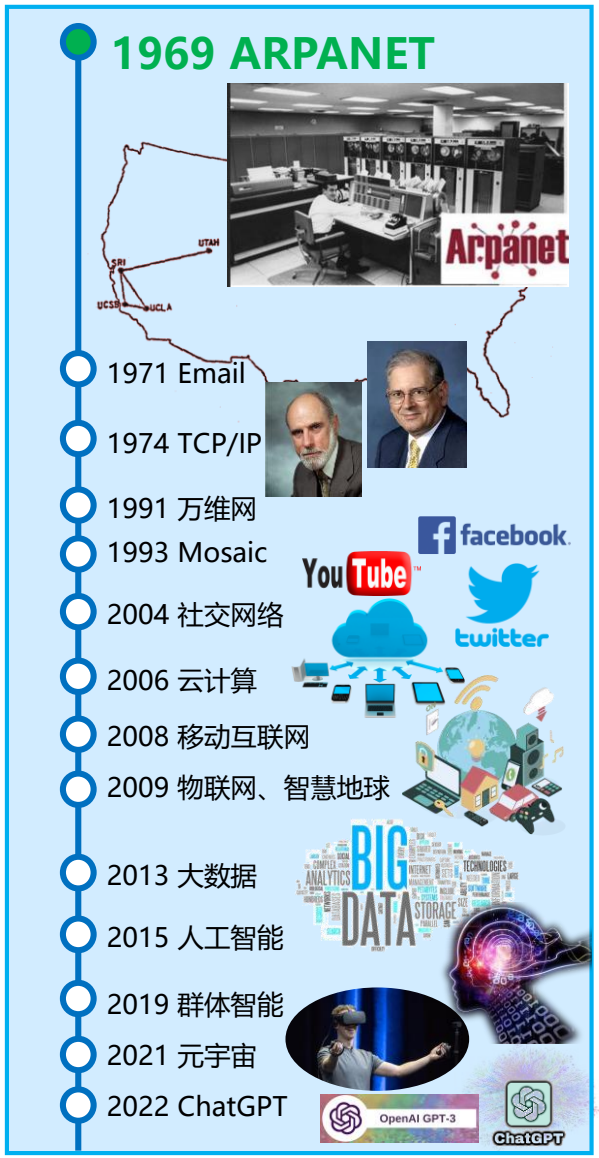
SAVA-X：安全可扩展的互联网域间源地址验证机制

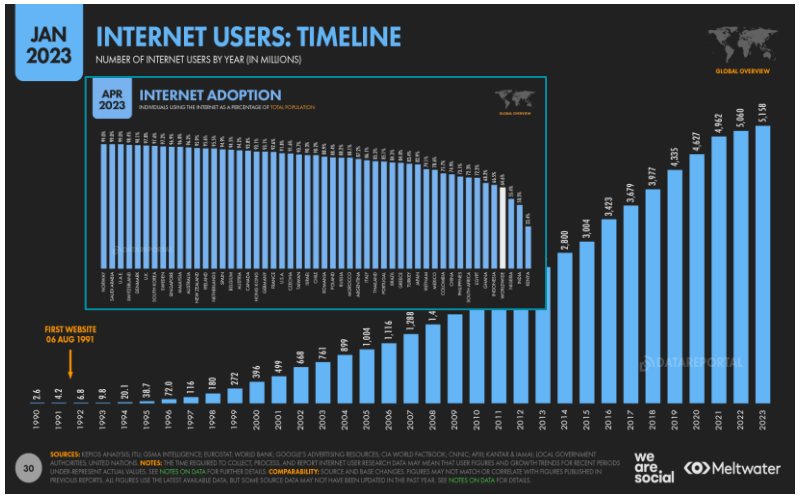
徐 恪

目录
CONTENTS

研究背景与现状

互联网已经发展成为网络空间





互联网规模持续增长

- 截至2023年4月，全球互联网用户数量达到51.8亿人，占世界人口的比重达到64.6% (DataReportal)
- 2021年全球数据储量达到84.5ZB，复合年均增长率为27.5% (IDC)

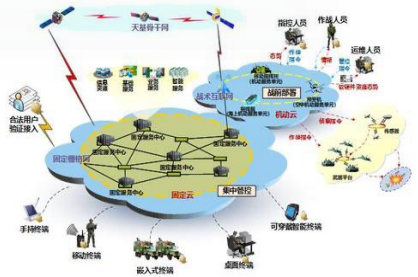
互联网应用领域普及广泛

- 互联网经过50多年发展，已经成为继陆、海、空和太空之后的人类第五疆域：网络空间
- 互联网成为承载国家政治、经济、文化、科技、军事的重要基础设施和国家重要战略资源

网络安全已经成为国家的重大战略需求

社会民生重要依赖

网络技术军事应用



网络空间对抗博弈

“没有网络安全就没有国家安全”

——2014年2月，习近平总书记在中央网络安全和信息化领导小组第一次会议上的讲话

“互联网核心技术是我们最大的‘命门’”

——2016年4月，习近平总书记在网络安全和信息化工作座谈会上的讲话

国际战略

2016年， 美国发布

《网络空间安全国家行动计划》

2020年欧盟外长发布

《欧盟数字十年的网络安全战略》

学术热点

关于网络空间安全的论文

WEB OF SCIENCE

连续三年超过5000篇文献

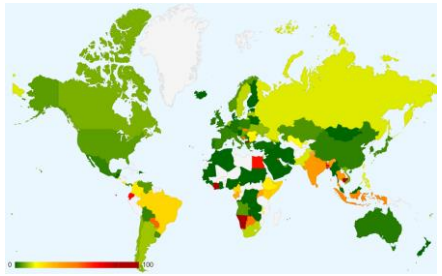
2021年超过5500篇

Google Scholar

近三年文献超过28万篇

2021年至今文献超过5万篇

互联网体系结构面临的安全威胁

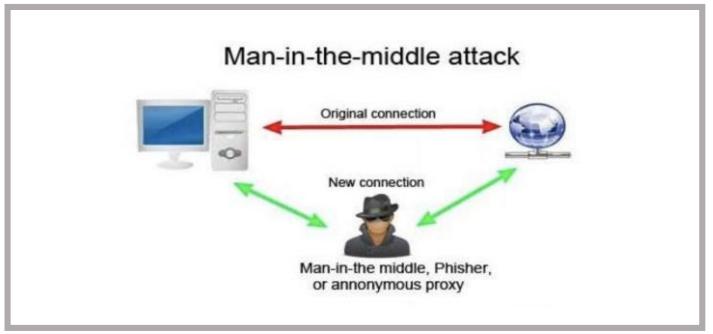


地址易被伪造

地址标识是互联网体系结构的基本载体和核心，**开放、易伪造**的IP地址，严重破坏网络通信真实性

隐私信息易泄露

路由体系是互联网进行数据传输的核心，**不可信的传输通道**造成严重信息泄露

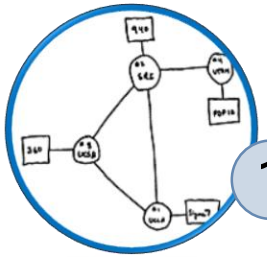


数据转发过程易受攻击

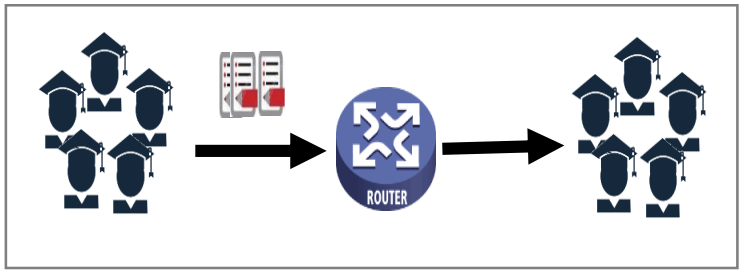
云端基础设施为互联网应用提供信任支撑，**仿冒伪造、单点故障**严重暴露用户隐私

其中承担着位置和身份双重角色的IP地址在数据传输过程中暴露出的严重缺陷是最根本的，IP地址欺骗已经成为大量攻击成功的一个先决条件

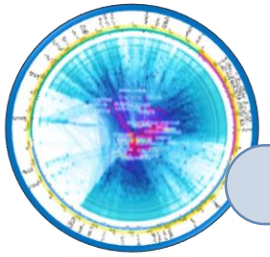
互联网体系结构面临的安全威胁



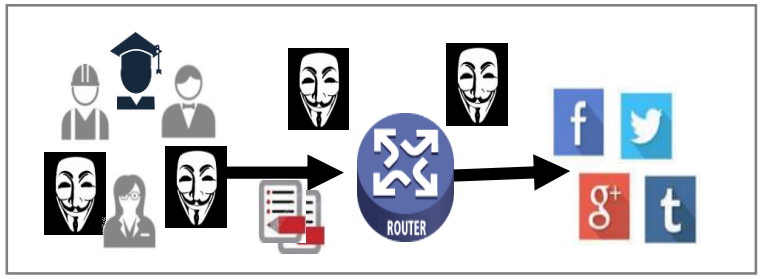
1980s前—用户彼此**信任**



"We didn't all know each other, but we all kind of **trusted** each other, and **that basic feeling of trust permeated the whole network** " —Danny Hillis



1980s后—用户**信任缺失**



" One has to pray when sending IP packets in the internet that **they won't fall in the wrong hands"**

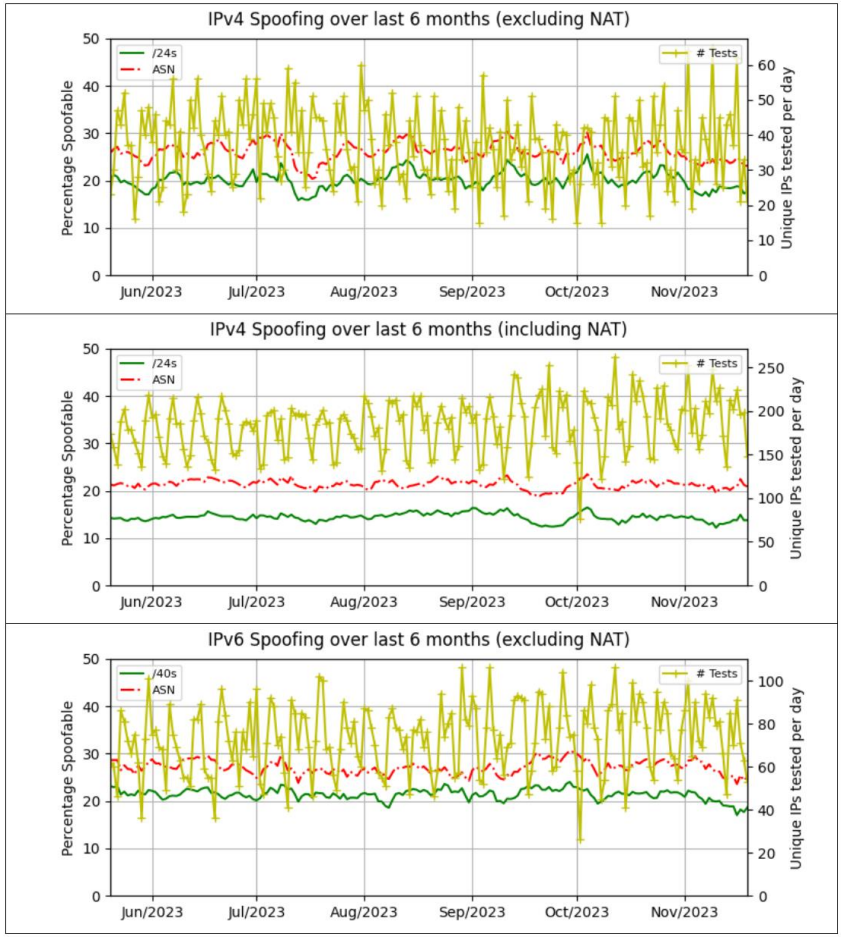
—Adrian Perrig

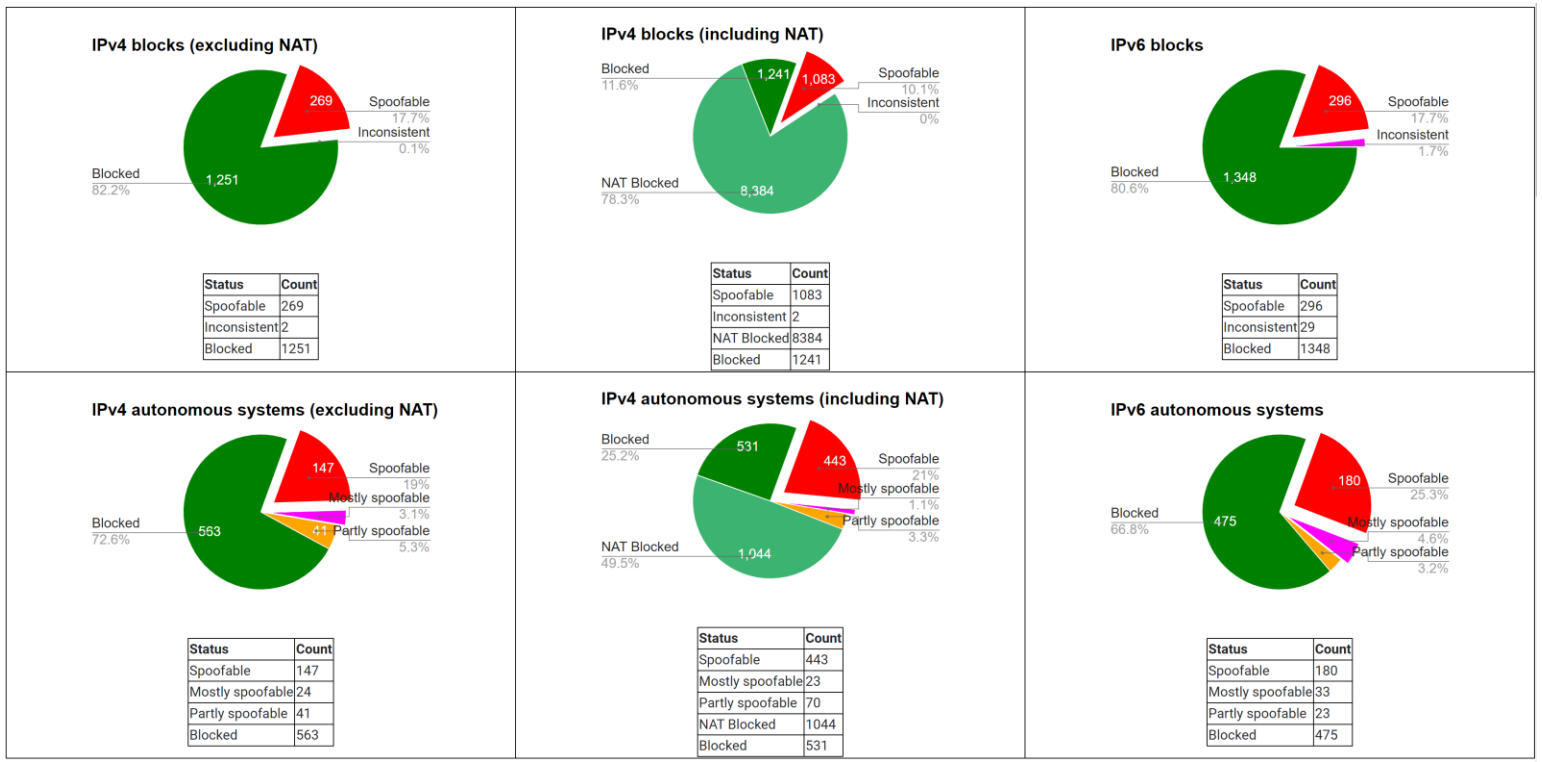
当前的互联网体系结构**缺乏安全可信基础**，很容易发生网络攻击，值得深入研究

——Vinton Cerf（图灵奖获得者、互联网之父）

互联网源地址伪造泛滥

- CAIDA成立Spoofer项目测量互联网对源地址欺骗的敏感性
- 截止2023年11月，全球超**1/6的IPv4**地址和**1/5的IPv6**地址**可以被伪造**





Status	Count
Spoofable	269
Inconsistent	2
Blocked	1251

Status	Count
Spoofable	1083
Inconsistent	2
NAT Blocked	8384
Blocked	1241

Status	Count
Spoofable	296
Inconsistent	29
Blocked	1348

Status	Count
Spoofable	147
Mostly spoofable	24
Partly spoofable	41
Blocked	563

Status	Count
Spoofable	443
Mostly spoofable	23
Partly spoofable	70
NAT Blocked	1044
Blocked	531

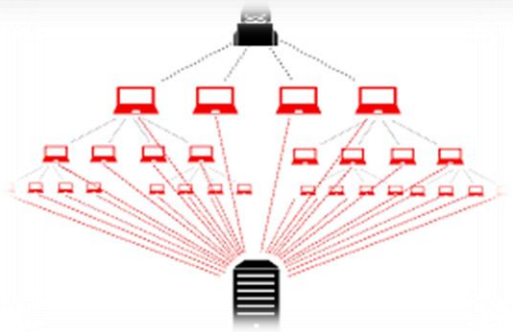
Status	Count
Spoofable	180
Mostly spoofable	33
Partly spoofable	23
Blocked	475

数据来源：https://spoofer.caida.org/summary.php

伪造源IP地址攻击

不伪造特定地址

目的是隐藏自身信息，使得目的主机即使被攻击，也无法追溯到攻击源，避免网络审查



DDoS（分布式拒绝攻击）攻击

- 攻击者**随机伪造IP地址**，同时向目的主机发送服务请求
- 目的主机的资源因为大量请求而占满，无法再响应其他请求，甚至直接崩溃

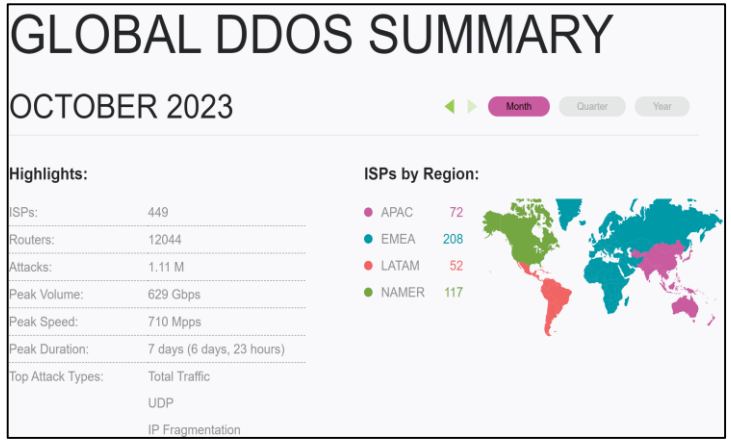
伪造特定地址

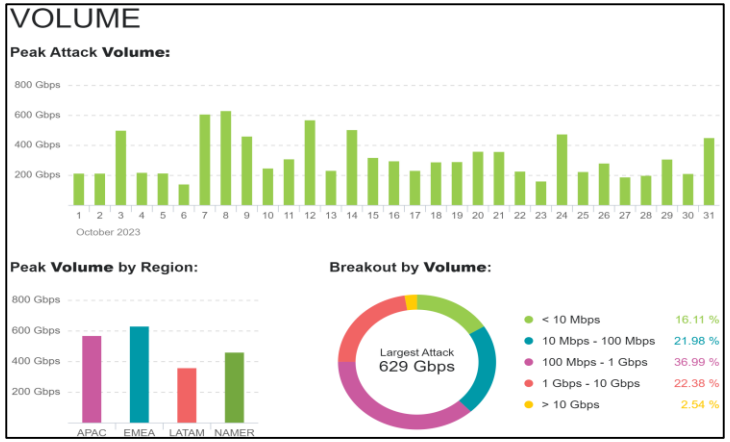
基于特定IP地址和目的主机的信任关系，伪造特定IP地址取得目标主机的信任以执行恶意指令或获取机密信息

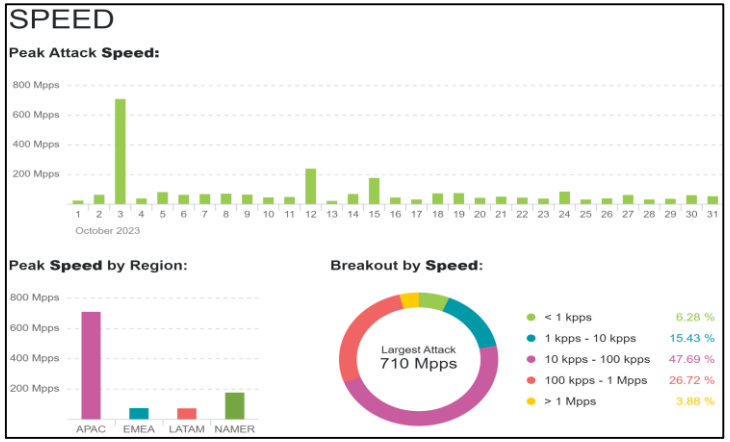
远程访问注入攻击

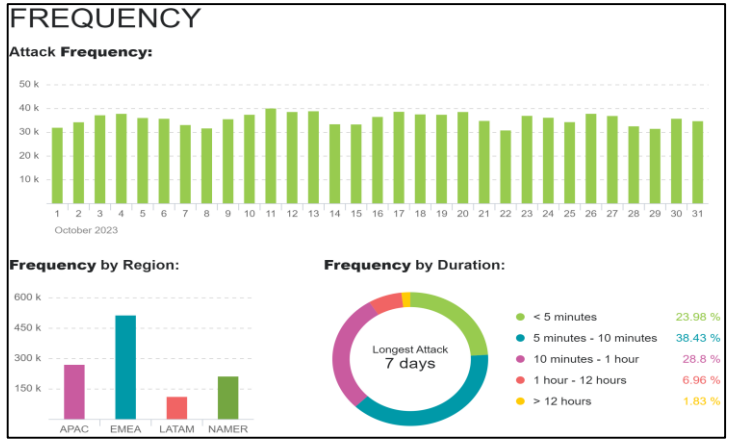
- 利用DDoS攻击使被攻击主机暂时**停止响应**
- **猜测**出被攻击主机和目的主机之间**连接标识信息**
- 向目的主机**发送恶意脚本**执行恶意指令，破坏目的主机，获取机密信息，甚至控制目的主机

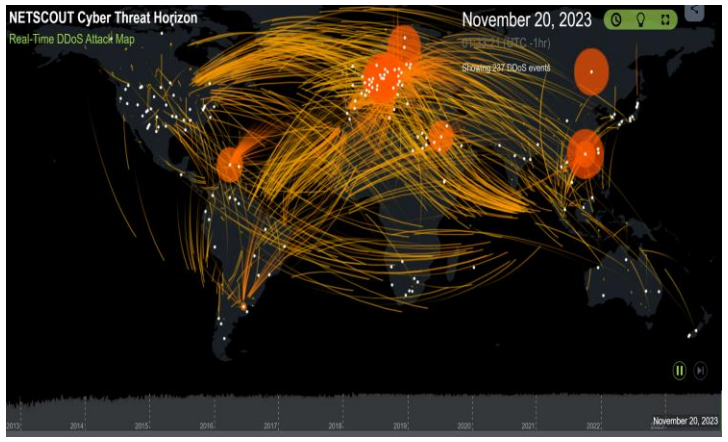
伪造源IP地址攻击

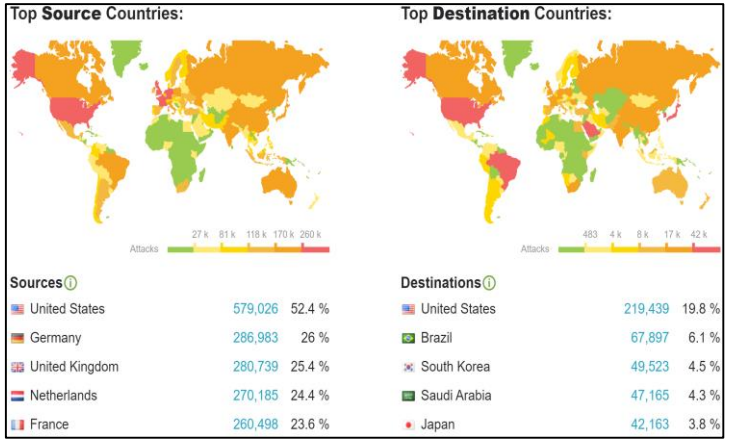












- 2023年10月，全球互联网依然DDoS攻击频发（每天超3万次，**整月超111万次**）峰值流量达**629Gbps**，峰值包速率**710Mpps**，最长攻击**持续7天**

数据来源：https://horizon.netscout.com/

源地址验证机制和技术体系

IP地址脆弱性

1. 数据包都是01序列，是同质的
2. IP包头中IP源地址可以随意填
3. 数据包中不存在签名，无法验证
4. 网关等设备不会对出流量数据包源地址进行检测

IP协议栈底层设置，难以修正

真实源地址的设计目标

1. 经授权的：IP源地址必须是经互联网IP地址管理机构分配授权的，不能伪造
2. 唯一的：IP源地址必须是全局唯一的
3. 可追溯的：网络中转发的IP分组，可根据其IP源地址找到其所有者和位置

主要的四类源地址验证机制

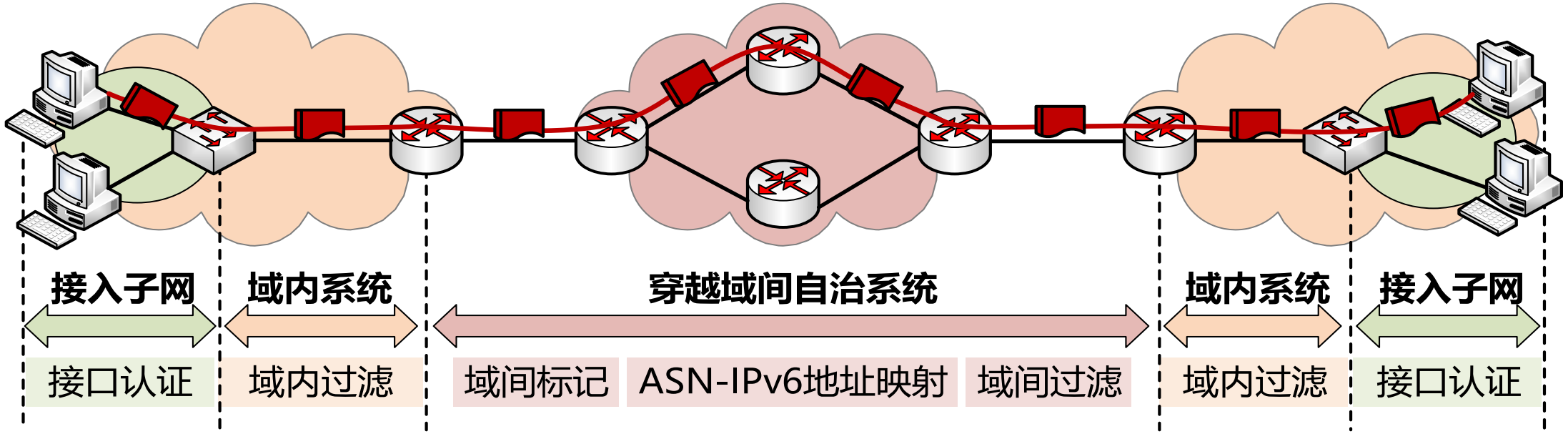
- **基于数据包加密签名和标记信息**
- **基于路由信息**
- **基于分组转发跳数**
- **基于域间商业关系**

源地址验证机制和技术体系

技术分类	技术	过滤位置	依赖技术	部署特征	制约因素	防御效力	实现开销
基于数据包加密签名和标记信息	SPM	源/目的端	加密技术	1. 仅部署者受益 2. 支持增量部署	可扩展性低	1. 假阴性高 2. 假阳性低	高
	SMA						
	DISCS						
	IPsec						
	PASSPORT	传输路径					
基于域间路由信息	IEF	源端	无	部署激励低	部署激励低		低
	uRPF	传输路径	路径合法性	部署激励随部署率上升而逐渐降低	1. 未部署者受益明显 2. 受拓扑以及路由动态性影响明显	1. 假阴性低 2. 假阳性高	未知
	DPF						中
	SN						
	SAVE						
	BASE						
基于域间商业关系	BAR-SAV		商业关系和路径合法性				低
	ARBIF		商业关系				
基于分组转发跳数	HCF	目的主机	报文跳数	仅部署者收益	防御可被彻底绕过	假阴/阳性高	

源地址验证机制和技术体系

2005年，**清华大学**在国际上首次提出**真实源地址验证体系结构SAVA**，从**接入网、域内和域间**三个层次设计源地址验证关键技术，实现了基于真实地址的用户标识与管理，形成系列化IETF国际标准，推动IETF成立了接入网真实源地址验证SAVI（Source Address Validation Improvements）工作组，开展了规模试验和部署。



SAVA-X的技术挑战与核心机制

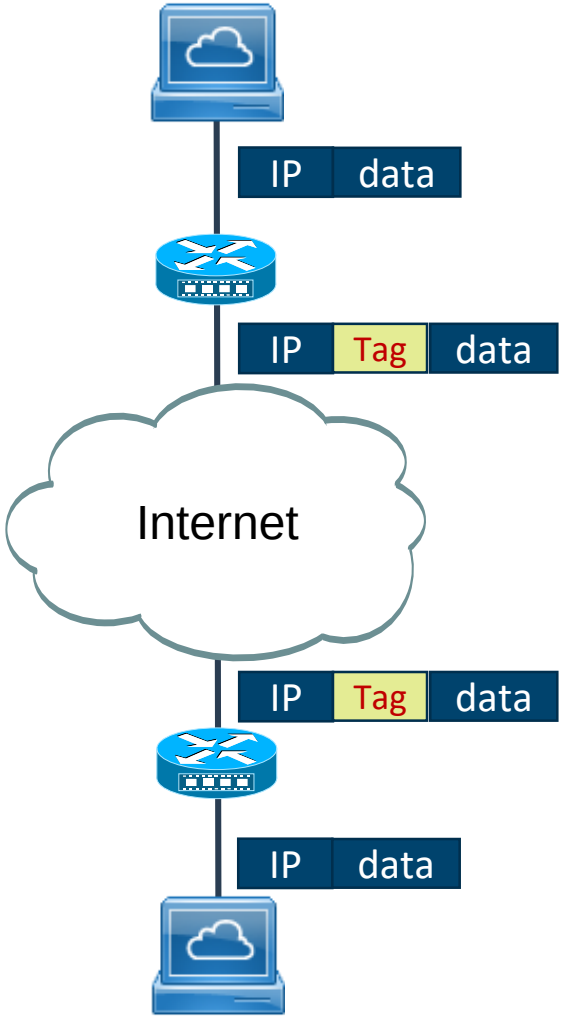
传统数据面源地址验证机制

目标

对自治域之间的伪造源地址流量进行识别和过滤，实现对自治域的保护

具体机制概述

- 通过在AS之间建立验证组进行源地址验证，验证机制部署在AS的边界路由器上
- 边界路由器为本域内发往其它组内成员的报文进行AS级别的源地址前缀检查， 保证源自本AS的报文携带的源地址确实属于本AS
- 边界路由器为源自本AS、目的为其它成员AS的报文添加用以标识本 AS 身份的“标签”，该标签可验证，确保AS地址前缀不被冒用



SAVA-X的设计动机与优化方向

问题1

大规模网络带来的扩展性和管理性挑战

(一对一状态维护引发状态空间爆炸)

问题2

难以严格剔除非部署域作恶

(Onpath节点冒用标签/修改数据包)

问题3

缺乏对真实源地址设备的验证

(接入/域内机制是否工作难以检验)

问题4

域间僵化的自治域结构

(源地址验证范围和粒度的灵活性)

✓层次化改造

✓防篡改机制

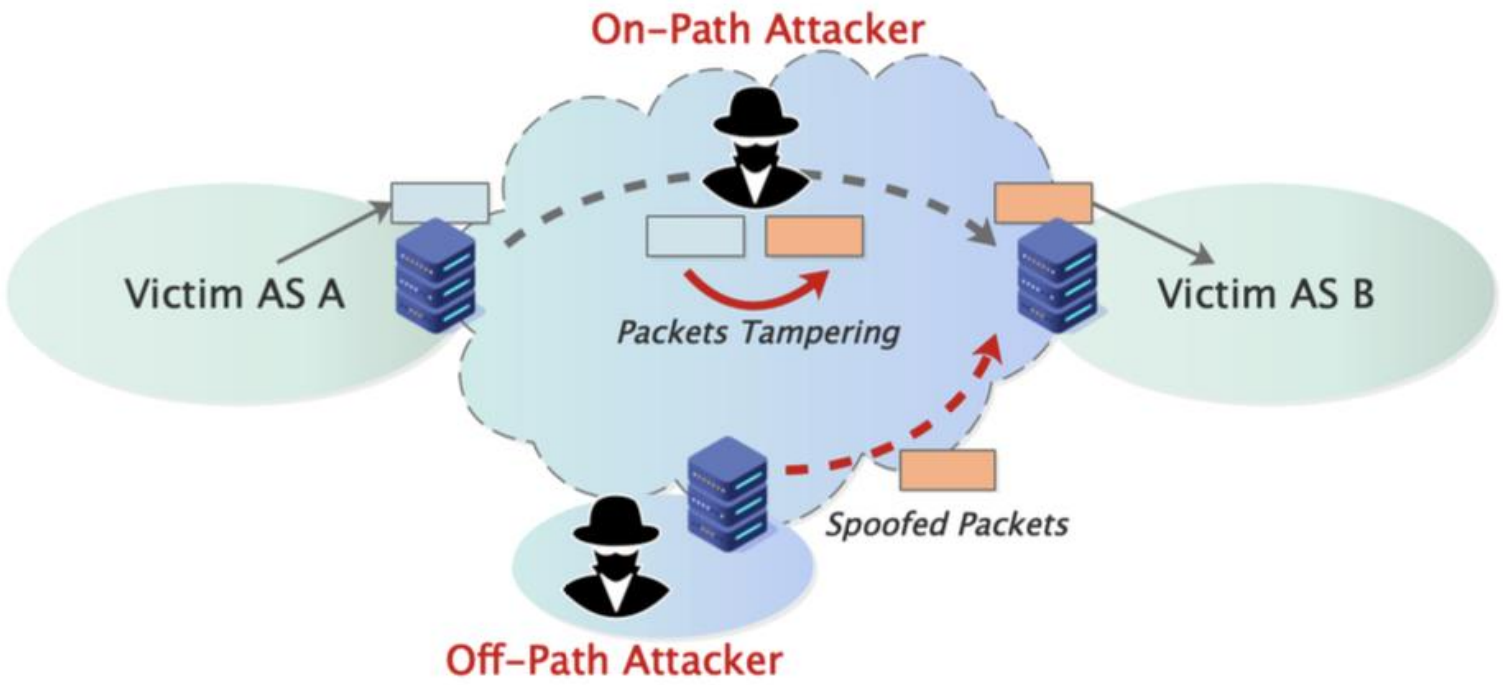
✓标签机制扩展

✓地址域方案

支撑

分布式信任基础设施

威胁模型与设计目标



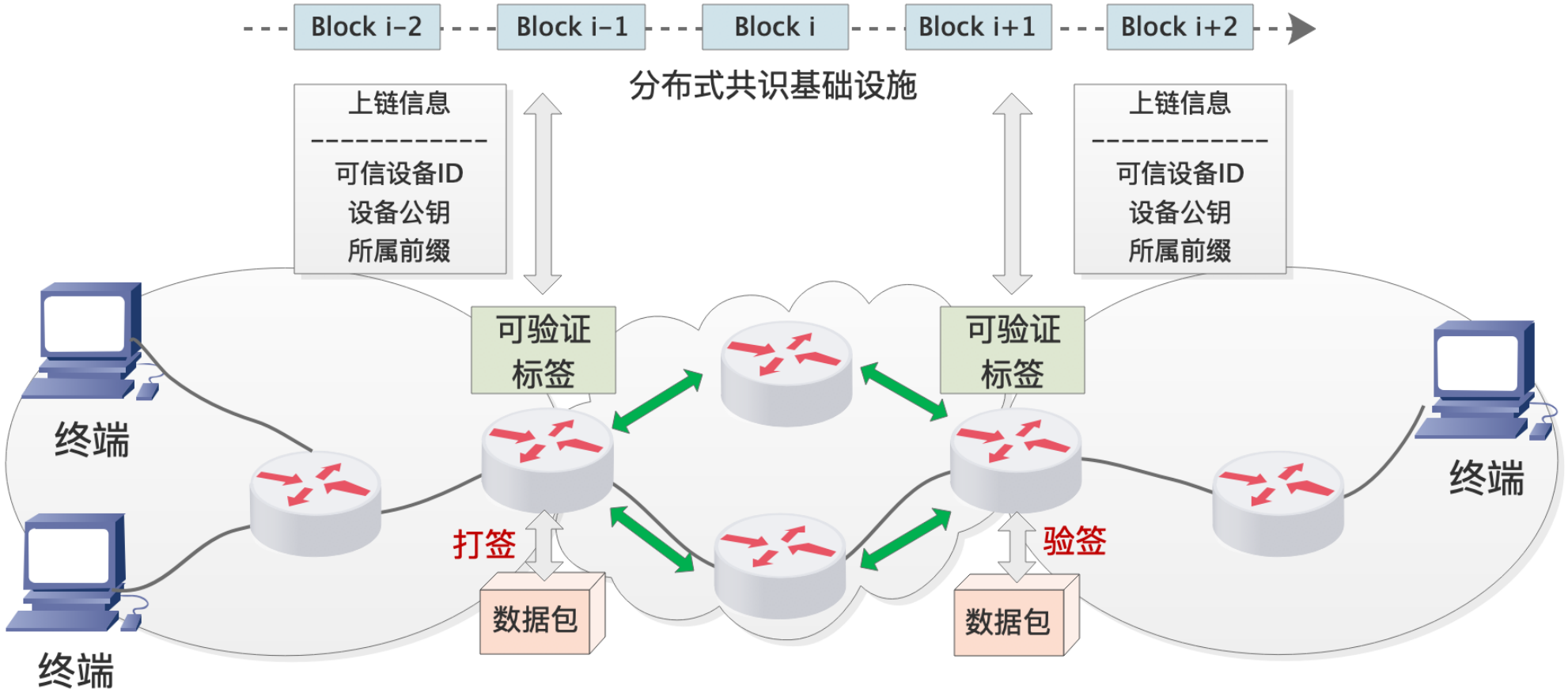
假设与威胁模型

- 攻击者可以**篡改**经过的数据包**源地址**，可以**截获合法的数据包标签**并拼凑非法的数据包载荷
- 假设存在互联网规模的可验证资源分配记录（如RPKI），具备自治系统（**ASN-合法前缀-可验证公钥**）的映射信息

SAVA-X设计目标

低数据面开销 | 高可扩展性 | 伪造流量尽早过滤 | 灵活的验证粒度

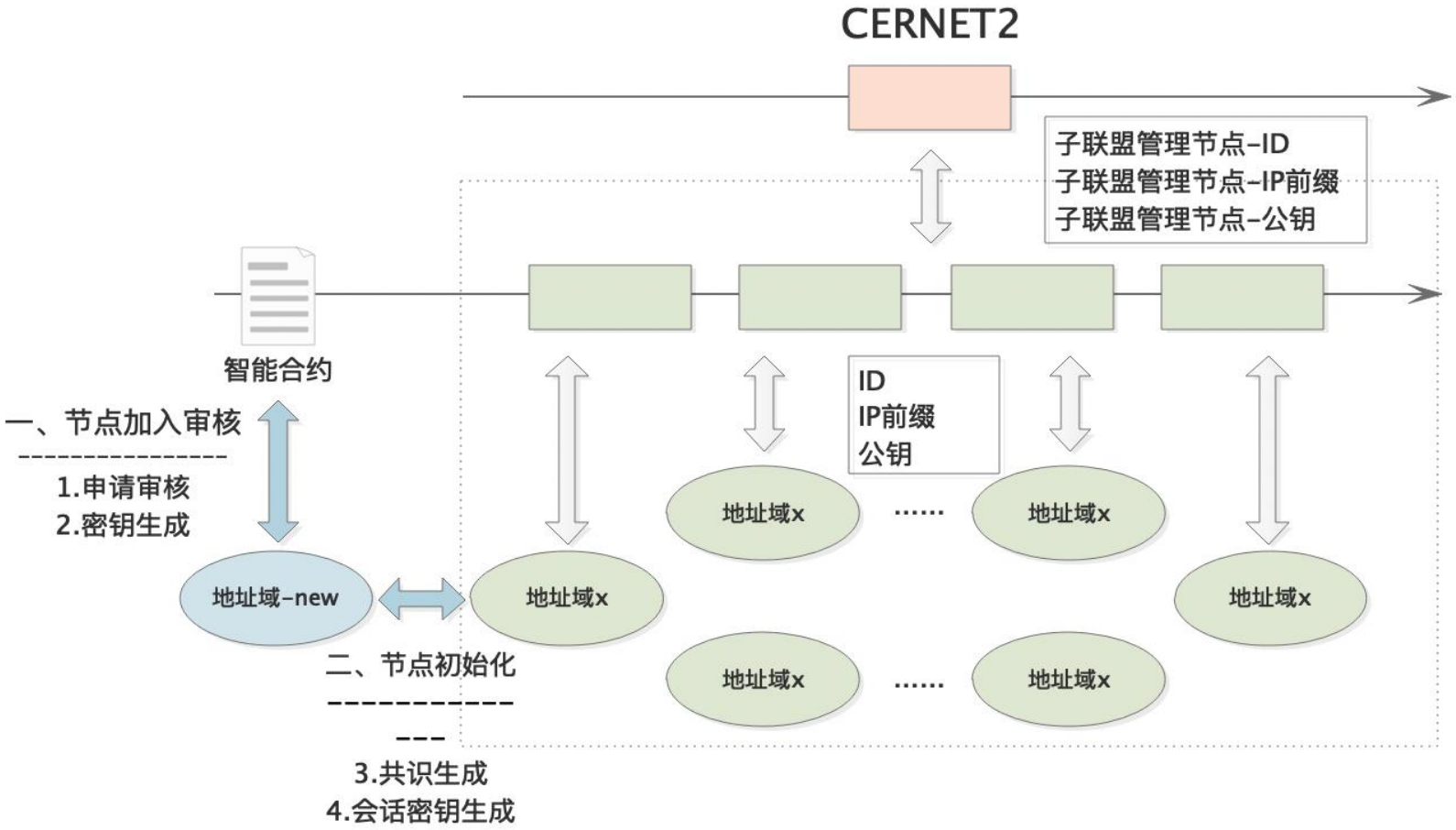
SAVA-X概述



分布式共识基础设施支撑的域间端到端可验证信任机制

基于分布式基础设施的状态机维护 → 规模问题 → 层次化信任传递与标签验证/替换机制 → 管理问题 → 面向地址域的信任联盟管理

节点管理与标签协商



地址域

- **一组IP地址前缀**组成的集合，及其对应的网络范围，称为一个地址域。
- 地址域**与IP地址空间分配过程相对应**，规模可大可小，若干AS可以合并为一个地址域，一个AS内部也可划分多个地址域。

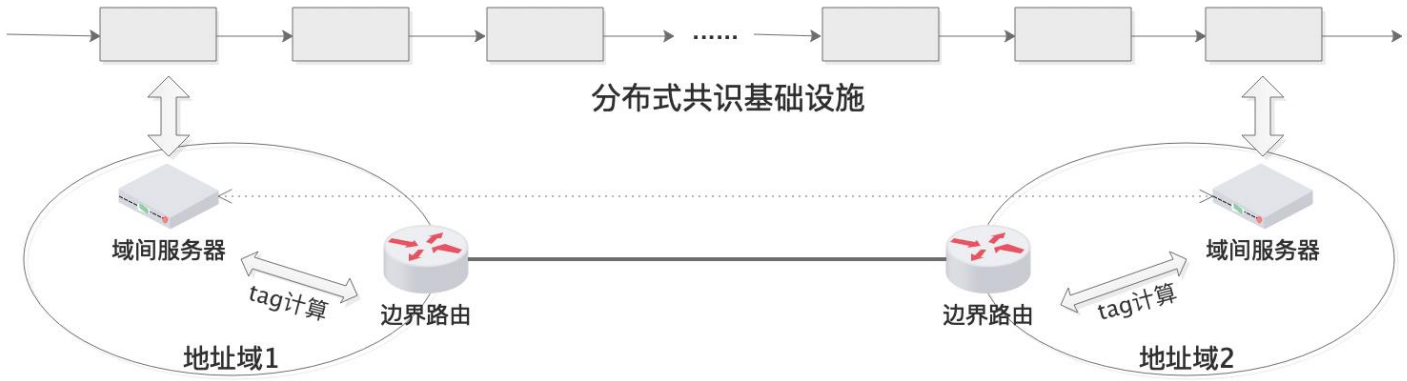
申请审核：智能合约运行地址域资质审核流程，管理服务各节点自行判断、投票表决

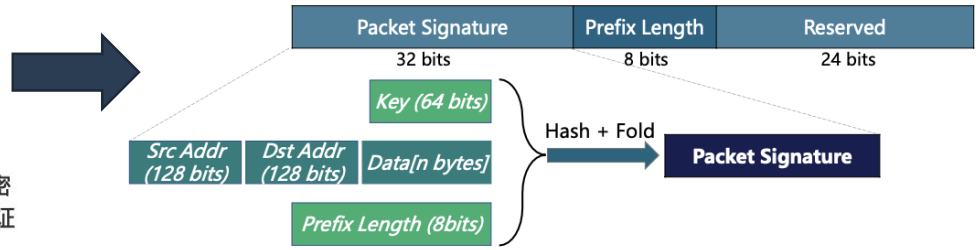
密钥生成：申请通过后，智能合约自动生成地址域公私钥对并下发

共识生成：将新节点的地址域-IP前缀-节点公钥映射信息发布于信任服务，形成共识

会话密钥生成：新节点与其他节点交互，生成会话密钥，初始化维护状态机

节点管理与标签协商

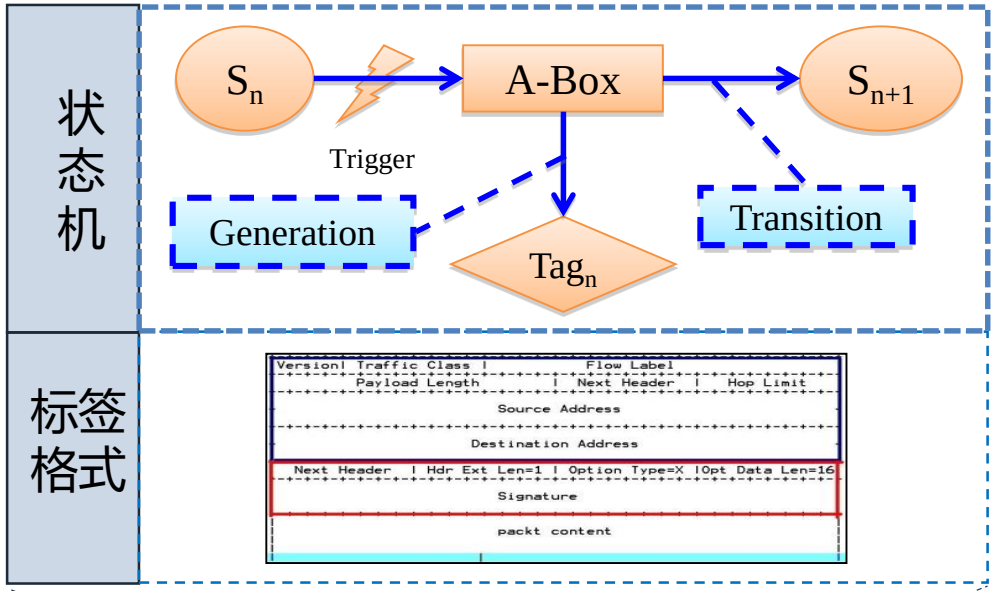




去中心化改造
- 兼容设备端
- 高效转发
- 可靠的密钥协商

规模扩展 → 状态机维护空间爆炸

节点管理与标签协商

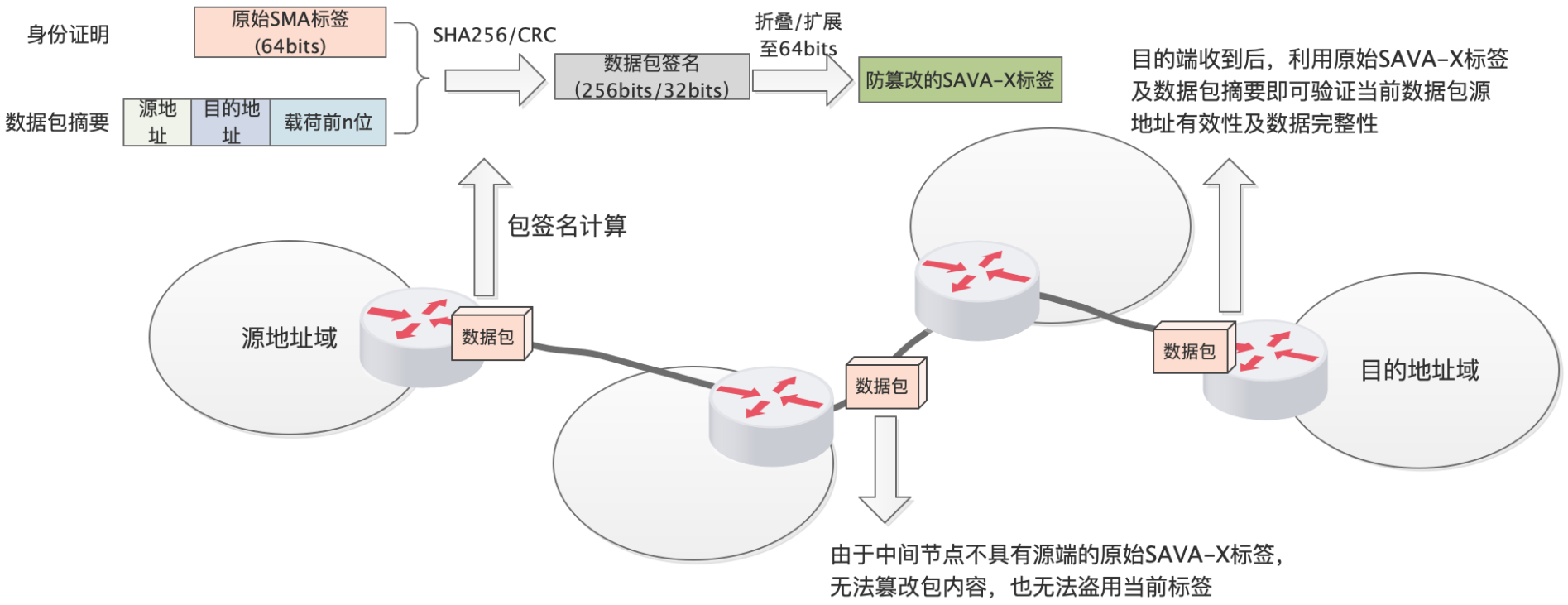


- 状态机用于生成和管理标签
- 每个地址域源针对不同地址域生成不同的状态机
- 标签作为一个新类型的 Option 加入 IPv6 的 Destination Option Header 中
- 商用平台实现已支持100Gbps吞吐

1.获取目的地址前缀
2.查询对应地址域号
3.检索对应标签
4.扩展头添加标签

1.获取源地址前缀
2.查询对应地址域号
3.检索对应标签
4.对比数据包中标签
5.放行/丢弃

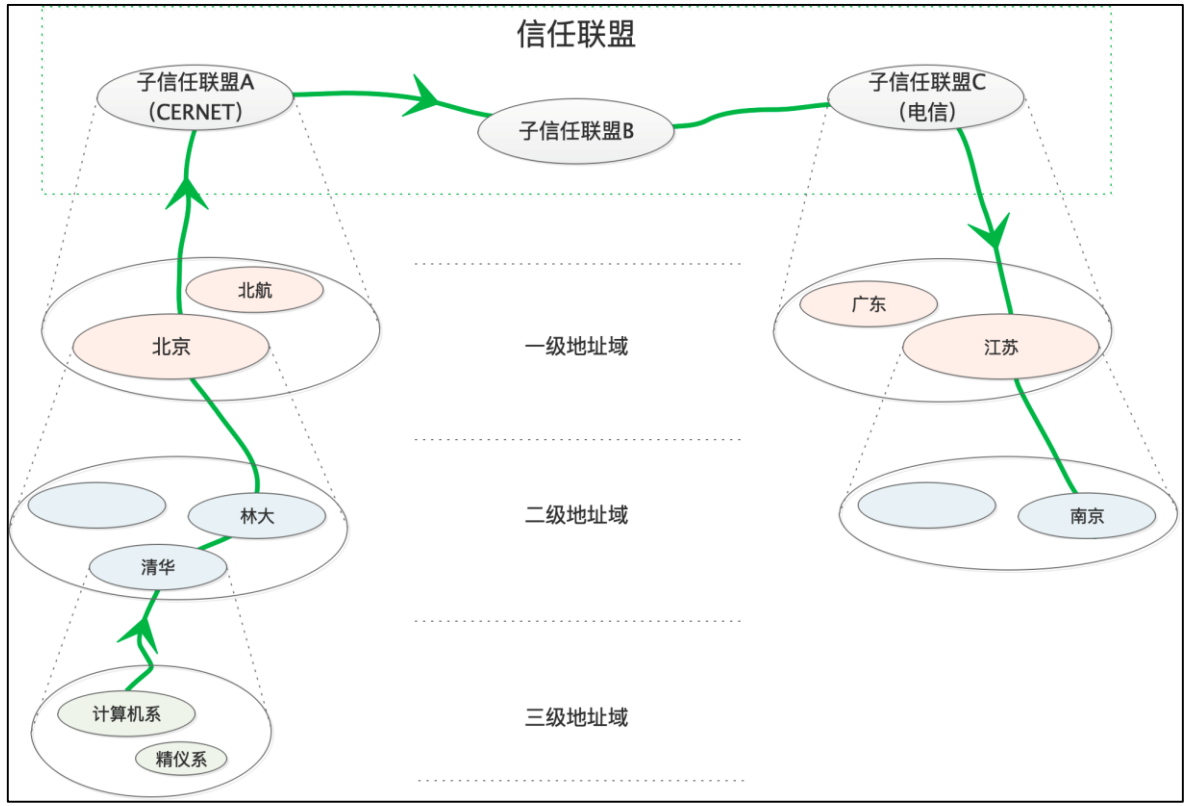
节点管理与标签协商

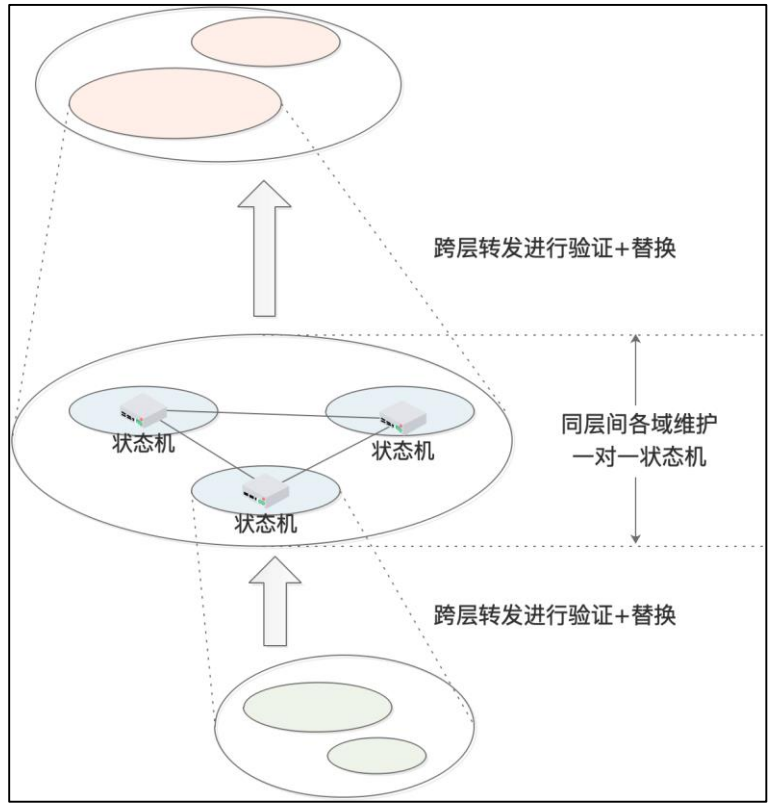


合法标签重放：合法数据包标签携带在数据包头部，可以被On-path的恶意节点成果截获，之后拼接非法载荷来实现攻击目的

SAVA-X防重放和拼接攻击：SAVA-X数据包标签的生成本身依赖时钟同步状态机，具备对简单重放攻击的防御能力。同时，SAVA-X在标签生成时将数据包载荷摘要加入签名部分，防止拼接攻击

层次化设计与标签替换



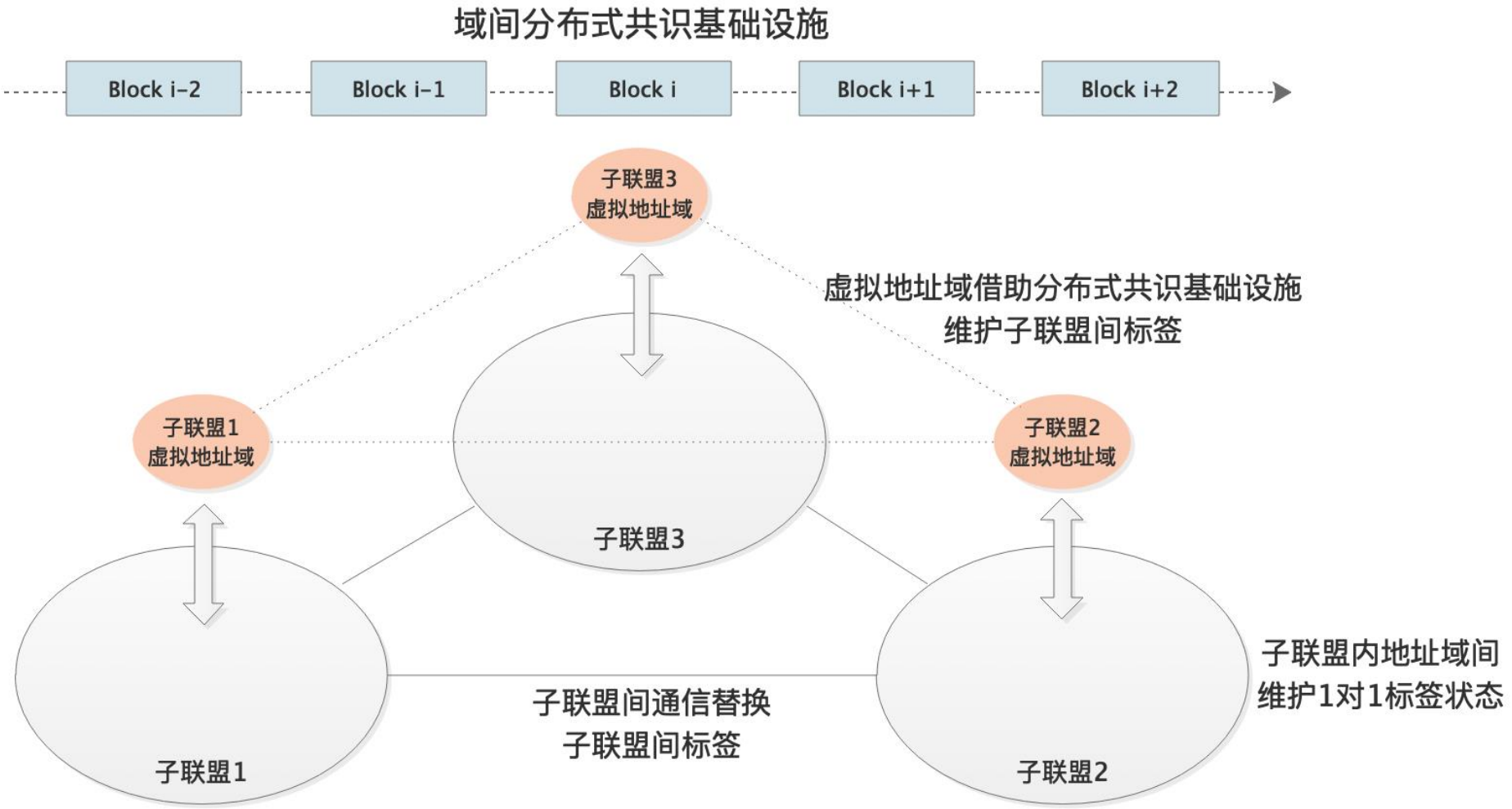


层次化信任：同层节点维护直接信任关系，跨层交互依赖层间信任传递，解决可扩展性以及状态机空间爆炸问题

SAVA-X分层：五层结构（不要求全部具备），自上而下为信任联盟、子信任联盟（CERNET/电信网）、一级（地址域、地址域）/二级（院系）/三级（楼宇）地址域

标识验证与替换：层内节点维护全连接状态机，通过标识验证转发；跨层时通过层间逻辑网关节点进行层内验证+层间标识替换，

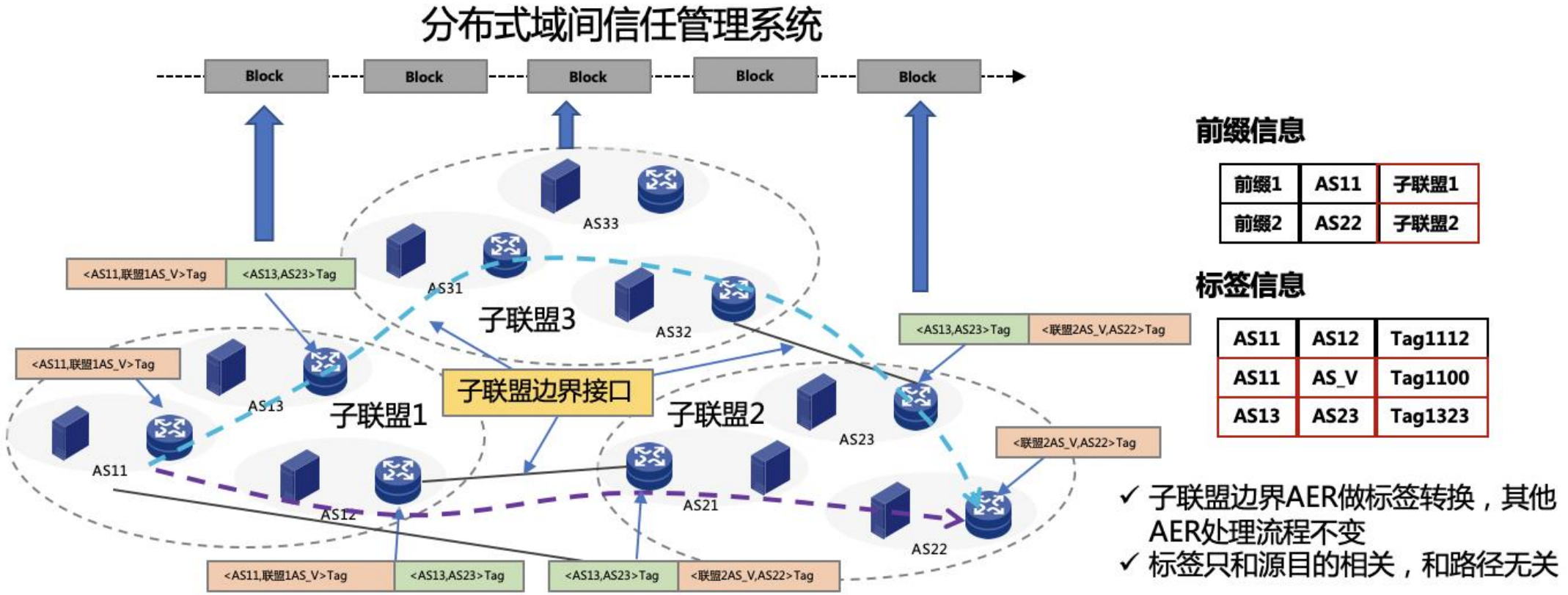
层次化设计与标签替换



子联盟内：各地址域间维护1对1标签状态，通信过程不涉及标签替换

子联盟间：边界地址域进行标签替换（虚拟地址域维护子联盟间标签），利用虚拟地址域避免多径传输带来的标签替换困境，实现**标签验证与路由路径解耦**

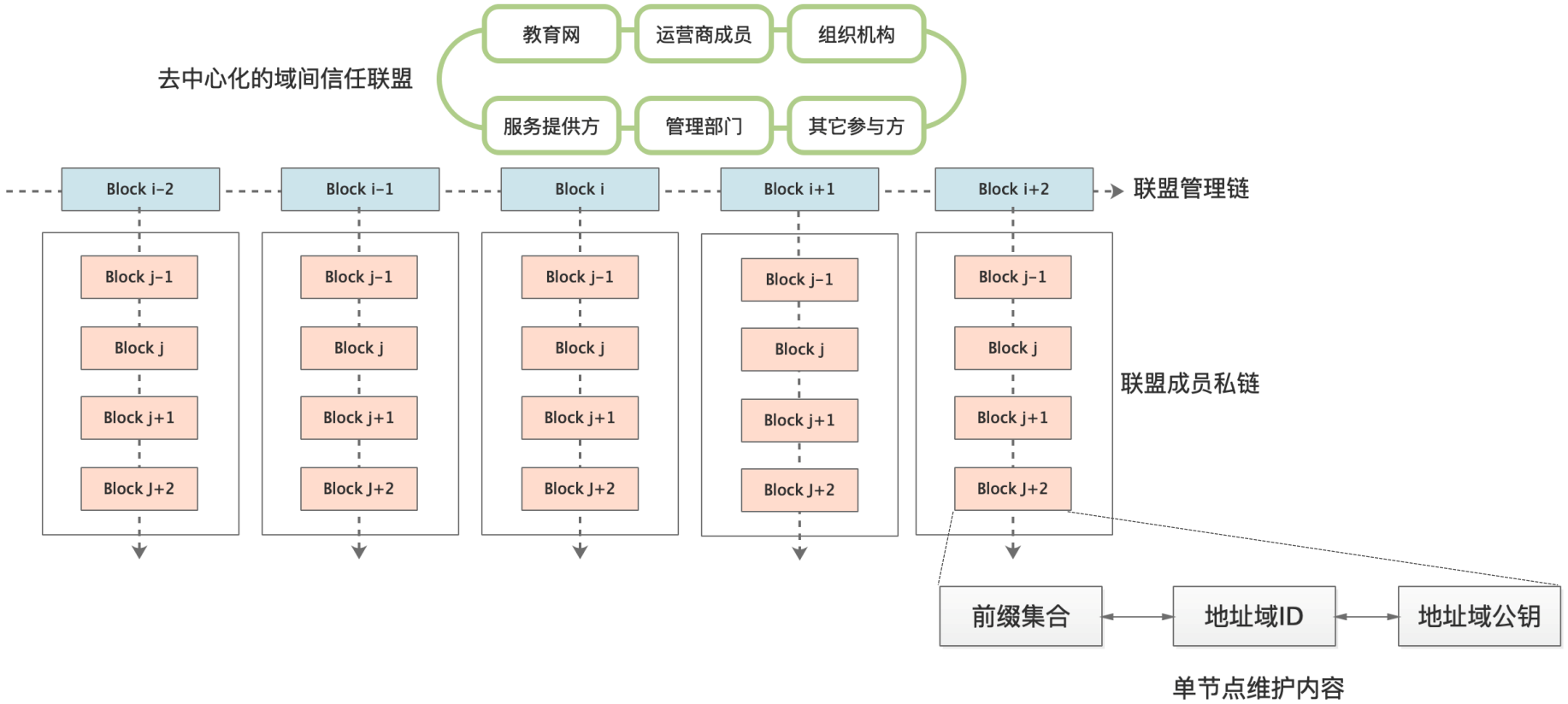
层次化设计与标签替换



跨子联盟：子联盟间转发，标签为源端-目的端子联盟级标签，即从源子联盟到目的子联盟的所有数据包无论转发路径为何、经过哪个边界网关，均使用同样的SAVA-X标签，保障子联盟间转发不受域间多径传输影响。

子联盟内：与跨子联盟转发类似，子联盟内所有跨层转发，其SAVA-X标签均使用的两层间标签，与跨层路径无关，不受多径传输影响。如同层转发，则因为同层节点间保持两两状态机维护，无需进行标签替换，不受转发路径动态性影响。

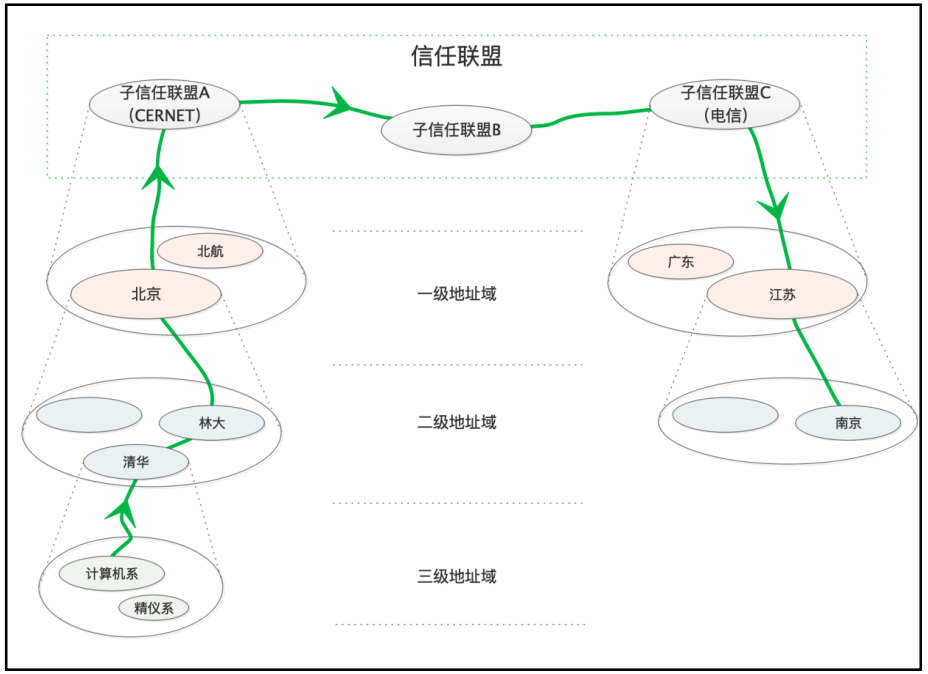
面向地址域的信任联盟管理

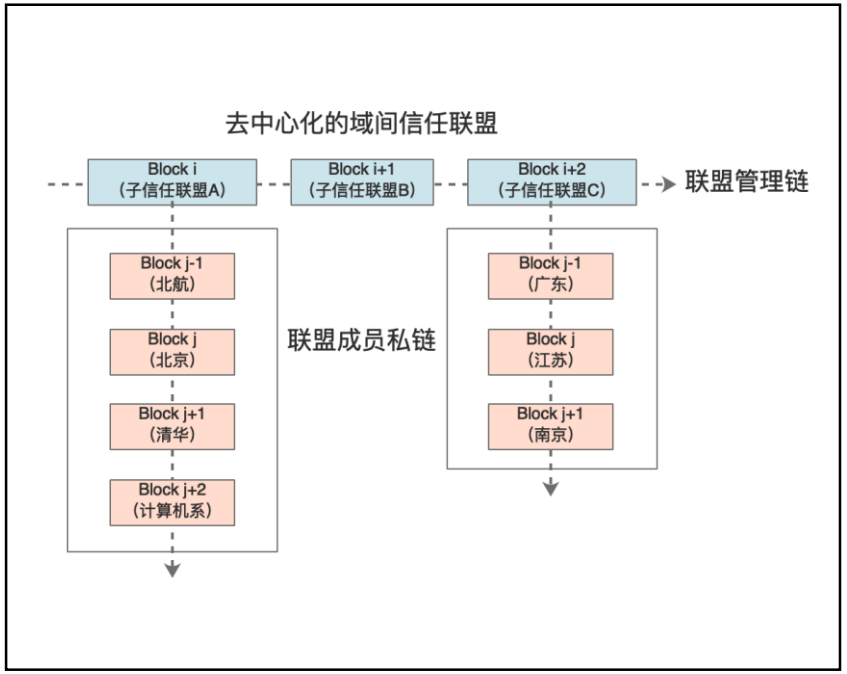


子联盟内：新节点加入，统一由子联盟根节点审核，审核通过分配节点ID、公钥，形成节点内容共识，同层节点初始化状态机；子联盟内使用统一地址域ID，不同子联盟内可使用不同ID（如教育网使用私链节点自增ID，电信网使用地址域号）

子联盟间：新节点加入，由管理委员会共同审核投票表决，子联盟间地址域ID使用联盟管理链节点自增ID

面向地址域的信任联盟管理

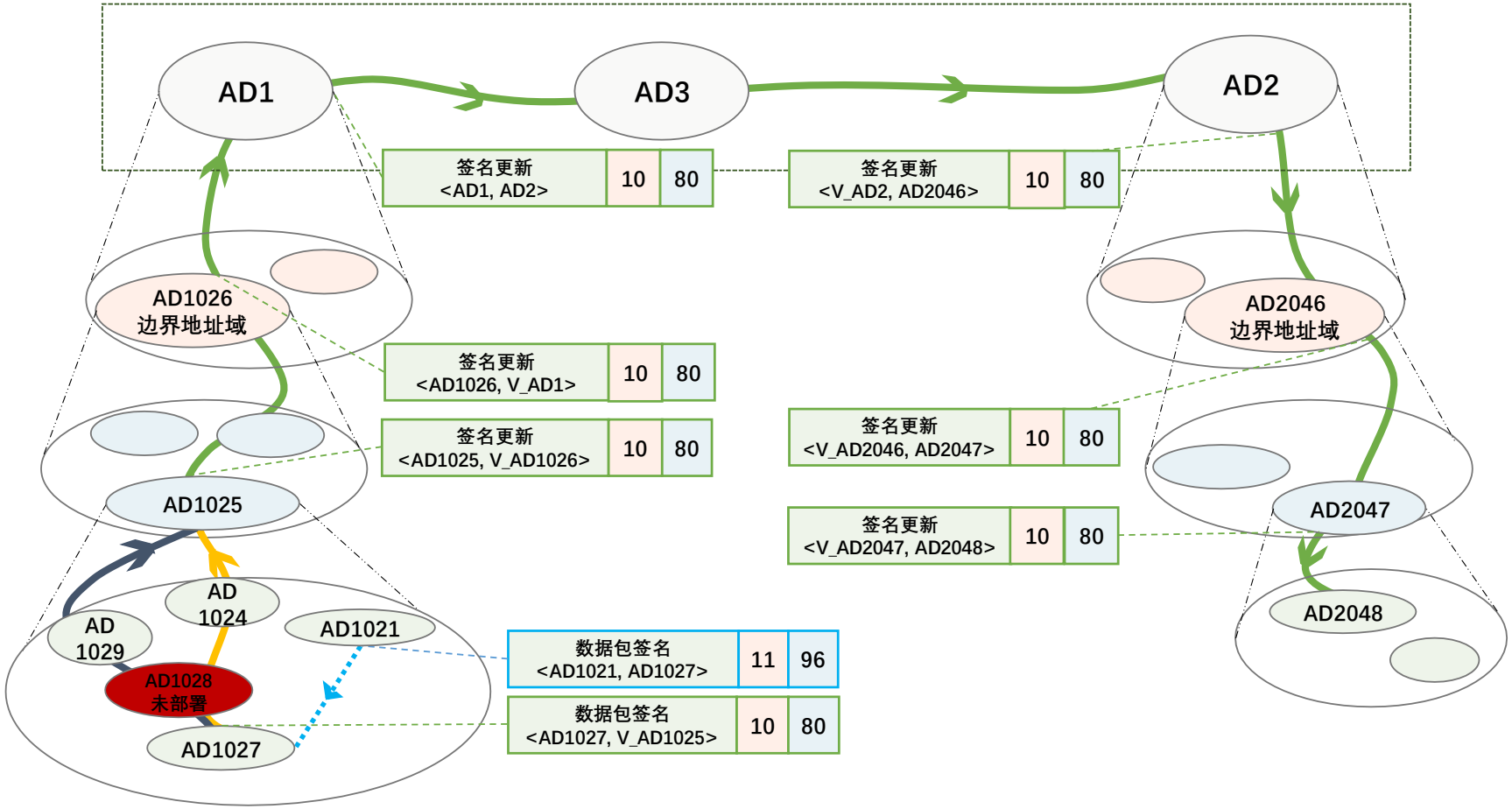




联盟成员私链：子联盟（运营商网络）内无层次，所有地址域节点组成该子联盟私链。私链内新增节点，由私链主节点集中管理（审核/登记/密钥分发）。例如新增“清华电子系”均需通过教育网主节点审核，通过后分配密钥并将节点信息上链。

地址域ID：由于层次化机制本质是信任域间传递，并不会暴露内部节点信息，所以SAVA-X方案不要求全局地址域ID唯一，仅要求子联盟内ID唯一。例如教育网内部可统一使用私链节点ID做为地址域ID，电信网可继续使用AS号，两者间SAVA-X可正常运行

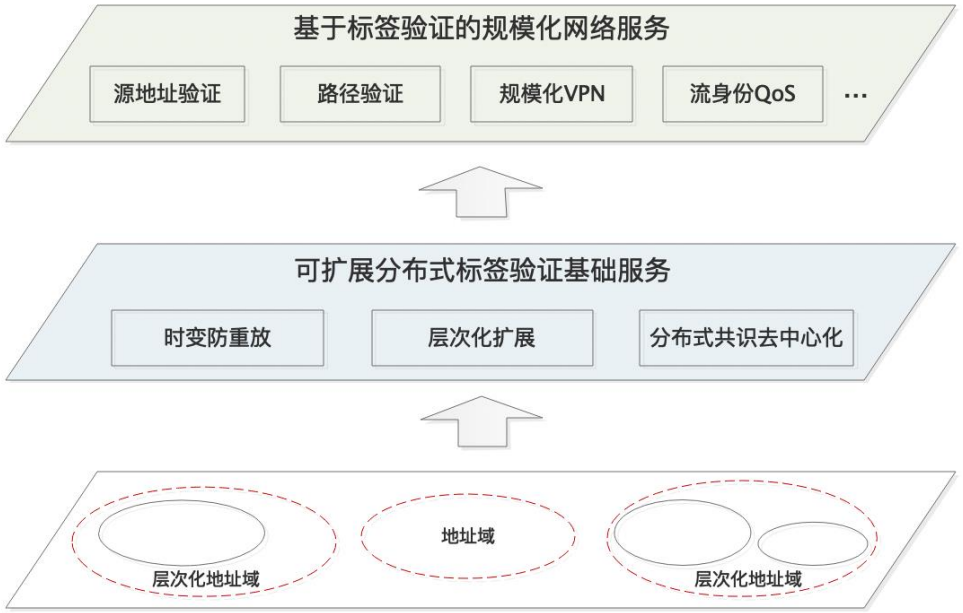
面向地址域的信任联盟管理

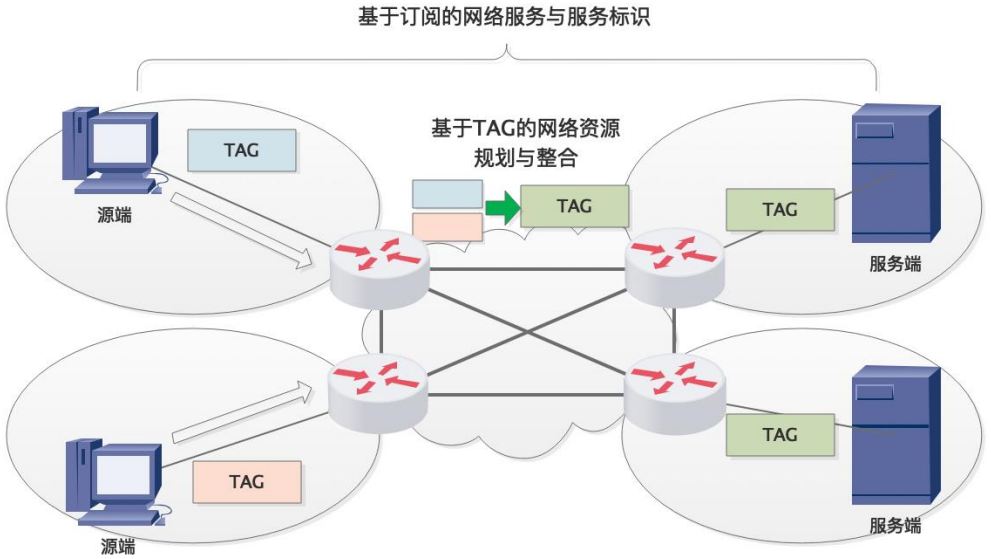


标签验证：根据源地址+可信前缀长度得到前缀，根据前缀查询地址域ID，由地址域ID检索状态机标签，计算摘要，验证签名

标签更新：根据目的IP查询对端位置，在本层内，则查询到对端状态机替换标签；如需跨层，标签更新为本域跨层标签（本域ID-上层所属域ID）；如需跨子联盟，则标签更新为本子联盟和目标子联盟间跨联盟标签（所有路径使用相同标签，A-C）

数据包标签扩展





以SAVA-X的层次化管理机制为基础，建立起**可扩展分布式标签验证基础服务**

以任意节点间的标签验证服务为基础，建立起规模化的**网络服务及动态订阅机制**，例如多粒度的源地址验证、转发路径验证、规模化VPN、灵活QoS服务等

复杂度分析

共识时间消耗

区块产生速率：目标Tps/（区块包含数据量）

区块大小：区块包含数据数*数据平均大小

区块包含数据数：包含数越多，被执行平均等待时间越久，但投票等消耗带宽量降低

每个节点维护邻居节点数为t（假设为8）

举例：如果目标Tps为10000T/s，假设数据平均大小为250B，区块包含10000笔数据，则Leader节点的带宽消耗为：8*(2.5MB+60B)/s，普通节点带宽消耗为平均（16*60B+2.5MB)/s，所以若总共有100个节点，对Leader节点带宽消耗为20MB/s，对普通节点带宽消耗为2.5MB/s

结论：地址域的维护信息是低频更新，分布式共识支撑SAVA-X的系统设计并不会带来额外的性能瓶颈

复杂度分析

- N个AS，两两维护状态机
- 某AS的每个AER存储所有其它AS对应的标签
- 单个AER
- 状态机存储
  - $O(2*(N-1))=O(N)$，2是同时可能有两个标签生效
- 状态机更新（更新需要遍历TAG表）
  - $O(2*(N-1)*(N-1))=O(N^2)$
- 验证

- 设信任联盟为L层，即联盟树形结构是高为L，N个叶子节点的满m叉树，最后一层联盟各节点都有相同的叶子节点个数$\left\lceil \frac{N}{m^{L-1}} \right\rceil$
- AER：最底层信任联盟内路由器，不进行标签替换
- TAER：每层信任联盟边界路由器，进行标签替换，AD-V→Alli
- 状态机存储
  - AER：$O\left(2\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)\right)=O\left(\frac{N}{m^{L-1}}\right) \overset{m=\sqrt[L]{N}}{\Longrightarrow} O\left(N^{\frac{1}{L}}\right)$
  - TAER：其最大时即从下向上一直作为跨联盟的TAER。

- 标签替换
  - AD_V标签的替换
  - 联盟标签替换
- 复杂度上届即最差情况下，是从一个最高级别子联盟下最层AD到达另外一个最高级别子联盟下的AD
  - 共需要$L-1$次标签替换：$L-2$次AD_V标签，1次联盟标签
  - $O\left((L-1)\cdot\left(2\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)+2(L-1)(m-1)+2\left((L-1)(m-1)+\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)\right)\right)\right) \overset{m=\sqrt[L]{N}}{\Longrightarrow} O\left(L\cdot N^{\frac{1}{L}}\right)$

- 验证开销
  - t_{SM}：标签查询单位开销，$\overline{S_{PRE}}$：层次信任联盟IP前缀数，是S_{PRE}(全局)的子集
  - t_{PRE}：IP前缀和所属AS对应关系查询单位开销，t_{OPE}：添加移除标签的单位开销
- 最低层次信任联盟内通信
  - $\overline{Cost_{max}}=2\cdot\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)\cdot t_{SM}+2\cdot\overline{S_{PRE}}\cdot t_{PRE}+2t_{OPE}$
- 跨信任联盟通信
  - $\overline{\overline{Cost_{max}}}=\left(\left(2\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)+2(L-1)(m-1)+2\left((L-1)(m-1)+\left(\left\lceil \frac{N}{m^{L-1}} \right\rceil -1\right)\right)\right)\right)\cdot t_{SM}+2\cdot(S_{PRE}+(L-2)\cdot\overline{S_{PRE}})\cdot t_{PRE}+2\cdot(L-1)\cdot t_{OPE}$

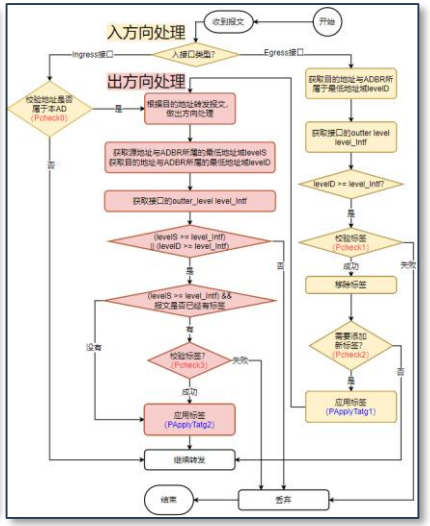
结论：对比传统方案，SAVA-X在数据**标签存储和更新复杂度上有指数降低**。而在通信开销方面，同层通信开销降低，**跨层通信开销上界则提升至L（联盟层数）的多项式倍**。

实现与标准化工作

SAVA-X实现


NIDTGA
用户总数
314,169
在线用户
12,330
异常用户
301,839
告警信息
515,927
设备总数
27,812
地址域总数
328,448
最大地址域层级
392,698
正在处理的域间共识请求
48,899
域间分布式共识基础设施
详情 »
顶级地址域[中国]: 100000
一级地址域[华北]: 1000001

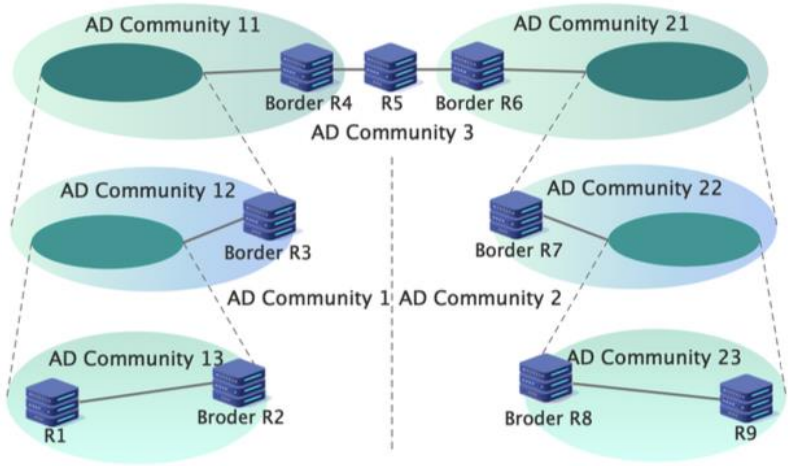

异常流量
可疑流量
安全流量
未保护流量
受保护流量
流量使用情况
2023-11-13
2023-11-21
发送流量
接收流量

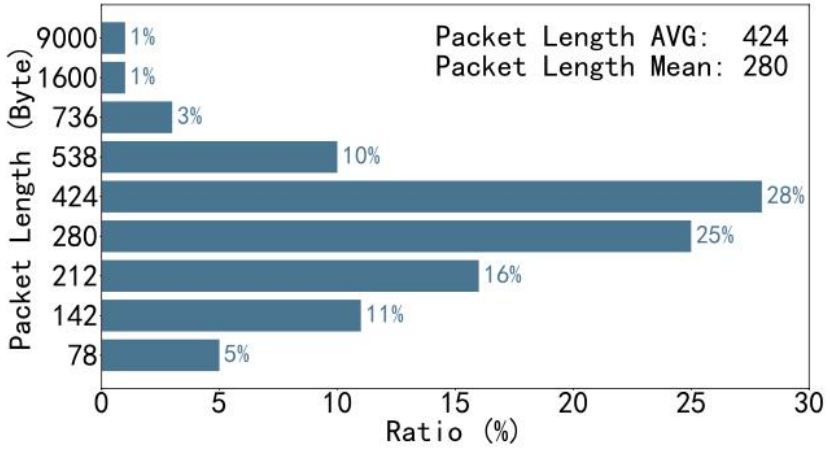

入方向处理
出方向处理
开始
收到报文
入接口类型?
Ingress接口
Egress接口
校验地址是否属于本AD (Pcheck0)
根据目的地址转发报文，做出方向处理
获取源地址与ADBR所属的最低地址域levelS
获取目的地址与ADBR所属的最低地址域levelD
获取接口的outter_level level_intf
(levelS >= level_intf) || (levelD >= level_intf)
(levelS >= level_intf) && 报文是否已经有标签
校验标签? (Pcheck3)
应用标签 (PApplyTaf2)
继续转发
结束
丢弃
获取目的地址与ADBR所属于最低地址域levelD
获取接口的outter level level_intf
levelD >= level_intf?
校验标签 (Pcheck1)
成功
失败
移除标签
需要添加新标签? (Pcheck2)
应用标签 (PApplyTaf1)


地址域详情
[中国]: 100000 > [华北]: 1000001
一级地址域[华北]: 1000001
ACS
AER
前缀
地址
公钥地址
5642:da92:e30e:800d:2d8b:7f3a:1857:f186
sBH2HLRFiKmMmfEwCfHgBfW2IJKqCNWnbbG5gJVb4JFtiRlohE/sbCAJQqCrIITJn29xvHqsS+PetJlRkbRFHP+rg2Tt20TtpC
设备位置
源地址验证使能
ffcf:e8cc:12f7:3e01:7005:320c:cf09:554e
内部
否
bdbc:c60c:7316:f498:dd35:3fd7:9a57:6873
是
前缀长度
是否活跃
6368:7f25:f02b:4545:946d:6b55:8920:e0b1
897
3d38:de8a:62f8:391a:dc08:e318:117c:9650
587
3fa9:e5ae:f8ce:1074:aa4d:13bf:21be:fe53
856
流量异常情况
2023-11-21
(根据所选日期展示当天的流量信息)


大数据可视化平台
节点数 0 0 3 5

SAVA-X实现

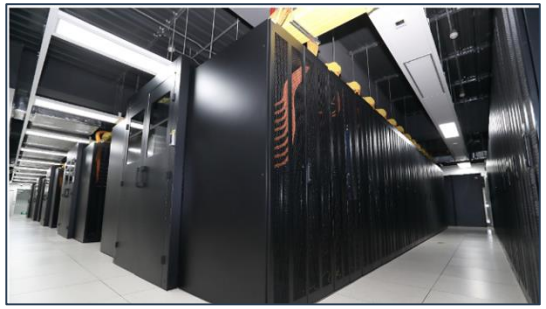


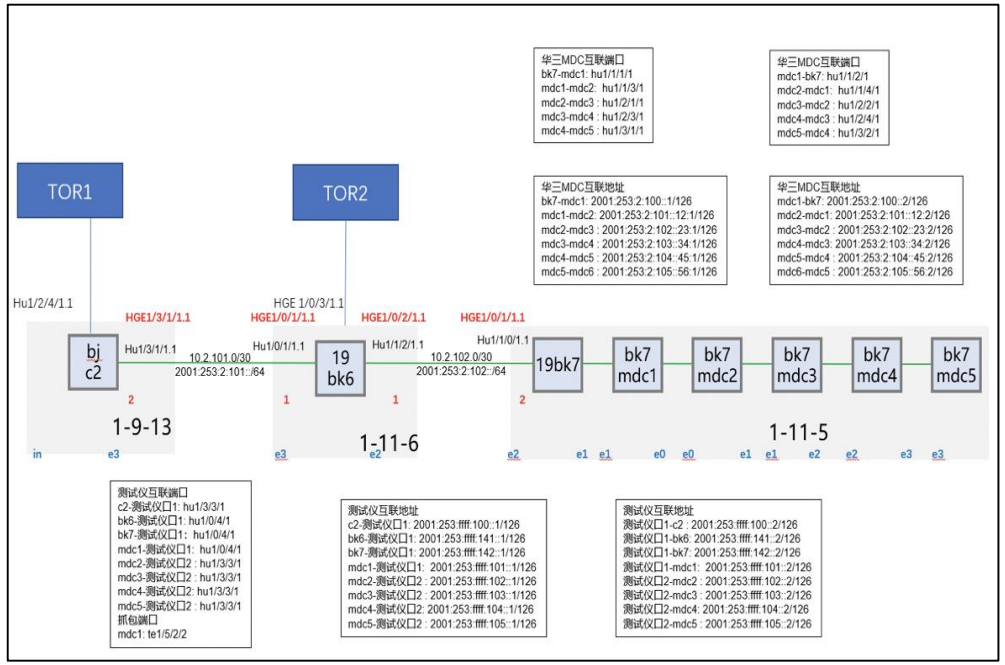


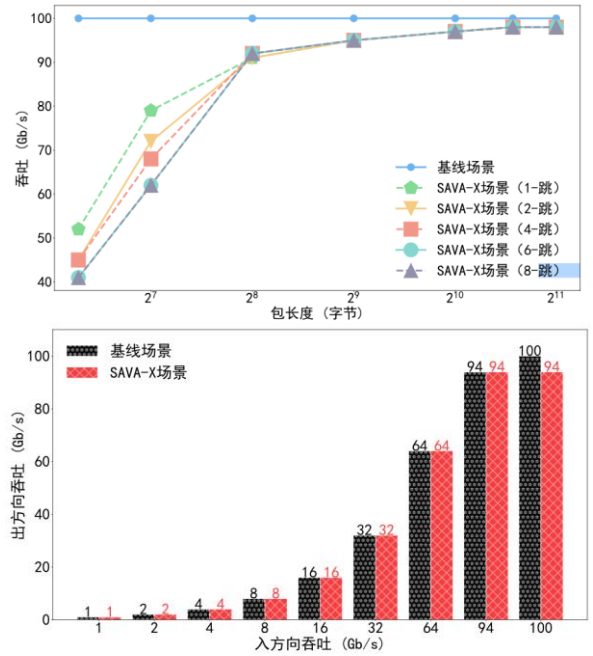
SAVA-X在CR19000系列核心路由器上，按照运营商真实数据包的大小占比，进行了三层共计9个AS的转发性能测试

结论：SAVA-X在商用路由平台上，可以支持单接口100Gbps的吞吐支持，延迟增加约0.07%。

SAVA-X实现







国家重大科技基础设施FITI，连接全国35个城市40所高校的核心节点，目前在清华节点完成**SAVA-X功能和基础性能测试**

SAVA-X标准化工作

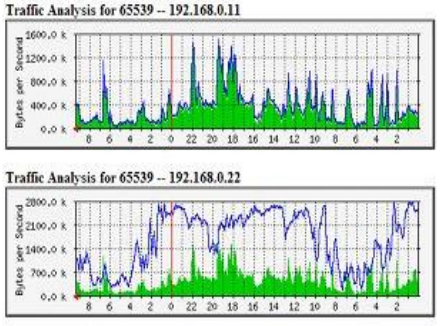
序号	项目编号	项目名称	牵头单位	标准编号
1	2022-1152T-YD	域间源地址验证(SAVA-X)技术要求 第5部分：地址域部署	清华大学	YD/T 4432.5-2023
2	2022-1151T-YD	域间源地址验证(SAVA-X)技术要求 第4部分：地址域的创建、选择和注册指南	清华大学	YD/T 4432.4-2023
3	2021-1010T-YD	域间源地址验证(SAVA-X)技术要求 第3部分：控制服务器和边界路由器通信协议	清华大学	YD/T 4432.3-2023
4	2021-1009T-YD	域间源地址验证(SAVA-X)技术要求 第2部分：数据平面	清华大学	YD/T 4432.2-2023
5	2021-1008T-YD	域间源地址验证(SAVA-X)技术要求 第1部分：控制平面	清华大学	YD/T 4432.1-2023

SAVA-X已推动CCSA立项7项，其中5项（控制平面、数据面平面、通信协议、地址域管理和部署）已正式确立为行业标准。目前正在IETF推动SAVA-X标准立项。

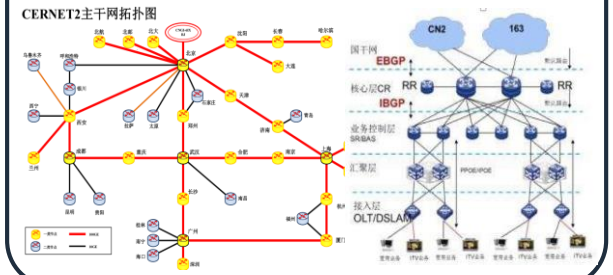
总结与展望

SAVA-X技术挑战与机制创新

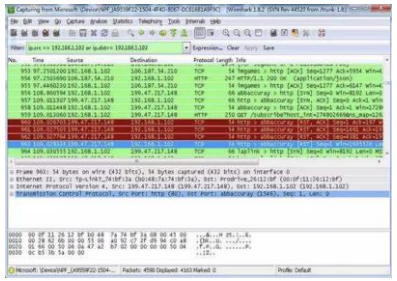
域间大吞吐的挑战



多运营商和大规模带来的扩展性的挑战



混合部署带来的防篡改防仿冒挑战



基于状态机源地址验证的高性能域间数据通路

基于分布式域间信任的地址域层次化扩展

数据包防篡改防伪造机制

分布式域间信任基础设施

SAVA-X技术展望

三大威胁

体系融合

机制设计

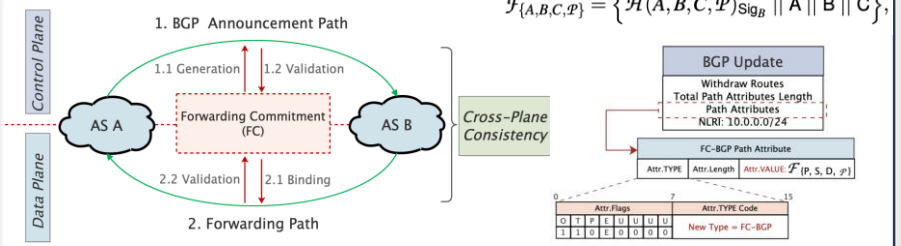
信任锚点

路由泄漏

路由劫持

源地址伪造

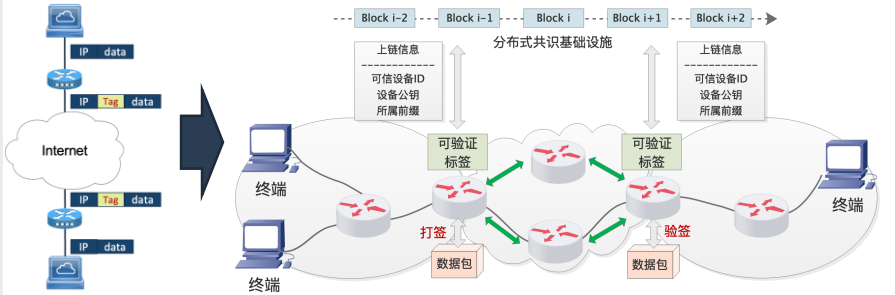
VRO 和 FC-BGP



$$\mathcal{F}_{\{A,B,C,\mathcal{P}\}} = \left\{ \mathcal{H}(A,B,C,\mathcal{P})_{\mathrm{Sig}_B} \,||\, \mathrm{A} \,||\, \mathrm{B} \,||\, \mathrm{C} \right\},$$

控制面信任机理和传递验证机制

SAVA-X



数据面真实性验证机制

分布式域间信任基础设施

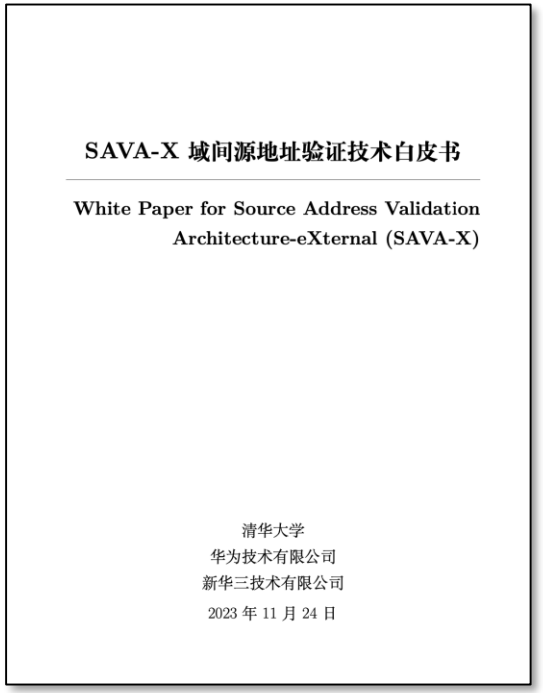
在统一技术体系中**融合控制面和数据面机制**，解决互联网三大安全挑战

SAVA-X技术白皮书

清华大学等共同发布了关于SAVA-X技术白皮书，从**技术背景、技术架构、层次化设计、实现与应用**等角度详细描述了SAVA-X的相关机制设计

白皮书下载网址：

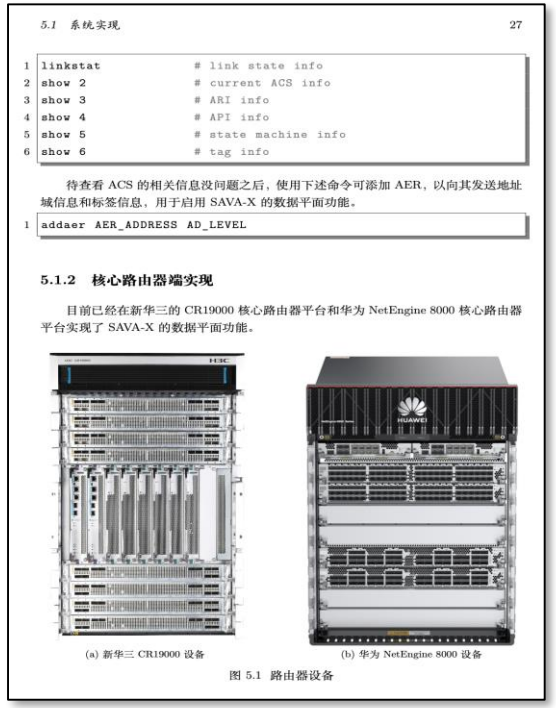
http://thucsnet.com/wp-content/papers/SAVA-X.pdf



SAVA-X 域间源地址验证技术白皮书

White Paper for Source Address Validation Architecture-eXternal (SAVA-X)

清华大学
华为技术有限公司
新华三技术有限公司
2023 年 11 月 24 日



5.1 系统实现 27

```
linkstat          # link state info
show 2            # current ACS info
show 3            # ARI info
show 4            # API info
show 5            # state machine info
show 6            # tag info
```

待查看 ACS 的相关信息没问题之后，使用下述命令可添加 AER，以向其发送地址域信息和标签信息，用于启用 SAVA-X 的数据平面功能。

```
addaer AER_ADDRESS AD_LEVEL
```

5.1.2 核心路由器端实现

目前已经在新华三的 CR19000 核心路由器平台和华为 NetEngine 8000 核心路由器平台实现了 SAVA-X 的数据平面功能。

(a) 新华三 CR19000 设备 (b) 华为 NetEngine 8000 设备

图 5.1 路由器设备

敬请批评指正

谢 谢！