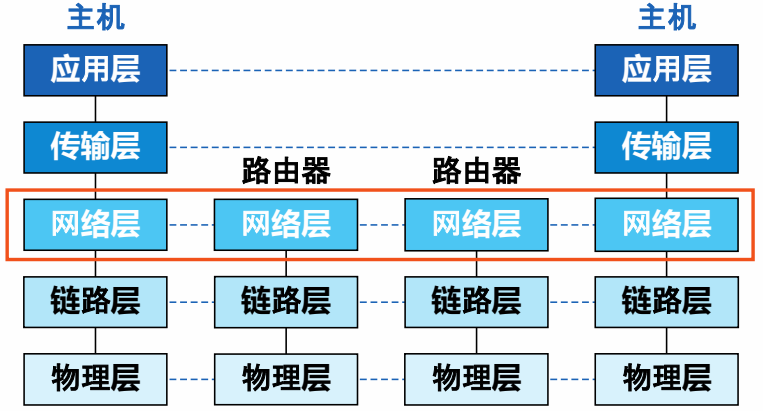
真实源地址验证

清华大学

互联网体系结构是互联网的核心技术

- 互联网体系结构研究互联网各部分功能组成及其相互关系
- 网络层承上启下，保证全网通达，是体系结构的核心
- 网络层设计包括传输格式、转发方式、以及路由控制

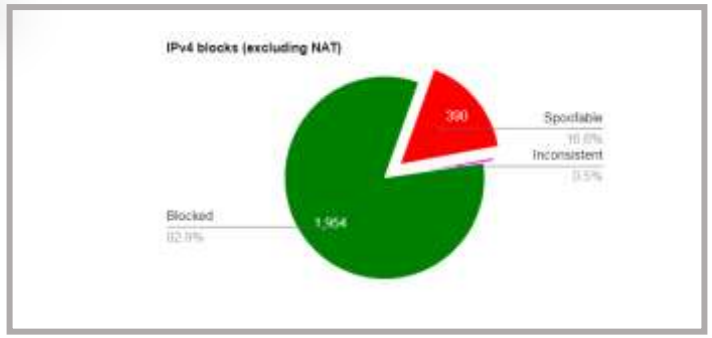


体系结构设计

- **与通信技术无关**：仅转发数据包，可运行于任何通信技术之上
- **与边缘创新无关**：增加边缘创新应用/服务，网络无需做任何改变
- **支持大规模扩展**：支持十亿级规模扩展
- **完全开放**: 对所有新协议、新技术、新应用提供开放服务

Vinton Cerf

互联网体系结构安全现状

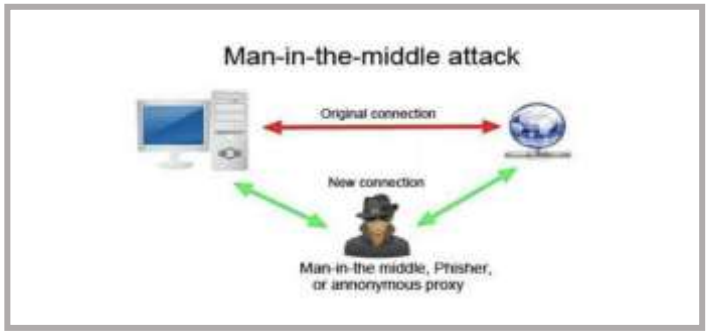


地址易被伪造

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

本章的内容组织

第一节
真实源地址验证体系结构设计背景

- IP地址欺骗
- 真实源地址验证体系结构SAVA的产生

回顾历史，分析当前互联网源地址易被伪造的原因

第二节
真实源地址验证体系结构设计原则

- 当前互联网的地址结构
- 真实源地址验证SAVA体系结构设计原则

总揽全局，提炼真实源地址验证体系结构设计原则

第三节
SAVA体系结构、关键技术、应用与推广

- 真实源地址验证SAVA体系结构
- 动态自适应的地址分配分组监听
- 分布式路由同步
- 域间层次化联盟
- 应用与推广

全面认识，了解SAVA体系结构的各个层次

针对地址易被伪造原因设计针对性对策

根据设计原则构建SAVA总体结构

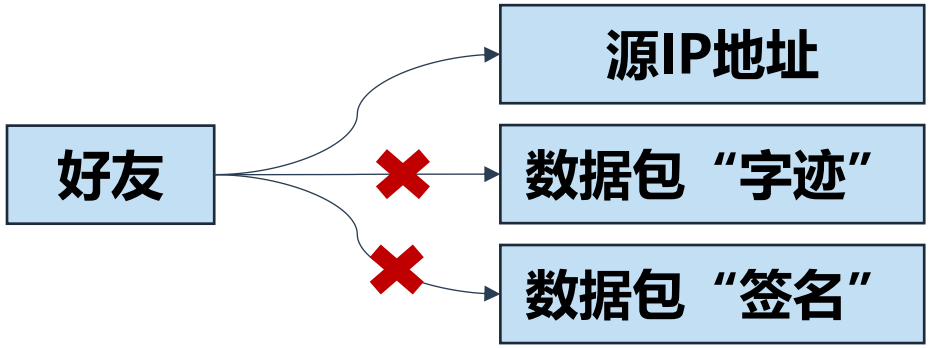
第1节　真实源地址验证体系结构设计背景

- IP地址欺骗
- 真实源地址验证体系结构SAVA的产生

IP通信可靠性

IP通信中信任关系的转移

- IP数据包都是01序列，也就是大家的“字迹”都是相同的
- IP数据包头中不携带签名信息，也就是“签名”是不存在的



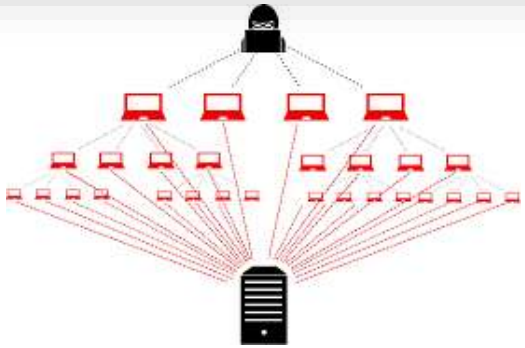
IP通信中信任关系只转移到了IP地址，也就是发件人地址上。但这是不可靠的！

- 伪造源IP地址是非常简单的，构造IP数据包头时可以随意填一个IP地址
- 网关在进行数据包转发时，**不会验证**数据包中源IP地址是否来自网关所在的局域网中

基于IP地址伪造的攻击

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

- 攻击者随机伪造许多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目的主机
- 猜测出被攻击主机和目的主机之间连接标识信息，达到与目的主机连通
- 向目的主机发送恶意脚本执行恶意指令，实现破坏目的主机，获取机密信息，甚至控制目的主机

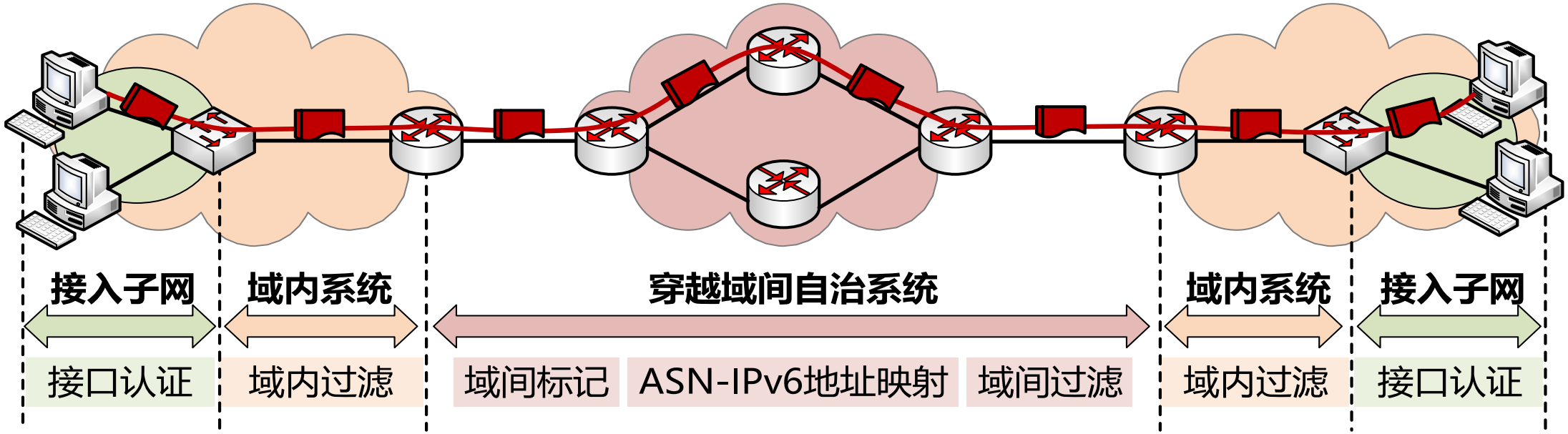
网络攻击现状 https://horizon.netscout.com/

现有IP地址伪造防御方法缺陷

- 现有源地址验证技术相互独立，只能部分地解决源地址验证的问题，没有形成一个完整的覆盖整个网络的整体结构
- 同时存在以下问题：
  - **算法复杂、协议开销大**
  - **缺乏部署激励**
  - **完备性不足**
  - **可扩展性不足**
  - ……

真实源地址验证体系结构SAVA

- 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。
  - 分层次的源地址保障方案设计SAVA（RFC5210）
  - 接入网内监听地址分配控制报文，动态绑定端设备IP与通信端口 （SAVI） （RFC 7039）
  - 自治域间建立信任联盟实现源地址验证（SAVA-X）



第2节 真实源地址验证体系结构设计原则

- 当前互联网的地址结构
- 真实源地址验证SAVA体系结构设计原则

自治域

- 出于管理的便利性和扩展目的，全球的互联网被分成很多自治域AS（Autonomous System）。一个自治域可以是一个简单的网络，也可以是一个或多个实体管理控制的网络群体
- 同一自治域内的网络具有相同的域内路由IGP协议，如OSPF、RIP等，自治域间采用域间路由策略BGP协议
- 运营商、机构、公司等都可以申请自治系统号ASN，各自分配的IP地址被清楚标记归属哪个ASN。截止到2021年1月，全球共分配177776个ASN，其中中国占2883个

- **划分自治域后，路由器只需要保存本自治域内的链路状态，因此路由器存储、更新、查询的资源占用保持在合理区间内，整个网络路由更加快捷**
- **自治域也为网络的个性化提供了可能。自治域内路由策略修改不影响网络其他部分，每个自治域可以根据自身需求采用不同的路由策略**

SAVA设计原则-可扩展性

SAVA体系结构是可演进的体系结构，应具备可扩展性以适应复杂的网络环境以及新的需求，支持在整个互联网不同位置、不同粒度需求的大规模部署

当前网络在可部署性上并不是均匀的，在部分区域，能够做到主机粒度的验证，但是很多区域却很难控制

需要划分灵活可变的源地址验证粒度，满足不同部署区域的需求和整体架构的可扩展性需求

IP网络是一个扁平化的结构，但是扁平的源地址验证结构会导致每一个验证实体具备所有对等实体的信息来完成验证

需要建立层次化，寻找合理的层次间关系，使得各层之间可以共同协作，同时避免层次之间的过度依赖

SAVA设计原则-可演进

与已有协议兼容

SAVA体系结构建立在当前互联网体系结构基础上，整体的技术依附于现有体系结构实现，因此必须要求技术对应协议与现有体系结构协议兼容

自身部署可演进

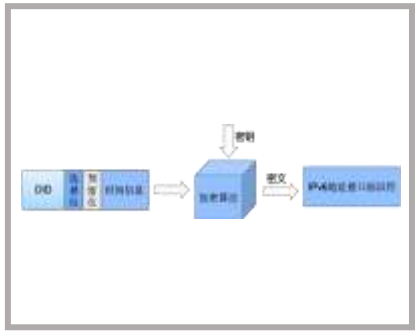
SAVA的部署是一个持续性的过程，所以会出现部分区域已经部署SAVA，而部分区域尚未部署SAVA的情况，需要考虑在发展部署的过渡阶段SAVA自身的兼容性

运营商之间可演进

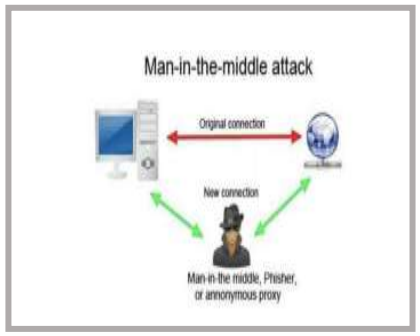
考虑到网络中不同运营商的存在，SAVA体系结构还应允许运营商可以采用各自不同的实现，SAVA系统各部分相互独立，且功能彼此不依赖

SAVA设计原则-安全性

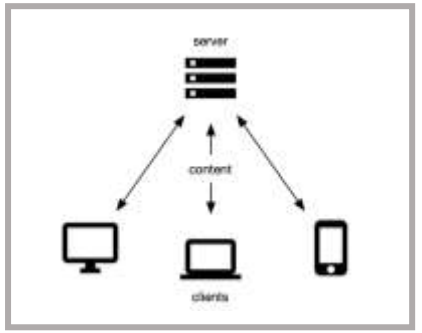
- SAVA体系结构的构建是支撑真实可信互联网体系结构实现，通过将安全性赋予现有体系结构，弥补其信任缺失的问题，所以保障SAVA自身的安全性至关重要
- 可信标识风险
  - 标识应当具备唯一性、可追溯性
- 数据转发风险
  - 需保证携带标签的数据包转发中不被篡改，即使篡改也应被及时并准确地识别
- 单点信任风险
  - 标签的验证应当不依赖于中心化的网络基础设施，以免引入网络基础设施的信任风险



可信标识风险

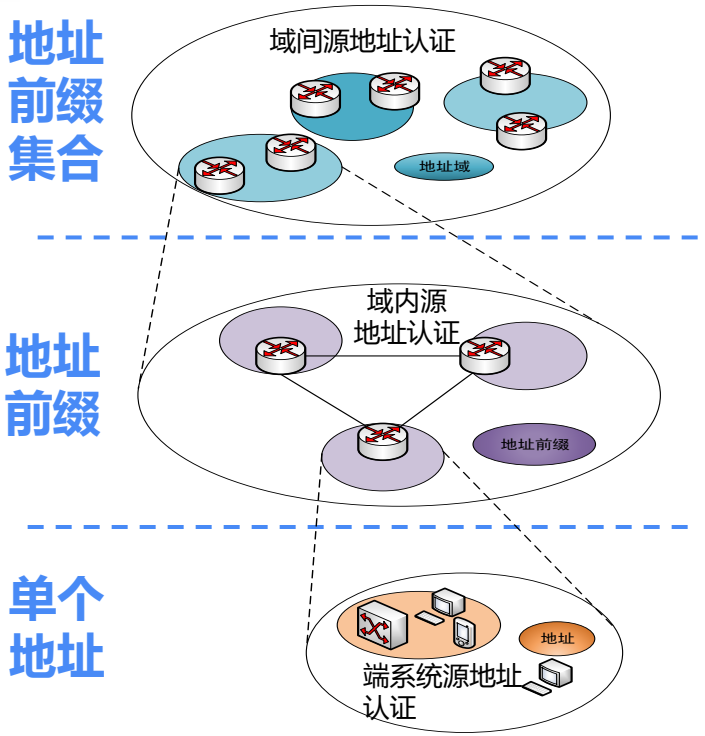


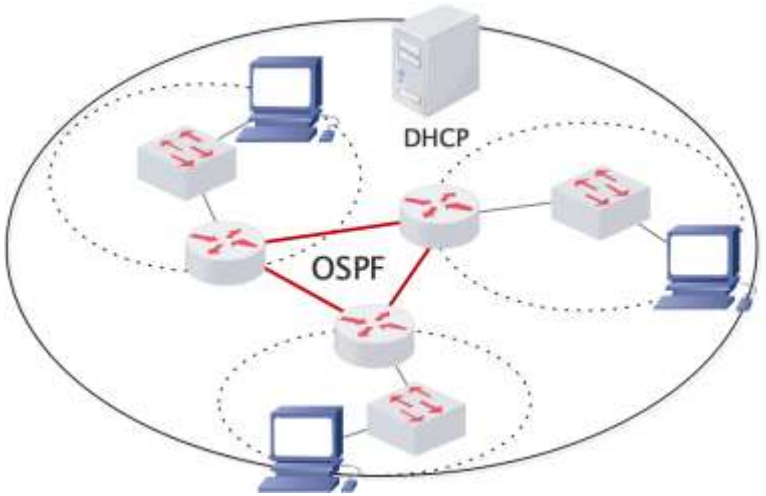
数据转发风险

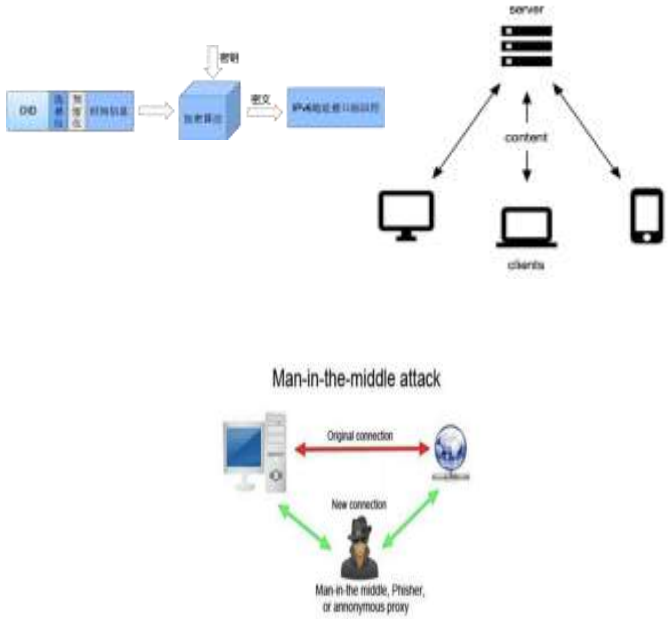


单点信任风险

真实源地址验证体系结构SAVA设计原则







“单个地址-地址前缀-地址前缀集合” 分层协作

演进式创新

安全性

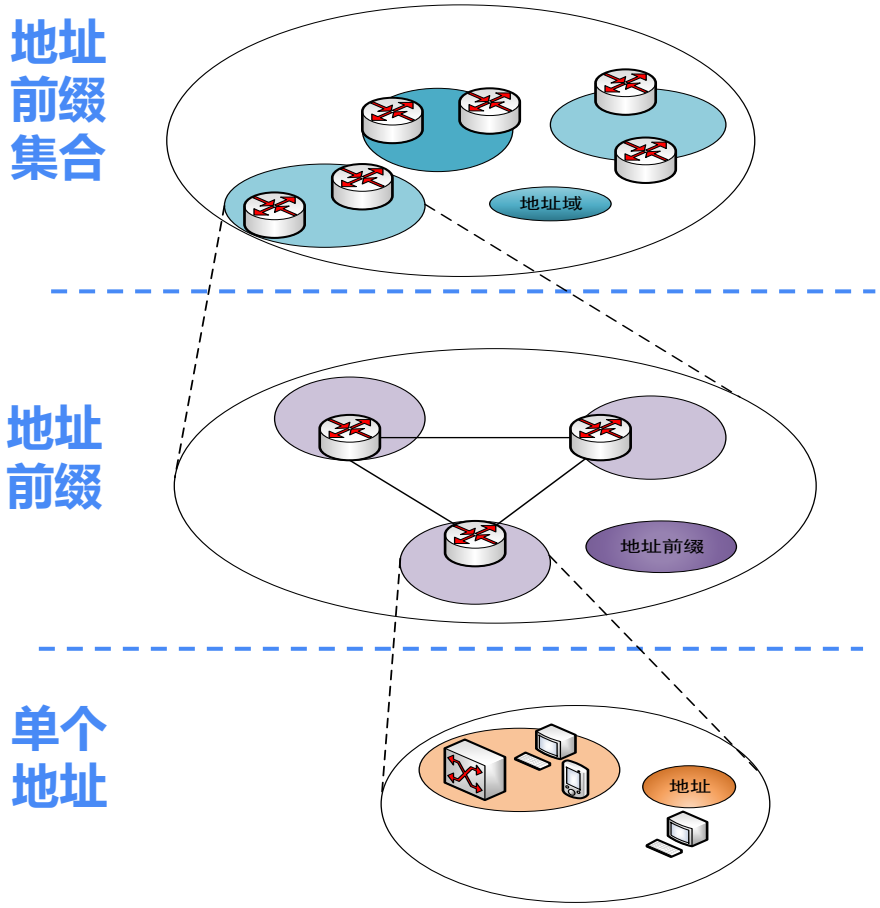
第3节 SAVA体系结构及其关键技术

- 真实源地址验证SAVA体系结构
- 动态自适应的地址分配分组监听
- 分布式路由同步
- 域间层次化联盟
- 应用与推广

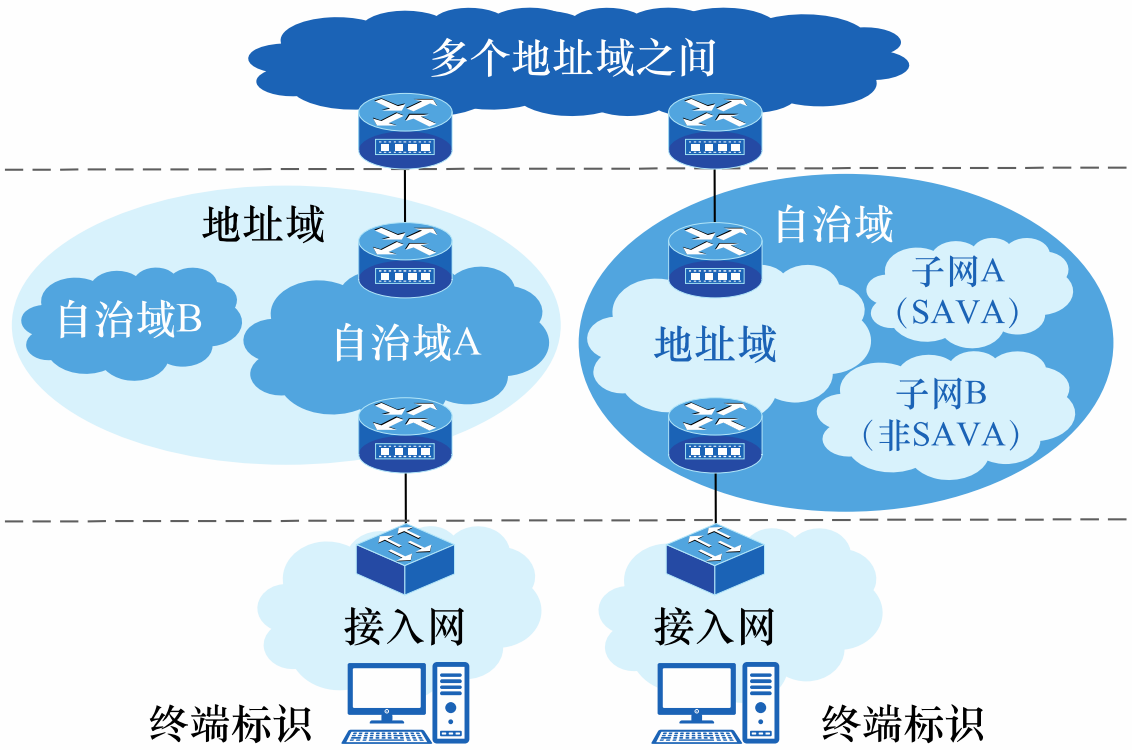
面向地址域的新型源地址验证SAVA体系结构

地址域：同一机构所属的全部IP地址中的可部分管理范围

- 以一个校园网为例，地址域可以是某一个院系下的某个所某个组，也可以是某个所、某个院系，甚至可以是整个校园网
- “地址域”显著提升体系结构的灵活性，实现了部署结构灵活的源地址真实性验证体系结构
- 接入网、地址域内和地址域间三层结构，具有**松耦合、多重防御、支持增量部署**等优点



面向地址域的新型源地址验证SAVA体系结构



SAVA-X (eXternal)
地址域间源地址验证
IPv6地址前缀集合粒度

- 在地址域间层面提供地址域级别的联盟内可验证能力以及保护自身不被伪造的能力

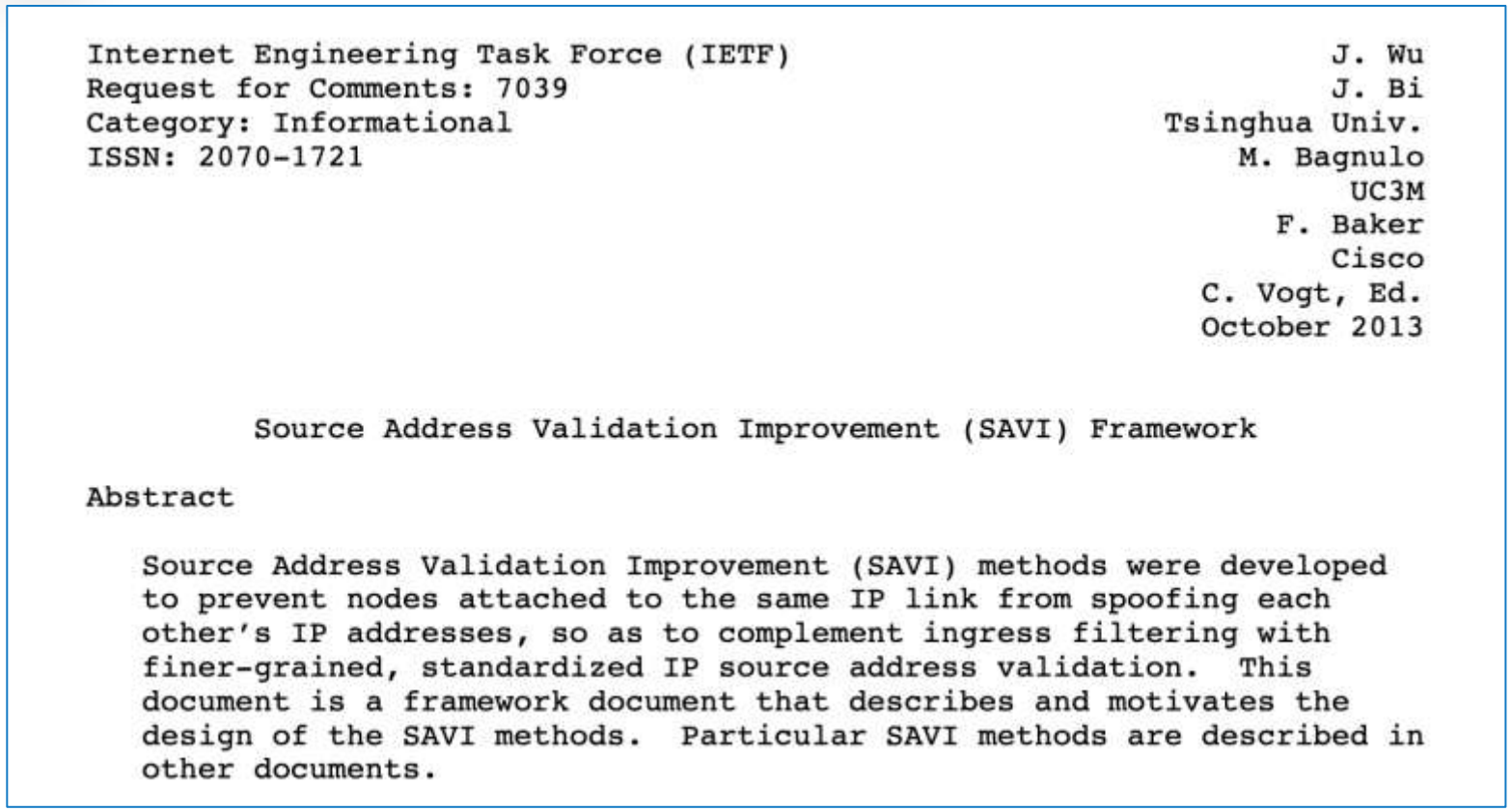
SAVA-P (Prefix)
地址域内源地址验证
IPv6地址前缀粒度

- 在地址域内层面提供前缀级别的保护能力，以保护核心设备不被攻击

SAVA-A (Access)
接入网内源地址验证
IPv6地址粒度
与终端标识绑定并携带

- 接入层面提供主机粒度的源地址验证能力，以保证地址使用的可追溯性

接入网真实源地址验证技术SAVI



Internet Engineering Task Force (IETF)
Request for Comments: 7039
Category: Informational
ISSN: 2070-1721

J. Wu
J. Bi
Tsinghua Univ.
M. Bagnulo
UC3M
F. Baker
Cisco
C. Vogt, Ed.
October 2013

Source Address Validation Improvement (SAVI) Framework

Abstract

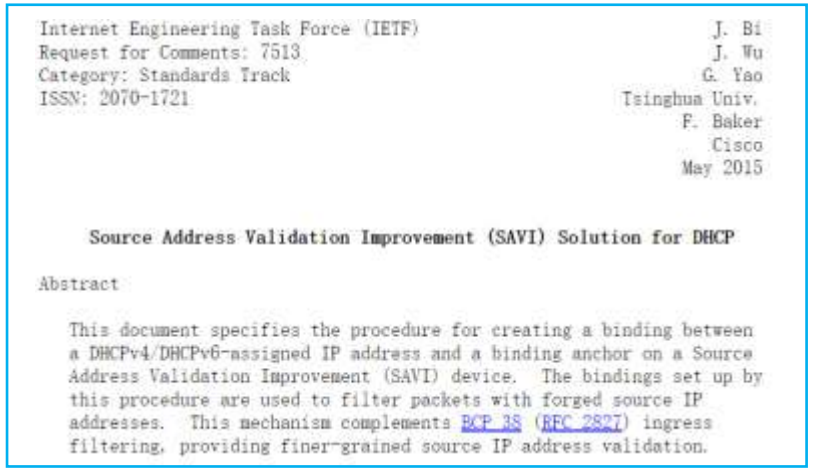
Source Address Validation Improvement (SAVI) methods were developed to prevent nodes attached to the same IP link from spoofing each other's IP addresses, so as to complement ingress filtering with finer-grained, standardized IP source address validation. This document is a framework document that describes and motivates the design of the SAVI methods. Particular SAVI methods are described in other documents.

RFC 7039: Source Address Validation Improvement (SAVI) Framework

- 提供端系统粒度的源地址验证
- 无需主机参与，完全依赖网络实现
- 以此为基础，可以提供对用户的追溯、计费、审计等能力
- 基于报文监听生成绑定表的技术方案SAVI-CPS（Control Packet Snooping）
- 被IETF SAVI工作组采纳成为工作组系列标准

SAVI验证方式

- 针对多种接入网技术、多种地址分配方式、多种终端类型，SAVI设计了**各种对应的验证方式**
  - 所有相关网络设备在同一个网络管理机构管理控制下
  - 解决方案与接入子网地址管理分配和控制策略密切相关
  - 解决方案与端系统的接入方式密切相关



Internet Engineering Task Force (IETF)
Request for Comments: 7513
Category: Standards Track
ISSN: 2070-1721

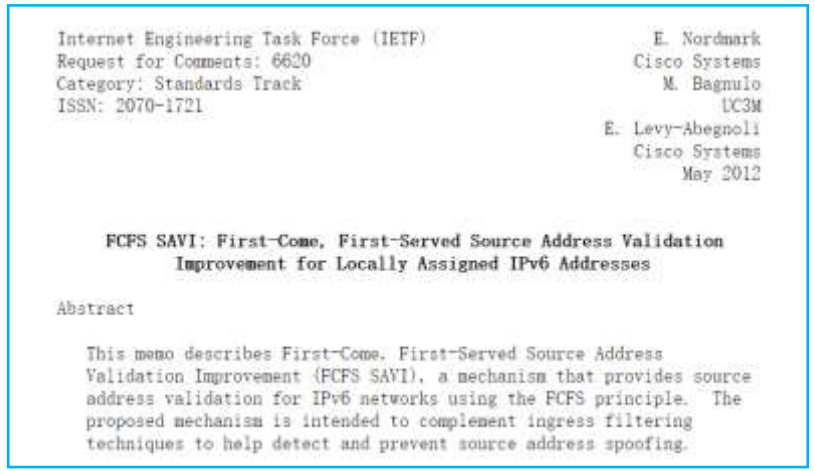
J. Bi
J. Wu
G. Yao
Tsinghua Univ.
F. Baker
Cisco
May 2015

Source Address Validation Improvement (SAVI) Solution for DHCP

Abstract

This document specifies the procedure for creating a binding between a DHCPv4/DHCPv6-assigned IP address and a binding anchor on a Source Address Validation Improvement (SAVI) device. The bindings set up by this procedure are used to filter packets with forged source IP addresses. This mechanism complements BCP 38 (RFC 2827) ingress filtering, providing finer-grained source IP address validation.

SAVI-DHCP (RFC 7513)
DHCP场景下的绑定建立和验证问题



Internet Engineering Task Force (IETF)
Request for Comments: 6620
Category: Standards Track
ISSN: 2070-1721

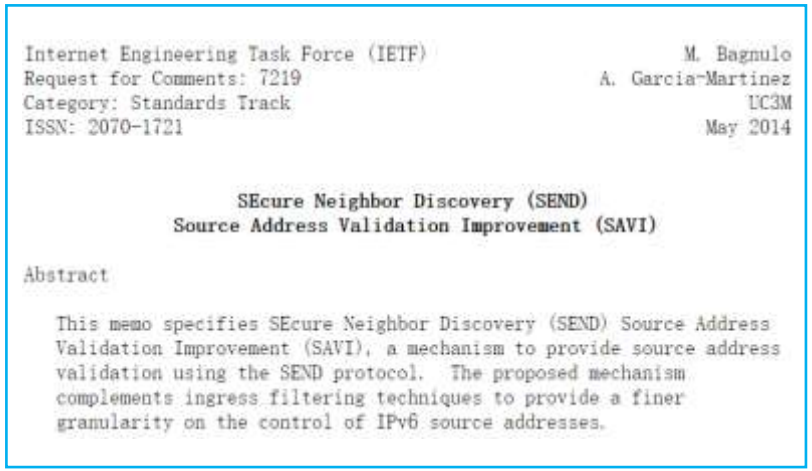
E. Nordmark
Cisco Systems
M. Bagnulo
UC3M
E. Levy-Abegnoli
Cisco Systems
May 2012

FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses

Abstract

This memo describes First-Come, First-Served Source Address Validation Improvement (FCFS SAVI), a mechanism that provides source address validation for IPv6 networks using the FCFS principle. The proposed mechanism is intended to complement ingress filtering techniques to help detect and prevent source address spoofing.

FCFS SAVI (RFC 6620)
无状态地址分配场景下的绑定建立和验证问题



Internet Engineering Task Force (IETF)
Request for Comments: 7219
Category: Standards Track
ISSN: 2070-1721

M. Bagnulo
A. Garcia-Martinez
UC3M
May 2014

SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI)

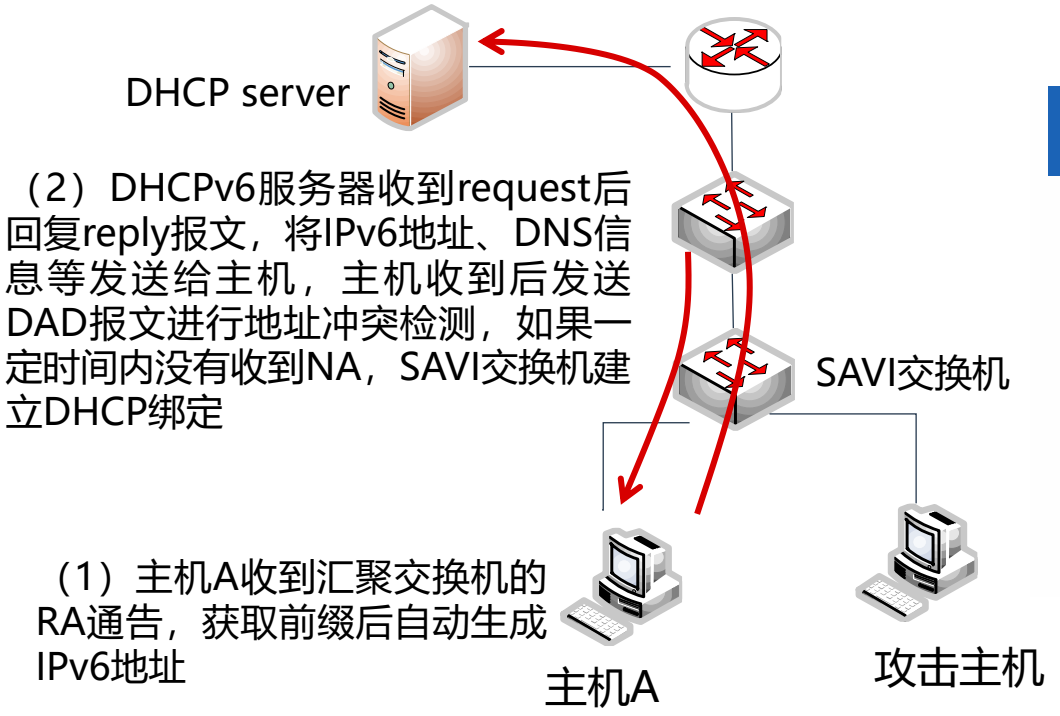
Abstract

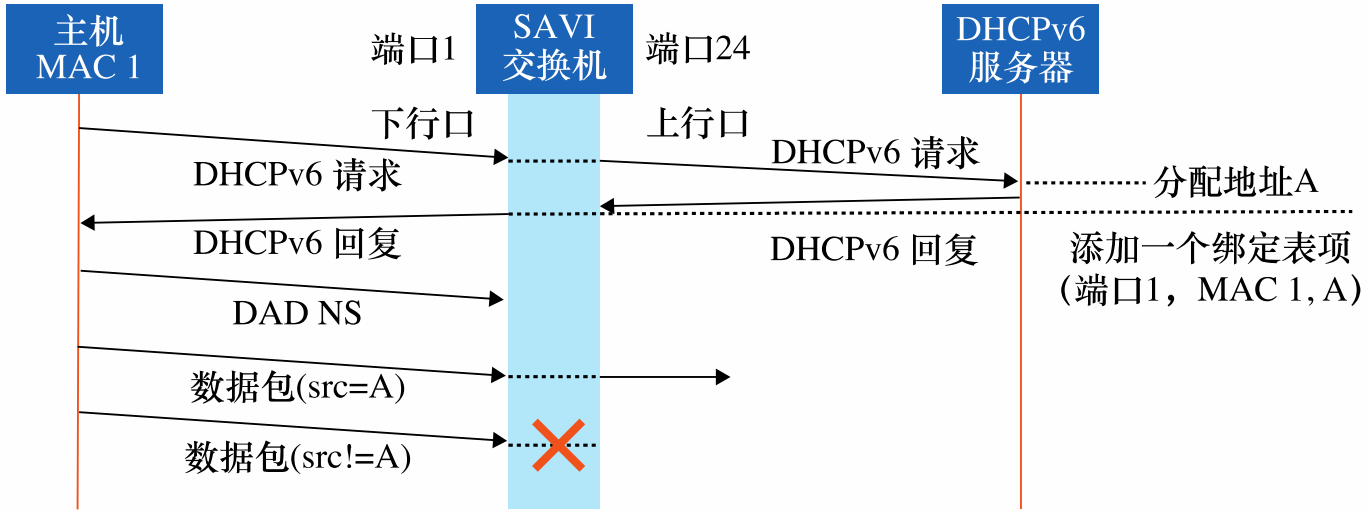
This memo specifies SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI), a mechanism to provide source address validation using the SEND protocol. The proposed mechanism complements ingress filtering techniques to provide a finer granularity on the control of IPv6 source addresses.

SEND SAVI (RFC 7219)
SEND地址分配场景下的绑定建立和验证问题

SAVI-DHCP(RFC 7513)

- 部署在接入设备上，网络中包含DHCP服务器、接入交换机、无线接入点等
- 通过执行DHCPv4/v6监听建立DHCP分配的地址和主机对应的绑定锚之间的绑定关系，用来验证报文中源地址的真实性





域内真实源地址验证技术SAVA-Prefix

技术目标

- 如果一个地址域与接入网相连，需保证从接入网流入地址域的流量，其源地址不会假冒该接入网之外的地址
- 如果接入网部署了SAVI，进行二次验证
- 如果接入网没有部署SAVI，缩小源地址假冒的范围（接入网级别）
- 保证从地址域内产生并流出地址域的流量，其源地址不会假冒地址域之外的地址

精准过滤

- 地址过滤的精确率（precision）100%
- 地址过滤的召回率（recall）100%

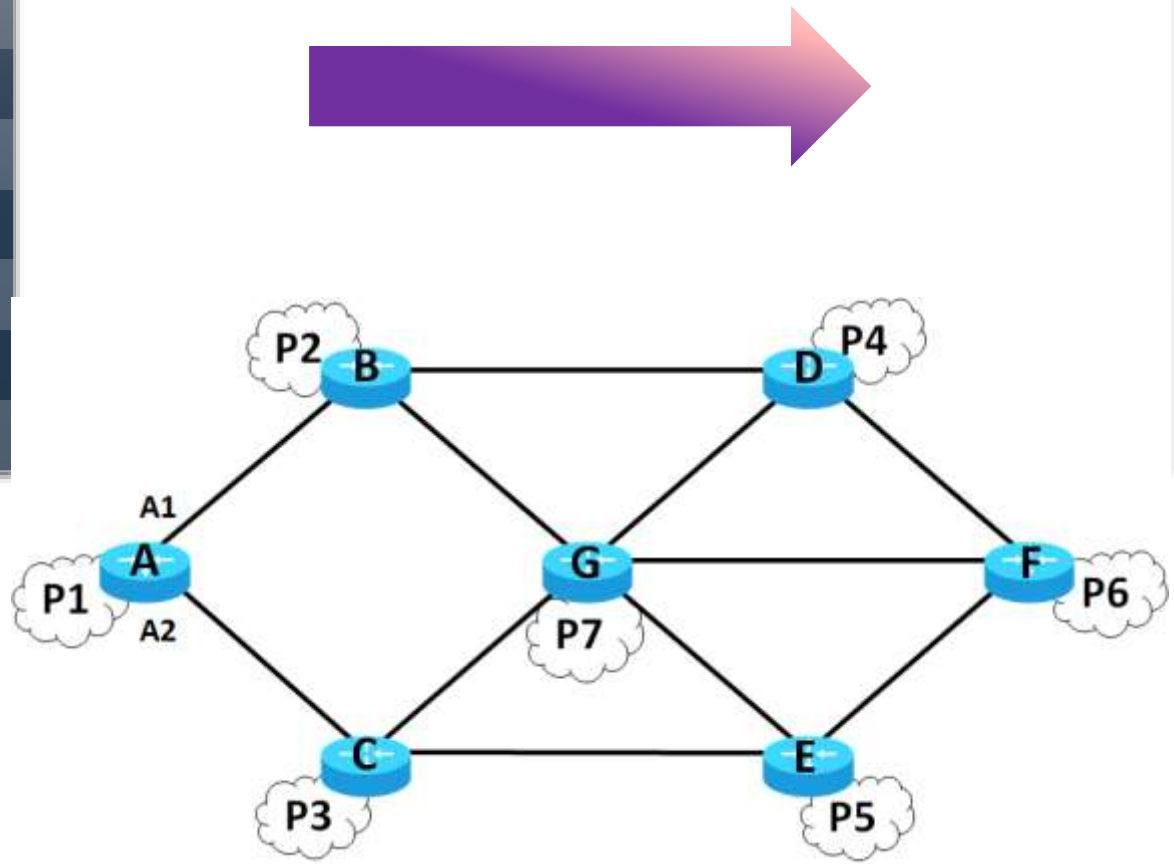
自动更新

- 自适应接入网地址分配和域内路由策略的动态更新，不完全依赖手动配置

SAVA-P：源地址验证表

根据目的地址选择分组的出接口（**路由转发表**）

FIB for A	
Dest Prefix	Next hop
P2	B
P3	C
P4	B
P5	C
P6	B
P7	B



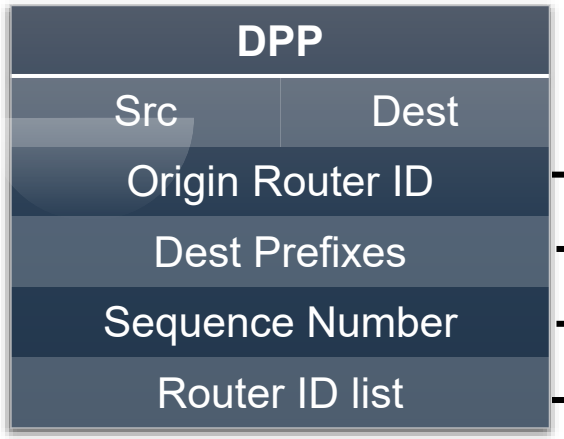
根据源地址验证分组的入接口（**源地址验证表**）

SAV table for A	
Src Prefix	Incom. Int.
P2	A1
P3	A2
P4	A1
P5	A2
P6	A2
P7	A2

基本框架

- Bootstrapping

路由器生成并发送SPA(source prefix advertisement)报文，广播路由器源前缀和路由器IP地址

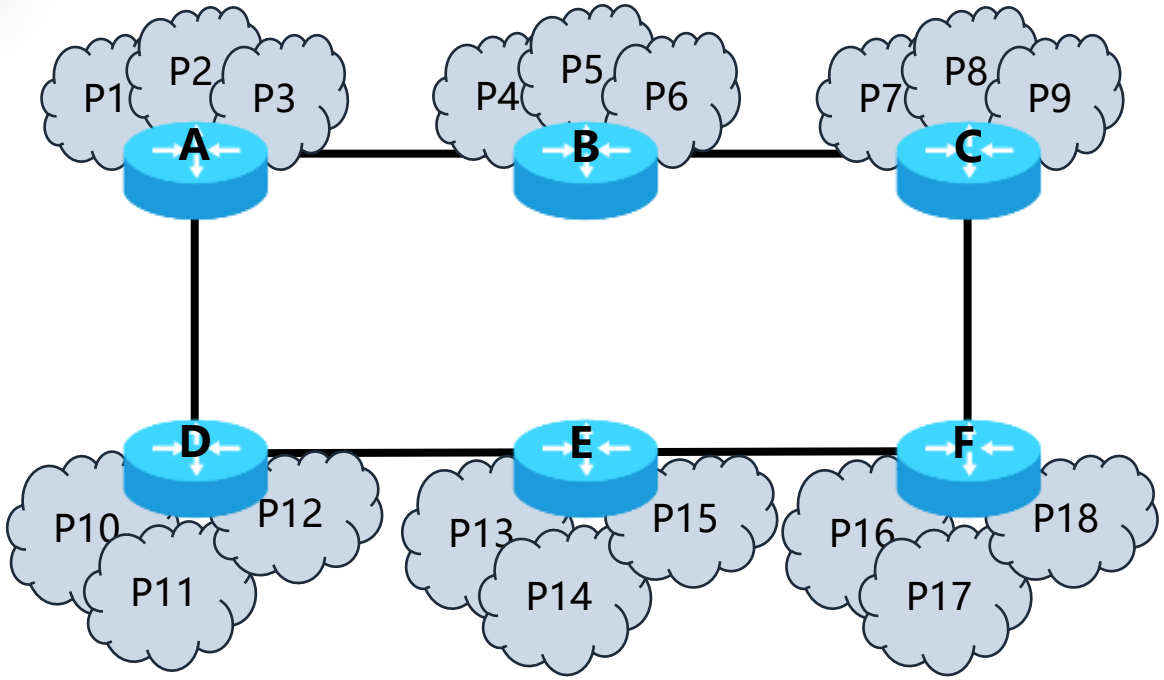


- 生成源地址验证表
- 指导接力发送
- 标识更新
- 路由环路检测

路由器基于本地FIB生成原始DPP报文并发送给邻居路由器

邻居路由器处理DPP报文，生成源地址验证表SAV并接力发送DPP报文

开销分析



Routing Table for A	
Dest	Next Hop
P4,P5,P6, P7,P8,P9	B
P10,P11,P12, P13,P14,P15, P16,P17,P18	D

假设域内路由器节点的数量是N，边的数量是E，路由器平均直连前缀的数量是K

方案	单节点处理的协议报文数量	单节点计算开销
SAVE	$O(K*N^2)$	O(1)
O-CPF	O(K*N)	最小 O(N*K*E)
本方案	O(N)	O(1)

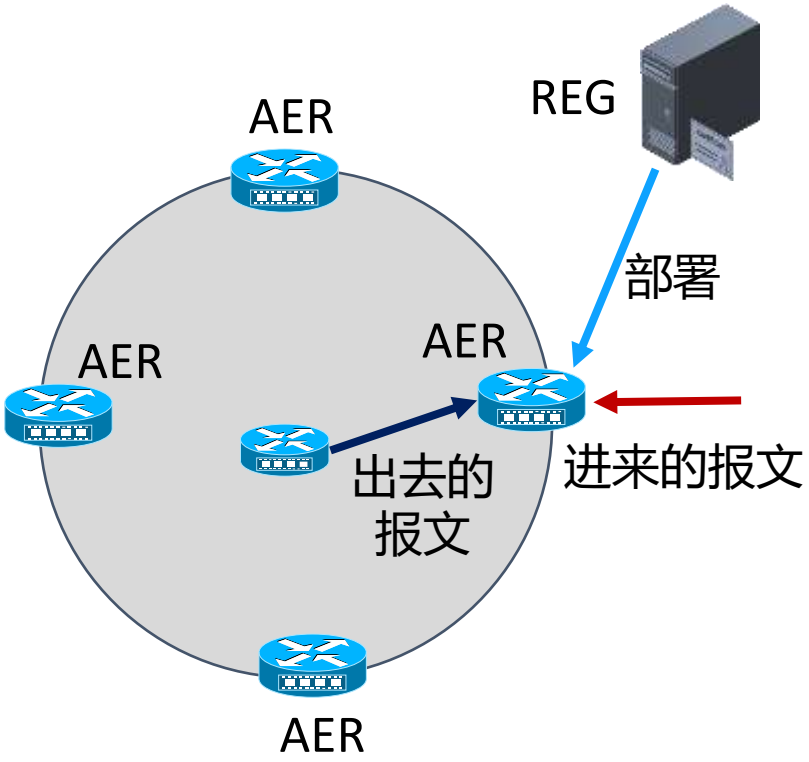
方案总结

设计目标	uRPF [RFC 3704, 8704]	SAVE [INFOCOM 2002]	O-CPF [CFI 2013]	SAVA-P
正确性 (解决路由不对称问题)	X	√	√	建立与转发表方向相反的源地址验证表，克服路由不对称问题
低开销 (通信开销和计算开销)	√	X	X	每台路由器处理的协议报文数量约为O(N)，N为网络内的路由器数量

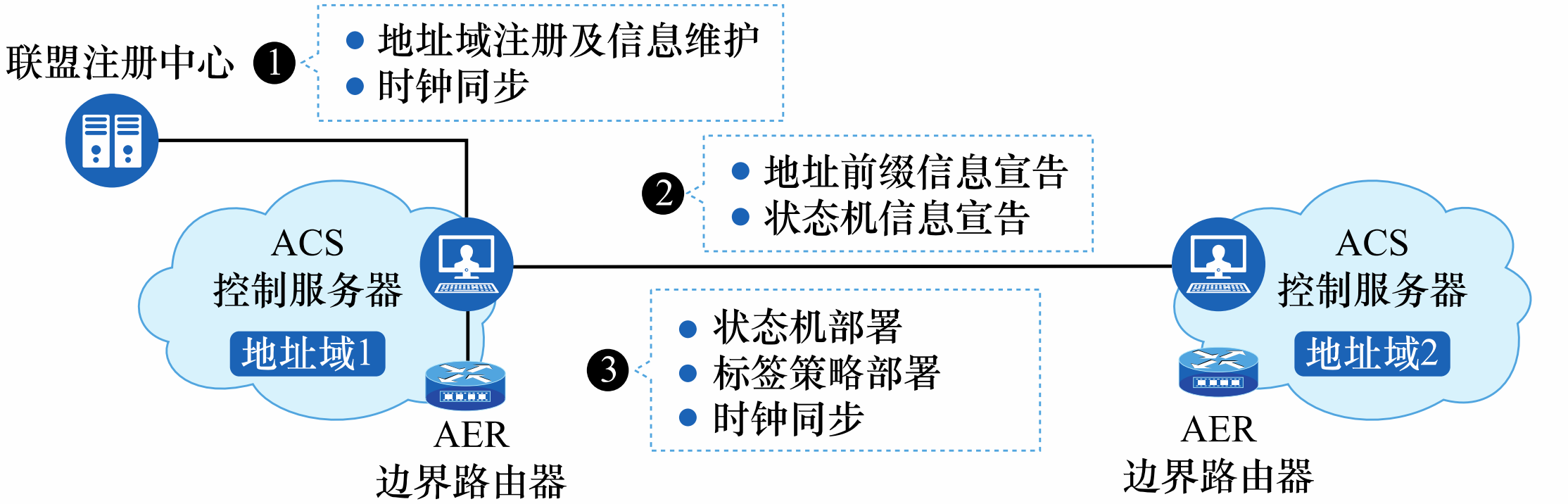
域间真实源地址验证技术SAVA-X

SMA （State Machine based Anti-spoofing）

- 通过在地址域之间建立信任联盟实现源地址验证，部署在联盟成员的边界路由器上
- 边界路由器为本域内发往其它联盟成员的报文进行地址域级别的源地址前缀检查，保证源自本地址域的报文携带的源地址确实属于本地址域
- 边界路由器为源自本地址域、宿于其它成员地址域的报文添加用以标识本地址域身份的**“标签”**，该标签可验证，确保地址域地址前缀不被冒用



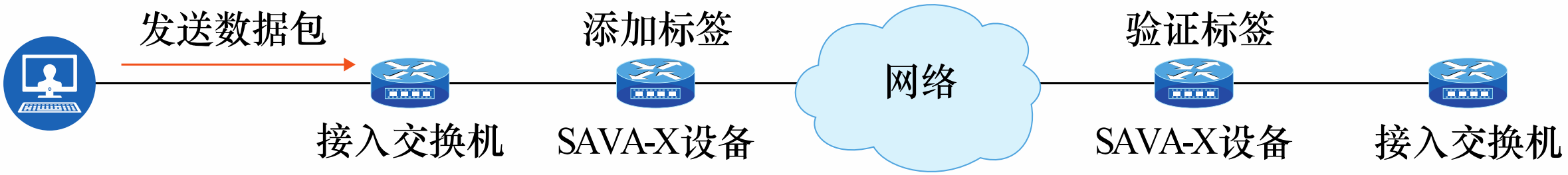
SAVA-X控制层



1 联盟成员注册与管理 | 2 状态机协商与同步 | 3 边界路由器配置

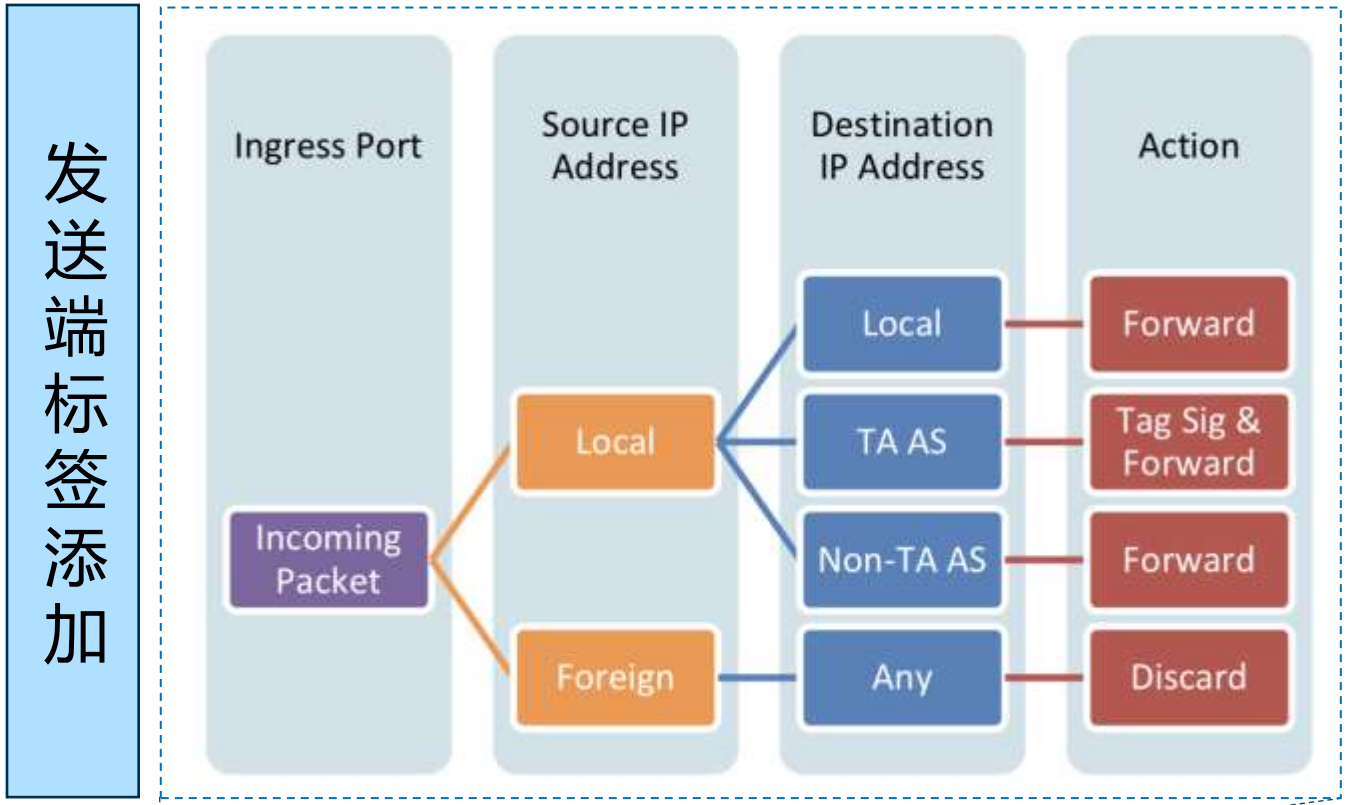
SAVA-X数据层

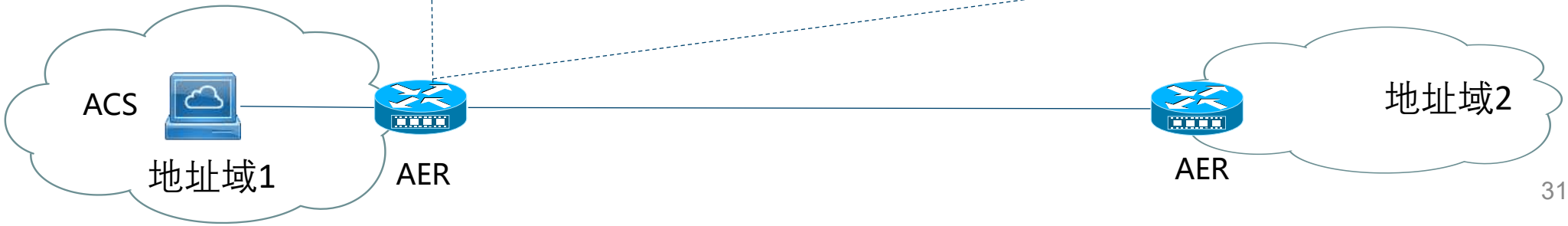
- 数据层面的参与主体是成员地址域的边界路由器，它主要负责**标签**的添加、验证和移除
- 发送方边界核心路由器在报文中添加标签，以传递源地址前缀的真实性
- 目的域在边界路由器检查标签正确性，以验证所关联源地址的真实性，过滤伪造报文



SAVA-X数据转发

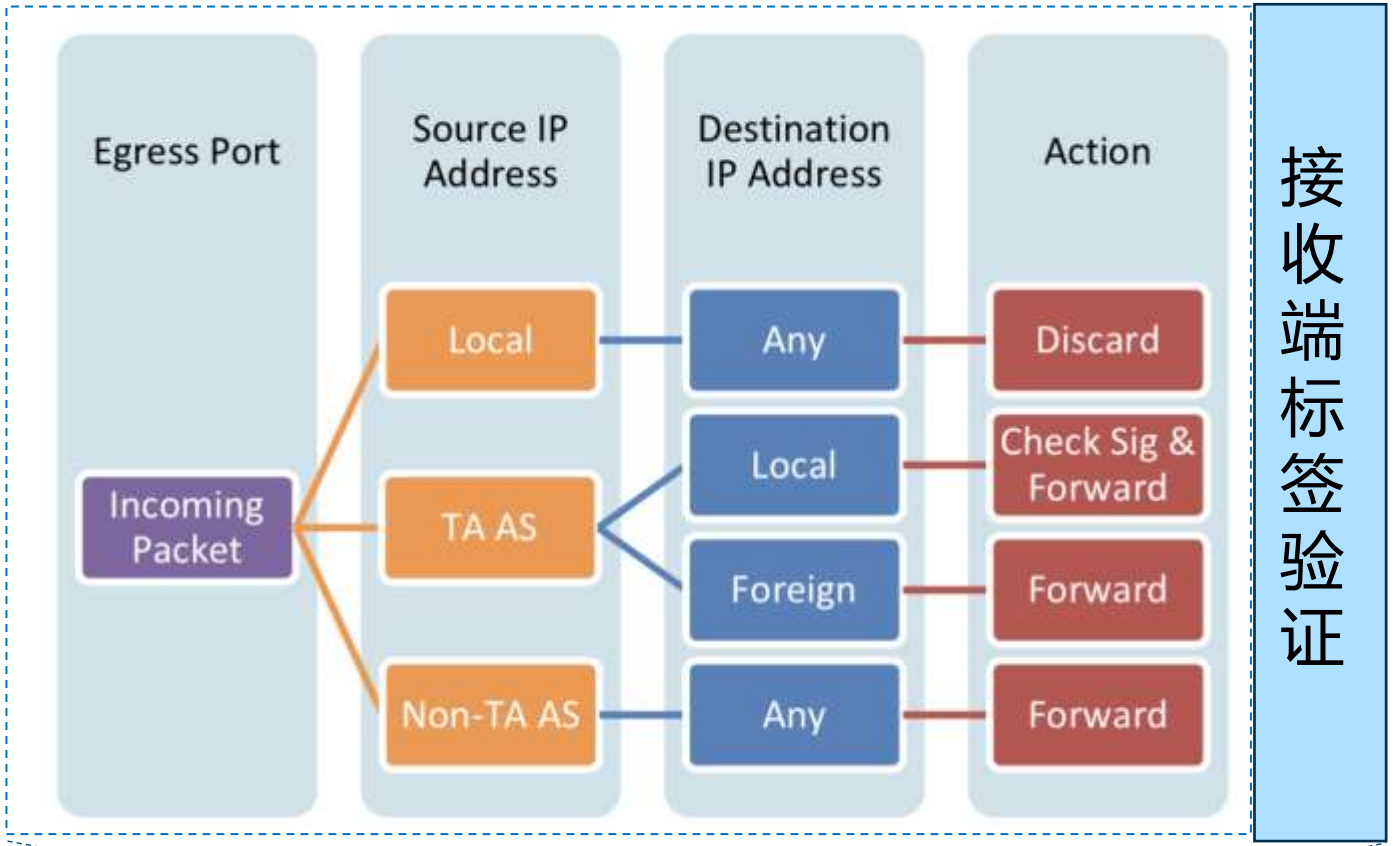
- 本域内进入 AER 的报文只应携带属于本地址域的源地址前缀
- 源地址属于本地址域、目的地址属于其它成员地址域的报文必须添加标签，其它报文直接转发

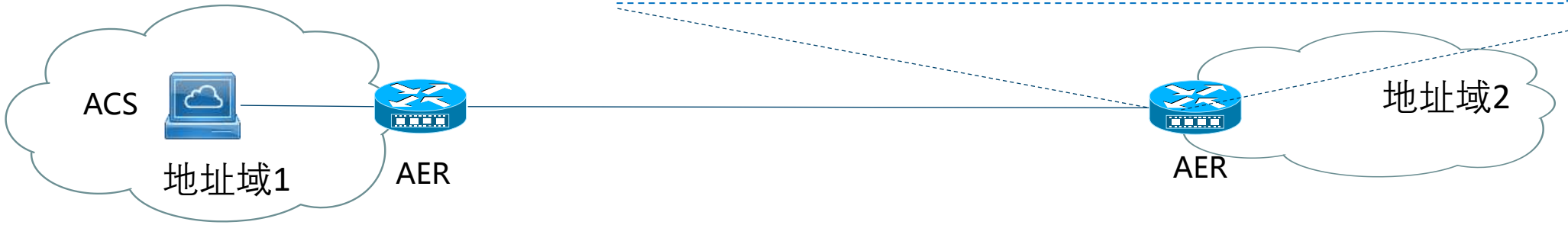




SAVA-X标签验证

- 从其它地址域进入 AER 的报文不应携带属于本地址域的源地址前缀
- 源地址属于其它成员地址域、目的地址属于本地址域的必须检查标签，其它报文直接转发
- 标签验证过程：AER访问ACS获取对应地址的地址域信息及标签信息，实现验证

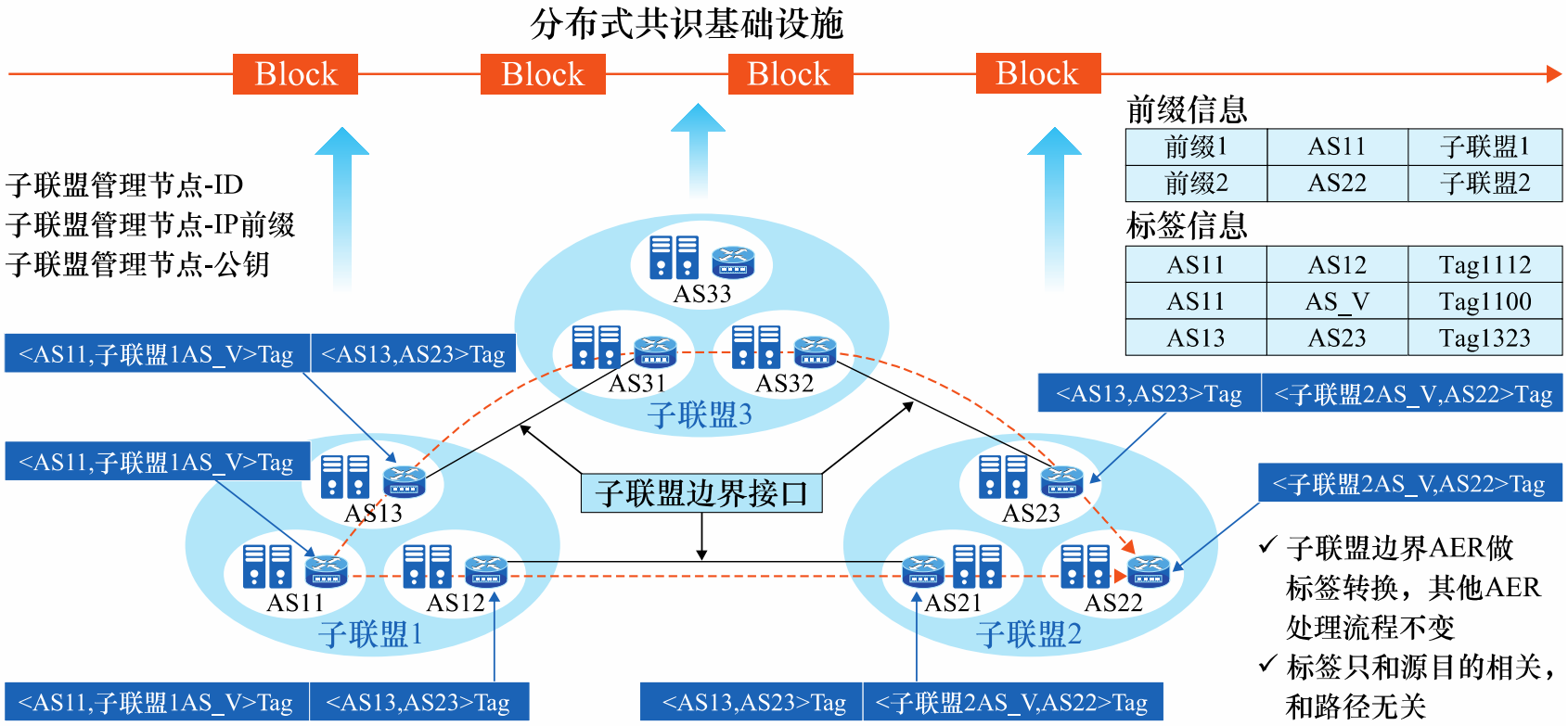




SAVA-X基于区块链的域间信任联盟

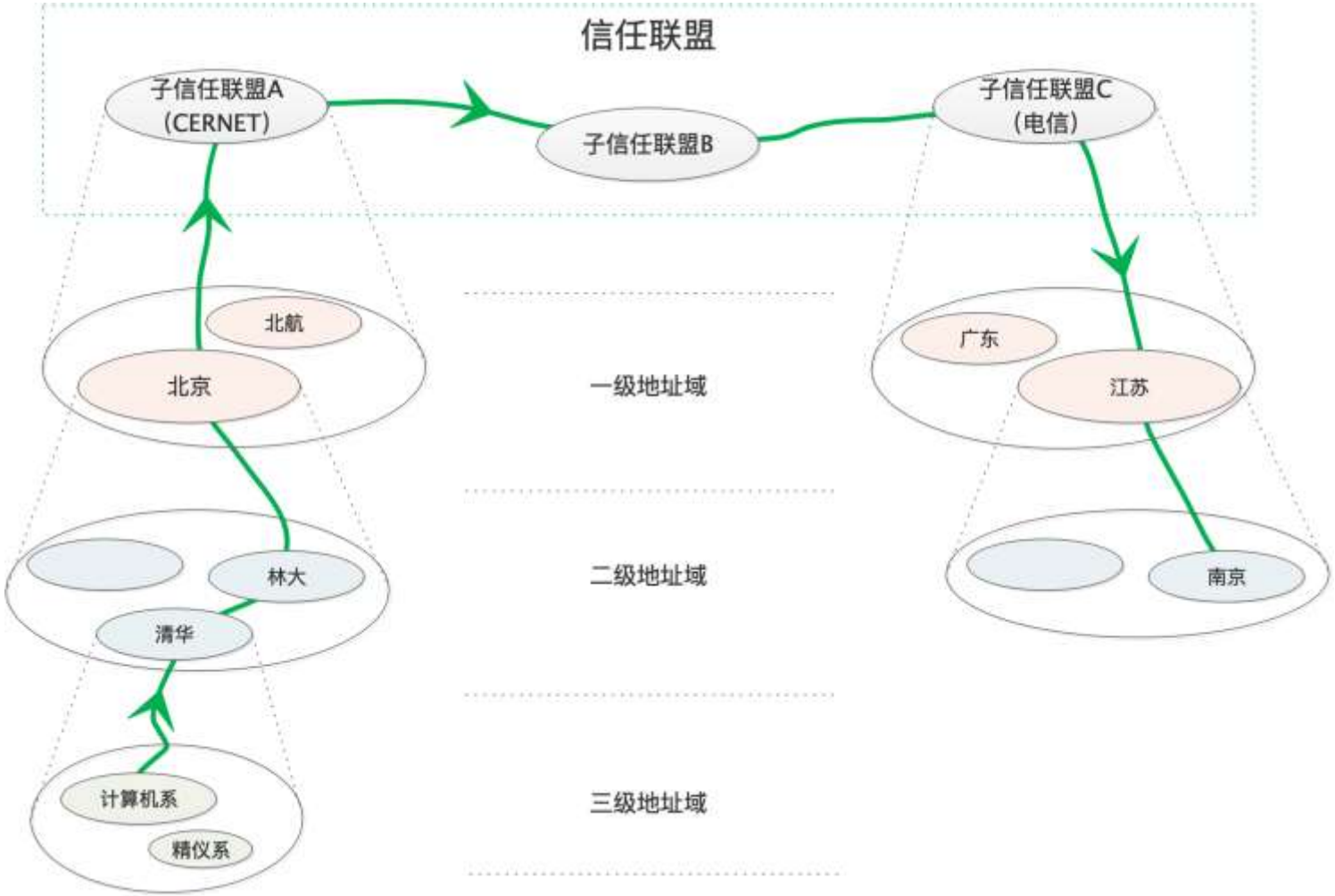
基于区块链的

域间信任联盟



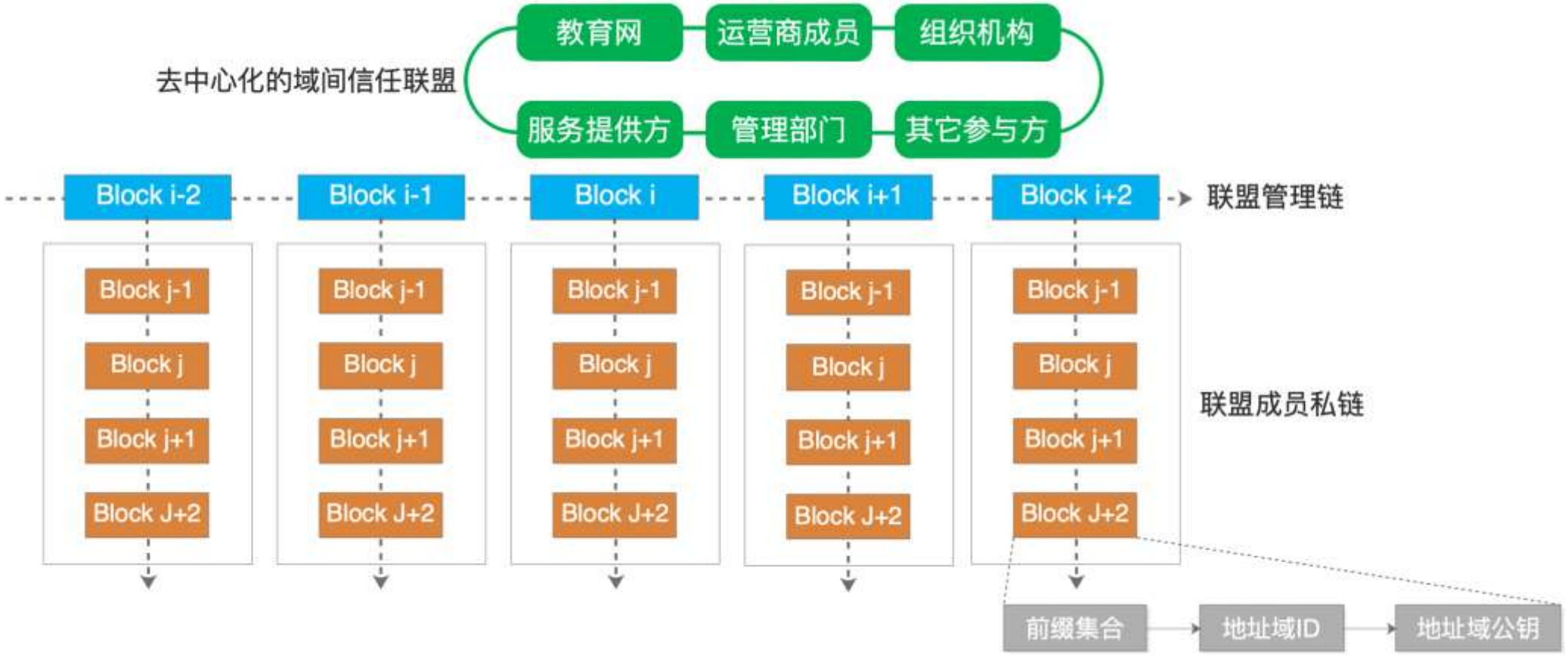
- 以密钥/证书+分布式结构+共识系统建立信任基础，利用区块链协商状态机种子
- 子联盟内：各地址域间维护1对1标签状态，通信过程不涉及标签替换。子联盟内选择主地址域
- 子联盟间：主地址域间交互子联盟级前缀和状态机，联盟间状态机采用主地址域号表示：<主地址域1, 主地址域2>
- 虚拟AS（AS_V）代表所有其他子联盟，包含所有其他子联盟前缀
- 边界地址域进行标签替换（虚拟地址域维护子联盟间标签），利用虚拟地址域避免多径传输带来的标签替换难题

层次结构



SAVA-X分层：支持五层结构（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（AS、地址域）/二级（院系）/三级（楼宇）地址域

信任联盟与节点管理



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

第4节 总结和展望

总结

从当前互联网体系结构出发，分析源地址易被伪造的原因，并基于当前体系结构提出源地址验证体系结构的设计原则，最后详细介绍SAVA体系总体结构、关键技术、应用推广

第一节
真实源地址验证体系结构设计背景

- IP地址欺骗
- 真实源地址验证体系结构SAVA的产生

当今互联网体系结构缺乏安全可信基础，未经验证的IP源地址为网络攻击提供了可乘之机

第二节
真实源地址验证体系结构设计原则

- 当前互联网的地址结构
- 真实源地址验证SAVA体系结构设计原则

真实源地址验证体系结构需要在坚持当前的互联网体系结构设计原则的基础上进行演进式创新

第三节
SAVA体系结构、关键技术、应用与推广

- 真实源地址验证SAVA体系结构
- 动态自适应的地址分配分组监听
- 分布式路由同步
- 域间层次化联盟
- 应用与推广

SAVA体系结构为上层应用提供识别基础和可信保障，有效防御利用地址伪造实施的各类攻击

总结 从互联网体系结构出发的应对思路

网络地址可伪造，缺乏合法性验证是当前互联网体系结构的一个根本安全缺陷，它也是各种攻击成功的必要条件之一

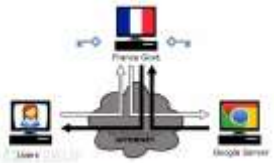
针对确保地址真实合法这一问题，构建真实源地址验证SAVA（Source Address Validation Architecture）体系结构

设计背景 → 设计原则 → 关键技术

展望 科学问题-开放网络的跨域可信访问

安全现状

用户及资源标识不可信

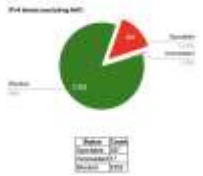


基础设施面临**仿冒伪造等问题**，无法确保用户和服务的真实性

路由不可信

路由体系无法为用户提供**可信的通信渠道**，可能造成严重信息泄露

IP地址不可信



具有**开放、易伪造特性**的IP地址，严重破坏网络通信真实性

科学问题

开放网络的跨域可信访问

机制设计

网络安全策略与行为一致性保证

展望 真实可信新一代互联网体系结构设计目标

围绕**开放网络的跨域可信访问这一核心科学问题**，突破网络安全可信通信需求与开放共享之间的矛盾，实现**网络及安全策略与网络行为一致性**保证，就迫切需要构建具有**可信、可知、可管**的新型网络体系结构

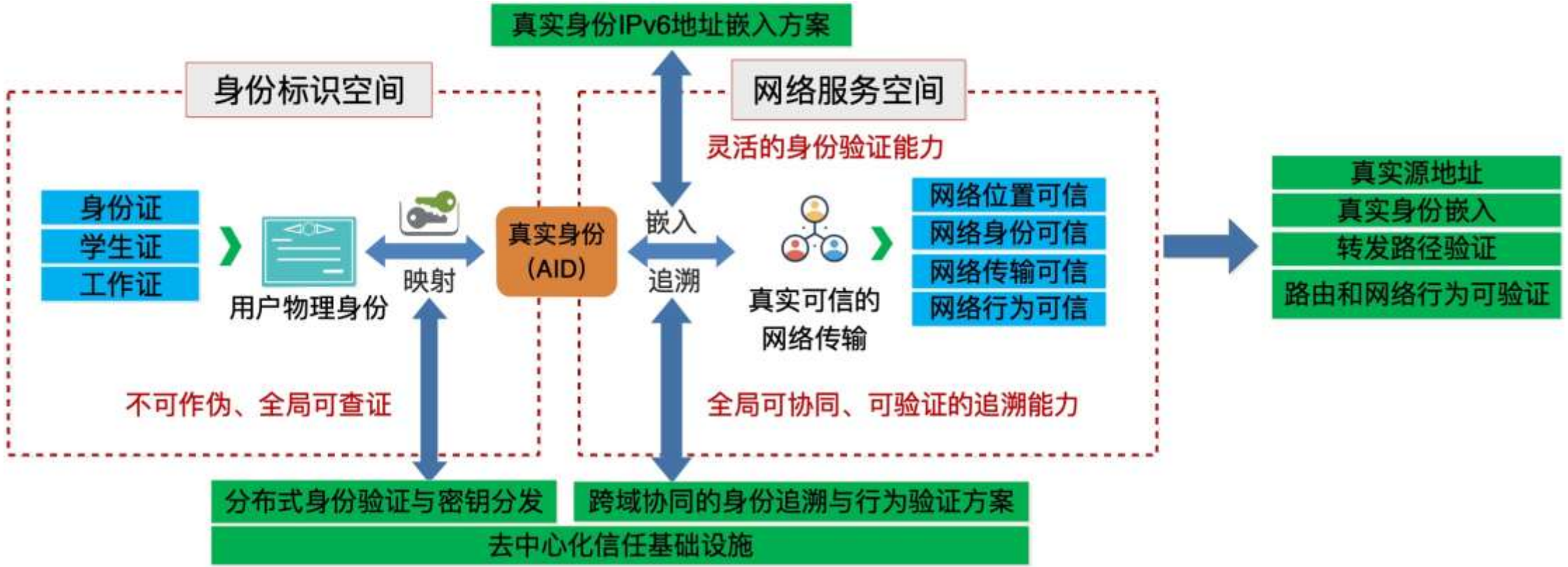
当前网络体系结构

网络及安全策略与网络行为一致性保证

- 一体化可信标识
- 跨域信任传递
- 高效可信连通
- 智能感知分析

真实可信的新型网络体系结构

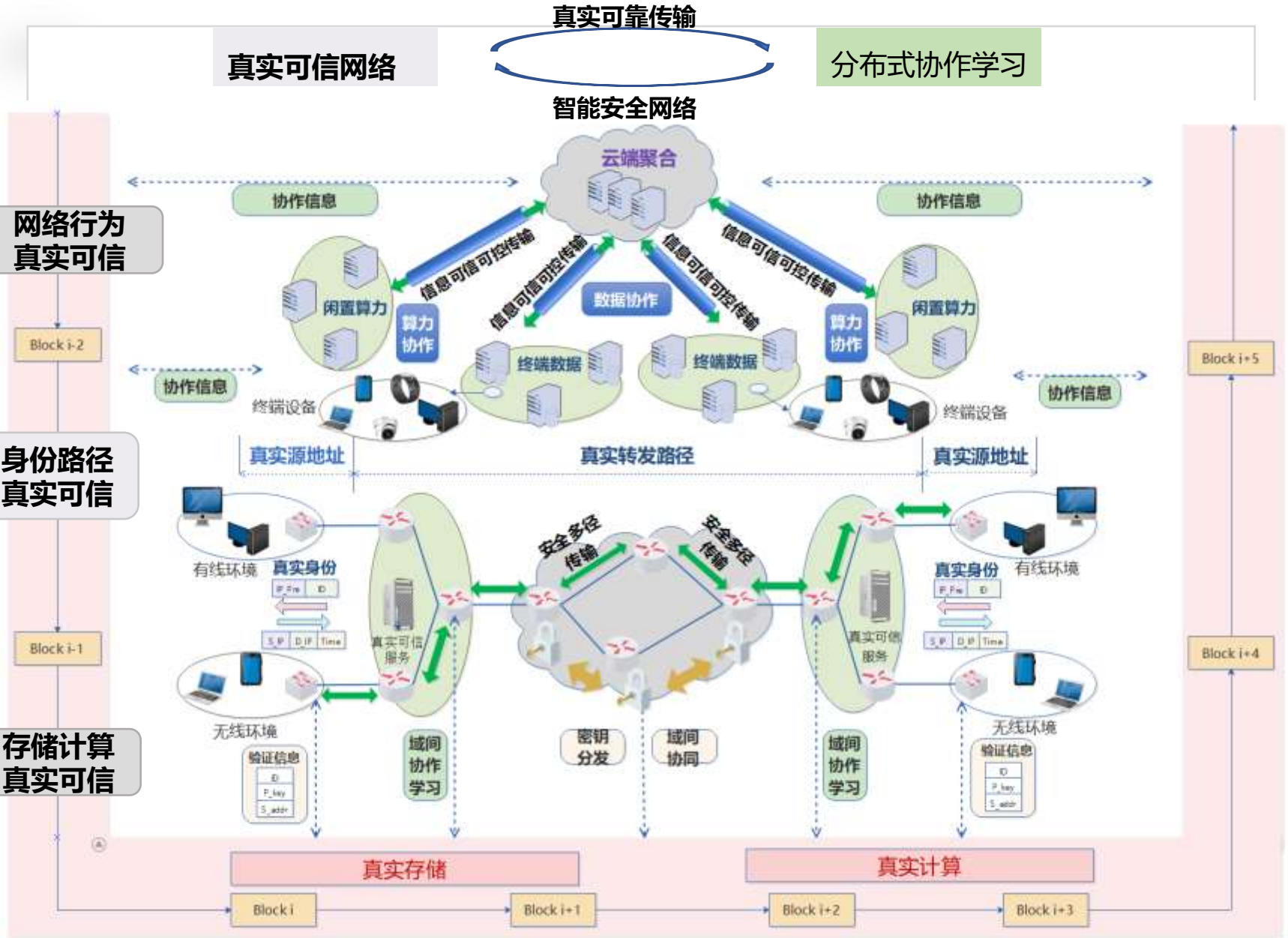
展望 新一代互联网体系结构要素



从通信元素、通信链路和基础设施出发，建立用户空间与网络空间的彼此信任关系，构建安全可信的互联网体系结构

- 以**真实地址、真实身份**为核心的身份标识空间
- 面向可信可靠传输的网络服务空间
- 去中心化的信任基础设施

展望 构建真实可信的新一代互联网体系结构



分布式协作学习

以网络真实可信为基础，采用分布式机器学习算法，打通域间网络数据孤岛，为安全可信的互联网注入智能，建立网络安全可信行为机制

真实地址真实身份

以分布式共识为基础，利用多维标识建立互联网信任平面，包括终端真实源地址、真实身份以及真实转发路径技术

分布式共识基础设施

以区块链为基础的互联网信任根，包括真实存储/计算服务