EduRoam in a box

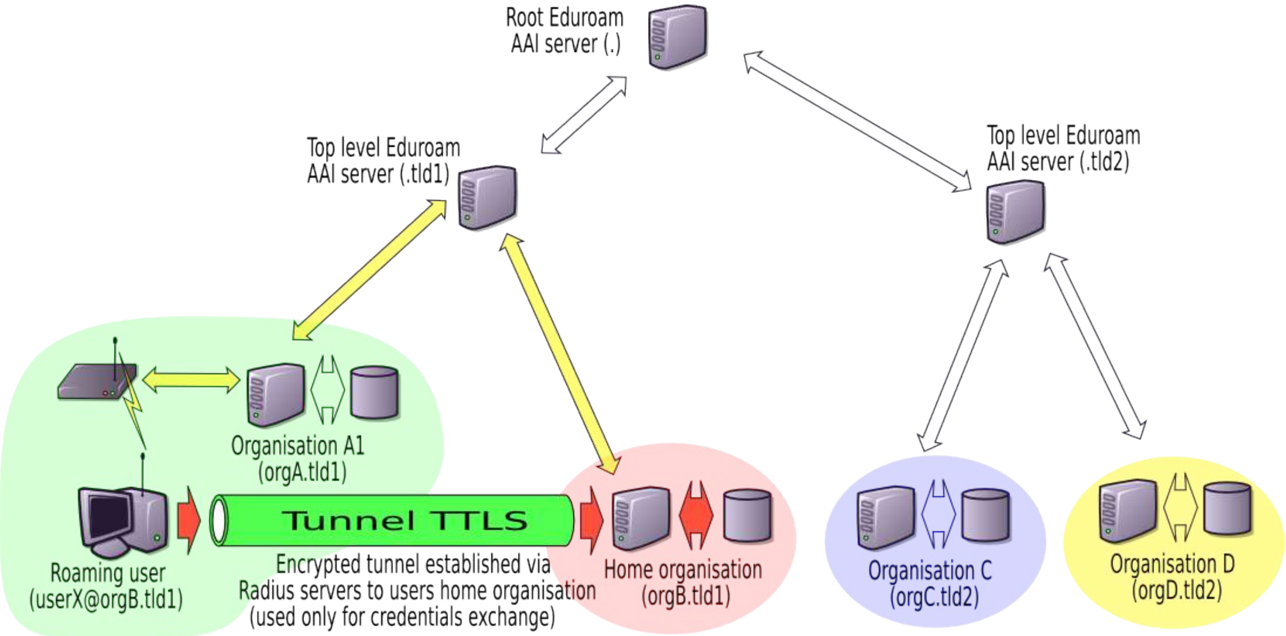
User Guide
(version: 20051117 - prerelease)

Author: Rok Papež (rok.papez@arnes.si)
NREN: Arnes
Date: 17.11.2005

1. About EduRoam in a box

1.1. Introduction to the EduRoam AAI system

EduRoam is an Authentication and Authorization Infrastructure system for seamless user roaming in computer networks for research and education community. The system is composed of the tree-like hierarchy of Radius servers who use statically configured routing to redirect access requests from the roaming users to their home institution server.



Picture 1: *Diagram of remote authentication: hierarhy of Radius servers is used for secure transport of credentials between roaming user and his home organisation. Authorisation is performed by the server in visited organisation.*

Usually for each country there is an NREN (or NREN like organization) that operates the top level national radius server and describes what the requirements of the end participating organizations in his "domain" are. For example in Slovenia organizations are among other things required to:

- Broadcast SSID "EduRoam"
- Use WPA/WPA2 wireless encryption
- User anonymous@orgX.si for outer username (the one outside the TTLS Tunnel)
- Send the real User-Name after successful authentication (so the accounting information can be linked to a correct username).
- All users must be in LDAP directory

On the other hand in Netherlands they:

- Use Dynamic-WEP (802.1x authentication)
- Used whichever SSID they liked

There are some standardized settings common to all the EduRoam members but mostly the NRENs have enforced their own view of the EduRoam in their respecitve country.

1.2. EduRoam deployment issues

Unfortunately setting up EduRoam servers isn't as trivial as it could be. Network administrators who might have been using to manage only simple non-configuring switches need to:

- Use 802.1q VLANs (for security separation of guest and more sensitive network)
- Deploy certain ethernet hardening technologies, example:
  - dhcp snooping
  - dynamic arp inspection
  - ...
  - Linux L2/L3 firewall (ebtables, arptables, iptables)
- Correctly secure and deploy the 802.11a/b/g (Wi-Fi) network
- Activate 802.1x authentication on wired and wireless network access points
- Configure the network access eqipment to use Radius authentication
- Set-up usualy a UNIX server to run essential servers:
  - dhcp
  - MySQL
  - LDAP directory
  - freeradius
  - monitoring / account merging custom server (EduRoam monitor)
  - postfix SMTP mail server
  - script for automated reporting of statistics to the NREN
- Usually for easier management the following tools are also installed:
  - Web LDAP management http://phpldapadmin.sourceforge.net/
  - Web MySQL management http://www.phpmyadmin.net/

Obviously this might be a big step-up for a network engineer if he needs to run all these “new” technologies. In practice ~50% of deployments were done in a “trial and error” way and this way quite some glitches were introduced into the system.

1.3. What “EduRoam in a box” is...

We wanted to:

- shorten the time required for deployment of EduRoam AAI servers
- reduce the number of errors
- make EduRoam more attractive to smaller organizations with less technical staff
- automate deployment of EduRoam “technical specification updates”
- introduce mechanism for easier reporting of statistics and Access Points database

“Eduroam in a box” is a web interface to a configuration wizard and a management web interface for the EduRoam system. It is a tool for network administrators to speed up deployment.

1.4. ... and what it's not.

“EduRoam in a box” isn't a magical wand for a 5-minute EduRoam set-up. It probably never will be because of the rather complex nature of operating the network with all these different technologies.

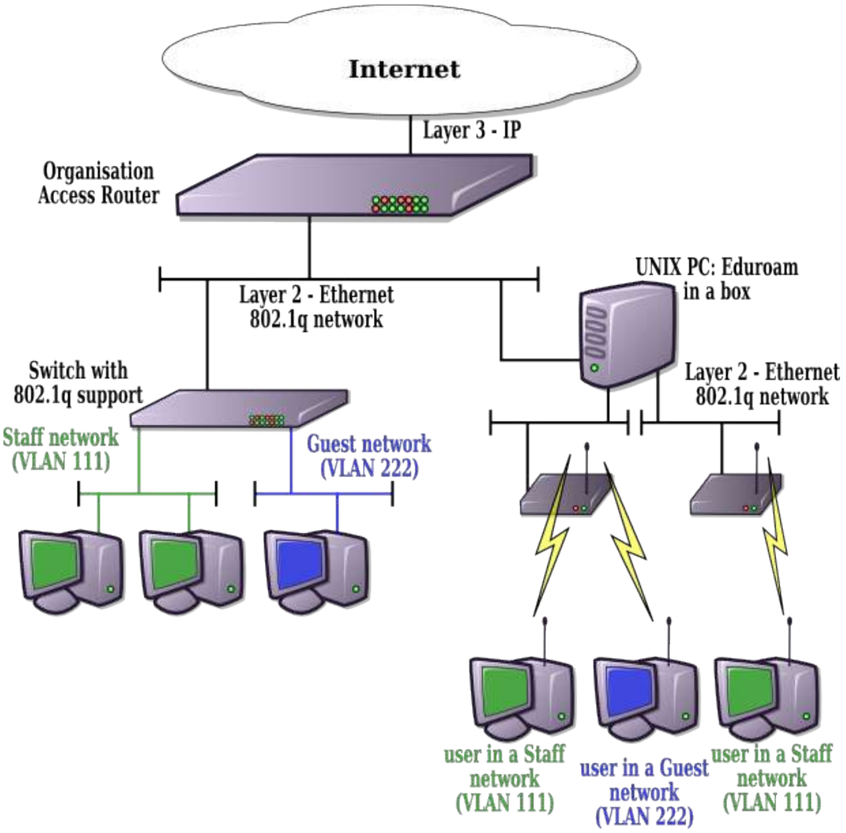
The person setting up the system still needs to be a network engineer, knowing how to configure the network equipment (access points, switches, dial-in servers, ...).

2. Requirements:

The following is required:

- Already established network
- A PC Computer with
  - at least 2 network interface cards
  - already installed and updated Fedora Core 4 Linux distribution
- Powered on and configured Access Points

2.1. EduRoam topology


Internet
Layer 3 - IP
Organisation Access Router
Layer 2 - Ethernet 802.1q network
UNIX PC: Eduroam in a box
Switch with 802.1q support
Layer 2 - Ethernet 802.1q network
Staff network (VLAN 111)
Guest network (VLAN 222)
user in a Staff network (VLAN 111)
user in a Guest network (VLAN 222)
user in a Staff network (VLAN 111)

Picture 2: "Eduroam in a box" network topology diagram

The system will bridge the 802.1q VLANs with full L2/L3 firewall so you can actually (this is by design) add the wireless network into an existing networks. Current design is only for two VLANs in mind. One is native/management and the other is user/wlan/.1q tagged. The Access Points should be configured as described in the section 2.2.

(**Note:** The use of native VLAN will be obsoleted. The plan is to have management VLAN 802.1q tagged and support for multiple user VLANs.)

2.2. Access Point configuration

(**Note:** This config is for WPA, IOS 12.2 and management interface on native VLAN; this will be obsoleted and we'll add support for WPA/WPA2 mixed wireless, IOS 12.3 and 802.1q tagged management VLAN)

```
version 12.2
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname ap<location>
!
enable secret <password>
!
username root secret <root password>
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
ip subnet-zero
ip domain name <domain name, ex: orgA.tld1>
ip name-server <dns1>
ip name-server <dns2>
ip name-server <dns3>
!
aaa new-model
!
!
aaa group server radius radius_grp
server <radius server 1> auth-port 1812 acct-port 1813
!
aaa authentication login default local
aaa authentication login radius_auth group radius_grp
aaa accounting update periodic 5
aaa accounting network default start-stop group radius_grp
aaa accounting connection default start-stop group radius_grp
aaa session-id common
!
bridge irb
!
!
interface Dot11Radio0
    no ip address
    no ip route-cache
    !
    # Which and How many VLANs depends on the network
    #encryption vlan <staff vlan> mode ciphers tkip
    encryption vlan <guest vlan> mode ciphers tkip
    [...]
    !
    ssid eduroam
        vlan <guest vlan>
        authentication open eap radius_auth
        authentication key-management wpa
        accounting default
        guest-mode
    !
    world-mode
    speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
    rts threshold 2312
    no preamble-short
    # Channel number should be provided by a site survey. Don't do automatic.
    channel 2472
    station-role root
    no cdp enable
    dot1x reauth-period server
    bridge-group 1
    bridge-group 1 subscriber-loop-control
    bridge-group 1 block-unknown-source
    no bridge-group 1 source-learning
    no bridge-group 1 unicast-flooding
!
interface Dot11Radio0.<guest vlan>
    encapsulation dot1Q <guest vlan>
    ip access-group block_client_tx in
    ip access-group block_client_rx out
    no ip route-cache
    bridge-group 100
    bridge-group 100 subscriber-loop-control
    bridge-group 100 block-unknown-source
    no bridge-group 100 source-learning
    no bridge-group 100 unicast-flooding
    bridge-group 100 spanning-disabled
!
interface FastEthernet0
    no ip address
    no ip route-cache
    duplex auto
    speed auto
!
interface FastEthernet0.<net management vlan>
    encapsulation dot1Q <net management vlan> native
    no ip route-cache
    bridge-group 1
    no bridge-group 1 source-learning
    bridge-group 1 spanning-disabled
!
interface FastEthernet0.<guest vlan>
    encapsulation dot1Q <guest vlan>
    no ip route-cache
    bridge-group 100
    no bridge-group 100 source-learning
    bridge-group 100 spanning-disabled
!
interface BVI1
    ip address <IP address> <network mask>
    no ip route-cache
!
ip default-gateway <default gateway for net management vlan>
no ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
!
# Every organisation should make her own filters. These are just the essential ones.
# We want to limit what clients can send to each other. No DHCP server spoofing!
ip access-list extended block_client_rx
    remark === block packets clients can receive ===
    deny udp any eq bootpc any eq bootps
    permit ip any any
# - disabled sending of DHCP replies (that's servers job!)
ip access-list extended block_client_tx
    remark === block packets clients transmit ===
    deny udp any eq bootps any
    permit ip any any
# - allow SSH access only from management workstations/network
ip access-list extended block_managment_access
    remark === limit access to AP login ===
    permit tcp <managment workstations network> <netmask> any eq 22
access-list <1-99> remark === limit access to SNMP ===
access-list <1-99> permit <eduroam server IP>
access-list <1-99> permit <managment workstation>
snmp-server community <snmp community> RO <1-99>
radius-server host <eduroam server IP> auth-port 1812 acct-port 1813 key <radius secret>
radius-server attribute 32 include-in-access-req format %i
radius-server authorization permit missing Service-Type
bridge 1 route ip
!
!
line con 0
line vty 0 4
    access-class block_managment_access in
line vty 5 15
    access-class block_managment_access in
!
ntp server <NTP1>
ntp server <NTP2>
end
```

(**Note:** It would be nice to add support for Access Point configuration deployment and automatic firmware updating. But currently this isn't planned for the release version.)

3. Installation:

First make sure system is updated by connecting it to the secure network with internet access and running:

```
yum -y update
```

Download the packages from http://www.pingo.org/eduroam/rpms/.
(**Note:** This URL is temporary and will change)

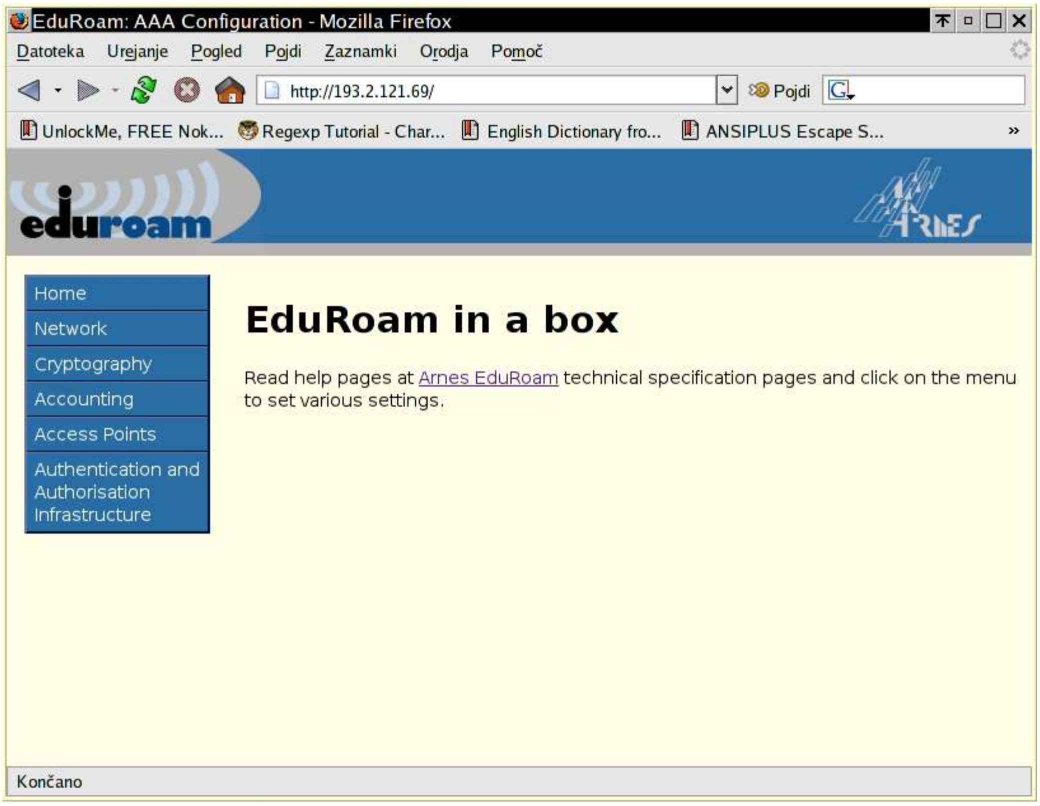
Make sure you reboot into the updated kernel and install the provided packages. The packages are inter-dependant and must be installed in correct order. You can of course just run:

```
rpm -i *.i386.rpm
```

If (when) rpm complains about the missing packages, they can be installed from online Fedora repository via yum:

```
yum -y install <package name>
```

After installing the package make sure apache is started, run a web browser from the installed PC and open the address http://127.0.0.1/eduroam. You will notice the web forms/pages that you insert data in one-by-one and confirm the entered data.



EduRoam in a box

Read help pages at Arnes EduRoam technical specification pages and click on the menu to set various settings.

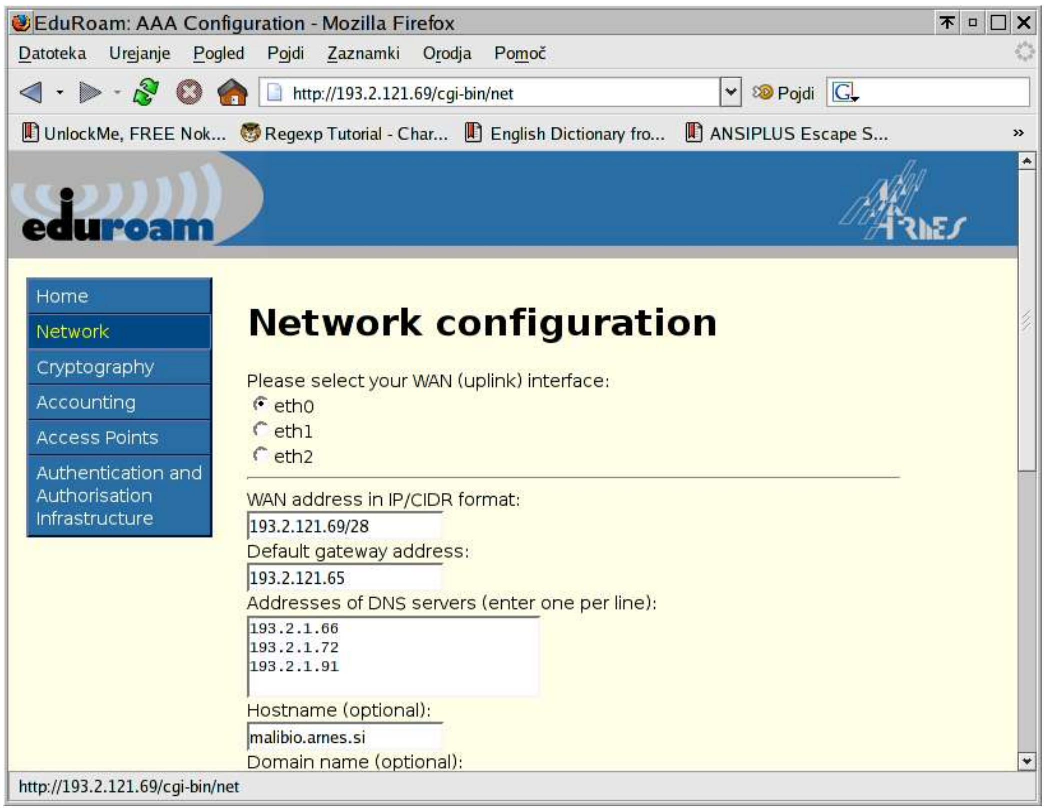
Picture 3: Eduroam in a box welcome screen

Every submitted web form configures some of the services, network interfaces, servers, inputs the data into the eduroam config settings, … .

3.1. Network configuration:

In the network configuration screen you set-up the server connectivity parameters. It will (re)configure the network interfaces of the server and the whole network subsystem (interfaces, VLANs, bridging, part of the firewall, resolver, ...).

The WAN (uplink) interface is the 802.1q tagged interface to the switch. Network management VLAN is untagged while the other (user traffic) VLANs are 802.1q tagged (currently only one user VLAN is supported by the server).


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka
Urejanje
Pogled
Pojdi
Zaznamki
Orodja
Pomoč
http://193.2.121.69/cgi-bin/net
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
http://193.2.121.69/cgi-bin/net

Network configuration

Please select your WAN (uplink) interface:
● eth0
○ eth1
○ eth2

WAN address in IP/CIDR format:
193.2.121.69/28

Default gateway address:
193.2.121.65

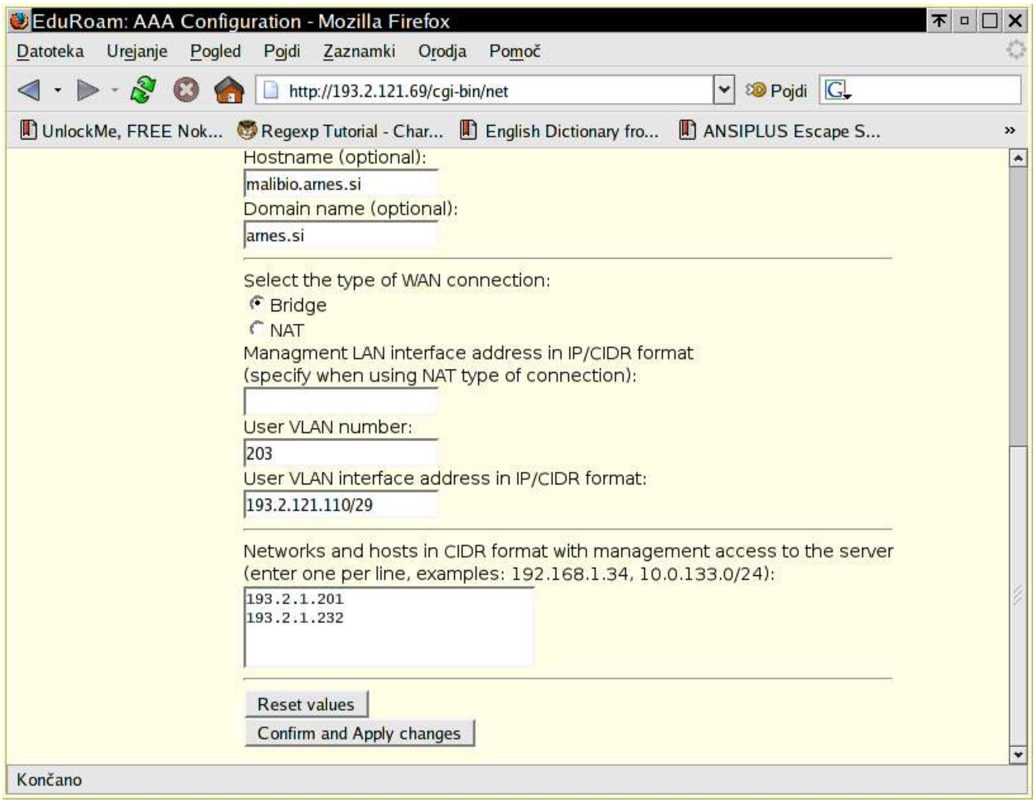
Addresses of DNS servers (enter one per line):
193.2.1.66
193.2.1.72
193.2.1.91

Hostname (optional):
malibio.arnes.si

Domain name (optional):

The **WAN address** is an IP address from the subnet assigned to the network management VLAN (should be the same network Access Points are configured on). The **default gateway** is the router address on the management network. The **DNS servers** are used by the server and also in the DNS configuration pushed to the clients via the dhcp. The **Hostname** specified is the name of the server and is actually not used anywhere (it's just for the completeness of the network subsystem configuration).

The specified **domain name** is also used in the dhcp confiuration and pushed to the clients. Currently the only **type of WAN connection** supported is the Bridge (**Note:** NAT support is planned for the final release). **Management LAN interface** should be configured only when using NAT. It sets the IP address of the Layer3 IP interface on the interfaces that connect to the Access Points. **User VLAN** number is the number of the 802.1q tagged VLAN for the users traffic. (Note: It is planned to support multiple user-vlans). One also needs to configure the **User VLAN interface address** on the user traffic VLAN. This is needed because dhcp is L3 protocol and needs to have a full IP interface to run on (Note: This might not be needed if the router of the user traffic VLAN acts as a dhcp proxy – see ip helper address on Cisco equipment; but this isn't tested/supported yet).


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/net
Pojdi
UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...
Reset values
Confirm and Apply changes
Končano

Hostname (optional): malibio.arnes.si

Domain name (optional): arnes.si

Select the type of WAN connection:

● Bridge

○ NAT

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

User VLAN number: 203

User VLAN interface address in IP/CIDR format: 193.2.121.110/29

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):

```
193.2.1.201
193.2.1.232
```

The networks and hosts for the **management access** to the server are the addresses that can be used for SSH remote access and for other management functions.

3.2 Cryptography:

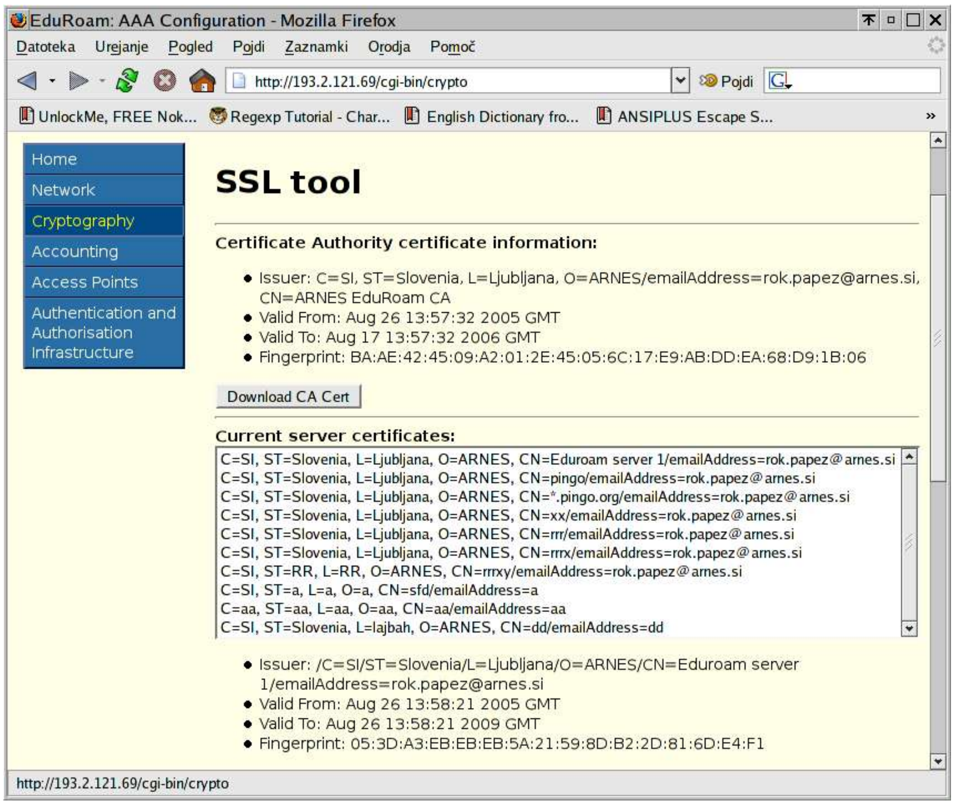
This section is just the Web interface to the OpenSSL toolkit. The operation should be straight forward; first you need to generate a **Certificate Authority** (CA) certificate which is a self-signed master certificate used to sign all the other issued certificates.

The most important field is the **Common Name**. For the CA certificate it is advised to clearly state so, for example: “University of Maribor CA”. For the radius authentication server you may use any text you find suitable. For example: “University of Maribor Eduroam AAA server”. This tool can be used to generate certificates also for other servers (https, pop3s, imaps, ...) but then you need to make sure that you enter the server FQDN (Fully Qualified Domain Name), for example: “www.arnes.si”.

Warning: You should be aware that the certificate requests and private key should be generated on the server they are meant to be used at and then only a request is sent to the CA server which signs it and sends back a valid certificates. This way the private key never leaves the server it belongs to. In our case the certificate key, request and certificate are generated on the Eduroam server and need to be exported to their respective server.

Warning 2: If you use this CA certificate to sign certificates for other purposes than the Eduroam AAI server, they can also be used to represent the valid Eduroam authentication server. So if someone steals for example your web server private key he can pose as a valid Eduroam server for you organization.

With these security warnings in mind, it's OK to use this tool to generate the certificates for other services. And this way you only need to distribute one CA server for the whole organization. Same as usual: it's security vs. usability.


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/crypto
Pojdi
UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...
Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure
Download CA Cert
http://193.2.121.69/cgi-bin/crypto

SSL tool

Certificate Authority certificate information:

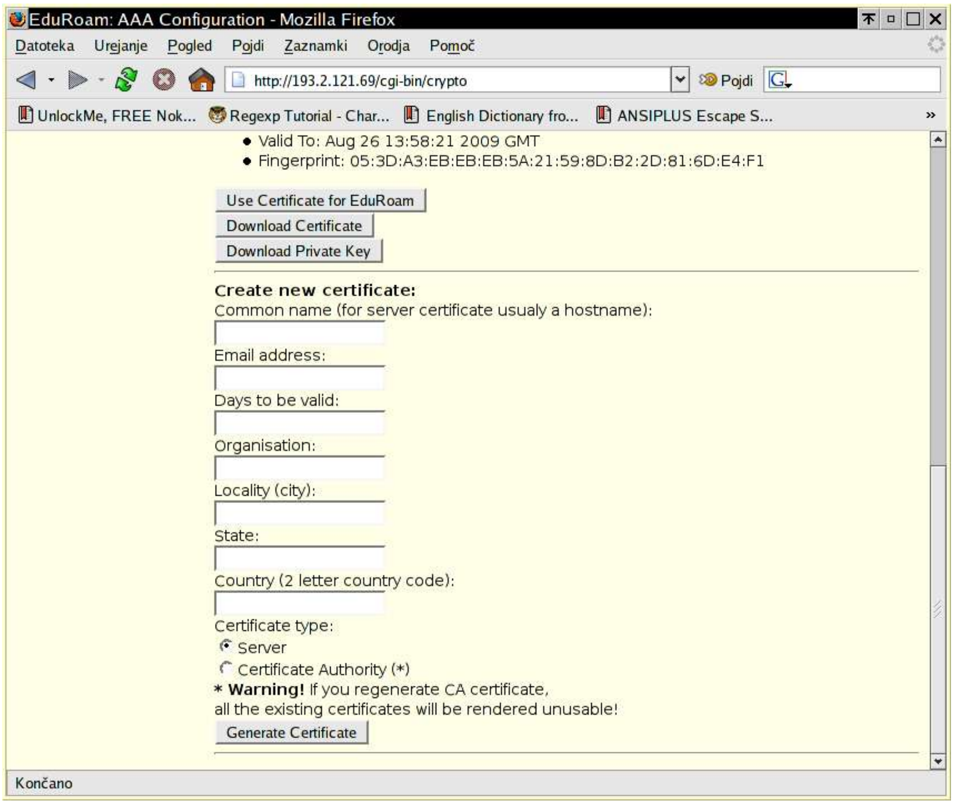
- Issuer: C=SI, ST=Slovenia, L=Ljubljana, O=ARNES/emailAddress=rok.papez@arnes.si, CN=ARNES EduRoam CA
- Valid From: Aug 26 13:57:32 2005 GMT
- Valid To: Aug 17 13:57:32 2006 GMT
- Fingerprint: BA:AE:42:45:09:A2:01:2E:45:05:6C:17:E9:AB:DD:EA:68:D9:1B:06

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=rrrx/emailAddress=rok.papez@arnes.si
C=SI, ST=RR, L=RR, O=ARNES, CN=rrrxy/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

For the countries that don't have states you can insert a dot (".") to keep the field empty or just type in the full country name.


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/crypto
Pojdi
UnlockMe, FREE Nok... Regexp Tutorial - Char... English Dictionary fro... ANSIPLUS Escape S...
Use Certificate for EduRoam
Download Certificate
Download Private Key
Generate Certificate
Končano

- 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

Create new certificate:

Common name (for server certificate usualy a hostname):

Email address:

Days to be valid:

Organisation:

Locality (city):

State:

Country (2 letter country code):

Certificate type:

● Server

○ Certificate Authority (*)

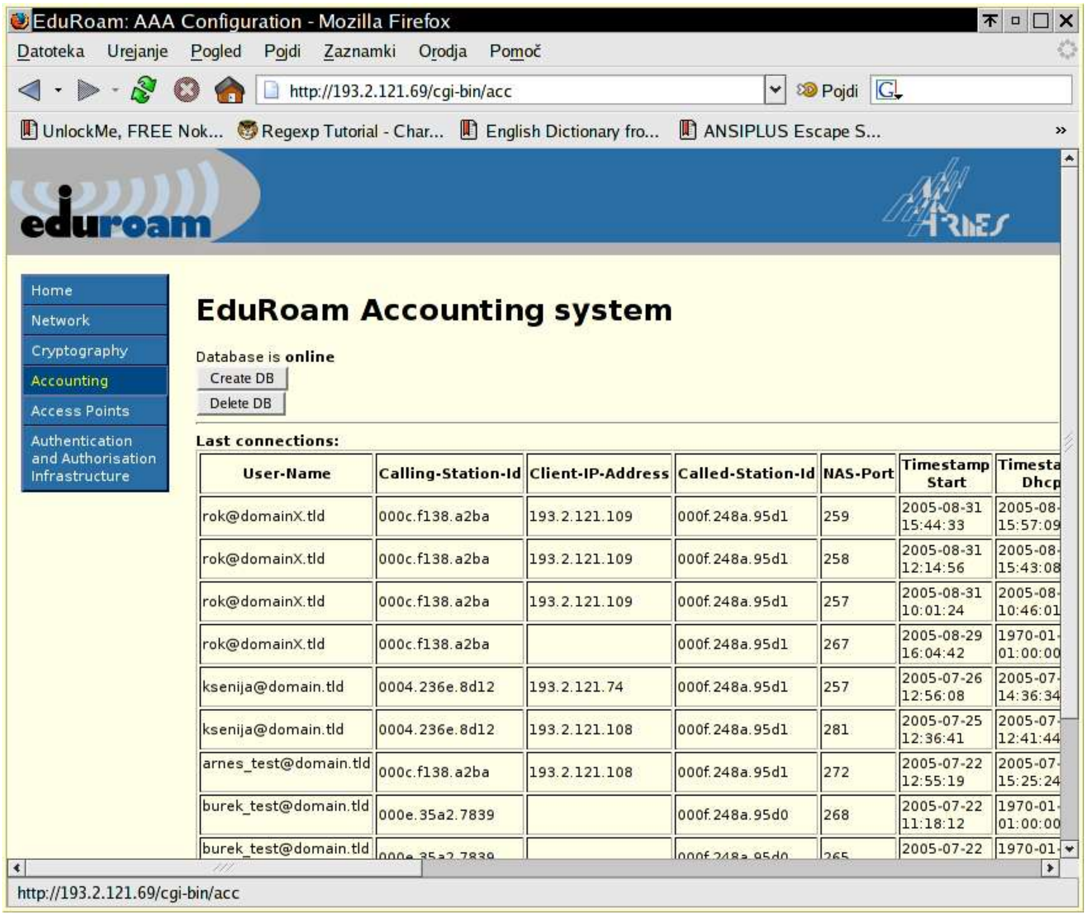
* **Warning!** If you regenerate CA certificate,
all the existing certificates will be rendered unusable!

After you generate a CA certificate you need to generate the Eduroam AAI server certificate. After it is generated you need to select it from the list and mark it for Eduroam use with the **Use the certificate for Eduroam** button.

If you create a new CA certificate it will overwrite the old one and render all the deployed certificates unusable.

3.3 Accounting:

The button **Create DB** creates the needed structures in the MySQL database. If there is a problem with a connection to the server, make sure the MySQL is started and that MySQL root user has full access without the password (If you password protect the MySQL administrator root user account make sure the password is set in the /root/.my.cnf file)


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/acc
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
Create DB
Delete DB
http://193.2.121.69/cgi-bin/acc

EduRoam Accounting system

Database is **online**

Last connections:

User-Name	Calling-Station-Id	Client-IP-Address	Called-Station-Id	NAS-Port	Timestamp Start	Timesta Dhcp
rok@domainX.tld	000c.f138.a2ba	193.2.121.109	000f.248a.95d1	259	2005-08-31 15:44:33	2005-08- 15:57:09
rok@domainX.tld	000c.f138.a2ba	193.2.121.109	000f.248a.95d1	258	2005-08-31 12:14:56	2005-08- 15:43:08
rok@domainX.tld	000c.f138.a2ba	193.2.121.109	000f.248a.95d1	257	2005-08-31 10:01:24	2005-08- 10:46:01
rok@domainX.tld	000c.f138.a2ba		000f.248a.95d1	267	2005-08-29 16:04:42	1970-01- 01:00:00
ksenija@domain.tld	0004.236e.8d12	193.2.121.74	000f.248a.95d1	257	2005-07-26 12:56:08	2005-07- 14:36:34
ksenija@domain.tld	0004.236e.8d12	193.2.121.108	000f.248a.95d1	281	2005-07-25 12:36:41	2005-07- 12:41:44
arnes_test@domain.tld	000c.f138.a2ba	193.2.121.108	000f.248a.95d1	272	2005-07-22 12:55:19	2005-07- 15:25:24
burek_test@domain.tld	000e.35a2.7839		000f.248a.95d0	268	2005-07-22 11:18:12	1970-01- 01:00:00
burek_test@domain.tld	000e.35a2.7839		000f.248a.95d0	265	2005-07-22	1970-01-

The **Delete DB** will clear all the structures and records.

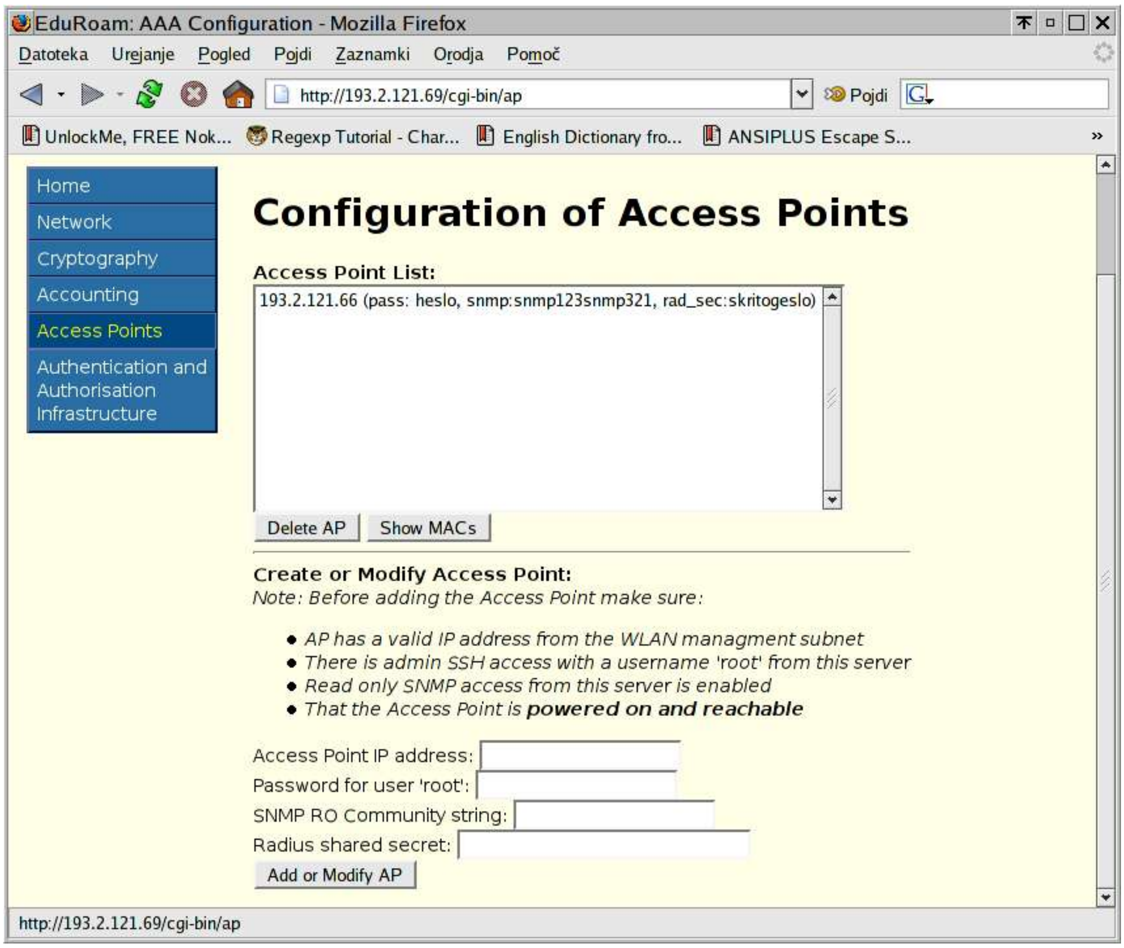
On this page you can see the last 10 successful authentications made to the Eduroam server via the displayed table. For accessing the accounting data you can use:

- “mysql” command line client
- administration GUI client: http://dev.mysql.com/downloads/administrator/
- query browser: http://dev.mysql.com/downloads/query-browser/
- web tool: http://www.phpmyadmin.net/.

The passwords for different MySQL service users are generated at random.

3.4 Access Points:

In this section the access points are added to the management system. The access points need to be correctly configured (check the manual section 2.2), connected to the LAN interfaces of the Eduroam server and be reachable from the server.


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/ap
Pojdi
UnlockMe, FREE Nok...
Regexp Tutorial - Char...
English Dictionary fro...
ANSIPLUS Escape S...
Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure
Delete AP
Show MACs
Add or Modify AP
http://193.2.121.69/cgi-bin/ap

Configuration of Access Points

Access Point List:

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

Create or Modify Access Point:

Note: Before adding the Access Point make sure:

- *AP has a valid IP address from the WLAN managment 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:

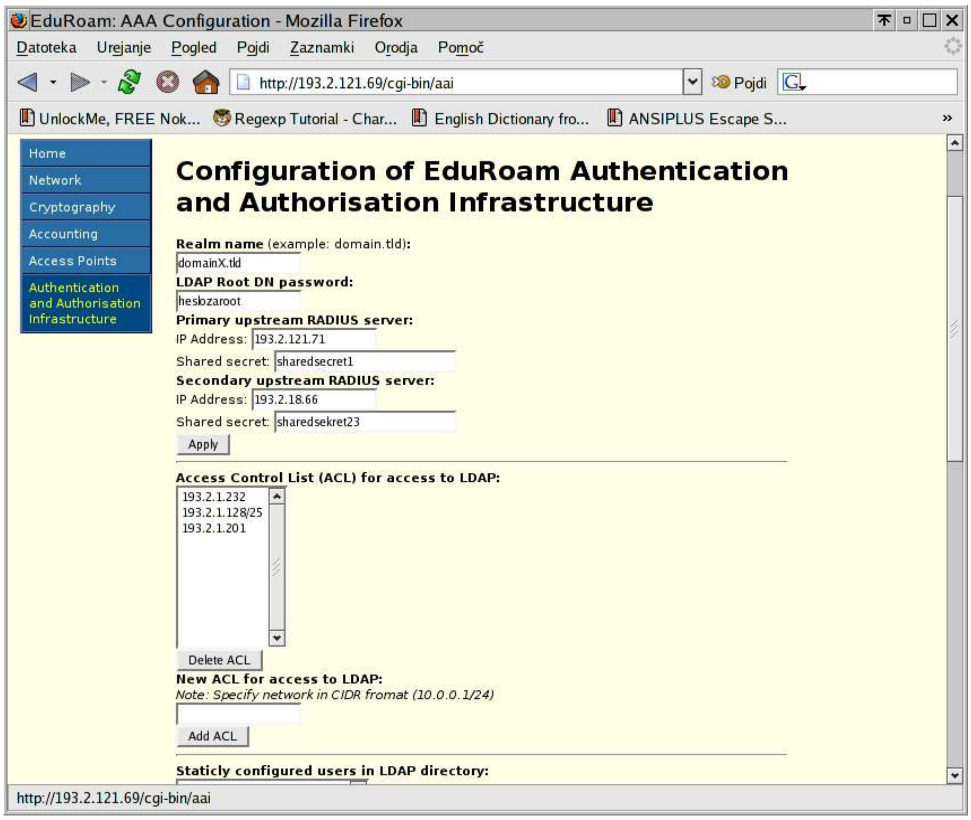
Radius shared secret:

When server is used in a Bridged mode the Access Point management interface will probably be in the same subnet as server WAN interface (they are in the same VLAN). For the NAT mode, the Access Points should be in the same subnet as the server Management LAN interface (again, they are in the same VLAN). See manual section 3.1 for more information.

All the data entered is mandatory and after you press the **Add or Modify AP** button the system will connect to the Access Point and retrieve the list of MACs used on the radio interface. (Note: This might change in the future, however it is planned to evolve this into the AP database and firmware/configuration management tool – XML export of AP database is planned).

3.4 Configuration of Eduroam AAI:

This is the most important part of the Eduroam server. You need to configure the **realm name** this server is authorite for. The LDAP directory **root DN** password is user specified but the DN is automatically set as specified by the realm (the number of dn components depends on the realm): <u>cn=root,dn=realm,dn=name,dn=tld</u>.


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/aai
Pojdi
UnlockMe, FREE Nok...
Regexp Tutorial - Char...
English Dictionary fro...
ANSIPLUS Escape S...
Home
Network
Cryptography
Accounting
Access Points
Authentication and Authorisation Infrastructure
http://193.2.121.69/cgi-bin/aai

Configuration of EduRoam Authentication and Authorisation Infrastructure

Realm name (example: domain.tld): domainX.tld

LDAP Root DN password: heslozaroot

Primary upstream RADIUS server:

IP Address: 193.2.121.71

Shared secret: sharedsecret1

Secondary upstream RADIUS server:

IP Address: 193.2.18.66

Shared secret: sharedsekret23

Apply

Access Control List (ACL) for access to LDAP:

193.2.1.232
193.2.1.128/25
193.2.1.201

Delete ACL

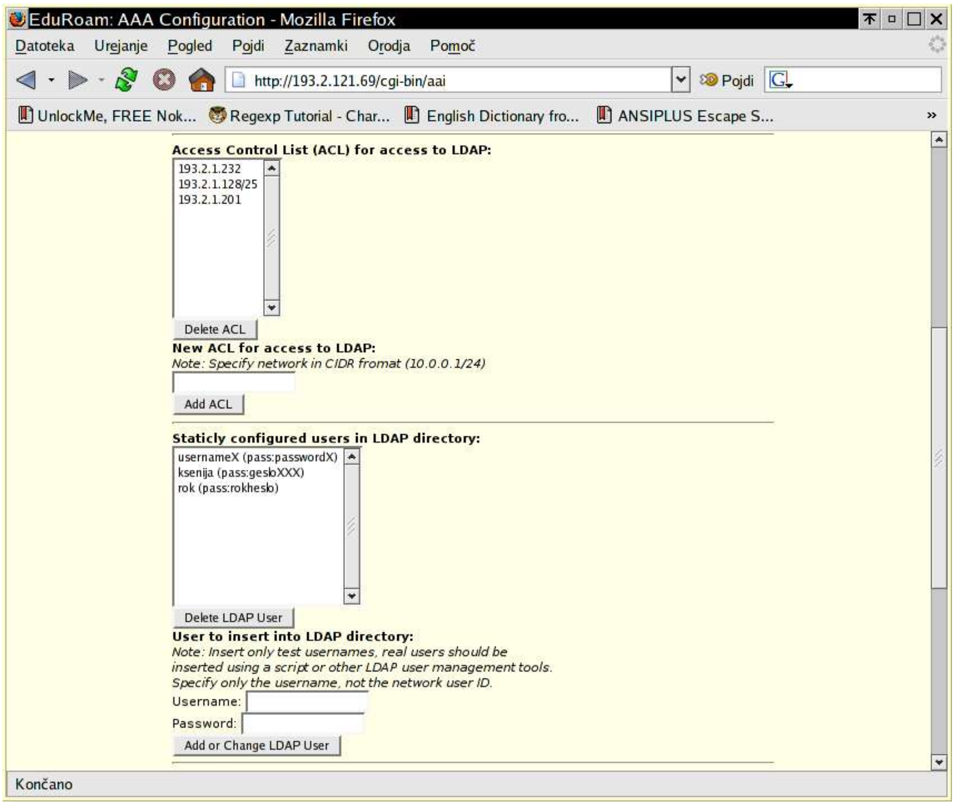
New ACL for access to LDAP:

Note: Specify network in CIDR fromat (10.0.0.1/24)

Add ACL

Staticly configured users in LDAP directory:

After the radius information is entered press **Apply** and the entered information is stored into the Eduroam system configuration. The changes don't take effect until you press **Commit changes** at the bottom of this section after you configured everything to your liking.


EduRoam: AAA Configuration - Mozilla Firefox
Datoteka Urejanje Pogled Pojdi Zaznamki Orodja Pomoč
http://193.2.121.69/cgi-bin/aai
Pojdi
UnlockMe, FREE Nok...
Regexp Tutorial - Char...
English Dictionary fro...
ANSIPLUS Escape S...
Končano

Access Control List (ACL) for access to LDAP:

193.2.1.232
193.2.1.128/25
193.2.1.201

Delete ACL

New ACL for access to LDAP:

Note: Specify network in CIDR fromat (10.0.0.1/24)

Add ACL

Staticly configured users in LDAP directory:

usernameX (pass:passwordX)
ksenija (pass:gesloXXX)
rok (pass:rokheslo)

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.

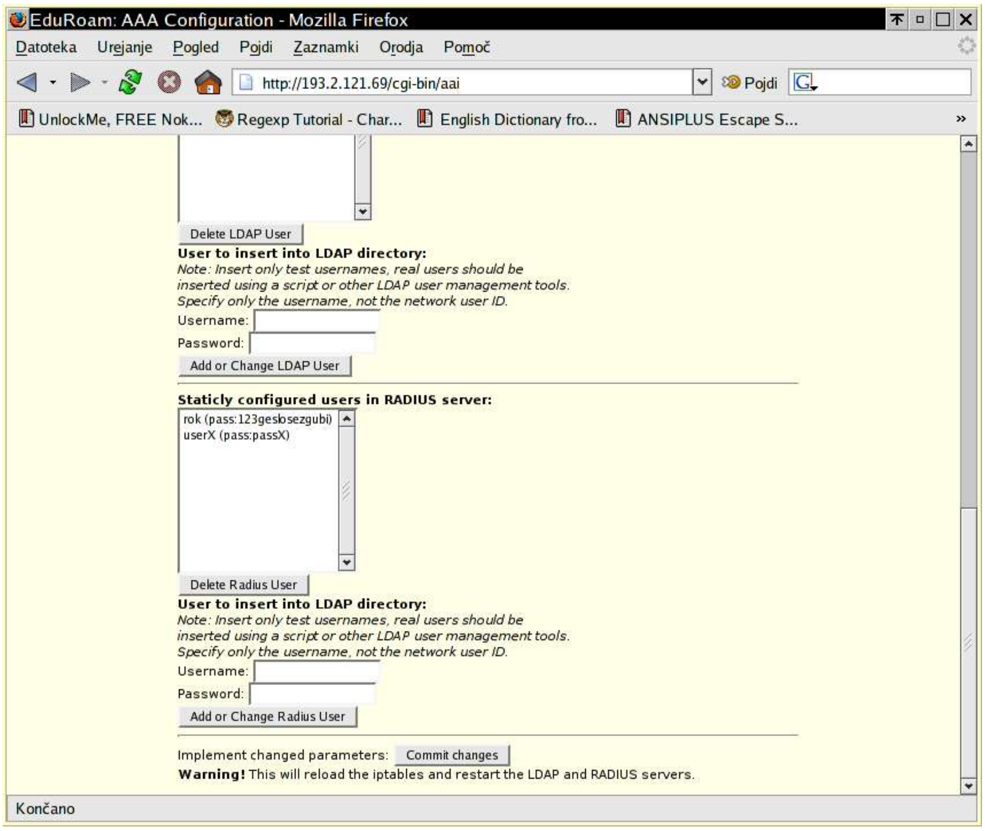
Username:

Password:

Add or Change LDAP User

The information from **ACL for access to LDAP** are used as input for firewall rules to allow incoming connection from trusted servers/workstations. A new ACL line can be added by typing it into the **New ACL for access to LDAP** field and pressing **Add ACL** or removed using the **Delete ACL**.

For testing it's wise to add a **Staticly configured user to LDAP** directory. This isn't intended to be used as administrative tool for adding users to the directory but only as a way to configure few test users.
Similarly the **Staticly configured user to RADIUS** are used to insert users directly into the Radius server.



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:

Staticly configured users in RADIUS server:
rok (pass:123geslosezgubi)
userX (pass:passX)

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:

Implement changed parameters:
Warning! This will reload the iptables and restart the LDAP and RADIUS servers.

After the settings are correctly configured press the **Commit changes** and the LDAP and Radius configurations are generated, services started and usernames created.

Congratulations! Eduroam system should now be operational ;-).... and since this isn't very likely, don't give up and read the next section....

4. Anatomy:

Most of the system resides in the /var/eduroam directory. All the paths if not specified otherwise are relative to this directory.

If you want to re-brand the system, it was designed with that in mind. You need to edit the files in ./html.

If you look in the ./system_templates directory you can see the template configuration files. These can be modified to tailor configuration to site or NREN need. Template files are read by the system, the data from Web forms inserted, the configurations are written and services restarted. This process is, because of the nature of CGI scripts, split into two parts, the cgi-bin scripts run by the apache web server are in the ./cgi-bin directory. They store the data into the ./etc directory and then call the suid wrapper ./helpers/eduroam_helper with the name of the 2nd stage script to run. The script must reside in the ./helpers directory and the allowed script names are hard-wired into the suid eduroam_helper binary.

The scripts in the ./helpers directory read the configuration from ./etc and output the needed services configurations and restart them.