[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/14 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 03826030.1

[43] 公开日 2006 年 3 月 8 日

[11] 公开号 CN 1745538A

[22] 申请日 2003.2.25 [21] 申请号 03826030.1
[86] 国际申请 PCT/DE2003/000712 2003.2.25
[87] 国际公布 WO2004/077739 德 2004.9.10
[85] 进入国家阶段日期 2005.8.25
[71] 申请人 西门子公司
地址 德国慕尼黑
[72] 发明人 弗兰克 - 尤维·安德森 尤维·福尔
[74] 专利代理机构 北京市柳沈律师事务所
代理人 邵亚丽 李晓舒

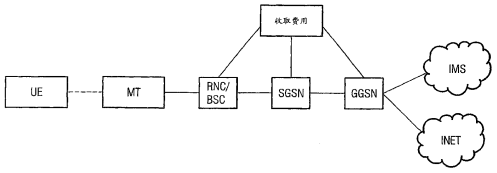
权利要求书 2 页 说明书 8 页 附图 2 页

[54] 发明名称

剥离出分配给专门组的 IP 信息包的方法和对应的 IP 信息包

[57] 摘要

本发明涉及一种在基于信息包的移动无线网络中剥离出分配给专门组的 IP 信息包的方法，其中在该移动无线网络的第一授权网络元件中对所有到达该移动无线网络的 IP 信息包就其是否分配给至少一个组进行检查，以及至少针对分配给一个专门组的 IP 信息包在至少一个、尤其是每个 IP 信息包的报头的一个字段中进行特定于该组的标记。



1. 一种在基于信息包的移动无线网络中剥离出分配给专门组的 IP 信息包的方法，其中

- 在该移动无线网络的第一授权网络元件中对所有到达该移动无线网络的 IP 信息包就其是否分配给至少一个组进行检查，以及

- 至少针对分配给一个专门组的 IP 信息包在至少一个、尤其是每个 IP 信息包的报头的一个字段中进行特定于该组的标记。

2. 根据权利要求 1 所述的方法，其特征在于，分别采用相应报头中字段元素没有被用于传输相应 IP 信息包的传输数据完全占用的字段。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，采用根据 IPv6 的规定而建立的 IP 信息包。

4. 根据上述权利要求中任一项所述的方法，其特征在于，作为相应报头的字段采用“流标签”字段。

5. 根据权利要求 1 至 3 中任一项所述的方法，其特征在于，作为相应报头的字段采用“接口 ID”字段。

6. 根据权利要求 1 至 3 中任一项所述的方法，其特征在于，作为相应报头的字段采用“扩展报头”字段。

7. 根据上述权利要求中任一项所述的方法，其特征在于，将在发送器端的 IP 堆栈和接收器端的 IP 堆栈之间的所述第一授权网络元件设置在一个数据信道上。

8. 根据上述权利要求中任一项所述的方法，其特征在于，作为专门组是所有分配给同一个 PDP 上下文的 IP 信息包。

9. 根据上述权利要求中任一项所述的方法，其特征在于，通过第二授权网络元件识别所述 IP 信息包的标记，并对相应的 IP 信息包进行特殊处理。

10. 根据上述权利要求中任一项所述的方法，其特征在于，只在一个第一次通过所述第一授权网络元件的 IP 信息包中这样进行标记，使得分配给同一组的所有其它 IP 信息包通过所述第二授权网络元件被识别为分配给同一组。

11. 根据权利要求 9 或 10 所述的方法，其特征在于，所述第二授权网络元件是费用采集位置，并且将所标记的 IP 信息包识别为免费。

12. 根据权利要求 9 至 11 中任一项所述的方法，其特征在于，在所述移动无线网络的、由 IP 信息包通过的边界元件上引入安全功能，在所述边界元件之间存在移动无线网络的授权网络元件，而所述安全功能消除在所有被标记的、且到达该移动无线网络的 IP 信息包中的标记。

13. 根据权利要求 12 所述的方法，其特征在于，所述安全功能采用位掩码。

14. 根据上述权利要求中任一项所述的方法，其特征在于，在接收端的终端中具有用于分析所到达 IP 信息包的标记的功能，以及对应于该分析的显示。

15. 一种具有报头和数据容器的 IP 信息包，其特征在于，该 IP 信息包分配给 IP 信息包的一个专门组，并且在所述报头的一个字段中记录特定于该组的标记。

16. 根据权利要求 15 所述的 IP 信息包，其特征在于，所述报头的字段是其字段元素没有被用于传输所述 IP 信息包的传输数据完全占据的字段。

17. 根据权利要求 15 或 16 所述的 IP 信息包，其特征在于，所述 IP 信息包根据 IPv6 规定建立。

18. 根据权利要求 15 至 17 中任一项所述的 IP 信息包，其特征在于，所述标记表明所述 IP 信息包是免费的。

剥离出分配给专门组的IP信息包的方法和对应的IP信息包

技术领域

本发明涉及一种用于剥离出可分配给专门组的IP信息包的方法以及一种IP信息包。

背景技术

在无线和有线通信网络中通常采用基于数据信息包（例如IP信息包，IP=互联网协议）传输的通信方法。在此称为基于信息包的移动无线网络。这种IP信息包由报头和与报头连接的数据容器（Datacontainer）组成。这种报头的结构例如在S. Deering和R. Hinden于1998年12月发表的文章“Network Working Group, Request for comments 2460, Internet Protocol, Version 6 (IPv6) Specification”，尤其是在第3章“IPv6 Header Format”中描述。报头和数据容器构成IP信息包。在报头中存储将IP信息包从IP信息包发送器传输到IP信息包接收器所需要的数据。

在基于信息包的移动无线网络中，费用采集除其它之外还基于对所传输的IP信息包的采集。在此，费用是根据从用户传输的和发送到用户的IP信息包的总量来计算的。在IP信息包流中，尤其是在采用IPv6版本的情况下，除了应用的纯有用数据之外还包含内部的信号发送数据，例如用于（无状态）配置或分割（MTU发现）的数据。所传输的发送信号的IP信息包在一个信道内通过移动无线网络的网络元件传输。在此，该IP信息包在该同一信道内如同有用IP信息包那样被传输。因此，发送信号的IP信息包不能很容易地与有用IP信息包区分或剥离开来。由此如上所述，针对该IP信息包向对应的用户征收了大量的费用，尽管该IP信息包没有传送实际的有用数据。发送信号的IP信息包更多的是用于满足网络运营商的要求和需要，对用户来说没什么重要性。在极端情况下还不运行应用软件。例如在所谓的“始终开机”的情况下传输包含IPv6发送信号的参数的IP信息包，该参数例如是路由地址（也就是IP信息包转接）。即使用户不使用诸如网页访问的服务，这些IP信息包也要在费用采集时被采集到，并向用户征收。

此外，多个应用可以使用一个 IP 信息包流来传输数据。通过多个应用同时使用一个 IP 信息包流在通过一个专门应用传输免费数据时会产生一个问题，即必须区分或剥离该数据。

此外还存在这样的可能性，操作员在特定情况下希望向用户免费提供任何服务，也就是非特定的单个应用，而是针对任意数据传输的完整 PDP 上下文。在此也产生如下问题：对应于该 PDP 上下文的 IP 信息包要从其他 IP 信息包剥离开来。

发明内容

因此，本发明要解决的技术问题是提供一种方法和一种 IP 信息包，借助它们可以按照可靠和廉价的方式剥离出分配给专门组的 IP 信息包。

该技术问题是通过根据权利要求 1 的方法和根据权利要求 15 的 IP 信息包解决的。优选的实施方式在对应的从属权利要求中给出。

根据本发明提供了一种在基于信息包的移动无线网络中剥离出分配给专门组的 IP 信息包的方法，其中在移动无线网络的第一授权网络元件中对所有到达该移动无线网络的 IP 信息包就其是否分配给至少一个组进行检查，并且至少针对分配给一个专门组的 IP 信息包在至少一个、尤其是每个 IP 信息包的报头的一个字段中进行标记。在此特别有利的是，该标记是在相应报头的、为了容纳传输数据而具有的字段中进行。

本发明的方法可以这样构成，采用相应报头中字段元素没有被用于传输 IP 信息包的传输数据完全占用的字段。由此可以有意义地使用“未使用”的字段元素。这涉及相应报头的这样的字段元素，在传输时为了容纳传输数据不需要或不完全需要这些字段元素，但这些字段元素还是被一起传输，必要时用“0”填满。

对于根据本发明的方法，优选采用根据互联网协议版本 6(IPv6)的规定而建立的 IP 信息包。

优选地，作为相应报头的字段采用“流标签”字段。该字段通常不需要用于存储传输数据，从而该字段的字段元素没有被占用，并且为标记提供了位置。

同样，优选的作为相应报头的字段采用 IP 信息包的对应报头的一个地址字段的“接口 ID”字段。报头的一个地址字段的“接口 ID”字段通常设

计为这样大，使得不需要所有的字段元素（位或字节）都用于容纳接口 ID 信息。由此根据本发明可以将未使用的位或字节用于标记。

此外有利的是，可以定义另一个其中进行标记的 IPv6 报头。这另一个报头被称为“扩展报头”。目前定义多个 IPv6 的扩展报头。在本发明的范围内还可以采用“逐段的选项报头（hop-by-hop option header）”类型的现有扩展报头，并通过使该报头具有上面描述的实际内容而在内容上建立该报头；在计算机科学领域称为 TLV（类型，长度，值）。

根据本发明的方法可以这样建立：将移动无线网络的第一授权网络元件上的标记写入相应报头的所述字段，其中在发送器端的 IP 堆栈和接收器端的 IP 堆栈之间的该第一网络元件设置在一个数据信道上。由此对可以访问该数据信道的装置（例如该数据信道的运营商的交换机）来说，有利的是可以通过该数据信道为传输的 IP 信息包设置标记。

在本发明方法的优选实施方式中，通过至少一个第二授权网络元件识别 IP 信息包的标记，并对相应的 IP 信息包进行特殊处理。

优选地，第二授权网络元件是费用采集位置，并且将所标记的 IP 信息包识别为免费。只在第一授权网络元件中将对费用重要的信息包与对费用不重要的信息包进行分离或剥离的花费，明显比在所有可以产生所谓费用票的网络元件中进行区分或识别的花费要少。如果涉及发送信号的、不应当计费的信息包，则基于直接 IP 信息包的计费通过剥离出一次性识别为发送信号的信息包并因此被标记的 IP 信息包而显著简化了该过程，因为在例如 n 个网络元件中节省了 n-1 次分类和剥离。根据本发明，产生所谓费用数据组（收费票）的其余网络元件只需注意是否具有标记，然后必要时对该信息包不采集费用数据（收费票）。如果供应商免费提供一个应用，则根据本发明，分配给该应用的 IP 信息包由对应的应用计算机在第一授权网络元件中进行标记。然后通过费用采集位置对该标记进行分析，并将被标记的 IP 信息包识别为免费。在此，只在一个网络元件中将对费用重要的信息包与对费用不重要的信息包进行分离或剥离并标记的花费，明显比在所有产生费用数剧组的网络元件中进行区分或剥离的花费要少。为此，这些网络元件必须使用具有免费应用的数据库，或具有该应用的目标地址和源地址的数据库。

此外还有一种可能性：操作员在特定情况下希望向其客户免费提供服

务。这例如不是在现有 PDP 上下文内特定 TCP-UDP 端口上的特定单个应用，而是用于任意 IP 数据传输的完整的免费 PDP 上下文。根据本发明，可以通过应用服务器对所有分配给该 PDP 上下文的 IP 信息包进行标记。由此通过费用采集位置识别所有分配给该 PDP 上下文的 IP 信息包并且不进行计费。

在本发明方法的另一个优选实施方式中，在由 IP 信息包通过的移动无线网络的边界元件上引入安全功能，在所述边界元件之间存在移动无线网络的授权网络元件，而所述安全功能消除在所有被标记的、且到达该移动无线网络的 IP 信息包中的标记。

其优点是，每个移动无线网络的边界的安全风险都可以如同在终端设备上那样被绕开。在传输 IP 信息包时可能如同在终端设备上那样，在有待通过的移动无线网络的网络边界上存在滥用的接入点。攻击者可能为此给所有 IP 信息包都设置表明该 IP 信息包为免费的标记。费用采集位置在费用采集时不考虑这些 IP 信息包，攻击者就可以免费的传输数据。根据本发明，通过在移动无线网络的、由待传输的 IP 信息包通过的边界元件上或在费用采集位置之前的另一个点上引入安全功能，可以提前抓住这种危险，其中所述安全功能消除在所有被标记的、且到达该移动无线网络的 IP 信息包中的标记。边界元件例如是 RNC（无线电网络控制器）或至移动信息包网络的转接计算机（网关）。借助该安全功能可以防止对该标记的非授权使用。在此，移动无线网络的其中引入了安全功能的边界元件要这样选择，使得该边界元件的那一端的所有网络元件都不能使用标记，也就是说在此不采集费用，也没有授权使用标记。因此，通过具有安全功能的边界元件那一端的网络元件的 IP 信息包的标记不会引起费用采集。移动无线网络的费用采集位置以及为了引入标记而授权的网络元件都位于具有安全功能的边界元件之间。通过引入安全功能可以授权通过该费用采集位置的 IP 信息包的标记，且不会出现滥用。

在本发明方法的优选实施方式中，安全功能采用位掩码。位掩码的使用，例如将一个零位掩码与一个具有一个被占用位的字节相加，是非常简单的方法，借助该方法可以消除用于剥离的标记。安全功能是一个简单的功能，其不需要很高的功率要求，并且对移动无线网络没有负担。不需要数据库和费事的求值方法。安全功能可以毫无问题地集成到移动无线网络

的现有网络元件中，并只对网络元件的功能产生非常小的负担。

在本发明方法的另一优选实施例中，在接收端的终端中具有用于分析所到达 IP 信息包的标记的功能，以及对应于该分析的显示。

在将标记例如用于表明免费传输 IP 信息包时，希望向用户例如显示免费传输的 IP 信息包的数量。这种显示的目的是向用户透明的表明对于该 IP 信息包的传输、也就是对应于特定服务的使用不收取费用。此外，应当向用户显示免费收到的 IP 信息包的总量。优选地，用于分析的功能在接收端的终端内通过一个到达的 IP 信息包占据一个位掩码，由此可以分析该 IP 信息包是否被标记传输，也就是说例如是否是免费传输的。通过在计数器上累加可以累加出免费传输的 IP 信息包的总量。合适的显示功能可以访问该计数器。

此外本发明还涉及一种具有报头和数据容器的 IP 信息包，其中该 IP 信息包分配给 IP 信息包的一个特殊组，并且在所述报头的一个字段中记录特定于该组的标记。

在本发明 IP 信息包的优选实施方式中，所述报头的字段是其字段元素没有被用于传输 IP 信息包的传输数据完全占据的字段。

此外，本发明的 IP 信息包优选根据 IPv6 规定建立。

优选地，这样建立所述 IP 信息包，使得所述标记表示出该 IP 信息包是免费的。

附图说明

下面借助附图详细解释本发明的其他优选实施方式。图中：

图 1 是用于显示本发明方法的实施方式的流程的 IP 基本结构的示意图；

图 2 是用于显示本发明方法的另一实施方式的另一种流程的 IP 基本结构的示意图。

具体实施方式

图 1 中示意性示出 IP 基本结构的一段。显示了与移动终端 MT 连接的所谓“用户设备” UE。通过该移动终端 MT 用户设备可以进入移动无线网络 MF。对该移动无线网络 MF 在该图中只示出了重要的网络元件。在该实

施例中示出根据 GPRS 规定（GPRS = 通用信息包无线电系统）工作的第三代移动无线网络。还示出 RNC（无线电网络控制器）和 BSC（基站控制器），后者形成输入节点。从 RNC 向 SGSN（服务 GPRS 支持节点）传递待传输的 IP 信息包。SGSN 是一个控制移动终端的移动性的控制网络节点。然后，从 SGSN 出发将 IP 信息包传递至 GGSN（网关 GPRS 支持节点）。GGSN 是 GPRS 网络的中央转接点，在该例中保证连接到数据信息包控制系统 IMS（IMS = IP 多媒体子系统）或诸如互联网的信息包数据网络。如果例如根据 IPv6 规定构造并因此具有报头和数据容器的 IP 信息包从互联网或 IMS 发送到用户设备 UE，其中例如要免费传输纯粹的发送信号信息包，则该 IP 信息包首先检查是否传输纯粹的发送信号数据。GGSN 检查所有从互联网或 IMS 到达该 GGSN 的 IP 信息包。如果 IP 信息包仅仅包含发送信号的数据，则 GGSN 作为移动无线网络的第一授权网络元件在该报头的一个字段中进行标记。该标记向所有后面的、还要被该 IP 信息包通过的网络元件表明，该 IP 信息包是免费传输的。SGSN 和 RNC 都可以用作费用采集位置，并因此可以安排所谓的费用数据组。此外，它们还可以，也就是被授权来分析该标记并将 IP 信息包识别为免费。在此，该标记优选在该 IP 信息包的报头的一个字段中，该字段的字段元素没有完全被用于传输该 IP 信息包的传输数据占据。在此，IP 信息包根据 IPv6 规定建立。标记例如添加到“流标签”字段中。此外还可以考虑将标记设置在“接口 ID”字段中。后者的尺寸通常设计得这样大，使得不是所有的字段元素都需要用于容纳接口 ID 信息。根据本发明，由此可以将未使用的位或字节用于填充该标记。此外还可以考虑定义另一个 IPv6 报头，即所谓的“扩展报头”并在其中设置标记。如果现在标记发送信号的信息包，则必须将该信息包首先识别为发送信号的信息包。为此例如可以用屏蔽已知的发送信号信息包的类型来对 IP 信息包的报头进行所谓的模式匹配。如果 IP 信息包正好在下一步也同样进行标记的网络元件中产生，则将该 IP 信息包作为发送信号的信息包的识别失效。

本发明方法的另一个应用可能例如是一种基于信息包的紧急呼叫。如果用户通过PDP上下文向可能的IMS紧急应用服务器发布基于IPv6的紧急呼叫，则该应用服务器这样标记分配给该特定PDP上下文的相应IP信息包，使得这些 IP 信息包被费用采集位置在分析该标记时识别为免费。由此防止由于可能缺乏金额而中断紧急呼叫。

本发明方法的另一个应用可能例如也可以是用于更新操作系统程序（固件）的免费服务。如果用户为了更新操作系统而通过 PDP 上下文向可能的应用服务器发布基于 IPv6 的更新要求，则该应用服务器根据本发明在分配给该 PDP 上下文的对应 IP 信息包的各报头中这样进行标记，使得这些 IP 信息包被费用采集位置在分析该标记时识别为免费。由此使得移动无线网络的运营商事后履行用于更新和修理由其运行的终端设备的义务，而不会向用户收取费用。

图 2 示出了 IP 基本结构的一段。显示出两个移动终端 MT1、MT2。该移动终端 MT1 和 MT2 通过移动无线网络和互联网（INET）相互连接。对该移动无线网络只示出几个重要的网络元件。移动终端 MT1 通过 RNC 进入移动无线网络。此外 SGSN 被显示为控制网络节点，GGSN 保证企业内部互联网进入在此示出的 MNO（移动网络操作员）。通过该企业内部互联网的一个网关可以进入互联网 INET。最后通过互联网可以连接到第二移动终端 MT2。为了传输 IP 信息包，在该例中采用 IP 第 6 版，即 IPv6。在采用本发明的方法时，应当为所有发送信号的信息包设置一个标记，由此由费用采集位置对发送信号的信息包进行分析并将相应的 IP 信息包识别为免费，并进行相应的处理。在网络边界上如同在移动终端上那样可以出现滥用的潜在接入点。为此，攻击者可能对所有 IP 信息包都设置一个特殊的标记，该标记由费用采集位置进行分析并将对应的 IP 信息包识别为免费。结果是，费用采集位置作为授权网络元件在费用采集时不考虑这些 IP 信息包，攻击者就能免费地传输数据。现在，在两个其间设置了移动无线网络的授权网络元件的重要边界元件上引入安全功能，该功能消除在所有被标记的、到达移动无线网络的 IP 信息包中的标记。在所示情况下，作为重要的边界元件采用 RNC 和 MNO 企业互联网的网关。在移动无线网络的边界元件中引入安全功能 SF。该功能 SF 的任务是防止对标记未经授权的使用。两个边界元件 RNC 和网关是这样选择的，使得该边界元件另一端的所有网络元件都不能授权对该标记的使用。边界元件这一端的所有网络元件可以使用该标记，也不会由于在该边界元件中引入安全功能而受到干扰。边界元件上的安全功能优选是一种用于消除所有通过该安全功能或相应边界元件的 IP 信息包中标记的简单方法。为了消除例如可以采用简单的位掩码。由于所有通过该安全功能的 IP 信息包都被掩蔽，因此不需要费事的分析方法。

按照该形式的安全功能可以集成在每个网关中。此外，安全功能没有很高的功率要求并且不对移动无线网络造成负担。而且不需要数据库。

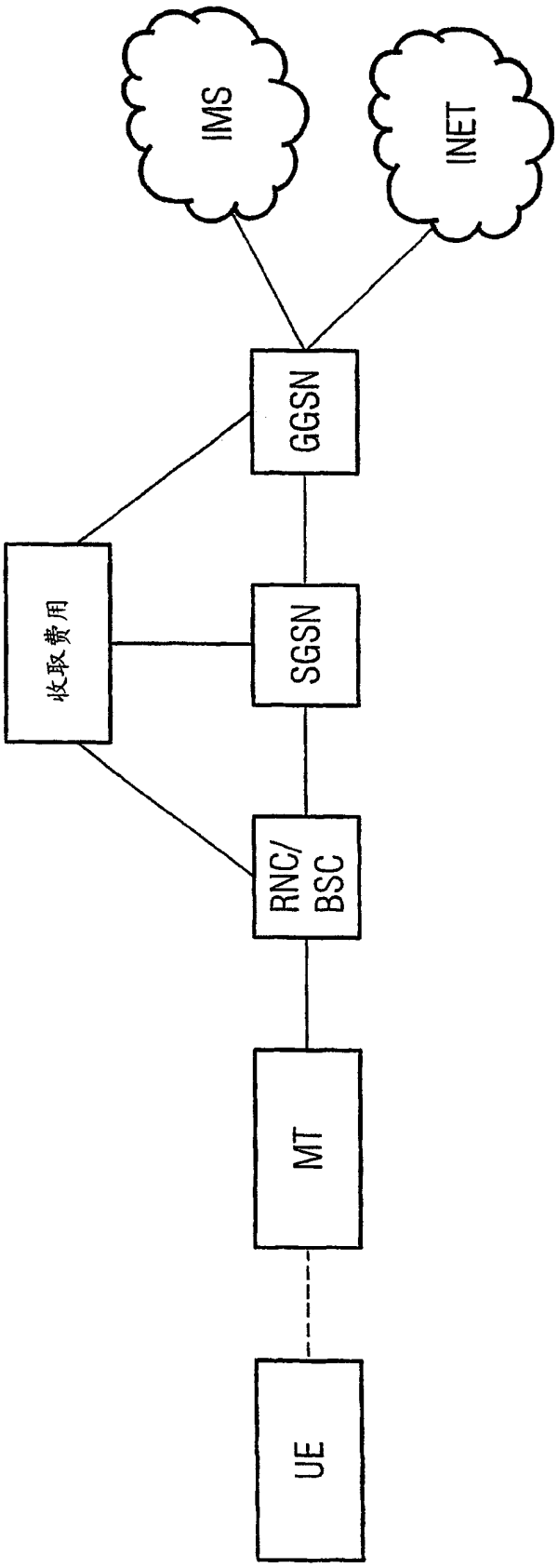


图 1

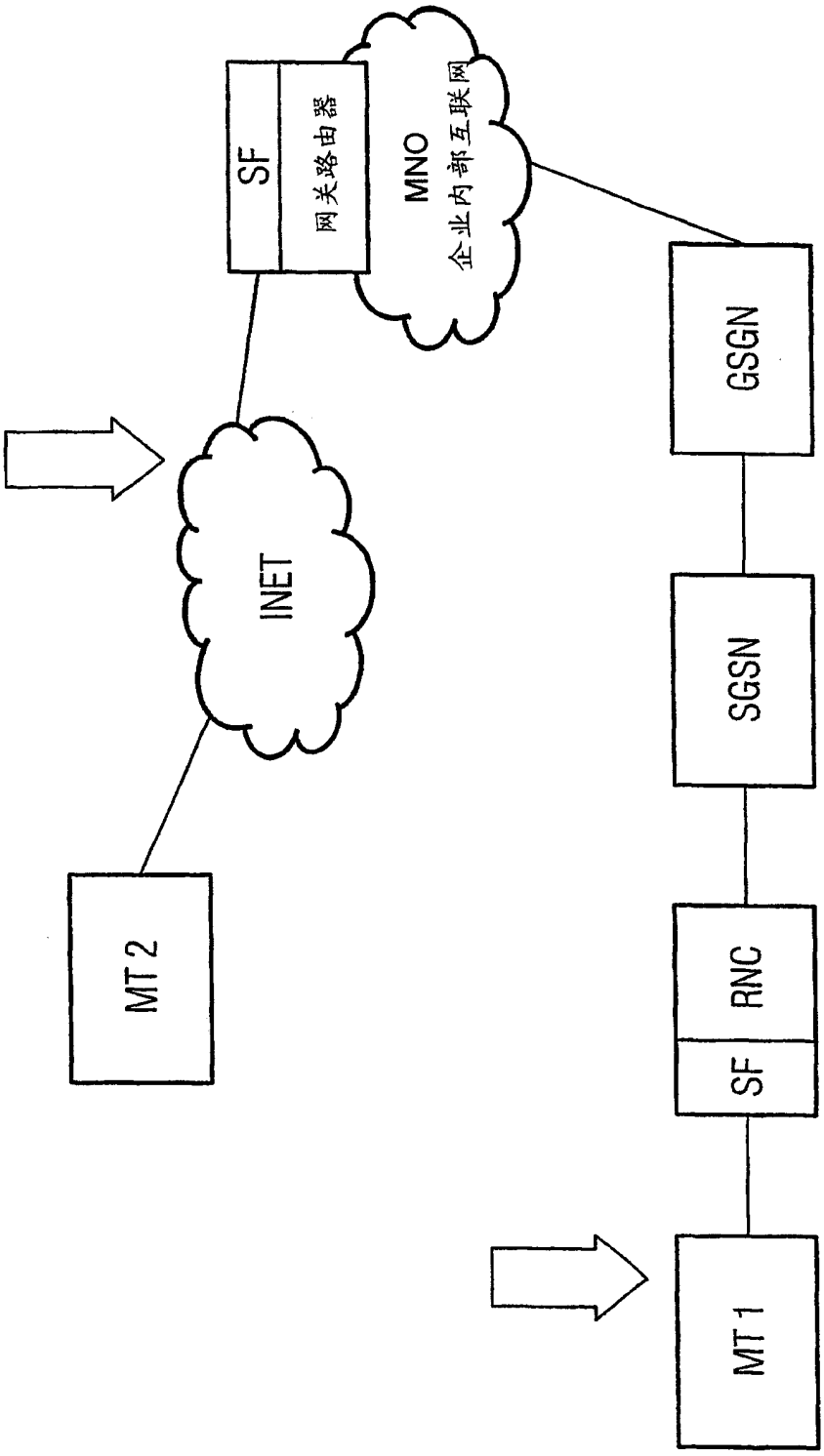


图 2