eduroam 服务配置、调试及故障排查方法

2017 年 5 月

一、eduroam 服务配置、调试

请按照如下顺序完成 eduroam 的配置和调试：

1. 配置 SSID“eduroam”，支持 802.1x 认证：

a) 在无线控制器上添加名称为“eduroam”的 SSID，并采用 WPA2-enterprise（即 802.1X）加密方式；

b) 安装配置radius 服务，配置无线控制器使用radius 服务器进行认证。

2. eduroam 基本功能——本校认证测试：

本校校园中，使用移动终端，选择 eduroam 无线网，输入本校账号用户名和密码（格式为“localid@本校域名”，如 00000@pku.edu.cn）。可以正常接入 eduroam，则为测试成功。该步骤主要是为了测试无线控制器、radius 服务器及 LDAP 之间是否能够正确配合工作。

3. 访客来访功能测试：

本校校园中，测试外校账号在本校能否正常关联到 eduroam 并通过认证。使用移动终端，选择 eduroam 无线网，输入北大测试账号（请登陆 eduroam@CERNET 主页 http://www.eduroam.edu.cn 获取测试账号）。可以正常接入 eduroam，则为测试成功。该步骤主要测试访客来访功能和本校的 eduroam SP 服务是否正常。

4. 本校出访功能测试：

在 eduroam 测试网站 https://radius.ics.muni.cz/eduroam-test/eduroam-test.cgi 上测试本校账号是否正常。该步骤主要测试本校的 eduroam IdP 服务是否正常。

上述 2、3、4 三步都通过测试，即表示 eduroam 调试顺利完成，完成调试后请将调试信息反馈至 eduroam@pku.edu.cn 。收到邮件后，我们会及时在 www.eduroam.edu.cn 上更新您的 eduroam 成员状态。

二、故障排查

1. 本校认证异常

当本地账号无法通过eduroam认证时，以freeradius为例，按如下顺序排查：

a) 使用 radiusd -X 命令，以 debug 模式启动 radius 服务，检查 radius 服务器是否能够收到无线控制器发来的认证请求；

b) 检查 debug 模式下 radius 服务器的输出日志，查看 radius 是否能够正确查询 LDAP 或其他用户身份数据库。

2. 访客来访——SP 服务异常

当 SP 服务不可用时，请按如下顺序排查：

a) traceroute 162.105.129.2 或 162.105.129.5，检查 radius 服务器能否访问到教育网根节点服务器，若能 trace 至 162.105.252.x 即表明根节点服务器可达；

b) 使用 radiusd -X 命令，以 debug 模式启动 radius 服务，检查 radius 服务器是否将用户的认证请求转发至教育网根节点服务器；

c) 若认证请求已转发，检查出口设备是否允许内网的 radius 服务器直接与 162.105.129.2 及 162.105.129.5 通讯。

3. 本校出访——IdP 服务异常

当 IdP 服务不可用时，请按如下顺序排查：

检查服务器能否收到教育网根节点服务器 162.105.129.2 或 162.105.129.5 发送来的 Status-server 报文。若无法收到，请检查校园网出口设备是否已经开放 radius 认证所需的 udp 1812 端口以及是否允许外网地址直接访问该端口。

当 raidus 服务器使用私有地址并通过 NAT 与外网通信时，为保证服务器从外网可达，请务必使用静态 NAT。若位于内网的 radius 服务器无法收到 Status-server 报文，请在 NAT 设备上查看 session 会话，确保 NAT 设备能够正常收到 Status-server 报文后，进一步检查 NAT 配置。