

[19] 中华人民共和国国家知识产权局

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



[12] 发明专利说明书

专利号 ZL 200410007041.X

[45] 授权公告日 2008 年 2 月 6 日

[11] 授权公告号 CN 100367699C

[22] 申请日 2004.2.26

[21] 申请号 200410007041.X

[30] 优先权

[32] 2003.3.10 [33] KR [31] 2003-14845

[73] 专利权人 三星电子株式会社

地址 韩国京畿道

[72] 发明人 金洙亨 金荣锡 吴润济

[56] 参考文献

CN1170995A 1998.1.21

JP2002-232342A 2002.8.16

审查员 刘剑波

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 戎志敏

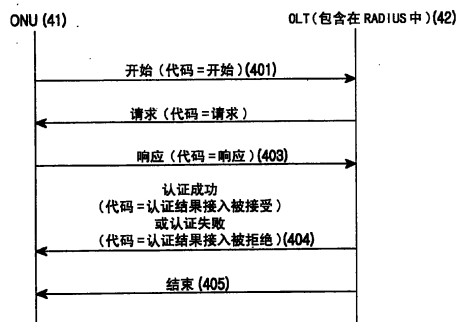
权利要求书 3 页 说明书 8 页 附图 5 页

[54] 发明名称

在以太无源光网络中的认证方法和装置

[57] 摘要

基于在 IEEE (电气和电子工程师学会) 802 中讨论的、同时以 IEEE 802.3 和 802.1d 为中心进行标准化的链接安全性方法, 提供一种认证方法, 能够使得 OLT 实现认证 ONU 的一个 RADIUS 服务器的功能。根据在 OLT 和 ONU 之间的使用, 简化适于在 OLT 和 RADIUS 服务器之间使用的 MD-5 算法, 使得其可被用在一个 EPON 结构中。记录有程序的一种计算机可读记录介质实现该认证方法。该认证方法包括把一个开始代码从光网络单元 (ONU) 发送到一个光线路终端 (OLT) 的步骤。该 ONU 在响应中接收针对该 ONU 的一个识别符的请求。从包括该标识符的该 ONU 的响应, 该 OLT 确定该认证是否成功或失败, 并且把分别的信息发送到该 ONU, 并且发送通知该 ONU 该认证处理已经结束的一个附加信息。



1. 在一个以太无源光网络中的一种认证方法，包括步骤：

(A) 使得一个光线路终端OLT从一个光网络单元ONU接收一个通知认证处理的开始的数据包，并且在接收到所述数据包之后，控制该OLT，以便把用于请求该ONU标识符的一个数据包发送到该ONU；

(B) 使得该OLT从ONU接收该识别符，并且把该标识符与先前的存储值比较，以便确定该标识符是否对应于该先前的存储值；

(C) 当在该步骤(B)确定有该对应关系时，则发送一个认证成功数据包到该ONU；

(D) 当在该步骤(B)确定不存在该对应关系时，则发送一个认证失败数据包到该ONU；并且

(E) 在完成步骤(C)或(D)之后，控制该OLT来通知该ONU已经结束一个认证处理，其中

使用在所述认证方法中的数据包的每一个都包括：

用于指示该数据包的目的地的目的地址(DA)字段；

用于指示该数据包的来源的信源地址(SA)字段；

用于指示一个LLID的逻辑连接标识符(LLID)字段；

用于指示数据包的传播类型的类型字段；

用于在其类型字段与其它数据包的类型字段完全相同时标识该数据包的子类型字段；

用于指示该数据包的版本信息的版本字段；

用于指示根据该数据包的一个认证操作的代码字段；

用于指示该数据包的数据的数据/协议数据单元(PDU)字段；以及

用于指示FCS信息的帧校验序列FCS字段，该FCS信息用于检测对应于该数据包的包括在将要以帧单元发送的信息中的一个帧的误差，该FCS信息被放置在该帧的末端。

2. 根据权利要求1的认证方法，其中，所述ONU的标识符是一个用户名。

3. 根据权利要求1的认证方法, 其中, 所述代码字段包括:

一个值“0x00”, 用于指示一个认证处理的开始;

一个值“0x01”, 用于指示对于认证内容的一个请求;

一个值“0x02”, 用于指示对于认证内容的发送;

一个值“0x03”, 用于指示一个认证处理的结束;

一个值“0x04”, 用于指示认证成功; 以及

一个值“0x05”, 用于指示认证失败。

4. 在一个以太网无源光网络中的一种认证方法, 包括步骤:

(A) 控制一个光网络单元ONU把通知一个认证处理的开始的数据包发送到一个光线路终端OLT, 并且使得该ONU从该OLT接收用于请求该ONU的一个标识符的数据包;

(B) 控制该ONU把该ONU的标识符发送到该OLT;

(C) 当确定在该标识符和先前存储在该OLT中的一个值之间存在对应关系时, OLT向ONU发送一个认证成功数据包, 并且根据该确定而以该ONU进行处理过程;

(D) 当确定不存在该对应关系时, 响应该认证失败数据包的发送而以ONU接收一个认证成功数据包, 并且根据该对应关系不存在的确定而以该ONU进行处理过程; 以及

(E)使得该ONU从该OLT接收通知一个认证处理已经结束的数据包, 该通知数据包被作为步骤(C)或(D)的确定的结果而发送, 其中

用在该认证方法中的数据包的每一个都包括:

用于指示该数据包的目的地的目的地址(DA)字段;

用于指示该数据包的来源的信源地址(SA)字段;

用于指示一个LLID的逻辑连接标识符(LLID)字段;

用于指示数据包的传播类型的类型字段;

用于在其类型字段与其它数据包的类型字段完全相同时标识该数据包的子类型字段;

用于指示该数据包的版本信息的版本字段;

用于指示根据该数据包的一个认证操作的代码字段;

用于指示该数据包的数据的数据/协议数据单元(PDU)字段; 以及

用于指示FCS信息的帧校验序列FCS字段，该FCS信息用于检测对应于该数据包的包括在将以帧单元发送的信息中的一个帧的误差，该FCS信息被放置在该帧的末端。

5. 根据权利要求4的认证方法，其中，所述ONU的标识符是一个用户名。

6. 根据权利要求4的认证方法，其中该代码字段包括：

一个值“0x00”，用于指示一个认证处理的开始；

一个值“0x01”，用于指示对于认证内容的一个请求；

一个值“0x02”，用于指示对于认证内容的发送；

一个值“0x03”，用于指示一个认证处理的结束；

一个值“0x04”，用于指示认证成功；以及

一个值“0x05”，用于指示认证失败。

在以太无源光网络中的认证方法和装置

技术领域

本发明涉及IEEE(电气和电子工程师学会)802中讨论的链接安全性,是以IEEE 802.3和802.1d为中心的标准化进程。这种链接安全性可以通过基于IEEE 802.1x(基于端口的网络接入控制)的认证方法或基于IEEE 802.10的SDE(安全数据交换)结构来实现。具体地说,本发明实现一种基于802.1x的简单而有效的认证方法,适用于EPON(以太无源光网络)结构中的认证。

背景技术

IEEE 802.1x既支持在每一终端和桥接LAN设备,即EAPOL(LAN上的EAP(可扩展认证协议))之间的认证,又支持在桥接LAN设备和RADIUS(远距认证拨入用户服务)服务器,即RFC 2869中描述的在RADIUS上的EAP之间的一种协议。

为了实现在现存网络结构中的认证,应该安装一个外部RADIUS服务器。在无线LAN中,由IEEE 802.1x建议的认证协议被用于实现针对用户的认证。该认证协议包括PAP(口令认证协议)、CHAP(查询信号交换认证协议)、EAP(扩展认证协议)等。在认证中使用MD-5(信息提要-5)算法来提供用于加密一个PDU(协议数据单元)的散列函数。具体地说,是在认证码和RADIUS服务器之间执行针对在RADIUS帧中的口令的加密处理。

图1是说明在使用MD-5查询一个传统EAP认证方法的实例中的信号流程示意图。用于一般EAP认证的系统包括一台作为客户机的PC(个人计算机)11、提供认证服务的认证服务器13和用于网络接入的NAS(网络接入服务器)12。

操作中,首先在PC 11和NAS 12之间确定的一个认证协议(101)。在此过程中,NAS 12仅执行对该认证服务器13的中继操作。NAS 12还基于在

认证服务器13和PC 11之间建立的认证而用于允许一个端口的使用。随后，PC 11使用一个用户名尝试对该认证服务器13的EAP认证(102)。

响应该认证尝试，该认证服务器13把包括用于一个散列函数的查询值的MD-5查询发送至该PC 11(103)。然后该PC 11则把包含一个散列值的MD-5发送至该认证服务器13 (104)。如果该发送的MD-5响应是正确的，则确定已经建立了成功认证。在此情况中，该认证服务器13发送一个认证成功信息(105)。随后该认证服务器13与一个目的地址连接。另一方面，如果从PC 11发送到认证服务器13的MD-5不正确，则确定该认证失败。在此情况中，该认证服务器13发送一个认证失败信息(105)，并且拒绝PC 11的接入。

图2是说明在上述EAP认证处理过程中使用CHAP的传统信号流程的示意图。“CHAP”也称作“MD-5 CHAP”，使用基于MD-5的单向表，通过加密响应来提供针对未授权接入的高级安全性。当PC 21，即一个接入客户机使用用户名登录到RADIUS服务器22时(201)，该RADIUS服务器22向PC 21发送一个包括对话ID和可选择查询字符串的CHAP查询(202)。PC 21随即RADIUS服务器22发送一个包含用户名、由可选密码单向加密的查询字符串、对话ID和密码的CHAP响应信息(203)。RADIUS服务器22核查该CHAP响应信息，如果该CHAP响应信息有效(204)则发送CHAP成功信息(204)，从而实现该PC 21的接入。

图3是说明一个通常EAPOL帧格式的一个实例的示意图，包括目的地址(DA) 301、信源地址(SA) 302、传播类型(E类型)303、版本304、分组类型305、数据包主体长度306和数据包主体307。E类型303表示使用“0x88-8e”的帧结构。但是，这样一个传播类型“0x88-8e”被使用在现存的无线LAN中，所以应该使用“0x88-8e”之外的传播类型，以便避免混淆。

EPON是IEEE 802标准化协会现行实行的生效的标准，与传统的点对点以太网相比，其操作在以点对多点类型的光通信网络中，因此与点对点类型网络相比其具备经济上的优势。正在进行中的有效研究针对的是称为“MPCP(多点控制协议)”的一个集中MAC(媒体接入控制)协议，以及用于模拟在EPON上点对点传递的一个方案。

但是, 尽管IEEE 802.1x期望借助指定在端口单元中的控制操作的优势来提供用于标准认证的一个基础指导, 但是由于目前没有定义用于认证目标端点的标准, 因而在上述EPON中存在安全性的问题。因此需要设计在EPON结构中可用的一个认证协议。

但是在此连接方式中, 图1和图2示出的传统认证方法都具有各种问题。首先, 在使用现存RADIUS服务器来实现光网络单元(ONU)的认证の場合, 即使在小的ONU数量时, 由于为了一个期望的认证应该附加地构成一个外部服务器, 因而其带来了运营成本的增加和操作无效率。其次, 其难以在ONU(光网络单元)和OLT(光线路终端)之间使用一个EAP。在现存的以太网类型以重叠方式用于ONUの場合, 存在的问题是, 由于不同以太网类型是完全相同的, 因而其不可能把用于无线LAN和用于EPON的以太网类型彼此区别开。因此需要使用不同于现存以太网类型的一个新传播类型的帧结构, 即需要能够容易实现的一个新的格式。

第三, 必须修改或简化用于该ONU和OLT的认证协议。

第四, 基于传统的IEEE 802.1x的结构不能被用于使用针对端口控制的逻辑链接ID(LLID)的EPON结构, 因为它们是工作在基于桥接器端口控制功能的基础上。

发明内容

为解决这些问题, 本发明在一个方案中提供一种认证方法, 使得OLT实现RADIUS服务器认证ONU的功能。本方法简化适于使用在OLT和RADIUS服务器之间的MD-5算法, 适于在一个EPON结构中的OLT和ONU之间使用。而且, 提供了实现该认证方法的记录有一个程序的计算机可读记录介质。

在本发明的另一方案中, 与使用MAC地址实现端口控制的传统结构相比, 使得端口的控制能够使用一个口令和一个LLID变换表。

在一个方案中, 本发明提供了在一个以太无源光网络(EPON)中的一种认证方法, 包括步骤: (A) 使得一个光线路终端(OLT)从一个光网络单元(ONU)接收一个通知认证处理的开始的数据包, 并且响应该接收控制该OLT, 以便把用于请求该ONU标识符的一个数据包发送到该ONU; (B) 使

得该OLT从ONU接收该识别符,并且把该标识符与先前的存储值比较,以便确定该标识符是否对应于该先前的存储值;(C) 当确定存在该对应关系时,则发送一个认证成功数据包到该ONU;(D) 当确定不存在该对应关系时,则发送一个认证失败数据包到该ONU;以及 (E) 在完成步骤(C)或(D)之后,控制该OLT来通知该ONU已经结束一个认证处理。

在另一个方案中,本发明提供了在一个以太无源光网络(EPON)中的一种认证方法,包括步骤:(A) 控制一个光网络单元(ONU)把通知一个认证处理的开始的数据包发送到一个光线路终端(OLT),并且使得该ONU从该OLT接收用于请求该ONU的一个标识符的数据包;(B) 控制该ONU把该ONU的标识符发送到该OLT;(C) 当确定在该识别符和先前存储在OLT中的一个值之间存在对应关系时,响应该认证成功数据包的发送而以ONU接收一个认证成功数据包,并且根据该确定而以该ONU进行处理过程;(D) 当确定不存在该对应关系时,响应该认证失败数据包的发送而以ONU接收一个认证成功数据包,并且根据该对应关系不存在的确定而以该ONU进行处理过程;以及 (E)使得该ONU从该OLT接收通知一个认证处理已经结束的数据包,该通知数据包被作为步骤(C)或(D)的所说确定的结果而发送。

在另一个方案中,本发明提供了在一个以太无源光网络(EPON)中的一种认证装置,包括:一个总线接口,用于从外部路由器输入数据并且把数据输出到外部路由器;一个控制单元,用于根据一个认证处理接收一个OAM(操作、管理和维护)数据包,并且控制用于一个光网络单元(ONU)的数据服务;以及一个下游单元,用于在控制单元的控制之下交换通过该总线接口接收的数据。

附图说明

通过参照附图的最佳实施例的详细描述,本发明的上述和其它特征以及优点将变得显见,其中:

图1是说明在使用MD-5查询一个传统EAP认证方法的实例中的信号流程示意图;

图2是说明在使用CHAP的一个传统认证方法的实例中的信号流程的

示意图；

图3是示出一般EAPOL帧格式的一个实例的示意图；

图4是根据本发明用于在EPON中的ONU和OLT之间建立一个认证的方法流程图；

图5是说明使用在根据本发明的用于在EPON中的ONU和OLT之间建立一个认证的方法中所使用的认证数据包的结构实例的示意图；以及

图6是用于根据本发明的认证处理的OLT的一个LLID认证处理部件的实例方框图。

具体实施方式

将参照附图详细描述本发明的最佳实施例。在本发明的下列描述中，为了清楚起见，在此的结合已知功能和结构的详细描述将被省略。

虽然IEEE 802.1x既能够实现在每一终端和桥接LAN设备，即EAPOL之间的认证，又能够实现在桥接LAN设备和RADIUS服务器，即RFC 2869中描述的在RADIUS上的EAP之间的一种协议，但是本发明将实现使用一个OLT的RADIUS功能。

图4是根据本发明用于在EPON中的ONU和OLT之间建立一个认证的方法流程图。该ONU首先把通知认证处理的开始的一个数据包送到OLT(401)。在该OLT中，如下面涉及图5进一步讨论的那样，将重新定义在ONU和OLT之间交换的数据包。该开始数据包具有对应于表示一个认证操作的开始的“开始”的代码值。

当认证操作开始时，OLT送出请求一个用户名的标识的数据包(402)。此时，数据包的代码值具有对应于表示请求该用户名的标识的“请求”的一个值。

响应该“请求”数据包，ONU送出用户名到该OLT(403)。此时，数据包的代码值具有对应于表示该响应的“响应”值。

该OLT随即标识在由该ONU送出的认证数据包中所含有的该ONU的特征值或标识符(在图示的实施例中的用户名)。当OLT标识该ONU具有一个有效的“用户名”时，其送出一个认证成功数据包，即一个接入接受数据包(404)。另一方面，在该ONU具有一个无效的“用户名”的场合，该

OLT送出一个认证拒绝数据包，即一个接入拒绝数据包(404)。该ONU根据该“用户名”的有效或无效的确定进入处理。

在接入接受或拒绝之后(404)，OLT把通知该认证处理结束的数据包发送至该ONU。此时，该数据包具有对应于“认证结束”的代码值。

图5是说明使用在根据本发明的用于在EPON中的ONU和OLT之间建立一个认证的方法中所使用的认证数据包的结构实例的示意图。如图5所示，该认证数据包包括目的地址(DA)、信源地址(SA)、逻辑链接标识符(LLID)、类型、子类型、版本、代码、数据/PDU和帧校验序列(FCS)。

DA字段501指示数据包的目的地址，SA字段502表示数据包的来源、LLID字段503表示逻辑连接标识符、类型字段504表示数据包该传播类型、子类型字段505表示当其类型字段504与另一数据包的类型字段相同时的数据包、版本字段506表示数据包的版本信息、代码字段507表示根据该数据包的一个认证操作、数据/PDU字段508表示该数据包的数据、FCS字段509表示FCS信息，该FCS信息用于检测对应于该数据包的包括在将要以帧单元发送的信息中的一个帧的误差。FCS信息被放置在该帧的末端。

具体地说，认证数据包把IEEE 802.3ah EFM子类型“0x04”结合到一个传统的OAM(操作、管理和维护)帧中。此帧格式直至另一传播类型被设定之前可被使用而没有任何问题，因为IEEE 802.3ah不使用该子类型“0x04”，并且避免了上述可能由该E类型“0x888e”的使用而引发的混淆的可能性。

版本或代码字段506指示该认证数据包操作的方式。下列表格1中描述了认证数据包的不同操作：

表1

代码	名称	内容
x00	开始	开始认证处理
0x01	请求	请求认证内容(LLID)
0x02	响应	认证内容的传送(LLID)
0x03	结束	结束认证处理
0x04	认证结果接入接受	认证的成功
0x05	认证结果接入拒绝	认证的拒绝

根据上述的认证处理，EPON的OLT执行该ONU的认证。与此操作相关联，OLT需要一个处理部件，用于进行在针对该ONU的一个初始注册处理之后所需要的认证处理的处理功能，以便减轻在下游方向(OLT→ONU)中把不用认证的数据服务提供到该ONU的需要。使用在上游方向(ONU←OLT)中的一个端口级控制功能，该处理部件进一步减轻为了防止在一个具体服务器的端口上的溢出攻击的需要。

图6示出根据本发明的一个OLT的LLID认证处理部件的实例。该部件包括一个用于相对于一个外部路由器61执行数据的输入/输出的总线接口62、用于根据一个认证处理接收一个OAM数据包从而控制器针对该ONU的数据服务的控制单元64、和在控制器64的控制下交换经由总线接口62接收的数据的一个下游单元63。

根据例如图5的一个已收的OAM帧并且使用“ALTM(地址查找表格管理)+ACT(认证控制表)”，该控制单元64控制包括在该下游单元中的一个端口的切换操作。ALTM协议的使用使得能够在一个点到多点PON结构中，例如在一个共享式局域网结构中的ONU之间进行通信。通常，使用CAM(信息地址存储器)实现ALTM。

当连接到该OLT的一个ONU期望发送数据到该OLT时，将以在其将要发送的数据中插入一个LLID的状态执行数据传输。该OLT在其ALT中查寻一个目标单元MAC地址。在该OLT确定该目的地MAC地址对应于该OLT中的一个站点的场合，其在发送期望数据之前改变该LLID。该ALTM部件执行重新改变或删除一个接收帧的SA字段的功能。

使用该功能，有可能通过在一个训练处理中完全产生的表格中查寻该MAC地址，来把根据该ONU的MAC地址分别改变的LLID重新发送至该OLT的ONU下游。使用一个过滤功能，每一ONU都能够只接收发送到其上的一帧。因此，有可能在ONU之间通信。

在一个ACT的初始注册之后，每一ONU都通过该OLT的规划器把分配其上的一个LLID和其MAC地址输入到该OLT的ALT作为初始值，然后把请求认证的一个“开始”帧发送到该OLT。该MAC地址被以包括在相关的ONU的用户名中的状态发送到该OLT，使得其被用作一个ONU的认证所需要的参数。

该OLT把通过一个“响应”帧重新输入的LLID与作为MAC地址而先前指定和输入到该OLT的对应LLID进行比较。仅当该MAC地址彼此相同时，该OLT才提供根据其端口控制操作提供期望的服务。

使用“ALTM+ACT”进行的认证方法实行如下。首先，控制单元64接收一个OAM帧。当一个“开始”帧中的用户名与预先设置在该OLT中的值相同时，控制单元64发送一个“请求”帧，并且把一个LLID输入到下游单元63。当根据来自ONU的一个“响应”帧随后作出成功认证时，控制单元64产生一个端口匹配信号，从而标准连接端口对应于该LLID。

另一方面，当认证失败时，控制单元64产生一个端口不匹配信号，从而防止该端口被连接。

下列表2中描述了ACT的一个实例：

表2

LLID输入	认证先前定义的LLID	认证结果	MAC 地址
--------	-------------	------	--------

如从上述说明显见的那样，本发明提供了用于在一个EPON中认证ONU的简单协议，并且避免当使用无线LAN时可能出现的传播类型的重叠。

此外，有可能使用不实施任何RADIUS服务器的存在算法，并且以使用LLID的一个端口控制的方式来实现一个可靠的认证方法。

本发明的上述方法能够以一个计算机可读程序的形式实现，使得其能够存储在例如CD-ROM、软磁盘、硬盘、或磁光盘的一个记录介质上。

虽然已经结合了被认为是目前最实际和最佳的实施例描述了本发明，但是应该理解的是本发明不局限于该公开的实施例，相反，本发明将力图覆盖所附的权利要求书的精神和范围内的各种修改。

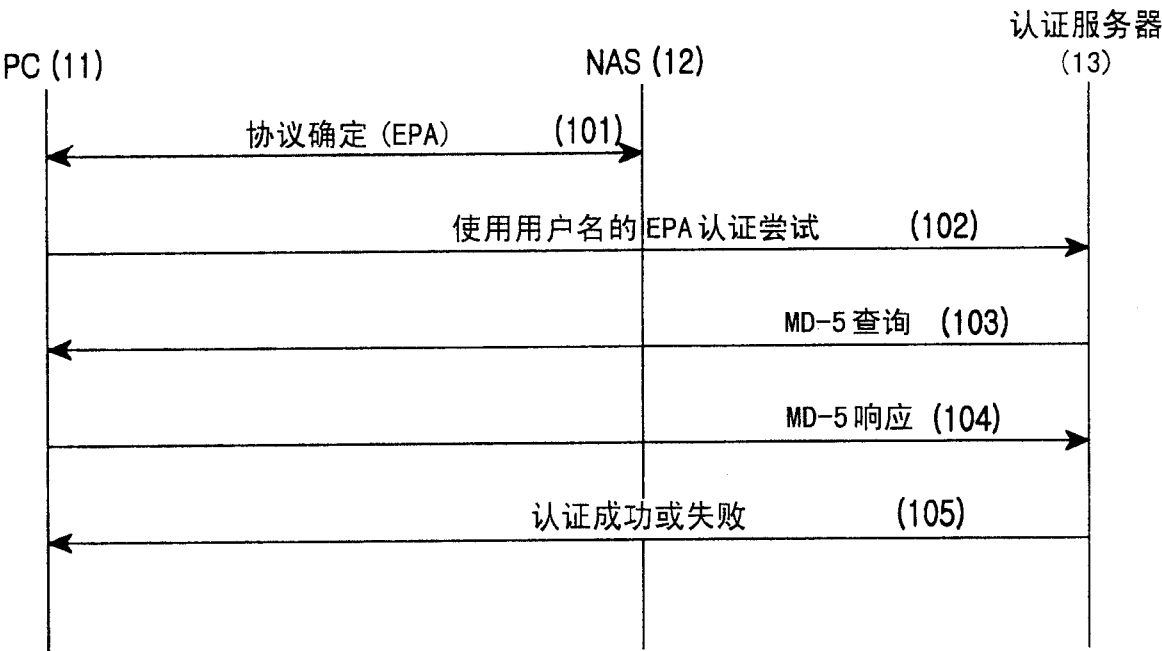


图 1

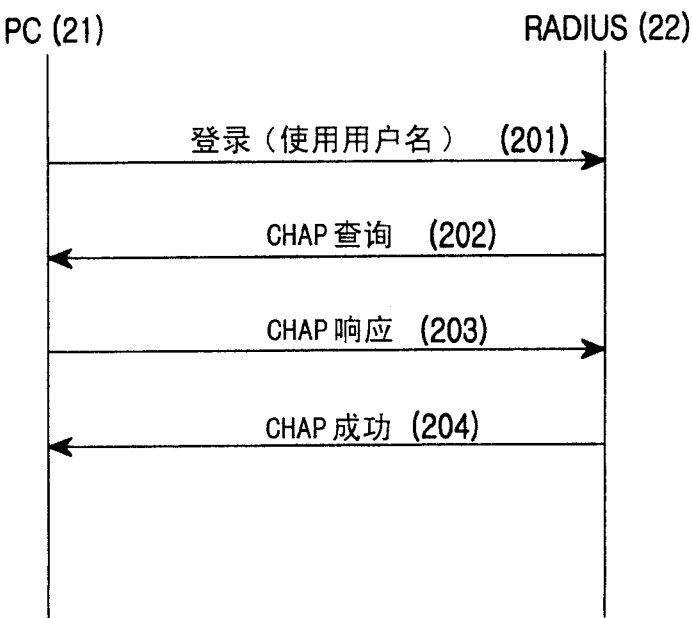


图 2

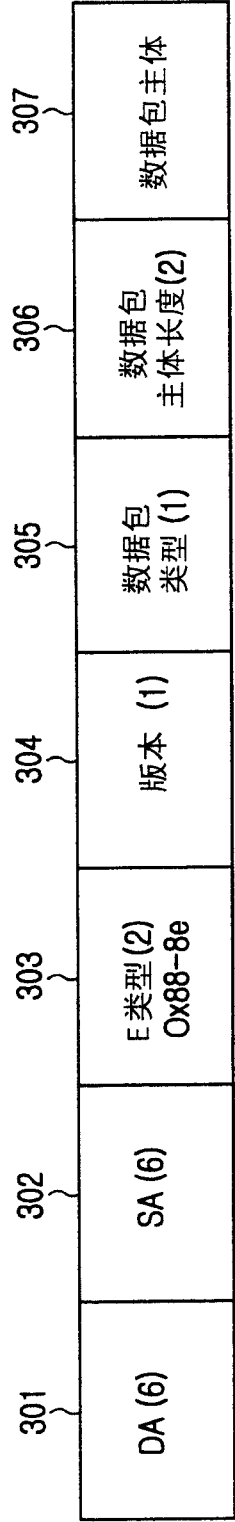


图 3

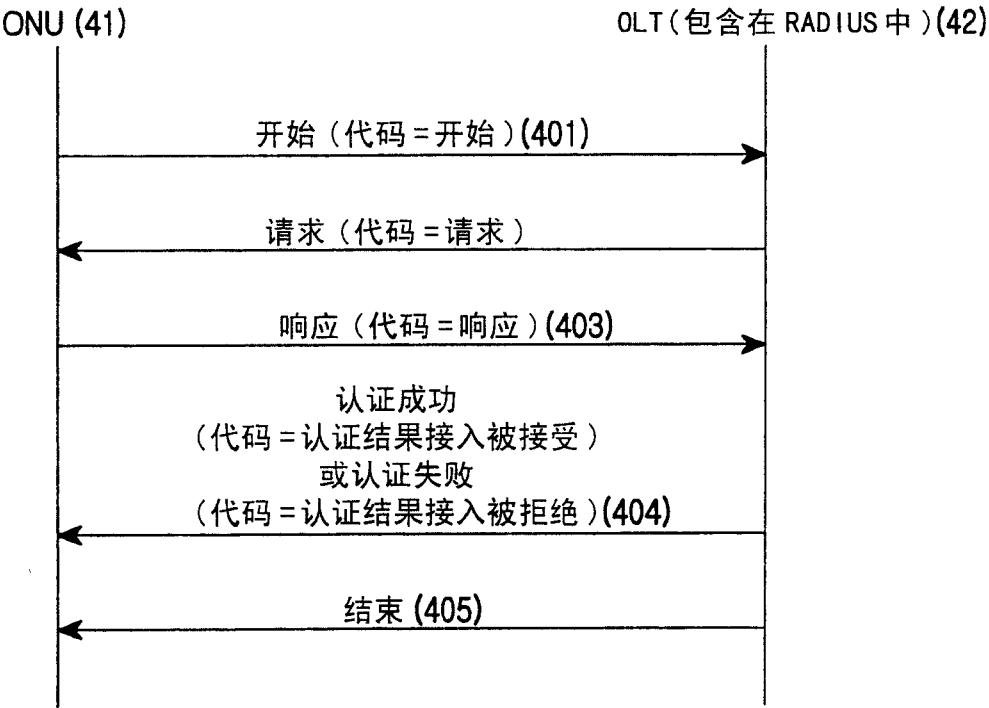


图 4

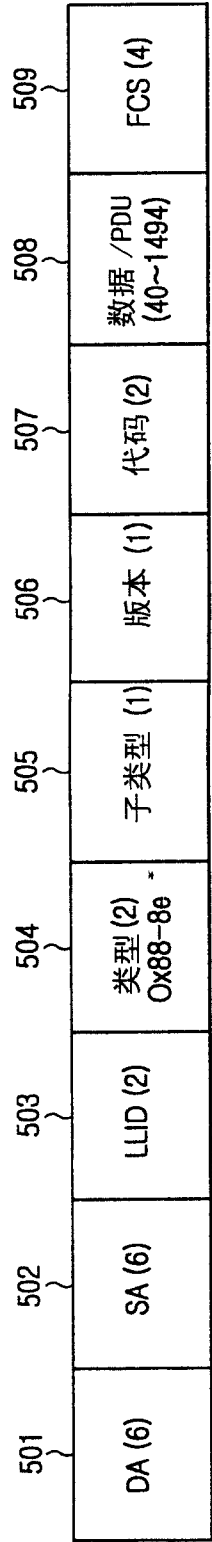


图 5

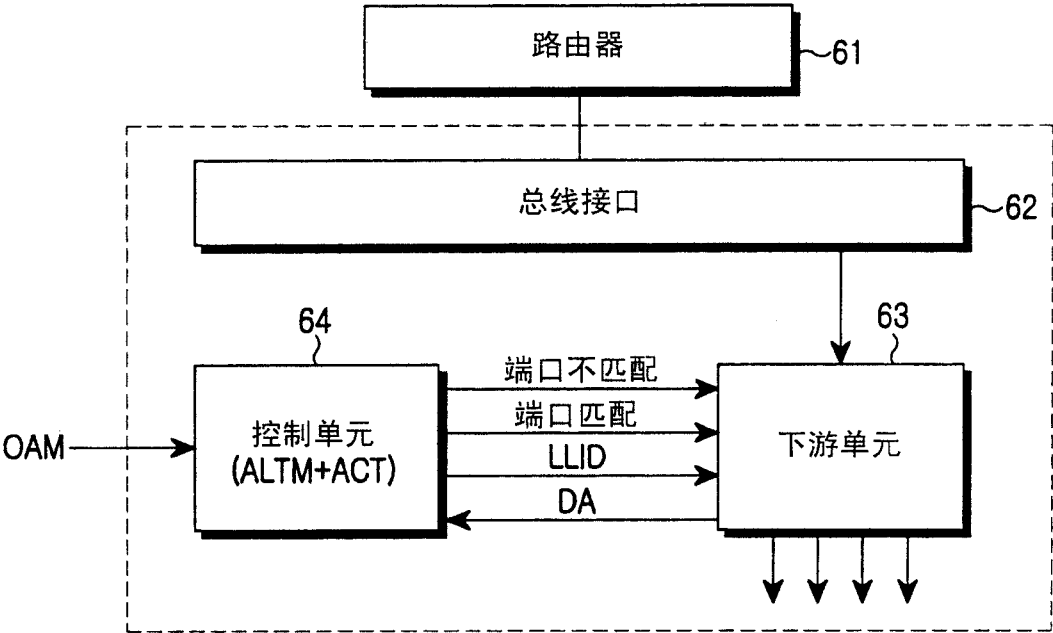


图 6