CERNET学术年会

IPv6 技术的应用创新与校园实践

张栋

福州大学计算机与大数据学院

（zhangdong@fzu.edu.cn）

目录

2.1.1 背景

未知威胁
隐蔽

校园网安全挑战愈发严峻！

安全问题
交织

“近日，安恒信息MSS安全托管运营团队监测到国内**多家高校DNS服务器**遭受攻击。安恒信息MSS团队第一时间对攻击情况进行了通告，针对多个受害用户开展应急响应工作，并协助用户恢复网络。”

“近日陆续有**大量高校自建DNS服务器遭受DDoS攻击**，互联网域名系统国家研究中心（ZDNS）监控到攻击事件后，第一时间对攻击情况与处置建议进行了通告，同时迅速开展应急响应协助用户恢复业务。”

网络安全问题

功能安全问题

数据安全问题

1 背景 —— 校园网DNS攻击案例

常见攻击特征

伪造成同网段的
随机IP地址

攻击包源IP

每秒收到数千个
攻击查询请求

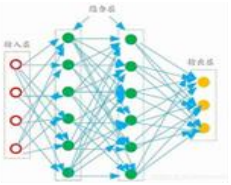
攻击流量

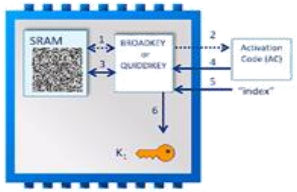
新增NS类型域名
的DGA子域名

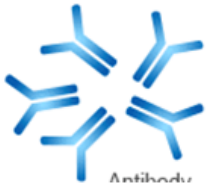
攻击域名

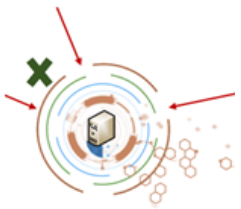
1 背景—— 校园网当今主要威胁

安全问题	主要威胁
1 **网络** 安全问题 漏洞利用威胁、帐号身份验证 恶意软件传播、社会网络钓鱼	网络入侵 DDoS攻击 恶意软件
2 **功能** 安全问题 未经授权访问、数据保护不足 数据保护不足、数据保护不足	身份验证漏洞 访问控制不当 不安全的应用程序
3 **数据** 安全问题 数据泄露风险、用户安全意识 数据篡改威胁、访问控制挑战	数据泄漏 数据篡改 数据备份和恢复









1 背景——校园网威胁现有解决方案

安全问题

1 网络 安全问题

漏洞利用威胁、帐号身份验证
恶意软件传播、社会网络钓鱼

2 功能 安全问题

后门攻击泛滥、未知漏洞潜伏
结构安全缺失、传统防御被动

3 数据 安全问题

数据泄露风险、用户安全意识
数据篡改威胁、访问控制挑战

解决方案

网络隔离
加密保护
安全监控

漏洞扫描
应用审计
身份认证

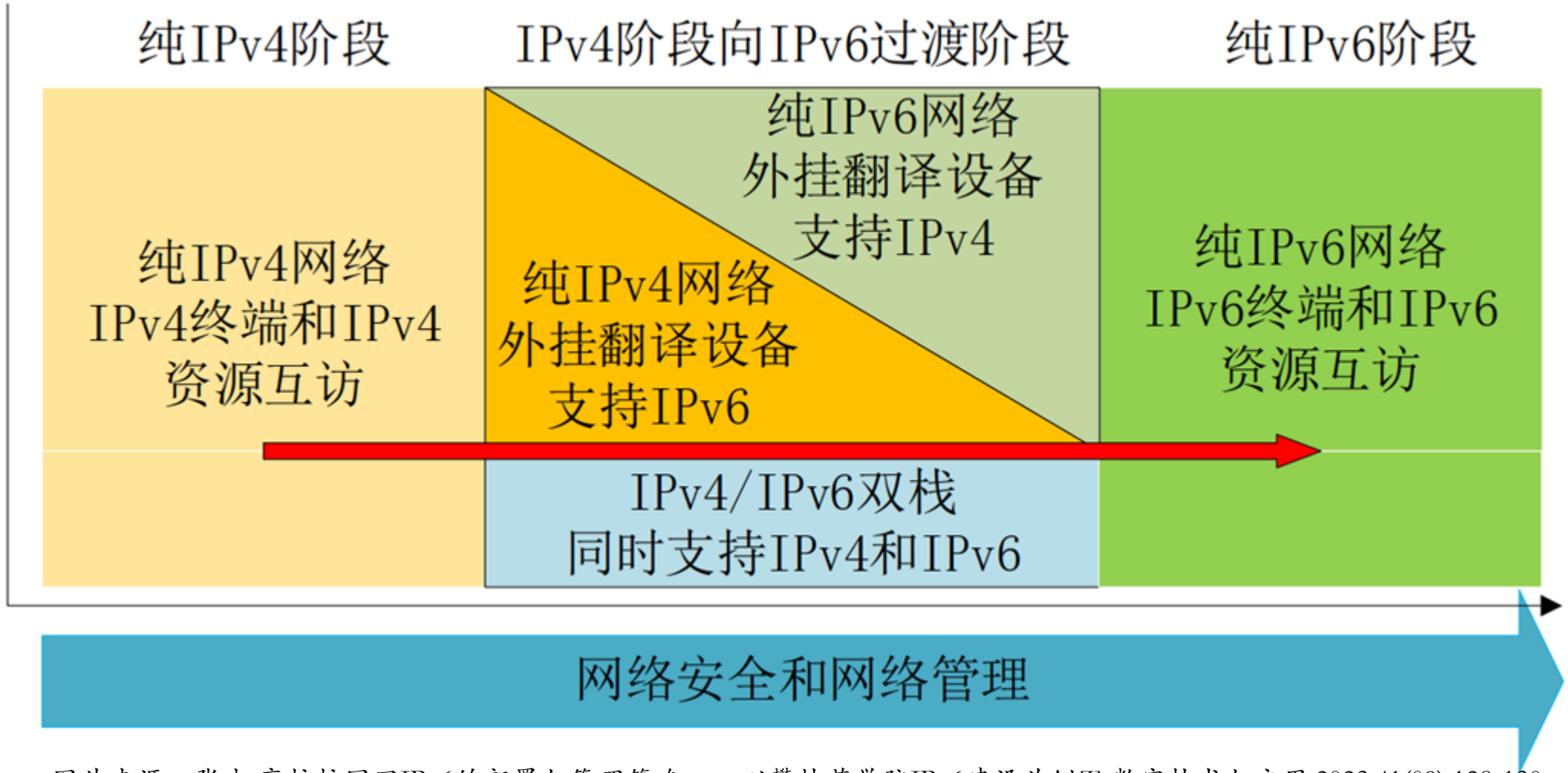
数据加密
数据备份
隐私保护

攻击方式多样

防御方式孤立

1 背景 —— IPv6发展阶段

➢ **现状：IPv4和IPv6长期共存，逐步发展，最终实现升级换代**



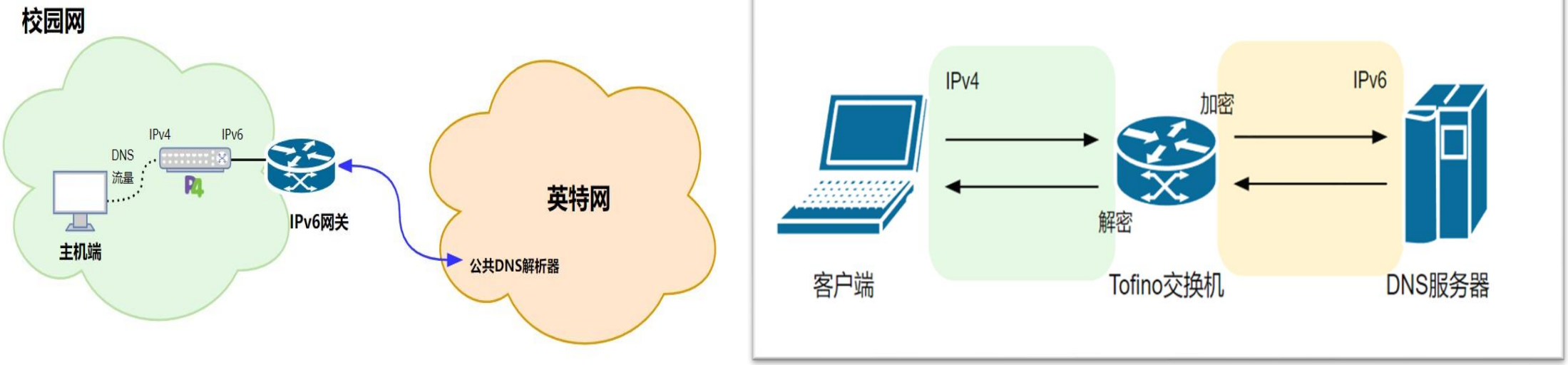
图片来源：张杰.高校校园网IPv6的部署与管理策略——以攀枝花学院IPv6建设为例[J].数字技术与应用,2023,41(09):128-130.

2 IPv6创新应用

基于网内计算(In-Network Computing)技术的IPv6应用创新实践探索

2.1 网内DNS加解密原型系统

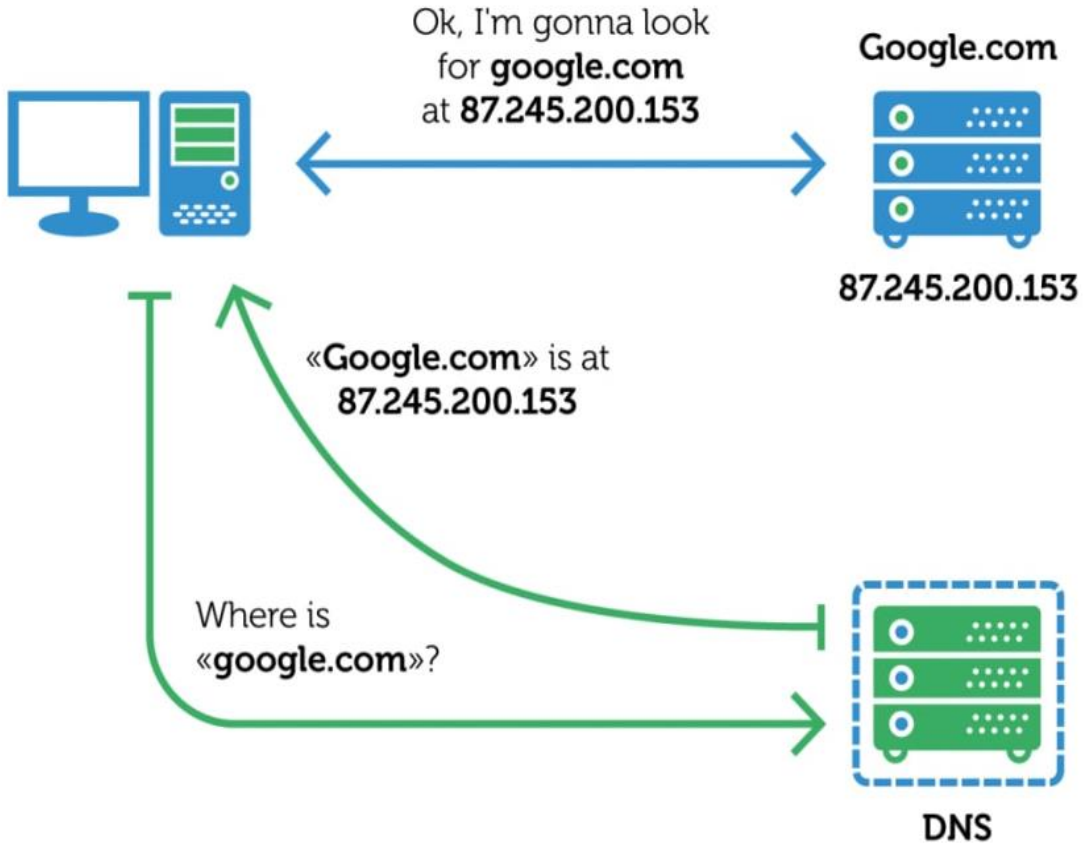
面向DNS安全，探索利用**IPv6**和**可编程交换设备**实现对用户和服务**透明的加密DNS**查询响应

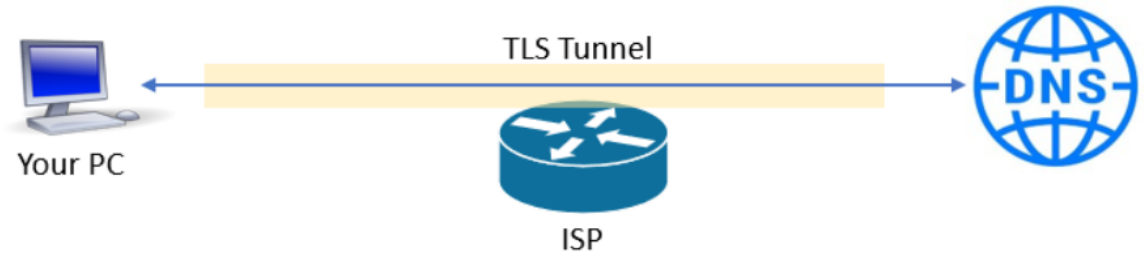


2.1.1 现状

现有DNS安全机制仍存在隐私泄露的风险

- DNS（域名系统）通常使用的加密方式是DNS over TLS（DoT）和DNS over HTTPS（DoH），可以在链路上加密DNS请求，但是在DNS服务器端，隐私仍然可能被泄露。





2.1.2 设计

目标 1 保障数据安全

利用在网计算实现DNS协议流量加解密，防止用户的隐私泄露

挑战 1

加解密的具体技术方案如何选择?

目标 2 兼容并可拓展

实现DNS流量加解密的同时，不需要改动现有客户端和服务器

挑战 2

如何实现加解密对客户端和DNS服务端无感?

目标 3 保障网络安全

能够有效阻止类似近期校园DNS攻击事件的发生

挑战 3

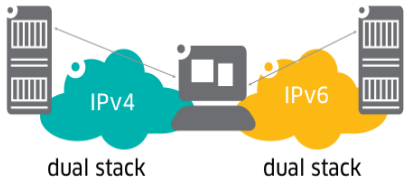
如何在加密时还可防止发送者伪造IP发起攻击?

2.1.2 设计

网内DNS加解密原型系统

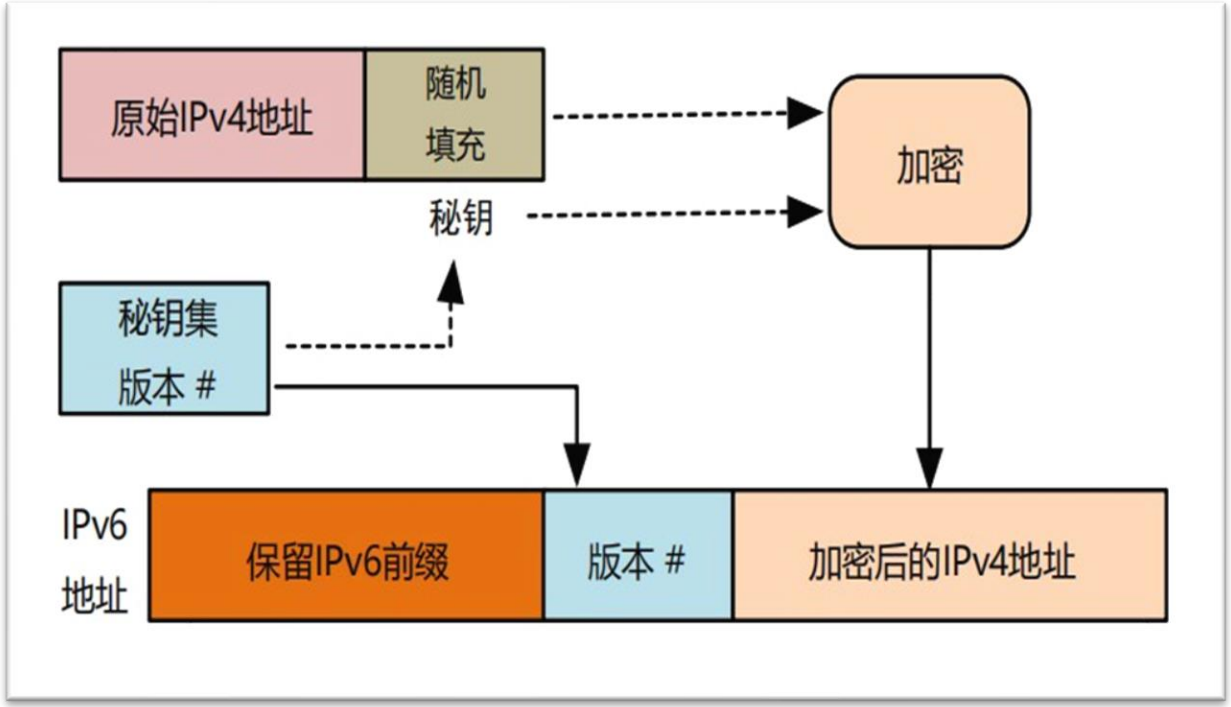
IPv4/IPv6双栈

- 将IPv4的DNS请求变换为IPv6的DNS请求
- 充分利用IPv6的128位字段



在可编程交换机之上实现流量加解密

- 异或操作
- 控制面下发多套密钥
- 随即填充



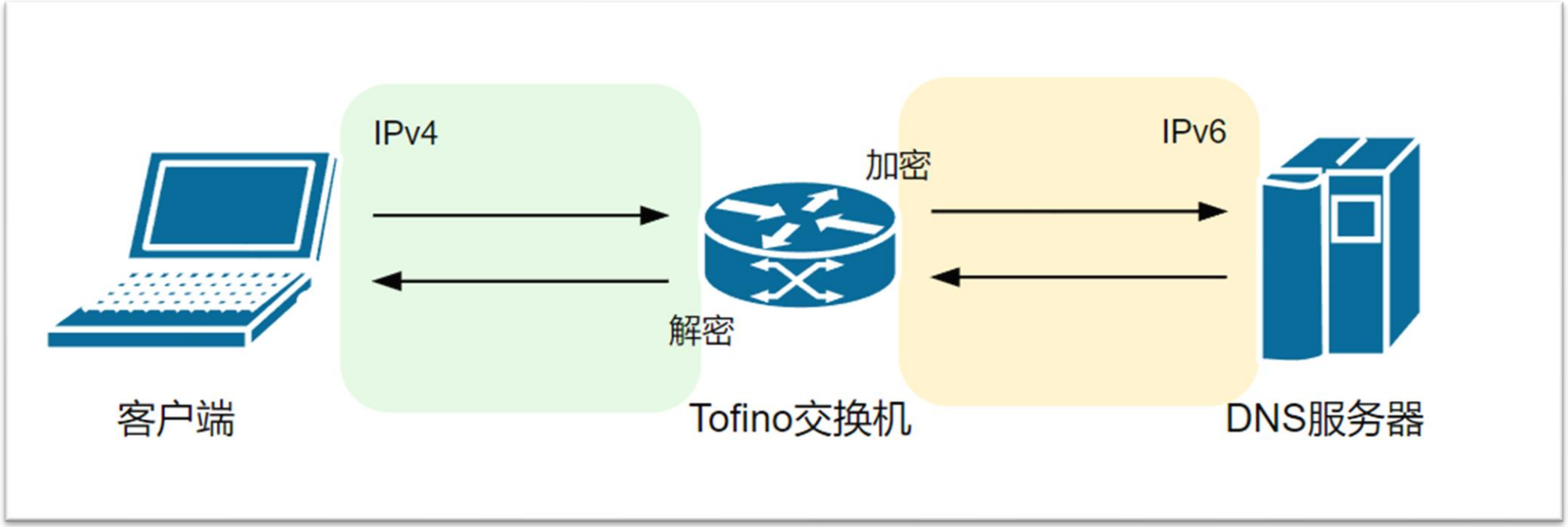
创新

查询加密	地址隐藏	系统透明	开销低
可以提供更好的DNS隐私	隐藏真实地址，有效抵御攻击	DNS客户端和服务器对加解密无感	交换机做代理实现低开销

2.1.3 实现

网内DNS加解密原型系统

- 在Tofino可编程交换机上实现DNS加解密程序，并且将其部署在IPv4/IPv6双栈网络进行测试。



2.1.4 验证

网内DNS加解密原型系统

- Tofino可编程交换机对DNS查询和相应报文分别进行加解密，客户端可以正常得到DNS查询结果。

创新

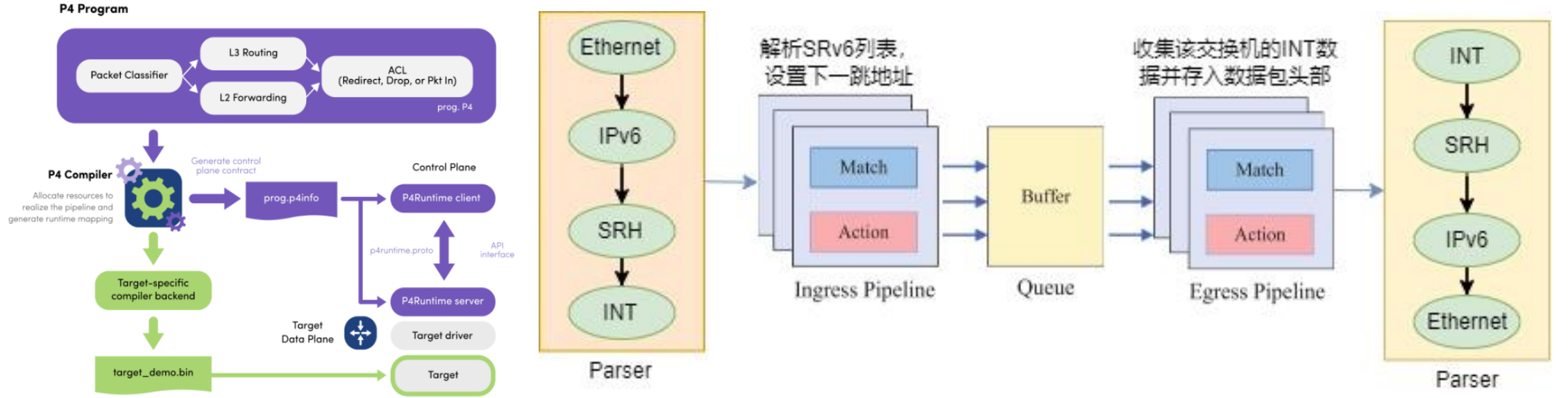
查询加密	地址隐藏
可以提供更好的DNS隐私	建立严格的访问控制机制
系统透明	**开销低**
DNS客户端和服务器对加解密无感知	降低代理开销和吞吐量

```
==========================================================================================
Custom packet sent: Source IP = 192.168.1.139 Destination IP = 37.97.199.195
Captured IPv4 packet: Source IP = 37.97.199.195, Destination IP = 192.168.1.139
==========================================================================================
Custom packet sent: Source IP = 192.168.1.139 Destination IP = 77.111.240.124
Captured IPv4 packet: Source IP = 77.111.240.124, Destination IP = 192.168.1.139
==========================================================================================
Custom packet sent: Source IP = 192.168.1.139 Destination IP = 97.74.110.52
Captured IPv4 packet: Source IP = 97.74.110.52, Destination IP = 192.168.1.139
==========================================================================================
Custom packet sent: Source IP = 192.168.1.139 Destination IP = 152.101.4.130
Captured IPv4 packet: Source IP = 152.101.4.130, Destination IP = 192.168.1.139
==========================================================================================
```

基于网内计算(In-Network Computing)技术的IPv6应用创新实践探索

2.2 SRv6+INT的网内测量原型系统

面向网络测量，获取**数据包级别、细粒度**的网络状态数据，可为网络安全分析检测服务



2.2.1 背景

IPv6校园网的过渡

- 更多的校园承载设备和用户
- 改进的路由寻址和数据包处理方式
- 基于IPv6的新技术知识

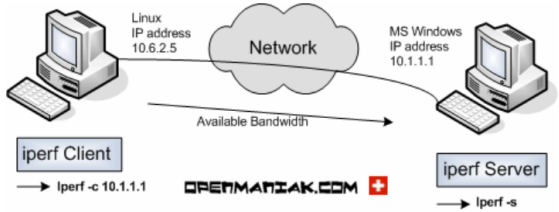
网络测量

- 时延、带宽、丢包率等网络性能监测
- 确保关键应用和服务的质量
- 安全性，异常流量、入侵检测
- 资源的合理分配

新需求：基于IPv6校园网的网络测量

2.2.2 现状

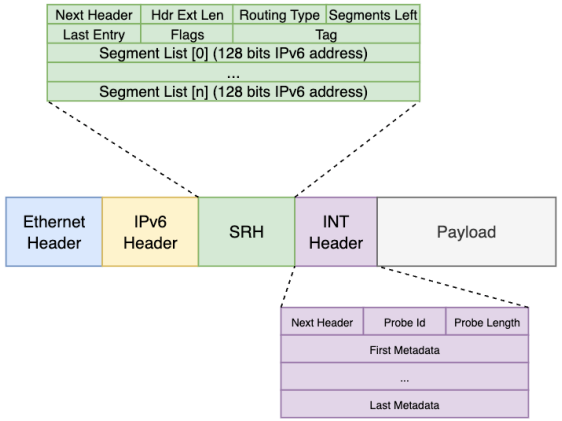
传统网络测量方案



局限：

- 局部的性能信息
- 采样点有限
- 开销大
- 配置管理复杂

基于INT网络测量方案



单独的INT还不足以对ipv6校园网进行全面的网络测量

- 数据包头部空间开销
- 传统INT只能跟随用户数据包

2.2.3 设计

目标 ① 支持双IP协议

实现IPv6和IPv4正常传输

目标 ② 缓解网络负载

轻量级头部
减少网络开销

目标 ③ 实时数据分析

实时测量与结果反馈

设计 ①

SRv6+INT 测量数据包头部
基于P4的测量数据包解析

设计 ②

逐跳减小的SRH头部处理

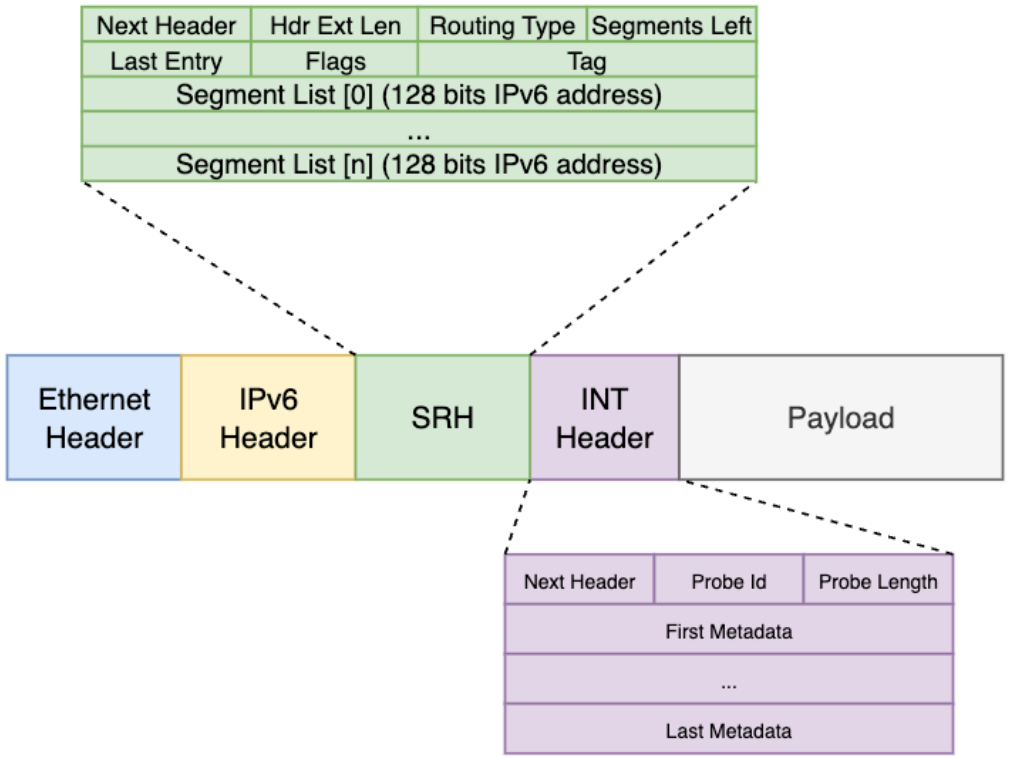
设计 ③

集成SRv6+INT
网内测量-监控系统

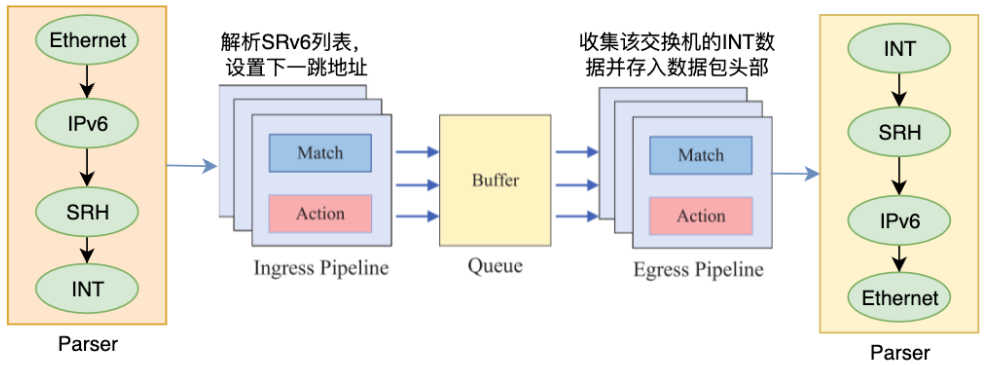
2.2.4 实现

SRv6+INT 的网内测量原型系统

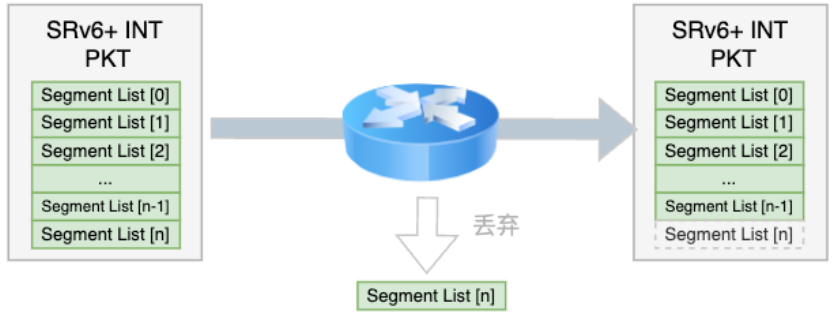
SRv6+INT 测量数据包头部



基于P4的测量数据包处理



逐跳减小的SRH头部处理



2.2.5 效果

方案 1

将IPv4地址加密成IPv6地址，DNS实际查询响应是在IPv6网络，攻击者**伪造源IP攻击失效**

保障**网络安全**

方案 2

DNS解析不受影响，保证了业务站点的**正常访问**

保障**功能安全**

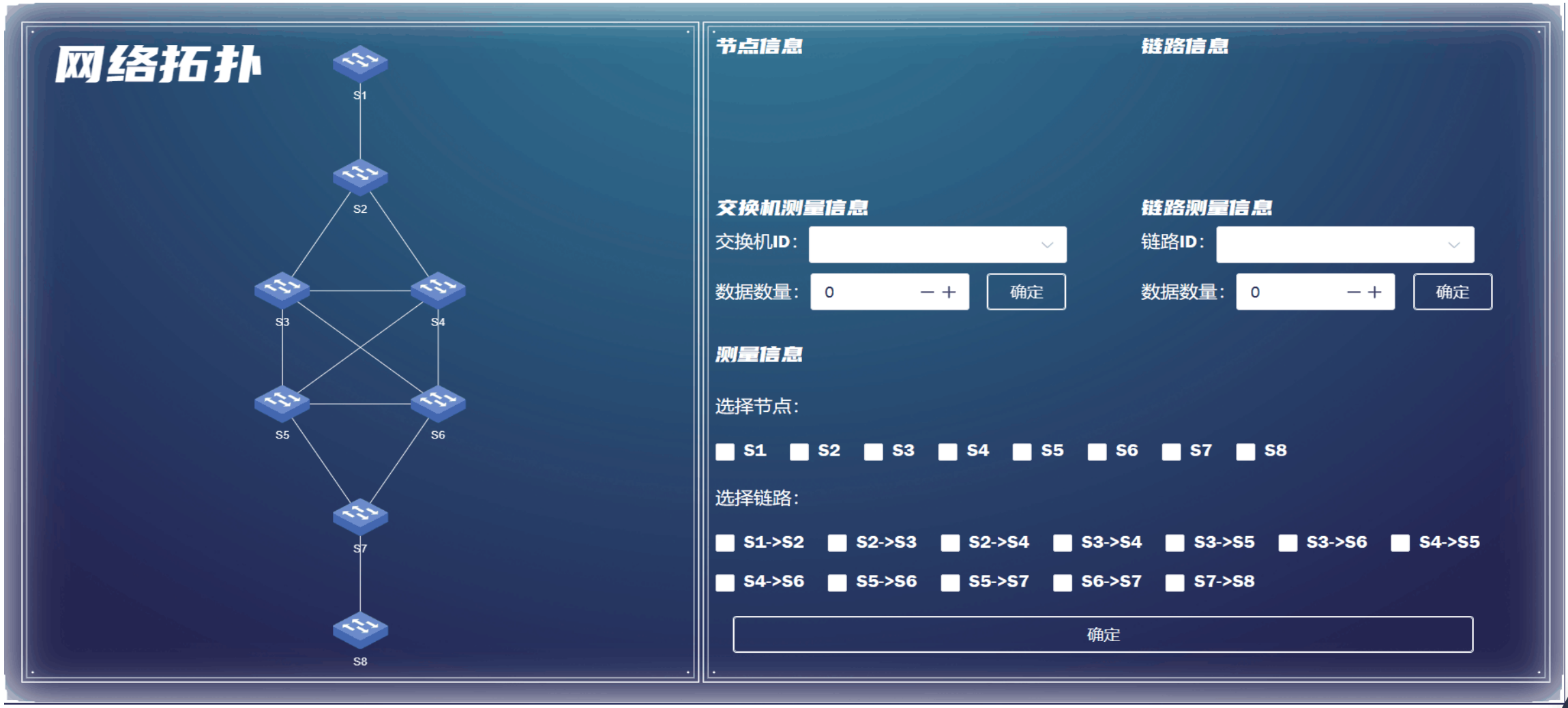
方案 3

查询者不需要了解DNS服务器的ipv6网络情况，所有**查询响应均为透明**

保障**数据安全**

2.2.5 效果

SRv6+INT 的网内测量原型系统



3 融入福大校园实践

福州大学已建立了较安全的IPv6应用环境，实现了校园网用户的IPv6普遍访问和校园网信息资源的IPv6普遍服务。

11000+
活跃用户

30000+
IPv6接入用户

>90%
IPv6/v4用户占比

174.87Mbps
入流量平均带宽

92.31Mbps
出流量平均带宽

850M
IPv6校园网进出流量

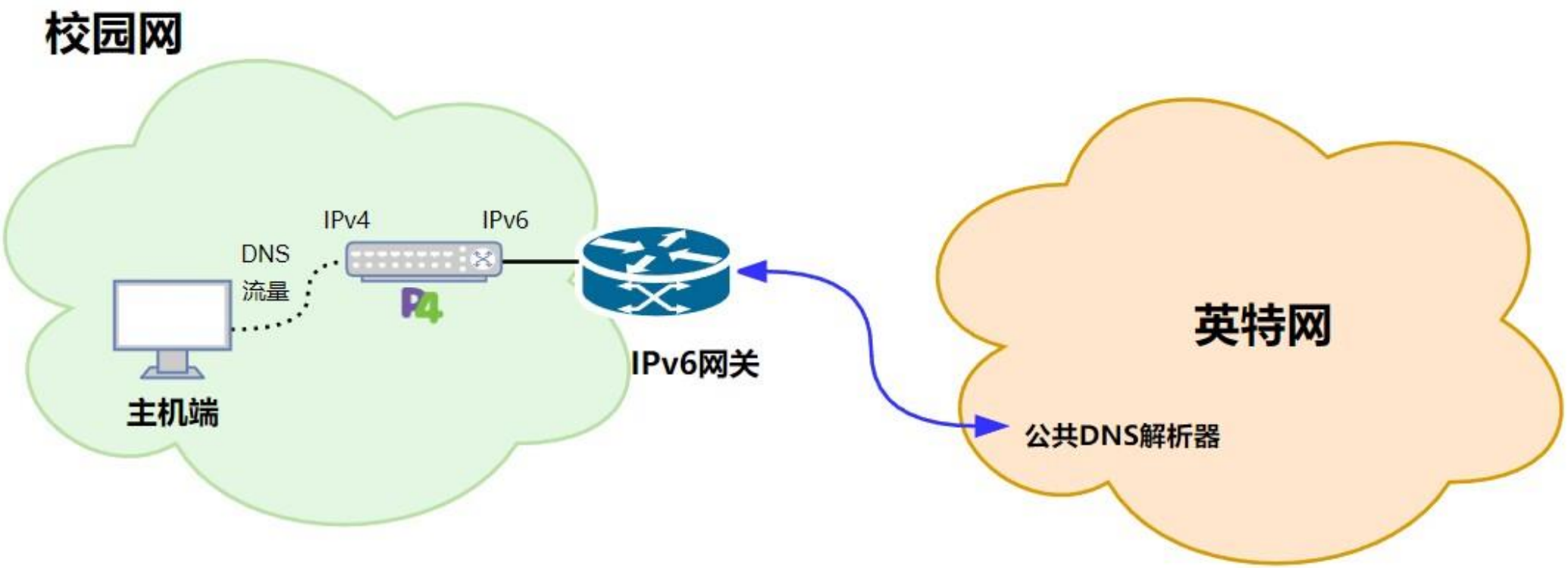
支持
校园网内教学、办公等固网终端全面支持IPv6，笔记本电脑、手机等移动网络终端基本支持IPv6

30+
单位使用本校节点IPv6接入服务

3 融入福大校园实践

网内DNS加解密原型系统在校园网的实际部署规划

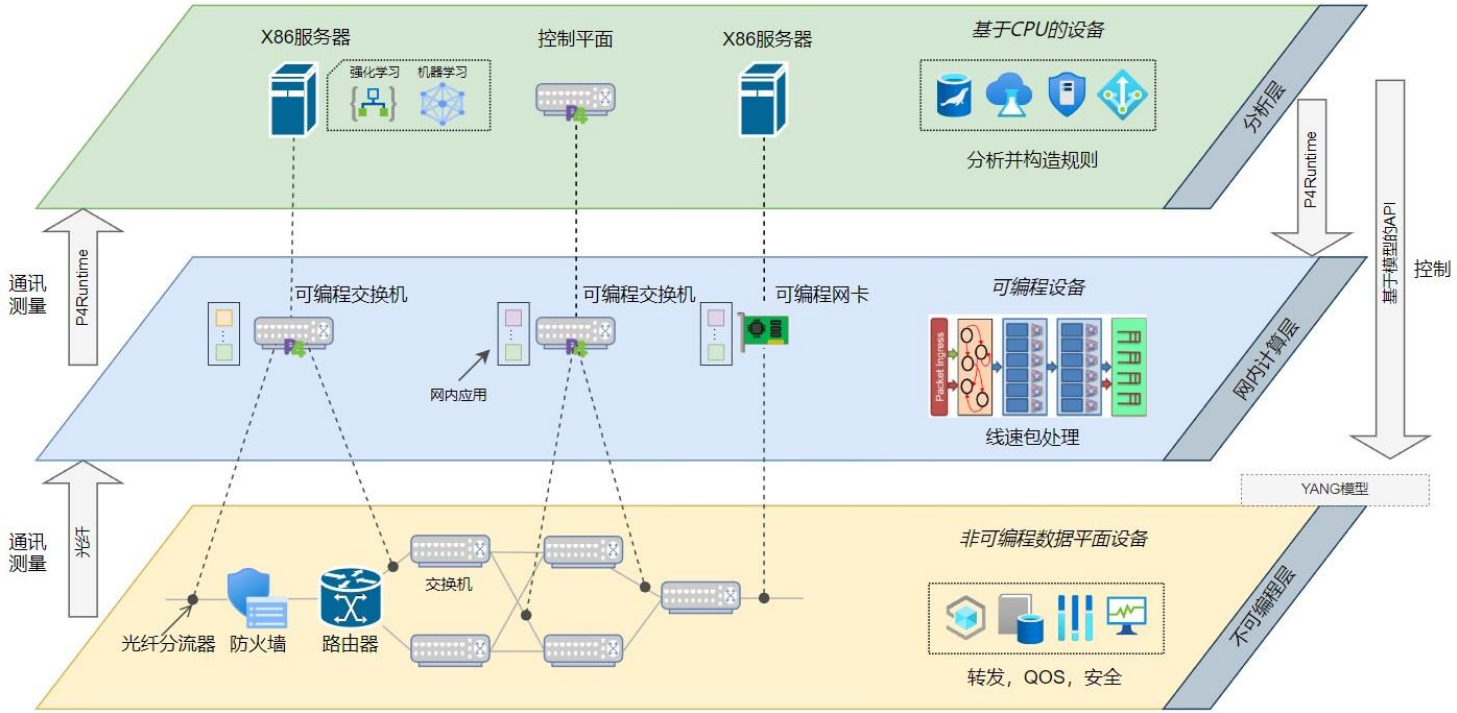
- 原型系统具备在IPv6校园网实际部署的能力



3 融入福大校园实践

网内计算设备在校园网的实际部署应用规划

- 在校园网中部署可编程交换设备，实现以线速运行定制的数据包处理功能，并以纳秒分辨率收集网络信息。



展望未来

IPv6校园网为一线教学科研赋能

高水平的研究成果离不开真实网络环境的实验数据，让校园网络为教学科研赋能，培养网络安全与信息化创新应用人才。

谢谢大家

张栋

福州大学计算机与大数据学院

（zhangdong@fzu.edu.cn）