(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107547558 B
(45)授权公告日 2020.09.08

(21)申请号 201710840584.7

(22)申请日 2017.09.18

(65)同一申请的已公布的文献号
申请公布号 CN 107547558 A

(43)申请公布日 2018.01.05

(73)专利权人 新华三技术有限公司
地址 310052 浙江省杭州市滨江区长河路466号

(72)发明人 徐燕成

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 105306353 A,2016.02.03
CN 105791458 A,2016.07.20
US 2012309416 A1,2012.12.06
LIU Bingyang.SMA: State Machine based Anti-spoofing.《中国科技论文在线》.2013,全文.

审查员 谭菲菲

权利要求书3页 说明书9页 附图5页

(54)发明名称

一种SMA组网的接入方法和装置

(57)摘要

本申请提供一种基于状态机的伪造源地址检查SMA组网的接入方法和装置,SMA组网中的自治系统AS边界路由器AER执行以下方法:接收SMA组网外的终端发送的第一报文;获取所述第一报文的SMA报文头中的指定位;如果所述指定位的值与第一预设值匹配,则确认所述第一报文为由SMA组网外的终端发送给SMA组网内的自治系统控制服务器ACS的认证报文;将所述认证报文重定向到本AS内的ACS进行认证;接收所述ACS返回的认证结果,如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS。如此,便完成了SMA组网外终端接入SMA组网的过程,实现了SMA组网外终端的远程办公。



CN 107547558 B

1.一种基于状态机的伪造源地址检查SMA组网的接入方法,其特征在于,所述方法应用于SMA组网中的自治系统AS边界路由器AER,包括:

接收SMA组网外的终端发送的第一报文,所述终端属于非信任联盟;

获取所述第一报文的SMA报文头中的指定位;

如果所述指定位的值与第一预设值匹配,则确认所述第一报文为由SMA组网外的终端发送给SMA组网内的自治系统控制服务器ACS的认证报文;

将所述认证报文重定向到本AS内的ACS进行认证;

接收所述ACS返回的认证结果,如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS。

2.如权利要求1所述的方法,其特征在于,所述接收所述ACS返回的认证结果,如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS,包括:

接收所述ACS返回的第二报文,所述第二报文的SMA报文头中的所述指定位的值为第二预设值,所述第二预设值用于表征所述第二报文为认证应答报文;

将所述认证应答报文转发给所述终端;

其中,当所述认证应答报文的SMA报文头中携带报文标签时,表征认证结果为通过,所述AER允许所述终端访问本AS;当所述认证应答报文的SMA报文头中不携带报文标签时,表征认证结果为不通过,所述AER禁止所述终端访问本AS;所述报文标签用于携带在所述终端与本AS之间来往的数据报文中。

3.如权利要求2所述的方法,其特征在于,所述AER允许所述终端访问本AS,包括:

保存与所述终端对应的SMA表项,该SMA表项记录有所述报文标签与所述终端的IP地址之间的对应关系;

基于该SMA表项在所述终端和本AS之间传输数据报文。

4.如权利要求2所述的方法,其特征在于,所述方法还包括:

如果所述第一报文的SMA报文头中的指定位的值与第三预设值匹配,则确认所述第一报文为由SMA组网外的终端发送给SMA组网内的ACS的发现报文;所述发现报文用于发现SMA组网中的ACS;

将所述发现报文重定向到本AS内的ACS;

接收所述ACS返回的第三报文,所述第三报文的SMA报文头中的所述指定位的值为第四预设值,所述第四预设值用于表征所述第三报文为发现应答报文;

将所述发现应答报文转发给所述终端,所述发现应答报文用于告知终端本AS内的ACS能够提供认证服务,以使所述终端向所述ACS发送认证报文。

5.如权利要求4所述的方法,其特征在于,所述发现报文和所述认证报文的目的IP地址为超文本传输协议HTTP服务器地址;

所述方法还包括:

建立针对所述终端的临时表项,所述临时表项中记录有所述HTTP服务器地址和所述终端的IP地址之间的对应关系;

在将所述发现报文和所述认证报文重定向到本AS内的ACS时,将所述发现报文和所述认证报文的目的IP地址修改为所述ACS的IP地址,并将修改后的所述发现报文和所述认证

报文转发给所述ACS;以及

在将所述发现应答报文和所述认证应答报文转发给所述终端时,将所述发现应答报文和所述认证应答报文的源IP地址修改为所述临时表项中记录的所述HTTP服务器地址,并将修改后的所述发现应答报文和所述认证应答报文转发给所述终端。

6.如权利要求1所述的方法,其特征在于,所述方法还包括:

接收所述ACS发送的针对所述终端的静默表项,所述静默表项用于指示所述终端认证超时或认证出错达到设定次数;

在预设时长内,禁止向所述ACS转发来自所述终端的报文。

7.如权利要求1-4中任一项所述的方法,其特征在于,所述指定位位于SMA报文头的DATA字段或预留字段中。

8.一种基于状态机的伪造源地址检查SMA组网的接入方法,其特征在于,所述方法应用于SMA组网外的终端,所述终端属于非信任联盟,包括:

生成报文并为生成的报文封装SMA头;所述SMA头中的指定位的值为第一预设值,所述第一预设值用于表征所述报文为认证报文;

将封装后的报文发送给SMA组网中的自治系统AS边界路由器AER,以使AER根据所述指定位的值将收到的报文重定向到自治系统控制服务器ACS进行认证。

9.一种自治系统AS边界路由器AER,其特征在于,包括:

接收单元,用于接收SMA组网外的终端发送的第一报文,所述终端属于非信任联盟;

获取单元,用于获取所述第一报文的SMA报文头中的指定位;

确认单元,用于在所述指定位的值与第一预设值匹配时,确认所述第一报文为由SMA组网外的终端发送给SMA组网内的自治系统控制服务器ACS的认证报文;

发送单元,用于将所述认证报文重定向到本AS内的ACS进行认证;

所述接收单元,还用于接收所述ACS返回的认证结果;如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS。

10.如权利要求9所述的AER,其特征在于,所述接收所述ACS返回的认证结果,如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS,包括:

所述接收单元,还用于接收所述ACS返回的第二报文,所述第二报文的SMA报文头中的所述指定位的值为第二预设值,所述第二预设值用于表征所述第二报文为认证应答报文;

所述发送单元,还用于将所述认证应答报文转发给所述终端;

其中,当所述认证应答报文的SMA报文头中携带报文标签时,表征认证结果为通过,所述AER允许所述终端访问本AS;当所述认证应答报文的SMA报文头中不携带报文标签时,表征认证结果为不通过,所述AER禁止所述终端访问本AS;所述报文标签用于携带在所述终端与本AS之间来往的数据报文中。

11.如权利要求10所述的AER,其特征在于,所述AER还包括:

SMA表项建立单元,用于在所述AER允许所述终端访问本AS时,保存与所述终端对应的SMA表项,该SMA表项记录有所述报文标签与所述终端的IP地址之间的对应关系;

所述发送单元和所述接收单元,还用于基于该SMA表项在所述终端和本AS之间传输数据报文。

12.如权利要求10所述的AER,其特征在于,

所述确认单元,还用于在所述第一报文的SMA报文头中的指定位的值与第三预设值匹配时,确认所述第一报文为由SMA组网外的终端发送给SMA组网内的ACS的发现报文;所述发现报文用于发现SMA组网中的ACS;

所述发送单元,还用于将所述发现报文重定向到本AS内的ACS;

所述接收单元,还用于接收所述ACS返回的第三报文,所述第三报文的SMA报文头中的所述指定位的值为第四预设值,所述第四预设值用于表征所述第三报文为发现应答报文;

所述发送单元,还用于将所述发现应答报文转发给所述终端,所述发现应答报文用于告知终端本AS内的ACS能够提供认证服务,以使所述终端向所述ACS发送认证报文。

13.如权利要求12所述的AER,其特征在于,所述发现报文和所述认证报文的目的IP地址为超文本传输协议HTTP服务器地址;

所述AER还包括:

临时表项建立单元,用于建立针对所述终端的临时表项,所述临时表项中记录有所述HTTP服务器地址和所述终端的IP地址之间的对应关系;

所述发送单元,在将所述发现报文和所述认证报文重定向到本AS内的ACS时,用于将所述发现报文和所述认证报文的目的IP地址修改为所述ACS的IP地址,并将修改后的所述发现报文和所述认证报文转发给所述ACS;以及,在将所述发现应答报文和所述认证应答报文转发给所述终端时,用于将所述发现应答报文和所述认证应答报文的源IP地址修改为所述临时表项中记录的所述HTTP服务器地址,并将修改后的所述发现应答报文和所述认证应答报文转发给所述终端。

14.如权利要求9所述的AER,其特征在于,

所述接收单元,还用于接收所述ACS发送的针对所述终端的静默表项,所述静默表项用于指示所述终端认证超时或认证出错达到设定次数;

所述发送单元,还用于在所述接收单元收到所述静默表项后,在预设时长内禁止向所述ACS转发来自所述终端的报文。

15.如权利要求9-12中任一项所述的AER,其特征在于,所述指定位位于SMA报文头的DATA字段或预留字段中。

16.一种终端,其特征在于,所述终端位于基于状态机的伪造源地址检查SMA组网外,所述终端属于非信任联盟,所述终端包括:

报文处理单元,用于生成报文并为生成的报文封装SMA头;所述SMA头中的指定位的值为第一预设值,所述第一预设值用于表征所述报文为认证报文;

发送单元,用于将封装后的报文发送给SMA组网中的自治系统AS边界路由器AER,以使AER根据所述指定位的值将收到的报文重定向到自治系统控制服务器ACS进行认证。

一种SMA组网的接入方法和装置

技术领域

[0001] 本申请涉及通信技术领域,尤其涉及一种SMA组网的接入方法和装置。

背景技术

[0002] SMA(State Machine based Anti-spoofing,基于状态机的伪造源地址检查)网络是一种IPv6(Internet Protocol Version 6,第6版互联网协议)自治系统间端到端的源地址验证方案,用来防止伪造源IPv6地址的攻击。该SMA网络包括相互信任的AS(Autonomous System,自治系统)组成的信任联盟,该AS包括ACS(AS Control Server,AS控制服务器)和与该ACS相连的AER(AS Edge Router,AS边界路由器)。

[0003] ACS向REG(Registration Center,联盟注册中心)注册成为信任联盟的成员后,REG负责将ACS的注册信息通知给同一个信任联盟内的其他成员ACS,使得ACS获知与哪些ACS属于同一个信任联盟,该ACS会与其他成员ACS建立连接,并将本地及从信任联盟中的其他ACS学习到的IPv6地址前缀和报文标签等信息发送给本AS的AER,以便AER根据IPv6地址前缀和报文标签等信息转发接收到的数据报文。

[0004] 对于属于非信任联盟的AS发送的报文,该报文在进入AER时会被AER识别出来并被丢弃,以保证信任联盟内的AS不会受到非信任联盟或者非法主机的攻击。

发明内容

[0005] 有鉴于此,本申请提供一种SMA组网的接入方法和装置,以解决SMA组网外终端无法接入SMA组网的问题。

[0006] 具体地,本申请是通过如下技术方案实现的:

[0007] 本申请第一方面,提供了一种SMA组网的接入方法,所述方法应用于SMA组网中的AER,包括:

[0008] 接收SMA组网外的终端发送的第一报文;

[0009] 获取所述第一报文的SMA报文头中的指定位;

[0010] 如果所述指定位的值与第一预设值匹配,则确认所述第一报文为由SMA组网外的终端发送给SMA组网内的ACS的认证报文;

[0011] 将所述认证报文重定向到本AS内的ACS进行认证;

[0012] 接收所述ACS返回的认证结果,如果认证结果为通过,则允许所述终端访问本AS;如果认证结果为不通过,则禁止所述终端访问本AS。

[0013] 本申请第二方面,提供了一种SMA组网的接入方法,所述方法应用于SMA组网外的终端,包括:

[0014] 生成报文并为生成的报文封装SMA头;所述SMA头中的指定位的值为第一预设值,所述第一预设值用于表征所述报文为认证报文;

[0015] 将封装后的报文发送给SMA组网中的AER,以使AER根据所述指定位的值将收到的报文重定向到ACS进行认证。

[0016] 本申请第三方面，提供了一种AER，具有实现上述第一方面所述方法的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。

[0017] 一种可能的实现方式中，所述AER包括：

[0018] 接收单元，用于接收SMA组网外的终端发送的第一报文；

[0019] 获取单元，用于获取所述第一报文的SMA报文头中的指定位；

[0020] 确认单元，用于在所述指定位的值与第一预设值匹配时，确认所述第一报文为由SMA组网外的终端发送给SMA组网内的自治系统控制服务器ACS的认证报文；

[0021] 发送单元，用于将所述认证报文重定向到本AS内的ACS进行认证；

[0022] 所述接收单元，还用于接收所述ACS返回的认证结果；如果认证结果为通过，则允许所述终端访问本AS；如果认证结果为不通过，则禁止所述终端访问本AS。

[0023] 另一种可能的实现方式中，所述AER包括通信接口、处理器、存储器和总线，所述通信接口、所述处理器和所述存储器之间通过总线相互连接；所述处理器通过读取所述存储器中存储的逻辑指令，执行本申请第一方面所述的SMA组网的接入方法。

[0024] 本申请第四方面，提供了一种终端，所述终端位于SMA组网外，具有实现上述第二方面所述方法的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块或单元。

[0025] 一种可能的实现方式中，所述终端包括：

[0026] 报文处理单元，用于生成报文并为生成的报文封装SMA头；所述SMA头中的指定位的值为第一预设值，所述第一预设值用于表征所述报文为认证报文；

[0027] 发送单元，用于将封装后的报文发送给SMA组网中的AER，以使AER根据所述指定位的值将收到的报文重定向到ACS进行认证。

[0028] 另一种可能的实现方式中，所述终端包括通信接口、处理器、存储器和总线，所述通信接口、所述处理器和所述存储器之间通过总线相互连接；所述处理器通过读取所述存储器中存储的逻辑指令，执行本申请第二方面所述的SMA组网的接入方法。

[0029] 本申请为SMA报文头的原有字段赋予了新的含义，AER在收到SMA组网外的终端发送的报文时，并不立即丢弃该报文，而是先检查该报文的SMA报文头中的指定位的值，如果该值与预先配置的第一预设值匹配，则认为该报文为认证报文，从而将该报文重定向到本AS内的ACS进行认证，如果认证通过，该SMA网络外的终端便可以加入并访问SMA网络，实现远程办公。

附图说明

[0030] 图1是本申请提供的一种SMA组网示意图；

[0031] 图2是本申请提供的方法流程图；

[0032] 图3是本申请提供的SMA组网外终端、AER、ASC三者之间的交互流程图；

[0033] 图4是本申请提供的AER的功能模块框图；

[0034] 图5是本申请提供的图4所示AER的硬件架构图；

[0035] 图6是本申请提供的终端的功能模块框图；

[0036] 图7是本申请提供的图6所示终端的硬件架构图。

具体实施方式

[0037] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

[0038] 在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0039] 应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0040] 在图1所示的SMA组网中，SMA组网内部包括AS_A、AS_B和AS_C以及REG，SMA组网外部包括AS_D和AS_E；其中，该AS_A中的ACS_A、AS_B中的ACS_B和AS_C中的ACS_C会分别向REG进行注册，从而使得AS_A、AS_B和AS_C可以注册在同一信任联盟中，通过注册后，这三个ACS之间可以相互学习对方AS内配置的IPv6地址(或IPv6地址前缀)以及相互协商报文标签，并将得到的IPv6地址(或IPv6地址前缀)和报文标签发送给本AS的AER，以便AER可以根据IPv6地址前缀和报文标签等信息转发接收到的数据报文。在图1中，AS_D和AS_E对于SMA网络而言属于非信任联盟，对于来源于AS_D和AS_E的报文，其在进入SMA组网时，会被SMA组网中的边缘设备AER识别出来并丢弃。

[0041] 由于SMA组网的上述特性，导致在实际环境下，如在企业内网、校园网络中应用SMA组网模式时，用户只能在SMA组网内办公，无法远程办公。

[0042] 为解决这一问题，本申请提供了一种针对SMA组网外终端的认证方案，SMA组网中的ACS对SMA组网外的终端认证通过后，SMA组网外的终端便能正常访问SMA组网。

[0043] 以下，首先对本申请涉及的部分概念进行解释说明。

[0044] 第一预设值至第六预设值：本申请中SMA组网外的终端如果要访问SMA组网，需要先获得SMA组网中的ACS的认证。为实现这一认证过程，本申请为原有的SMA报文头中的原有字段赋予了新的含义，具体如下：

[0045] 1)当报文的SMA报文头中的指定位为第一预设值时，表示该报文为由SMA组网外的终端发送给SMA组网内的ACS的认证报文，认证报文中携带终端的用户名和密码，可以用于请求ACS对终端的合法性进行认证，也可以用于请求ACS对已认证通过的终端进行续约；

[0046] 2)当报文的SMA报文头中的指定位为第二预设值时，表示该报文为由SMA组网内的ACS发送给SMA组网外的终端的认证应答报文，认证应答报文用于通告终端是否通过认证；若认证通过，则认证应答报文中还将携带ACS为终端分配的报文标签；

[0047] 3)当报文的SMA报文头中的指定位为第三预设值时，表示该报文为由SMA组网外的终端发送给SMA组网内的ACS的发现报文，终端可以在发送认证报文之前先发送发现报文，以发现SMA组网中的ACS；

[0048] 4)当报文的SMA报文头中的指定位为第四预设值时,表示该报文为由SMA组网内的ACS发送给SMA组网外的终端的发现应答报文,发现应答报文用于告知终端本AS内的ACS能够提供认证服务,终端收到发现应答报文后将向该ACS发送上述认证报文;

[0049] 5)当报文的SMA报文头中的指定位为第五预设值时,表示该报文为由SMA组网外的终端发送给SMA组网内的设备(包括ACS、终端等)的数据报文;

[0050] 6)当报文的SMA报文头中的指定位为第六预设值时,表示该报文为由SMA组网内的设备发送给SMA组网外的终端的数据报文。

[0051] 报文标签:在同一个信任联盟内,根据各个AS之间数据报文的传输方向组成AS对,并设置对应该AS对的报文标签,例如,以AS1作为发送数据报文的源AS,AS2作为接收数据报文的目的AS,则该AS1和AS2组成一个有序的AS对,该AS对对应一个报文标签,该报文标签为在AS1向AS2发送数据报文时对应的报文标签。本地AS的ACS基于学习到的对方AS内配置的IPv6地址(或IPv6地址前缀)以及与对方AS的ACS协商的报文标签生成SMA表项,并下发给本地的AER,SMA表项中记录了IPv6地址(或IPv6地址前缀)与报文标签的对应关系。本地的AER在接收到数据报文后,根据该数据报文的地址信息和从本地的ACS接收到的SMA表项,对该数据报文进行过滤,具体是,如果该数据报文的地址信息和报文标签与本地保存的SMA表项匹配,则允许该数据报文的转发,否则便丢弃该数据报文。本申请中,ACS在对SMA组网外的终端认证通过后,也会为该SMA组网外的终端分配报文标签,这样,便能实现SMA组网外的终端与SMA组网内设备的通信。

[0052] 下面结合说明书附图和各实施例对本申请技术方案进行说明。

[0053] 参见图2,在一个实施方案中,为实现SMA组网外的终端能够接入SMA组网,SMA组网中的AER在运行过程中执行如下步骤:

[0054] 步骤201:接收SMA组网外的终端发送的第一报文。

[0055] 步骤202:获取该第一报文的SMA报文头中的指定位。

[0056] 步骤203:如果该指定位的值与第一预设值匹配,则确认该第一报文为由SMA组网外的终端发送给SMA组网内的ACS的认证报文。

[0057] 步骤204:将该认证报文重定向到本AS内的ACS进行认证。

[0058] 步骤205:接收该ACS返回的认证结果,如果认证结果为通过,则允许该终端访问本AS;如果认证结果为不通过,则禁止该终端访问本AS。

[0059] 从步骤201至步骤205可以看出,本申请为SMA报文头的原有字段赋予了新的含义,AER在收到SMA组网外的终端发送的报文时,并不立即丢弃该报文,而是先检查该报文的SMA报文头中的指定位的值,如果该值与预先配置的第一预设值匹配,则认为该报文为认证报文,从而将该报文重定向到本AS内的ACS进行认证,如果认证通过,该SMA网络外的终端便可以加入并访问SMA网络,实现远程办公。

[0060] 请参考图3,以下通过SMA组网外终端、SMA组网中的AER和ACS三者之间的交互,来阐述本申请的具体实施过程。

[0061] 步骤301:SMA组网外终端向AER发送SMA报文头中指定位的值为第三预设值的发现报文。

[0062] 由于SMA组网外的AS属于非信任联盟,因此SMA组网外终端在访问SMA组网时,会主动发起连接,并在发送的报文中加入SMA报文头。

[0063] 这里,终端发出的发现报文的源IP地址为终端IP地址,目的IP地址为终端访问的网址的HTTP(Hyper Text Transfer Protocol,超文本传输协议)服务器地址。

[0064] 步骤302:AER收到上述报文后,获取该报文的SMA报文头中的指定位,发现该指定位的值与第三预设值匹配,则确认该报文为由SMA组网外终端发送给ACS的发现报文,从而将该发现报文重定向到本AS内的ACS。

[0065] 其中,将发现报文重定向到ACS的过程具体为:将发现报文的目的IP地址修改为本AS内的ACS的IP地址,然后将修改后的发现报文转发给ACS。

[0066] 作为本申请的一个实施例,这里AER还可以建立针对该终端的临时表项,该临时表项中记录有该终端的IP地址和该终端访问的HTTP服务器地址之间的对应关系。

[0067] 临时表项可以有以下两个用途:

[0068] 第一,后续AER收到ACS发送给该SMA组网外终端的报文时,可以利用此临时表项对ACS响应的报文做地址转换,这样可以令SMA组网外终端无法感知ACS的真实地址,有效保护ACS。

[0069] 第二,在步骤302中,AER如果确定收到某终端发送的发现报文,可以先查找本地是否存在与该终端的IP地址匹配的临时表项,如果存在则丢弃该发现报文,如果不存在则将该发现报文重定向到本AS内的ACS。这么做的原因在于,SMA组网外终端在收到ACS的应答前可能会发送多个发现报文,如果AER上已存在与某终端的IP地址匹配的临时表项,表明AER已向ACS转发该终端的发现报文,因此可以丢弃重复发送的发现报文,以减少对ACS的冲击。

[0070] 步骤303:ACS收到上述SMA报文头中指定位的值为第三预设值的报文并确定该报文为发现报文后,将该指定位的值修改为第四预设值,并将报文的源IP地址和目的IP地址互换,然后将修改后的报文发送给AER。

[0071] 这里ACS发送给AER的报文即为发现应答报文,此报文的源IP地址为ACS的IP地址,目的IP地址为SMA组网外终端的IP地址,报文内容与上述发现报文相同。

[0072] 作为一个实施例,ACS在向AER发送发现应答报文的同时(或之后),还可以启动一定时器,等待终端发起认证。如果定时器超时仍未收到终端发送的认证报文,或者在定时器有效期间该终端认证出错达到设定次数(如认证不通过达到5次),则ACS可以向AER下发针对该终端的静默表项,AER收到该静默表项后,可以在预设时长(如30分钟)内,不再向ACS转发来自该终端的报文,从而可以在一定程度上避免ACS受到冲击。

[0073] 步骤304:AER收到ACS发送的SMA报文头中指定位的值为第四预设值的发现应答报文后,将该发现应答报文转发给SMA组网外终端。

[0074] 这里AER在向终端转发发现应答报文时,可以利用利用上述建立的临时表项,将该发现应答报文的源IP地址,由ACS的IP地址修改为临时表项中记录的与该发现应答报文的目的IP地址对应的HTTP服务器地址,然后将修改后的发现应答报文转发给SMA组网外终端。转发过程中,AER并不修改发现应答报文的报文内容。

[0075] 步骤305:终端收到上述SMA报文头中指定位的值为第四预设值的报文并确定该报文为发现应答报文后,向AER发送SMA报文头中指定位的值为第一预设值的认证报文。

[0076] 这里,终端发出的认证报文的源IP地址和目的IP地址与步骤301中终端发出的发现报文的源IP地址和目的IP地址相同。此外,认证报文中还携带有该终端的用户名和密码。

[0077] 步骤306:AER收到上述报文后,获取该报文的SMA报文头中的指定位,发现该指定

位的值与第一预设值匹配，则确认该报文为由SMA组网外终端发送给ACS的认证报文，从而将该认证报文重定向到本AS内的ACS。

[0078] 其中，将认证报文重定向到ACS的过程具体为：将认证报文的目的IP地址修改为本AS内的ACS的IP地址，然后将修改后的认证报文转发给ACS。

[0079] 步骤307：ACS收到上述SMA报文头中指定位的值为第一预设值的报文并确定该报文为认证报文后，对该认证报文携带的用户名和密码进行认证，并基于认证结果向AER发送SMA报文头指定位的值为第二预设值的认证应答报文。

[0080] 无论认证通过与否，认证应答报文的SMA报文类型值均是第二预设值。但不同的是，如果认证通过，则认证应答报文的SMA报文头中会携带ACS为终端分配的报文标签，报文标签用于携带在该终端与本AS之间来往的数据报文中；如果认证未通过，则认证应答报文的SMA报文头中不携带该报文标签。

[0081] 步骤308：AER收到ACS发送的SMA报文头中指定位的值为第二预设值的认证应答报文后，将该认证应答报文转发给SMA组网外终端。

[0082] 这里AER在向终端转发认证应答报文时，可以利用利用上述建立的临时表项，将该认证应答报文的源IP地址，由ACS的IP地址修改为临时表项中记录的与该认证应答报文的目的IP地址对应的HTTP服务器地址，然后将修改后的认证应答报文转发给SMA组网外终端。

[0083] 作为一个实施例，在认证通过的场景下，AER还会在本地保存与该终端对应的SMA表项，该SMA表项记录了ACS为终端分配的报文标签与该终端的IP地址的对应关系。该SMA表项可以是ACS生成并下发给AER，也可以是AER根据收到的认证应答报文的目的IP地址和认证应答报文所携带的报文标签自行生成。

[0084] AER保存SMA表项之后，可以删除上述临时表项，以及设置SMA表项的老化时间。在SMA表项的老化时间结束之前，SMA组网外终端可以通过再次发送认证报文进行续约，ACS可以通过响应认证应答报文告知续约结果。如果续约成功，认证应答报文中将携带新的报文标签，后续终端发送给ACS的数据报文中也将使用该新的报文标签。每续约一次，便会修改一次报文标签，以保证报文标签的安全性和时效性。在续约成功时，AER上保存的SMA表项的老化时间也会更新，以及SMA表项中记录的报文标签也会更新为新的报文标签。

[0085] 当到达SMA表项的老化时间时，AER可以通过删除SMA表项，来主动断开SMA组网外终端与ACS的连接。

[0086] 步骤309：SMA组网外终端收到上述SMA报文头中指定位的值为第二预设值的报文并确定该报文为认证应答报文后，从该认证应答报文中读取报文标签；如果读取到，则确定认证通过，并在后续发送给该AS的数据报文中携带该报文标签。

[0087] 步骤309中所说的AS指的是对终端进行认证通过的ACS所在的AS，如果终端要访问SMA组网内的其它AS，则需要向其它AS发起认证请求，认证通过后才能访问。

[0088] 其中，SMA组网外终端访问AS内设备的过程具体为：

[0089] 1)SMA组网外终端向AER发送SMA报文头中指定位的值为第五预设值的数据报文；该数据报文中携带步骤309中从认证应答报文中读取到的报文标签。

[0090] 2)AER收到上述报文后，发现该报文的SMA报文头指定位的值与第五预设值匹配，从而确认该报文为由SMA组网外终端发送给本AS内设备的数据报文，进而查找与该数据报文的源IP地址以及该数据报文携带的报文标签所匹配的SMA表项；如果找到，则去掉该数据

报文中的报文标签，然后将该数据报文转发给该数据报文的目的IP地址对应的AS内设备；如果未找到，则丢弃该数据报文。

[0091] 3)假设AS内设备收到了上述SMA报文头中指定位的值为第五预设值的报文并确定该报文为数据报文后，对该数据报文进行解析处理，并基于处理结果向AER发送SMA报文头中指定位的值为第六预设值的数据报文。

[0092] 4)AER收到ACS发送的SMA报文头中指定位的值为第六预设值的数据报文后，将该数据报文转发给SMA组网外终端。

[0093] 如此，便实现了SMA组网外终端远程访问SMA组网内的设备。

[0094] 在本申请的一个实施例中，上述SMA报文头中的指定位可以位于SMA报文头的DATA字段或预留字段中。

[0095] SMA报文头的DATA字段有32位，在现有技术中一般用于携带密钥等身份识别信息。预留字段有5位，为未被使用的保留字段。

[0096] 当SMA头中指定位的值为第一预设值，即报文为认证报文时，报文中还会包括用户名和密码，用户名和密码也可以携带在DATA字段或预留字段中。同理，当SMA报文头中指定位的值为第二预设值，即报文为认证应答报文时，报文中还会包括报文标签，报文标签也可以携带在DATA字段或预留字段中。

[0097] 以上对本申请提供的方法进行了描述。下面对本申请提供的装置进行描述。

[0098] 参见图4，为本申请提供的一种AER，所述AER可以包括：

[0099] 接收单元401，用于接收SMA组网外的终端发送的第一报文。

[0100] 获取单元402，用于获取所述第一报文的SMA报文头中的指定位。

[0101] 确认单元403，用于在所述指定位的值与第一预设值匹配时，确认所述第一报文为由SMA组网外的终端发送给SMA组网内的ACS的认证报文。

[0102] 发送单元404，用于将所述认证报文重定向到本AS内的ACS进行认证。

[0103] 所述接收单元401，还用于接收所述ACS返回的认证结果；如果认证结果为通过，则允许所述终端访问本AS；如果认证结果为不通过，则禁止所述终端访问本AS。

[0104] 在其中一种实施方式中，所述接收单元401，还用于接收所述ACS返回的第二报文，所述第二报文的SMA报文头中的所述指定位的值为第二预设值，所述第二预设值用于表征所述第二报文为认证应答报文；

[0105] 所述发送单元404，还用于将所述认证应答报文转发给所述终端；

[0106] 其中，当所述认证应答报文的SMA报文头中携带报文标签时，表征认证结果为通过，所述AER允许所述终端访问本AS；当所述认证应答报文的SMA报文头中不携带报文标签时，表征认证结果为不通过，所述AER禁止所述终端访问本AS；所述报文标签用于携带在所述终端与本AS之间来往的数据报文中。

[0107] 在其中一种实施方式中，所述AER还可以包括：

[0108] SMA表项建立单元，用于在所述AER允许所述终端访问本AS时，保存与所述终端对应的SMA表项，该SMA表项记录有所述报文标签与所述终端的IP地址之间的对应关系；

[0109] 所述发送单元404和所述接收单元401，还用于基于该SMA表项在所述终端和本AS之间传输数据报文。

[0110] 在其中一种实施方式中，所述确认单元403，还用于在所述第一报文的SMA报文头

中的指定位的值与第三预设值匹配时，确认所述第一报文为由SMA组网外的终端发送给SMA组网内的ACS的发现报文；所述发现报文用于发现SMA组网中的ACS；

[0111] 所述发送单元404，还用于将所述发现报文重定向到本AS内的ACS；

[0112] 所述接收单元401，还用于接收所述ACS返回的第三报文，所述第三报文的SMA报文头中的所述指定位的值为第四预设值，所述第四预设值用于表征所述第三报文为发现应答报文；

[0113] 所述发送单元404，还用于将所述发现应答报文转发给所述终端，所述发现应答报文用于告知终端本AS内的ACS能够提供认证服务，以使所述终端向所述ACS发送认证报文。

[0114] 在其中一种实施方式中，所述发现报文和所述认证报文的目的IP地址为HTTP服务器地址；

[0115] 所述AER还可以包括：

[0116] 临时表项建立单元，用于建立针对所述终端的临时表项，所述临时表项中记录有所述HTTP服务器地址和所述终端的IP地址之间的对应关系；

[0117] 所述发送单元404，在将所述发现报文和所述认证报文重定向到本AS内的ACS时，用于将所述发现报文和所述认证报文的目的IP地址修改为所述ACS的IP地址，并将修改后的所述发现报文和所述认证报文转发给所述ACS；以及，在将所述发现应答报文和所述认证应答报文转发给所述终端时，用于将所述发现应答报文和所述认证应答报文的源IP地址修改为所述临时表项中记录的所述HTTP服务器地址，并将修改后的所述发现应答报文和所述认证应答报文转发给所述终端。

[0118] 在其中一种实施方式中，所述接收单元401，还用于接收所述ACS发送的针对所述终端的静默表项，所述静默表项用于指示所述终端认证超时或认证出错达到设定次数；

[0119] 所述发送单元404，还用于在所述接收单元401收到所述静默表项后，在预设时长内禁止向所述ACS转发来自所述终端的报文。

[0120] 在其中一种实施方式中，所述指定位位于SMA报文头的DATA字段或预留字段中。

[0121] 至此，完成图4所示AER的功能模块描述。

[0122] 对应地，本申请还提供了图4所示AER的硬件结构。参见图5，图5为本申请提供的图4所示装置的硬件结构示意图，该装置包括：通信接口501、处理器502、存储器503和总线504；其中，通信接口501、处理器502、存储器503通过总线504完成相互间的通信。

[0123] 其中，通信接口501，用于发送和接收报文。处理器502可以是一个CPU，存储器503可以是非易失性存储器(non-volatile memory)，并且存储器503中存储有SMA组网的接入逻辑指令，处理器502可以执行存储器503中存储的SMA组网的接入逻辑指令，以实现上述图3所示流程中AER的功能。

[0124] 至此，完成图5所示AER的硬件结构描述。

[0125] 参见图6，为本申请提供的一种终端，所述终端位于SMA组网外，所述终端可以包括：

[0126] 报文处理单元601，用于生成报文并为生成的报文封装SMA头；所述SMA头中的指定位的值为第一预设值，所述第一预设值用于表征所述报文为认证报文。

[0127] 发送单元602，用于将封装后的报文发送给SMA组网中的AER，以使AER根据所述指定位的值将收到的报文重定向到ACS进行认证。

[0128] 至此，完成图6所示终端的功能模块描述。

[0129] 对应地，本申请还提供了图6所示终端的硬件结构。参见图7，图7为本申请提供的图6所示装置的硬件结构示意图，该装置包括：通信接口701、处理器702、存储器703和总线704；其中，通信接口701、处理器702、存储器703通过总线704完成相互间的通信。

[0130] 其中，通信接口701，用于发送和接收报文。处理器702可以是一个CPU，存储器703可以是非易失性存储器，并且存储器703中存储有SMA组网的接入逻辑指令，处理器702可以执行存储器703中存储的SMA组网的接入逻辑指令，以实现上述图3所示流程中终端的功能。

[0131] 至此，完成图7所示终端的硬件结构描述。

[0132] 以上所述仅为本申请的较佳实施例而已，并不用以限制本申请，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请保护的范围之内。

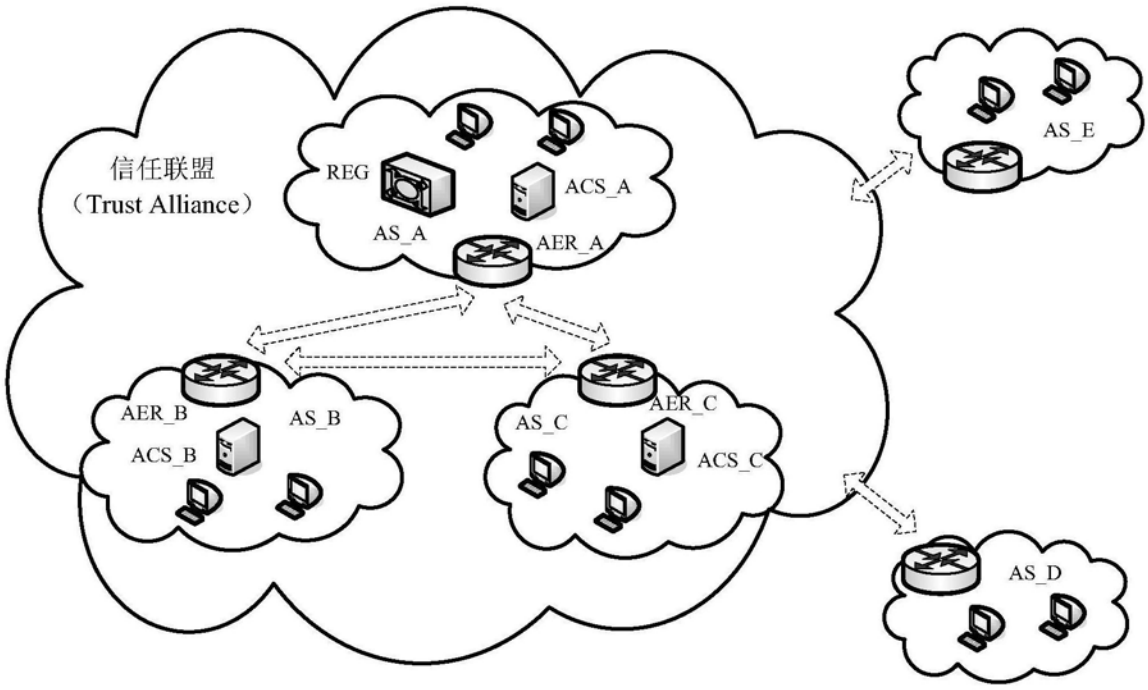

信任联盟
（Trust Alliance）
REG
ACS_A
AS_A
AER_A
AS_E
AER_B
AS_B
ACS_B
AS_C
AER_C
ACS_C
AS_D

图1

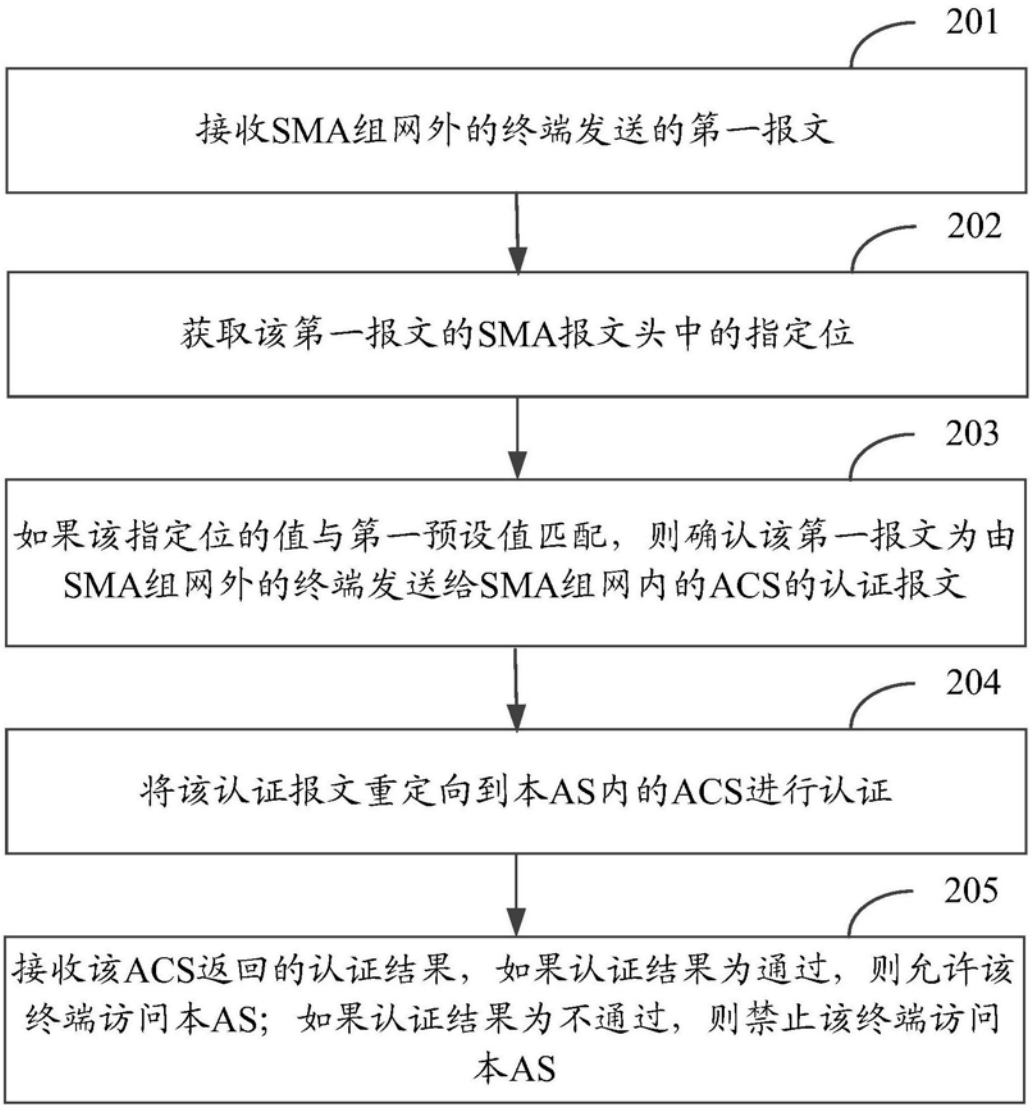

201
接收SMA组网外的终端发送的第一报文
202
获取该第一报文的SMA报文头中的指定位
203
如果该指定位的值与第一预设值匹配，则确认该第一报文为由SMA组网外的终端发送给SMA组网内的ACS的认证报文
204
将该认证报文重定向到本AS内的ACS进行认证
205
接收该ACS返回的认证结果，如果认证结果为通过，则允许该终端访问本AS；如果认证结果为不通过，则禁止该终端访问本AS

图2


SMA组网外终端
AER
ACS
301.SMA组网外终端向AER发送SMA报文头中指定位的值为第三预设值的发现报文
302.AER收到上述报文后，获取该报文的SMA报文头中的指定位，发现该指定位的值与第三预设值匹配，则确认该报文为由SMA组网外终端发送给ACS的发现报文，从而将该发现报文重定向到本AS内的ACS
303.ACS收到上述SMA报文头中指定位的值为第三预设值的报文并确定该报文为发现报文后，将该指定位的值修改为第四预设值，并将报文的源IP地址和目的IP地址互换，然后将修改后的报文发送给AER
304.AER收到ACS发送的SMA报文头中指定位的值为第四预设值的发现应答报文后，将该发现应答报文转发给SMA组网外终端
305.终端收到上述SMA报文头中指定位的值为第四预设值的报文并确定该报文为发现应答报文后，向AER发送SMA报文头中指定位的值为第一预设值的认证报文
306.AER收到上述报文后，获取该报文的SMA报文头中的指定位，发现该指定位的值与第一预设值匹配，则确认该报文为由SMA组网外终端发送给ACS的认证报文，从而将该认证报文重定向到本AS内的ACS
307.ACS收到上述SMA报文头中指定位的值为第一预设值的报文并确定该报文为认证报文后，对该认证报文携带的用户名和密码进行认证，并基于认证结果向AER发送SMA报文头指定位的值为第二预设值的认证应答报文
308.AER收到ACS发送的SMA报文头中指定位的值为第二预设值的认证应答报文后，将该认证应答报文转发给SMA组网外终端
309.SMA组网外终端收到上述SMA报文头中指定位的值为第二预设值的报文并确定该报文为认证应答报文后，从该认证应答报文中读取报文标签；如果读取到，则确定认证通过，并在后续发送给该AS的数据报文中携带该报文标签

图3

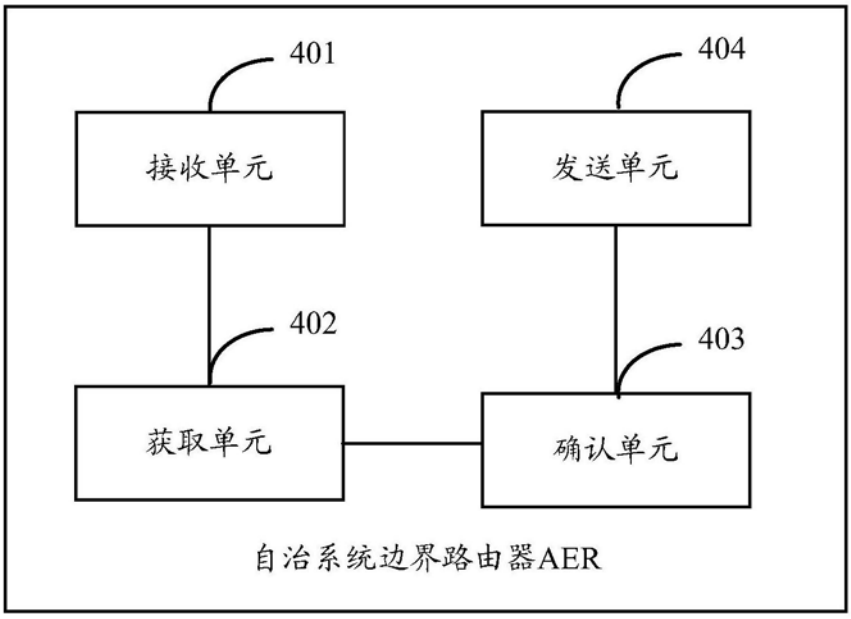

401
404
接收单元
发送单元
402
403
获取单元
确认单元
自治系统边界路由器AER

图4

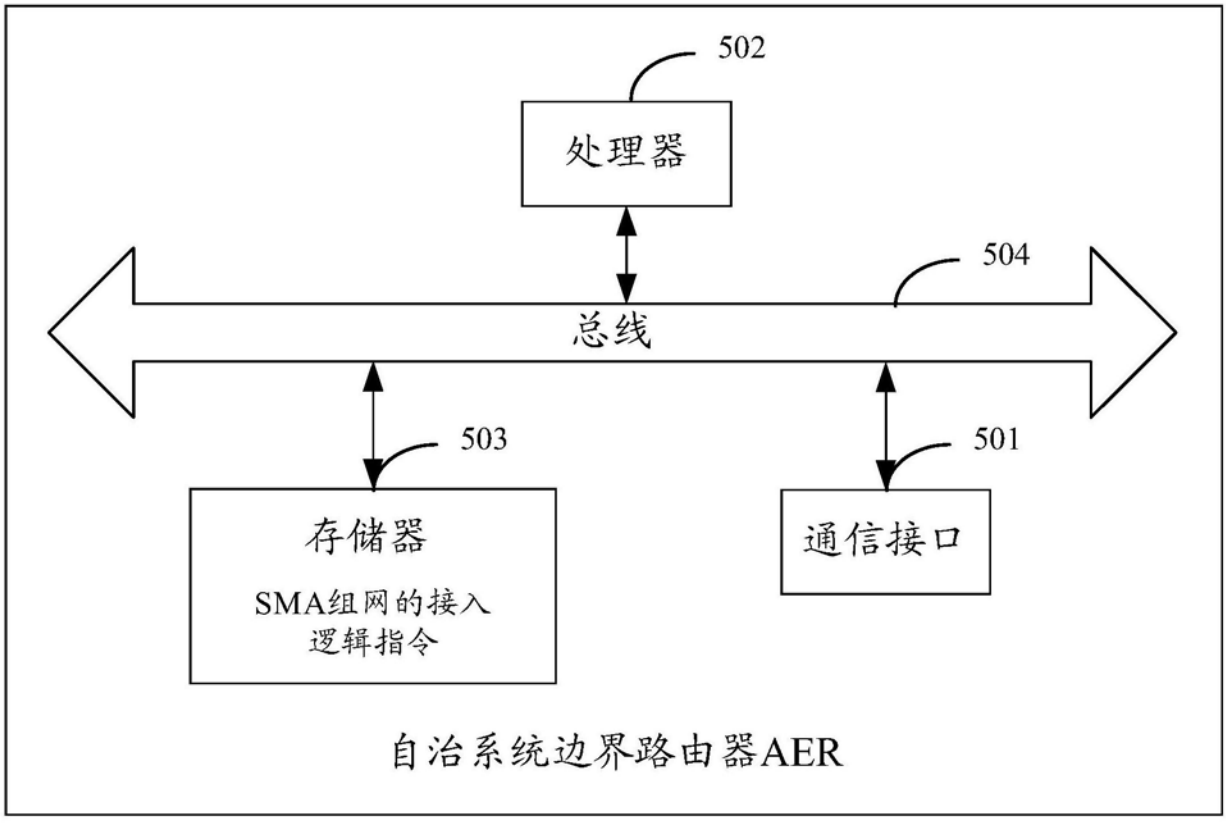

502
处理器
504
总线
503
501
存储器
SMA组网的接入
逻辑指令
通信接口
自治系统边界路由器AER

图5

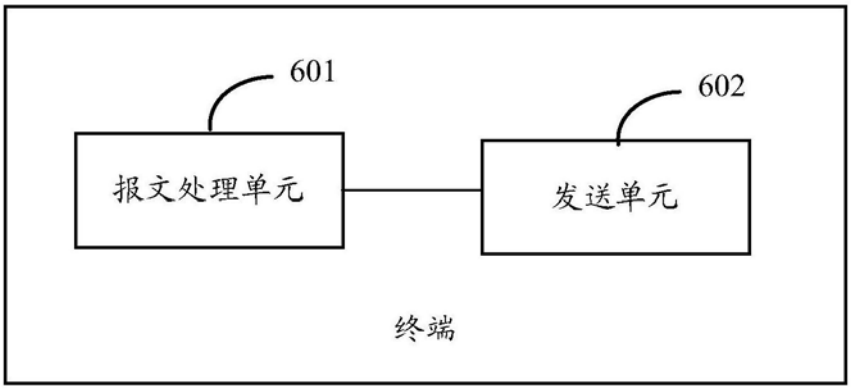

601
602
报文处理单元
发送单元
终端

图6

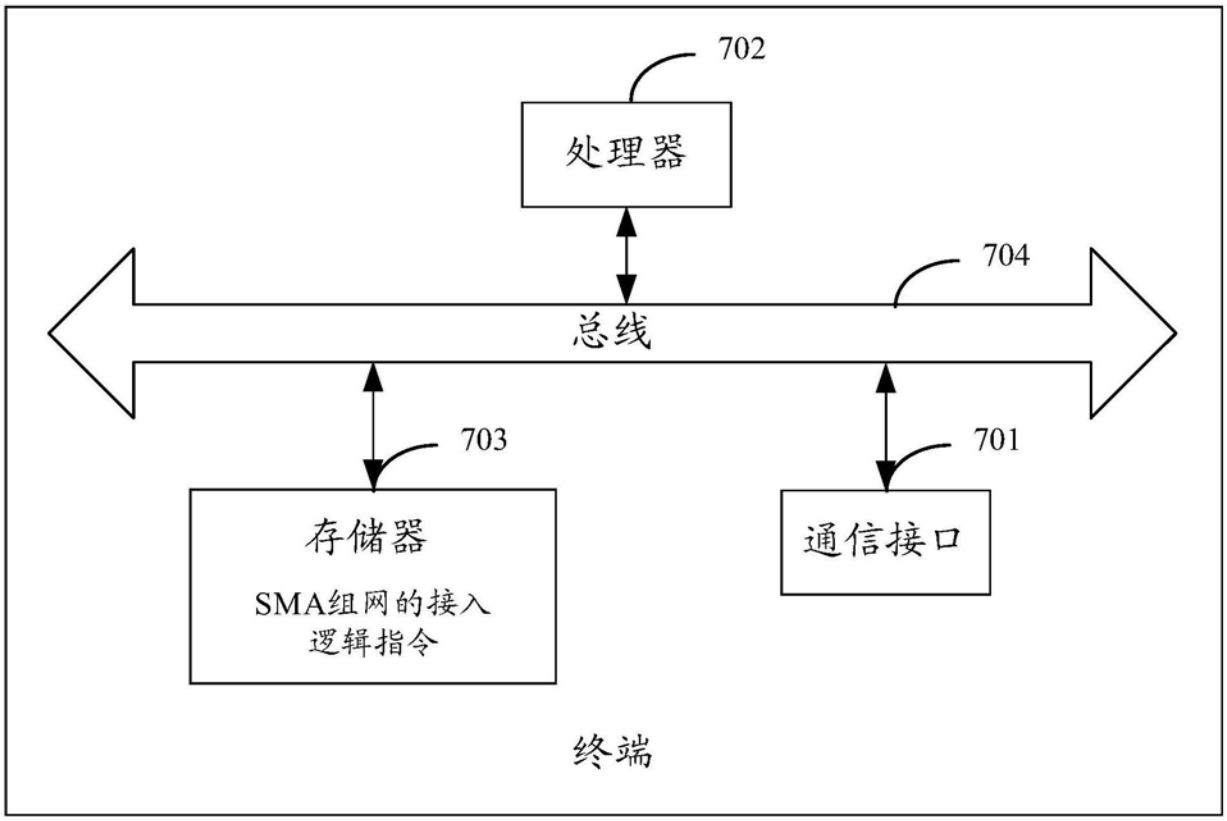

702
处理器
704
总线
703
701
存储器
SMA组网的接入
逻辑指令
通信接口
终端

图7