[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04Q 7/38
H04L 12/66 H04L 12/46
H04L 9/32 H04L 29/06

[12] 发明专利申请公开说明书

[21] 申请号 03138044.1

[43] 公开日 2004 年 12 月 8 日

[11] 公开号 CN 1553741A

[22] 申请日 2003.5.30 [21] 申请号 03138044.1

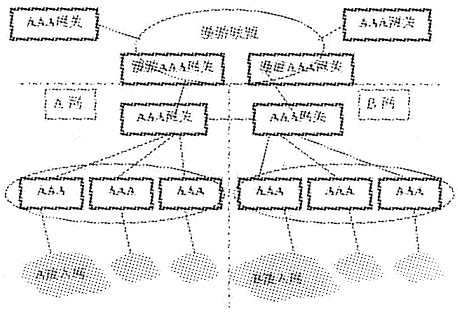
[71] 申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼
[72] 发明人 金 涛 周剑光 王 逵 管红光
[74] 专利代理机构 北京英赛嘉华知识产权代理有限责任公司
代理人 余 朦 方 挺

权利要求书 3 页 说明书 18 页 附图 6 页

[54] 发明名称 为用户提供网络漫游的方法和系统

[57] 摘要

本发明提供了一种为用户提供网络漫游服务的方法及系统。 本发明的方法在各个运营商的网络中配置了漫游转发装置，该漫游转发装置包括同一运营商在分层组网方式中的高层 AAA 服务器和星状组网中的中心 AAA 服务器，以及不同运营商之间的边界 AAA 网关和多个运营商之间的边界 AAA 网关和漫游联盟的 AAA 网关。 从而可以只在有限的几台设备上配置漫游的连接关系，实现了维护量小、多个运营商之间互通便利、以及网络安全性高等优点。



ISSN1008-4274

1. 一种在网络系统中为用户提供漫游服务的方法，所述网络系统包括客户终端；接入设备，包括漫游地接入设备和所述漫游用户的归属地接入设备；AAA服务器，包括漫游地AAA服务器和所述漫游用户的归属地AAA服务器；以及漫游转发装置，连接在所述漫游地AAA服务器与归属地AAA服务器之间，用于转发漫游用户的认证与计费信息，

所述方法包括：

（1）漫游地接入设备根据漫游用户的客户终端设备发来的接入请求，获取用户信息；

（2）漫游地接入设备将所述用户信息发送至漫游地AAA服务器进行认证；

（3）漫游地AAA服务器对用户信息进行识别，当确定为漫游用户时，将该用户的认证信息发送至漫游转发装置，通过漫游转发装置发送给该用户归属地的AAA服务器进行认证；

（4）该用户归属地的AAA服务器根据用户信息判断用户是否合法，然后将认证成功/失败报文通过漫游转发装置发送给所述漫游地AAA服务器；

（5）如果该用户归属地的AAA服务器发来的是认证成功报文，则所述漫游地AAA服务器将通知所述漫游地接入设备给用户授权；如果发来的是认证失败报文，则拒绝为该用户提供接入服务；

（6）在对所述用户认证成功后，所述漫游地接入设备向所述漫游地AAA服务器发出计费开始请求；

（7）所述漫游地AAA服务器将计费报文通过所述漫游转发装置转发至所述用户归属地AAA服务器进行计费。

2. 根据权利要求1所述的方法，其特征在于，所述步骤（3）进一步包括：所述漫游转发装置根据漫游地AAA服务器与所述归属地AAA服务器的协议类型及对报文格式的要求，进行协议适配和报文格式的变换。

3. 根据权利要求2所述的方法，其特征在于，所述漫游转发装置进行协

议适配和报文格式的变换是按照所述漫游转发装置配置的设备名和数字编码的映射表进行的。

4. 根据权利要求1、2或3所述的方法，其特征在于，所述认证方式是PPPoE认证、WEB认证或802.1X认证。

5. 根据权利要求4所述的方法，其特征在于，进一步包括在所述漫游转发装置中确定对用户认证报文的处理策略的过程，所述过程包括:

当收到用户的认证报文时，解析出认证报文属性;

判断是否需要进行配置数据的查找，如果是，则根据用户数据部分的内容确定对该认证报文处理的策略;

如果没有找到用户数据，则根据域数据部分中的内容确定对该认证报文处理的策略;

如果没有找到域数据，则使用缺省配置数据；以及

根据确定的处理策略，进行下一步处理。

6. 根据权利要求5所述的方法，其特征在于，进一步包括在漫游转发装置中保存所转发的用户认证和计费信息的步骤。

7. 一种为漫游用户提供漫游服务的网络系统，包括:

客户终端;

接入设备，所述接入设备用于为客户终端提供接入服务，包括漫游用户所在的漫游地接入设备和所述漫游用户的归属地接入设备;

AAA服务器，用于对接入设备转发的客户终端的用户信息进行认证和对接入成功的客户终端进行计费，包括漫游用户所在的漫游地AAA服务器和所述漫游用户的归属地AAA服务器，

其特征在于，所述系统还包括漫游转发装置，连接在所述漫游用户的漫游地AAA服务器与归属地AAA服务器之间，用于转发漫游用户的认证与计费信息。

8. 根据权利要求7所述的系统，其特征在于，属于同一网络运营商或企业的所述AAA服务器之间采用分层组网方式、星状组网方式、或者分层组网与星状组网以及网状/半网状组网方式的组合方式连接。

9. 根据权利要求8所述的系统，其特征在于，所述漫游转发装置包括所述分层组网的所述网络同一运营商或企业的网络中的高层AAA服务器、所述星状组网的所述同一网络运营商局域网或企业中的中心节点的AAA服务器、或者是所述的这两种AAA服务器的组合，用于为所述多个运营商或企业进行协议适配和认证报文的转发。

10. 根据权利要求7所述的系统，其特征在于，所述漫游转发装置包括连接在两个或多个网络运营商或企业之间的AAA网关，用于为所述多个运营商或企业进行协议适配和认证报文的转发。

11. 根据权利要求7所述的系统，其特征在于，所述漫游转发装置进一步包括与多个运营商或企业通过AAA网关互联的漫游联盟，用于为所述多个运营商或企业进行协议适配和认证报文的转发。

12. 根据上述权利要求任一项所述的系统，其特征在于，所述接入设备或AAA服务器中设置有漫游域模块，用于配置路径信息，以将漫游用户的认证和计费信息配置到可找到用户归属地AAA服务器的漫游转发装置上。

为用户提供网络漫游的方法和系统

发明领域

本发明涉及数据通信网络，特别涉及为用户提供网络漫游服务的方法和系统。

背景技术

现代社会已经进入信息社会，而通信网络作为信息的载体，已经应用到整个社会的各个方面。常用的通信技术有以太网、令牌网、FR（帧中继）、IP（因特网协议）、ATM（异步转移模式）等等，常用的通信网络有以太网组成的局域网、TCP/IP组成的广域网和INTERNET（因特网）等等。

在实际网络中，PC（个人计算机）与网络的连接可以有多种方式，例如通过LAN Switch（以太网交换机）、AP（无线接入点）、VDSL（甚高速数字用户线路）、ADSL（不对称数字用户线路）等方式接入网络。

在需要管理的网络中，需要放置RADIUS（远端用户拨入鉴权服务）认证服务器等AAA（认证、授权和计费）服务器，来验证用户身份的合法性。另外，在实际应用中，为保证网络的安全性和管理需要，一般要求对客户进行认证、授权和计费，以保证客户合理地享受运营商提供的网络服务。常用的用户认证手段有很多种，例如PPPoE（以太网承载的点到点协议）认证、WEB认证和802.1X认证等。

在实际应用中，一个用户的信息一般都会存储在该用户开户的AAA服务器中，称为“归属地”AAA服务器，用户开户的网络称为“归属地”网络。用户在获得上网的开户信息后（包括但不限于用户名/密码、智能卡等信息），可以在网络提供商NSP/ISP提供的整个网络内使用。因此，从地理上，用户可以从NSP/ISP（网络服务提供商/网络接入服务提供商）网络上任何一个地方上网。在用户未处于归属地网络（即漫游）的情况下，用户接入的网络叫做“漫游地”网络，用户接入的地方也通过AAA服务器进行认证、授权、计费，这个AAA服务器叫做“漫游地”AAA服务器。

以一个提供在北京和南京接入的ISP（网络接入服务提供商）为例。A用户为北京用户，即其归属地AAA服务器在北京。当A用户在南京而需要从南京的同一个ISP网络中使用网络业务，比如访问WWW网站等时，就需要为其提供网络漫游服务。

此时，对A用户而言，南京是“漫游地”，南京接入的AAA服务器是“漫游地”AAA服务器。由于A用户的信息在北京，因此，南京的“漫游地”AAA服务器必须从北京的归属地AAA服务器才能够获得A用户的信息。

现在，企业和运营商都有漫游服务功能，但其规模都比较小。目前的认证计费服务器组网都是网状组网。不同运营商之间要么没有互联互通，要么就是有限的几台AAA服务器之间网状组网）。从物理设备连接角度看，每个AAA服务器之间通过电信网/因特网连接，如图1(a)所示。从逻辑连接来看，实际AAA服务器之间是网状网，每一个AAA服务器都和其他所有AAA服务器之间有连接。如图1(b)所示。

用户认证、计费时，使用的都是用户名，其中用户帐号名组成是“用户名@域名”，目前漫游地和归属地之间的识别都是通过“用户名@域名”中的域名，例如“user@chinatelecom.sh.com”中的“chinatelecom.sh.com”来识别的。例如，域名为chinatelecom.sh.com表示此用户开户AAA服务器是上海电信的AAA服务器。而“user@163.com”中的“163.com” 表示此用户开户AAA服务器即归属地AAA服务器在广东电信。

上述现有技术存在如下问题:

1. 由于所有AAA服务器是网状连接的，所有AAA服务器都必须知道其他所有存在连接关系的AAA服务器，需要在每一台AAA服务器上进行配置，因此，域名的增加、删除和改变往往波及整网所有的AAA服务器，维护量很大，维护难度也很大。

2. 不同运营商、企业之间如果采用网状连接的话，必须知道彼此的AAA配置，因此安全性很差。而且由于运营商之间管理问题，很难同步，维护难度非常大。

3. 由于AAA服务器之间是网状连接，所有认证、计费信息都是分散进行的，不同区域的同一运营商、以及不同运营商之间无法统一结算。

4. 每个运营商、企业之间互通时，都是商定双边协议，因此，一个运营商或者企业要和多个运营商或者企业互通时，要多次商定双边协议。不仅在协议之间有差别，很不方便，而且在技术上难度也较大。

5. 由于接入服务器或者类似的接入设备也需要配置所有的AAA服务器对应的关系，往往一个接入设备只能配置有限的域名关系，因此，扩展性差，而且维护量大。

发明内容

因此，本发明的目的就是要克服现有技术在实现用户漫游服务功能方面存在的上述缺陷。

根据本发明的第一方面，提供一种在上述系统中为用户提供漫游服务的方法，该方法包括:

（1）漫游地接入设备根据漫游用户的客户终端设备发来的接入请求，获取用户信息;

（2）漫游地接入设备将用户信息发送至漫游地AAA服务器进行认证;

（3）漫游地AAA服务器对用户信息进行识别，当确定为漫游用户时，将该用户的认证信息发送至漫游转发装置，通过漫游转发装置发送给该用户归属地的AAA服务器进行认证;

（4）该用户归属地的AAA服务器根据用户信息判断用户是否合法，然后将认证成功/失败报文通过漫游转发装置发送给所述漫游地AAA服务器;

（5）如果该用户归属地的AAA服务器发来的是认证成功报文，则所述漫游地AAA服务器将通知所述漫游地接入设备给用户授权;如果发来的是认证失败报文，则拒绝为该用户提供接入服务;

（6)在对所述用户认证成功后，所述漫游地接入设备向所述漫游地AAA服务器发出计费开始请求;

（7）所述漫游地AAA服务器将计费报文通过所述漫游转发装置转发至所述用户归属地AAA服务器进行计费。

本发明中所述的认证与计费方法可采用例如PPPoE、802.1X、WEB认证等常规方式。本领域技术人员可以理解，虽然在各种认证方法的过程中，接入设备和AAA服务器之间略有差别，但在本发明的上述方法中并不产生实质

性的差别。

根据本发明的第二方面，提供一种为用户提供漫游服务的系统，该系统包括：客户终端，接入设备和AAA服务器，其中接入设备用于为客户终端提供接入服务，所述AAA服务器用于对接入设备转发的客户终端的认证报文进行认证和对接入成功的客户终端进行计费，其特征在于，所述系统还包括漫游转发装置，用于在漫游用户的漫游地AAA服务器与归属地AAA服务器之间转发漫游用户的认证与计费信息。

在本发明的上述系统中，漫游转发装置可以包括分层组网的同一运营商网络中的高层AAA服务器、星状组网时中心AAA服务器、运营商边界的AAA网关。

在本发明的上述系统中，所述接入设备或AAA服务器中可以设置漫游域模块，用于配置路径信息，以将漫游用户的认证和计费信息配置到可找到用户归属地AAA服务器的漫游转发装置上。

本发明具有如下优点：

1、对于同一运营商或企业，只需要在有限的几台AAA服务器上配置漫游的连接关系，维护量小。

2、不同运营商、企业之间通过AAA服务器网关转发用户认证信息和计费信息，从而彼此之间通过网间接口互联，安全性高，易操作，维护量少。此外，通过AAA网关互联，所有认证、计费信息都是统一进行的，同一运营商的不同区域、以及不同运营商之间可以统一结算、统计。

3、当一个运营商或者企业要和多个运营商或者企业互通时，只要商定一次协议即可和所有运营商或者企业互通，协议完全一致，技术难度低，商定时间短。

4、接入设备或者类似的接入设备不需要配置所有的AAA服务器对应的关系，只要配置核心的关系和一个漫游关系，扩展性好，并且可以对接入设备实现零维护。

附图说明

通过详细文字说明并结合以下附图，本发明的上述目的、特征及优点将变得更加易于理解，其中：

图1（a）和（b）是说明现有的AAA服务器网状组网方式的示意图；

图2是说明在本发明优选实施方案中同一运营商的AAA服务器组网方式的示意图，其中图2（a）是分层组网方式；图2（b）是星状组网方式；

图3是分层组网方式中对高层AAA服务器进行配置的流程图；

图4是说明根据本发明优选实施方案的两个不同运营商之间组网方式的示意图；

图5是说明根据本发明优选实施方案在多个不同运营商之间组网方式的示意图；

图6是说明根据本发明优选实施方案的用户漫游认证、计费流程的流程图；

图7是说明根据本发明优选实施方案的协议适配过程的时序图，其中图7（a）表示相同协议之间的适配过程，图7（b）表示不同协议之间的适配过程。

具体实施方式

下面结合附图具体说明本发明的优选实施方案。

在本发明中，对用户认证和计费的方法可以采用如上所述的常规的PPPoE认证与计费、WEB认证与计费和802.1X认证与计费等方法。在本说明书中以PPPoE认证和计费为例来说明。

实施例1：同一运营商/企业中不同区域的漫游

同一运营商/企业的主要问题是网状连接问题，也就是常说的N^2问题，因此，可以采用其他组网方式，包括但不限于分层网络和星状网络解决这个问题。

在本发明的一个实施例中，分层组网如图2（a）所示，底层AAA服务器之间并不互联，由高层AAA服务器之间配置整网连接组成网状网络或者半网状网络，从而大大缓解了维护工作量，一般会降低一个数量级。

其中，在高层AAA服务器之间典型的配置例如为：

[用户数据部分]

用户名=lisi@local.com

属性=普通用户

下一个认证主服务器=

下一个认证备服务器=

下一个计费主服务器=

下一个计费备服务器=

这里需要说明，上面的配置中等号后面为空表示该用户是本地的AAA认证用户（域名为local.com），没有下一个服务器。

用户名=zhangsan@beijing.com

属性=proxy用户

下一个认证主服务器=10.1.1.1:1812

下一个认证备服务器=10.1.1.2:1812

下一个计费主服务器=10.1.1.3:1813

下一个计费备服务器=10.1.1.4:1813

共享密钥=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

[域名部分]

域名=roaming

属性=proxy

下一个认证主服务器=10.1.1.1:1812

下一个认证备服务器=10.1.1.2:1812

下一个计费主服务器=10.1.1.3:1813

下一个计费备服务器=10.1.1.4:1813

共享密钥=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

[default(缺省)]

属性=proxy !或者discard(丢弃)等

下一个认证主服务器=10.1.1.1:1812

下一个认证备服务器=10.1.1.2:1812

下一个计费主服务器=10.1.1.3:1813

下一个计费备服务器=10.1.1.4:1813

共享密钥=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

以上给出了一个简单的示例性的配置文件，以说明对分层组网中高层AAA服务器进行配置的方法。在实际当中，一般可以通过文本文件、二进制文件和数据库方式存储，通过手工编辑、配置界面如命令行或者GUI（图形用户界面）进行上述配置。具体处理流程如图3所示。

下面结合图3说明高层AAA服务器根据上述配置确定对漫游用户的认证报文的处理策略的过程：

1）当高层AAA服务器收到用户RADIUS报文时，解析出RADIUS报文属性；

2）根据各种常规的策略，以及例外处理（例如代码中固定特殊数据策略、系统管理员数据策略等等），判断是否需要进行配置数据的查找。如果是，转步骤3）；如果否，则转步骤8）。

3）根据用户数据部分的内容进行判断，如果从用户数据部分可以找到对应的数据，则以此数据中配置的策略来判断后续处理是进行认证计费，还是进行RADIUS Proxy（即远端用户拨入鉴权服务的代理），以及其他方式如丢弃、强制失败等等。同时，还要判断一些辅助的参数，比如RADIUS Proxy的下一步认证计费服务器地址、端口号、共享密钥等等。特别要说明的是，共享密钥可以明文，也可以通过对称/不对称加密方式进行保存，如常用的DES、3DES等。

4）如果没有找到用户数据，则转步骤5）；如果找到用户数据，则转步骤8）。

5）根据域数据部分中的内容进行判断，如果域数据部分可以找到对应的数据，以此数据所配置的策略来判断下一步处理是进行认证计费，还是进行RADIUS Proxy，以及其他方式如丢弃，强制失败等等。同时，还要判断一些辅助的参数，比如RADIUS Proxy的下一步认证计费服务器地址、端口号、共享密钥等等。特别要说明的是，共享密钥可以明文，也可以通过对称/不对称加密方式进行保存，如常用的DES、3DES等。

6）如果没有找到域数据，则转步骤7）；如果找到域数据，则转步骤8）。

7）使用缺省配置数据。

8）用户报文处理策略已经搜索完毕，根据找到的处理策略，进行下一步处理，包括RADIUS转发、认证、计费、丢弃等等。

根据上述的配置及处理过程，所有底层AAA服务器只要配置一条域数据或者缺省数据即可，从而可以大大缓解维护工作量，一般会降低一个数量级。但是高层AAA服务器之间，需要根据漫游的域，进行完全的配置。例如A服务器到B服务器有10个漫游域，A服务器到C服务器有5个漫游域，这样A服务器需要配置15个漫游域，其他的B、C服务器也一样。根据需要配置成为网状或者半网状网络。

分层组网的方式可以是两层，也可以是多层。

在本发明的另一种实施例中，也可以采用星状网络进行AAA服务器的组网，如图2（b）所示。

其具体的配置格式和处理流程与上述分层组网的方式相同。

因此，在配置时，所有星状网络上的边缘AAA服务器只要配置一条域数据或者缺省数据即可，从而可以大大减轻维护工作量，一般会降低一个数量级。而在星状网络中的中心节点的AAA服务器上，与上述分层组网中的高层AAA服务器类似，需要根据漫游的域进行完全的配置。即，整网上所有的漫游域都应该在中心节点AAA服务器上找到对应的配置。

在实际组网中，可以组合使用网状/半网状、层状、星状等等多种网络的某一种，或者多种组合使用。

用户漫游接入流程以PPPoE的认证为例，如图5所示。具体过程如下：

1) PPPoE 客户端向 PPPoE 服务器设备发送一个 PADI（PPPoE 激活发现初始报文）报文，开始 PPPoE 接入。

2) PPPoE 服务器向客户端发送 PADO 报文(PPPoE 激活发现提供报文)。

3) 客户端根据回应，发起 PADR（PPPoE 激活发现请求报文）请求给 PPPoE 服务器。

4) PPPoE 服务器产生一个 session id（会话标识），通过 PADS （PPPoE 激活发现会话报文）发给客户端。

5) 客户端和 PPPoE 服务器之间进行 PPP（点到点协议）的 LCP（链路控制协议）协商，建立链路层通信。同时，协商使用 CHAP（质询握手验证

协议）认证方式。

6) PPPoE 服务器通过 Challenge（质询）报文发送给认证客户端，提供一个 128 比特的 Challenge （即服务器产生的随机字）。

7) 客户端收到 Challenge 报文后，将密码和 Challenge 用公知的 MD5 算法处理，然后在 Response（回应）报文中把它发送给 PPPoE 服务器。

8) PPPoE 服务器将 Challenge、Challenge-Password 和用户名一起送到漫游地 RADIUS（远端用户拨入鉴权服务）用户认证服务器（即 AAA 服务器）进行认证。

9) 漫游地 RADIUS 用户认证服务器根据用户名识别是一个漫游用户，其归属地例如在北京，那么就先将此认证报文转发到中间 AAA 服务器，该中间的 AAA 服务器一般是分层组网时的高层 AAA 服务器或者星状组网时的中心接点 AAA 服务器。中间 AAA 服务器主要是完成 Proxy（代理服务器）的功能，例如是 RADIUS 代理服务器，执行典型的如公知的 RFC2865、RFC2866、RFC2869 的 RADIUS Proxy 功能。由此将“漫游地” AAA 服务器发过来的认证、计费报文按照域名配置寻找“归属地” AAA 服务器的路径，然后向下一个中间 AAA 服务器发送，直到发送到“归属地” AAA 服务器。中间 AAA 服务器可以是同一个区域内的，也可以是在不同区域。中间 AAA 服务器一般不直接做用户认证、计费功能，而是根据各种域名配置的路径信息，转发认证、计费报文。

10) 归属地 RADIUS 用户认证服务器根据用户信息判断用户是否合法，然后将回应认证成功/失败报文象在步骤 9）中那样通过中间 AAA 服务器发送到漫游地 RADIUS 用户认证服务器。

11) 漫游地 RADIUS 用户认证服务器将认证成功/失败报文转发到 PPPoE 服务器。如果成功，则携带协商参数以及用户的相关业务属性给用户授权。如果认证失败，则流程到此结束。

12) PPPoE 服务器将认证结果返回给客户端。

13) 用户进行 NCP（网络控制协议）（如 IPCP 即 IP 控制协议）协商，通过 PPPoE 服务器获取到规划的 IP 地址等参数。

14) 认证如果成功，PPPoE 服务器发起计费开始请求给漫游地 RADIUS 用户计费服务器。

15) 漫游地RADIUS用户计费服务器发现用户是漫游用户，其归属地在北京，那么就如同上述步骤9）那样将此计费报文通过中间AAA服务器转发到归属地RADIUS用户计费服务器，进行真正的计费。

16) 归属地RADIUS用户计费服务器回应计费开始应答报文，通过中间服务器转发给漫游地RADIUS用户计费服务器。

17) 漫游地RADIUS用户计费服务器将回应的计费开始应答报文转发给PPPoE服务器。

用户此时通过认证，并且获得了合法的权限，可以正常地接受网络服务。

当用户希望终止网络业务的时候，同样也可以通过PPPoE断开网络连接，此时会按照14）~17）中的过程发送计费终止报文。

如上所述，在该实施例中，用户的认证、计费报文在“漫游地”AAA服务器和“归属地”AAA服务器之间转发时（主要在步骤9）、10）和15）、16）中），要经过中间的多个AAA服务器。

实施例2：两个不同运营商/企业之间漫游

在每个运营商/企业边界上设置一个AAA网关，当用户在两个运营商/企业之间漫游时，彼此之间所有的认证、计费漫游都走这个网关。所有AAA服务器，除了配置本地用户认证、计费信息外，将所有漫游用户的域名都配置成为到AAA网关的缺省路径或者漫游路径。具体配置过程与上面对分层组网或星状组网中的配置相同。网络内的各AAA服务器无需配置每一个漫游域名对应的路径。这样，当在两个网络之间进行维护时，每增加、删除、修改一个新的域名，只需要在该AAA网关上进行对应的路径修改，而网络内的AAA服务器不需要做改动，从而减小了维护工作量。

同时，由于不同的运营商采用的协议可能不同，因此通过AAA网关方式，可以在AAA网关上进行协议适配，进行统一的认证统计，计费结算。目前协议适配有RADIUS-RADIUS、RADIUS-DIAMETER等，这些协议可以单向适配，但一般都是双向适配。

协议适配有两种方法：

1. 在使用同一种协议时，由于网关两侧对协议中认证、计费等属性有各自不同的要求，需要一个转换的过程，即在网关上进行属性转换，以满足

网关两侧的要求。具体地说，以RADIUS-RADIUS为例，AAA网关处理时序图如图7（a）所示。下面结合图7（a）说明协议适配的流程:

1）某一个AAA服务器向AAA网关发出RADIUS认证请求报文，其内容典型地包括例如用户名“zhangsan@beijing.com”、用户接入设备名、用户的密码等。

2）AAA网关识别出（一般简单地可以按照域名识别，也可以严格按照上述AAA处理流程识别）这个AAA服务器的报文格式和另一侧的AAA服务器的报文格式要求不一致，例如另一侧的AAA服务器要求所有用户名大写，并且要求提供用户漫游地AAA服务器的地址，而且用户接入设备名必须给出一个接入设备对应的数字编码，而不是名字。此时，该AAA网关根据该另一侧AAA服务器的要求，将接收到的RADIUS报文中的用户名全部改为大写，增加一个用户漫游地AAA服务器地址的属性并填入AAA服务器对应的IP地址，最后按照事先配置好的设备名和数字编码的映射表，改为对应的数字编码。然后将改变后的RADIUS重新组包发送给该另一侧的AAA服务器。

3）上述另一侧的AAA服务器在认证成功后，将认证成功报文返回给AAA网关。认证成功报文一般包括用户名、用户接入设备名等。

4）上述AAA网关接收到该报文后，识别出报文格式不匹配，按照上述协议适配过程的逆过程进行处理。将用户名保留或者变成小写，将用户接入设备名按照事先配置好的设备名和数字编码的映射表，从数字编码改为对应的设备名。

其他如RADIUS认证报文、计费报文处理流程也与上述过程基本一致。

在上述协议适配过程中，目前常用的技术是表格映射，即运营商A和运营商B之间的属性映射表，从而在转换时按照表格中的属性和规定的转换方法进行转换和逆转换。

当然，本发明并不局限于表格印射的方法，也可以使用其他广泛应用的方法如软件模块或者插件方法。例如，运营商A需要和运营商B之间漫游，则也可以在AAA网关上增加一个软件模块或者插件完成协议适配功能。其中，重新改变AAA网关软件或者增加补丁，来完成这个功能是最简单的方法。

2. 如果使用不同的协议，例如RADIUS、DIAMETER（一种兼容RADIUS协议的增强型AAA协议）等协议，那么就需要网关进行转换，从一种协议报

文转换成为另外一种协议报文。以RADIUS-DIAMETER为例，AAA网关处理时序图如图7（b）所示：

1）某一个AAA服务器向AAA网关发起RADIUS认证请求报文，内容典型的如用户名“zhangsan@beijing.com”、用户接入设备名、用户的密码等。

2）AAA网关识别出（一般简单的可以按照域名识别，也可以严格按照上述AAA处理流程识别）这个AAA服务器的报文格式和另外一侧的AAA服务器的报文格式要求不一致，例如另外一侧的AAA服务器要求使用DIAMETER协议，并且要求所有用户名大写、要求提供用户漫游地AAA服务器的地址、而且用户接入设备名必须给出一个接入设备对应的数字编码，而不是名字。此时，AAA网关根据要求，将接收到的RADIUS报文中的用户名全部改为大写，增加一个用户漫游地AAA服务器地址的属性并填入AAA服务器对应的IP地址，最后按照事先配置好的设备名和数字编码的映射表，改为对应的数字编码。然后将新的DIAMETER请求组包发送给该另外一侧的AAA服务器。

3）上述另外一侧的AAA服务器在认证成功后，将DIAMETER应答报文（包含认证成功信息）返回给AAA网关。认证成功报文一般包括例如用户名、用户接入设备名等。

4）AAA网关接收到该报文后，识别出报文格式不匹配，按照上述协议适配过程的逆过程进行处理。将DIAMETER协议转换为RADIUS协议，并且将用户名保留或者变成小写，将用户接入设备名按照事先配置好的设备名和数字编码的映射表，从数字编码改为对应的设备名。

其他如RADIUS认证报文、计费报文和DIAMETER处理流程也与上述过程基本一致。

与上述相同协议的适配过程类似，在不同协议的适配过程中，目前常用的技术是表格映射，即运营商A和运营商B之间属性映射表，从而在转换时按照表格中的属性和规定的转换方法进行转换和逆转换。当然也可以采用本领域普遍使用的方法如软件模块或者插件方法。其中最简单的方法是重新改变AAA网关软件或者增加补丁，来完成这个功能。

在本发明该实施例的用户漫游接入流程中，步骤（1）-（8）基本与前述实施例中的基本相同。不同之处在于，在步骤（9）中，如果漫游地RADIUS

用户认证服务器根据用户名识别是一个漫游用户，并且其归属地服务器是属于另一个运营商的，那么就先将此认证报文转发到漫游地的 AAA 网关。在 AAA 网关中使用标准的 Proxy 功能（典型的如公知的 RFC2865、RFC2866、RFC2869 的 RADIUS Proxy 功能），转发到归属地 AAA 网关上。归属地 AAA 网关也使用标准的Proxy功能将认证报文转发到归属地的RADIUS用户认证服务器上进行真正的认证。

在步骤（10）中，归属地RADIUS用户认证服务器根据用户信息判断用户是否合法，然后将认证成功/失败报文通过归属地AAA网关和漫游地AAA网关，转发到漫游地RADIUS用户认证服务器。此后的过程同实施例1的步骤（11）至（13）。

用户计费过程如下:

14）认证如果成功，PPPoE服务器发起计费开始请求给漫游地RADIUS用户计费服务器。

15）漫游地RADIUS用户计费服务器发现用户是漫游用户，那么就如同上述步骤9）那样将此计费报文通过中间AAA网关（漫游地AAA网关和归属地AAA网关）转发到归属地RADIUS用户计费服务器，进行真正的计费。

16）归属地RADIUS用户计费服务器回应计费开始应答报文，通过中间AAA网关（归属地AAA网关和漫游地AAA网关）转发给漫游地RADIUS用户计费服务器。

17）漫游地RADIUS用户计费服务器将回应的计费开始应答报文转发给漫游地PPPoE服务器。

实施例3: 多个运营商之间的漫游

当某一个特定用户漫游时，只能是两个运营商实体之间的漫游，但是当某个接入设备上接入的用户漫游时，就会出现在多个运营商之间的漫游。判断多个运营商之间的漫游，实际上就是判断某一个用户漫游情况的总和。

每个运营商、企业之间互通时，都是商定双边协议，因此，一个运营商或者企业，要和多个运营商或者企业互通时，要多次商定双边协议，而且协议之间有差别，很不方便，而且有技术难度。

通过组建一个漫游联盟，在联盟内进行所有漫游数据配置，使得所有接

入到漫游联盟的运营商、企业都可以互相漫游。并且一个运营商或者企业要和多个运营商或者企业互通时，只要与漫游联盟商定一次协议即可和所有运营商或者企业互通，协议完全一致，技术难度低，商定时间短。

同时，漫游联盟通过边界的AAA网关和各个运营商、企业网的AAA网关互联，可以提供协议适配、认证统计、计费结算等等。

为了实现认证统计和计费结算等，在运营商或者企业AAA网关，以及漫游联盟的AAA网关上除了报文转发、协议转换外，还要将认证信息、计费信息存储、计算汇总，从而使得两个连接的实体（例如运营商和运营商之间）可以核对详细的认证、计费信息（即对帐功能），以及双方汇总的认证信息的统计和计费信息的结算。例如，一般运营商和运营商之间有结算协议，假设计费信息是漫游地运营商和归属地运营商之间是3：7分成，则根据汇总后的计费信息进行收入结算。因此，在本发明中，将认证、计费信息存储在AAA网关上，即可采用常规的认证统计、计费结算、以及对帐方法。

“漫游联盟”可以指一个组织，在这里还可以指一组统一配置、管理的AAA服务器。从“漫游联盟”外来看，这些AAA服务器就有点类似上述的AAA网关，但这些AAA服务器不再是点对点的关系，而是一个多对多的关系。在上述网关基础上进行更进一步的要求，包括多对多的配置、多对多的适配等。其中配置的格式以及搜索过程如实施例2中所述，在本例中，需要额外说明的就是“漫游联盟”的AAA服务器中需要配置各互通的运营商之间所有相关的漫游关系，以及漫游时协议适配的要求。

同时，漫游联盟内部结构，可以是这些漫游联盟边缘的AAA服务器的网状互联，也可以有它内部的组网，可以组合使用网状/半网状、层状、星状等等多种网络的某一种，或者多种组合使用。需要说明，这里指的网络都是指AAA服务器直接的逻辑网络，不是指物理连接网络。

每当增加、删除、修改一个漫游客户的信息，例如域名和归属地AAA服务器信息，漫游联盟内部就要进行配置修改，使得漫游联盟内部所有和漫游客户相连的边缘AAA服务器都知道改动后的信息。根据漫游联盟内部组网结构不同，漫游联盟内部配置改动也不同。如果是网状/半网状网络，则需要每个相关的边缘AAA服务器都修改；如果是层状网络，则需要高层的AAA服务器修改；如果是星状网络，则需要中心节点AAA服务器修改。其他网络

也一样，原则就是能够保证修改后提供正确的AAA路径。

对漫游联盟的AAA网关进行配置以及实现在漫游联盟的AAA网关上进行协议适配的具体方法与两个运营商/企业之间的AAA网关之间的协议适配方法相同。

用户漫游接入流程基本如前所述，唯一不同的地方是用户通过“归属地”AAA服务器后到“漫游地”AAA服务器之间，还需要经过中间的各个实体的AAA网关，以及漫游联盟的AAA网关。

具体地说，就是以AAA网关为边界，中间实体一般是(漫游地AAA服务器→)本运营商AAA网络→本运营商AAA网关→漫游联盟→对端运营商AAA网关→对端运营商AAA网络(→归属地AAA服务器)。在每个中间实体上，都实现常规的Proxy功能，例如RADIUS Proxy功能。在漫游联盟的边缘AAA服务器上，需要做协议适配。适配过程与实施例2中所说明的相同，不再赘述。

漫游联盟的AAA服务器或者AAA网关逻辑上是独立于各运营商的，一般可以是一个独立组织提供的网络。但是，运营商之间也可以合作，将当前自己网络中的AAA服务器或AAA网关划出来作为漫游联盟的AAA服务器使用。此外，漫游联盟甚至可以不是独立的硬件，而仅仅由一个软件模块实现其功能。漫游联盟网关和运营商网关逻辑功能上是独立的，但是可以在同一个物理实体例如运营商网关上实现。

在该实施例 3 的用户漫游接入流程中，步骤（1）-（8）基本与前述实施例中的基本相同。不同之处在于，在步骤（9）中，如果漫游地 RADIUS 用户认证服务器根据用户名识别是一个漫游用户，并且其归属地服务器是属于另一个运营商的，那么就先将此认证报文转发到漫游地的 AAA 网关。再经过中间的各个实体。以 AAA 网关为边界，中间实体一般是(漫游地 AAA 服务器→)本运营商 AAA 网络→本运营商 AAA 网关→漫游联盟→对端运营商 AAA 网关→对端运营商 AAA 网络(→归属地 AAA 服务器)。在 AAA 网关中都使用标准的 Proxy 功能（典型的如公知的 RFC2865、RFC2866、RFC2869 的 RADIUS Proxy 功能），转发到归属地 AAA 网关上。归属地 AAA 网关也使用标准的Proxy功能将认证报文转发到归属地的RADIUS用户认证服务器上进行真正的认证。

在步骤（10）中，归属地RADIUS用户认证服务器根据用户信息判断用户是否合法，然后将认证成功/失败报文从归属地的AAA网关经过中间的各个实体的AAA网关，以及漫游联盟的AAA网关到漫游地RADIUS用户认证服务器。此后的过程同实施例1的步骤（11）至（13）。

用户计费过程如下:

14）认证如果成功，漫游地PPPoE服务器发起计费开始请求给漫游地RADIUS用户计费服务器。

15）漫游地RADIUS用户计费服务器发现用户是漫游用户，那么就如同上述步骤9）那样将此计费报文通过中间漫游转发装置（归属地的AAA网关经过中间的各个实体的AAA网关，以及漫游联盟的AAA网关）转发到归属地RADIUS用户计费服务器，进行真正的计费。

16）归属地RADIUS用户计费服务器回应计费开始应答报文，通过中间漫游转发装置（归属地的AAA网关经过中间的各个实体的AAA网关，以及漫游联盟的AAA网关归属地AAA网关和漫游地AAA网关）转发给漫游地RADIUS用户计费服务器。

17）漫游地RADIUS用户计费服务器将回应的计费开始应答报文转发给漫游地PPPoE服务器。

实施例4：接入设备和AAA服务器漫游接入

由于接入设备（例如接入服务器）接入的用户需要漫游时，都是通过接入设备上配置的域名知道用户连接到的归属地AAA服务器，或者相连的AAA网关等对应关系，但往往一个接入设备只能配置有限的域名关系，一般在几十个左右，典型的如32个，扩展性差，当需要配置漫游的域名时，肯定无法满足运营或者管理的需要。而且，漫游中每增加一个归属地，就要在全网所有的接入设备上增加新的漫游的域名，因此，维护量非常大。

在本发明的该实施例中，通过在接入设备上设置一个漫游域模块，使得除本接入设备核心的关系例如本地归属网络的AAA服务器等之外，其他漫游用户都走漫游域，使得所有漫游用户都接到对应的高层AAA服务器或者直接接到AAA网关，由它们再将漫游信息转发到归属地。

在漫游域模块中，所有本地认证的都会直接配置用户对应的AAA服务器

（认证、计费）；所有有特殊要求（例如某个接入企业要求配置企业的AAA服务器，而该AAA服务器不是本地认证用户，则需要特殊配置）的也会直接配置用户对应的AAA服务器（认证、计费）。

考虑到每个漫游域模块配置一次维护量太大，因此，设置一个“漫游域”配置项，在该配置项中，所有非本地、非特殊要求的用户，都走漫游域配置的AAA服务器进行认证和计费，这个AAA服务器可以是上述的AAA网关，或者任意一个可以找到用户归属地AAA服务器路径的AAA服务器。

在配置漫游域时，可以利用上面提到的“用户名@域名”中的所有域名信息，也可以是域名信息中的一部分。例如zhangsan@telecom.beijing.com，可以按照域名“telecom.beijing.com”就进行漫游配置处理，也可以按照域名“beijing.com”就进行漫游配置处理。配置方法与前述实施例中的相同。

通常，AAA服务器也可以设置漫游域模块，将所有漫游用户直接通过漫游域转到其他AAA服务器或者AAA网关上。其实现方法与接入设备提供漫游域的方法相同。

这样，接入服务器或者类似的接入设备、以及AAA服务器不需要配置所有的AAA服务器对应的关系，只要配置核心的关系和一个漫游关系。也就是说，在进行增加、修改、删除等网络漫游关系的改动时，只需要在某一个AAA网关或者漫游联盟上配置一次，由于所有接入设备和漫游地或者中间AAA服务器上都配置了漫游关系，因此，无需在所有设备和漫游地或者中间AAA服务器上修改，就可以马上使用。其扩展性好，可以做到漫游的零维护。

用户漫游接入流程基本同前例，只是在接入设备、AAA服务器漫游配置和控制上进行了优化。

其具体过程是，在经过上述实施例中步骤（1）至（7）后，在步骤（8）中，如果漫游地接入服务器（PPPoE 接入服务器）根据例如用户名识别出是漫游用户，则直接通过漫游域模块找到对应的 AAA 网关或者漫游联盟，或是找到归属地 AAA 服务器的路径，将此认证报文转发到漫游地的 AAA 网关。或者，当接入服务器中未设置漫游域模块而在 AAA 服务器（在本例中为RADIUS用户认证服务器）中设置了漫游域模块时，在步骤（9）中，RADIUS用户认证服务器根据用户名识别是一个漫游用户，则也可以通过其配置的漫游域模块找到对应的 AAA 网关或者漫游联盟，或是找到归属地 AAA 服务

器的路径，将此认证报文转发到漫游地的 AAA 网关。在 AAA 网关中使用标准的 Proxy 功能（典型的如公知的 RFC2865、RFC2866、RFC2869 的 RADIUS Proxy 功能），转发到归属地 AAA 网关上。归属地 AAA 网关也使用标准的 Proxy 功能将认证报文转发到归属地的 RADIUS 用户认证服务器上进行真正的认证。

在步骤（10）中，归属地RADIUS用户认证服务器根据用户信息判断用户是否合法，然后将认证成功/失败报文同样按照上述方法通过归属地RADIUS用户认证服务器中配置的漫游域模块找到对应的AAA网关或者漫游联盟，从而转发到漫游地RADIUS用户认证服务器。此后的过程同实施例1的步骤（11）至（13）。

用户计费过程如下:

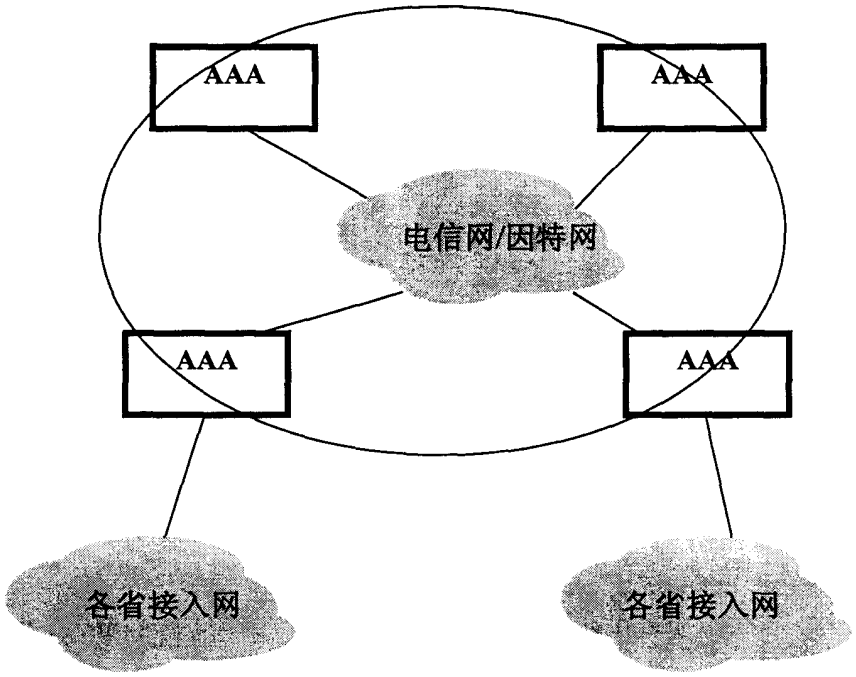
14）认证如果成功，PPPoE服务器发起计费开始请求给漫游地RADIUS用户计费服务器。

15）漫游地RADIUS用户计费服务器发现用户是漫游用户，那么就如同上述步骤9）那样将此计费报文通过漫游地RADIUS用户认证服务器中配置的漫游域模块找到对应的AAA网关或者漫游联盟，从而转发到归属地RADIUS用户计费服务器，进行真正的计费。

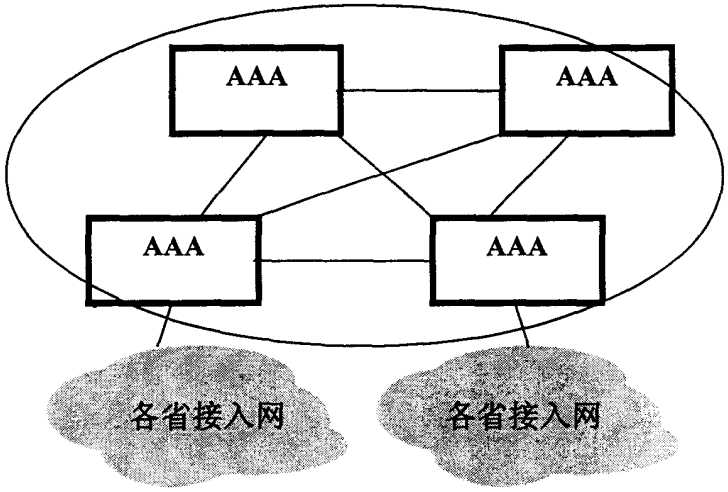
16）归属地RADIUS用户计费服务器回应计费开始应答报文，通过配置的漫游域模块找到对应的AAA网关或者漫游联盟，从而转发到漫游地RADIUS用户计费服务器。

17）漫游地RADIUS用户计费服务器将回应的计费开始应答报文转发给漫游地PPPoE服务器。

尽管上面结合多个实施例对本发明进行了说明，但是这些说明的目的只是为了便于对本发明有更为清楚和全面理解，而不是对本发明的限定。例如，在本发明的这些实施例中是以PPPoE认证方式为例来说明的，显然本发明也可用于除PPPoE以外的例如WEB认证、802.1X认证以及其它常规的网络用户认证方法。另外，本发明也不限于在说明书中提到的RADIUS、DIAMETER等协议为用户提供漫游服务。因此，对本发明实施例的各个细节显然可以进行各种修改和采用各种等同的替代手段，这些修改和等同替代仍属于本发明的范围。

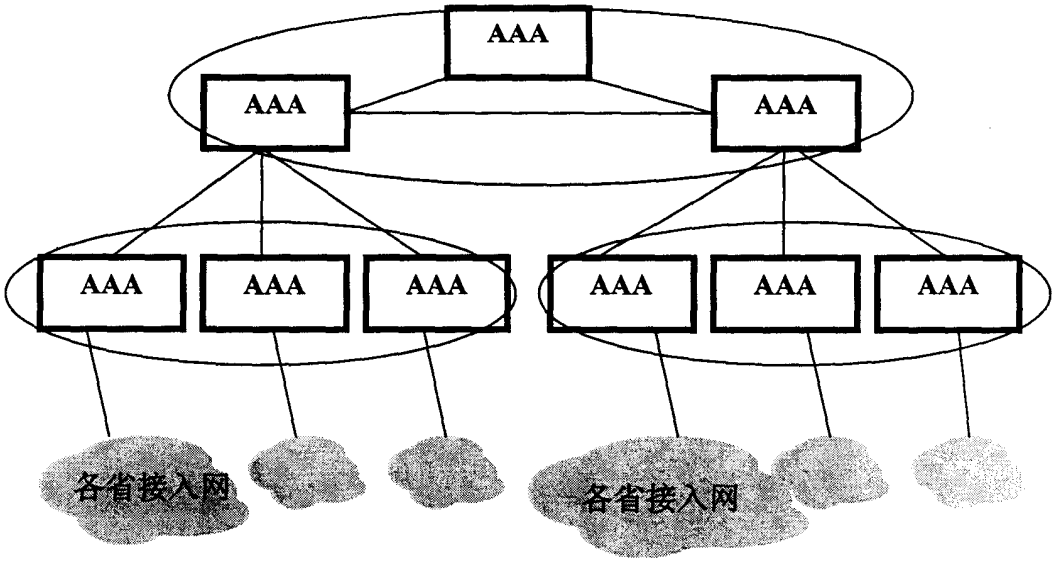

AAA
AAA
电信网/因特网
AAA
AAA
各省接入网
各省接入网

（a）

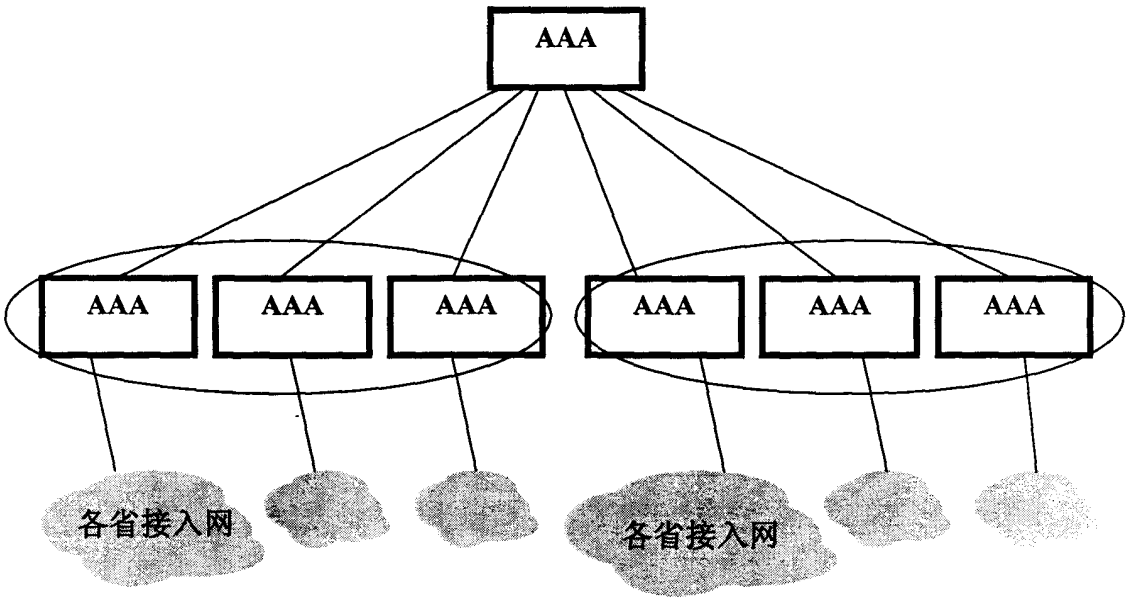

AAA
AAA
AAA
AAA
各省接入网
各省接入网

（b）

图 1


AAA
AAA
AAA
AAA
AAA
AAA
AAA
AAA
AAA
各省接入网
各省接入网

（a）


AAA
AAA
AAA
AAA
AAA
AAA
AAA
各省接入网
各省接入网

(b)

图 2

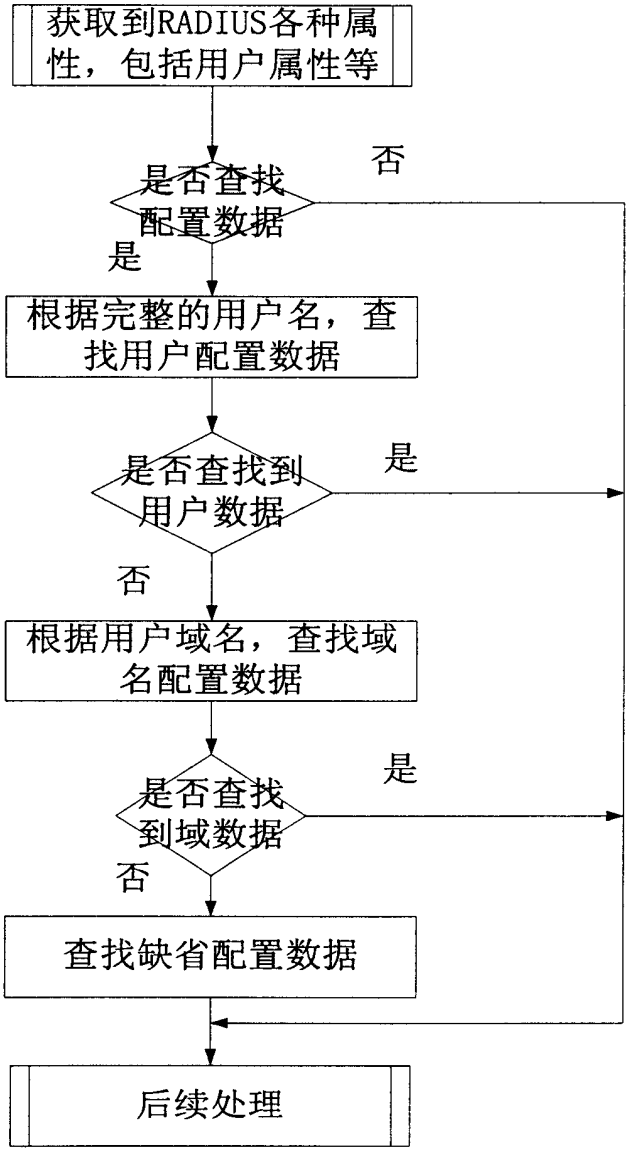

获取到RADIUS各种属性，包括用户属性等
是否查找配置数据
否
是
根据完整的用户名，查找用户配置数据
是否查找到用户数据
是
否
根据用户域名，查找域名配置数据
是否查找到域数据
是
否
查找缺省配置数据
后续处理

图 3

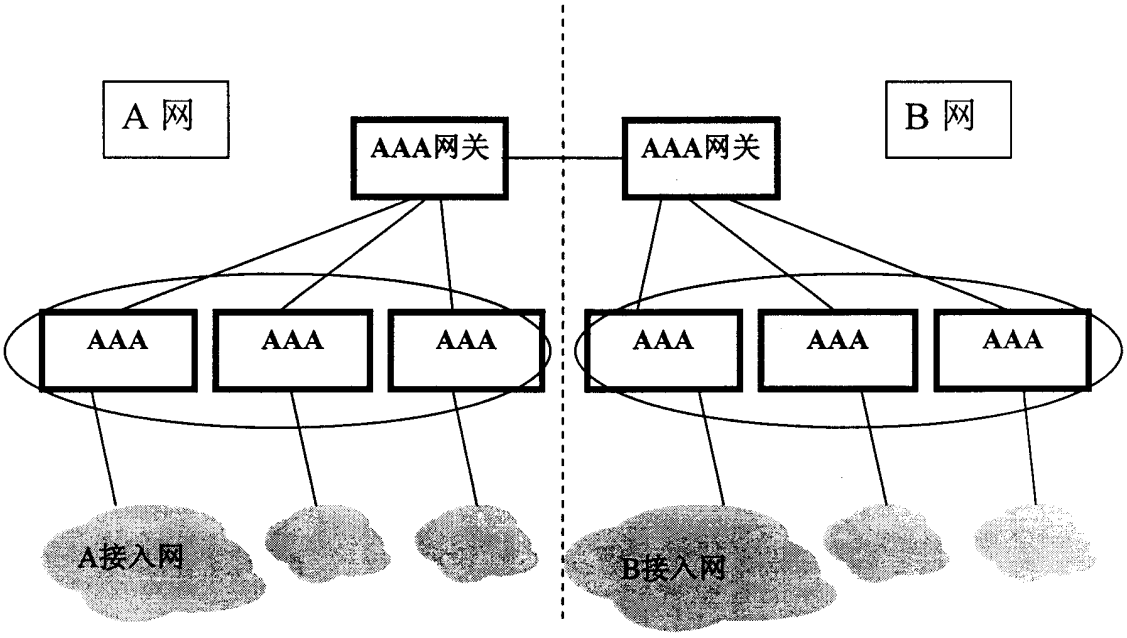

A 网
B 网
AAA网关
AAA网关
AAA
AAA
AAA
AAA
AAA
AAA
A接入网
B接入网

图 4

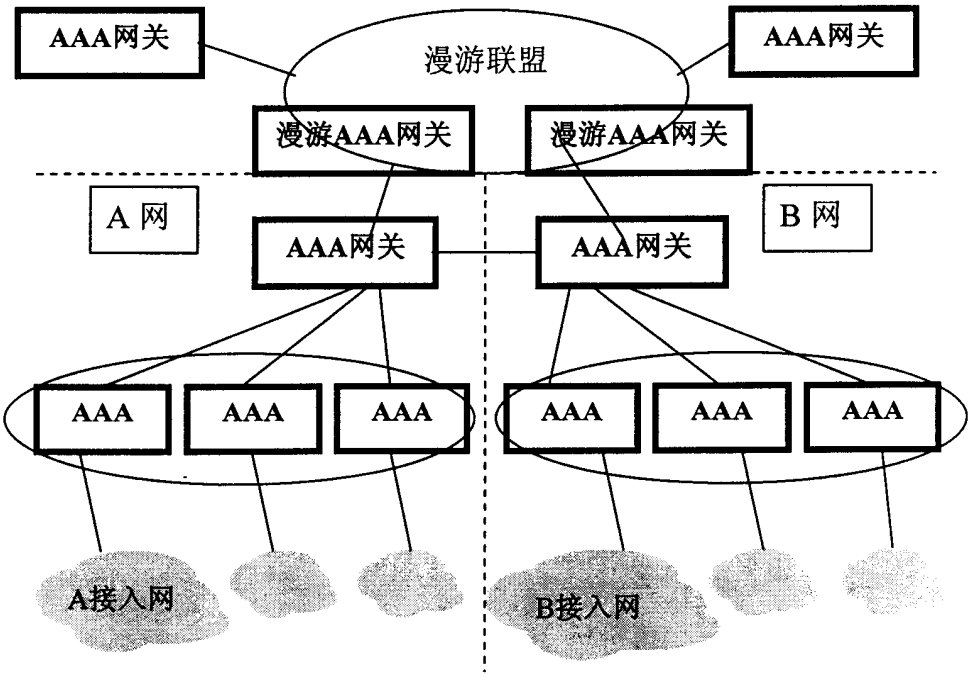

AAA网关
漫游联盟
AAA网关
漫游AAA网关
漫游AAA网关
A 网
B 网
AAA网关
AAA网关
AAA
AAA
AAA
AAA
AAA
AAA
A接入网
B接入网

图 5

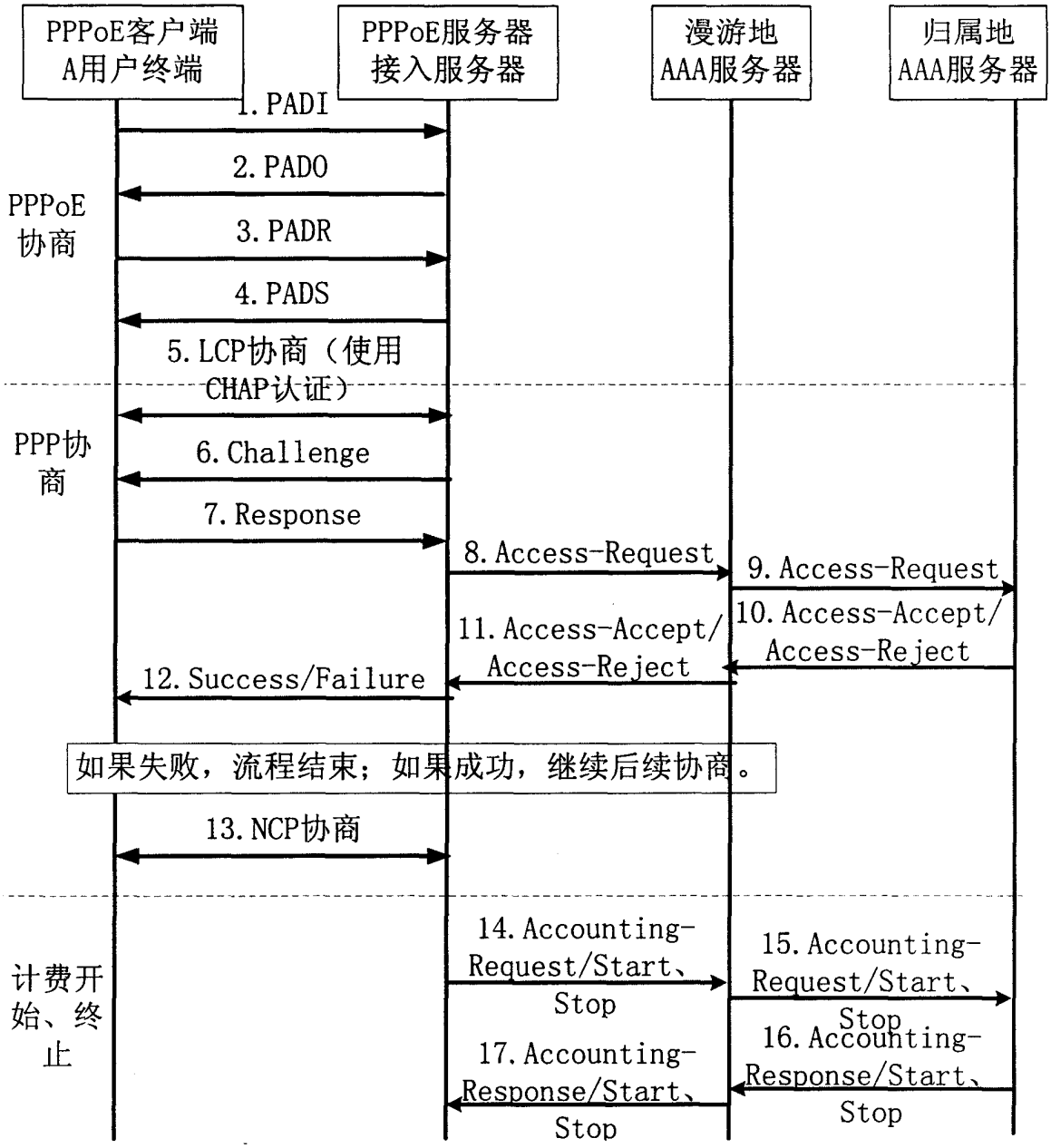
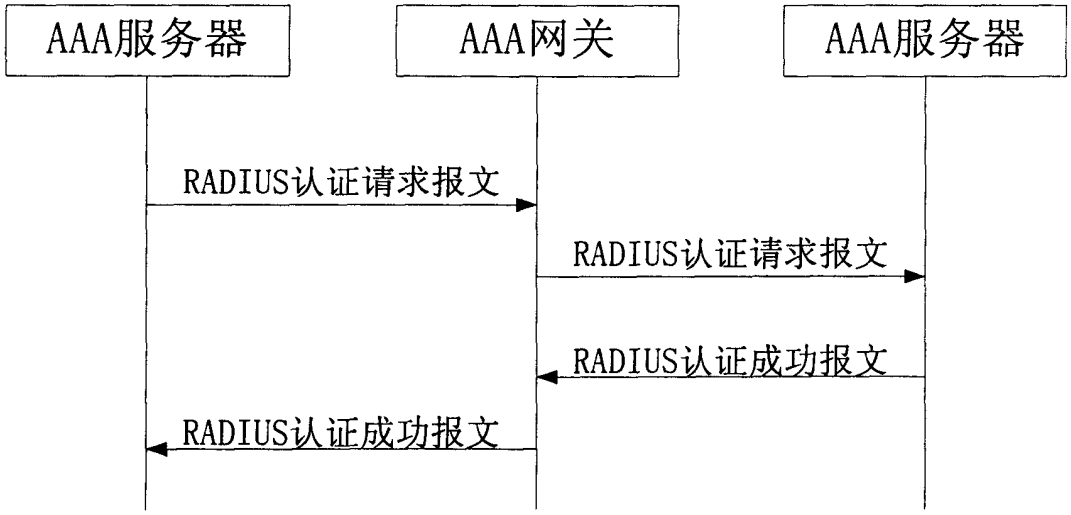
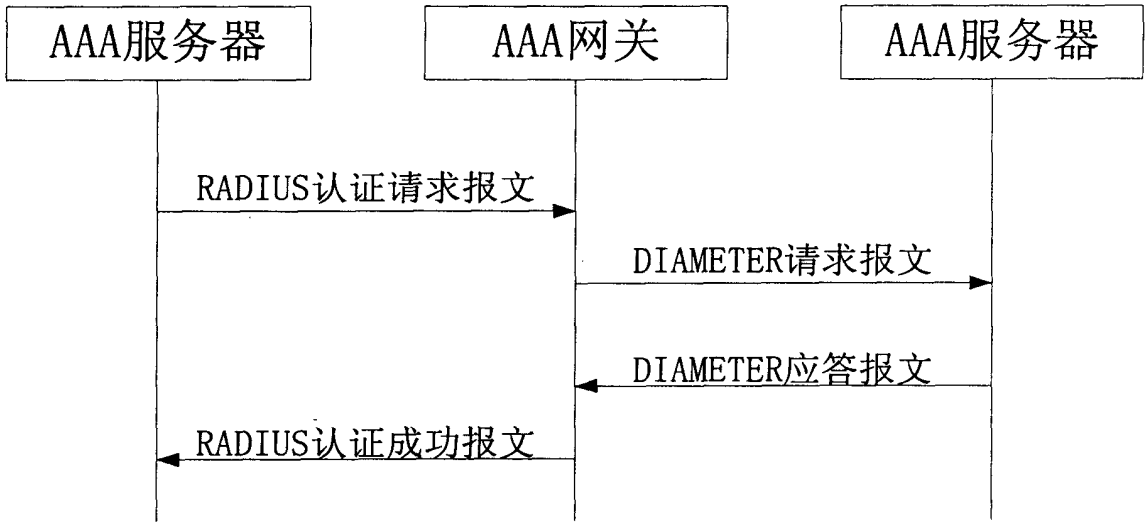

PPPoE客户端
A用户终端
PPPoE服务器
接入服务器
漫游地
AAA服务器
归属地
AAA服务器
1. PADI
2. PADO
PPPoE
协商
3. PADR
4. PADS
5. LCP协商（使用
CHAP认证）
PPP协
商
6. Challenge
7. Response
8. Access-Request
9. Access-Request
10. Access-Accept/
Access-Reject
11. Access-Accept/
Access-Reject
12. Success/Failure
如果失败，流程结束；如果成功，继续后续协商。
13. NCP协商
计费开
始、终
止
14. Accounting-
Request/Start、
Stop
15. Accounting-
Request/Start、
Stop
16. Accounting-
Response/Start、
Stop
17. Accounting-
Response/Start、
Stop

图 6


AAA服务器
AAA网关
AAA服务器
RADIUS认证请求报文
RADIUS认证请求报文
RADIUS认证成功报文
RADIUS认证成功报文

（a）


AAA服务器
AAA网关
AAA服务器
RADIUS认证请求报文
DIAMETER请求报文
DIAMETER应答报文
RADIUS认证成功报文

（b）

图 7