



Connect. Communicate. Collaborate

# Eduroam in a box - Easy setup of eduroam server

Rok Papež, ARNES

Terena Networking Conference,  
Catania, 17. May 2006

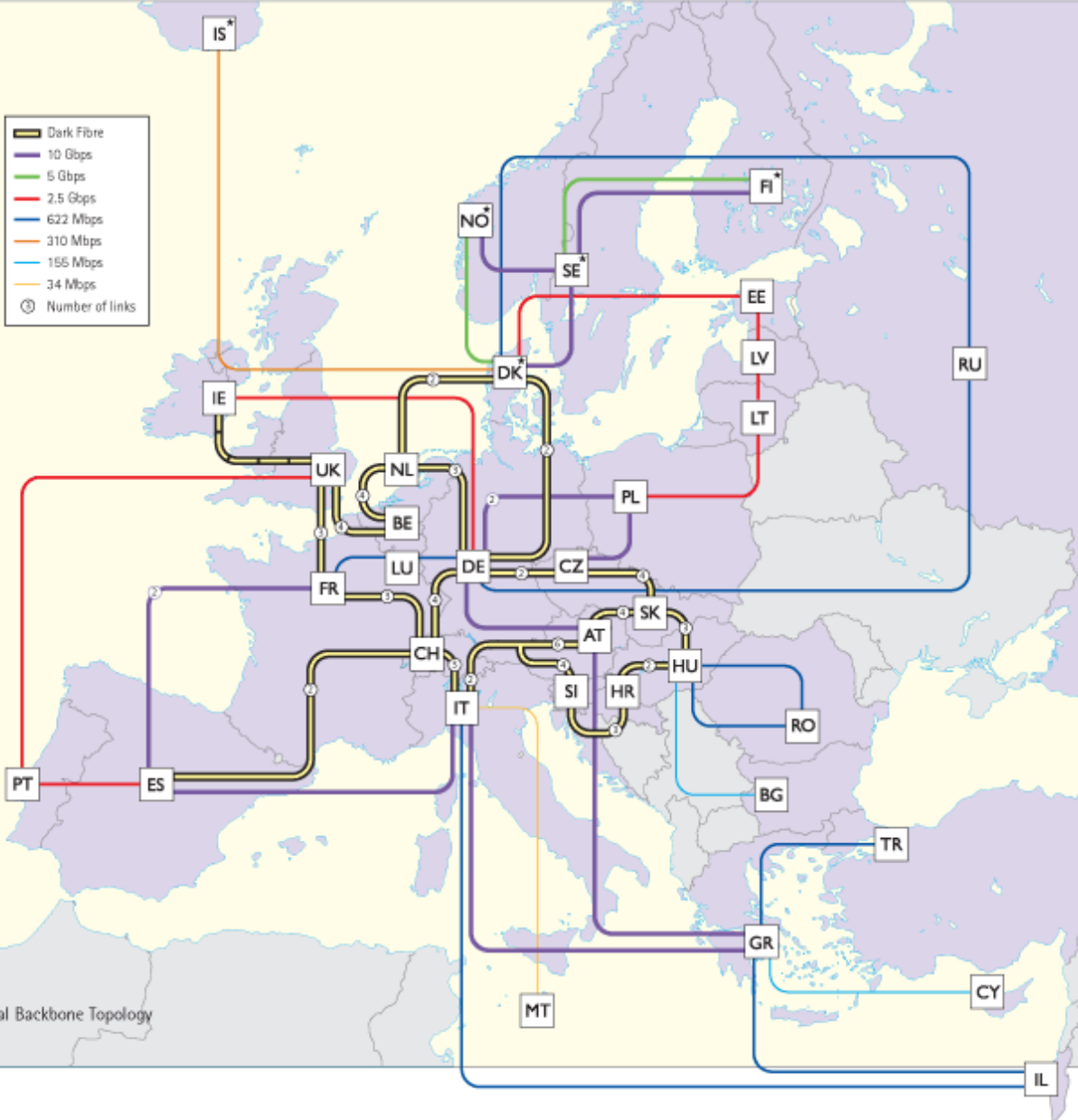


Connect. Communicate. Collaborate

## GÉANT2 Topology

Can you find  
Slovenia (SI) ?

Picture from GÉANT2 example slide



# Eduroam in Slovenia



Connect. Communicate. Collaborate

- National eduroam = international eduroam + local requirements
- Well defined technical specifications
  - High technical standards
    - WPA(2) Enterprise
    - SSID: „eduroam“
    - Send real User-Name with Access-Accept
    - Monitor connections
      - Closing stale connections
      - Full logging + IP
    - Hardening the ethernet (L2/L3 security)

# Setting up eduroam.si



Connect. Communicate. Collaborate

- Organised identity management
  - LDAP directory
- Suitable network infrastructure
  - Access Points
  - Guest network (optional)
  - 802.1x on wired ethernet (optional)
  - Hardening the ethernet (L2/L3 security)
  - Eduroam server (placed in higher security network)
    - LDAP, FreeRADIUS, DHCP, MySQL, Monitoring software



Connect. Communicate. Collaborate

# Is eduroam complex ?

- Yes and No :)
- Depends on the organisation
  - Network infrastructure
  - IT personnel
- Bigger organisations
  - Usually not
  - Just fine tune existing systems
- Smaller organisations:
  - Can be a BIG project
  - Outsourced IT



Connect. Communicate. Collaborate

# Eduroam in a box goals

- Simplify and speed-up deployment
- Require less technical skills
  - Easy installation
  - Easy configuration
- Deploy proven solution (template configuration, less errors)
- Turn-key solution
- Harden the ethernet (L2/L3 security)
- Usable by other NRENs and for site deployment
  - Localisation
  - Themes
  - Custom template configurations

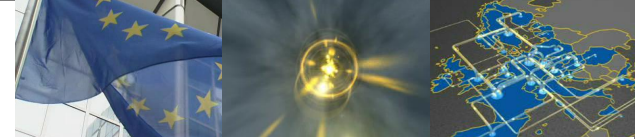


Connect. Communicate. Collaborate

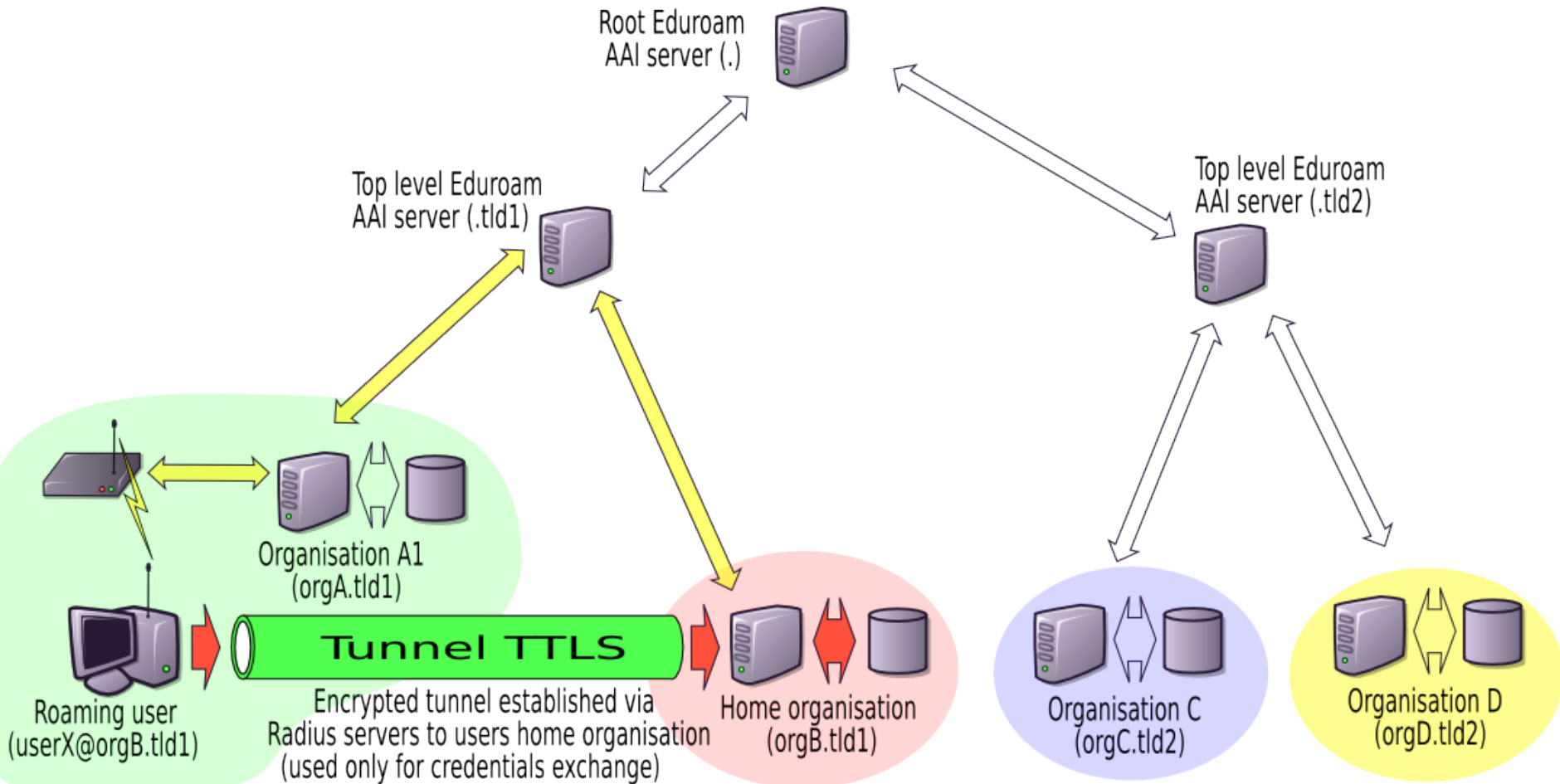
# Eduroam in a box

- 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>

# „Where does EiAB fit in ?“



Connect. Communicate. Collaborate



# System set-up



Connect. Communicate. Collaborate

- 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

# Stable version (0.3.6)



Connect. Communicate. Collaborate

- Is a part of Pingo 4.x/Fedora Core 4 operating system
- Actual deployment
  - Turn-key solution (bridge mode)
  - Customizable for a more complex deployment
    - CTK – Central technical library from Uni of Ljubljana
- Internal testing
  - Quality Assurance
  - Usability
- External feedback

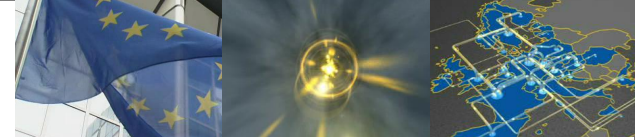


Connect. Communicate. Collaborate

# In development (0.4.x)

- Simplified interface
- More functionality
  - Standalone
  - Bridge
    - 802.1q retagging
  - NAT
- Smarter framework
  - Aware of components
  - Improved handling of input (validation)
  - Data dependant User Interface

# Screenshot 1: DNS



Connect. Communicate. Collaborate

The screenshot shows the eduroam configuration interface. On the left is a navigation menu with the following items: Home, System, Network, Physical Interfaces, Virtual LANs, IP address, Gateway, Hostname, DNS (highlighted in yellow), NTP, Firewall, Certificates, AAI servers, Access Points, and Commit Changes. The main content area is titled "A list of DNS servers:" and contains a scrollable list with two entries: 10.0.13.2 and 192.168.8.22. Below the list is a "Delete DNS" button. Underneath is a section for "New DNS server:" with a note: "Note: Specify host with numeric IP address (example: 192.168.12.34)". This section includes an empty text input field and an "Add DNS" button.

# Screenshot 2: Type



Connect. Communicate. Collaborate

Home
System
Authentication
Trusted hosts
Eduroam type
Network
Certificates
AAI servers
Access Points
Commit Changes

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.  
Because 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:

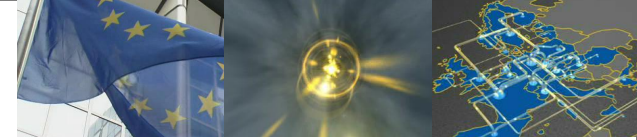
- Standalone
- Bridge
- Bridge with retagging
- NAT

*NOTE: Portal will work only for local users!*

Web portal

Apply

# Screenshot 3: Radius peers



Connect. Communicate. Collaborate

Home

System

Network

Certificates

AAI servers

Realm

Radius peerings

Radius users

LDAP password

LDAP ACL

LDAP users

Access Points

Commit Changes

## 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

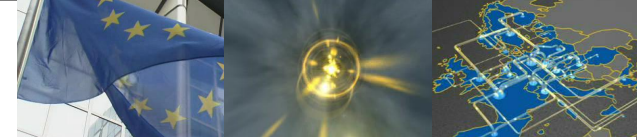
### Secondary upstream RADIUS server:

IP Address: 10.0.70.2

Shared secret: happy\_secret2

Apply

# Screenshot 4: Commit changes



Connect. Communicate. Collaborate

Home

System

Network

Certificates

AAI servers

Access Points

Commit Changes

## 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:

Status	Name	Description
Pending	bridge	Network bridging and security mechanisms
Pending	dhcp	DHCP server configuration
Pending	firewall	IP firewall settings (iptables)
Pending	interfaces	Network interface configuration
OK	ldap directory	Configuration of data in LDAP directory
OK	ldap server	LDAP server configuration
OK	network	Fundamental network settings
OK	ntp	NTP time synchronisation over the network
OK	radius	RADIUS server general configuration
OK	radius clients	RADIUS client devices and peers
OK	radius proxy	RADIUS server request proxying
OK	radius users	Statically configured users in RADIUS settings
Pending	resolver	Eduroam server resolving (DNS) settings

Commit changes

Rebuild everything

# A few words about the future...



Connect. Communicate. Collaborate

- Don't predict it :)
- Exception to the rule: EiAB will still be cool :)
- Interesting functionalities to add ?
  - Access point database (AP phone book)
  - Daily statistics and graphing
  - Automatic AP configuration and management
  - Debugging of failed attempt
  - Web redirect for temporary events
  - VPN tunnel for off-site Access Points
- EiAB demo site ?

# Questions ?



Connect. Communicate. Collaborate

Web: <http://eduroam.sourceforge.net>

Support: [aaa-podpora@arnes.si](mailto:aaa-podpora@arnes.si)

Mail: [rok.papez@arnes.si](mailto:rok.papez@arnes.si)