA Configuration - Mozilla Firefox". The address bar shows the URL "http://10.0.10.69/cgi-bin/aaai". The browser's menu bar includes "Datoteka", "Urejanje", "Pogled", "Pojudi", "Zaznamki", "Orodja", and "Pomoč". The browser's toolbar shows navigation buttons and a search icon. The browser's tab bar shows several tabs, including "UnlockMe, FREE Nok...", "Regex Tutorial - Char...", "English Dictionary fro...", and "ANSIPLUS Escape S...".

The main content area of the browser displays the "Configuration of EduRoam Authentication and Authorisation Infrastructure" page. The page has a left-hand navigation menu with the following items: "Home", "Network", "Cryptography", "Accounting", "Access Points", and "Authentication and Authorisation Infrastructure" (which is highlighted in yellow). The main content area is titled "Configuration of EduRoam Authentication and Authorisation Infrastructure" and contains the following sections:

- Realm name** (example: domain.tld):
domainX.tld
- LDAP Root DN password:**
hesbzaroot
- Primary upstream RADIUS server:**
IP Address: 10.0.10.71
Shared secret: sharedsecret1
- Secondary upstream RADIUS server:**
IP Address: 10.0.11.66
Shared secret: sharedsekret23

Below these sections is an "Apply" button. The next section is "Access Control List (ACL) for access to LDAP:", which contains a list of IP addresses and subnets: 10.0.13.232, 10.0.13.64/28, and 10.0.14.223. Below this list is a "Delete ACL" button. The final section is "New ACL for access to LDAP:", which includes a note: "Note: Specify network in CIDR format (10.0.0.1/24)". Below this note is an input field and an "Add ACL" button. At the bottom of the page, there is a section titled "Statically configured users in LDAP directory:" with an input field below it.

The browser's status bar at the bottom shows the URL "http://10.0.10.69/cgi-bin/aaai".

Eduroam in a box „AAI“ 2/3

The screenshot shows a web browser window titled "EduRoam: AAA Configuration - Mozilla Firefox". The address bar contains the URL "http://10.0.10.69/cgi-bin/aai". The browser's menu bar includes "Datoteka", "Urejanje", "Pogled", "Pojudi", "Zaznamki", "Orodja", and "Pomoč". The browser's tab bar shows several open tabs, including "UnlockMe, FREE Nok...", "Regex Tutorial - Char...", "English Dictionary fro...", and "ANSIPLUS Escape S...".

The main content area of the browser displays the "Access Control List (ACL) for access to LDAP:" section. It features a list box containing the following IP addresses and ranges:

- 10.0.13.232
- 10.0.13.64/28
- 10.0.14.223

Below the list box is a "Delete ACL" button. Underneath is the "New ACL for access to LDAP:" section, which includes a note: "Note: Specify network in CIDR format (10.0.0.1/24)". There is an empty text input field and an "Add ACL" button below it.

The next section is "Statically configured users in LDAP directory:", which contains a list box with the following entries:

- usernameX (pass:passwordX)
- ksenija (pass:gesbXXX)
- rok (pass:rokhesb)

Below the list box is a "Delete LDAP User" button. The final section is "User to insert into LDAP directory:", which includes a note: "Note: Insert only test usernames, real users should be inserted using a script or other LDAP user management tools. Specify only the username, not the network user ID." Below the note are two text input fields labeled "Username:" and "Password:", followed by an "Add or Change LDAP User" button.

At the bottom of the browser window, the status bar displays the text "Končano".

Eduroam in a box „AAI“ 3/3

EduRoam: AAA Configuration - Mozilla Firefox

Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč

http://10.0.10.69/cgi-bin/aai

UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...

Delete LDAP User

User to insert into LDAP directory:
Note: Insert only test usernames, real users should be inserted using a script or other LDAP user management tools. Specify only the username, not the network user ID.

Username:

Password:

Add or Change LDAP User

Statically configured users in RADIUS server:

rok (pass:123geslosezgubi) ▲

userX (pass:passX)

Delete Radius User

User to insert into LDAP directory:
Note: Insert only test usernames, real users should be inserted using a script or other LDAP user management tools. Specify only the username, not the network user ID.

Username:

Password:

Add or Change Radius User

Implement changed parameters:

Warning! This will reload the iptables and restart the LDAP and RADIUS servers.

Končano

Eduroam in a box - Summary

- Skeleton/base is done
- Rough around the edges
- Still work to do
- Field deployments
- Support for other equipment
 - „Big EduRoam“ - Catalyst 3750
 - Other Access Points