# 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

# 前 言

缺乏对源地址真实性的验证机制是当前互联网体系结构存在的一个重大安全设计缺陷。当前互联网面临的主要安全威胁中，以伪造源地址为基础的攻击手段（如身份哄骗、中间人攻击、分布式拒绝服务攻击、路由劫持、域名系统缓存投毒等）占据了重要地位，对互联网的安全性和可用性造成极大的破坏，使得网络的安全可信面临极大的挑战，真实源地址验证成为亟需突破的互联网核心技术之一。

源地址验证体系结构将源地址验证技术分为了三个层次：接入网层、地址域内层、地址域间层。其中地址域间层处于多个不同网络运营商的管理范围，网络连接复杂多变，网络用户缺乏信任，同时域间网络往往是网络的核心所在，承担的流量极其庞大，需要平衡效率和安全，因此需要一套简单、轻量、高效的机制，以抵御域间源地址伪造攻击。

域间源地址验证（SAVA-X）方案构建了层次化信任联盟机制，将现有网络按照一定的标准，划分为层次化可自嵌套的地址域层级联盟；通过联盟链维护地址域数字资源信息，保证地址域信息真实可靠不可篡改；地址域之间两两维护一对时间同步状态机，通过时间触发状态机的状态迁移同时生成加密标签，实现无通信开销的标签轮换机制。在数据面通信时，地址域的边界路由器处理数据包中携带的标签，源端地址域添加标签、中间地址域验证替换标签、目的端地址域验证移除标签，通过标签的正确性，保证源地址的真实性，实现域间源地址验证。

清华大学联合华为和新华三，共同攻关真实源地址验证关键技术，目前已经完成了体系结构的总体设计和支撑平台的研发，华为的 NE8000 系列核心路由器，新华三的 CR16000 和 CR19000 系列核心路由器均已经支持域间源地址验证能力，可以开展现网实验并支持实际商业化部署。

# 目 录

# 第一章　互联网源地址安全现状

自 1967 年美国实施 ARPANET 计划以来，互联网从最初的 4 个主机节点发展到了今天的全球自治互联。互联网成功渗入了政治外交、经济金融、军事战争、社会生活、文化娱乐等各个方面，互联网的持续发展极大的便利了人们的生产生活，促进了社会的长足进步和经济的持续发展，已成为最重要的人类社会信息基础设施和国家战略资源。

互联网的成功是天时地利人和共同作用的结果，但最为重要的是构建了 TCP/IP（Transmission Control Protocol/Internet Protocol）体系结构，如图1.1所示，TCP/IP 体系结构是互联网发展成功的关键所在。

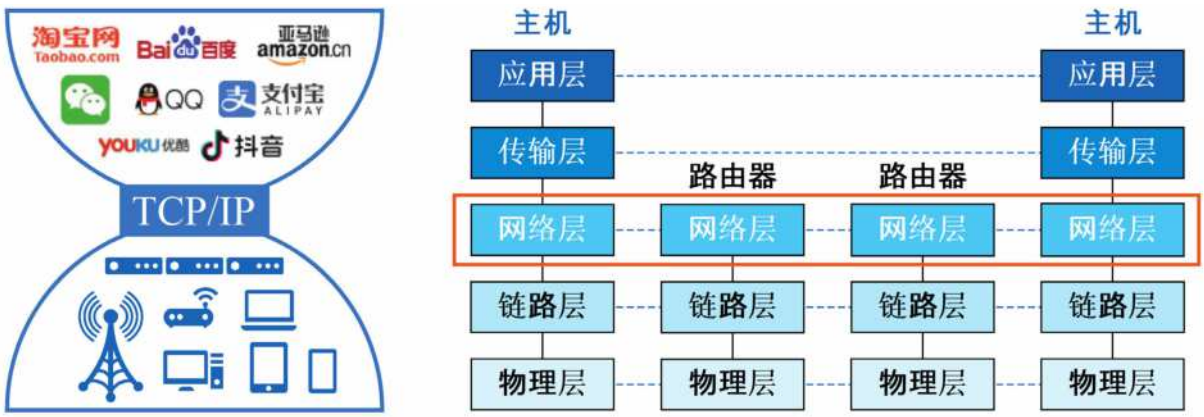


图 1.1　互联网窄腰模型

互联网协议（Internet Protocol，IP）作为最为重要的两个互联网的标准协议之一，“IP on everything” 和 “everything over IP”，使得 IP 起着承上启下的作用，保证了全网通达。IP 是异构网络互联的基础，也是体系结构的核心，更是互联网能够快速迭代发展的基石。作为互联网早期设计者的 Vinton Cerf 指出 IP 在设计上：

- 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。

在 20 世纪 80 年代设计运行之初，互联网节点稀疏，节点之间彼此信任，同时受限于当时通信技术的发展，互联网采用了“尽力而为”的转发方式，中间节点转发 IP 数据包的时候，不会检查数据包的源 IP 地址，只是根据目的 IP 地址进行转发。尽管依托于 IP 协议良好的高瞻远瞩式设计，互联网能够高速迭代发展至今，但是伴随互联网的蓬勃发展，用户节点数量激增，纷繁复杂的网络连接致使节点间信任缺失。

作为重要的基础设施之一，互联网由于网络初始设计上的缺陷，缺乏对源 IP 地址真实性的验证机制，致使网络自身的安全性和可靠性仍然难以得到保障。IP 协议是互联网的核心协议，源 IP 地址真实性的缺失影响到互联网体系结构的各个层面。当前互联网面临的主要安全威胁中，以伪造源 IP 地址为基础的攻击手段，如身份哄骗、中间人攻击、分布式拒绝服务攻击、路由劫持、域名系统（Domain Name System，DNS）缓存投毒等，占据了重要地位。利用这一缺陷发起的网络攻击层出不穷，不仅对网络的持续发展产生了一定的制约，而且对人们的生产生活造成了重大困扰。互联网巨擎 Vinton Cerf 指出，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。

IP 地址具有语义二重性，使得 IP 地址既可以作为用户的身份信息标识，又可以作为用户的地理位置信息标识，身份信息标识体现为用户在网络中的身份，位置信息标识则体现在用于从目的设备向源设备反向发送数据。伪造 IP 地址则既可以隐藏攻击者身份，又可以隐藏攻击者位置。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互联网最根本的威胁，使得应用伪造 IP 地址已经成为大量攻击成功的一个先决条件。同时，伪造 IP 地址的威胁不仅存在于网络层：基于 IP 协议的许多协议，使用 IP 地址这个并不安全的标识作为通讯对方的标识，因而只要伪造了源地址，相应地就欺骗了这些协议，这使得伪造源地址攻击的能力超出网络层范围，危害到其它更上层的协议。通过禁用或者过滤源 IP 地址这种简单的策略并不会明显减少攻击流量，导致受害者遭受攻击的时无法进行有效的反制以及防御，同时使得定位溯源攻击者也变得异常困难。

网络设备使用假冒的源 IP 地址发起网络攻击或进行不正当网络活动的行为被称为**源 IP 地址伪造**，即源 IP 地址伪造是指网络设备使用并不属于它的 IP 地址作为源地址发送数据包的行为，经过修改后的源地址称为伪造源地址。利用源地址伪造的手段，网络攻击的发起者可以隐匿自己的身份和位置，逃避法律的制裁。使用伪造的源地址的网络攻击行为难以被追溯，这是当前伪造源地址行为泛滥的原因。借助伪造源地址发起的分布式拒绝服务攻击（Distributed Denial of Service，DDoS）是当前互联网公认的最大的安全威胁之一。随着源地址伪造手段的大量使用，基于真实地址的网络计费、管理、监控和安全认证等都无法正常进行，对互联网基础设施和上层应用都造成了严重的危害。随着互联网的发展，基于源地址伪造的网络攻击愈发猖獗，IP 地址可伪造、不可信等问题给网络可信安全访问带来严重的威胁，甚至严重危害到社会和国家的安全。

总的来说，源地址伪造主要带来了如下 3 方面的安全问题：

1. 一些攻击类型，例如远程访问注入攻击（CWE-78）[1]，在原理上依赖于假冒源地址，它们需要伪造特定的地址才能成功发起攻击；

2. 一些攻击类型，例如分布式拒绝服务攻击，虽然可以不伪造特定源地址就可以发起攻击，但是一旦采用了伪造源地址，则可以起到隐藏攻击真实源头的目的，令管理者不易发现和制止；

3. 目前很多应用以源地址为资源使用的标识，例如可使用 IP 登录的应用网站，在地址假冒的情况下，攻击者可以盗用网络资源，损害了网络运营者的利益。

根据应用互联网数据分析中心（Center for Applied Internet Data Analysis，CAIDA）的统计报告[2]，如图1.2所示，当前互联网，在不支持网络地址转换（Network Address Transition，NAT）技术的 IPv4 网络中，有 18.8% 的 IP 地址块可以被伪造，有 30.4% 的自治域支持伪造源地址；在支持 NAT 技术的 IPv4 网络中，有 8.5% 的 IP 地址块可以被伪造，有 24.7% 的自治域支持伪造源地址；在 IPv6 网络上有 17.4% 的 IP 地址块可以被伪造，有 35.0% 的自治域支持伪造源地址。测量结果表明，在互联网上伪造源地址是相对容易实现的。

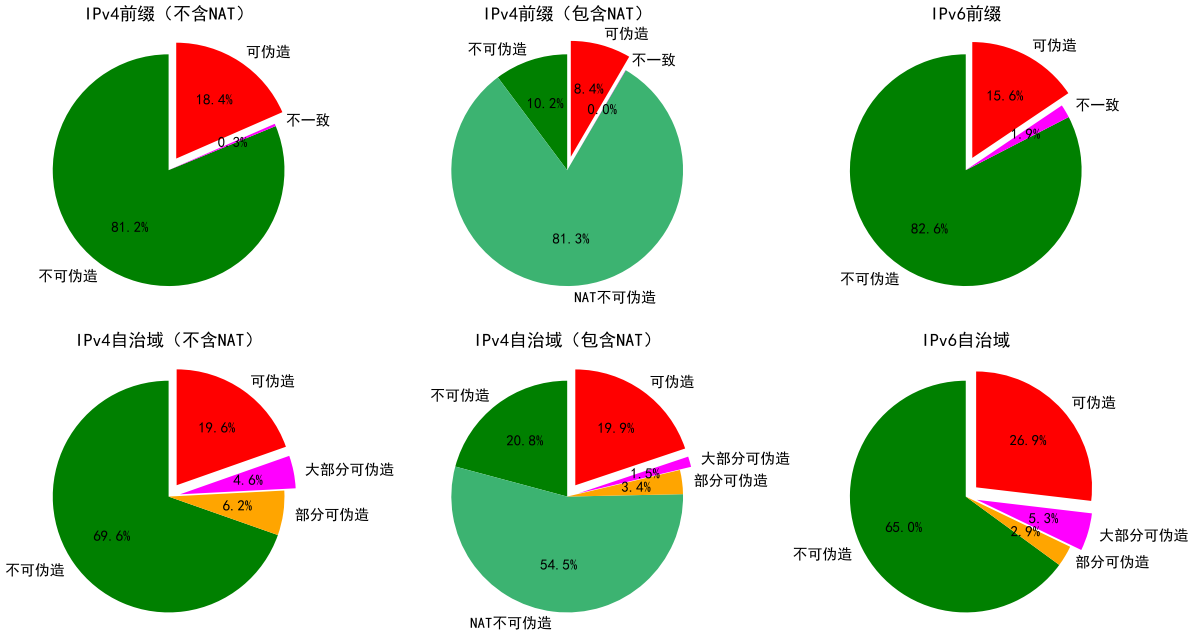


图 1.2 IP 源地址可伪造现状

令人不可思议的是，作为防御手段的最佳实践 BCP38[3]，在实际部署中，入口过滤的部署率小于出口过滤部署率：67.0% 的 IPv4 自治域和 74.2% 的 IPv6 自治域，不会

[1] https://cwe.mitre.org/data/definitions/78.html

[2] https://spoofer.caida.org/summary.php，2023.04.25

[3] https://www.rfc-editor.org/info/bcp38

过滤声称来自他们网络的外部流量[4]。这表明大多数自治域的路由器使用的是一种“宽进严出”的策略，即自治域网络管理者基于某种考虑，可能是防御手段的假阳性，也可能是用户体验，即便知道进入本自治域的一些数据包是伪造的，也没有进行过滤，这体现了源地址伪造的猖獗和治理的复杂性。

[4]https://www.caida.org/projects/spoofer/spoofer-flyer.pdf

# 第二章　项目背景

## 2.1　源地址伪造问题

网络设备使用并不属于它的 IP 地址作为源地址发送数据包的行为称之为源地址伪造。源地址伪造可以发生的根本原因是互联网设计时假设了网络内部成员互相之间都是可以信任的，并没有充分地考虑随着网络规模扩大和网络信息开放，网络成员之间信任缺失带来的安全威胁。在网络中，终端设备通信时发出数据包，以路由器等为代表的中间转发设备只是根据数据包的目的地址进行转发，而不对数据包的源地址进行任何校验和检查，为源地址伪造的发生提供了基础设施上的支持。

源地址可伪造是互联网的一个核心安全问题，众多类型的网络攻击都需要直接或者间接地借助于源地址伪造技术。当网络中的设备使用伪造的 IP 源地址进行通信时，ISP 在管理上将面临以下两方面的困难：

- **难以追溯攻击者的身份和位置**。IP 地址具有语义二重性，IP 地址是一台终端设备在网络中的唯一标识，它既标识设备在网络中的位置，同时也标识设备在网络中的身份。数据包中伪造的 IP 源地址同时隐藏了攻击者的地理位置及其身份信息，导致通过 IP 地址对攻击者进行溯源追踪难以实现，使得攻击者可以逃脱法律的惩戒和制裁。难以追溯攻击者的身份和位置是当前互联网中依托于伪造源地址发起网络攻击行为泛滥的重要原因。

- **难以防御基于伪造源地址的网络攻击**。现在使用的两个 IP 协议版本中，IPv4 的地址空间有 $2^{32}$ 个地址，IPv6 的地址空间则扩大到了 $2^{128}$ 个地址，即便是去掉标准规定的私有地址和保留地址之后，IP 地址空间仍然十分庞大。过于庞大地址空间就导致网络管理者无法使用访问控制列表（Access Control List，简称 ACL）等简单的策略，通过禁止某些 IP 地址访问的方式来防御网络攻击。

TCP/IP 协议栈是互联网事实上的协议栈标准。根据 TCP/IP 协议栈的设计，IP 协议是互联网的核心协议之一，起着承上启下的作用。TCP/IP 协议栈中，IP 的上层协议如 TCP、UDP 等，依赖于不安全、不真实的 IP 地址作为通信双方的标识，一旦使

用了伪造的 IP 源地址，也就实现了对基于 IP 的上层协议的欺骗和伪造，危害到了上层协议的安全性和真实性。

互联网已经成为社会生活中重要的基础设施，是国家的战略资源。然而基于源地址伪造的网络攻击愈发频繁和猖獗，严重威胁到了社会中重要网站和服务的安全性和可用性，给现实社会带来了巨大的经济财产损失。增强互联网中的端系统和路由设备对数据包源地址的验证和过滤能力，对于提升互联网的安全性、可用性、鲁棒性以及人类社会健康良好的生产生活都具有重要意义。

## 2.2 域间源地址验证方案

在国内外工业界和学术界的一致努力下，当前对于 IP 源地址进行验证过滤已经提出了比较多的方案。按照清华大学在 2008 年在 IETF 提出的 RFC 5210 的分类方法，可以将源地址验证工作分为三层：接入网源地址验证层（简称接入层）、自治域内源地址验证层（简称域内层）、自治域间源地址验证层（简称域间层）。三层之间保护粒度越来越粗，保护范围越来越大。由于接入层和域内层都是位于同一个 ISP 运行、维护、管理下，其部署相对方便，但是域间层涉及到不同 ISP 的协作，容易发生不信任的情况，更有可能发生源地址伪造。因此，在本文中只关注并分析自治域间源地址验证技术方案。

自治域间源地址验证技术，通常需要不同的自治域之间相互协作，通过分工协作来传递过滤规则，共同完成源地址验证并且过滤伪造源地址数据包的任务。自治域间源地址验证方案根据技术原理以及特点可以分为两个大类：一类是借助于域间路由信息，通过现有的路由协议携带数据包转发路径上的源地址相关属性信息，验证相关信息正确性保证源地址真实性；另一类是基于加密标签签名的方案，通过对数据包进行加密或者签名，通过加密算法的安全性保证源地址真实性。

### 2.2.1 基于域间路由信息的方案

基于域间路由信息方案的基本假设是，在一般情况下，攻击者能够伪造数据包中的源地址，但是并不能更改数据包的转发路径。基于域间路由信息的源地址验证方案通过 BGP 等外部边界网关路由协议，来携带数据包转发路径上的源地址属性信息，这些属性通常是一些自治域级别的信息，例如自治域路径、路径长度以及路径标识等信息。自治域的边界路由器通过源地址属性信息来检验经过它的流量是否发生了源地址伪造问题。

单播反向路由查找技术（unicast Reverse Path Forward，简称 uRPF）具有三种常见的工作模式：严格模式、宽松模式和可行模式。工作在严格模式下的 uRPF，检查数据包的入接口是否和反向到达数据包中 IP 源地址的出接口相匹配。如果不匹配，则认

为数据包使用了伪造源地址并进行过滤。由此可见，只有在对称路由的网络中可以启用严格模式的 uRPF，对称路由网络中数据包的转发方向和到达方向具有一致性。但是，随着 ISP 和用户对网络可用性和健壮性期望的提高以及新的自治域加入网络，两个对等自治域之间可达路径逐步增加，拓朴结构变得复杂，路由对称性难以得到保证，增加了数据包正向转发和反向转发非对称的可能性，导致严格模式下的 uRPF 方案假阳性问题严重。工作在宽松模式下的 uRPF，不关注数据包到底从路由器的哪个接口接收，而只检查路由表中是否存在和数据包 IP 源地址相对应的表项。如果存在对应表项，则认为数据包源地址是真实的，否则过滤数据包。宽松模式的 uRPF 并不能过滤已经存在于路由表项中的伪造源地址数据包，存在着严重的假阴性问题，其过滤能力比较差。在检查时去掉对默认路由的检查，这时如果路由表项包含了所有的合法可达地址，那么将能够提高宽松模式的 uRPF 过滤效果。工作在可行模式下的 uRPF，扩展了严格模式，增加了数据包到达接口的可行范围，在一定程度上降低了严格模式的假阳性，但同时也增加了假阴性。当网络中的等价路径较多时，增加数据包到达的可行接口实质上已经退化为了宽松模式，此时假阳性问题和假阴性问题都存在。

出入口过滤（Ingress Egress Filtering，简称 IEF）是一种部署在网络的边界路由器上过滤数据包的技术，它过滤来自该网络但是其源地址却不属于该网络，以及发送至该网络但是其源地址却是该网络的数据包，前者为出口过滤（Egress Filtering），后者为入口过滤（Ingress Filtering）。由于网络庞大的 IP 地址空间，相比于出口过滤，入口过滤方法在网络中更为常见。入口过滤常常被使用在服务提供自治域（Provider AS）和客户自治域（Customer AS）之间的链路上以及自治域出口处，用于过滤伪造源地址的流量。入口过滤的过滤规则的建立依赖于手动配置或者依赖于路由表的 uRPF。由于只需要依赖于现有路由表而不需要其它额外的信息，入口过滤是一种非常高效的方法。实际上，如果每一个自治域的出口路由器都部署了入口过滤，那么互联网上自治域粒度的源地址就一定是真实的。但是根据调查研究，互联网上只有 80% 的自治域部署启用了 BCP 38 即入口过滤技术，剩下 20% 的自治域则未启用该技术，方案的完整性受到破坏。而且当 Customer AS 使用的是和 Provider AS 无关的前缀时，或者 Customer AS 是一个多宿主的自治域时，基于 uRPF 生成的过滤规则可能会存在假阳性问题，致使方案的可部署性遭受挑战。对于其它类型的自治域间链路，由于路由的对称性基本不存在，所以入口过滤并不完全适用。而基于手动配置的入口过滤，存在配置过于复杂以及很难适应网络动态变化的情况。

分布式包过滤（Distributed Packet Filtering，简称 DPF）是一个重要的基于路由进行过滤的工作，其核心思想是在自治域间部署基于流和接口的绑定关系或者基于路由地址前缀的过滤规则。通过实验模拟，DPF 证明了其构建的过滤规则在互联网上是有效的，只需要 20% 左右的自治域部署 DPF 就可以使 70% 的自治域免于基于源地址伪造技术的攻击。但是 DPF 只是提出了一个方案框架，并没有给出如何生成过滤规则表。同时也没有说明为了避免“公共地的悲剧”，作为公共物品的源地址伪造防御方案，应

该如何推进自治域的部署。DPF 的后续工作都在研究如何生成过滤规则表。这些工作可以分为两个方向，一是完全自治域本地化地生成过滤规则表；二是依赖于自治域合作生成过滤规则表。在第一个方向上的代表工作是域间包过滤方案（Inter-Domain Packet Filter，简称 IDPF），它通过学习 BGP 更新报文（BGP Update）来推断出源和目的自治域之间可能的路径信息和相互之间的关系。IDPF 依赖于 Valley-free 特性来生成本地的过滤表，“Valley-free” 即自治域间商业关系的无低谷特性，任何自治域都不愿意为其自身以及 Customer AS 之外的任何流量付费。由于自治域间 Valley-free 路径的多样性，IDPF 生成的过滤规则表实际上比较宽松，限制了方案的过滤能力。DPF 在第二个方向上的代表工作有 BASE 和 BGP Selection Notice。BASE 和 BGP Selection Notice 都需要通过修改 BGP 协议来传播路径信息，以帮助其它自治域生成正确的过滤规则表。BASE 方案需要部署自治域向 BGP 宣告中加入标签，收到宣告的自治域学习到标签并将标签和源地址前缀进行绑定以建立过滤规则表。BGP Selection Notice 方案为 BGP 新增加选路通知报文，将选路策略通过 BGP 宣告通知路径上的所有自治域，进而建立过滤规则表。

基于跳数计数过滤方案（Hop Count Filtering，简称 HCF）是依赖于数据包从源自治域到检查点自治域的跳数和 IP 源地址前缀之间的关系，对数据包源地址进行验证的方法。在域间路由稳定的情况下，从一个源自治域到检查点自治域所需要经过的跳数是固定的。检查点自治域首先从数据包的 IP 数据包头中的 Time-To-Live（TTL）字段推断出数据包所设置的初始 TTL 值，然后用推断出的 TTL 值减去 TTL 现值就可以得到数据包所经历的跳数。如果事先建立了地址前缀和跳数之间的映射关系，那么就可以判断数据包源地址的真实性。HCF 最大的优势是：对于终端设备或者边缘网络等出口很少的网络，上述基于路由方向的过滤方案无法很好地工作，而这时基于跳数过滤可以起到较好的效果。另外地址前缀和跳数的对应关系也可以通过学习或者探测的方式获得，无需制定新的协议。但是自治域间网络抖动以及路由动态性的存在使得 HCF 方案获得的是一个区间范围的可行解集，为了减少假阳性，其源地址验证保护粒度相当粗放，同时由于初始 TTL 值是可以伪造的，HCF 方案假阴性问题严重，造成其实际应用相当困难。

### 2.2.2 基于加密标签签名的方案

基于加密标签签名的技术方案主要依靠源端自治域在数据包中打上特定的标记，然后由目的端自治域负责检查标记和数据包源地址的匹配关系，这是一类端到端的验证方案。端到端验证的一个明显优势就是与路由无关，所以不用处理路由带来的动态性和复杂性，然而其明显的缺陷就是需要同时修改路由设备的控制平面和数据平面。首先这类方案需要一个控制平面的协议来交换密钥信息，此外，必须在数据包中添加一些额外信息。除去处理效率方面的考虑，这种模式可能会影响其它协议的工作。此外，如果数据包本身已经是最大长度且网络不支持分片，这时也就无法向数据包中插入信息。

IPSec 方案是一类经过了 IETF 标准化的方案，它可以为 IP 层的通讯提供认证和加密的机制。通讯中的双方可以通过在数据包中添加和检查认证头（Authentication Header，简称 AH），IPSec 使用 AH 确保数据包来自于 IP 源地址的拥有者而非伪造源地址。IPSec 除了用在通讯双方的主机之间，也可以用在两个网络之间，或者主机和网络之间，通过使用协商好的密钥，构建一条端到端的隧道，隧道的机密性、完整性和不可篡改性由协商的端到端密钥和加密算法来保证。尽管 IPSec 经过多年的发展，已经是一项十分成熟的技术方案，在现在的网络中作为 VPN（Virtual Private Network，简称 VPN）方案使用，但是 IPSec 在用于源地址保护时，却有着不可忽略的缺陷。如果使用互联网密钥交换技术（Internet Key Exchange，简称 IKE）来进行密钥交换，则 IPSec 方案最大的问题在于，交换密钥的双方无法证明各自对于所使用地址的所有权，例如一个主机可以用一个同一个子网下没有被分配给它的地址和对方完成密钥交换，这可能来源于中间人攻击。此外，IPSec 的数据包验证采用摘要算法单向哈希如 MD5 或者 SHA1，验证开销较大，使得路由器可能成为 DoS 攻击的目标，从而瘫痪网络，因此在实际中，AH 报文头应用较少，IPSec 常常作为一种 VPN 技术存在，并不能大范围应用于互联网全局。

SPM 方案（Spoofing Prevention Method，简称 SPM）建立了信任联盟机制，每个部署 SPM 方案的自治域都必须加入信任联盟，但在决定部署 SPM 方案之前自治域则是自愿选择部署的。处于信任联盟之内的所有成员自治域都需要承担为其它成员自治域提供源地址验证过滤的义务。该方案需要事先协商要使用的特定标签，该标签具备方向性，源自治域到目的自治域和目的自治域到源自治域需要使用不同的标签。在通信时源端自治域的边界路由器向数据包添加标签，目的端自治域的边界路由器验证数据包中的标签，通过标签正确性来保证数据包源地址的真实性。而对于信任联盟之外的其它自治域，由于缺少必要的协商标签的过程，信任联盟内的自治域则不会为其提供该项源地址验证过滤支持。由此可知，SPM 最大的弊端是不会阻止信任联盟之外的源地址伪造，对于目的地址是信任联盟内部的自治域才会校验数据包的源地址，否则并不会进行过滤操作，因此 SPM 方案只有通过扩大信任联盟部署规模才能防止更多的源地址伪造。只有当全局部署时，SPM 的部署收益才能有显著地提升，部分部署时其部署收益变化不大。同时由于在自治域间通信时，SPM 方案所使用的标签是事先协商确定的，没有做到逐包变化，所以面临着标签重放攻击，攻击者可以线上窃听标签并进行重放，造成方案的假阴性问题。

可审计 IP 方案（Accountable Internet Protocol，简称 AIP）将网络划分为独立的可审计域，在可审计域内和可审计域间可以进行源地址验证。网络设备和可审计域都使用一个 160 位的比特串作为自身标识，该标识使用了加密生成地址（Cryptographically Generated Addresses，简称 CGA）的技术来生成，其具有自验证的能力。每一个数据包中都包含了源网络设备标识、源可审计域标识、目的网络设备标识、目的可审计域标识这样的四元组，依靠标识的自验证能力，转发路径上的数据包转发者和数据包接收

者都可以检查数据包源标识的真实性。AIP 的优势在于使用全局性的自验证地址可以避免引入验证所需要的密钥基础设施，同时可验证性的可审计域标识使得伪造源地址的数据包在汇聚到接收者之前就可以被大量过滤，避免了由于加密验证开销导致的资源耗尽式的拒绝服务攻击。但是 AIP 使用的加密生成地址的方式是一种非常激进的设计，和现在的互联网体系结构完全无法兼容，无法适用于 IPv4 或 IPv6 下的地址结构。即便不考虑地址的后向兼容性，由于 AIP 中的地址标识采用加密的方式完全随机生成，不具备地址前缀汇聚性，导致网络中每一个路由设备需要存储非常巨大的路由表，和现在的路由体系结构也无法兼容。这种方案在目前条件下看来还不具有可行性。

Passport 方案可以在自治域内和自治域间进行源地址验证。Passport 方案设计时考虑了现有的网络体系结构，因此具备一定的向后兼容的性质。Passport 方案原理是在数据包中插入根据源端自治域和检查端自治域之间的密钥产生的加密内容，又称为消息认证码（Message Authentication Code，简称 MAC）。和 IPSec 的端到端的检查不同，Passport 方案考虑了路径上节点对数据包真实性进行检查的能力，因此它是一个结合了基于域间路由信息和基于加密标签签名的方案。在端系统上，端系统需要产生和自治域边界路由器之间的 MAC-P，以及和目的端之间的 MAC。边界路由器在检查数据包中的 MAC-P 通过之后会移除 MAC-P，并且在数据包中插入本自治域和路径上其它自治域之间的 MAC。MAC 会被路径上的自治域逐一检查，直到数据包到达目的端自治域。Passport 实际上是一种在数据包转发路径上也能够检查数据包 MAC 并进行替换的方案，这种检查替换的特性可以很好地防止伪造源地址的攻击流量汇聚到目的端受害者自治域。尽管 Passport 方案考虑了向后兼容性，但是它依然需要一个全局的信任基础设施来帮助其生成自治域之间的 MAC，以及一个自治域内的公钥基础设施来帮助产生主机和边界路由器之间的 MAC。此外，在数据包中插入 MAC，实际上是路由器和主机暂不具备的功能，所以需要 ISP 付出巨大的成本去大量的升级现有设备。此外，插入和检查 MAC 使用的对称密钥算法或者单向哈希摘要算法会给路由器带来较大的开销。除去性能和部署上的考虑，Passport 方案在终端设备地址真实性上的考虑略有欠缺。现在的终端设备配置的地址通常并非是固定不变的，而是依靠 DHCP 等协议动态分配的。在动态分配地址的情况下，边界路由器实际上很难知道终端被授权使用哪一个地址，这时检查源地址的真实性实际上是没有意义的。同时由于域间路由的动态性，Passport 方案在转发路径上使用了逐段检查，但是又没有使用如分段路由等源路由技术，这无可避免地增加了方案的假阳性。

SMA 方案（State Machine-based Anti-spoofing）是一个基于时序状态机的轻量化的 SPM 演化方案。SMA 方案最大的优点是使用基于时序同步状态机的方式，在自治域本地通过状态机的运行生成一致性标签，取代了 SPM 繁琐的密钥交换过程，提升了控制面的安全性。SMA 作为一个端到端的方案，通过标签的真实性保证源地址的真实性，中间路由器无需感知如何处理标签选项头，可以和现有部署了 IPv6 但是没有部署 SMA 机制的路由器兼容。但是一个比较严重的问题是 SMA 没有充分考虑互联网较为

明显的层次化拓扑分布，互联网上最多的自治域类型是 Stub AS，这种类型的 AS 没有下联自治域，其本身可能具有多个出入口，也可能只有唯一的一个出入口。由该类型自治域的上游自治域进行源地址验证，就可以保障该自治域的源地址真实性。由此 SMA 机制实际上维护了大量的非必要的状态机，浪费了较多资源。同时，SMA 方案同其它端到端方案一样，其更大的弊端是没有实质性减少网络数据包转发路径中的伪造流量，这些流量只有到达了目的自治域的边界路由器才会因为源地址检查未通过而被丢弃，中间路由器没有对源地址进行检查，所以造成的后果是网络中仍然可能充斥着大量的伪造流量。通过合理的层次化让中间部署了源地址验证方案的路由器参与源地址验证有助于解决这两个问题。

分布式协作系统（Distributed Collaboration System，简称 DISCS）是 SPM 的拓展方案，在其基础上完善了方案具体的实施方法。DISCS 依托于不同自治域之间的协作，其将信任联盟划分为了不同的防御联盟，一个自治域可以自愿加入和其存在共同利益的防御联盟。同时 DISCS 将可选、可传递的路径属性设置到 BGP 更新消息中，在联盟成员间进行传递，以区分不同的防御联盟。最终 DISCS 将整个互联网划分为多个并行的防御联盟，每个防御联盟内提供与 SPM 类似的防御保护能力，但防御联盟之间并不建立防御共识。DISCS 最大的贡献是可以按需调用防御功能，而不需要自治域边界路由器一直开启防御功能，这对于提升方案性能和执行效率具备实际意义。部署 DISCS 的自治域需要实现 4 个防御函数，用于实现协同防御功能。这些防御函数包括目的保护、密码学的目的保护、源保护和密码学的源保护。联盟成员在收到攻击时，其可以请求其它联盟成员执行最适合的防御函数。当攻击停止时，其它联盟成员将会停止防御函数执行。按需调用的协作方式降低了防御开销，同时降低了假阳性问题。但是 DISCS 的防御联盟建立依托于 BGP 协议的安全性，后者的安全性也是目前互联网亟待攻克的难题，因此 DISCS 的部署也受到了挑战。

# 第三章　源地址验证体系结构

针对源地址可伪造这一国际互联网重大技术挑战，清华大学提出了分而治之、端网协同的真实源地址验证体系结构（Source Address Validation Architecture，SAVA）[1]。真实源地址验证体系结构 SAVA，用于在网络层提供一种透明的服务，确保互联网中转发的每一个分组都使用“真实源 IP 地址”，具备三层含义：

- **经授权的**：源 IP 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；
- **唯一的**：源 IP 地址必须是全局唯一的；
- **可追溯的**：网络中转发的 IP 分组，可根据其源 IP 地址找到其所有者和位置。

下一代互联网管理的现状是：不同的网络管理者负责管理各自的网络，这些网络的互联构成全球互联网。其中，一个网络管理者可以拥有一个或多个自治域（Autonomous System，AS），一个自治域也可以包含多个网络管理者的网络。由于 IP 地址作为互联网的通信标识具有全球唯一性，每个网络管理者拥有其独属的 IP 地址前缀集合，称其为地址管理域，简称**地址域**（Address Domain，AD）。按地址域划分接入网内、地址域内和地址域间三个层次、不同粒度的源地址验证体系，具有系统化、层次化、松耦合、多重防御、支持增量部署的优点，显著提升了源地址验证体系结构的灵活性和适应能力，更加适应下一代互联网实际运行管理现状。

根据下一代互联网管理现状，改进的面向地址域的新型源地址验证 SAVA 体系结构，如图3.1所示，针对接入网、地址域内、地址域间三个层次，分别确定了单个地址、地址前缀、前缀集合的不同验证粒度，相应提出了地址同步、多模异构的真实源地址接入验证方法 SAVA-A（SAVA-Access），路由同步、动态过滤的真实源地址域内前缀验证方法 SAVA-P（SAVA-Prefix），多域同步、协作信任的真实源地址域间验证方法 SAVA-X（SAVA-eXternal），实现了：

- 不同层次可以实现不同粒度的 IPv6 源地址真实性验证；

[1]SAVA 工作已经于 2008 年在互联网工程任务组（Internet Engineering Task Force，IETF）进行了标准化，编号是 RFC 5210：A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience（`https://datatracker.ietf.org/doc/rfc5210/`）

- 每一层次，允许不同网络运营商采用不同方法技术验证源 IP 地址真实性；
- 整体结构简单性和各部分组成的灵活性的平衡。

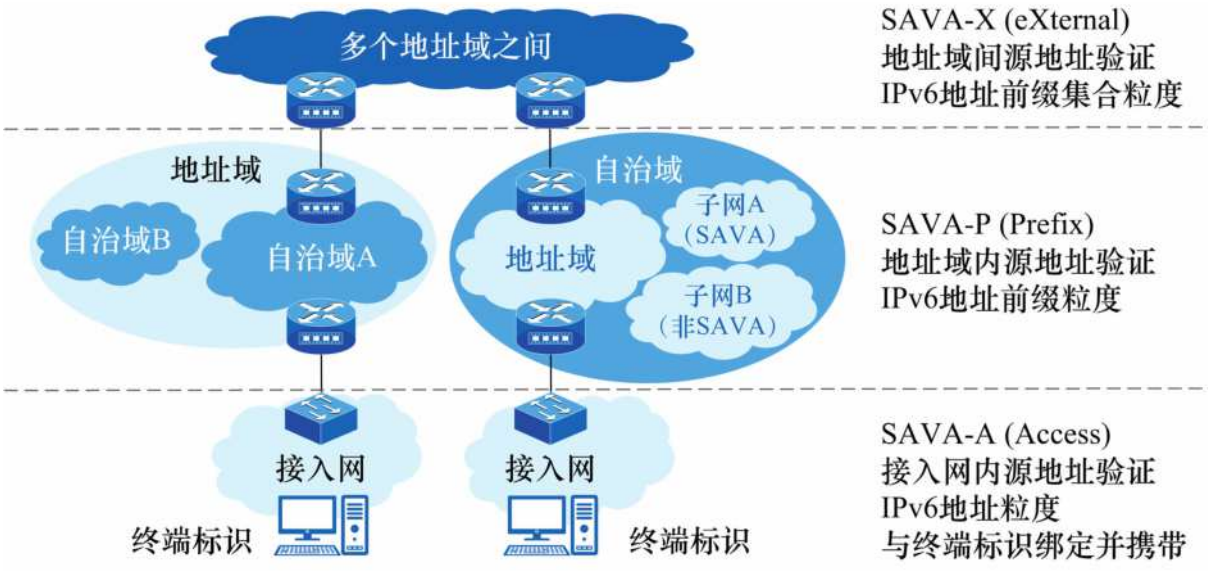


图 3.1 下一代互联网真实源地址验证体系结构 SAVA

源地址验证体系结构中，接入层是地址粒度最细的层次，它保证了设备接口级别的安全，具有最精确的源地址验证保护粒度；地址域内层是中等地址粒度的层次，它保证了自治域内部的源地址的真实性，防止内部子网设备伪造源地址，保证地址前缀级别的安全，但是两者都不能保证来自更大范围的外部网络地址的真实性。同时接入网层和地址域内层基本都是属于同一网络运营者在管理，其相对于地址域间层的源地址验证较为简单，而域间层的源地址验证可能会涉及到不同 ISP 之间的相互信任与协作，迫切需要系统地解决分布式非协作网络跨域可信访问难等安全问题。

域间真实源地址验证技术 SAVA-X 主要的目标是提供地址域前缀粒度的源地址真实性。SAVA-X 以地址域为单位，地址域是一个 IP 地址前缀所对应的所有 IP 地址组成的地址集合，由加入 SAVA-X 方案的所有地址域共同组成的信任联盟，内部经过划分形成分层的地址域信任联盟，称为地址域层级联盟，每一层都有其层级编号，编号从 0 开始。地址域之间使用状态机进行端到端的源地址检查验证；部署 SAVA-X 的地址域共同组成信任联盟，联盟成员之间彼此可信任、可验证、可追溯，对联盟外的源地址伪造具有识别和过滤能力。

扁平式的域间源地址验证方案不利于方案增量部署实施，且不能及时丢弃伪造流量，使得伪造流量只有到达目的端地址域才会被丢弃，浪费了宝贵的网络带宽。层次化域间源地址验证技术方案依据流量关系、地理位置等方式，将网络划分为层次化可嵌套的地址域，通过逐级验证替换标签的方式及时发现伪造流量，解决了上述两个问题。为了增加可扩展性、增强增量部署能力且能尽早过滤伪造源 IP 地址的数据包，SAVA-X 设计了信任联盟的层次化方法，采用一种基于轻量级标签替换的地址域端到地址域端

的加密认证机制，使得整个信任联盟系统构成一种具有源地址验证功能的、层次化的体系结构。通过虚拟地址域、层次化标签替换等技术实现了多域协同、多域聚类的域间信任传递，解决了多径传输场景下地址域间 IP 地址前缀集合粒度的真实源地址验证问题。

SAVA-X 提出了基于端到端验证的域间源地址验证机制 SMA (State Machine based Anti-spoofing)。通过维护同步状态机生成加密标签签名来实现端到端源地址验证，是 SAVA-X 方案的核心机制。基于状态机同步的域间源地址验证 SMA 技术，是一种端到端验证机制，通过引入状态机自动同步，实现低开销、轻量化的对称密钥更新机制。将 SMA 技术应用于域间真实源地址验证，是以地址域为单位，地址域之间使用状态机进行端到端的源地址检查验证；部署的地址域共同组成信任联盟，联盟成员之间彼此可信任、可验证、可追溯，对联盟外的源地址伪造有识别和过滤能力，因此对部署方提供了保护和部署激励，支持增量部署。

SAVA-X 设计了数据包防篡改机制，通过把数据包中的部分信息和状态机产生的标签进行拼接并计算其 Hash 值，达到逐包签名效果，并在目的端地址域的边界路由器上验证签名，从而有效抵御攻击者复用标签的攻击方式。

SAVA-X 的具体技术内容在第四章介绍，SAVA-X 的实现部署应用工作在第五章介绍，在 CCSA TC3 WG2 以及 IETF 进行标准化的进展情况在第六章介绍。

# 第四章　层次化域间源地址验证技术

## 4.1　总体机制

扁平信任联盟结构的域间源地址验证方案，要求加入信任联盟的每两个地址域之间都维护至少一个时间同步状态机[1]，协商初始状态以及状态迁移间隔等状态机相关参数。在时间同步后，各状态机在本地运行，由时间触发状态迁移的同时生成一个加密位串作为标签，源端地址域的边界路由器（AD Edge Router，AER）发送数据包时添加标签，目的端地址域的边界路由器收到数据包验证移除标签，通过标签的正确性，保证源地址的真实性。但是当信任联盟内包含大量的对等地址域时，以扁平信任联盟方式在互联网全局进行增量部署是比较困难的，尤其是在部署后期，每新增一个对等地址域，需要信任联盟内的所有地址域都与新增地址域维护一个时间同步状态机，这在网络管理运维上是及其困难的。同时在扁平模式下，中间节点地址域不会检查数据包，伪造流量只有在到达目的端地址域后才会被检查丢弃，伪造流量仍然充斥着整个网络，浪费了宝贵的网络带宽资源。

为了增加可扩展性，并且能够尽早丢弃伪造流量，SAVA-X 设计了层次化的信任联盟方案。在扁平信任联盟结构的域间源地址验证方案的基础上，立足实际网络拓扑结构和域间路由机制，通过合理的分层标准，SAVA-X 将部署了验证机制的所有网络划分成多层级地址域信任联盟，每一级地址域联盟可以作为成员（抽象为一个系统整体）自下而上的参加更高级别的地址域信任联盟，形成一种多级并存的、层次化的信任联盟体系结构。

SAVA-X 层次化结构示意图如图4.1所示，通过引入实现标签替换的“中继代理”联盟边界地址域（Trust Alliance Edge AD，TAE-AD），如 $AD3$、$AD4$，将每一层级联盟和外界网络隔离，在确保域间高速通信的同时使得下层联盟和更高层联盟内部的网络环境彼此互不可见、互无影响，有效降低了边界路由设备状态机存储、查找、同步和处理等验证开销，即使在规模较大的层次结构中仍然能保证验证的有效性和简单化，着力体现“先部署先受益”的特点，具有一定的增量部署激励。报文经过 TAE-AD 时，

[1]状态机是有方向性的，且状态机存在轮换，由此如果双向标签不一致或者状态机即将到期，就需要维护两个及以上的状态机。本文后续考虑最简单情况，即不区分状态机方向、不考虑状态机轮换，因此两个地址域之间只维护一个状态机。