源地址验证 SAV 技术白皮书

目 录

1 概述

1.1 产生背景

互联网体系结构在设计之初，假设所有网络成员均是可信的，没有考虑网络成员不可信带来的安全威胁。随着互联网的开放式蓬勃发展，网络成员的可靠性无法得到保障。而网络设备只基于报文的目的 IPv6 地址对报文进行转发，不对转发报文的 IPv6 源地址的真实性进行任何验证，使得伪造 IPv6 源地址的攻击大量出现。基于真实 IPv6 源地址的网络计费、管理、监控和安全认证都无法正常进行，对互联网基础设施和上层应用都造成了严重的危害。

SAV（Source Address Validation，源地址验证）是一种真实 IPv6 源地址验证体系结构，能够实现在 IPv6 环境下的 IPv6 源地址验证、真实身份溯源，对非法攻击流量进行阻断，提升 IPv6 网络的安全性。

1.2 技术优点

SAV 技术能够在互联网中实现不同粒度的 IPv6 源地址验证，对互联网的安全和应用提供如下便利：

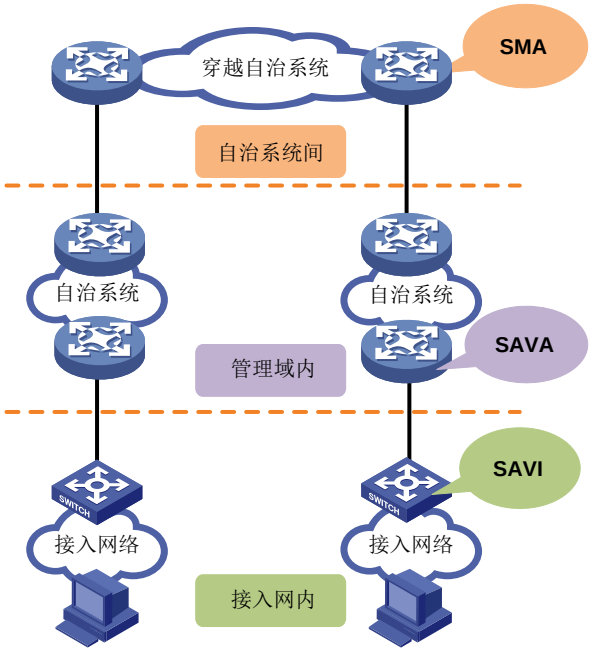
- 易于追踪攻击事件，定位攻击者。确保源地址的真实性，可以防止攻击者隐匿自己的身份和位置，使得攻击行为的溯源变得简单。
- 可以解决基于伪造源地址的攻击。如今许多大规模的网络攻击手段都基于伪造源地址技术（比如 DDoS），消除了伪造源地址的报文即消除了这些攻击，网络环境将变得更加安全。
- 支持基于源地址的网络计费和管理。报文源地址的真实性，为基于源地址的网络计费、管理、监控以及安全认证等业务正常准确运行提供了保证。

1.3 体系结构

SAV 很好地适应了现在的互联网分层体系，支持分层部署在网络不同位置、满足不同粒度需求的源地址验证。根据在网络中部署位置的不同，SAV 体系包含如下三种技术：

- SAVI（Source Address Validation Improvement，源地址有效性验证）：部署在接入网，在接入层面提供主机粒度的源地址验证，保证接入主机的合法性。
- SAVA（Source Address Validation Architecture，源地址验证架构）：部署在骨干网连接接入网的边界设备上，在管理域内提供 IPv6 前缀粒度的保护能力，以保护核心设备不被仿冒源地址的非法主机攻击。
- SMA（State Machine based Anti-spoofing，基于状态机的伪造源地址检查）：部署在 AS 间，在 AS 域间提供 AS 粒度的源地址验证能力，以保护本 AS 内的主机和服务器不被仿冒源地址的非法主机攻击。

图1 SAV 体系结构



2 SAVI 技术实现

2.1 SAVI简介

SAVI 功能可以用于过滤接口上收到的 IPv6 报文，可以防止 IPv6 源地址非法的 DHCPv6 协议报文、ND 协议报文和 IPv6 数据报文形成攻击。配合其它安全功能，可在设备上生成 IPv6 地址与客户端接入端口的绑定关系表项，根据该绑定表项对报文 IPv6 源地址进行检查。如果报文信息与某绑定表项匹配，则认为该报文为合法报文，正常转发；否则将该报文丢弃。

与 SAVI 配合使用的安全功能包括 DHCPv6 Snooping、ND Snooping 和 IP Source Guard 中 IPv6 静态绑定表项功能。

说明

- DHCPv6 Snooping 是 DHCPv6 的一种安全特性，用来保证客户端从合法的服务器获取 IPv6 地址，并可以记录 DHCPv6 客户端 IPv6 地址与 MAC 地址的对应关系。
- ND Snooping 功能用于二层交换网络环境，设备通过侦听 ND 或者数据报文来创建 ND Snooping 表项，该表项内容包括报文的源 IPv6 地址、源 MAC 地址、所属 VLAN 和报文入端口等信息。
- IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

2.2 SAVI运行机制

本节以SAVI与DHCPv6 Snooping功能配合为例，介绍SAVI运行机制。如图2所示，DHCPv6 client1通过DHCPv6自动方式获取IPv6地址，Switch上开启了DHCPv6 Snooping功能和SAVI功能。

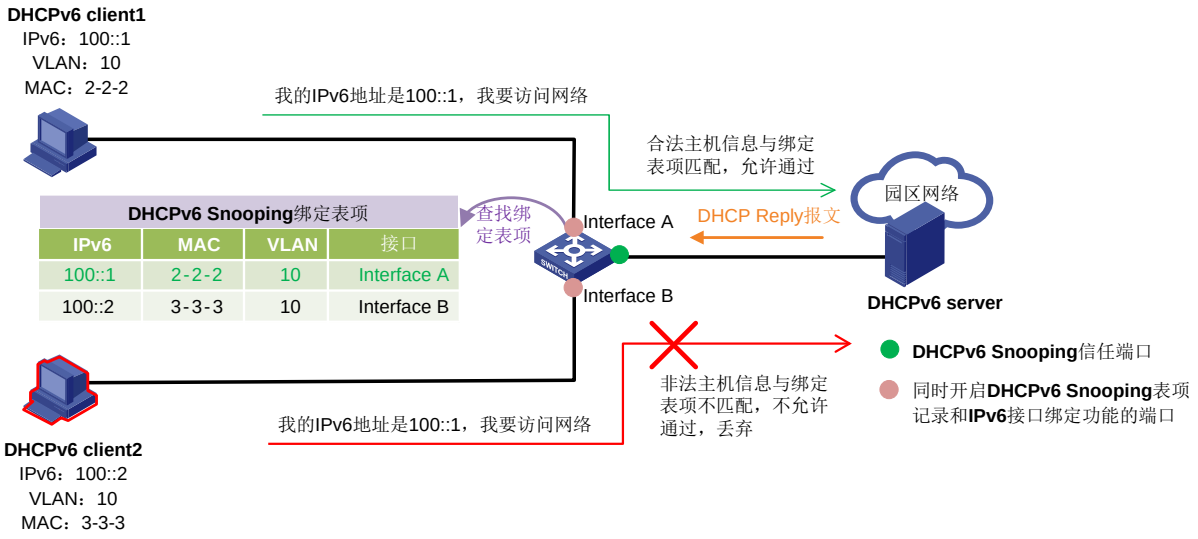
(1) DHCPv6 client1通过广播的形式发送DHCPv6请求报文，Switch将请求报文通过信任端口发送给DHCPv6 Server。DHCP Server将含有IPv6地址信息的DHCPv6 Reply报文回复给Switch。

(2) Switch上的配置的DHCPv6 Snooping功能通过监听DHCPv6 client1与DHCPv6 server之间交互的DHCPv6报文，记录DHCPv6 Snooping表项，该表项包括DHCPv6 client1的MAC地址、获取到的IPv6地址、Switch与DHCPv6 client1连接的端口及该端口所属的VLAN等信息。

(3) Switch根据记录的DHCPv6 Snooping表项信息生成DHCPv6 Snooping绑定表项。比如，Switch通过监听client1和DHCPv6 Server之间的DHCPv6报文，获取到client1的MAC地址为2-2-2、client1从DHCPv6 server分配到的IPv6地址为100::1、Switch与client1相连的接口为Inerface A、Interface A所属VLAN为VLAN 10，根据这些信息生成了一条DHCPv6 Snooping绑定表项。

(4) 假设此时client2想要仿冒client1的IPv6源地址发送攻击报文，Switch收到报文后，查找DHCPv6 Snooping的绑定表项发现没有与之匹配的表项，无法通过报文合法性检查，因此该报文将被丢弃，防止了非法报文形成的攻击。

图2 SAVI运行机制（与DHCPv6 Snooping功能配合）



2.3 SAVI典型应用场景

1. DHCPv6-Only 场景

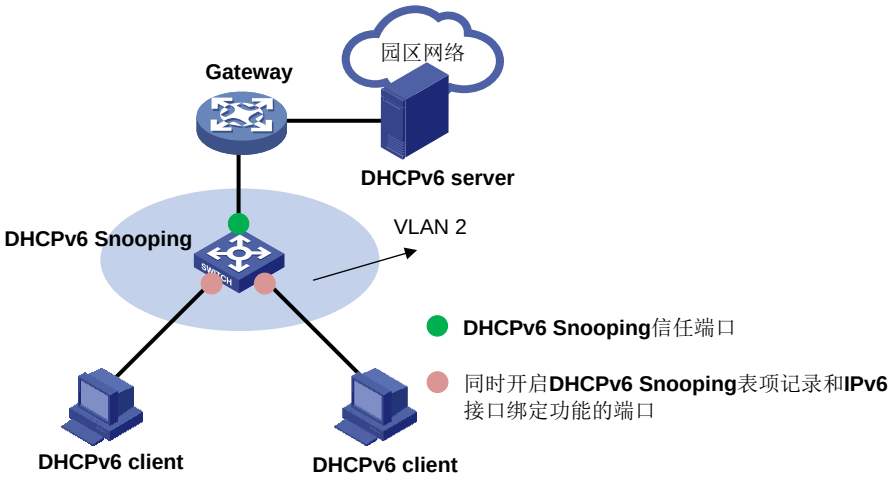
此场景中，与配置SAVI功能的设备（Switch）连接的主机只能通过DHCPv6方式动态获取地址。在Switch上开启SAVI功能后，SAVI对报文源IPv6地址合法性检查过程如下：

(1) 在 Switch 上配置 DHCPv6 Snooping 功能，将 Switch 与 DHCPv6 server 相连的接口设置为信任端口，使得 DHCPv6 Client 能通过 DHCPv6 服务器获取 IPv6 地址。

(2) 在连接 DHCPv6 Client 的接口上开启 DHCPv6 Snooping 地址表项记录功能，在接口上监听 DHCPv6 报文，生成 DHCPv6 Snooping 表项。

(3) 在 VLAN 2 中开启 ND Detection 功能，在连接 DHCPv6 Client 的所有接口上开启 IPv6 接口绑定功能，利用动态生成的 DHCPv6 Snooping 表项对接口收到的 DHCPv6 协议报文、ND 协议报文（除 RA、RR 报文）报文和 IPv6 数据报文进行源地址的合法性检查，确保接入用户的合法性。

图3 DHCPv6-Only 场景典型组网图



2. SLAAC-Only 场景

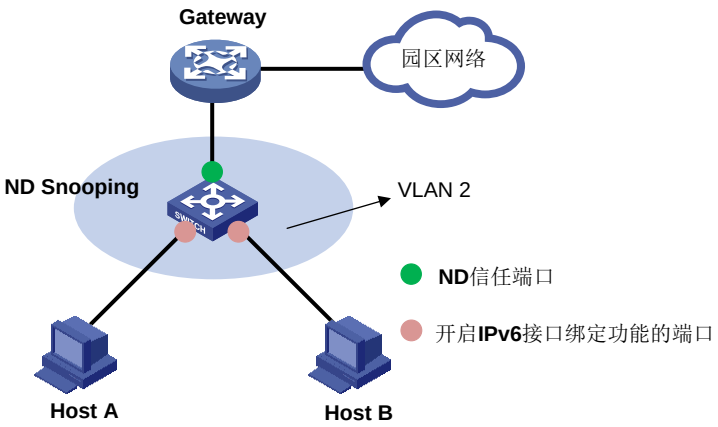
此场景中，与配置 SAVI 功能的设备（Switch）连接的主机只能通过无状态自动配置方式动态获取地址。在 Switch 上开启 SAVI 功能后，SAVI 对报文源 IPv6 地址合法性检查过程如下：

(1) 在 Switch 上配置 ND Snooping 表项获取功能，通过 ND 报文的源地址（包括全球单播地址和链路本地地址）生成 ND Snooping 表项。

(2) 将 Switch 上与园区网络网关相连的接口配置为 ND 信任端口，与 Host 相连的所有端口采用默认配置（即为 ND 非信任端口）。

(3) 在 VLAN 2 中开启 ND Detection 功能，在连接 Host 的所有接口上开启 IPv6 接口绑定功能，利用动态生成的 ND Snooping 表项对接口收到的 ND 报文和 IPv6 数据报文进行源地址的合法性检查，确保接入用户的合法性。

图4 SLAAC-Only 场景典型组网图



3. DHCPv6 与 SLAAC 混合场景

此场景中，与配置 SAVI 功能的设备（Switch）连接的主机可以通过 DHCPv6 方式和无状态自动配置方式两种动态获取地址。在 Switch 上开启 SAVI 功能后，SAVI 对报文源 IPv6 地址合法性检查过程如下：

(1) 在 Switch 上配置 DHCPv6 Snooping 功能，将 Switch 与 DHCPv6 server 相连的接口设置为信任端口，使得 DHCPv6 Client 能通过 DHCPv6 服务器获取 IPv6 地址。

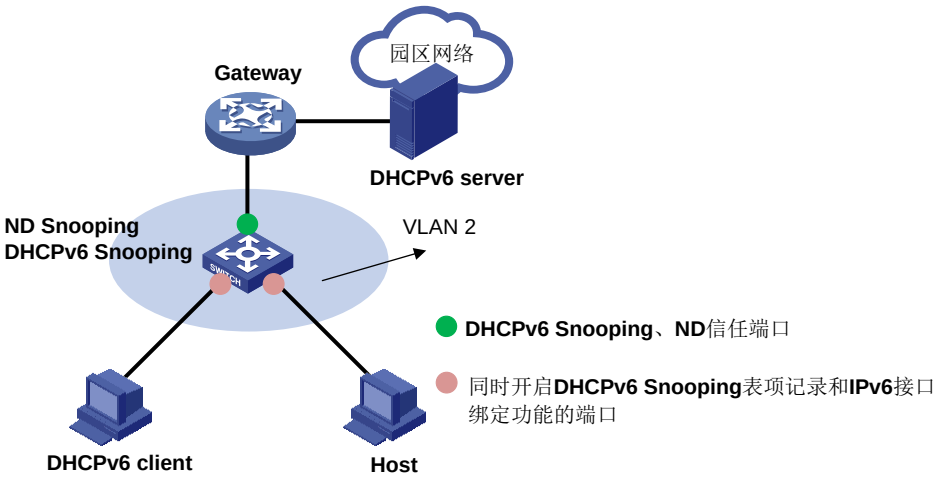
(2) 在连接 DHCPv6 Client 的接口上开启 DHCPv6 Snooping 地址表项记录功能，在接口上监听 DHCPv6 报文，生成 DHCPv6 Snooping 表项。

(3) 在 Switch 上配置 ND Snooping 表项获取功能，通过 ND 报文的源地址（包括全球单播地址和链路本地地址）生成 ND Snooping 表项。

(4) 将 Switch 上与园区网络网关相连的接口配置为 ND 信任端口，与 Host 相连的所有端口采用默认配置（即为 ND 非信任端口）。

(5) 在 VLAN 2 中开启 ND Detection 功能，在连接 DHCPv6 Client 和 Host 的所有接口上开启 IPv6 接口绑定功能，使 Switch 根据 DHCPv6 Snooping、ND Snooping 表项，对从所有接口收到 DHCPv6 协议报文、ND 协议报文和 IPv6 数据报文进行源地址合法性检查，确保接入用户的合法性。

图5 DHCPv6 与 SLAAC 混合场景典型组网图



说明

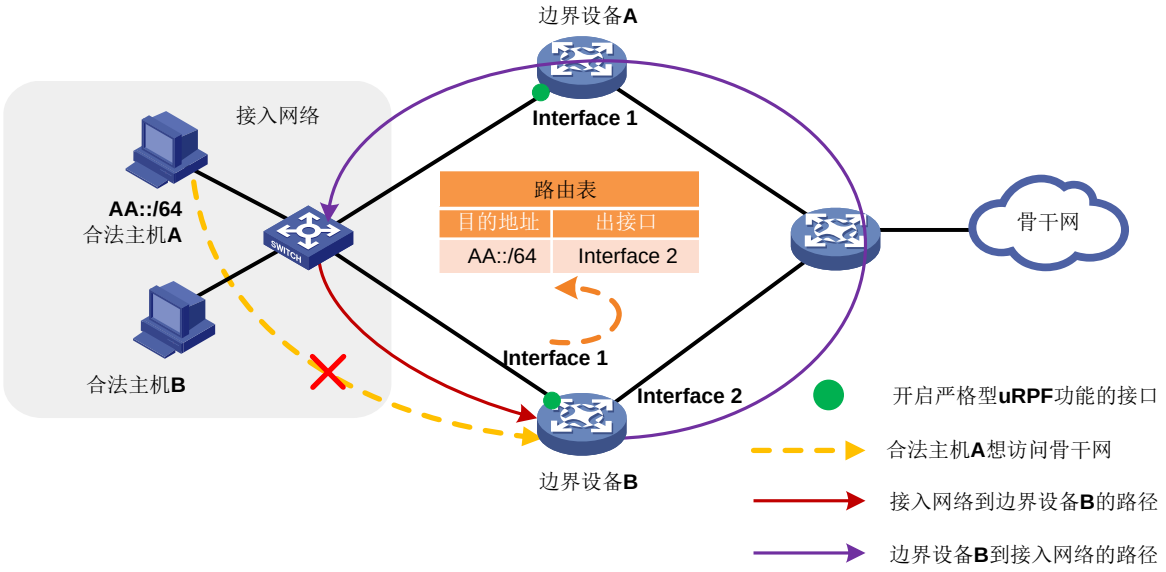
可在上述三种场景中，同时叠加配置 IP Source Guard 中 IPv6 静态绑定表项，使得指定 IPv6 地址、MAC 地址的 DHCPv6 协议报文、ND 报文和 IPv6 数据报文能够通过源地址合法性检查。

3 SAVA 技术实现

3.1 SAVA产生背景

在 IPv6 网络中，IPv6 uRPF（unicast Reverse Path Forwarding，单播反向路径转发）功能可以用来防范基于 IPv6 源地址欺骗的攻击。在多接入（同一接入网络通过多台边界设备接入骨干网）的组网中，当出现路由不对称（即报文进入设备的入接口和设备去往报文 IPv6 源地址的出接口不一致）时，若在边界设备 A 和 B 的 Interface 1 接口上均开启严格型 uRPF 功能，边界设备 A 和 B 会将接入网络中合法的用户报文错误地判断为 IPv6 源地址伪造报文，将其丢弃。SAVA 可以解决此类场景下合法报文被误判为伪造报文的问题。

图6 SAVA 产生背景



3.2 SAVA简介

SAVA 是一种根据设备的路由信息检查攻击报文的技术，用来防范基于 IPv6 源地址欺骗的攻击，主要部署在与接入网相连的骨干网内边界设备上。在设备的接入网侧接口上开启 SAVA 功能后，设备会为该接入网络中的所有的网络前缀生成 SAVA 表项。该接口收到 IPv6 报文后，如果存在报文 IPv6 源地址对应的 SAVA 表项，则认为该 IPv6 源地址合法，转发该报文；否则，表示报文 IPv6 源地址不应该存在于接入网络中，报文非法，被丢弃。

3.3 SAVA运行机制

边界设备 A 和边界设备 B 各自与接入网相连的接口上均开启 SAVA 功能，同时边界设备 B 上配置了同步远端路由条目的 Tag。以边界设备 B 为例，SAVA 表项生成过程如图 7 所示，分为如下几个步骤：

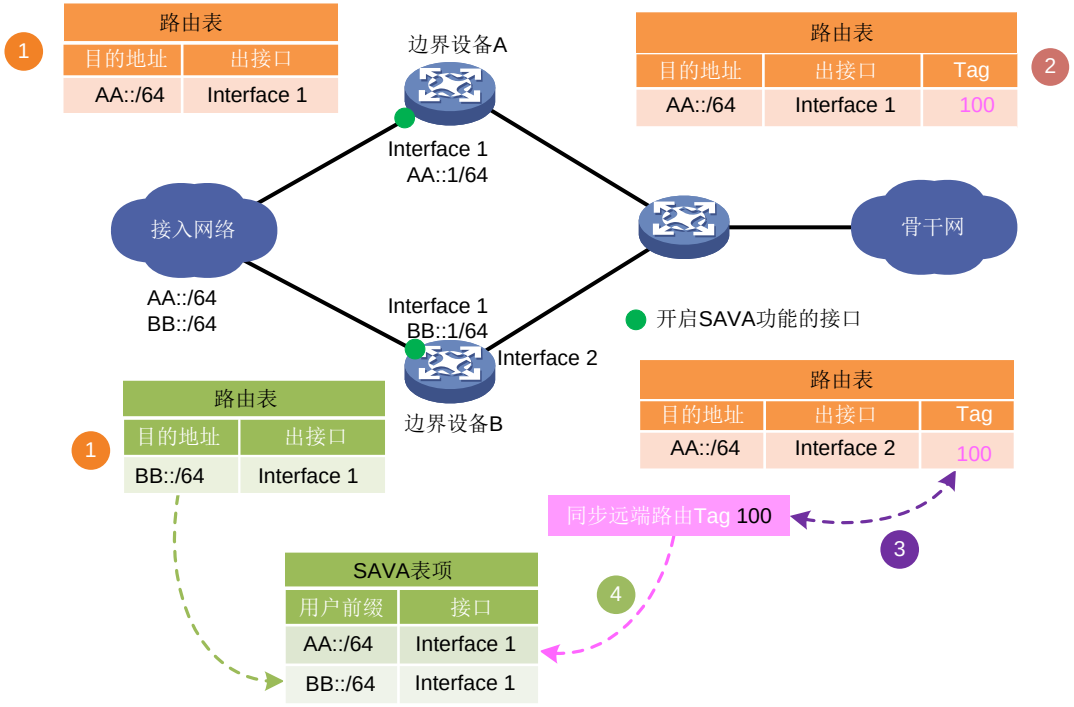
(1) 边界设备 A 和 B 分别从本地学习的、到达接入网络的路由信息中获取用户前缀，这些路由信息包括与接入网络相连的直连路由、静态路由和动态路由。本例中以静态路由为例来说明。

(2) 边界设备 A 为本地学习的、到达接入网络的路由信息通过路由策略配置特定路由信息的 Tag，并将此路由信息引入骨干网的动态路由协议中。

(3) 边界设备 B 通过动态路由协议学习到设备 A 发布的带有 Tag 的路由信息。如果路由信息中的 Tag 值与边界设备 B 上配置的同步远端路由条目的 Tag 值相同，则边界设备 B 从该路由信息中获取边界设备 A 学习到的合法用户前缀信息，用于生成 SAVA 表项。

(4) 边界设备 B 将根据本地路由和远端同步路由获取到的所有的合法用户前缀信息来生成与该接口绑定的 SAVA 表项。SAVA 表项信息包含合法用户前缀、前缀长度和绑定的接口。

图7 SAVA 表项生成过程



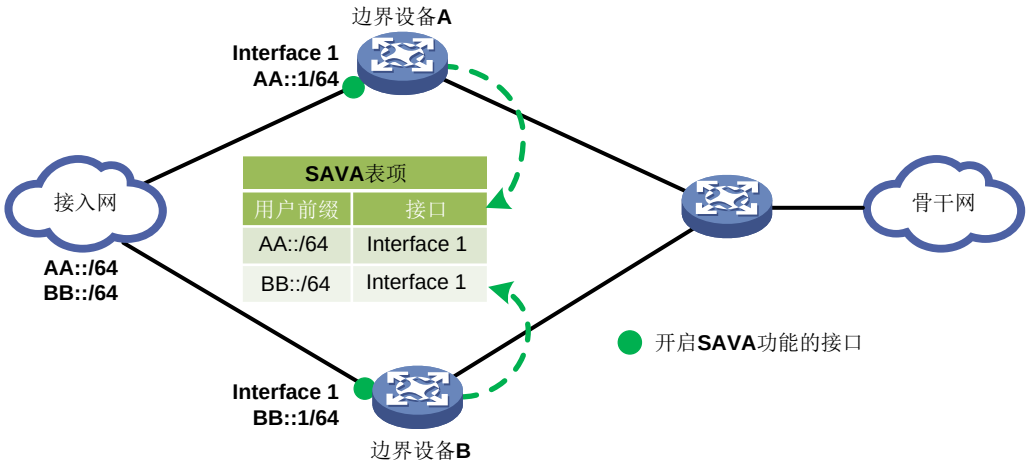
3.4 SAVA典型应用场景

3.4.1 边界设备与接入网络直连场景

此场景中，接入网络中的用户直接通过边界设备 A 和 B 双归属接入骨干网。接入网络具有多个网段。边界设备上，接入网络侧的接口地址前缀只有部分与接入网络内合法用户前缀相同。

在边界设备 A 和 B 与接入网络侧相连的接口上均配置 SAVA 功能后，边界设备 A 和 B 将根据本地路由和远端同步路由获取到的所有的合法用户前缀信息来生成与该接口绑定的 SAVA 表项，解决了严格型 uRPF 只根据本地路由表来检查造成的误判断。通过配置 SAVA 功能，接入网络中所有来自合法前缀的用户发送的报文，均能在任意边界设备上通过源地址验证，访问骨干网。

图8 边界设备与接入网络直连场景典型组网图

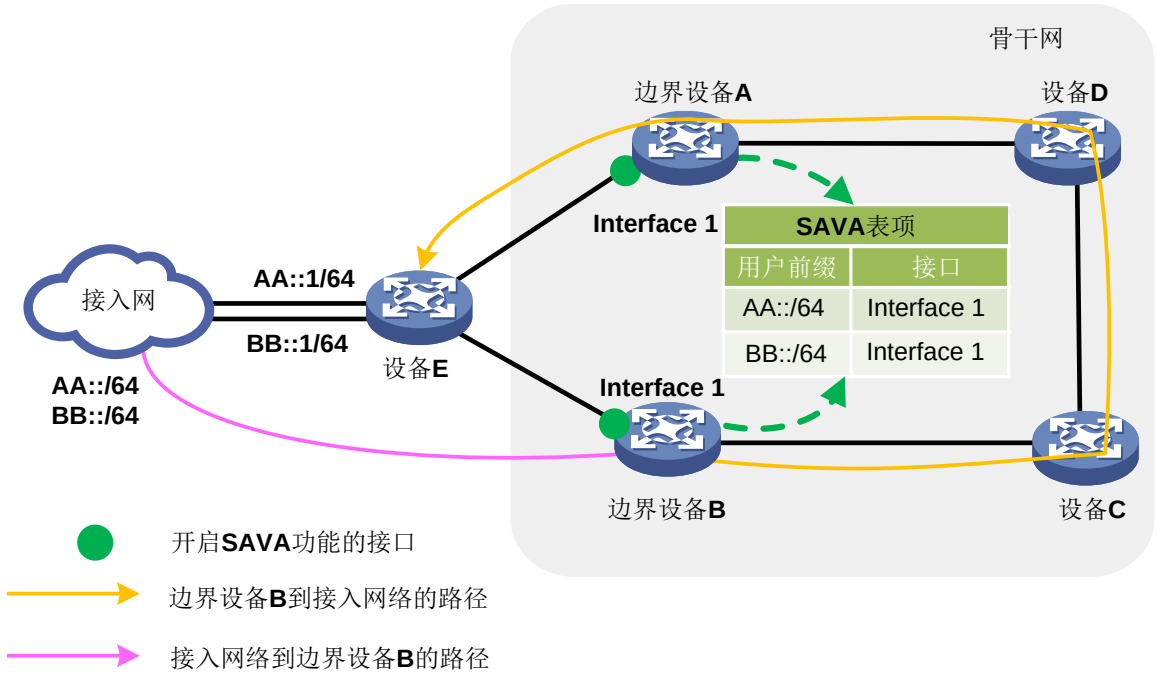


3.4.2 边界设备与接入网络非直连场景

此场景中，接入网络的用户通过一台中间设备接入到边界设备 A 和 B。接入网络的上下行流量可能存在不对称的情况。比如，路由收敛完毕后，边界设备 B 到接入网络的路径为边界设备 B→设备 C→设备 D→边界设备 A→设备 E→接入网络，接入网络到边界设备 B 的路径为接入网络→设备 E→边界设备 B。

在边界设备 A 和 B 与接入网络侧相连的接口上均配置 SAVA 功能后，接入网络中所有来自合法前缀的用户的报文，均能在任意边界设备通过源地址验证，访问骨干网。

图9 边界设备与接入网络非直连场景典型组网图

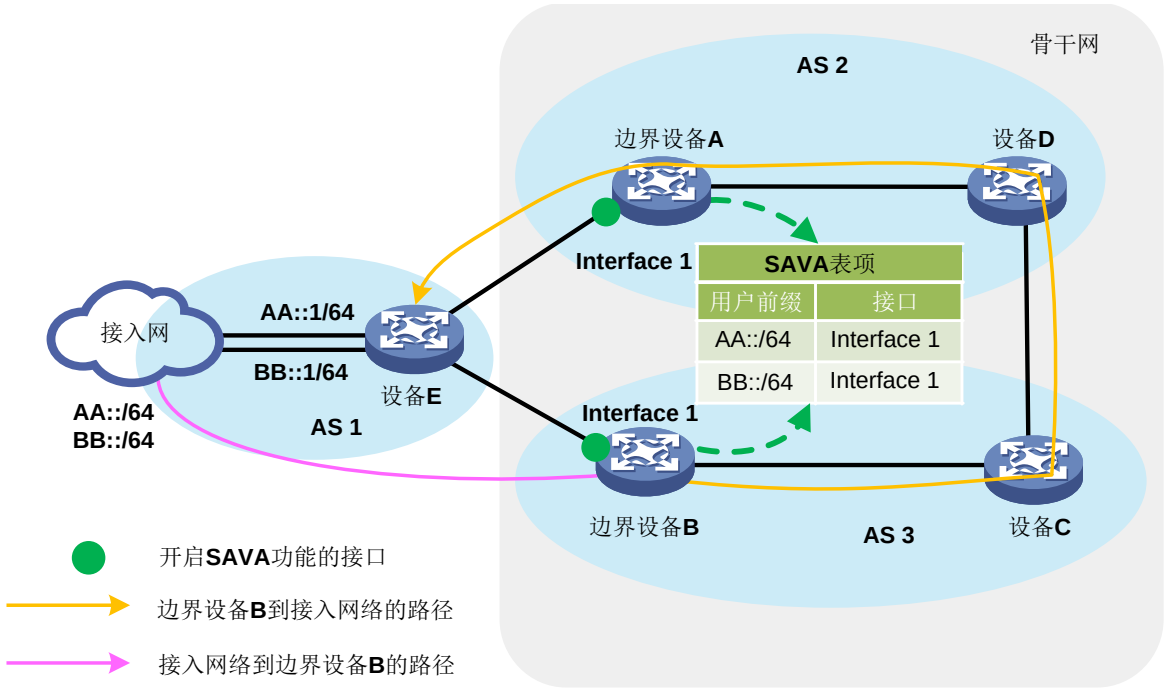


3.4.3 边界设备与接入网络非直连跨 AS 场景

此场景中，同一接入网络通过位于不同 AS 的边界设备接入到骨干网。接入网络的上下行流量可能存在不对称的情况。比如，路由收敛完毕后，边界设备 B 到接入网络的路径边界设备 B→设备 C→设备 D→边界设备 A→设备 E→接入网络，接入网络到边界设备 B 的路径为接入网络→设备 E→边界设备 B。

在边界设备 A 和 B 与接入网络侧相连的接口上均配置 SAVA 功能后，接入网络中所有来自合法前缀的用户发送的报文，均能在任意边界设备上通过源地址验证，访问骨干网。其中，每个 AS 域内设备之间通过域内路由协议（比如 OSPFv3）同步路由条目，AS 域间设备通过 BGP 协议同步路由条目。

图10 边界设备与接入网络非直连跨 AS 场景典型组网图



4 SMA 技术实现

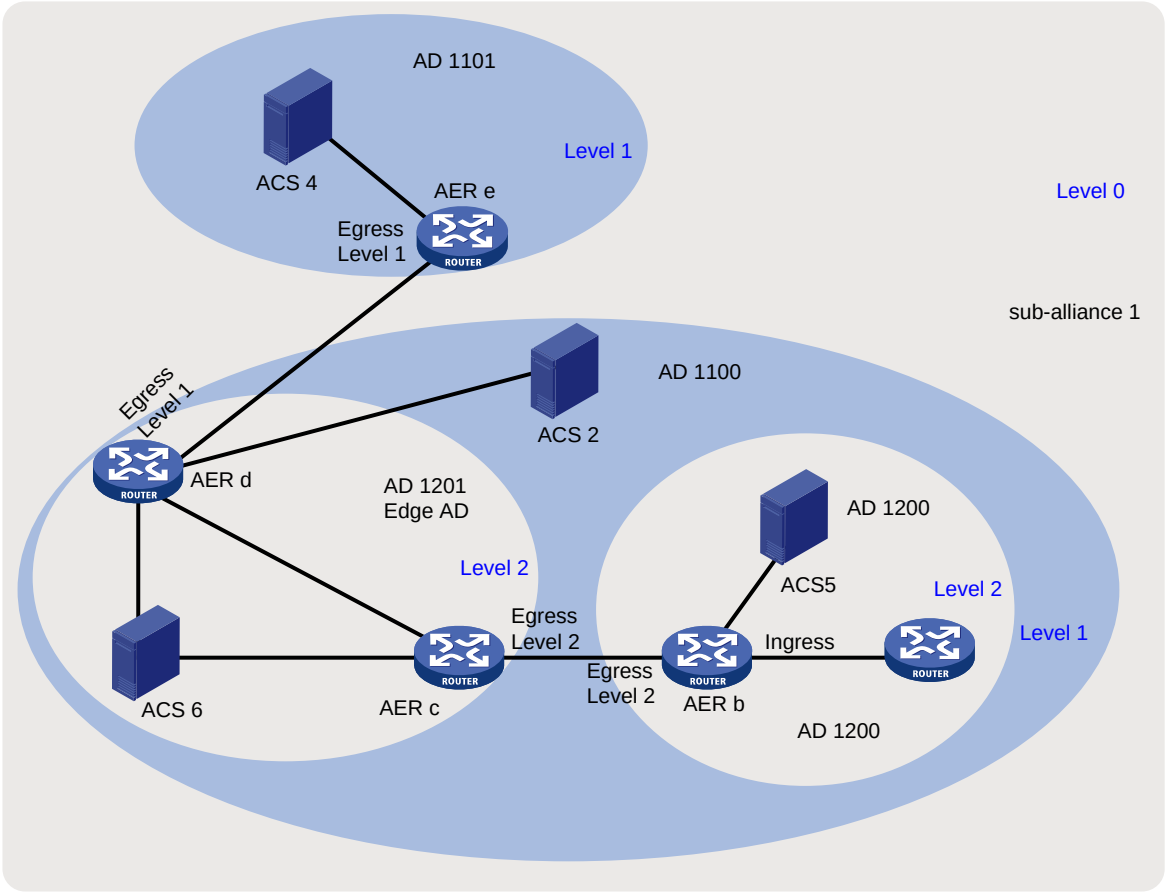
4.1 SMA简介

SMA 是一种 IPv6 自治系统间端到端的源地址验证方案，通过在 AS 之间建立信任联盟来进行 IPv6 源地址的验证。在地址域的边界设备 AER 上部署 SMA 功能，在 AER 上检查报文的源 IPv6 地址和报文标签，实现防止伪造源 IPv6 地址的攻击。

4.2 SMA体系结构

SMA 体系主要由 ACS（AS Control Server，AS 控制服务器）和 AER（AS Edge Router，AS 边界路由器）构成，如图 11 所示。

图11 SMA 体系结构



4.3 SMA基本概念

- 子信任联盟：彼此信任的一组 AD（Addrees Domain，地址域）组成的集合，通过子信任联盟号来标识，如图 12 中的 sub-alliance 1。
- 信任联盟：SMA 体系中所有 AD 的集合。
- AD（Addrees Domain，地址域）：同一个机构下所管理的所有 IP 地址部署的范围，是子信任联盟管理的对象，通过地址域编号来标识，比如，上图中的 AD 1101、AD 1200 和 AD 1201。同一个子联盟内的不同的地址域可以分成不同的地址域层级，最多可以划分为 4 层。比如，上图中的 Level 0、Level 1 和 Level 2。其中，Level 0 为最高地址级别，Level 2 为最低地址级别。例如，首先以县市为单位划分多个一级地址域，再以机构为单位划分多个二级地址域（比如学校、企事业单位），以楼宇或部门为单位划分三级地址域。
  - 边界地址域：当前层级的地址域中与其他层级相连的地址域。比如，图 12 中的 AD 1201。
  - 非边界地址域：除了边界地址域的其他地址域。比如，图 12 中的 AD 1101 和 AD 1200。

  当一个地址域划分了更低级别的地址域后，原地址域中所有的设备都必须从属于更低级别的地址域中。如图 12 所示，Level 0 的地址域中划分了低一级别的地址域 Level 1，那么属于 Level 0 的所有设备都必须从属于划分后的 Level 1 地址域。

- ACS（AS Control Server，AS 控制服务器）：每个层级的地址域都需要有相应的 ACS，用于和其它地址域内的 ACS 交互信息，并向本地址域内的 AER 宣告、更新注册信息、前缀信息以及状态机信息。具体来讲，ACS 具有如下功能：
  - 与属于相同信任联盟中各子信任联盟的其他 ACS 建立连接，交互各地址域内的 IPv6 地址前缀、状态机等信息。
  - 向本地址域 AER 宣告和更新联盟映射关系、地址前缀信息以及状态机生成的标签信息。
- AER（AS Edge Router，AS 边界路由器）：负责接收 ACS 通告的 IPv6 地址前缀、标签等信息，并在地址域之间转发报文。一个 AER 可以是多个不同层级地址域的边界路由器。AER 上的接口可配置为如下两种类型：
  - Ingress 接口：连接到本地址域内部未开启 SMA 功能的路由器的接口。
  - Egress 接口：连接到其他地址域的 AER 的 Egress 接口。


说明

- 目前，我司设备只能作为 AER。
- 为了提高安全性，ACS 与 ACS 之间、ACS 与 AER 之间的通信均基于 TCP 协议，并可配置为基于 SSL（Secure Sockets Layer，安全套接字层）的连接。
- ACS 之间互相协商用于生成和更新标签的状态机，并将状态机部署到本地址域的 AER 上。报文在通过地址域边界时需要根据地址域级别替换 SMA 标签。
- SMA 标签作为一个新类型的 Option 加入 IPv6 的 Destination Option Header 中，这种新定义的 Option 称作 SMA Option。

4.4 SMA运行机制

SMA 通过在 AER 上检查报文的源 IPv6 地址和报文标签实现对伪造源 IPv6 地址攻击的防御。报文在通过地址域边界时需要根据地址域级别替换 SMA 标签。报文离开地址域时，根据源 IPv6 地址和当前 AER 同属的最低级别地址域替换标签；报文进入地址域时，根据目的 IPv6 地址和当前 AER 同属的最低级别地址域替换标签。

1. AER 接收报文时的处理过程

AER 接收到报文后，处理过程如图 12 所示。

(1) 检查接收报文的接口类型是否为 Ingress。
  - 若接口类型是 Ingress，则进入步骤(2)。
  - 若接口类型是 Egress，则进入步骤(3)。

(2) 检查报文源地址前缀是否属于当前地址域。
  - 若属于当前地址域，则继续按照 IPv6 路由表转发该报文。
  - 若不属于当前地址域，则丢弃报文。

(3) 检查报文目的 IPv6 地址是否属于本子联盟：
  - 若不属于本子联盟，则继续按照 IPv6 路由表转发该报文。
  - 若属于本子联盟，则进入步骤(4)。

(4) 检查报文的目的 IPv6 地址是否属于本地址域以及本域内更低级别地址域：

- 若不属于，则继续按照 IPv6 路由表转发该报文。
- 若属于，则进入步骤(5)。

(5) 校验报文的子联盟内标签。

- 校验成功，进入步骤(6)。
- 校验失败，丢弃该报文。

(6) 检查报文是否需要向本地域内更低级别的地址域转发。

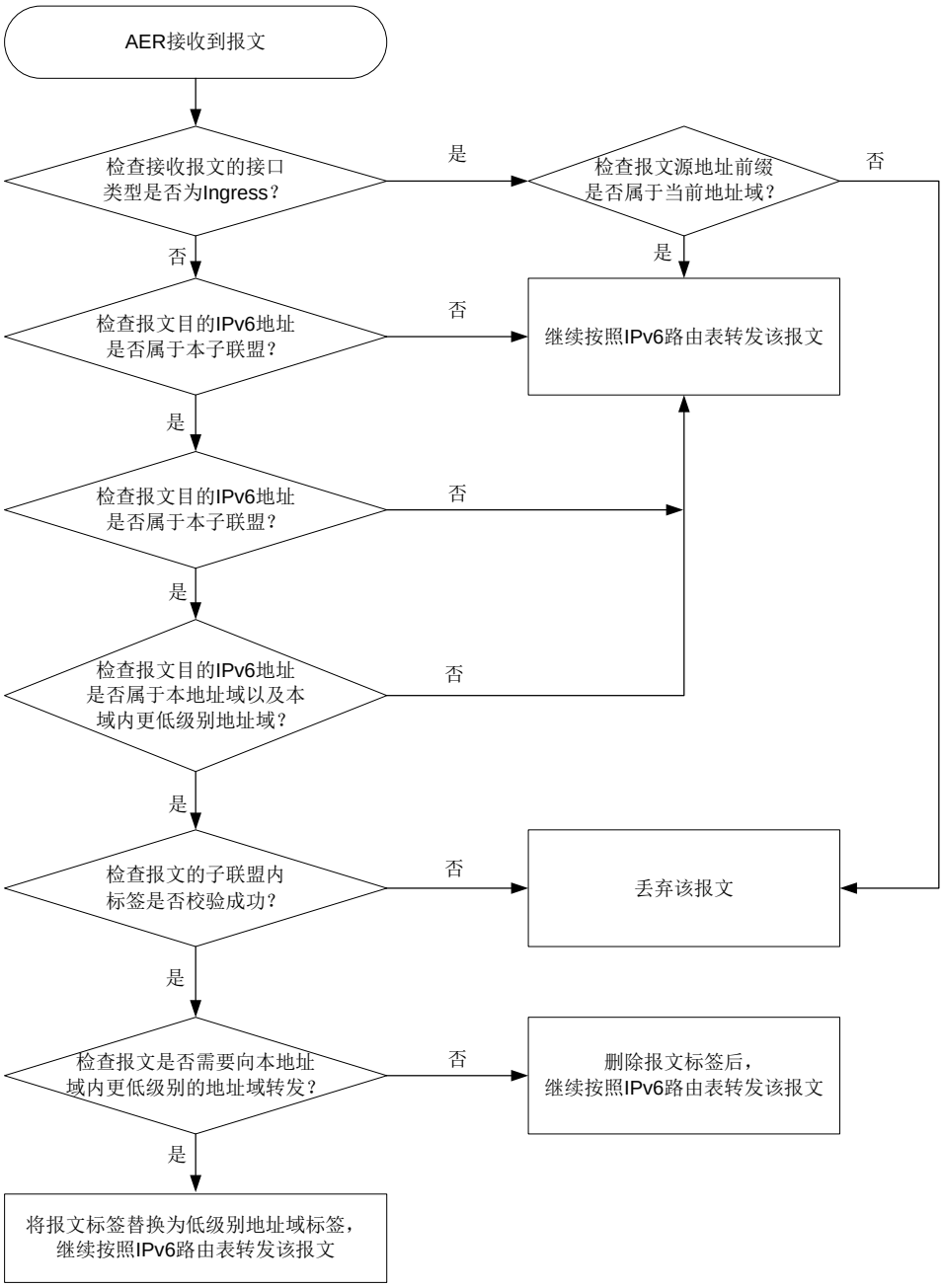
- 若不需要，删除报文标签后，继续按照 IPv6 路由表转发该报文。
- 若需要，则将报文标签替换为低级别地址域标签，继续按照 IPv6 路由表转发该报文。

说明

报文中携带的 Common level（AER 与 IPv6 前缀所属的公共地址域最高级别）与收到报文接口的地址域进行比较，若 Commen level 比接口的地址域级别高，报文就不需要向本地址域内更低级别的地址域转发，否则就需要向本地址域内更低级别的地址域转发。

低级别地址域内的 AER 收到报文后，继续按照如上步骤进行处理。

图12 AER 接收报文时的处理过程



2. AER 发送报文时的处理过程

当 AER 从 Egress 口接收到报文并发往其他地址域时，处理过程如图 13 所示。

(1) 判断报文源地址前缀是否属于当前地址域。

- 若属于，对报文添加标签后，继续按照 IPv6 路由表转发该报文。
- 若不属于，则进入步骤(2)。

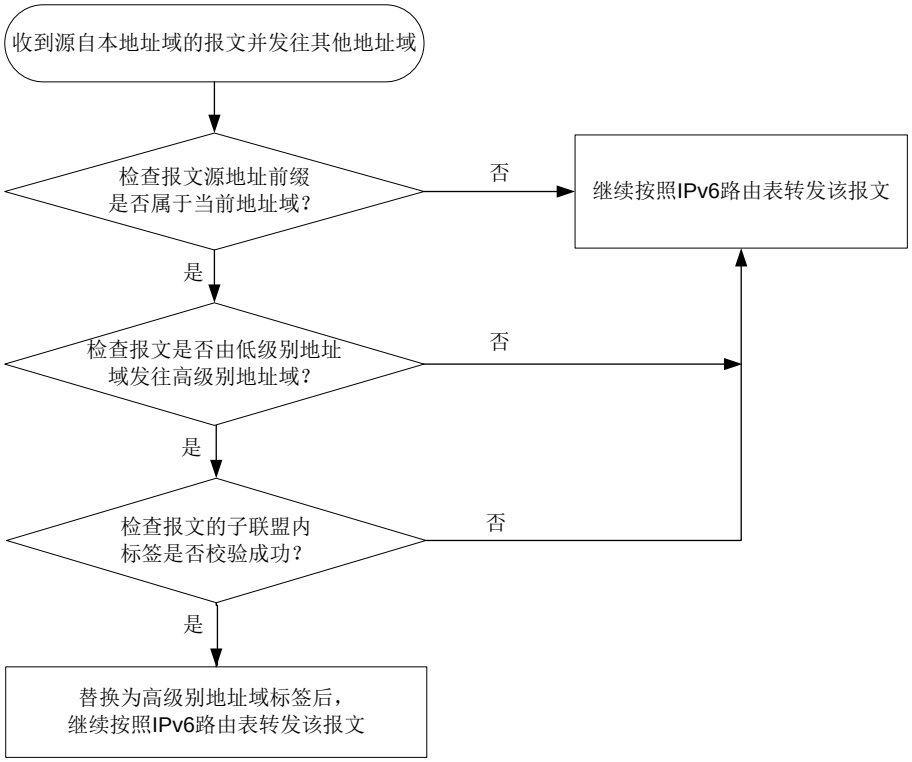
(2) 检查报文是否由低级别地址域发往高级别地址域。

- 若是，则需要校验标签，进入步骤(3)。
- 若不是，则继续按照 IPv6 路由表转发该报文。

(3) 校验报文的子联盟内的标签。

- 校验成功，替换为高级别地址域标签后，继续按照 IPv6 路由表转发该报文。
- 校验失败，丢弃该报文。

图13 AER 发送报文时的处理过程

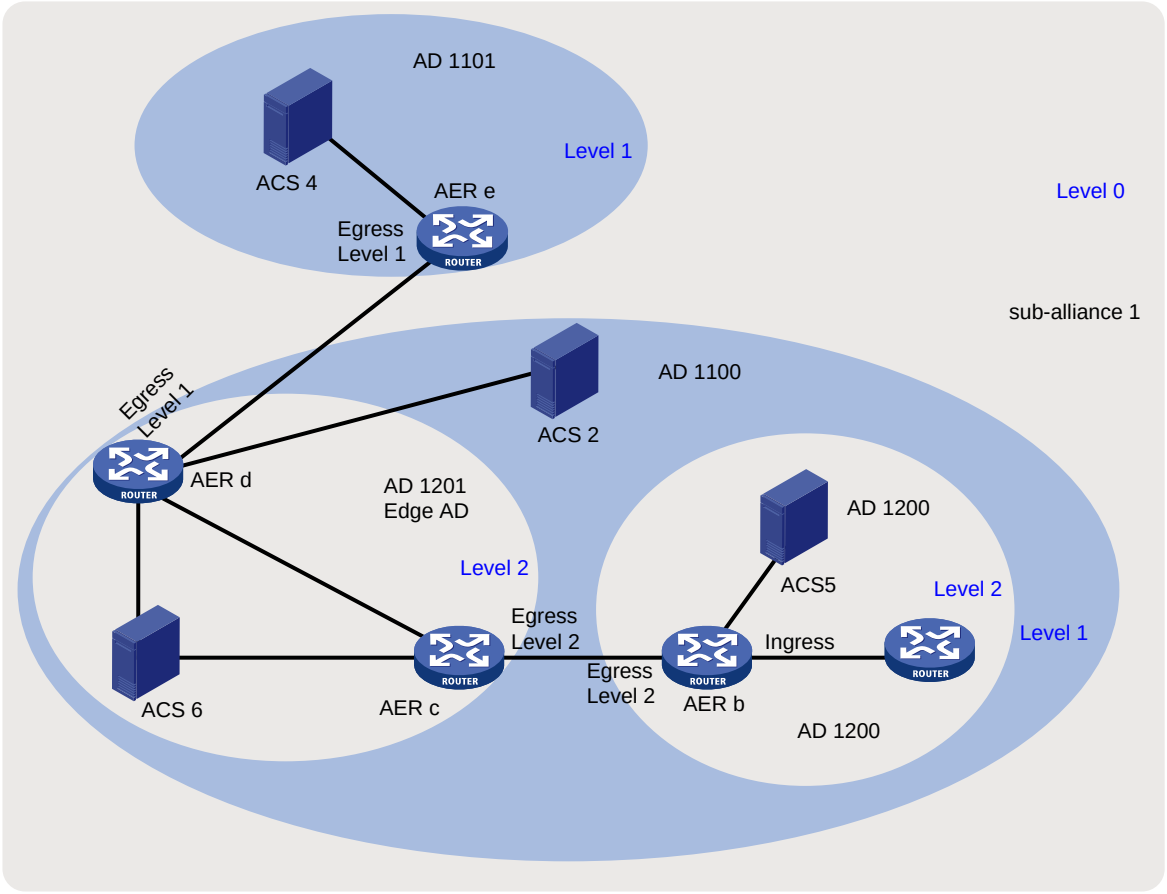


4.5 SMA典型应用场景

如图 14 所示，AER b 是二级地址域 AD 1200 的边界路由器，AER c 是二级地址域 AD 1201 的边界路由器；AER d 是一级地址域 AD 1100 和二级地址域 AD 1201 的边界路由器，AER e 是一级地址域 AD 1101 的边界路由器。AD 1201 是 AD 1100 的边界地址域，AD 1100、AD 1101 和 AD 1200 是非边界地址域。AD 1100、AD 1101 和 AD 1200 和 AD 1201 同属于子联盟 1。

ACS 和 AER 之间使用 SSL 或者 TCP 建立连接，在 AER 上可以收到由 ACS 发送的 IPv6 地址前缀及标签信息。AER 将根据该地址前缀及标签信息检查报文，防止伪造源 IPv6 地址的攻击。

图14 SMA 典型组网图



5 参考文献

- RFC 6602：FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses
- RFC 7039：Source Address Validation Improvement (SAVI) Framework
- RFC 7513：Source Address Validation Improvement (SAVI) Solution for DHCP
- RFC 8074：Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario
- draft-li-savnet-intra-domain-problem-statement-00：Source Address Validation in Intra-domain Networks (Intra-domain SAVNET) Gap Analysis, Problem Statement and Requirements
- draft-wu-savnet-inter-domain-problem-statement-00：Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Problem Statement and Requirements