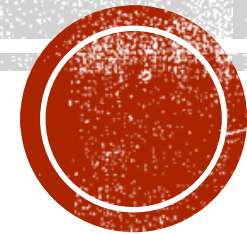
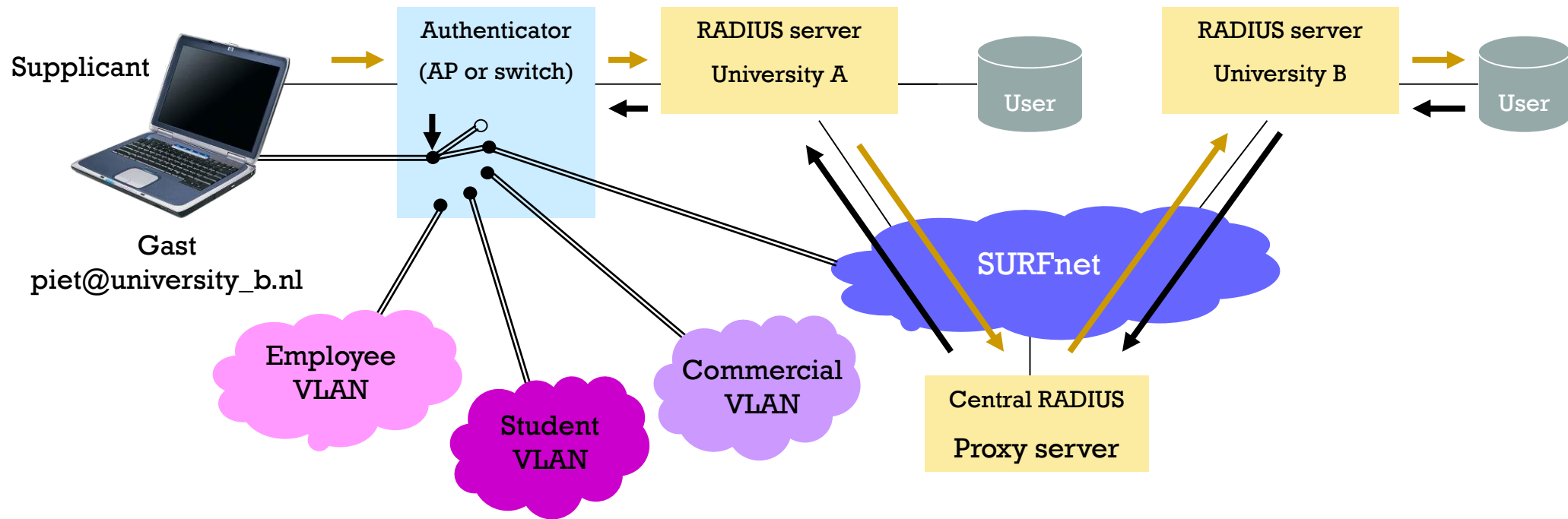


# EDUROAM TECHNICAL SETUP

การตั้งค่า Radius สำหรับ Institute Level



# EDUROAM NETWORK ACCESS

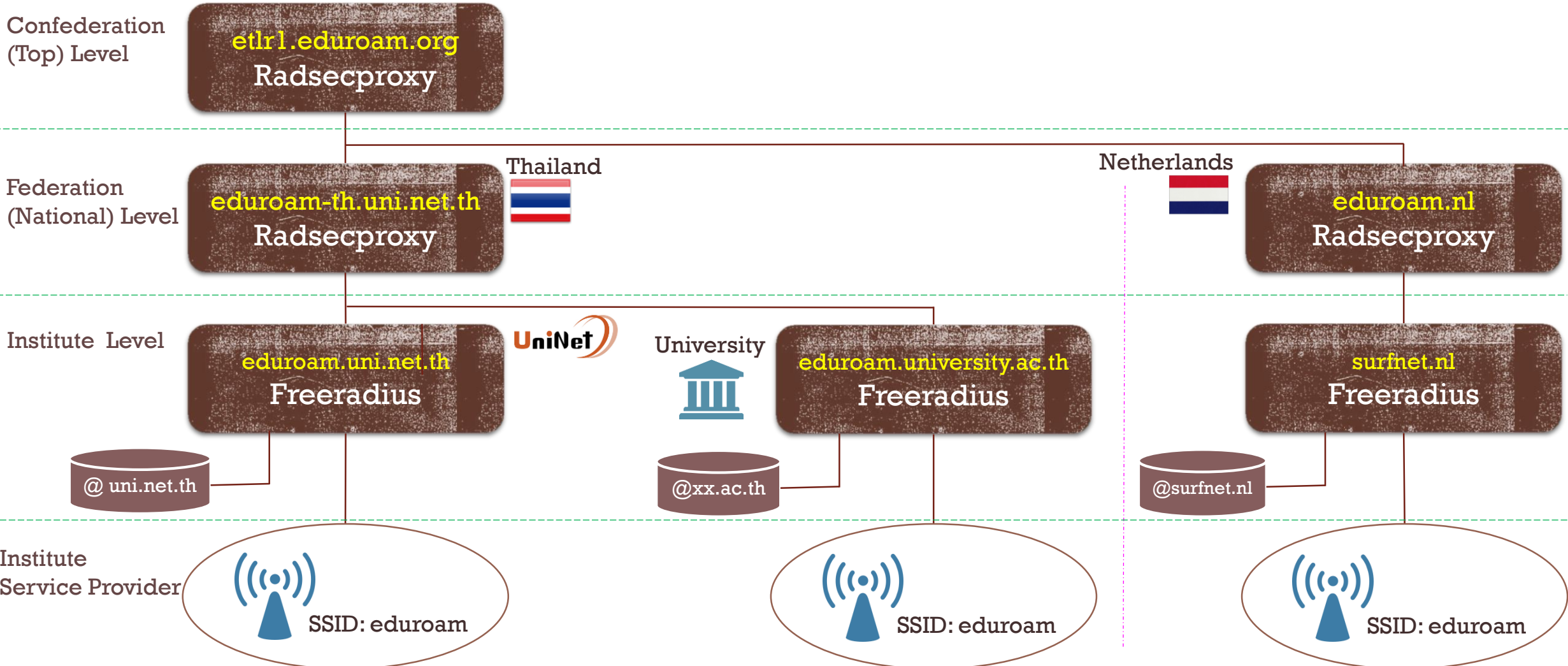


—→ signalling  
 == data

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



# LOGICAL TOPOLOGY



# RADIUS CONFIGURATION FOR INSTITUTE LEVEL

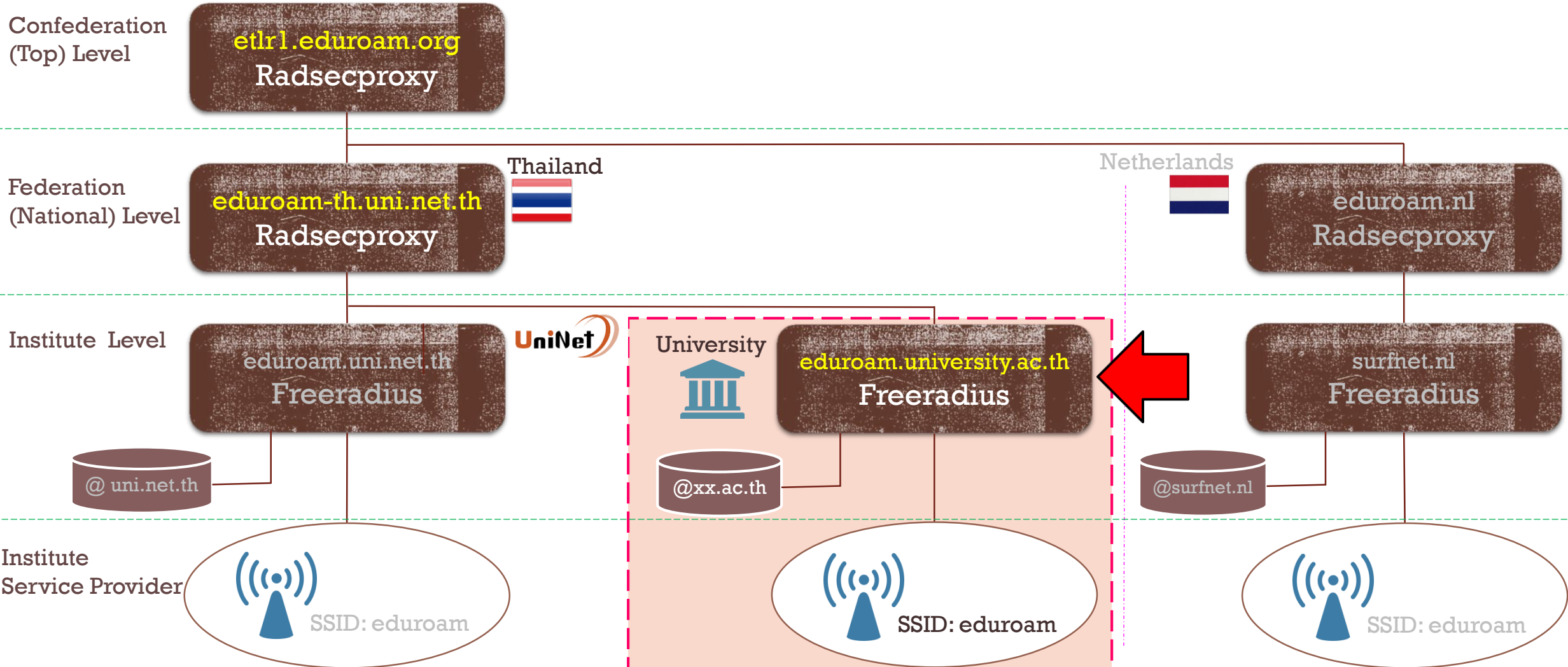
- Server Requirements :



- » **Server operating system**  
Recommended operating system : Linux or Ubuntu
- » **Radius Server**  
Freeradius version 2 or later



# LOGICAL TOPOLOGY



# RADIUS CONFIGURATION FOR INSTITUTE LEVEL

- Files were modified :
  - » /etc/raddb/radiusd.conf
  - » /etc/raddb/sites-enabled/eduroam
  - » /etc/raddb/clients.conf
  - » /etc/raddb/proxy.conf
  - » /etc/raddb/eap.conf
  - » /etc/raddb/sites-enabled/eduroam-inner-tunnel
  - » /etc/raddb/users



# /etc/raddb/radiusd.conf

```
security {
    max_attributes = 200
    reject_delay = 0
    status_server = yes
}
proxy_requests = yes
```



```
listen {
    type = auth
    ipaddr = *
    port = 1812
}
listen {
    type = auth
    ipv6addr = ::
    port = 1812
}
listen {
    type = acct
    ipaddr = *
    port = 1813
}
listen {
    type = acct
    ipv6addr = ::
    port = 1813
}
```



# /etc/raddb/sites-enabled/eduroam

```
server eduroam {
    authorize {
        auth_log
        suffix
        eap
    }
    authenticate {
        eap
    }
    preacct {
        suffix
    }
    accounting {
    }
    post-auth {
        reply_log
        Post-Auth-Type REJECT {
            reply_log
        }
    }
    ...
}
```

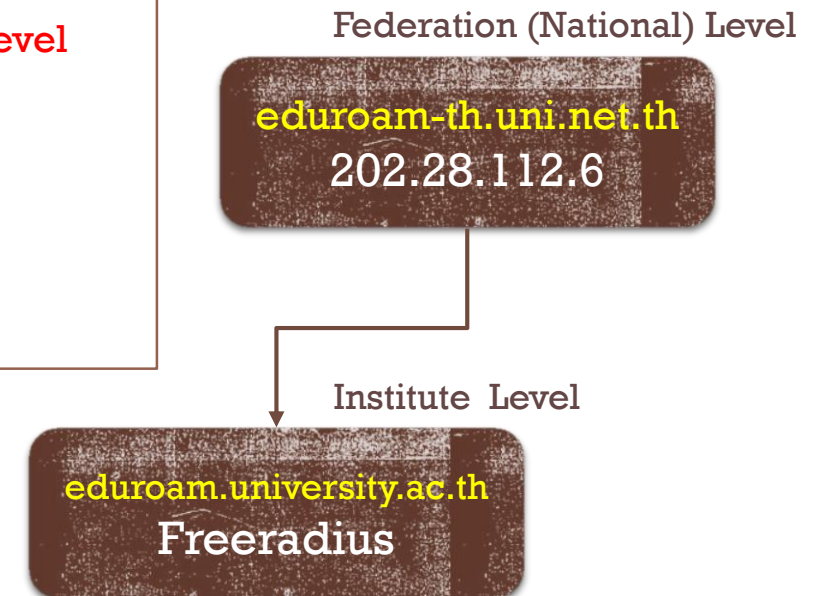
```
...
pre-proxy {
    pre_proxy_log
    if (Packet-Type != Accounting-Request) {
        attr_filter.pre-proxy
    }
}
post-proxy {
    post_proxy_log
    attr_filter.post-proxy
}
}
```



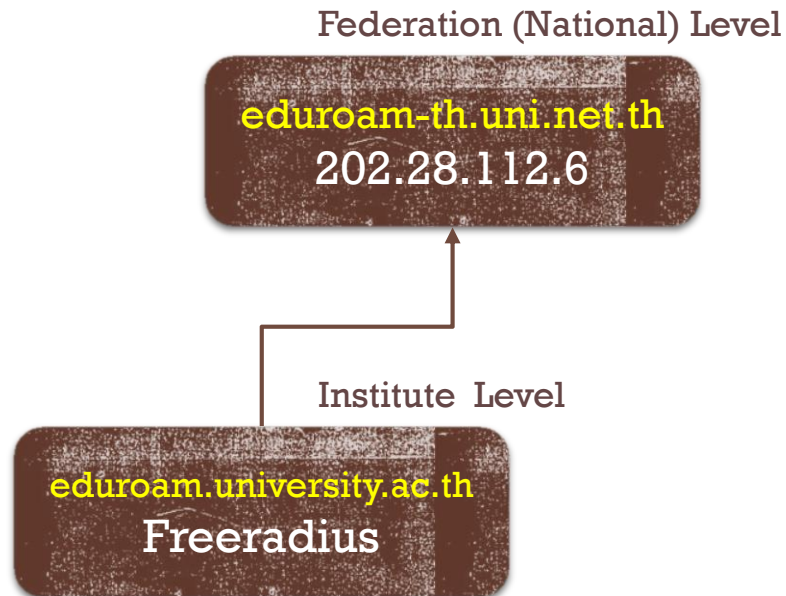


# /etc/raddb/clients.conf

```
#Allow asking from eduroam-TH to eduroam.university.ac.th
client eduroam-th-to-university {
    ipaddr      = 202.28.112.6
    netmask     = 32
    secret      = shared_secret_between_university_to_eduroam-th_level
    require_message_authenticator = no
    shortname   = eduroam-th-to-university
    nastype     = other
    virtual_server = eduroam
}
```



# /etc/raddb/proxy.conf



```
#Allow asking from eduroam.university.ac.th to eduroam-TH
proxy server {
    default_fallback = yes
}
home_server eduroam-th {
    type      = auth+acct
    ipaddr    = 202.28.112.6
    port      = 1812
    secret    = shared_secret_between_university_to_eduroam-th_level
    status_check = status-server
}
home_server_pool EDUROAM{
    type          = fail-over
    home_server   = eduroam-th
}
realm university.ac.th {
    nostrip
}
realm DEFAULT {
    auth_pool = EDUROAM
    nostrip
}
```

# /etc/raddb/eap.conf

```
eap {
    default_eap_type = peap
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no

    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_password = whatever
        private_key_file = ${certdir}/server.key
        certificate_file = ${certdir}/server.pem
        CA_file = ${cadir}/ca.pem
        dh_file = ${certdir}/dh
        random_file = /dev/urandom
        fragment_size = 1024
        include_length = yes
        check_crl = no
        cipher_list = "DEFAULT"
    }
}
...
```

```
...
    ttls {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "eduroam-inner-tunnel"
    }

    peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "eduroam-inner-tunnel"
    }

    mschapv2 {
    }
}
```



# /etc/raddb/sites-enabled/eduroam-inner-tunnel

```
server eduroam-inner-tunnel {  
    authorize {  
        auth_log  
        eap  
        files  
        mschap  
        pap  
    }  
    authenticate {  
        Auth-Type PAP {  
            pap  
        }  
        Auth-Type MS-CHAP {  
            mschap  
        }  
        eap  
    }  
    ...  
}
```

```
...  
    post-auth {  
        reply_log  
        Post-Auth-Type REJECT {  
            reply_log  
        }  
    }  
}
```



# /etc/raddb/users

```
guest1@university.ac.th  Cleartext-Password := "guest1"  
guest2@university.ac.th  Cleartext-Password := "guest2"  
guest3@university.ac.th  Cleartext-Password := "guest3"  
.  
.  
.
```



# EDUROAM TECHNICAL SETUP



การตั้งค่า Radius สำหรับ Institute Level

