



南昌大学

NANCHANG UNIVERSITY

AI驱动的物联网IPv6 地址 分配与访问控制

时间：2025.12 汇报人：刘承启

论文作者：刘承启，付爱英，刘继鹏，叶青，郭祥耀





目录

CONTENTS



研究背景与研究目标

Research Background and Objectives



方案设计与实施

Scheme Design and Implementation



实验

Experiment



结语

Conclusion

◎ 物联网终端大规模普及带来的挑战

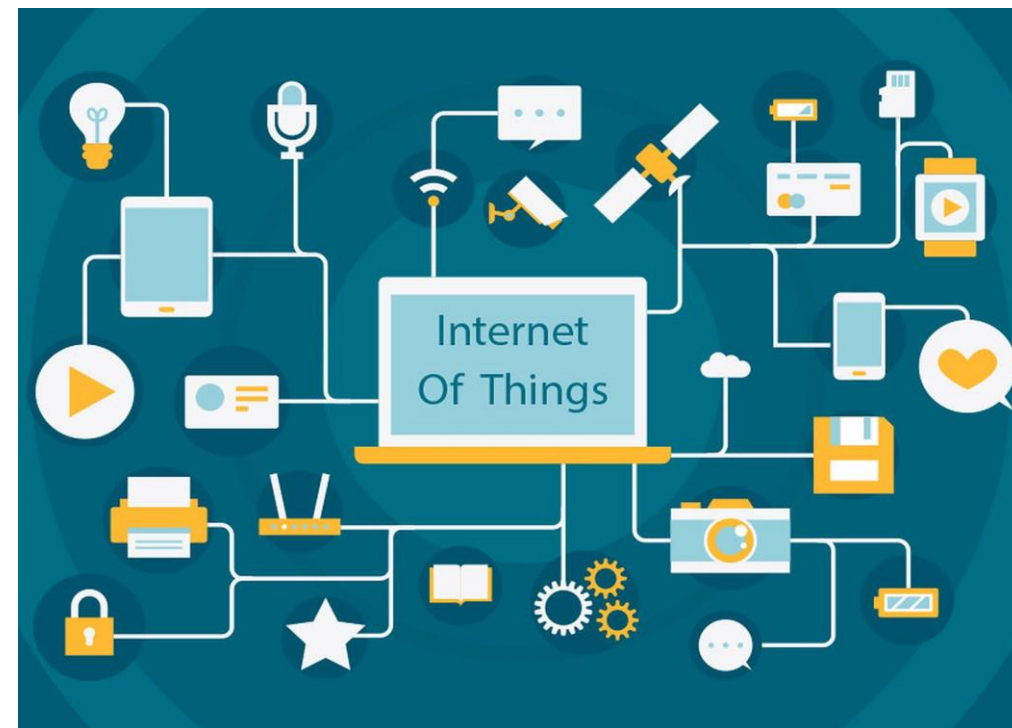
全球物联网终端数量预计在2025年突破198亿，海量终端接入带来地址管理、溯源与访问控制等严峻挑战。

◎ 物联网IPv6地址分配与访问控制的现状与挑战

在物联网领域，IPv4地址分配与安全防护机制已较为成熟，而IPv6环境下虽已涌现多种地址分配与安全方案（如SAVI、地理位置编码及身份嵌入等），但在动态授权、业务隔离以及智能策略自适应调整等方面仍有提升空间。

◎ AI技术发展为网络管理带来新机遇

AI Agent在智能运维领域展现出潜力，为IPv6地址的智能分配与访问控制动态优化提供了新的技术路径。





实现地址可溯源

通过将业务类型、位置与设备标识进行语义编码并嵌入IPv6地址，使每个地址具备业务与终端身份信息，实现精准溯源。

业务逻辑隔离

基于语义编码的IPv6地址，系统可自动识别业务类型并部署差异化的访问控制策略，实现业务间的逻辑隔离与安全域划分。

智能访问控制

利用AI Agent实时分析网络日志与威胁情报，动态生成并调整访问控制策略，实现自适应、智能化的安全防护。

整体架构



图1 系统架构图

人机交互层

提供物联网终端授权注册入口，收集业务类别、接入位置和终端标识等信息，基于语义编码与加密技术构建可溯源的IPv6地址。

智能管控层

由多个功能Agent协同工作，实时监测设备状态、聚合日志信息、动态生成安全策略，并通过执行Agent下发配置，实现自动化管控与策略调整。

支撑与执行层

包括DHCPv6服务、设备状态监控、日志审计与ACL策略引擎，为地址分配、状态采集、策略执行与溯源提供底层支撑与保障。

整体 workflow

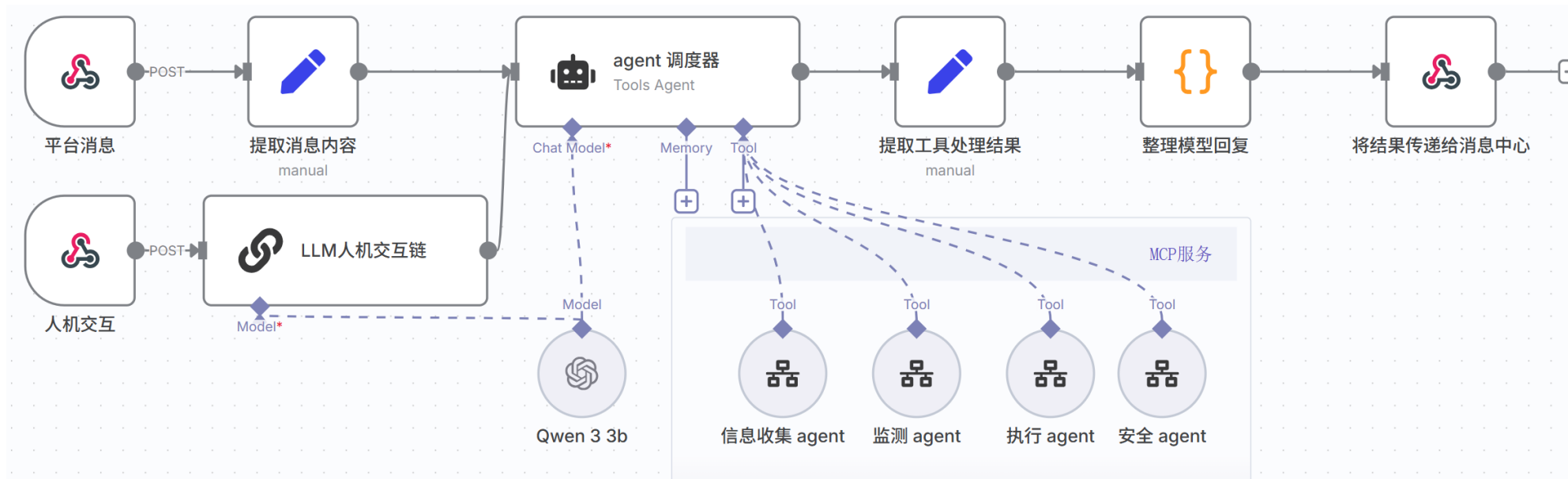


图2 整体 workflow 图

整体实施 workflow 如图所示。平台消息与人机交互作为输入入口，经参数提取与大语言模型（本文使用 Qwen3 30b）解析后，由 Agent 调度器统一协调，并调用监测、信息收集、安全与执行等 Agent，完成日志聚合、状态监测、地址绑定及访问控制策略下发。最终，结果经由 MCP 服务汇总整理并反馈至消息中心。

语义编码

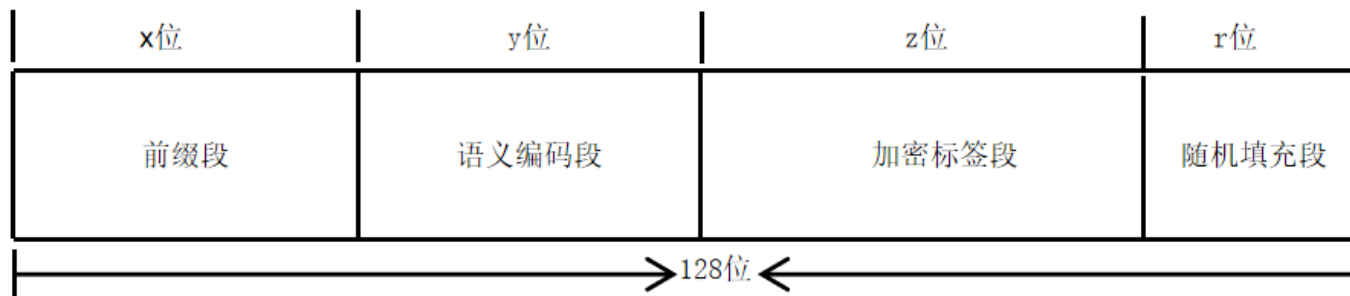


图3 基于语义编码的IPv6地址结构

可控、可溯源的IPv6地址结构如上图所示，地址组成部分依次为：CERNET分配的全球可路由的前缀段P(x)，业务类型、终端接入位置等信息组成的语义编码段E(Y)，设备标识（MAC）和部署密钥生成的加密标签段M(Z)和随机填充段R(W)。

层级化构建语义编码段，即按照“业务类型—园区—楼栋—其他”逻辑逐级映射具体定义如下：业务类型，m位，编号M；园区，t位，编号T；楼栋，b位，编号B；扩展，d位，编号D。满足， $m+t+b+d=y$ ，m，t，b，d的值可以根据自己的情况设定相应的具体值，甚至可以取值为0。



IPv6地址生成算法

IPv6地址表达式为：

$$IPv6_addr = P(x) \parallel E(y) \parallel M(z) \parallel R(w) \quad (1)$$

约束： $x+y+z+w=128$ 。为保持路由一致性，取 $x \leq |X|$ ，其中 X 为CERNET分配前缀， $|X| \in [32, 64]$

语义编码段(按高→低位)表达式为：

$$E(y) = M(m) \parallel T(t) \parallel B(b) \parallel D(d) \quad (2)$$

层级化构建IPv6地址，即按照“业务类型—园区—楼栋—其他”逻辑逐级映射。

加密标签段：

该段长度为 z 位（本文 $z=48$ ），由终端MAC地址或DUID的低48位经AES-128-FF1格式保留加密(Format-Preserving Encryption,FPE)得到，用于唯一标识设备并避免隐私泄露，表达式为：

$$M(z) = FF1_Enc_K(T, BaseID) \quad (3)$$

其中，BASEID为设备原始标识符， K 为128位共享密钥， T 为Tweak参数（由用户自定义）。

随机填充段：

当 $x+y+z < 128$ 时，用 $w=128-(x+y+z)$ 位由密码学安全随机数生成器(CSPRNG)产生的比特串进行填充，保证地址总长度为128位。随机填充置于末尾，不参与加密，每次生成均不同，从而增强地址的随机性与不可预测性。

AI驱动的IPv6地址分配

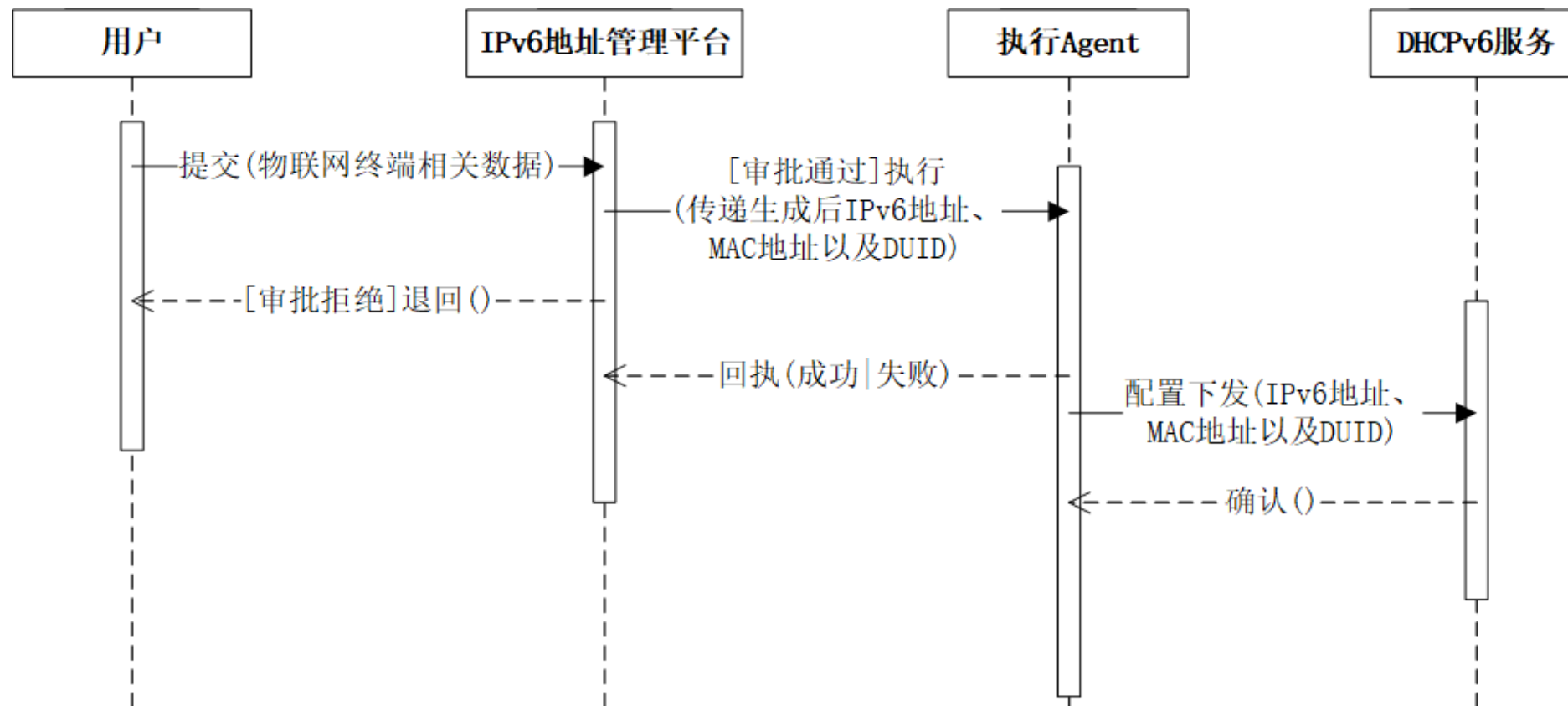


图4 终端注册审核及地址生成流程

AI驱动的终端绑定与删除的工作流

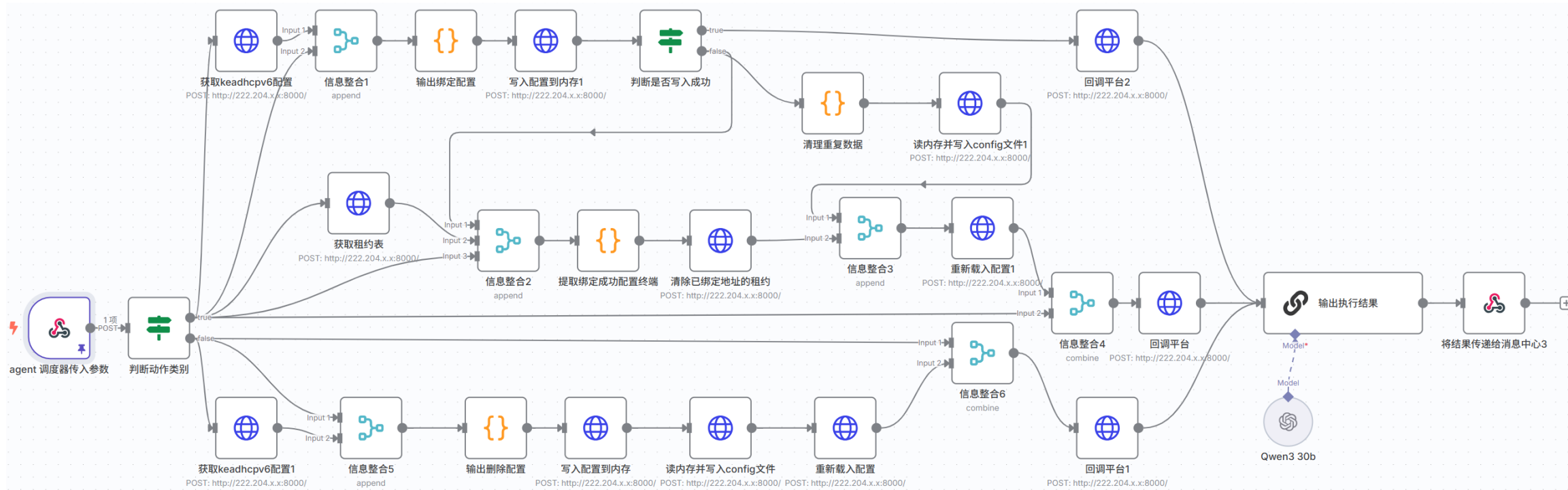


图5 终端绑定及删除工作流

AI代理根据终端注册信息自动完成语义地址绑定与配置持久化。终端上线时，系统依据DUID检测绑定记录和旧租约状态，动态完成地址分配、旧租约清理或接入拒绝，实现全生命周期可溯可控的地址管理。

AI驱动的安全策略动态调整

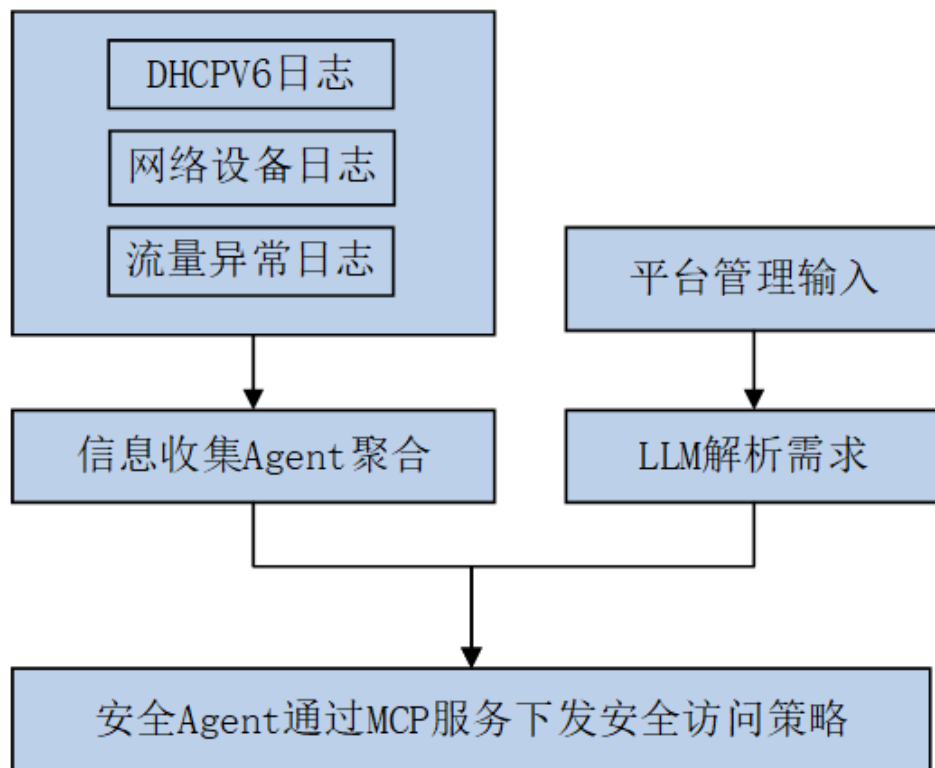


图6 物联网动态安全策略调整机制

- 信息收集Agent聚合DHCPv6日志、网络设备日志及流量异常日志等多源数据。
- 安全Agent结合流量异常日志进行实时分析，当检测到异常行为时，能够动态生成并调整访问控制列表（ACL），以快速隔离潜在威胁。
- 利用LLM模块支持管理员的自然语言输入请求，通过解析需求并自动生成对应的访问控制策略，实现从“人类意图”到“策略规则”的智能转换。

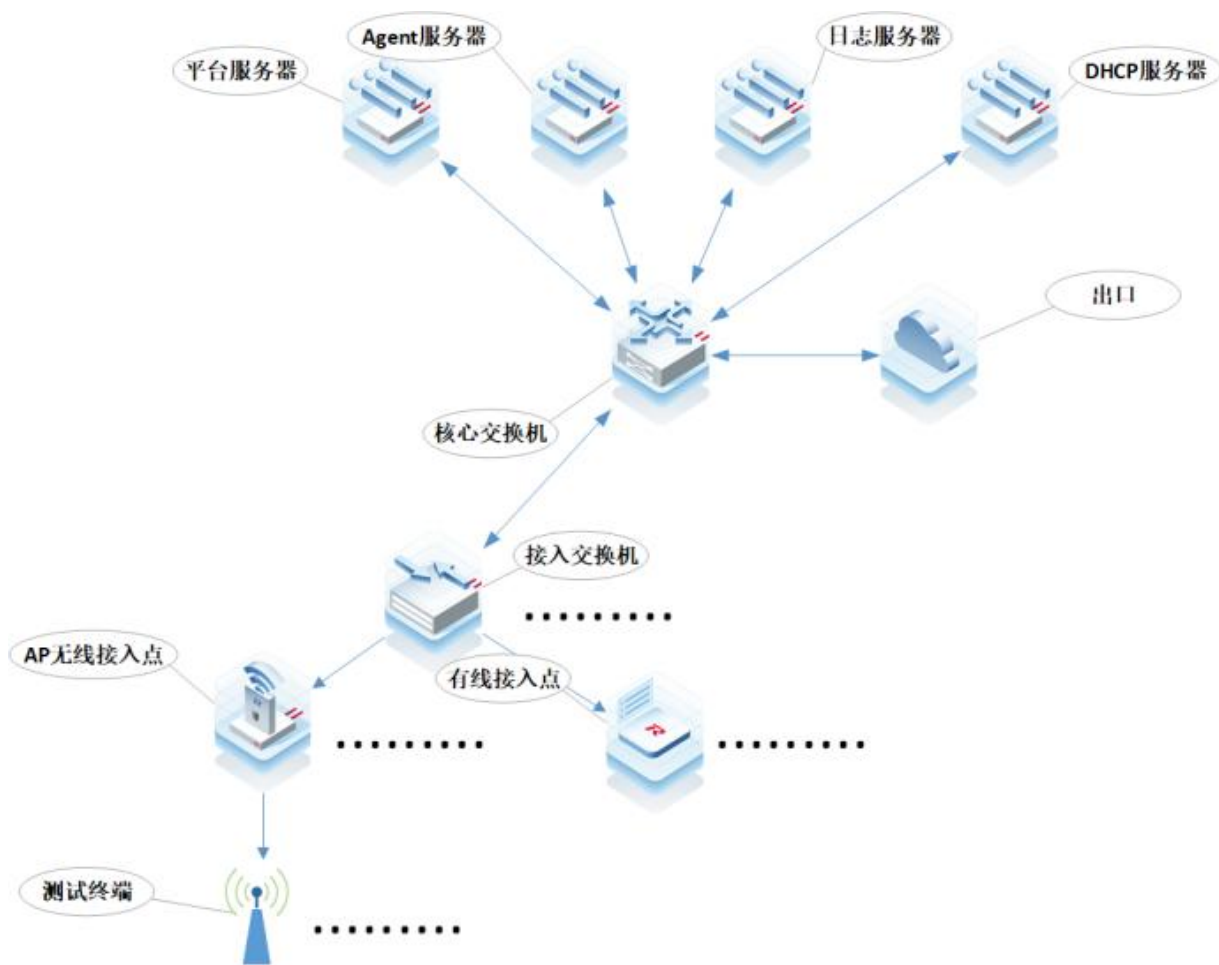


图7 实验网络拓扑图

实验硬件及软件参数

模块	设备/软件	配置/说明
计算与控制节点	Agent服务器	8核CPU, 32 GB RAM
	DHCPv6服务器	8核CPU, 32 GB RAM; Kea版本: 300.001
	算力服务器	6核CPU, 32GB RAM, GPU RTX3090 24G
	IPv6管理平台	8核CPU, Django 3.2.9, Python
网路基础设施	核心交换机	N18007, 万兆上联, 关闭无关限速/ACL
	接入交换机	多台, 用于连接终端与DHCPv6服务器
	安全日志来源	态势感知、防火墙等
终端侧	IoT测试终端	Windows10电脑、ios手机、树莓派 (Linux)

1.Kea DHCPv6绑定配置耗时与负载规模关系

实验设计:

验证Kea DHCPv6环境下, 评估由平台触发Agent修改配置文件执行地址绑定配置操作时的端到端性能。以平台下发时间为起点, Kea返回响应的时间为终点, 二者差值定义为单次绑定耗时。为评估不同负载下的变化趋势, 预先在DHCPv6配置文件中设定一定规模数量的绑定关系。假设已绑定数量 N 取值为:

$$N = \{0, 2000, 4000, 6000, 8000, 10000, 12000, 14000\}$$

每一规模下进行10轮实验。实验过程中, 记录平台下发绑定请求的平均耗时。

实验结果:

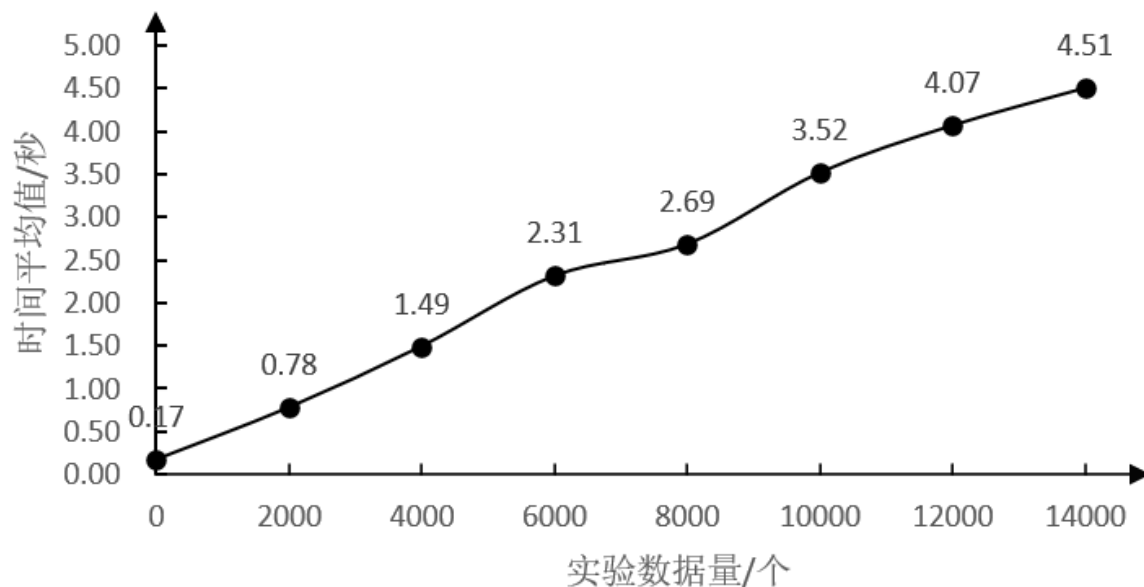


图8 Kea DHCPv6绑定配置耗时与负载规模关系

2.不同DUID类型在DHCPv6动态切换中的性能分析

实验设计:

本实验通过模拟不同终端在强制切换IPv6地址时的表现，对比了四种DUID类型的性能。实验在控制条件下，让各类终端重新获取地址并记录其切换时间、成功率、是否依赖租约及延迟波动情况，以此评估它们在动态网络环境中的适应性与稳定性。

实验结果:

表1 多种DUID类型在不同Renew-timer下的切换性能指标

DUID 类型	Renew-timer	切换时延(ASL)	租约依赖度(LDR)	切换成功率(SR)	时延抖动(Jitter)
DUID-LLT	/	1.108	0	100%	0.031
	60	88.5	100%	100%	0.007
DUID-EN\DUID-LL\DUID-UUID	300	298.7	100%	100%	0.001
	1000	951.2	100%	100%	0.001

DUID-LLT 表现最好：换地址最快（约1.1秒），不依赖租约，成功率高且稳定。

其他三类（EN/LL/UUID）依赖租约：换地址慢（等待时间随租约时长增加），虽然成功率也高且稳定，但不够快。

结论：在需要快速切换的场景可优先使用 DUID-LLT；其他类型适合对实时性要求不高的稳定设备。

3.Agent驱动的ACL策略下发延迟对比分析

实验设计:

该实验通过对比LLM触发与Agent触发两种模式下ACL策略的下发效率，设计了三个核心指标:

- 1) 端到端时延: 测量从策略触发到实际生效的总时间, 反映响应速度;
- 2) 收敛成功率: 统计策略在30秒内成功部署的比例, 检验系统时效可靠性;
- 3) 回滚成功率: 评估策略撤销后网络恢复原状态的能力, 验证系统的可逆性与可控性。

通过实验评估两种触发模式在策略部署速度、稳定性与灵活性上的实际表现。

实验结果:

表2 ACL策略下发延迟对比

场景	轮次	时延(Median/P95,s)	收敛成功率	回滚成功率
S1	10	13.84/16.67	100%	100%
S2	10	6.475/6.489	100%	100%

```
N18014E(config)#ipv6 access-list ipv6_acl
N18014E(config-ipv6-acl)#show this

Building configuration...
!
100 deny ipv6 host 2001:250:6C00:5E:5CF5:A84:F827:C816 any
10001 permit ipv6 240C:C901:A:A::/64 240C:C901:A:B::/64
50000 permit ipv6 any host 2001:250:6C00:3:8241:26FF:FE5F:EE2E
50001 permit ipv6 host 2001:250:6C00:3:8241:26FF:FE5F:EE2E any
!
end
```

图9 下发ACL规则查看

Agent触发模式响应更快(中位时延约6.48秒), LLM触发模式较慢(中位时延约13.84秒)。

两者在策略成功下发与回滚方面均表现稳定可靠。

LLM模式时延较高, 主要因其在指令输入和语义解析阶段需额外处理开销

总结

本文研究了IPv6地址相关的语义编码及AI驱动的物联网地址分配与访问控制机制，并在实验环境中模拟了大规模物联网终端可控、快捷和稳定上线，并能根据网络安全状况智能动态调整访问控制策略，验证了该机制的可行性与有效性。



未来研究方向

- ◆ **融合语义编码与格式保留加密：**拓展IPv6地址的业务识别能力，实现跨管理域的安全访问控制与隐私保护。
- ◆ **引入强化学习机制：**使策略生成具备自适应性，根据网络动态实现智能化、差异化的安全决策。

感谢观看
THANKS FOR LISTENING