[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200610062834.0

[43] 公开日 2007 年 3 月 7 日

[11] 公开号 CN 1925394A

[22] 申请日 2006.9.25
[21] 申请号 200610062834.0
[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 张 科

[74] 专利代理机构 深圳中一专利商标事务所
代理人 欧阳启明

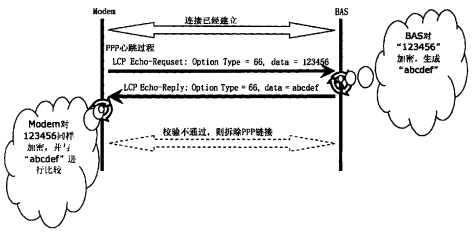
权利要求书 2 页 说明书 7 页 附图 2 页

[54] 发明名称

一种接入终端与运营商绑定的方法

[57] 摘要

本发明公开了一种接入终端与运营商绑定的方法，所述的方法包括如下步骤：a. 局端服务器 BAS 在接收到报文后采用约定的加密算法对其中的私有信息进行加密，然后通过响应报文将加密后的私有信息传送到接入终端；b. 所述的接入终端采用约定的加密算法对所述的私有信息进行加密，并将加密后的私有信息与所述的响应报文中携带的加密后的私有信息比较，如果两者不一致，则终止拨号流程或者拆除链路。 采用本发明的技术方案可以有效的防止用户利用运营商提供的接入终端接入到其他运营商的网络，避免运营商之间的恶性竞争，并且实现简单，不会改变用户习惯，对业务发放没有要求，而且不改变组网方式。



1、一种接入终端与运营商绑定的方法，其特征在于，所述的方法包括如下步骤:

a、局端服务器 BAS 在接收到报文后采用约定的加密算法对其中的私有信息进行加密，然后通过响应报文将加密后的私有信息传送到接入终端;

b、所述的接入终端采用约定的加密算法对所述的私有信息进行加密，并将加密后的私有信息与所述的响应报文中携带的加密后的私有信息比较，如果两者不一致，则终止拨号流程或者拆除链路。

2、根据权利要求 1 所述的方法，其特征在于，其中步骤 a 具体包括:

a1、所述的接入终端向所述的BAS发送链路控制协议LCP报文，所述的LCP报文中携带所述的私有信息;

a2、所述的BAS收到所述的LCP报文后采用约定的加密算法对其中的私有信息加密，然后通过LCP响应报文将加密后的私有信息发送到所述的接入终端。

3、根据权利要求2所述的方法，其特征在于，其中步骤b具体包括:

b1、所述的接入终端采用约定的加密算法对所述的私有信息进行加密;

b2、所述的接入终端将加密后的私有信息与从BAS收到的加密后的私有信息比较，如果两者不一致，则终止拨号流程或者拆除链路。

4、根据权利要求 1 所述的方法，其特征在于，其中步骤 a 具体包括:

a1、所述的接入终端截取客户端发送给所述的BAS的LCP报文，在所述的LCP报文中插入所述的私有信息后发送到所述的BAS;

a2、所述的BAS收到所述的LCP报文后采用约定的加密算法对其中的私有信息加密，然后通过LCP响应报文将加密后的私有信息发送到所述的接入终端。

5、根据权利要求4所述的方法，其特征在于，其中步骤b具体包括:

b1、所述的接入终端采用约定的加密算法对所述的私有信息进行加密;

b2、所述的接入终端将加密后的私有信息与从BAS收到的加密后的私有信息比较，如果两者不一致，则将所述的LCP响应报文丢弃。

6、根据权利要求5所述的方法，其特征在于，其中步骤b2之后还包括:

所述的客户端收不到所述的LCP响应报文，则终止拨号流程或者拆除链路。

7、根据权利要求2或者4所述的方法，其特征在于，所述的私有信息是通过LCP报文中的选项option携带的。

8、根据权利要求1或者2或者3或者4或者5所述的方法，其特征在于，所述的私有信息为LCP报文中随机生成的option的数据Data字符串。

9、根据权利要求2或者3或者4或者5所述的方法，其特征在于，所述的LCP报文为点到点协议PPP心跳报文。

10、根据权利要求 1 所述的方法，其特征在于，所述的接入终端为远程测控单元 RTU 或者家庭网关 HGW。

一种接入终端与运营商绑定的方法

技术领域

本发明涉及xDSL（数字用户线）技术领域，具体来说，涉及到ADSL中接入终端与运营商绑定的技术。

背景技术

PPP（Point-to-Point Protocol 点到点协议）协议中提供了一整套方案来解决链路建立、维护、拆除、上层协议协商、认证等问题。PPP协议包含这样几个部分：链路控制协议LCP（Link Control Protocol）、网络控制协议NCP（Network Control Protocol）和认证协议，最常用的包括口令验证协议PAP（Password Authentication Protocol）和挑战握手验证协议CHAP（Challenge-Handshake Authentication Protocol）。

一个典型的链路建立过程分为三个阶段：创建阶段、认证阶段和网络协商阶段。

LCP负责创建链路，在这个阶段，将对基本的通讯方式进行选择。链路两端设备通过LCP向对方发送配置信息报文（Configure Packets）。一旦一个配置成功信息包（Configure-Ack packet）被发送且被接收，就完成了交换，进入了LCP开启状态。

在认证阶段，客户端会将自己的身份发送给远端的接入服务器。该阶段使用一种安全验证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。在认证完成之前，禁止从认证阶段前进到网络层协议阶段。如果认证失败，认证者应该跃迁到链路终止阶段。

最常用的认证协议有口令验证协议(PAP)和挑战握手验证协议(CHAP)。PAP是一种简单的明文验证方式，NAS（网络接入服务器，Network Access Server）要求用户提供用户名和口令，PAP以明文方式返回用户信息。CHAP是一种加密的验证方式，能够避免建立连接时传送用户的真实密码，NAS向远程用户发送一个挑战口令（challenge），其中包括会话ID和一个任意生成的挑战字串（arbitrary challenge string），远程客户必须使用MD5单向哈希算法（one-way hashing algorithm）返回用户名和加密的挑战口令，会话ID以及用户口令，其中用户名以非哈希方式发送。

认证阶段完成之后，PPP将调用在链路创建阶段选定的各种网络控制协议（NCP）。选定的NCP解决PPP链路之上的高层协议问题，例如，在该阶段IP控制协议（IPCP）可以向拨入用户分配动态地址。

PPP协议是目前广域网上应用最广泛的协议之一，它的优点在于简单、具备用户验证能力、可以解决IP分配等。

家庭拨号上网就是通过PPP在用户端和运营商的接入服务器之间建立通信链路。在宽带接入技术日新月异的今天，PPP也衍生出新的应用，典型的应用是在ADSL（非对称数据用户环线，Asymmetrical Digital Subscriber Loop）接入方式当中，PPP与其他的协议共同派生出了符合宽带接入要求的新的协议，如PPPoE(PPP over Ethernet 基于以太网的PPP)、PPPoA(PPP over ATM 基于异步传输的PPP)。

利用以太网（Ethernet）资源，在以太网上运行PPP来进行用户认证接入的方式称为PPPoE。PPPoE即保护了用户方的以太网资源，又完成了xDSL的接入要求，是目前xDSL接入方式中应用最广泛的技术标准。

现有的通信技术中，xDSL（数字用户线）已经是家庭和小企业宽带接入的主流。数字用户线技术是一种通过电话双绞线，即无屏蔽双绞线（Unshielded Twist Pair，UTP）进行数据传输的高速传输技术，包括非对称数字用户线（Asymmetrical Digital Subscriber Line，ADSL），甚高速数字用

户线（Very-high-bit-rate Digital Subscriber Line，VDSL）、基于综合业务数字网（Integrated Services Digital Network，ISDN）的数字用户线（ISDN Digital Subscriber Line，IDSL）和单线对高速数字用户线（Single-pair High-bit-rate Digital Subscriber Line，SHDSL）等。

目前xDSL接入最普遍的方式是采用PPPoE拨号方式登录运营商网络。在PPPoE方式下，接入终端一般有两种工作模式：路由模式（route）和桥接模式（bridge）。

路由模式下，PPPoE拨号由Modem发起，Modem获得公网IP地址，对下分配私网IP地址给PC等家庭网络内部设备，Modem提供路由转发服务。

桥接模式下，PPPoE拨号由PC或者家庭内部路由器发起，拨号发起者获取IP地址，Modem只提供数据通路，不对数据作转发和其它处理。

此处的Modem指的是xDSL接入方式的接入终端RTU（远程测控单元）、HGW（家庭网关）等。

目前运营商发展xDSL用户的时候，很多都采用开通业务赠送接入终端的方式。但由于运营商之间的竞争关系，某些运营商可能会采用“带猫入网”的优惠方式（用户可以自带接入终端入网），从其它运营手上抢夺用户资源，这样用户将有可能接受某一运营商赠送的接入终端，以“带猫入网”的方式接入另一运营商的网络，从而造成运营商之间的恶性竞争。

从运营商的角度来说，尤其是对于那些免费赠送接入终端的运营商来说，希望有一种合理的方式将其终端和接入网绑定，从技术上限制用户将接入终端用于其它运营商的网络，以维护自身的利益，但现有技术中对此问题尚未有理想的解决方案。

发明内容

本发明的目的在于提供一种接入终端和运营商绑定的方法，以解决将接

入终端与提供该接入终端的运营商绑定的问题。

为实现上述目的，本发明采用的技术方案如下：

一种接入终端与运营商绑定的方法，所述的方法包括如下步骤：

a、局端服务器 BAS 在接收到报文后采用约定的加密算法对其中的私有信息进行加密，然后通过响应报文将加密后的私有信息传送到接入终端；

b、所述的接入终端采用约定的加密算法对所述的私有信息进行加密，并将加密后的私有信息与所述的响应报文中携带的加密后的私有信息比较，如果两者不一致，则终止拨号流程或者拆除链路。

其中步骤 a 具体包括：

a1、所述的接入终端向所述的BAS发送链路控制协议LCP报文，所述的LCP报文中携带所述的私有信息；

a2、所述的BAS收到所述的LCP报文后采用约定的加密算法对其中的私有信息加密，然后通过LCP响应报文将加密后的私有信息发送到所述的接入终端。

其中步骤b具体包括：

b1、所述的接入终端采用约定的加密算法对所述的私有信息进行加密；

b2、所述的接入终端将加密后的私有信息与从BAS收到的加密后的私有信息比较，如果两者不一致，则终止拨号流程或者拆除链路。

其中步骤 a 具体包括：

a1、所述的接入终端截取客户端发送给所述的BAS的LCP报文，在所述的LCP报文中插入所述的私有信息后发送到所述的BAS；

a2、所述的BAS收到所述的LCP报文后采用约定的加密算法对其中的私有信息加密，然后通过LCP响应报文将加密后的私有信息发送到所述的接入终端。

其中步骤b具体包括：

b1、所述的接入终端采用约定的加密算法对所述的私有信息进行加密;

b2、所述的接入终端将加密后的私有信息与从BAS收到的加密后的私有信息比较，如果两者不一致，则将所述的LCP响应报文丢弃。

其中步骤b2之后还包括:

所述的客户端收不到所述的LCP响应报文，则终止拨号流程或者拆除链路。

所述的私有信息是通过LCP报文中的选项option携带的。

所述的私有信息为LCP报文中随机生成的option的数据Data字符串。

所述的报文为点到点协议PPP心跳报文。

所述的接入终端为远程测控单元 RTU 或者家庭网关 HGW。

本发明克服现有技术的不足，在 Modem 与 BAS 交互的过程中，BAS 接收到 Modem 发送的报文后对其中的私有信息按照约定的算法进行加密，然后将加密后的私有信息通过 LCP 响应报文返回给 Modem，Modem 采用约定的算法对原私有信息进行加密，并且将加密后的私有信息和从 BAS 返回的加密私有信息进行比较，如果两者不一致，则终止 PPPoE 拨号过程或者拆除已经建立的链路。采用本发明的技术方案可以有效的防止用户利用运营商提供的接入终端接入到其他运营商的网络，避免运营商之间的恶性竞争，并且实现简单，不会改变用户习惯，对业务发放没有要求，而且不改变组网方式。

附图说明

图 1 为本发明实施例一流程图;

图 2 为本发明实施例二流程图;

具体实施方式

本发明的基本原理是在Modem与BAS交互的过程中，BAS接收到Modem

发送报文后对其中的私有信息按照约定的算法进行加密，然后将加密后的私有信息通过LCP响应报文返回给Modem，Modem采用约定的加密算法对原私有信息进行加密，并且将加密后的私有信息和从BAS返回的加密私有信息进行比较，如果两者不一致，则终止PPPoE拨号过程或者拆除已经建立的链路。

首先，需要在LCP协议中扩展一个自定义option（选项）项，用来在LCP报文中携带私有信息，在PPP的两端必须都能识别此参数。

如下表所示，在LCP Option中扩展一个私有Type（类型）（譬如0x66）参数用于进行BAS身份校验，Data字段定义为字符串。在LCP协商过程中，或者在LCP心跳报文中，由Modem生成一串随机字符，通过扩展参数将其发向BAS，BAS通过特定算法对其进行加密（譬如使用用户名作密钥对该随机字符加密），并通过此私有参数将其加密后字符串返回给Modem，Modem使用约定的加密算法加密随机字符后将加密结果与从BAS收到的加密后的随机字符比较，如果两者相同，则说明Modem与BAS采用的加密算法相同，Modem为接入网运营商提供，如果两者不一致则说明Modem与BAS采用的加密算法不相同，Modem不是该接入网运营商提供，则断开PPP连接。

Type	Length	Data
66	xxx	字符串

以下结合附图和具体实施例进行详细说明。

实施例一：路由模式下通过私有信息识别接入网

路由模式下，PPPoE拨号由Modem发起。Modem将自定义option添加到LCP报文中，随机生成Data字符串，BAS对Data字段加密处理后，通过响应报文发回Modem，Modem采用与约定的加密算法对Data字段进行加密，然后由Modem将加密后的Data字段与从BAS收到的Data字段比较，如果两者不一致，则将链路拆除。

以下以PPP心跳报文为例说明此过程，流程如图1所示。

1、连接建立后，Modem向BAS发送心跳报文，其中携带自定义的option，option TYPE = 66，随机生成的Data = 123456;

2、BAS对123456 加密，生成abcdef;

3、BAS返回心跳应答报文，其中携带自定义的option，option TYPE = 66，Data = abcdef;

4、Modem采用与BAS约定的加密算法对123456加密，判断加密后的结果是否为abcdef，如果不是，转步骤5;

5、将链路拆除。

实施例二：桥接模式下通过私有信息识别接入网

桥接模式下，PPPoE拨号过程由PC发起，在桥接处理流程中加入PPP的检测点，截获并解析PPP报文。如果是上行数据，由Modem在原报文中插入扩展参数，发给BAS进行认证。如果是下行数据，先由Modem进行校验，进而剥掉扩展参数并将其发向PC。

同样以心跳报文为例说明，其流程如图2所示：

1、PC向BAS发送心跳报文，Modem检测到是PPP报文则截取并对其进行解析，在心跳报文中插入自定义的option，option TYPE = 66，随机生成的Data = 123456，然后将其转发到BAS;

2、BAS对123456 加密，生成abcdef;

3、BAS返回心跳响应报文，其中携带自定义的option，option TYPE = 66，Data = abcdef;

4、Modem截取心跳响应报文，提取其中的Data字符串，同时采用约定的加密算法对123456进行加密，判断加密后的结果是否为abcdef，如果不是，转步骤5;

5、Modem将心跳响应报文丢弃;

6、PC收不到心跳响应报文，自动拆链。

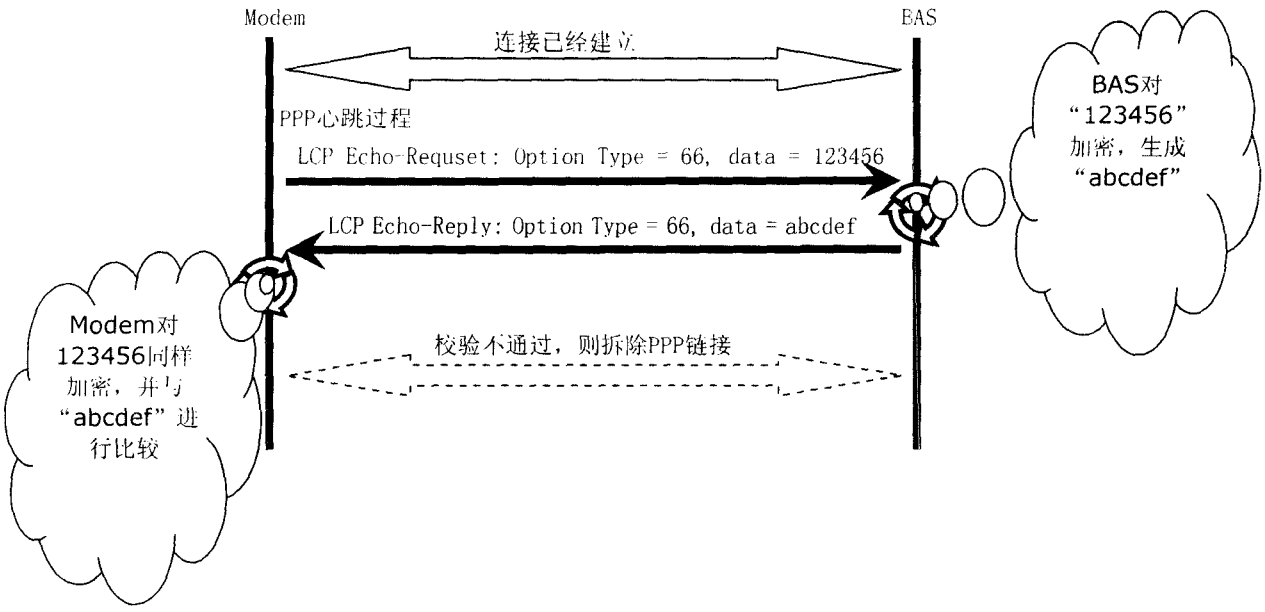

Modem
BAS
连接已经建立
PPP心跳过程
LCP Echo-Requset: Option Type = 66, data = 123456
LCP Echo-Reply: Option Type = 66, data = abcdef
校验不通过，则拆除PPP链接
BAS对“123456”加密，生成“abcdef”
Modem对123456同样加密，并与“abcdef”进行比较

图 1

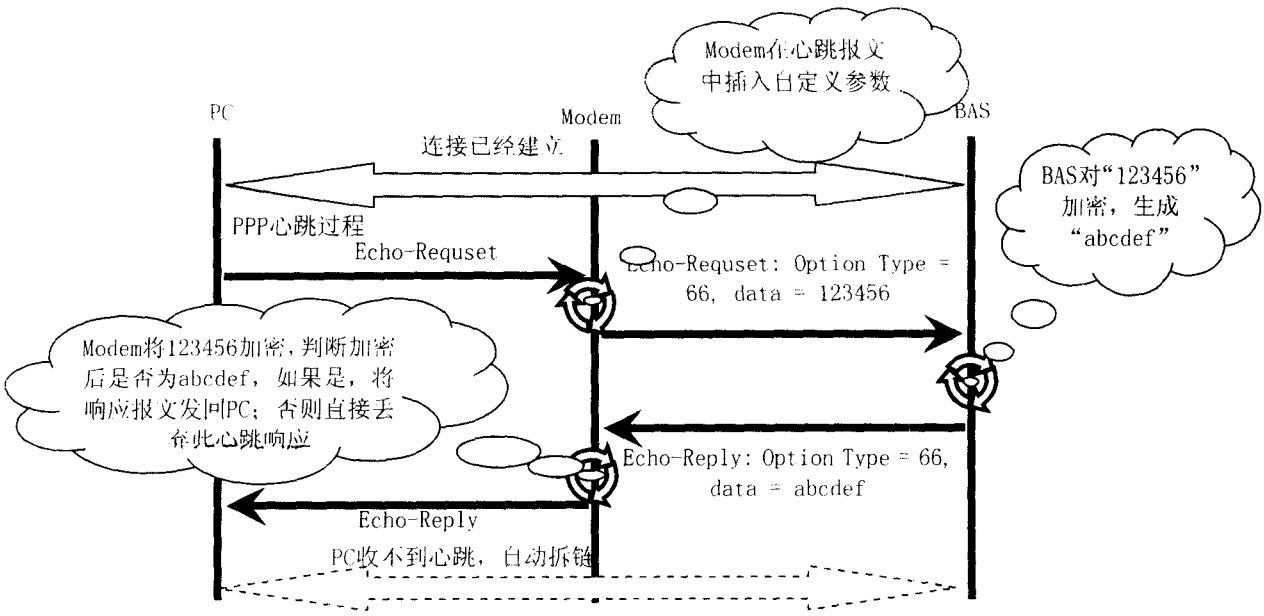

Modem在心跳报文
中插入自定义参数
PC
Modem
BAS
连接已经建立
BAS对“123456”
加密，生成
“abcdef”
PPP心跳过程
Echo-Requset
Echo-Requset: Option Type =
66, data = 123456
Modem将123456加密，判断加密
后是否为abcdef，如果是，将
响应报文发回PC；否则直接丢
弃此心跳响应
Echo-Reply: Option Type = 66,
data = abcdef
Echo-Reply
PC收不到心跳，自动拆链

图 2