



(12) 发明专利

(10) 授权公告号 CN 102238059 B

(45) 授权公告日 2015.05.13

(21) 申请号 201010153057.7

(22) 申请日 2010.04.20

(73) 专利权人 中兴通讯股份有限公司

地址 518057 广东省深圳市南山区高新技术  
产业园科技南路中兴通讯大厦法务部

(72) 发明人 晏祥彪 江华

(74) 专利代理机构 北京安信方达知识产权代理  
有限公司 11262

代理人 田红娟 龙洪

(51) Int. Cl.

H04L 12/70(2013.01)

H04L 29/12(2006.01)

(56) 对比文件

CN 1801764 A, 2006.07.12,

CN 101123536 A, 2008.02.13,

Hongbin Luo, et al. . A DHT-Based

Identifier-to-Locator Mapping Approach for

a Scalable Internet. 《IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS》. 2009, 第 20 卷 (第 12 期), 第 1790-1802 页.

D. Farinacci. Locator/ID Separation Protocol(LISP). 《Network working Group internet-Draft draft-ietf-lisp-05》. 2009, 全文.

许东晓等. 一种基于位置标识与身份标识分离协议的移动性快速切换方法. 《上海交通大学学报》. 2010, 第 44 卷 (第 2 期), 第 156-160 页.

审查员 李红玲

权利要求书3页 说明书11页 附图3页

(54) 发明名称

数据报文处理方法、系统及接入服务节点

(57) 摘要

本发明涉及数据报文处理方法、服务接入节点及系统，该方法基于身份位置分离网络实现，DNS 服务器中保存端主机域名和 AID 的对应关系，该方法包括：A、源端主机向 DNS 服务器发送 DNS 查询报文，其中携带目的端主机的域名，DNS 服务器向源端主机返回包含目的端主机的 AID 的 DNS 响应报文；B、接入服务节点 (ASN) 侦听 DNS 响应报文，获取响应报文中的目的端主机的 AID；C、ASN 根据目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识 (RID)；D、ASN 接收所述源端主机发送给目的端主机的数据报文后，根据目的端主机的 RID 进行数据报文转发。本发明方法、服务接入节点及系统可以提高数据报文转发效率。

201，源端主机向DNS服务器发送DNS查询报文，其中携带目的端主机的域名，DNS服务器向源端主机返回包含目的端主机的AID的DNS响应报文

202，ASN侦听DNS响应报文，截获响应报文中的目的端主机的AID

203，ASN根据目的端主机AID向映射服务器查询获取目的端主机的RID

204，ASN接收所述源端主机发送给目的端主机的数据报文后，根据所述目的端主机的RID进行数据报文转发

1. 一种数据报文处理方法,其特征在于,该方法基于身份位置分离网络实现,域名系统(DNS)服务器中保存端主机域名和接入标识(AID)的对应关系,该方法包括:

A、源端主机向 DNS 服务器发送 DNS 查询报文,其中携带目的端主机的域名,所述 DNS 服务器向所述源端主机返回包含目的端主机的 AID 的 DNS 响应报文;

B、接入服务节点(ASN)侦听 DNS 响应报文,获取响应报文中的目的端主机的 AID;

C、所述 ASN 根据所述目的端主机的 AID 向映射服务器查询获取所述目的端主机的路由标识(RID);

D、所述 ASN 接收所述源端主机发送给目的端主机的数据报文后,根据所述目的端主机的 RID 进行数据报文转发。

2. 如权利要求 1 所述的方法,其特征在于:步骤 B 中,ASN 从接收的转发网络报文中,侦听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

3. 如权利要求 1 所述的方法,其特征在于:步骤 A 中,所述 DNS 查询报文经过 ASN 转发至 DNS 服务器,步骤 B 中,所述 ASN 从 DNS 响应报文中获取目的端主机的 AID 后,将所述 DNS 响应报文转发给源终端;所述源终端根据所述 DNS 响应报文中的目的端主机 AID 向目的端主机发送数据报文。

4. 如权利要求 1 所述的方法,其特征在于:步骤 C 具体包括:所述 ASN 向映射服务器查询前先查询本地缓存,若本地缓存中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,缓存目的端主机的 AID 和 RID 的映射关系。

5. 如权利要求 1 所述的方法,其特征在于:步骤 D 中,所述 ASN 接收到所述源端主机发送给目的端主机的数据报文后,先查询本地缓存,若本地缓存中没有或者正在查询目的端主机的 AID 和 RID 的映射关系,则等待收到所述映射服务器的映射查询响应后,再进行报文转发。

6. 如权利要求 1 所述的方法,其特征在于:所述 ASN 采用封装或替换的方式实现数据报文转发。

7. 如权利要求 1 所述的方法,其特征在于:步骤 D 中,所述源端主机发送的数据报文中源、目的地址分别为源、目的端主机的 AID,所述 ASN 进行数据报文转发时,用源、目的端主机的 RID 对源端主机发送的数据报文进行封装,封装后的数据报文的源、目的地址分别为源、目的端主机的 RID,且封装后的报文还包括源、目的端主机的 AID。

8. 如权利要求 1 所述的方法,其特征在于:所述源端主机发送的数据报文的源、目的地址分别为源、目的端主机的 AID,所述 ASN 进行数据报文转发时,用源、目的端主机的 RID 替换源、目的端主机的 AID,所述 AID 与 RID 唯一对应。

9. 一种接入服务节点,其特征在于,该接入服务节点(ASN)位于身份位置分离网络,所述身份位置分离网络包括 DNS 服务器,用于保存端主机域名和接入标识的对应关系,接收端主机发送的携带目的端主机的域名的 DNS 查询报文,以及向端主机返回携带目的端主机的 AID 的 DNS 响应报文,所述 ASN 包括:

侦听模块,与报文处理模块连接,用于侦听 DNS 响应报文,获取响应报文中的目的端主机的接入标识(AID);

映射查询模块,与所述侦听模块连接,用于根据获取的目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识 (RID) ;

报文处理模块,与所述映射查询模块及侦听模块连接,用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的 RID 进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文。

10. 如权利要求 9 所述接入服务节点,其特征在于 :所述 ASN 的侦听模块从所述报文处理模块收到的转发网络报文中,侦听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

11. 如权利要求 9 所述的接入服务节点,其特征在于 :所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

12. 如权利要求 9 所述的接入服务节点,其特征在于,所述 ASN 还包括与所述映射查询模块连接的映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用于向所述映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

13. 如权利要求 9 所述的接入服务节点,其特征在于 :所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后,还用于通知映射查询模块查询映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系,则等待映射查询模块收到所述映射服务器的映射查询响应后,再进行报文转发。

14. 如权利要求 9 所述的接入服务节点,其特征在于 :所述 ASN 的报文处理模块采用封装或替换的方式实现数据报文转发。

15. 一种数据报文处理系统,其特征在于,该数据报文处理系统基于身份位置分离网络实现,该系统包括端主机、接入服务节点 (ASN) 及 DNS 服务器,其中 :

所述端主机,包括域名查询模块及报文收发模块,其中,域名查询模块用于向 DNS 服务器发送携带目的端主机的域名的 DNS 查询报文,以及接收所述 DNS 服务器返回的携带目的端主机的 AID 的 DNS 响应报文;报文收发模块用于根据所述 DNS 响应报文中的目的端主机 AID 向目的端主机发送数据报文及接收数据报文;

所述 ASN 包括 :

侦听模块,与报文处理模块连接,用于侦听 DNS 响应报文,获取响应报文中目的端主机的接入标识 (AID) ;

映射查询模块,与所述侦听模块连接,用于根据获取的目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识 (RID) ;

报文处理模块,与所述映射查询模块及侦听模块连接,用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的 RID 进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文;

DNS 服务器用于保存端主机域名和接入标识的对应关系,接收端主机发送的 DNS 查询报文,以及向端主机返回 DNS 响应报文。

16. 如权利要求 15 所述的系统,其特征在于 :所述 ASN 的侦听模块从所述报文处理模块收到的转发网络报文中,侦听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

17. 如权利要求 15 所述的系统,其特征在于 :所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

18. 如权利要求 15 所述的系统,其特征在于,所述 ASN 还包括与所述映射查询模块连接映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系 ;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用于向所述映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

19. 如权利要求 15 所述的系统,其特征在于 :所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后,还用于通知所述映射查询模块查询映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系,则等待映射查询模块收到所述映射服务器的映射查询响应后,再进行报文转发。

20. 如权利要求 15 所述的系统,其特征在于 :所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文中源、目的地址分别为源、目的端主机的 AID,进行数据报文转发时,用源、目的端主机的 RID 对源端主机发送的数据报文进行封装,封装后的数据报文的源、目的地址分别为源、目的端主机的 RID,且封装后的报文还包括源、目的端主机的 AID。

21. 如权利要求 15 所述的系统,其特征在于 :所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文的源、目的地址分别为源、目的端主机的 AID,进行数据报文转发时,用源、目的端主机的 RID 替换源、目的端主机的 AID,所述 AID 与 RID 唯一对应。

## 数据报文处理方法、系统及接入服务节点

### 技术领域

[0001] 本发明涉及一种通信领域，尤其涉及身份位置分离网络中的数据报文的处理方法、系统及接入服务节点。

### 背景技术

[0002] 3G 和 4G 是无线通信领域对下一代网络的研究核心，旨在基于全 IP 分组核心网提高无线移动通信的质量；NGN 和 NGI 分别是电信网和互联网领域对下一代网络融合的研究；CNGI 旨在构建基于 IPv6 的下一代互联网；虽然各种研究存在很大差异，但是各种研究普遍接受的观点是：未来网络是基于分组的统一承载网络。因此研究下一代网络构架将以互联网为主要参考对象。互联网从其诞生以来一直保持高速发展，已成为当前最成功、最具生命力的通信网络，其灵活可扩展性、高效的分组交换、终端强大的功能等特点非常符合新一代网络的设计需要，互联网将是新一代网络设计的主要参考蓝本。然而，互联网的结构还远远没有达到最优，存在很多重大的设计问题。除 IP 地址空间无法满足应用需要外，还主要表现在以下方面：

[0003] 互联网发明于二十世纪七十年代，人们难以预计今天世界上将存在大量的移动终端和多家乡终端，因此当时的互联网协议栈主要是针对以“固定”方式连接的终端而设计。在当时的网络环境下，由于终端基本上不会从一个位置移动到其它位置，发送的地址就是接收的地址，路径是可逆的，所以具有身份和位置双重属性的 IP 地址能够非常好的工作，IP 地址的身份属性与位置属性之间没有产生任何冲突。IP 地址同时代表身份和位置恰恰满足了当时的网络需求。从当时的网络环境来看，这种设计方案简单有效，简化了协议栈的层次结构。但毋庸置疑的是，IP 地址的身份属性与位置属性之间存在着内部矛盾。IP 地址的身份属性要求任意两个 IP 地址都是平等的，虽然 IP 地址可以按照组织机构进行分配，但是连续编码的 IP 地址之间没有必然的关系，或者至少在拓扑位置上没有必然的关系；IP 地址的位置属性则要求 IP 地址基于网络拓扑（而不是组织机构）进行分配，处于同一个子网内的 IP 地址都应该处于一个连续的 IP 地址块中，这样才可以使网络拓扑中的 IP 地址前缀聚合，从而减少路由器设备的路由表的条目，保证路由系统的可扩展性。

[0004] 伴随着网络规模和技术的发展，一些动态分配 IP 地址的技术逐步出现，如动态主机配置协议 (DHCP, Dynamic Host Configuration Protocol)，这就开始打破 IP 地址唯一表示一个终端的假定。私有 IP 地址空间的使用和网络地址转换 (NAT, Network Address Translator) 技术的诞生使得情况继续恶化。在这种情况下同时具有身份属性与位置属性的 IP 地址将难以继续胜任它的角色，IP 地址的双重属性问题已经凸显出来。除了技术层面的需求发生了显著变化以外，互联网的用户状况也已经发生了巨大的改变。在互联网诞生之后的最初几年中，互联网基本上被一些处于共同团体且相互信任的人员使用，传统互联网协议栈也是基于此种假设而设计的；而目前的互联网用户则是鱼龙混杂，人们难以继续互相信任。在这种情况下，缺乏内嵌安全性机制的互联网也需要发生变革。

[0005] 总的来说，IP 地址双重属性的内在矛盾将导致如下主要问题：

[0006] 1. 路由可扩展问题。关于互联网路由系统的可扩展性存在一个基本的假定：

[0007] “地址按照拓扑进行分配,或者拓扑按照地址进行部署,二者必选其一”。IP 地址的身份属性要求 IP 地址基于终端所属的组织机构(而不是网络拓扑)进行分配,而且这种分配要保持一定的稳定性,不能经常改变;而 IP 地址的位置属性要求 IP 地址基于网络拓扑进行分配,以便保证路由系统的可扩展性。这样,IP 地址的两种属性就产生了冲突,最终引发了互联网路由系统的可扩展问题。

[0008] 2. 移动性问题。IP 地址的身份属性要求 IP 地址不应该随着终端位置的改变而变化,这样才能够保证绑定在身份上的通信不中断,也能够保证终端在移动后,其它终端仍能够使用它的身份与之建立通信联系;而 IP 地址的位置属性则要求 IP 地址随着终端位置的改变而改变,以便 IP 地址能够在新的网络拓扑中聚合,否则网络就必须为移动后的终端保留单独的路由信息,从而造成路由表条目的急剧增长。

[0009] 3. 多家乡问题。多家乡通常指终端或网络同时通过多个 ISP 的网络接入到互联网。多家乡技术的优点包括增加网络的可靠性、支持多个 ISP 之间的流量负载均衡和提高总体可用带宽等。但是,IP 地址双重属性的内在矛盾使得多家乡技术难以实现。IP 地址的身份属性要求一个多家乡终端始终对其他终端展现不变的身份,无论该多家乡终端是通过几个 ISP 接入到互联网;而 IP 地址的位置属性则要求一个多家乡终端在不同的 ISP 网络中使用不同的 IP 地址通信,这样才能保证终端的 IP 地址能够在 ISP 网络的拓扑中聚合。

[0010] 4. 安全和位置隐私问题。由于 IP 地址同时包含终端的身份信息和位置信息,所以通信对端和恶意窃听者都可以根据一个终端的 IP 地址同时获得该终端的身份信息和拓扑位置信息。总的来说,自从传统互联网的体系结构建立以来,互联网的技术环境和用户群体都已经发生了翻天覆地的变化,互联网需要随之进行革新。IP 地址的双重属性问题是困扰互联网继续发展的根本原因之一,将 IP 地址的身份属性和位置属性进行分离,是解决互联网所面临问题的一个很好的思路。新网络将基于这种思路进行设计,提出一种身份信息与位置信息分离映射的网络结构,以解决现有互联网存在的一些严重弊端。

[0011] 为了解决身份和位置的问题,业界进行了大量的研究和探索,所有身份与位置分离方案的基本思想都是将原本绑定在 IP 地址上的身份与位置双重属性分离。其中,有些方案采用应用层的 URL(统一资源定位符 UniformResource Locator, URL 是用于完整地描述 Internet 上网页和其他资源的地址的一种标识方法。) 或 FQDN(合格域名 Fully Qualified Domain Name) 作为终端的身份标识等;有些方案引入了新的名字空间作为身份标识,如 HIP(Host Identity Protocol) 在以 IP 地址为位置标识的网络层上增加主机标识;有些方案将 IP 地址进行分类,部分 IP 作为身份标识,部分 IP 作为位置标识,如 LISP(Locator/ID SeparationProtocol) 位置身份分离协议。

[0012] 其中比较有代表性的是基于网络的解决方案,其核心思想是将网络分为两个部分,一个部分是传输网络或者转发网络,位于整个网络的中心;另一部分是边缘网络或者接入网络,通过接入交换路由器连接到转发网络;其中接入网络和转发网络的地址空间和路由信息是相互隔离的。

[0013] 如图 1 所示,基于网络的身份位置分离方案中将传统的 IP 地址的双重功能分离分别为身份标识和位置标识,其中身份标识为端主机的身份属性,由于方案设计中作用在在接入网络,因此也称为接入标识 AID(Access ID), AID 作为端主机的身份标识,作用域在接

入网络中；其中位置标识为端主机的位置属性，由于方案设计中作用在转发网络中，用于转发网络的路由，因此也称为路由标识 RID(Route ID)，RID 作为端主机的路由标识，作用域在转发网络；接入服务节点 ASN(Access Service Node) 完成移动终端 AID 和 RID 在映射服务器的注册和查询。

[0014] 移动终端向通信对端 CN 发起通信时，由其接入服务节点 ASN 向身份位置映射服务器发起位置查询过程，查询获得目的终端的当前位置信息，返回给源端接入服务节点，保证其能够正确发起通信连接。

[0015] ASN :Access Service Node, 接入服务节点, ASN 维护移动终端与网络的连接关系，为移动终端分配 RID，并处理终端切换的位置更新，处理终端位置信息登记注册，计费 / 鉴权，维护 / 查询通讯对端的 AID-RID 映射关系。

[0016] ASN 封装、路由并转发终端发出的数据报文。ASN 收到源终端发来的数据报文时，根据数据报文中的通信对端 AID 查询本地缓存表中的 AID-RID 映射表：查到对应的 AIDc-RIDc 映射条目，将 RIDc 封装在数据报文头部并转发到转发网络；没有查到对应的 AIDc-RIDc 映射条目，向映射转发平面发出查询 AIDc-RIDc 映射关系的流程。

[0017] GSR :General Switch Router, 通用交换路由器。路由并转发以 RID 为目的地址的数据报文。

[0018] 转发网络主要功能是根据数据报文中的路由标识 RID 进行选路和转发数据报文。

[0019] 映射服务器主要功能是保存移动节点的 AID-RID 的映射信息，处理移动节点的登记注册流程，处理通信对端的位置查询流程。

[0020] 上述方案存在的问题：

[0021] 源端接入服务节点 ASNs 发起位置查询过程的触发条件是终端“发起通信”。在发起通信过程中，可能需要源端接入服务节点 ASNs 进行通信对端 CN 位置查询过程，此时源端接入服务节点 ASNs 中没有通信对端位置和身份之间的映射关系，即对端的 RIDc(路由标识)-AIDc(接入标识)的映射表项，无法按照 RIDc 标识的路由转发数据报文。根据不同的网络传输条件和网元位置，源端接入服务节点 ASNs 发起的通信对端 CN 位置查询过程可能持续几百毫秒到几秒的时间。

[0022] 在这种情况下 ASNs 收到终端发给对端的数据报文，发起对端映射信息的查询，等待映射服务器返回对端的映射信息，ASNs 必须对接收到的数据报文进行缓存，消耗大量的资源，等待的时间越长，缓存的数据量越大，必然影响正常的转发性能；同时还存在安全方面的隐患，容易形成对映射服务器的攻击。

## 发明内容

[0023] 本发明要解决的技术问题是提供一种数据报文处理方法、服务接入节点及系统，以提高数据报文转发效率。

[0024] 为解决以上技术问题，本发明提供一种数据报文处理方法，该方法基于身份位置分离网络实现，域名系统 (DNS) 服务器中保存端主机域名和接入标识 (AID) 的对应关系，该方法包括：

[0025] A、源端主机向 DNS 服务器发送 DNS 查询报文，其中携带目的端主机的域名，所述 DNS 服务器向所述源端主机返回包含目的端主机的 AID 的 DNS 响应报文；

- [0026] B、接入服务节点(ASN)侦听DNS响应报文,获取响应报文中的目的端主机的AID;
- [0027] C、所述ASN根据所述目的端主机的AID向映射服务器查询获取所述目的端主机的路由标识(RID);
- [0028] D、所述ASN接收所述源端主机发送给目的端主机的数据报文后,根据所述目的端主机的RID进行数据报文转发。
- [0029] 进一步地,步骤B中,ASN从接收的转发网络报文中,侦听DNS响应报文,并根据DNS报文格式、DNS的端口号、DNS的接入标识或DNS的路由标识,判断收到的转发网络报文是否为DNS响应报文。
- [0030] 进一步地,步骤A中,所述DNS查询报文经过ASN转发至DNS服务器,步骤B中,所述ASN从DNS响应报文中获取目的端主机的AID后,将所述DNS响应报文转发给源终端;所述源终端根据所述DNS响应报文中的目的端主机AID向目的端主机发送数据报文。
- [0031] 进一步地,步骤C具体包括:所述ASN向映射服务器查询前先查询本地缓存,若本地缓存中没有目的端主机的AID和RID的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的RID,缓存目的端主机的AID和RID的映射关系。
- [0032] 进一步地,步骤D中,所述ASN接收到所述源端主机发送给目的端主机的数据报文后,先查询本地缓存,若本地缓存中没有或者正在查询目的端主机的AID和RID的映射关系,则等待收到所述映射服务器的映射查询响应后,再进行报文转发。
- [0033] 进一步地,所述ASN采用封装或替换的方式实现数据报文转发。
- [0034] 进一步地,步骤D中,所述源端主机发送的数据报文中源、目的地址分别为源、目的端主机的AID,所述ASN进行数据报文转发时,用源、目的端主机的RID对源端主机发送的数据报文进行封装,封装后的数据报文的源、目的地址分别为源、目的端主机的RID,且封装后的报文还包括源、目的端主机的AID。
- [0035] 进一步地,所述源端主机发送的数据报文的源、目的地址分别为源、目的端主机的AID,所述ASN进行数据报文转发时,用源、目的端主机的RID替换源、目的端主机的AID,所述AID与RID唯一对应。
- [0036] 为解决以上技术问题,本发明还提供一种接入服务节点,该接入服务节点(ASN)位于身份位置分离网络,所述身份位置分离网络包括DNS服务器,用于保存端主机域名和接入标识的对应关系,接收端主机发送的携带目的端主机的域名的DNS查询报文,以及向端主机返回携带目的端主机的AID的DNS响应报文,所述ASN包括:
- [0037] 侦听模块,与报文处理模块连接,用于侦听DNS响应报文,获取响应报文中的目的端主机的接入标识(AID);
- [0038] 映射查询模块,与所述侦听模块连接,用于根据获取的目的端主机的AID向映射服务器查询获取目的端主机的路由标识(RID);
- [0039] 报文处理模块,与所述映射查询模块及侦听模块连接,用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的RID进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文。
- [0040] 进一步地,所述ASN的侦听模块从所述报文处理模块收到的转发网络报文中,侦听DNS响应报文,并根据DNS报文格式、DNS的端口号、DNS的接入标识或DNS的路由标识,

判断收到的转发网络报文是否为 DNS 响应报文。

[0041] 进一步地,所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

[0042] 进一步地,所述 ASN 还包括与所述映射查询模块连接的映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用于向所述映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

[0043] 进一步地,所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后,还用于通知映射查询模块查询映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系,则等待映射查询模块收到所述映射服务器的映射查询响应后,再进行报文转发。

[0044] 进一步地,所述 ASN 的报文处理模块采用封装或替换的方式实现数据报文转发。

[0045] 为解决以上技术问题,本发明还提供一种数据报文处理系统,该数据报文处理系统基于身份位置分离网络实现,该系统包括端主机、接入服务节点(ASN)及 DNS 服务器,其中:

[0046] 所述端主机,包括域名查询模块及报文收发模块,其中,域名查询模块用于向 DNS 服务器发送携带目的端主机的域名的 DNS 查询报文,以及接收所述 DNS 服务器返回的携带目的端主机的 AID 的 DNS 响应报文;报文收发模块用于根据所述 DNS 响应报文中的目的端主机 AID 向目的端主机发送数据报文及接收数据报文;

[0047] 所述 ASN 包括:

[0048] 倾听模块,与报文处理模块连接,用于监听 DNS 响应报文,获取响应报文中目的端主机的接入标识(AID);

[0049] 映射查询模块,与所述倾听模块连接,用于根据获取的目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识(RID);

[0050] 报文处理模块,与所述映射查询模块及倾听模块连接,用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的 RID 进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文;

[0051] DNS 服务器用于保存端主机域名和接入标识的对应关系,接收端主机发送的 DNS 查询报文,以及向端主机返回 DNS 响应报文。

[0052] 进一步地,所述 ASN 的倾听模块从所述报文处理模块收到的转发网络报文中,监听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

[0053] 进一步地,所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

[0054] 进一步地,所述 ASN 还包括与所述映射查询模块连接映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用

于向所述映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

[0055] 进一步地，所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后，还用于通知所述映射查询模块查询映射信息缓存模块，若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系，则等待映射查询模块收到所述映射服务器的映射查询响应后，再进行报文转发。

[0056] 进一步地，所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文中源、目的地址分别为源、目的端主机的 AID，进行数据报文转发时，用源、目的端主机的 RID 对源端主机发送的数据报文进行封装，封装后的数据报文的源、目的地址分别为源、目的端主机的 RID，且封装后的报文还包括源、目的端主机的 AID。

[0057] 进一步地，所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文的源、目的地址分别为源、目的端主机的 AID，进行数据报文转发时，用源、目的端主机的 RID 替换源、目的端主机的 AID，所述 AID 与 RID 唯一对应。

[0058] 本发明数据报文处理方法、接入业务节点及系统基于身份位置分离网络架构，接入服务节点 (ASN) 收到源端主机发送的数据报文前，根据源端主机查询 DNS (domain name system, 域名系统) 返回的数据报文侦听到目的端主机的 AID，并向映射服务器查询 AID-RID 的映射信息，从而提高 ASN 对源端主机数据报文的转发效率，改善 ASN 的转发性能。

## 附图说明

- [0059] 图 1 身份和位置分离的网络架构的组成示意图；
- [0060] 图 2 是本发明数据报文处理方法的流程示意图；
- [0061] 图 3 是本发明接入服务节点的模块结构示意图；
- [0062] 图 4 是本发明数据报文处理系统的模块结构示意图。

## 具体实施方式

[0063] 本发明数据报文处理方法、接入业务节点及系统的主要思想是基于身份位置分离网络架构，接入服务节点 (ASN) 收到源端主机发送的数据报文前，根据源端主机查询 DNS (domain name system, 域名系统) 返回的数据报文侦听到目的端主机的 AID，并向映射服务器查询 AID-RID 的映射信息，从而提高 ASN 对源端主机数据报文的转发效率，改善 ASN 的转发性能。

[0064] 本发明所说的身份位置分离网络架构，将传统互联网的 IP 地址标识身份和位置的双重功能进行分离，实现对移动性、多家乡性、IP 地址动态重分配、减轻路由负载及下一代互联网中不同网络区域之间的互访等问题的支持。

[0065] 身份位置分离架构网络具有以下特点：网络划分为接入网和转发网，接入网位于转发网的边缘，负责所有终端的接入。转发网负责不同通过接入网接入的终端的路由。接入服务节点位于转发网和接入网的分界点，具有与接入网接口，与转发网接口。接入网与转发网在拓扑关系上没有重叠。用户终端间进行通信只需使用对端的身份标识进行识别，身份标识作用在接入网，也称为接入标识。接入服务节点为终端提供接入服务，维护用户连接，转发用户数据。

[0066] 图 2 为本发明实施例的数据报文处理方法的流程图，本发明数据报文处理流程包

括：

[0067] 201：源端主机根据要访问的目的端主机的域名向 DNS 服务器发送 DNS 查询报文，其中携带目的端主机的域名，所述 DNS 服务器向所述源端主机返回包含目的端主机的接入标识（AID）的 DNS 响应报文；

[0068] 在传统的 DNS 服务器中存储端主机的域名和 IP 地址的对应关系，在本发明的身份和位置分离网络中，DNS 服务器中存储端主机的域名和接入标识（即端主机的身份属性）的对应关系，同时 DNS 服务器在身份和位置分离网络中有自己的接入标识和路由标识。

[0069] 源端主机和目的端主机通信时，源端主机根据目的端主机的域名利用 DNS 客户端协议查询 DNS 服务器以得到目的端主机的接入标识 AID，DNS 服务器返回包含目的端主机接入标识 AID 的响应报文，源接入服务节点 ASN 倾听该响应报文，获取目的端主机的 AID。

[0070] DNS 服务器的接入标识是系统设定的公知地址，源端主机发送的 DNS 查询报文和服务器返回 DNS 响应报文的传输必须经过 ASN。

[0071] DNS 的报文格式如下：

[0072]

标识	标志
问题数	资源记录数
授权的资源记录数	额外资源记录数
查询问题	
回答（资源记录数可变）	
授权（资源记录数可变）	
额外信息（资源记录数可变）	

[0073] 其中：

[0074] 标识字段：用于报文标识，终端设置，DNS 服务器使用该标识返回结果；

[0075] 标志字段：16 位，重要位段的定义如下：

[0076]

位数	名称	说明
1 位	QR	0 表示查询报文 1 表示响应报文
4 位	Opcode	0 表示标准查询
1 位	AA	表示授权回答
1 位	TC	表示可切断
4 位	Rcode	返回码，0 表示无差错

[0077] DNS 查询报文中的问题部分通常只有一个问题，格式包括查询名、查询类型和查询类，查询名就是需要查找的域名，如“ZTE.COM.CN”。查询类为 1 是指互联网地址 IP，本发明为接入标识。

[0078] DNS 响应报文中的资源记录，在 DNS 报文格式中的最后 3 个字段，回答字段、授权字段和额外字段，采用资源记录格式，格式如下：

[0079]

域名	类型	类
生存时间	资源数据长度	资源数据

[0080] 其中：域名是记录中资源数据对应的名字，它的格式和前面的查询名字段格式一样。

[0081] 类型说明 RR 的类型码，它和前面的查询类型值是一样的。通常为 1，表示互联网数据。

[0082] 生存时间是客户程序保留该资源记录的秒数，资源记录通常的生存时间为 2 天。

[0083] 资源数据长度说明资源数据的数量，该数据的格式依赖域类型字段的值，对于类型 A 资源数据是 4 字节的 IP 地址（本发明中为接入标识）。

[0084] 202，ASN 倾听 DNS 响应报文，获取响应报文中的目的端主机的接入标识（AID）；

[0085] ASN 从收到的转发网络报文（本发明中将转发网络发送过来的报文称为转发网络报文）中倾听 DNS 响应报文，判断该报文是否是 DNS 的响应报文，如果是，则实时提取 DNS 响应报文中的目的端主机的 AID，完成倾听功能，并将 DNS 响应报文转发给源端主机，源端主机接收到该 DNS 响应报文后，生成目的地址为目的端主机的接入标识的数据报文，并发送给源端 ASN。

[0086] ASN 可根据以下三种方式判断接收的报文是否为 DNS 响应报文：

[0087] 1、ASN 根据上述的 DNS 的报文格式判断是否为 DNS 响应报文；

[0088] 2、DNS 均支持 UDP 和 TCP，并使用特定的端口号，如 DNS 的端口号为 53，DNS 的查询报文的目的端口号为 53，DNS 响应报文的源端口号为 53，ASN 根据源端口号判断是否为 DNS 响应报文；

[0089] 3、DNS 有特定的接入标识及路由标识，ASN 根据源端地址中的接入标识或路由标识进行判断。

[0090] 203，ASN 根据目的端主机 AID 获取目的端主机的 RID；

[0091] 若 ASN 本地缓存有映射关系，则 ASN 获取目的端主机 AID 后先查询本地缓存的映射关系，若在本地缓存中未查到目的端主机的映射关系，则 ASN 向身份位置分离网络的映射服务器发送映射查询请求，根据映射服务器的映射查询响应获取目的端主机的 RID，并根据映射服务器返回的目的端主机 RID 在本地缓存保存目的端主机的 AID 和 RID 的映射关系；

[0092] 若 ASN 本地缓存中没有保存映射关系，则 ASN 获取目的端主机 AID 后直接向映射服务器查询目的端主机的 RID。

[0093] ASN 向映射服务器查询目的端主机的 RID 时，查询请求中携带目的端主机的 AID，向身份位置分离网络的映射服务器查询映射信息，即目的端主机所属的接入服务节点的位

置 RID。

[0094] 204, ASN 接收所述源端主机发送给目的端主机的数据报文后,根据所述目的端主机的 RID 进行数据报文转发。

[0095] 接收数据报文与获得映射服务器返回的 RID 之间一定有时间差,多数情况是先收到终端的数据报文,这种情况下,先查询本地缓存,若本地缓存中没有或者正在查询目的端主机的 AID 和 RID 的映射关系,则缓存数据报文,等待收到映射查询响应后,再进行报文转发;如果先收到映射服务器返回的映射信息,不管是否收到终端的数据报文,应该立即将 RID 进行本地映射表的缓存,这样 ASN 收到终端的数据报文以后就可以直接进行本地查询。

[0096] 源端主机发送的数据报文中源、目的地址分别为源、目的端主机的 AID, ASN 接收所述源端主机发送给目的端主机的数据报文后,根据数据报文中的目的端主机 AID 查询本地缓存获取目的端主机 RID,并根据目的端主机 RID 进行数据报文转发。

[0097] 数据报文转发的方式有以下两种:

[0098] (1) 封装转发

[0099] 源接入服务节点 ASNs 利用查询到的 RID 封装该数据报文,封装后的数据报文的源、目的地址分别为源其中包括源、目的端主机的 RID,且封装后的报文还包括源、目的端主机的 AID;然后通过转发网络发送给目的接入服务结点 ASNd, ASNd 解封装后发送给目的端主机。

[0100] (2) 替换转发

[0101] 源接入服务节点 ASNs 利用查询到的 RID 替换该数据报文中的目的主机的 AID,然后通过转发网络发送给目的接入服务结点 ASNd, ASNd 将接收数据报文 RID 替换回 AID 后发送给目的端主机。

[0102] 需要说明的是,替换转发的情形下,源端主机的 AID 和源 ASN 分配的 RID 是一一对应的,同样的目的端主机的 AID 和目的端 ASN 分配的 RID 也是一一对应的。

[0103] 本发明中,通过 ASN 倾听 DNS 响应报文,提前获取目的端主机的 AID,并在本地未缓存目的端主机的映射关系的情况下,提前向映射服务器进行查询,从而减少数据报文的缓存,减少缓存器的大小,减少数据管理的任务量,使得 ASN 设备有更多的资源来进行数据转发,提高转发数据的处理效率。

[0104] 图 3 所示,为实现以上方法,本发明还提供了一种接入服务节点,该接入服务节点 (ASN, Access Service Node) 位于身份位置分离网络,所述身份位置分离网络包括 DNS 服务器,用于保存端主域名和接入标识的对应关系,接收端主机发送的携带目的端主机的域名的 DNS 查询报文,以及向端主机返回携带目的端主机的 AID 的 DNS 响应报文,

[0105] 所述 ASN 的功能包括:维护终端与网络的连接关系,为终端分配 RID,处理终端切换的位置更新,处理终端的登记注册,计费 / 鉴权,维护 / 查询通讯对端的 AID-RID 映射关系;ASN 封装、路由并转发送达终端或终端发出的数据报文。ASN 收到终端发来的数据报文时,根据数据报文中的通信对端 AIDc 查询本地映射表中的 AID-RID 映射表:没有查到对应的 AIDc-RIDc 映射条目,向映射服务器发出查询 AIDc-RIDc 映射关系的流程。

[0106] GSR:General Switch Router,通用交换路由器,路由并转发以 RID 为目的地址的数据报文。

[0107] 与本发明相关地, ASN 包括:

[0108] 倾听模块,与报文处理模块连接,用于监听 DNS 响应报文,获取响应报文中目的端主机的接入标识 (AID) ;

[0109] 映射查询模块,与所述倾听模块连接,用于根据获取的目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识 (RID) ;

[0110] 报文处理模块,与所述映射查询模块和倾听模块连接,用于接收、处理并转发数据报文、DNS 查询及响应报文以及映射查询及响应报文,与本发明相关地,包括用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的 RID 进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文。

[0111] 进一步地,所述 ASN 的倾听模块从所述报文处理模块收到的转发网络报文中,监听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

[0112] 进一步地,所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

[0113] 进一步地,所述 ASN 还包括与所述映射查询模块连接的映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用于向所述映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

[0114] 进一步地,所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后,还用于通知所述映射查询模块查询映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系,则缓存该数据报文,等待映射查询模块收到所述映射服务器的映射查询响应后,再进行报文转发。

[0115] 所述 ASN 的报文处理模块采用封装或替换的方式实现数据报文转发,具体如上所述。

[0116] 本发明还提供一种数据报文处理系统,如图 4 所示,该系统基于身份位置分离网络实现,该系统包括端主机、接入服务节点 (ASN) 及 DNS 服务器,其中:

[0117] 所述端主机,包括域名查询模块及报文收发模块,其中,域名查询模块用于向 DNS 服务器发送携带目的端主机的域名的 DNS 查询报文,以及接收所述 DNS 服务器返回的携带目的端主机的 AID 的 DNS 响应报文;报文收发模块用于根据所述 DNS 响应报文中的目的端主机 AID 向目的端主机发送数据报文及接收数据报文;

[0118] 所述 ASN 包括:

[0119] 倾听模块,与报文处理模块连接,用于监听 DNS 响应报文,获取响应报文中目的端主机的接入标识 (AID) ;

[0120] 映射查询模块,与所述倾听模块连接,用于根据获取的目的端主机的 AID 向映射服务器查询获取目的端主机的路由标识 (RID) ;

[0121] 报文处理模块,与所述映射查询模块及倾听模块连接,用于接收、处理并转发数据报文、DNS 查询及响应报文以及映射查询及响应报文,与本发明相关地,包括用于接收源端主机发送给目的端主机的数据报文,还用于根据映射查询模块获取的 RID 进行数据报文转发;还用于接收及转发从转发网络发来的发送给其下源端主机的报文;

[0122] DNS 服务器用于保存端主机域名和接入标识的对应关系,接收端主机发送的 DNS 查询报文,以及向端主机返回 DNS 响应报文。

[0123] 所述 ASN 的侦听模块从所述报文处理模块收到的转发网络报文中,侦听 DNS 响应报文,并根据 DNS 报文格式、DNS 的端口号、DNS 的接入标识或 DNS 的路由标识,判断收到的转发网络报文是否为 DNS 响应报文。

[0124] 所述报文处理模块,还用于接收并转发的报文包括源端主机发送给 DNS 服务器的 DNS 查询报文以及 DNS 服务器发送给源端主机的 DNS 响应报文。

[0125] 所述 ASN 还包括与所述映射查询模块连接映射信息缓存模块,用于缓存端主机的 AID 和 RID 的映射关系;所述映射查询模块向映射服务器查询前,先查询所述映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 的映射关系,再向映射服务器发送映射查询请求,根据映射服务器的映射查询响应获取目的端主机的 RID,还用于向所述映射信息映射信息缓存模块保存目的端主机的 AID 和 RID 的映射关系。

[0126] 所述 ASN 的报文处理模块接收到所述源端主机发送给目的端主机的数据报文后,还用于通知映射查询模块查询映射信息缓存模块,若映射信息缓存模块中没有目的端主机的 AID 和 RID 映射关系,则报文处理模块内部缓存该数据报文,等待映射查询模块收到所述映射服务器的映射查询响应后,再进行报文转发。

[0127] 所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文中源、目的地址分别为源、目的端主机的 AID,进行数据报文转发时,用源、目的端主机的 RID 对源端主机发送的数据报文进行封装,封装后的数据报文的源、目的地址分别为源其中包括源、目的端主机的 RID,且封装后的报文还包括源、目的端主机的 AID。

[0128] 所述 ASN 的报文处理模块接收的所述源端主机发送的数据报文的源、目的地址分别为源、目的端主机的 AID,进行数据报文转发时,用源、目的端主机的 RID 替换源、目的端主机的 AID,所述 AID 与 RID 唯一对应。

[0129] 若源端 ASN 发送的数据报文是封装后的数据报文,则目的端 ASN 对接收的数据报文进行解封装还原;若源端 ASN 发送的数据报文是替换后的数据报文,则目的端 ASN 对接收的数据报文进行替换还原;即目的端 ASN 对报文的操作是源端 ASN 的反操作。

[0130] 进一步地,所述身份位置分离网络还包括映射服务器,所述映射服务器,用于根据 ASN 的查询向所述 ASN 返回 RID。

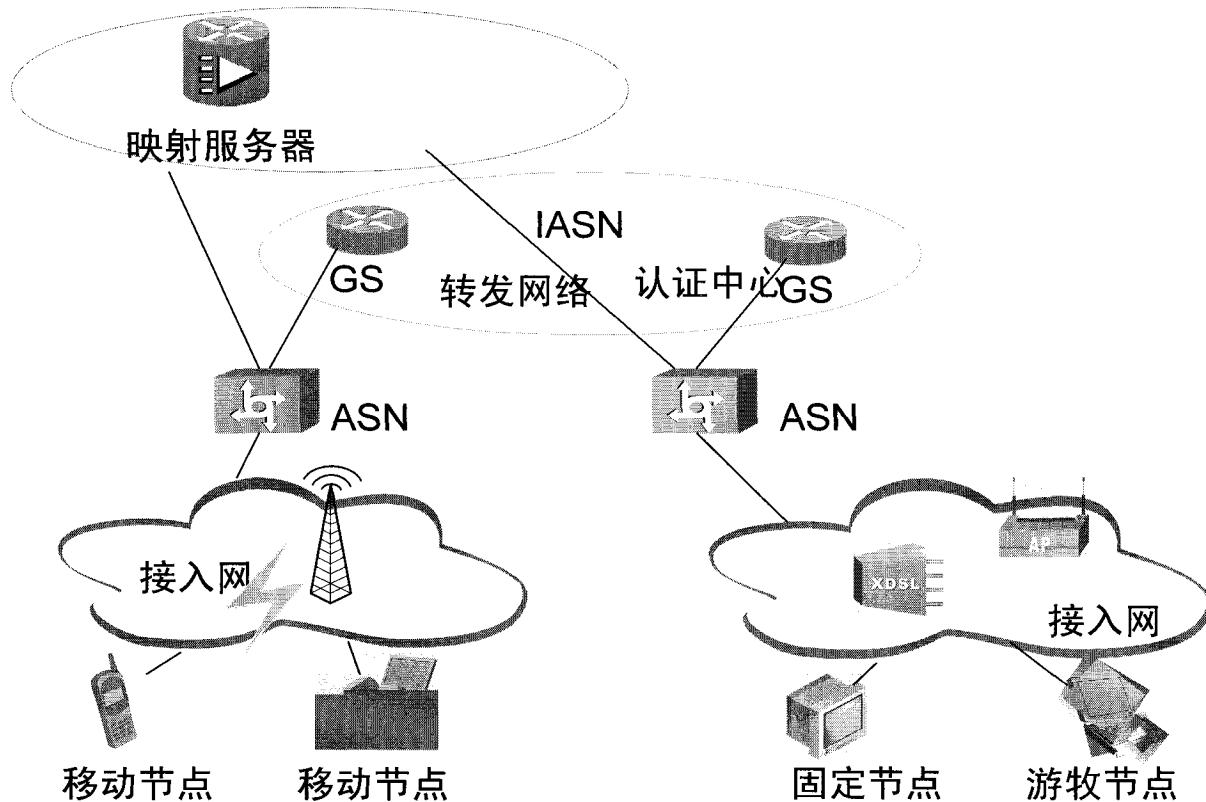


图 1

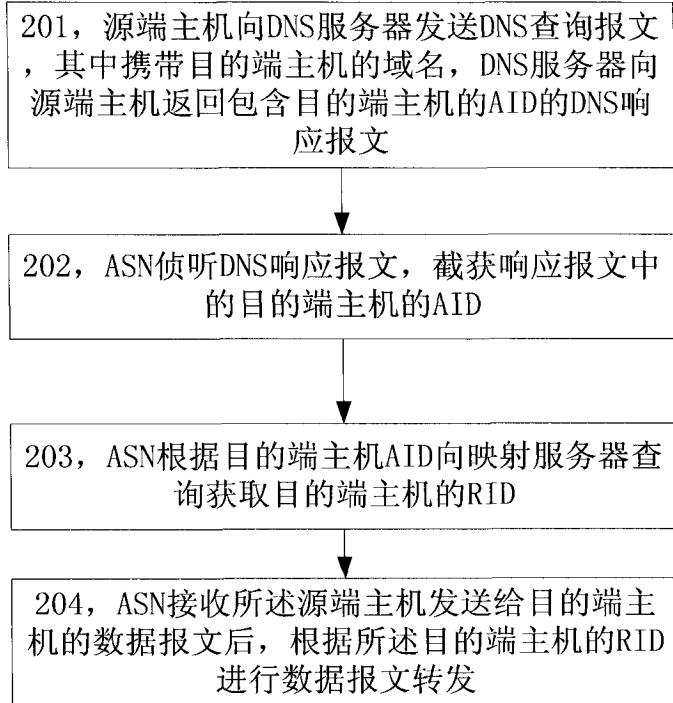


图 2

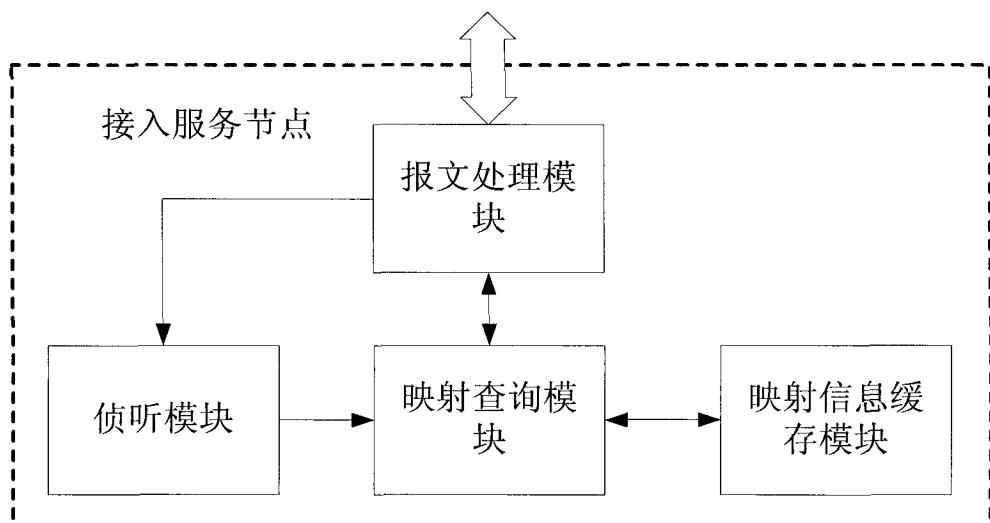


图 3

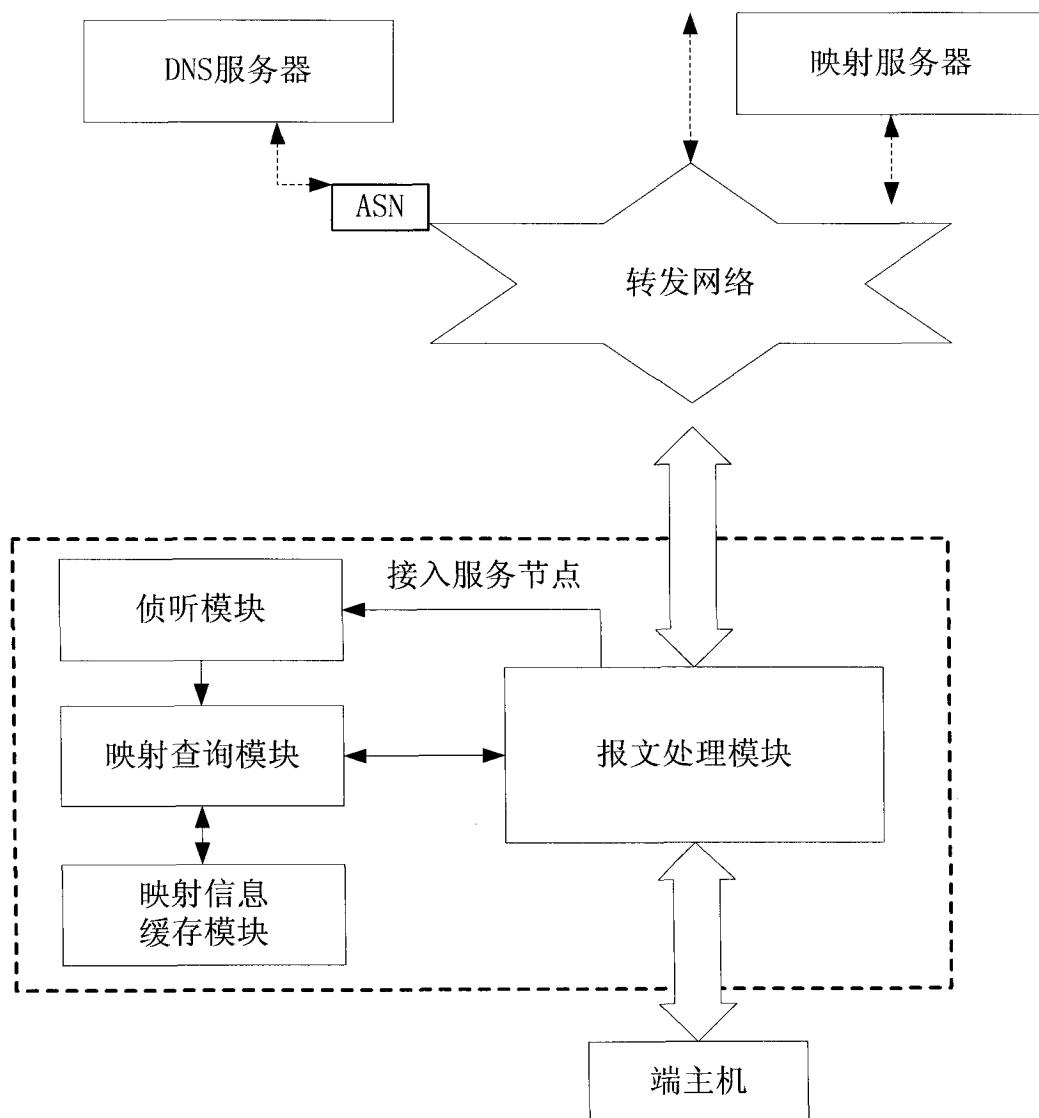


图 4