北京大学
PEKING UNIVERSITY

基于EDUROAM的漫游用户管理

北京大学计算中心 付中南

2015/11/26

北京大学
PEKING UNIVERSITY

内容目录

一．eduroam简介与现状

二．基于eduroam的无线漫游用户管理

三．eduroam在北京大学

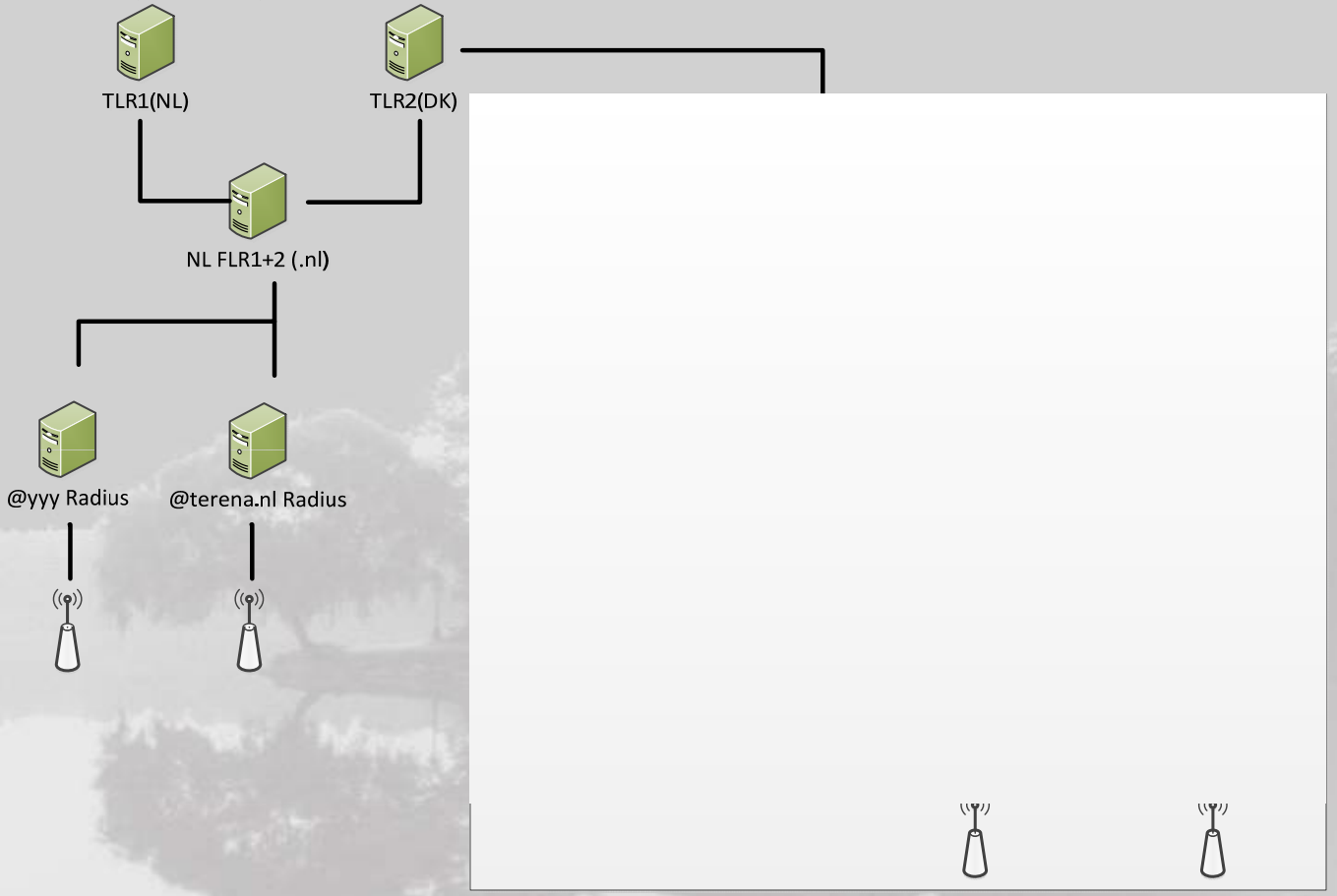
eduroam简介与现状

eduroam简介

- eduroam，education roaming的缩写
- 2003年起源于欧洲
- 一种安全的全球无线漫游服务，为各个国家的教育科研网NREN（National Research & Education Network）广泛采用
- 免费使用

eduroam简介与现状

eduroam简介



eduroam简介与现状

eduroam简介

- eduroam认证服务器，包括顶级服务器（TLR）、联盟级服务器（FLR）、区域级服务器（ILR）等
- eduroam运营者，包括服务提供者（SP）和身份提供者（IdP）
- eduroam用户身份，指用户接入eduroam时使用的ID，格式为XXX@Realm

eduroam简介与现状

eduroam现状

- 截止2015年，eduroam已覆盖74个国家和地区
- 中国大陆地区于2014年11月正式加入eduroam，由中国科学院网络中心负责联盟级认证服务器的建设及维护
- 中国教育网于2015年4月加入eduroam，由北京大学负责教育网内区域级认证服务器的建设与维护

北京大学
PEKING UNIVERSITY

内容目录

一．eduroam简介与现状

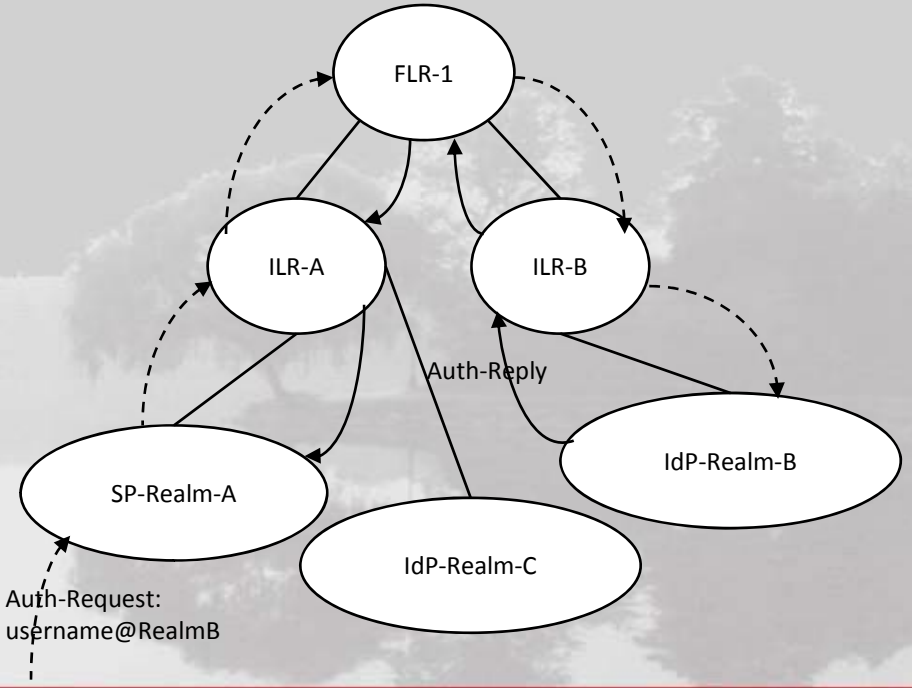
二．基于eduroam的漫游管理

三．eduroam在北京大学

基于eduroam的漫游管理

eduroam的技术原理

- eduroam的核心技术是通过radius的proxy认证将用户在漫游状态下的认证请求转发至用户身份所在地完成认证



基于eduroam的漫游管理

eduroam的技术原理

- 为了实现上述的proxy，每一级认证服务器都必须维护一张认证转发表

域名	转发目的
local	Local-IdP IPAddress
Realm1	Realm-1-IdP IPAddress
Realm2	Realm-2-IdP IPAddress
Default（可选）	ILR/FLR/TLR IPAddress

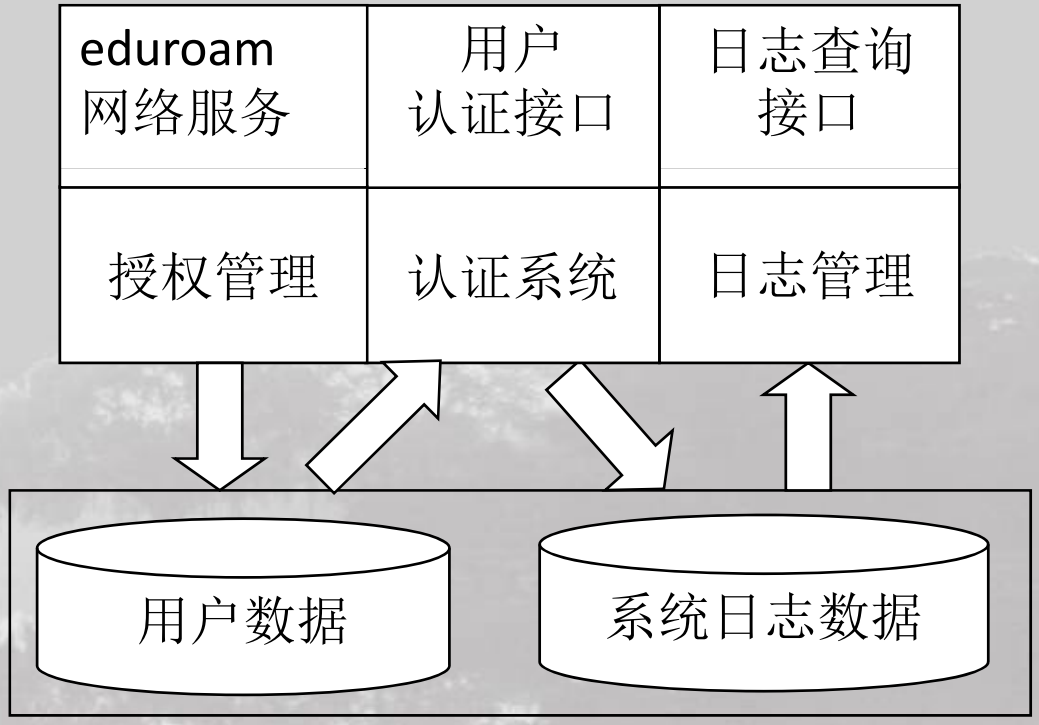
基于eduroam的漫游管理

eduroam存在的问题

- 对用户缺乏有效的监管和控制

基于eduroam的漫游管理

基于eduroam的漫游用户管理系统



基于eduroam的漫游管理

基于eduroam的漫游用户管理系统

- 用户授权管理子系统
  - 原则上，eduroam架构允许已加入eduroam组织的大学/科研单位的用户免费使用全球范围内任何可搜索到的eduroam无线网。
  - 实际应用中，校园网管理人员需要根据自己校园网的实际情况对能够在本机构内使用eduroam网络的用户进行控制。
  - 用户授权管理子系统可以根据域名对用户进行批量管理，也可以根据用户ID对单个用户进行管理。

基于eduroam的漫游管理

基于eduroam的漫游用户管理系统

- 用户认证子系统
  - 整个漫游系统的核心部分。
  - 用户认证子系统在开始用户认证之前，首先检查用户身份数据，判断该用户是否已具备合法身份。
  - 如果是，则根据用户认证请求中的域名信息，将用户的认证请求转发到相应的认证服务器。
  - 反之，则直接拒绝该认证请求。

基于eduroam的漫游管理

基于eduroam的漫游用户管理系统

- 日志管理子系统
  - 日志管理子系统主要负责eduroam系统日志的收集、分析和查询等任务。
  - 系统日志由两部分组成：
    - 作为SP产出的日志，记录漫游用户在本地的使用情况
    - 作为IdP产生的日志，记录本地用户在漫游状态下的认证情况

北京大学
PEKING UNIVERSITY

内容目录

一．eduroam简介与现状

二．基于eduroam的无线漫游用户管理

三．eduroam在北京大学

北京大学 PEKING UNIVERSITY

eudroam在北京大学

北京大学校园网概况

- 北京大学校园网始建于1989年，经过二十五年的高速发展，已成为国内高校规模最大的校园网络之一。
- 目前，北京大学校园网已经在全部教学区和公共区域、部分办公区楼宇和部分学生宿舍区实现了有线及无线网络大规模覆盖。
- 漫游用户主要在教学区域和公共区域使用无线网络。因此，北京大学首先在教学区域和公共区域部署eduroam无线网。

eudroam在北京大学

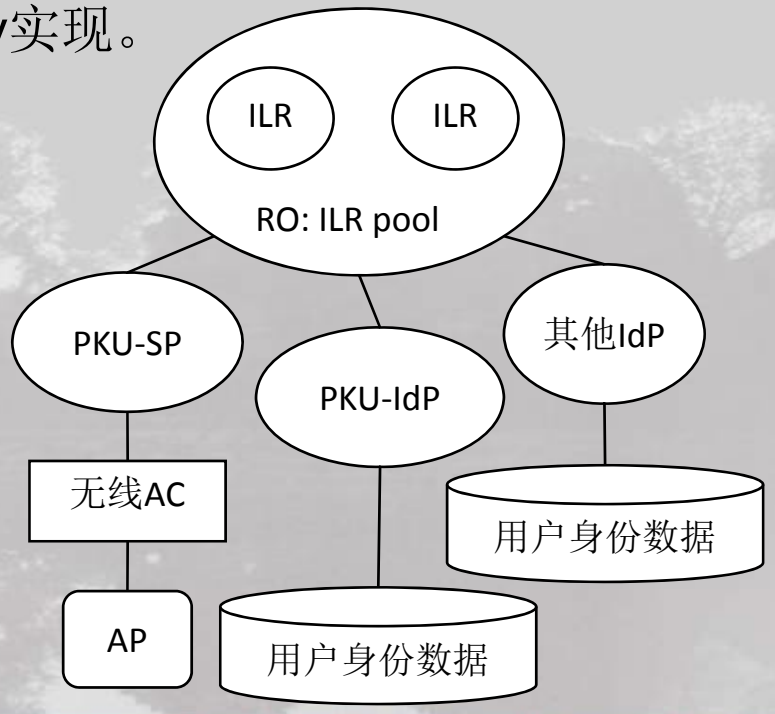
漫游用户管理

- 漫游用户管理确保了机构的漫游网络管理权及用户访问控制。
- 通常情况下，提交了真实有效身份的漫游用户都可以访问漫游网络。
- 北京大学网络用户必须先在网络服务门户中申请开通eduroam后才能获得合法eduroam身份ID
- 漫游用户在北京大学校内必须提交个人真实信息，否则无法接入eduroam。

eudroam在北京大学

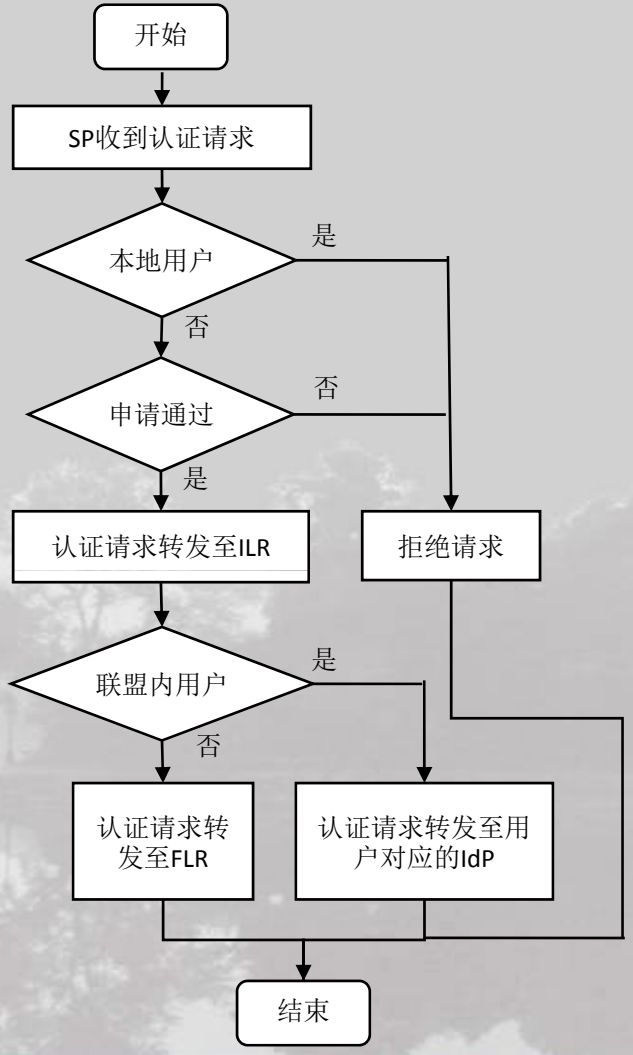
漫游用户认证

- 北京大学除了在本校提供eduroam服务外，还是中国教育科研网的根节点，在整个eduroam体系中共扮演了ILR、SP和IdP三个角色。
- SP与IdP使用freeradius实现，ILR只负责认证转发而不直接对用户提供服务，故使用radsecproxy实现。



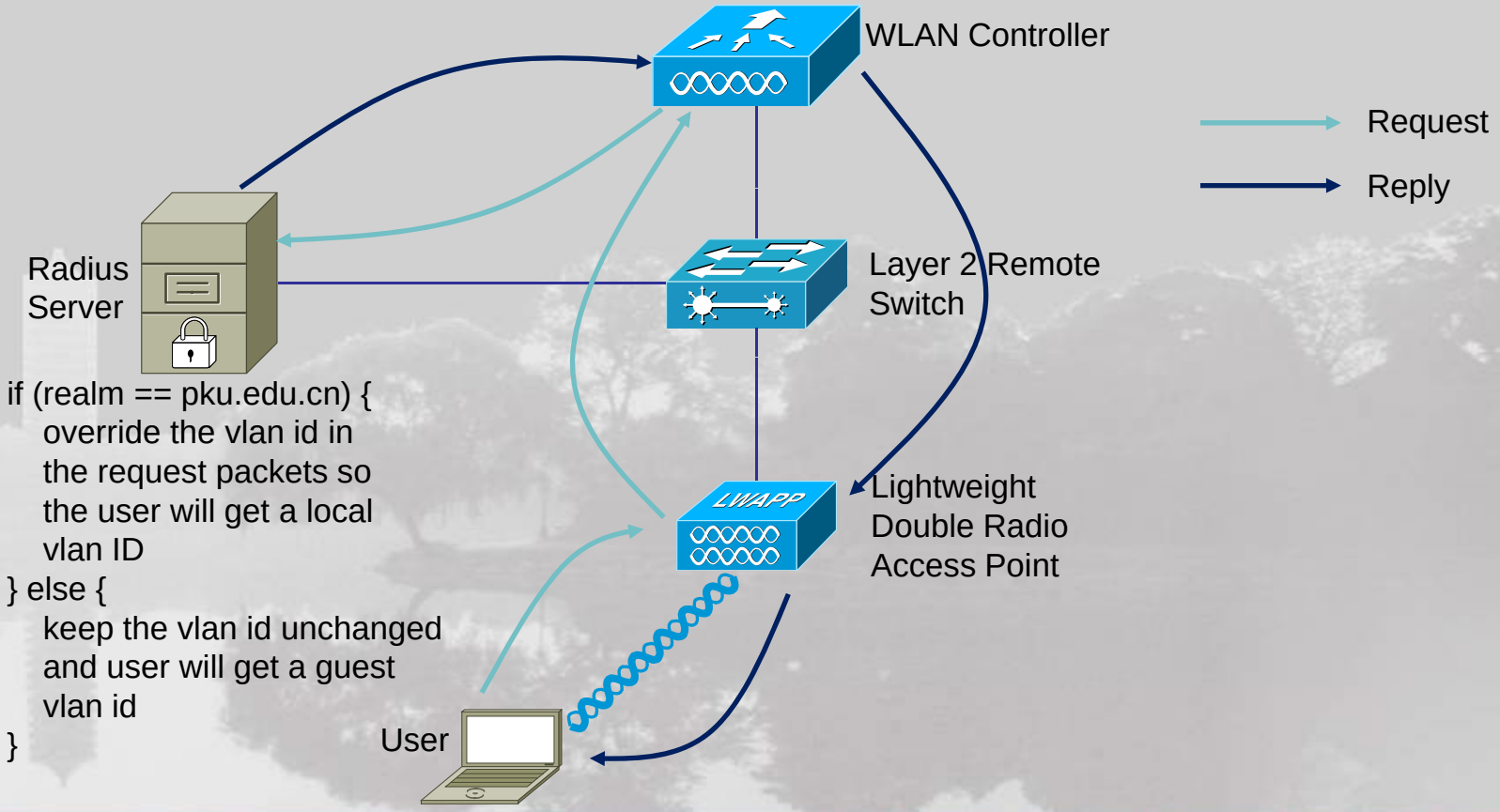
eudroam在北京大学

漫游用户认证



eudroam在北京大学

向本地用户提供测试服务



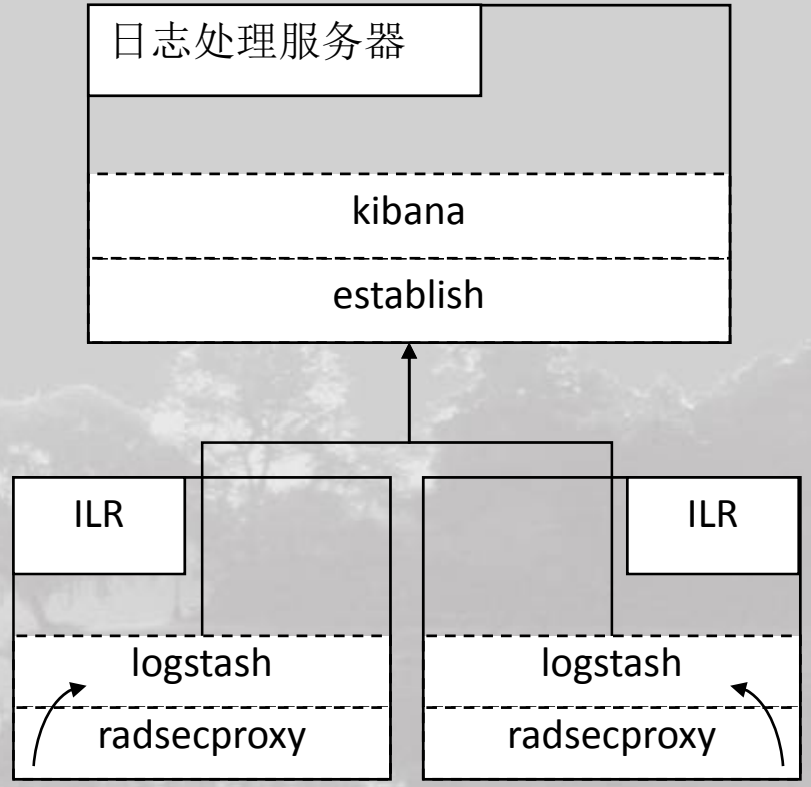
eudroam在北京大学

系统日志存储和管理

- 日志处理采用了logstash+establish+kibana的组合。
- logstash负责从ILR产生的日志中提取我们需要的内容后上传到establish，kibana从establish中读取数据形成日志查询界面。

eudroam在北京大学

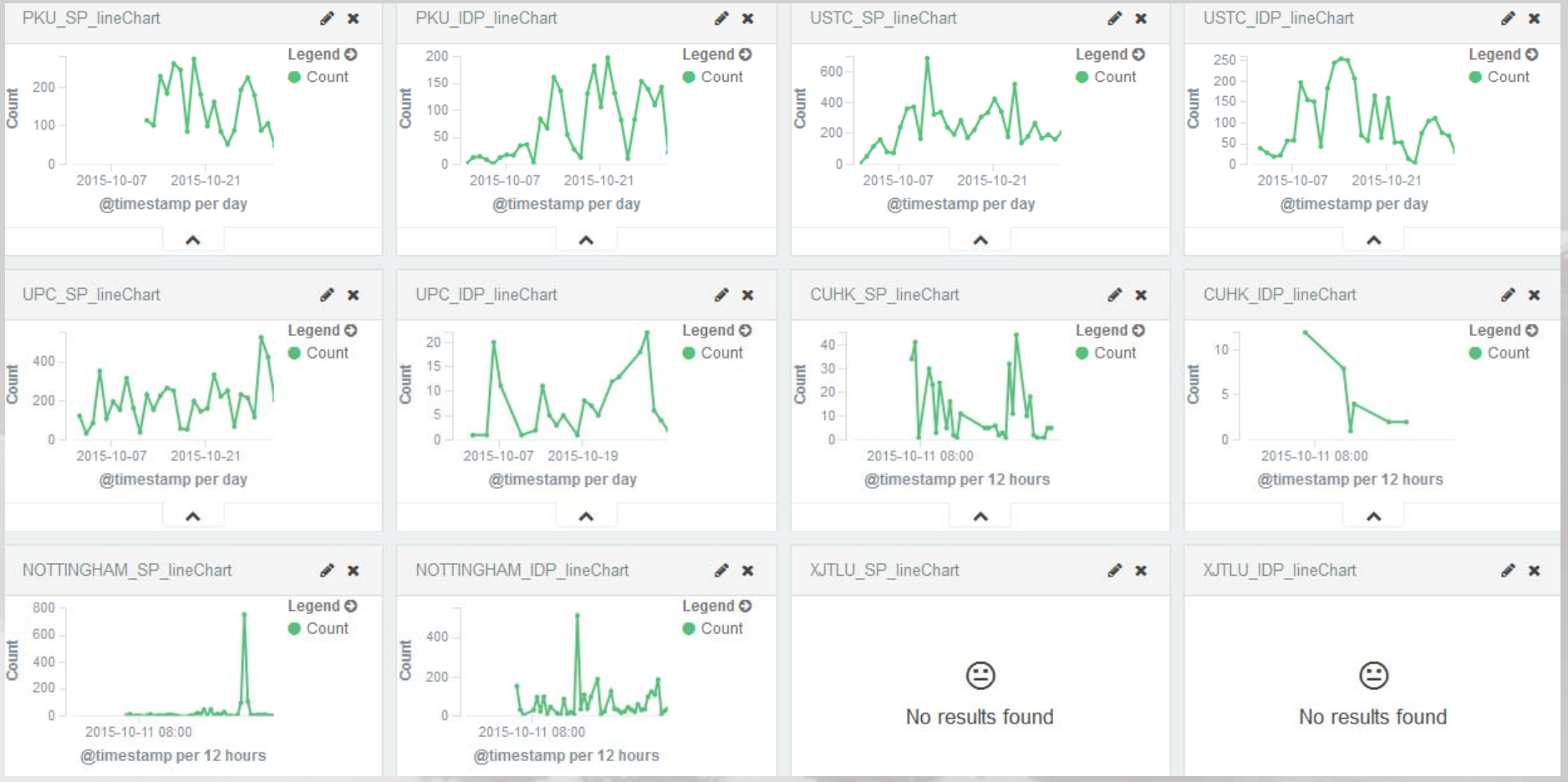
系统日志存储和管理



北京大学
PEKING UNIVERSITY

eudroam在北京大学

系统日志存储和管理



北京大学
PEKING UNIVERSITY

谢谢！