[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200710124345.8

[43] 公开日 2009 年 5 月 6 日

[11] 公开号 CN 101425919A

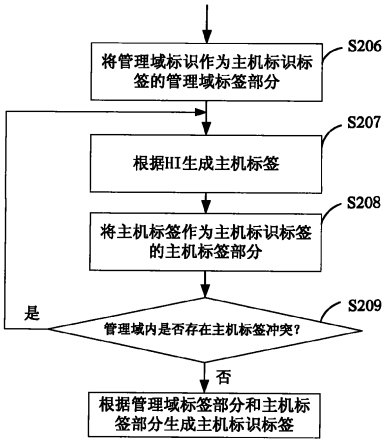
[22] 申请日 2007.11.2
[21] 申请号 200710124345.8
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 蒋 胜 徐小虎
权利要求书 5 页 说明书 13 页 附图 5 页

[54] 发明名称

主机标识标签的生成、分配方法和设备、网络

[57] 摘要

本发明实施例公开了一种主机标识标签、生成主机标识标签的设备、方法，分配主机标识标签的设备、方法，以及主机标识协议网络，其中，主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为将使用该主机标识标签的通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。 在结构上便可以保证 HIT 的结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。



1、一种生成主机标识标签的方法，其特征在于，将通信设备所在的管理域的管理域标识作为主机标识标签的管理域标签部分，将通过加密算法生成的主机标签作为主机标识标签的主机标签部分，至少根据所述管理域标签部分和主机标签部分为所述通信设备生成主机标识标签。

2、如权利要求 1 所述的方法，其特征在于，还进一步包括，预先确定该通信设备所在的管理域内不存在服务器，由通信设备本身将其所在的管理域的管理域标识作为主机标识标签的管理域标签部分，将通过加密算法生成的主机标签作为主机标识标签的主机标签部分，至少根据所述管理域标签部分和主机标签部分为所述通信设备生成主机标识标签。

3、如权利要求 1 所述的方法，其特征在于，还进一步包括，在生成所述主机标识标签后，在管理域内检测是否存在相同的主机标识标签。

4、如权利要求 3 所述的方法，其特征在于，如果管理域内还存在相应的其他主机标识标签，则为所述通信设备重新生成主机标识标签。

5、如权利要求 1 所述的方法，其特征在于，在生成所述主机标识标签后，如果检测到所述管理域内存在服务器，则向所述服务器请求新的主机标识标签。

6、如权利要求 5 所述的方法，在所述通信设备收到所述新的主机标识标签后，停止使用所述至少根据所述管理域标签部分和主机标签部分为所述通信设备生成主机标识标签。

7、如权利要求 1 至 6 中任一所述的方法，其特征在于，所述加密算法为 SHA1、SHA256、SHA384 中的一种。

8、如权利要求 1 至 6 中任一所述的方法，其特征在于，所述管理域标识由域名系统 DNS、动态主机分配协议 DHCP、路由公告 RA、公钥基础设施 PKI、认证、授权、计费 AAA 中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

9、一种分配主机标识标签的方法，其特征在于，在收到通信设备的请求后，为所述通信设备分配主机标识标签，其中，所述主机标识标签至少包括

管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识,所述主机标签部分为根据加密算法生成的主机标签。

10、如权利要求 9 所述的方法，其特征在于，在分配所述主机标识标签后，在所述管理域内检测是否存在相同的主机标识标签。

11、如权利要求 10 所述的方法，其特征在于，如果所述管理域内还存在相同的其他主机标识标签，则为所述通信设备重新分配主机标识标签。

12、如权利要求 9 或 10 或 11 所述的方法，其特征在于，所述加密算法为 SHA1、SHA256、SHA384 中的一种。

13、如权利要求 9 或 10 或 11 所述的方法，其特征在于，所述管理域标识由域名系统 DNS、动态主机分配协议 DHCP、路由公告 RA、公钥基础设施 PKI、认证、授权、计费 AAA 中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

14、一种主机标识标签，其特征在于，至少包括管理域标签部分和主机标签部分，所述管理域标签部分为将使用该主机标识标签的通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

15、如权利要求 14 所述的主机标识标签，其特征在于，所述加密算法为 SHA1、SHA256、SHA384 中的一种。

16、如权利要求 14 所述的主机标识标签，其特征在于，所述管理域标识由域名系统 DNS、动态主机分配协议 DHCP、路由公告 RA、公钥基础设施 PKI、认证、授权、计费 AAA 中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

17、一种分配主机标识标签的服务器，其特征在于，包括:

存储模块，用于保存主机标识标签;

接收模块，用于接收通信设备的请求;

分配模块，在所述接收模块接收到通信设备的请求时，用于在存储模块中选择主机标识标签;

发送模块，用于将所述分配模块选择的所述主机标识标签发送出去;

其中，所述主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

18、如权利要求 17 所述的分配主机标识标签的服务器，其特征在于，还包括检测模块，用于在所述管理域内检测是否存在与所述分配模块选择的所述主机标识标签相同的主机标识标签。

19、如权利要求 17 或 18 所述的分配主机标识标签的服务器，其特征在于，所述加密算法为 SHA1、SHA256、SHA384 中的一种。

20、如权利要求 17 或 18 所述的分配主机标识标签的服务器，所述管理域标识由域名系统 DNS、动态主机分配协议 DHCP、路由公告 RA、公钥基础设施 PKI、认证、授权、计费 AAA 中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

21、一种生成主机标识标签的通信设备，其特征在于，包括:

管理域标识生成模块，用于根据管理域标识生成主机标识标签的管理域标签部分;

主机标签生成模块，用于根据加密算法生成主机标识标签的主机标签部分;

主机标识标签生成模块，用于至少根据所述管理域标识生成模块生成的所述管理域标签部分和所述主机标签生成模块生成的所述主机标签部分生成主机标识标签;

其中，所述管理域标识为将使用该主机标识标签的通信设备所在的管理域的标识。

22、如权利要求 21 所述的生成主机标识标签的通信设备，其特征在于，还包括:

接收模块，用于接收主机标识标签请求，并触发所述管理域标识生成模块、主机标识标签生成模块、主机标识标签生成模块;

发送模块，用于将所述主机标识标签生成模块生成的所述主机标识标签

发送出去。

23、如权利要求21所述的生成主机标识标签的通信设备，其特征在于，还包括检测模块，用于在所述管理域内检测是否存在与所述主机标识标签生成模块生成的所述主机标识标签相同的主机标识标签。

24、如权利要求21所述的生成主机标识标签的通信设备，其特征在于，还包括探测模块，用于在所述管理域内探测是否存在服务器。

25、如权利要求21至24任一所述的生成主机标识标签的通信设备，其特征在于，所述加密算法为SHA1、SHA256、SHA384中的一种。

26、如权利要求21至24任一所述的生成主机标识标签的通信设备，其特征在于，所述管理域标识由域名系统DNS、动态主机分配协议DHCP、路由公告RA、公钥基础设施PKI、认证、授权、计费AAA中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

27、一种主机标识协议网络，其特征在于，包括至少一台通信设备和服务器，

所述通信设备用于向服务器发出主机标识标签请求；

所述服务器用于在收到所述通信设备的请求时，为所述通信设备发送主机标识标签；

其中，所述主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

28、如权利要求27所述的主机标识协议网络，其特征在于，所述通信设备和服务器在同一个管理域内。

29、如权利要求27所述的主机标识协议网络，其特征在于，所述通信设备还用于在其所在的管理域内检测是否存在与所述主机标识标签相同的主机标识标签。

30、如权利要求27所述的主机标识协议网络，其特征在于，所述服务器还用于在所述通信设备所在的管理域内检测是否存在与所述主机标识标签相

同的主机标识标签。

31、如权利要求 27 所述的主机标识协议网络，其特征在于，还包括检测设备，用于在所述通信设备所在的管理域内检测是否存在与所述主机标识标签相同的主机标识标签。

32、如权利要求 27 至 31 任一所述的主机标识协议网络，其特征在于，所述加密算法为 SHA1、SHA256、SHA384 中的一种。

33、如权利要求 27 至 31 任一所述的主机标识协议网络，其特征在于，所述管理域标识由域名系统 DNS、动态主机分配协议 DHCP、路由公告 RA、公钥基础设施 PKI、认证、授权、计费 AAA 中的一种在所述管理域内分发，或者通过预先静态分发的方式在所述管理域内分发。

主机标识标签的生成、分配方法和设备、网络

技术领域

本发明涉及网络通信技术领域，尤其涉及主机标识标签、生成主机标识标签的设备、方法，分配主机标识标签的设备、方法，以及一种主机标识协议网络。

背景技术

目前的 IP 网络（包括因特网、IP 企业网络、城域网络）已经发展了多年，其最初的设计背景已经不能满足现今网络发展的需要。

在现今的 IP 通信技术中，IP 地址扮演了双重角色。从网络的角度来看，IP 地址具备寻址和路由的功能，IP 地址标识了 IP 设备/节点在网络中的位置，网络路由协议根据 IP 地址将 IP 分组送到指定的目的地。而从应用的角度来看，IP 地址又代表着通信节点的身份，应用不需要关注通信节点的具体位置，而只需要关注 IP 地址所代表的身份即可。

随着网络和业务的不断发展，IPv4 的地址变得越来越稀少，下一代 IP 网络的需求越来越迫切，再加上网络移动性和网络多归属特性的需求不断增长，这三个因素导致 IP 地址的双重角色成为越来越成为问题的焦点。

主机标识协议(Host Identity Protocol，HIP)在所述背景下应运而生。主机标识协议在网络层和传输层之间，引入了新的协议层和基于不对称加密的命名空间，打破了身份标志和拓扑位置的绑定。HIP 协议的架构如图 1 所示，在传输层和网络层之间引入了一个主机标识层 HIP。在主机标识协议中，IP 地址仅被作为网络中的位置标识来使用，因此HIP将传输层和IP互连层隔离。传输本身不关心底层的IP协议，传输层向应用层提供的接口主要包括身份ID和协议端口。HIP 层主要完成主机标识向 IP 地址的转化过程，因此，HIP 需要维护主机标识同 IP 地址的映射关系，包括对端主机标识和 IP 地址的映射关系、本端主机标识和 IP 地址的映射关系。

主机标识协议所使用的标志称为主机标识（Host Identity，HI），代表一个全球唯一的静态的名字，用来标识一个主机，该标志实质上是一对公私钥

对中的公钥。由于 HI 的长度因不同的公钥系统算法而不同，所以在实际协议中通常使用固定长度的主机标识标签（Host Identity Tag，HIT）。主机标识标签可以用在 HIP 层面的数据封装中，也可以支持高效的 HIP 层面标识的索引、查找。

HIT 为 128 位二进制数，由 HI 经过加密混乱算法生成，为扁平化、单一层次的结构。然而，发明人却发现该结构不利于 HIT 的分配管理。作为一个需要在整个 Internet 范围内可查找检索的标识，HIT 必须具有全球唯一性，但是目前缺少相应的可实施的技术方案来保证 HIT 的全球唯一性；而现有的主机标识标签结构，也不利于提出和部署相应的方案。

发明内容

为了保证生成结构化、层次化的 HIT，本发明实施例提供以下技术方案：

一种生成主机标识标签的方法，将通信设备所在的管理域的管理域标识作为主机标识标签的管理域标签部分，将通过加密算法生成的主机标签作为主机标识标签的主机标签部分，至少根据所述管理域标签部分和主机标签部分为所述通信设备生成主机标识标签。

一种分配主机标识标签的方法，在收到通信设备的请求后，为所述通信设备分配主机标识标签，其中，所述主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

一种主机标识标签，至少包括管理域标签部分和主机标签部分，所述管理域标签部分为将使用该主机标识标签的通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

一种分配主机标识标签的服务器，包括：

存储模块，用于保存主机标识标签；

接收模块，用于接收通信设备的请求；

分配模块，在所述接收模块接收到通信设备的请求时，用于在存储模块中选择主机标识标签；

发送模块，用于将所述分配模块选择的所述主机标识标签发送出去；

其中，所述主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

一种生成主机标识标签的通信设备，包括：

管理域标识生成模块，用于根据管理域标识生成主机标识标签的管理域标签部分；

主机标签生成模块，用于根据加密算法生成主机标识标签的主机标签部分；

主机标识标签生成模块，用于至少根据所述管理域标识生成模块生成的所述管理域标签部分和所述主机标签生成模块生成的所述主机标签部分生成主机标识标签；

其中，所述管理域标识为将使用该主机标识标签的通信设备所在的管理域的标识。

一种主机标识协议网络，包括至少一台通信设备和服务器，

所述通信设备用于向服务器发出主机标识标签请求；

所述服务器用于在收到所述通信设备的请求时，为所述通信设备发送主机标识标签；

其中，所述主机标识标签至少包括管理域标签部分和主机标签部分，所述管理域标签部分为所述通信设备所在的管理域的管理域标识，所述主机标签部分为根据加密算法生成的主机标签。

通过本发明实施例所提供的主机标识标签、生成主机标识标签的设备、方法，分配主机标识标签的设备、方法，以及主机标识协议网络，在结构上便可以保证 HIT 的结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。

附图说明

图 1 示出了现有技术中 HIP 架构组成;

图 2 为本发明实施例中生成 HIT 前的流程示意图;

图 3 为本发明实施例中生成 HIT 的流程示意图;

图 4 为本发明实施例中是对生成的 HIT 进行授权和身份验证的流程示意图;

图 5 为本发明实施例中已有 HIT 的通信设备检测服务器的流程示意图;

图 6 为本发明实施例中分配 HIT 的服务器的组成示意图;

图 7 为本发明实施例中生成 HIT 的通信设备的组成示意图;

图 8 为本发明实施例中 HIP 网络组成示意图。

具体实施方式

下面，将对本发明实施例进行详细描述。

将 HIT 结构化、层次化，从而可以保证 HIT 的全球唯一性，即，可以将 HIT 的 128 位进行分段，一部分表示使用该 HIT 的通信设备所在的 HI 管理域（以下称"管理域"），一部分表示使用该 HIT 的通信设备本身的主机标签。分配给 HI 管理域标识的部分如果较多，则用来标识的主机数量就会减少，反之，如果用来标识的主机数量得到保证，则标识的 HI 管理域数量就会减少。

国际网络组织可以为 HI 管理域统一管理分配标识，该标识可以是唯一的，以区分不同的 HI 管理域。当然，这个标识还可以继续分层，标识中的某些字段可以表示特定的含义，例如表示国家、地理位置、组织、运营商等等信息。然后由 DNS（Domain Name System，域名系统）、DNSSEC（Domain Name System Security，域名系统的安全协议）、DHCP（Dynamic Host Configuration Protocol，动态主机分配协议）、RA（Router Advertisement，路由公告）、PKI（Public Key Infrastructure，公钥基础设施）、AAA（Authentication, Authorization, and Accounting，认证、授权、计费）等第三方在管理域内进行分发，或者，通过预先静态分发的方式在管理域内分发，比如，在接入网络之前，预先在通信设备内部进行静态配置，等等。

而通信设备本身的主机标签也应至少保证在该通信设备所在的管理域内

的唯一性，避免在同一个 HI 管理域内出现重复的主机标签。与 HI 管理域标识类似，主机标签也可以继续分层，主机标签中的某些字段可以表示特定的含义，例如表示国家、地理位置、组织、制造商等等信息。

一个通信设备可以拥有一个 HIT，也可以拥有多个 HIT，只要保证所使用的这些 HIT 在全球都是唯一的即可。当然，因为 HIP 可以支持多台主机共用一个 HI 来支持集群服务，也就是说，不同 IP 地址的主机可以使用同一个 HI 共享一个连接或应用，进而，不同 IP 地址的主机可以使用同一个 HIT。

表一是 HIT 的一种结构实施例，在该种格式的 HIT 中，前面 32 位用于标识 HI 管理域，后面 96 位是用于标识主机的主机标签，可以看到，在这样的结构中，可以表示出最多 2^{32} 个 HI 管理域和 2^{96} 个通信设备。

表一

32 位	96 位
HI管理域的标识	主机标签

而表二是 HIT 的另一种结构实施例，在该种格式的 HIT 中，前面 112 位用于标识主机标签，后面 16 位用于标识 HI 管理域，这样，就可以最多表示 2^{16} 个 HI 管理域和 2^{112} 个通信设备。

表二

112 位	16 位
主机标签	HI管理域的标识

当然，HIT 的具体结构划分可以有多种，如果仅将 HIT 的 128 位划分成 HI 管理域标识和主机标签的话，可以用表三来表示，而 HI 管理域的标识和主机标签两部分的位置可以互换，而且，在下表所示的 HIT 结构中，还允许存在用小于 n 位的字符来表示 HI 管理域标识。

表三

n 位	(128-n) 位
HI管理域的标识	主机标签

当然，还可以在这两部分之外再进行划分，本领域普通技术人员可以理解的是，在 128 位的 HIT 划分过程中，可以将一些划分出来的部分作为固定的部分与 HI 管理域标识或者主机标签进行合并，即，可以在 HIT 的任意部分设定为固定的字符，如表四所示，该固定字符也可以出现在 HIT 128 个字符中的其他位置，且 HI 管理域标记和主机标签也可以互换。

表四

m 位	n 位	(128-n-m) 位
固定字符	HI管理域的标识	主机标签

因为 HIT 需保证其全球唯一，所以，无论采用什么格式来表示 HIT，各通信设备或者主机都可以识别使用，当然，优先使用同一种格式的 HIT。而且，无论采取何种结构的 HIT，都可以允许实现变长 HIT，比如，如果将 HIT 划分为 HI 管理域和主机标签两部分，那么，可以允许使用不同长度的字符来表示 HI 管理域或者主机标签。

HIT 可以由各通信设备自动生成，也可以向主机标识标签分配设备（以下称为“服务器”）请求，该服务器可以是一种管理域内管理分配 HIT 的设备，存储有 HIT，可以在请求时向该网络或者 HI 管理域内的通信设备分发 HIT。当然，也可以由管理员为各通信设备进行人工配置。

这样的 HIT 结构便可以保证其结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。

以下根据附图，会对 HIT 的生成过程进行详细描述。

如图 2 所示，图 2 示出了通信设备生成 HIT 前的流程。

S101：通信设备可以首先判断其所在的管理域内是否存在服务器。

优选地，可以首先判断其所在的管理域内是否存在具有 HIT 分配或者生成功能的服务器。

S102：如果存在上述服务器的话，通信设备就可以向服务器请求分配一个 HIT。

具体来说，通信设备可以通过 HIP 或者其他具备主机标识标签请求功能的协议向服务器发出该请求。服务器在分配 HIT 时，可以从存储 HIT 的表项中按照一定策略选择未被使用的 HIT，每分配完一次 HIT，服务器便可以对存储该 HIT 的表项进行刷新，保证该表项中的 HIT 未被使用，删除掉已经使用了的 HIT，或者，给已分配出去的 HIT 设置已使用标记，避免下次分配时再使用。

当然，也可以不设置上述表项，而改由服务器生成一个主机标签（比如利用加密混乱算法），再和管理域标识一起或者再加上其他固定字符一起组成一个唯一的 HIT，分配给发出请求的通信设备，并对已生成分配的 HIT 进行记录。

加密混乱算法有多种，比如 SHA1、SHA256、SHA384、SHA0、SHA224、SHA512、MD4、MD5、HAVAL、RadioGatún、RIPEMD、RIPEMD 320、RIPEMD 128、RIPEMD 160、RIPEMD 256、TIGER 等算法，其基本特征是可重复性、不可逆。

而为了保证分配的 HIT 是唯一的，服务器可以在分配 HIT 之前向该管理域内的通信设备进行检测。比如，对于服务器根据请求而生成的 HIT，若服务器本身没有存储以前的 HIT 分配记录，或者，服务器存储已分 HIT 的表项出现故障时，服务器可以使用已生成而未分配或已选择而未分配的 HIT，在域内进行广播，等待冲突回应，如果在预定时间内收到冲突回应，则说明管理域内已经存在该 HIT，服务器需要重新生成或者重新选择，并且，在存在存储 HIT 表项时，需要对该表项进行刷新，将该 HIT 删除或者设置已使用标记。如果没有收到回应，则说明在管理域内还没有使用该 HIT，可以向通信

设备分配该 HIT。当然，这样的检测可以是周期性地，进一步的，还可以在发出消息后启动定时器，若定时器超时还没收到冲突回应，则说明在管理域内还没有使用该 HIT。

或者，服务器可以遍历其保存的记录，查询一下是否生成的 HIT 之前已被记录，如果没有记录，则说明这次生成的 HIT 未被使用，如果已经存在相应记录，则服务器还需要再次生成或者分配一个 HIT。

如果该管理域内没有服务器，则通信设备可以直接生成 HIT，具体生成的过程可参见图 3 以及下文描述。

S103: 通信设备直接生成 HIT 时，可以事先判断一下是否具有 HIT 自动生成功能，如果有的话，便可以执行 S104 由通信设备直接生成 HIT; 如果没有该功能，或者该功能未被使能，则可以如 S105 所示进行告警。如果管理域内的所有通信设备都已经实现配置或者使能了该功能，则 S103 也可以忽略。

S104: 由通信设备生成 HIT，具体流程请见下文描述。也可以不必进行前述步骤，直接由通信设备生成 HIT。

S105: 如果通信设备没有该功能，或者该功能未被使能，则可以进行告警，通知管理员，或者记入日志。

在通信设备具有或者使能了自动生成 HIT 的功能时，便可以自动生成 HIT，下面会根据图 3 对 HIT 的生成流程进行介绍。

S206: HI 管理域中的通信设备可以首先将管理域标识作为主机标识标签的管理域标签部分。关于 HI 管理域标识，通信设备可以使用 HIP 协议等网络协议，定期或者不定期地从该管理域内的其他特定设备上获取管理域标识的信息，该特定设备也可以定期或者不定期地在管理域内向通信设备发送公告，告知本管理域的管理域标识，所述的特定设备可以是服务器，也可以是不具备 HIT 生成或者分配功能的其他设备。本领域普通技术人员可以理解的是，当然也可以通过其他方式或者机制获取或者生成其所在的管理域的管理域标识，而且，可以保证该管理域标识与其他管理域的标识不会出现重复。

S207：根据 HI 生成主机标签。在生成主机标签的过程中，至少将通信设备的 HI 作为一个输入，可以使用加密算法生成，比如 SHA1、SHA256、SHA384、SHA0、SHA224、SHA512、MD4、MD5、HAVAL、RadioGat ú n、RIPEMD、RIPEMD 320、RIPEMD 128、RIPEMD 160、RIPEMD 256、TIGER 等加密混乱算法，其基本特征是可重复性、不可逆。通信设备的 HI 是由其所在的管理域的权威机构分配的，并且可以保持固定不变。

S208：将生成的主机标签作为主机标识标签的主机标签部分。

S209：使用生成的主机标签进行域内检测，以确定域内是否存在相同的主机标签。在检测时可以广播发送包含待检测的主机标签的冲突检测报文；判断在规定的检测时间内是否收到申明所述主机标签不能使用的冲突报文；如果收到，则判定所述主机标签冲突，重新执行 S207（当然，也可以从 S206 开始执行）；否则，判定所述主机标签不冲突，根据管理域标签部分和主机标签部分，一起或者再加上其他固定字符一起生成主机标识标签 HIT。

也可以在将管理域标签部分和主机标签部分（或者其他固定字符，如果有）一起组成 HIT 后，在所述管理域内对生成的该 HIT 进行检测，判断是否存在冲突，如果存在，则重新生成主机标识标签。在检测时可以广播发送包含待检测的主机标签的冲突检测报文；判断在规定的检测时间内是否收到申明所述主机标签不能使用的冲突报文；如果收到，则判定所述主机标签冲突，重新生成主机标识标签；否则，判定所述主机标签不冲突，使用该 HIT。

当然，也可以先生成主机标签并确定域内不存在主机标签冲突，再根据管理域标识生成管理域标识标签部分，最后再生成 HIT；也可以不分先后顺序，只要能够生成唯一的管理域标签部分和唯一的主机标识部分就可以。

如果是由服务器生成的 HIT，则服务器还需要将其发送给做出请求的通信设备。如果是由该通信设备本身生成的 HIT，则该通信设备便可以使用该 HIT 进行后续步骤了。

下面根据图 4 介绍一下生成 HIT 后的授权和身份验证流程。

S310：通信设备可以根据生成的 HIT 进行授权和身份验证。具体来说，

该通信设备可以向服务器请求该授权和身份验证，也可以向管理域内或者域外的其他设备请求该授权和身份验证。

S311：判断是否通过了授权和身份验证。

S312：如果没有通过，则可以进行告警，通知管理员，或者记入日志。

S313：如果通过，则可以使用该 HIT。

如果通信设备本身已经有了一个 HIT，它也可以在管理域内进行定期或者不定期的检测服务器是否存在，在服务器存在的情况下，可以优先选择请求服务器分配一个 HIT，并使用该分配的 HIT，具体可结合图 5 来介绍。

S414：通信设备可以定期或者不定期地检测管理域内是否存在服务器（是否新增加了服务器，或者，使能了服务器的相关功能）。

S415：如果没有检测到服务器，则继续使用原有的 HIT。

S416：如果服务器被检测到，则可以从服务器请求一个 HIT，服务器分配 HIT 时可以参考前面所述的流程，此处不再赘述。

S417：在收到服务器分配的 HIT 后，该通信设备可以停止使用原先已有的 HIT，而改为使用新分配的 HIT，或者，也可以将其原有的 HIT 上报给服务器，在确定原有的 HIT 没有出现冲突时，同时使用新分配的 HIT 和原有的 HIT。

生成主机标识标签后，可以由该通信设备或者管理域内的服务器，对在该主机标识标签的使用情况进行定期或者不定期的监控，判断是否存在 HIT 冲突，如果与本管理域或者其他管理域内的其他通信设备所使用的主机标识产生冲突等错误，则可以进行告警，由管理员进行调整。当然，在出现冲突的情况下，冲突各方可将其包含 HIT 的相应信息发送给服务器，由服务器根据特定策略进行仲裁，比如，对于较晚使用 HIT 的通信设备，可以由其所在的管理域的服务器自动为其生成分配一个新的未被使用的 HIT。

通过本发明实施例所提供的生成方法所生成的 HIT，在结构上便可以保证其结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该

HI 管理域的范围内检索主机标签，提高了查询效率。

另外，本发明实施例还提供了一种能够生成 HIT 的设备，如图 7 所示，至少包括管理域标识生成模块 201、主机标签生成模块 202、主机标识标签生成模块 203。管理域标识生成模块 201 会选择将管理域标识作为主机标识标签的管理域标签部分，而主机标签生成模块 202 则将通过加密算法（比如加密混乱算法）等生成的主机标签作为主机标识标签的主机标签部分，而主机标识标签生成模块 203 则可以将管理域标识生成模块 201 和主机标签生成模块 202 生成的内容，加工组合成 HIT。加工组合时，可以直接将二者按照一定顺序组成 HIT（具体顺序前文已描述，此处不再赘述），也可以在二者之外再增加固定字符等组成 HIT。

当然，这样的设备不仅可以是为自己生成 HIT，也可以是根据其他设备的请求，为其生成 HIT，这时可能会需要一个接收模块 204 来接收相关的请求，在 HIT 生成模块生成之后，再由发送模块 205 发送出去。

另外，为了保证 HIT 的唯一性，还可以包括一个检测模块 206，对 HIT 生成模块生成的 HIT，在域内进行检测，具体的检测可以是在生成后使用前，也可以是在生成并使用以后。

再者，为了探测网络内是否存在服务器，还可以再包括一个探测模块 207，定期或者不定期地探测管理域内是否存在服务器，具体探测时可以使用 HIP 协议，当然也可以使用其他协议。

通过本发明实施例所提供的通信设备所生成的 HIT，在结构上便可以保证其结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。

另外，本发明实施例还提供了一种能够分配 HIT 的服务器设备，如图 6 所示，可以包括接收模块 101、存储模块 103、分配模块 102、发送模块 104。

存储模块 103 中存有 HIT 表，在接收模块 101 接收到通信设备的请求时，分配模块 102 可以依据一定的策略，比如按照顺序选择、随机选择、根据标

记选择等等，到存储模块 103 中选择出一个 HIT，通过发送模块 104 发送出去，分配 HIT 后，可以对存储模块 103 中所存储的 HIT 表进行更新。

当然，为了保证 HIT 的唯一性，还可以包括一个检测模块 105，对分配模块 102 选择出的 HIT，在域内进行检测，如果域内不存在相同的 HIT，则由发送模块 104 发送出去。具体的检测机制前文已有描述，此处不再赘述。

通过本发明实施例所提供的服务器设备所分配的 HIT，在结构上便可以保证其结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。

本发明实施例还提供一种 HIP 网络，如图 8 所示，包括至少一台通信设备 301 和服务器 302。通信设备 301 在需要获得 HIT 时，可以向服务器 302 发出请求，由服务器 302 为其生成或者分配一个 HIT，服务器将 302HIT 发送给发出请求的通信设备 301 后，可以由服务器 302 或者通信设备 301 定期或者不定期地在网络内检测是否存在其他相同的 HIT，当然，还可以在该 HIP 网络之外设置一台检测设备，定期或者不定期地在前述网络内检测是否存在其他相同的 HIT，具体的生成或者分配过程前文已经描述，此处不再赘述。

通过本发明实施例所提供的网络所生成的 HIT，在结构上便可以保证其结构化和层次化，进而保证其全球唯一性，也便于集中管理、查询，比如进行 HIT 查找检索的时候，就可以先检索 HI 管理域的标识部分，再在该 HI 管理域的范围内检索主机标签，提高了查询效率。

当然，本发明实施例还提供一种计算机可读介质，本发明实施例的计算机可读介质可以是包含、存储、传达、传播或者传输计算机程序的介质，所述计算机程序为使用指令以运行本发明实施例所提供的方法、系统装置、系统或者设备的程序，或者是与该指令有关的程序。该计算机可读介质可以是电子、磁、电磁、光学、红外或者半导体的系统、装置、设备、传播介质或者计算机存储器。

本领域普通技术人员可以理解的是，在本发明实施例中，“通信设备”可

以是 IP 网络内一种可被单独认知的实体（cognizable entity），只要这些设备可以使用 HIT，比如主机、PC、路由器、交换机、服务器等等。而“服务器”则是指一个管理域或者多个管理域内的一种管理、分配 HIT 的通信设备，可以在其他通信设备请求时，为其分配全球唯一的 HIT，当然，作为一种通信设备，其本身也能为自己生成 HIT。而“HI 管理域”或者“管理域”则是指具有由国际网络组织统一管理分配的、相同的标识的通信设备共同所在的网络区域，在该 HI 管理域内，各通信设备都拥有同一个 HI 管理域标识，以区分不同的 HI 管理域内的其他通信设备，并且，该区域内的通信设备都应该由统一的管理或者权威机构分配唯一的 HI。HI 管理域标识还可以继续分层，标识中的某些字段可以表示特定的含义，例如表示国家、地理位置、组织、运营商等等信息。然后由 DNS、DNSSEC、DHCP、RA、PKI、AAA 等第三方在管理域内进行分发，或者，通过预先静态分发的方式在管理域内分发，等等。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

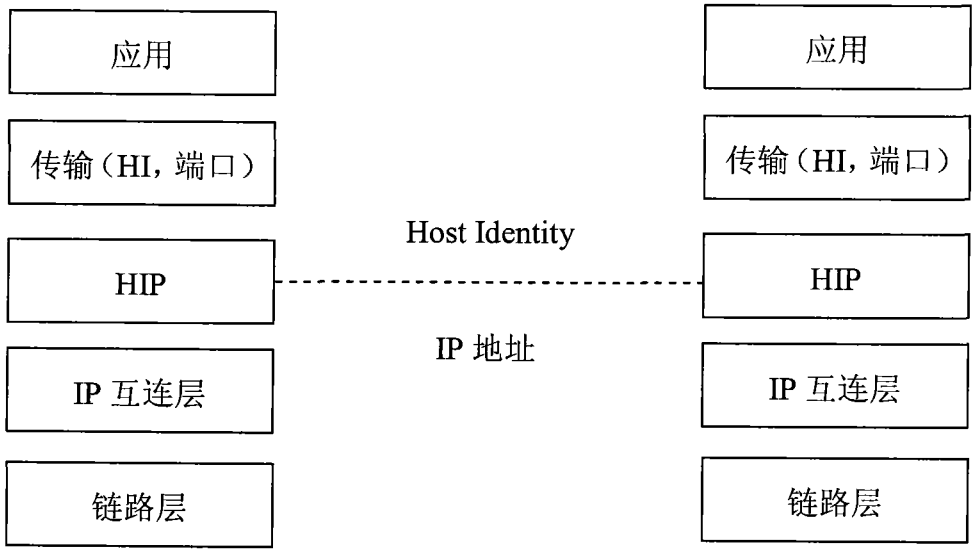

应用
传输（HI，端口）
HIP
IP 互连层
链路层
Host Identity
IP 地址
应用
传输（HI，端口）
HIP
IP 互连层
链路层

图 1

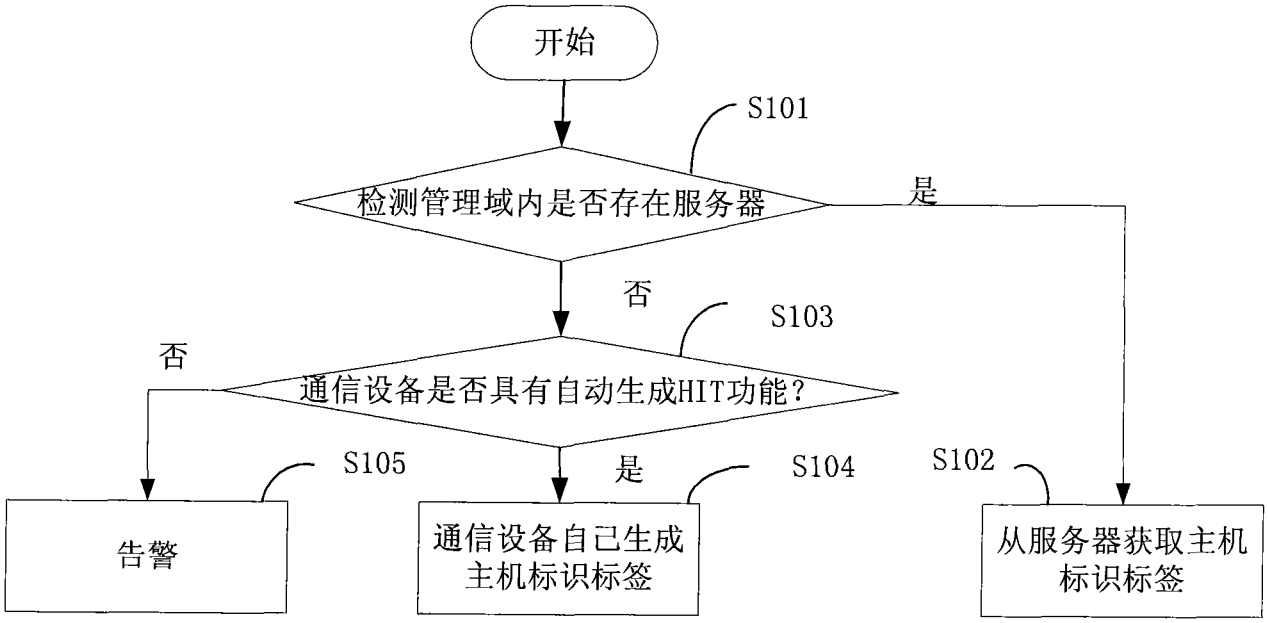

开始
S101
检测管理域内是否存在服务器
是
否
S103
否
通信设备是否具有自动生成HIT功能?
S105
是
S104
S102
告警
通信设备自己生成
主机标识标签
从服务器获取主机
标识标签

图 2

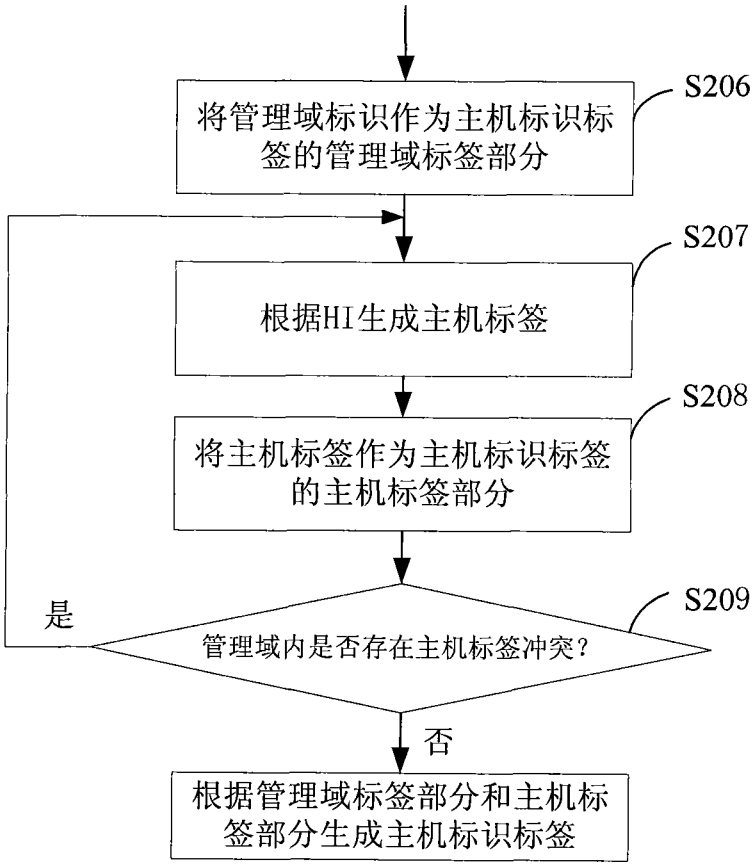

将管理域标识作为主机标识标签的管理域标签部分
S206
根据HI生成主机标签
S207
将主机标签作为主机标识标签的主机标签部分
S208
管理域内是否存在主机标签冲突?
S209
是
否
根据管理域标签部分和主机标签部分生成主机标识标签

图 3

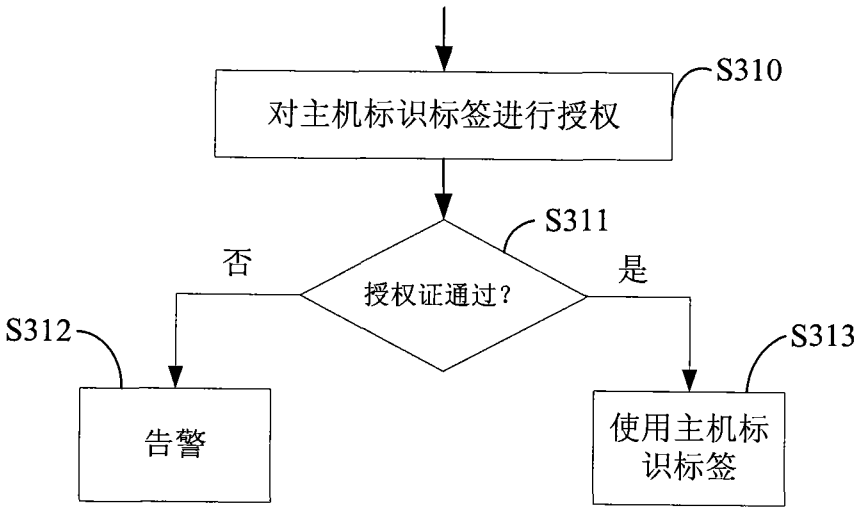

对主机标识标签进行授权
S310
授权证通过?
S311
否
是
S312
S313
告警
使用主机标识标签

图 4

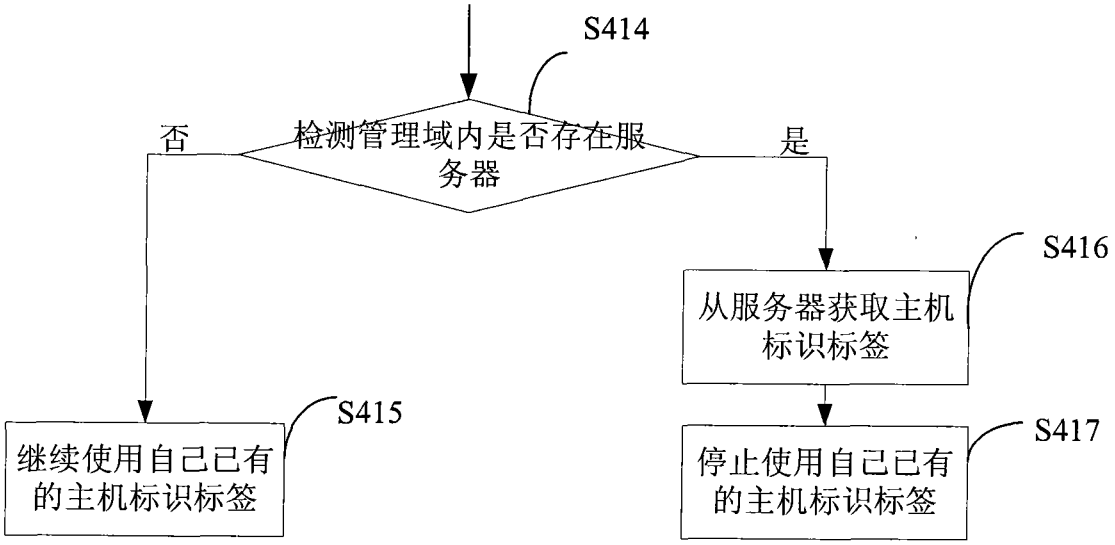

S414
检测管理域内是否存在服务器
否
是
S415
继续使用自己已有的主机标识标签
S416
从服务器获取主机标识标签
S417
停止使用自己已有的主机标识标签

图 5

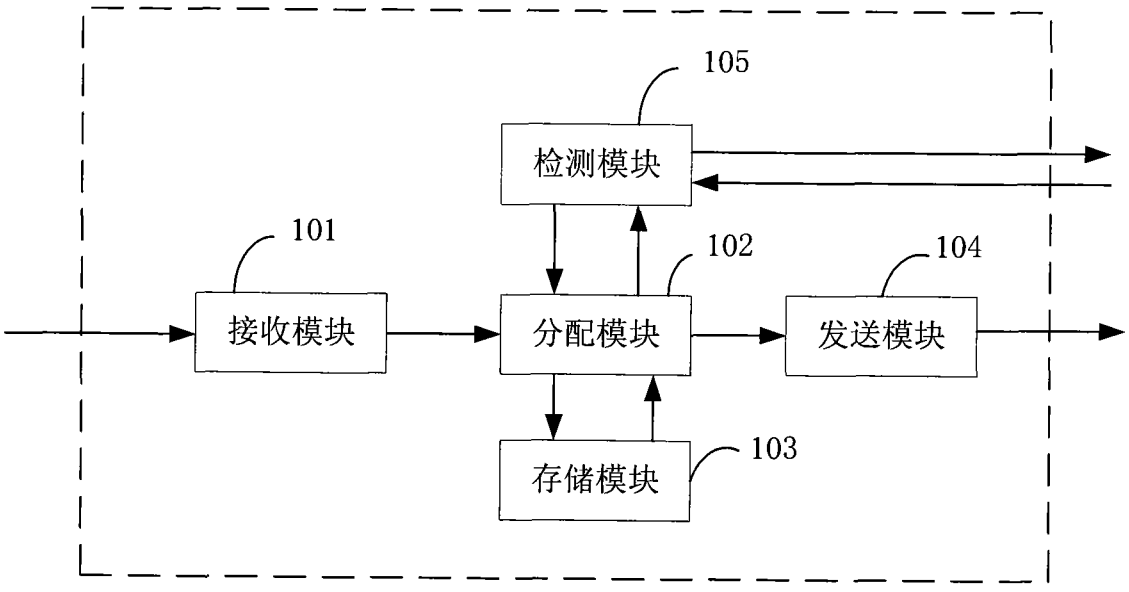

105
检测模块
101
102
104
接收模块
分配模块
发送模块
存储模块
103

图 6

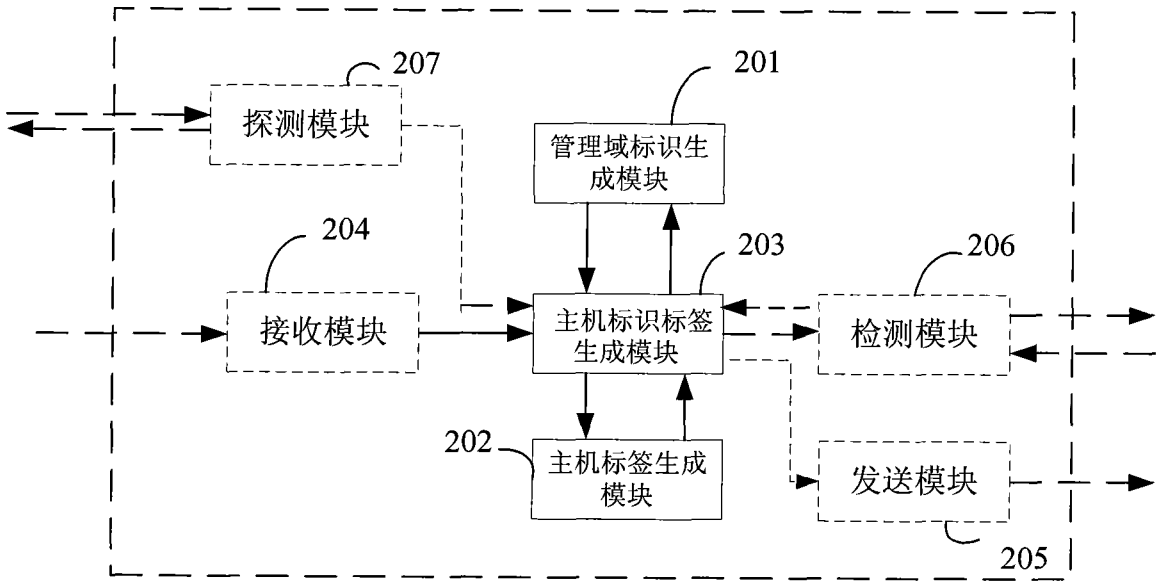

207
探测模块
201
管理域标识生成模块
204
接收模块
203
主机标识标签生成模块
206
检测模块
202
主机标签生成模块
发送模块
205

图 7

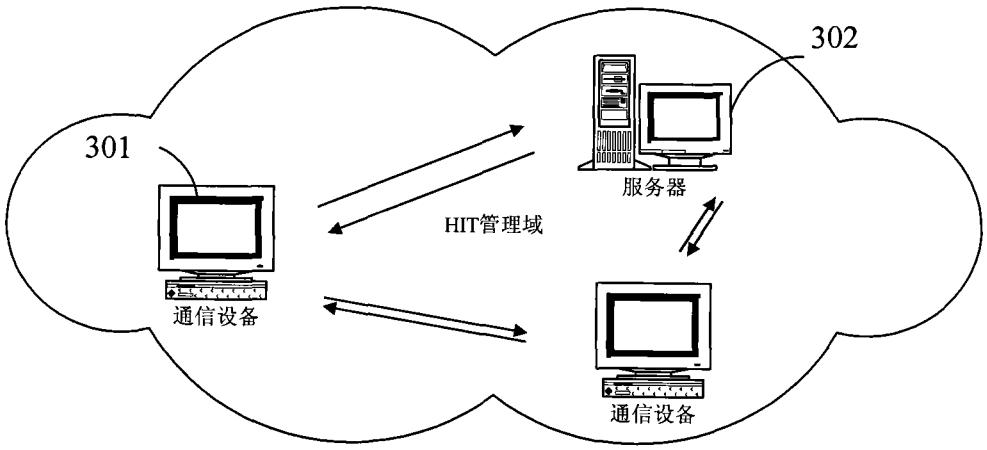

302
301
服务器
HIT管理域
通信设备
通信设备

图 8