A practical guide to Eduroam

Rok Papež
ARNES - Academic and research network of Slovenia
rok.papez@arnes.si

Nicosia, January 2007
Eduroam AAI

Akademska in raziskovalna mreža Slovenije

Diagram showing the architecture of Eduroam AAI with a root server, top level server, and various organisations interconnected through a tunnel established via Radius servers to users' home organisations (used only for credentials exchange)
Access Points
   – Enterprise grade equipment

Wired network
   – Broadband to internet
   – VLAN (802.1q)
   – Security (guest network)

Radius AAA server
   – Local authentication
   – Foreign request proxying

Supplicant
   – Eduroam client
   – Server certificates
Wired and wireless network

NREN network - Internet

Access Router

802.1q switch

802.1q tagged VLANs
L2 switched network

Staff ethernet

Students ethernet

802.1q switch

802.1q switch

802.1q tagged VLANs
L2 switched network

Eduroam Guest

802.1q access points
Technology used
- SSID=eduroam
- WPA Enterprise (+ WPA2/802.11i)
- Dynamic VLANs
- Support for legacy networks (multiple SSIDs)

Radius configuration
- EAP-TTLS + PAP
- anonymous@domain outer identity
- Send real user-name in Access-Accept (accounting)
- Log full radius accounting + IP address
- Freeradius
Radius server: Freeradius

Installation
- RPM packages for Fedora Core (http://www.pingo.org/eduroam)
- From source: http://www.freeradius.org
- Regexp patch from: http://www.eduroam.si
- Part of the installed UNIX operating system

Configuration
- Manually
- Using the “eduroam in a box” web interface

Realm proxying
- Eduroam realm name == DNS domain
- Delegate wildcard sub-domains (*.domain.tld)
  - Authorisation based on full realm name
- Loop prevention
Freeradius manual configuration:
Proxying (Sending the requests)

/etc/raddb/proxy.conf:

# handle our realm locally
realm domain.tld {
}

# blackhole and NULL are handled (denied in users file) locally
realm blackhole.domain.tld {
    regex = ".*\.domain\.tld"
}
realm NULL {
}

realm DEFAULT {
    type = radius
    authhost = 10.0.0.2:1812
    accthost = 10.0.0.2:1813
    secret   = *****
    nostrip
Freeradius manual configuration: Proxying (Receiving requests)

/etc/raddb/clients.conf:

```bash
# Upstream radius server
client 10.0.0.2 {
    secret    = *****
    shortname = primary_radius
    nastype   = other
}
```
Freeradius manual configuration:  
Proxying and Local LDAP search

/etc/raddb/users:

# Users with a blackhole or NULL realm should be rejected
DEFAULT Realm == NULL, Auth-Type := Reject
DEFAULT Realm == blackhole.domain.tld, Auth-Type := Reject

# If user isn't found, check LDAP directory for it.
# But only for the inner tunnel request.
DEFAULT Realm == domain.tld, Freeradius-Proxied-To == 127.0.0.1, Autz-Type := LDAP
    Fall-Through = yes
Freeradius manual configuration:  
Access to LDAP

/etc/raddb/radiusd.conf:

```ini
[modules]
ldap {
    server = "localhost"
    basedn = "dc=domain,dc=tld"
    filter = "(siEduPersonPrincipalName=%{User-Name})"
    identity = "cn=root,dc=domain,dc=tld"
    password = "*****"
    password_attribute = "userPassword"
    start_tls = no
}

[authorize]
Aautz-Type LDAP {
    ldap
}
```
**AAI peers**

Define at least the primary radius server to forward requests for unknown realms to. This is usually the upstream radius server.

---

**Primary upstream RADIUS server:**
- IP Address: 192.168.1.255
- Shared secret: randomnoiseintext

**Secondary upstream RADIUS server:**
- IP Address: 10.0.70.2
- Shared secret: happy_secret2

[Apply]
Configure Radius group:

```
aaa group server radius radius_grp
server 10.2.18.130 auth-port 1812 acct-port 1813
```

Configure network (SSID)

```
dot11 ssid eduroam
vlan 251
authentication open eap radius_auth
authentication key-management wpa
accounting default
guest-mode
```

Configure radio interface

```
interface Dot11Radio0
  encryption vlan 251 mode ciphers aes-ccm tkip
  ssid eduroam

interface Dot11Radio1
  encryption vlan 251 mode ciphers aes-ccm tkip
  ssid eduroam
```
Set RADIUS server connection secret:

```
radius-server host 10.0.0.130 auth-port 1812 acct-port 1813 key **********
```

Configure server part:

```
/etc/raddb/clients.conf:

# ===============
# Access Points
# ===============

client 10.0.0.131 {
  secret    = **********
  shortname = ap1
  nastype   = cisco
}
```
Connecting without the eduroam client
- Setting up windows wireless
- Setting up SecureW2
- First connect problem (certificates)

Connecting with the eduroam client
- Uses secureW2 site deployment
- Certificates are pre-installed
- SecureW2 is pre-configured
  - username/password
- Wireless encryption settings
- ftp://ftp.arnes.si/software/eduroam
Eduroam client configuration
Windows wireless configuration

3com Properties
- Use Windows to configure my wireless network settings
- Available networks:
- Preferred networks:
- eduroam (Automatic)

eduroam properties
- Network name (SSID): eduroam
- Wireless network key
  - Network Authentication: WPA
  - Data encryption: TKIP
- Network key:
- Confirm network key:
- Key index (advanced): 1
- The key is provided for me automatically
- This is a computer-to-computer (ad hoc) network; wireless access points are not used
Eduroam in a box

Configuration wizard
- AAI server (LDAP, Radius, SQL, DHCP, ...)
- Web based

Certificate handling

Connection monitoring

Logging

Ethernet security mechanisms

Easy to use:
- Part of local Linux distribution
- Install and open http://localhost/eduroam

OpenSource: http://eduroam.sourceforge.net
Eduroam in a box:
DNS configuration

A list of DNS servers:
10.0.13.2
192.168.8.22

New DNS server:
Note: Specify host with numeric IP address (example: 192.168.12.34)
Commit changes

All the configured settings are applied on this screen. The Commit changes button commits only the pending changes while the Rebuild everything button reconfigures all the components. Rebuilding everything can take a lot of time.

Eduroam in a box configuration components:

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>bridge</td>
<td>Network bridgeing and security mechanisms</td>
</tr>
<tr>
<td>Pending</td>
<td>dhcp</td>
<td>DHCP server configuration</td>
</tr>
<tr>
<td>Pending</td>
<td>firewall</td>
<td>IP firewall settings (iptables)</td>
</tr>
<tr>
<td>Pending</td>
<td>interfaces</td>
<td>Network interface configuration</td>
</tr>
<tr>
<td>OK</td>
<td>ldap directory</td>
<td>Configuration of data in LDAP directory</td>
</tr>
<tr>
<td>OK</td>
<td>ldap server</td>
<td>LDAP server configuration</td>
</tr>
<tr>
<td>OK</td>
<td>network</td>
<td>Fundamental network settings</td>
</tr>
<tr>
<td>OK</td>
<td>ntp</td>
<td>NTP time synchronisation over the network</td>
</tr>
<tr>
<td>OK</td>
<td>radius</td>
<td>RADIUS server general configuration</td>
</tr>
<tr>
<td>OK</td>
<td>radius clients</td>
<td>RADIUS client devices and peers</td>
</tr>
<tr>
<td>OK</td>
<td>radius proxy</td>
<td>RADIUS server request proxying</td>
</tr>
<tr>
<td>OK</td>
<td>radius users</td>
<td>Staticly configured users in RADIUS settings</td>
</tr>
<tr>
<td>Pending</td>
<td>resolver</td>
<td>Eduroam server resolving (DNS) settings</td>
</tr>
</tbody>
</table>
System supports the following modes:

- **Standalone** - for use with any type of networks. In this most simple mode system provides no extra firewalling functionality or client security checking.
- **Bridge** - in this mode the Access Points are connected to the server on the additional network ports. The system uses VLANs to establish a bridging (functions like a Layer2, ethernet switch) between the router and the Access Points. In this mode clients use public IP addresses (Gateway is on the router and not this server).
- **Bridge with retagging** - this mode is similar to the "Bridge" mode. In addition it also remaps the 802.1q tags for the inner interface.
  
  Becouse the Access Points are usually well dispersed around the campus it is hard to connect them all physically to the same server. With retagging the same network can be fed back into the same switch.
- **NAT** - This mode is similar to the 'Bridge' mode, but the server acts as an address translating router and clients get addresses from the private address space.
- **Guest portal** - this setting will enable the use of open network with web login. Since this is in violation of the eduroam policy only local users are allowed to use weblogin.
- **TODO**: Mixed modes for different networks.

**Select the type of eduroam server:**

- Standalone
- Bridge
- Bridge with retagging
- NAT

*NOTE: Portal will work only for local users!*
Eduroam in a box: Bridge type

NREN network - Internet

Access Router

802.1q tagged VLANs L2 switched network

802.1q switch

Staff ethernet

Students ethernet

Eduroam in a box: Bridge installation type

802.1q tagged VLANs L2 switched network

802.1q access points

Eduroam Guest
It's easy to use:
- PC with multiple ethernet cards
- Install Linux
- Install EiAB („yum install eduroam“)
- Connect the PC to the wired network
- Connect Access Points to the PC
- Open http://localhost/eduroam
- Configure the system and commit changes
Gathering statistics

- Network planning
- PR team
- Easy with good accounting in SQL database

Network use varies a lot

- Summer vacations
- Winter vacations
- Exam periods

Steep climb

- network logins
- number of active users
- Most of the users are from technical faculties
Eduroam network logins
Student survey October 2005

- Use of any wi-fi
  - Only 15.2% of students use Wi-Fi technology (routers, sharing of internet connection with a neighbor at home ...)
  - Eduroam is being used by 5% of students

- Reasons for not using the eduroam
  - Not informed about it
  - Don't own a laptop
  - They don't know how to use it
  - Bad experience with use

- Why students don't bring laptops to lectures
  - Don't want to stand out
  - Afraid of damage or theft
Bob Metcalf, Xerox, 1972
Unauthorized network use
  – Rogue Access Points

MAC spoofing

ARP attacks
  – Router
  – Other users

DHCP attacks
  – DOS
  – Eavesdropping

IP spoofing
Ethernet security mechanisms

- Network login (wireless or wired - 802.1x)
- Wireless connection encrypted (WPA)
- Special mechanisms on a router/switch
  - ip dhcp snooping
  - ip arp inspection
  - ip verify source
- IP security
  - Firewall
  - ACL
Future of eduroam in Slovenia

- Eduroam on wired networks
  - Testing of equipment (switches)
  - Looking at the possibility to use for dial-up

- RadSec for inter-radius connections

- Eduroam_client
  - Localization
  - Limited development resources

- Eduroam in a box
  - Deploying eduroam in smaller organisations/departments
  - Web configuration wizard and management tool
  - (optional) built in firewalling (L2/L3 security)
  - Free software
Eduroam.si

http://www.eduroam.si

mailto: aaa-podpora@arnes.si