如何构建校园级的 eduroam 网络

1. 总览

eduroam 无线 WIFI 全球漫游服务联盟，目前已经覆盖全球七十多个国家和地区的大学及科研机构。参与该联盟的机构只需在本单位设立 eduroam 账户，即可在全球实现无线网络访问的无障碍漫游。您在国外参加学术活动时可直接访问当地的 eduroam 并连入无线网。部署 eduroam 的 SSID 必须为“eduroam”。

关于如何构建校园级的 eduroam 网络，在 eduroam 官网有详细的说明文档。本文档主要帮助中国的用户快速了解 eduroam 在校园或楼宇现有网络环境下的部署方法，包括部署架构、要求和简要步骤。

总体上，全球 eduroam 设施主要包括以下三部分服务：

1）顶级 RADIUS 服务器 Confederation top-level RADIUS Server (TLR)

2）联盟级 RADIUS 服务器 Federation-Level RADIUS servers (FLRs)

3）校园级 RADIUS 服务器 IdP and SP RADIUS infratructure

顶级 TLR 服务器设置在欧洲荷兰和丹麦 eduroam 中心，负责根据地域（例如.nl, .dk, .au, .cn 等）将不同的认证包转发到不同的 FLR 服务器。

eduroam 在每个国家或地区会有 FLR 服务器，负责转发 TLR 以及中国大陆各科研教育机构 IDP(Identity Provider)/SP(Service Provider)之间的认证请求。

本文中所述，即为构建校园级的二级 eduroam 网络，通常部署于研究所或大学校园里，即支持 IDP/SP 级别的 RADIUS 服务器，完成终端的 eduroam IDP 认证和 SP 服务功能。每一个 eduroam IDP 负责认证该所属域的用户，通过校验本地用户的加密密钥对；而 SP 负责连接具有 RADIUS 功能的 AP 或交换机，并负责与认证访问用户所在域的 RADIUS 服务器建立加密通道，并进行实现认证，漫游上网。通常 IDP 和 SP 可部署于一台 RADIUS 服务器上。

eduroam 网络采用 RADIUS/TLS 协议，用户账号使用类似于”user@realm”的格式，其中 realm 通常指用户所在机构的 dns 域，后缀需符合该机构所在地域的域名标识（例如使用 user@example.cn 的账号才能完成到.cn 的 FLR 的认证路由）。

为了实现 RADIUS 间安全的用户信息认证，AP 或交换机需要使用 IEEE 802.1X 的协议（SP 端），支持 EAP 协议（Extensible Authentication Protocol ）。作为 IDP

端，可使用多种方式的 EAP 方法。通常在 eduroam 中采用的方法有：

- PEAP ("Protected EAP")
- TTLS ("Tunneled TLS")
- TLS ("Transport Layer Security")
- FAST ("Flexible Authentication via Secure Tunneling")

2. RADIUS 服务器安装和 SP 配置

1）下载软件：http://freeradius.org/download.html

2）安装软件，命令如下：

```
./configure
make
make check
make install
```

3）配置 clients.conf 文件(通常在/usr/local/etc/raddb 目录)，添加 FLR 服务器：

```
client cstnet-flr-1 {
        ipaddr          = 159.226.11.46
        netmask         = 32
        secret          = YOUR_SECRET
        shortname       = cstnet-flr-1
}
#注：此处 secret 字段需要和 FLR 服务器配置文件中的相关字段匹配，
#在申请通过后会有审批方发给 KEY。
#大学用户（即用户后缀为 edu.cn），请将 cstnet-flr-1 替换为 ilr.edu.cn
#IP 地址由 159.226.11.46 更改为 162.105.129.2 或 162.105.129.2
```

4）配置 clients.conf 文件，添加无线控制器：

```
client AC1 {
        ipaddr              = ADDRESS_OF_AP_OR_SWITCH
        netmask             = 32
        secret              = YOUR_SECRET
        shortname           = AC1
}
#注：此处 secret 字段需要和无线控制器配置中的相关字段匹配，
#ipaddr 为无线控制器的 IP 地址
```

5）配置转发策略

配置 proxy.conf 文件，添加认证转发策略。以 cstnet.cn IDP 服务器为例，后缀为 cstnet.cn 和不带后缀的用户名在本地认证，具体配置如下：

```
realm realm.cn {
}
realm NULL {
}
realm LOCAL {
}
```

除后缀为 realm.cn(本单位用户)和不带@后缀的用户名外，其他认证请求转发至 159.226.11.46（如果本单位为大学用户，即用户后缀为 edu.cn，请指向到 162.105.129.2 或 162.105.129.2）。

```
home_server cstnet-flr-1 {
        type            = auth+acct
        ipaddr          = 159.226.11.46
        port            = 1812
        proto           = udp
        secret          = QYa9ga0pFldNaoF9RKWy1KYZ2i5LD2E
        status_check    = status-server
}
home_server_pool EDUROAM {
        type            = fail-over
        home_server     = cstnet-flr-1
}
realm DEFAULT {
        pool            = EDUROAM
        nostrip
}
#在这个配置案例中 Realm DEFAULT 是配置上行的路由转发规则。
#大学用户（即用户后缀为 edu.cn），请将 cstnet-flr-1 替换为 ilr.edu.cn
#IP 地址由 159.226.11.46 更改为 162.105.129.2 或 162.105.129.2
```

6）配置 CA。这里使用了 CNNIC 的快捷证书作为 EAP 的服务器证书，主要是在 eap.conf 下的 tls 标签内增加以下的配置：

```
certdir = ${confdir}/certs/er.cstnet.cn
cadir = ${confdir}/certs/er.cstnet.cn
private_key_password = PASSWORD
private_key_file = ${certdir}/er.cstnet.cn.key
certificate_file = ${certdir}/er.cstnet.cn.pem
CA_file = ${cadir}/quick.pem
CA_file = ${cadir}/cnnicroot.pem
```

3. eduroam IDP 设置

通常来讲，每一个 IDP 部署的 RADIUS 服务器，都会指向到本地已有的用户认证数据库，上层的 eduroam 路由会通过用户的格式（例如 user@realm）路由

到用户所在的 RADIUS IDP 认证服务器，完成整个认证过程。

RADIUS 服务器上的 IDP 认证，可以采用本地配置文件方式，可以通过连接数据库方式，也可以通过使用用户认证 LDAP 方式。下面以 LDAP 配置为例。

LDAP 的配置主要集中在/usr/local/etc/modules/ldap.conf 文件中。

```
server = "ldap.passport.escience.cn"
identity = "DC=eduroam,DC=passport,DC=cstnet"
password = PASSWORD_FOR_LDAP
basedn = "DC=eduroam,DC=passport,DC=cstnet"
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
```

需要修改的地方是注意 filter 配置，这个是用来查询用户使用的。为了能够支持 WPA2 协议，LDAP 中需要用 ntPassword 字段存储用户的使用 NTHash 后的密码。如有需要检查 ldap.attrmap 文件，确保下面这行配置在配置文件中。

```
checkItem       NT-Password                     ntPassword
```