(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109150751 B
(45)授权公告日 2022.05.27

(21)申请号 201710459379.6
(22)申请日 2017.06.16
(65)同一申请的已公布的文献号
申请公布号 CN 109150751 A
(43)申请公布日 2019.01.04
(73)专利权人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱
(72)发明人 李亮 薛永灵 陈昭宇 刘俊飞
(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
专利代理师 蒋冬梅 栗若木
(51)Int.Cl.
H04L 47/2475(2022.01)
H04L 47/80(2022.01)
H04M 1/663(2006.01)

(56)对比文件
CN 106293901 A,2017.01.04
CN 103384250 A,2013.11.06
CN 106815038 A,2017.06.09
CN 105389193 A,2016.03.09
US 2015188949 A1,2015.07.02
US 2016210578 A1,2016.07.21

审查员 郭海波

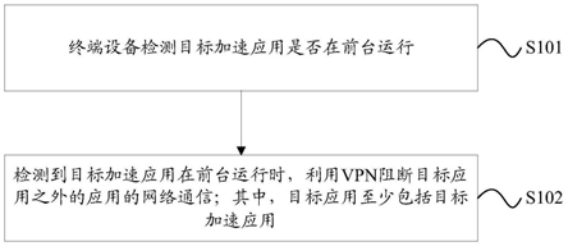
权利要求书2页 说明书10页 附图3页

(54)发明名称

一种网络控制方法及装置

(57)摘要

本文公开了一种网络控制方法及装置;上述网络控制方法,包括:终端设备检测目标加速应用是否在前台运行;当检测到目标加速应用在前台运行时,利用VPN阻断目标应用之外的应用的网络通信,其中,目标应用至少包括:目标加速应用。如此,通过阻断目标应用之外的应用的网络通信,提高了目标应用占用的带宽,从而达到了目标应用的加速目的,并提高了终端设备的用户使用体验。



CN 109150751 B

1.一种网络控制方法,其特征在于,包括:

终端设备检测目标加速应用是否在前台运行;

当检测到所述目标加速应用在前台运行时,利用虚拟专用网络VPN阻断目标应用之外的应用的网络通信,当所述目标加速应用结束前台运行时,恢复所述目标应用之外的应用的网络通信,其中,所述目标应用至少包括:所述目标加速应用。

2.根据权利要求1所述的方法,其特征在于,所述目标应用还包括:与所述目标加速应用关联的应用。

3.根据权利要求1所述的方法,其特征在于,所述利用VPN阻断目标应用之外的应用的网络通信,包括:

控制所述目标应用采用物理网卡提供的网络通道进行网络通信;

控制所述目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信,并暂时阻断所述VPN虚拟网卡提供的网络通道。

4.根据权利要求3所述的方法,其特征在于,所述方法还包括:

在检测到所述目标加速应用结束前台运行时,恢复所述VPN虚拟网卡提供的网络通道。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

在检测到所述目标加速应用在前台运行时,拦截来自拦截列表中记录的号码的电话和短消息;

将拦截的电话和短消息的信息以悬浮窗形式显示在显示界面。

6.一种网络控制装置,其特征在于,包括:

第一检测模块,适于检测目标加速应用是否在前台运行;

第一控制模块,适于当所述第一检测模块检测到所述目标加速应用在前台运行时,利用虚拟专用网络VPN阻断目标应用之外的应用的网络通信,当所述目标加速应用结束前台运行时,恢复所述目标应用之外的应用的网络通信,其中,所述目标应用至少包括:所述目标加速应用。

7.根据权利要求6所述的装置,其特征在于,所述第一控制模块适于通过以下方式利用VPN阻断目标应用之外的应用的网络通信:

控制所述目标应用采用物理网卡提供的网络通道进行网络通信;

控制所述目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信,并暂时阻断所述VPN虚拟网卡提供的网络通道。

8.一种网络控制方法,其特征在于,包括:

终端设备检测前台运行的应用是否满足设定条件;

在检测到所述前台运行的应用满足设定条件时,利用虚拟专用网络VPN阻断目标应用之外的应用的网络通信;当满足设定条件的应用结束前台运行时,恢复所述目标应用之外的应用的网络通信,其中,所述目标应用至少包括所述前台运行的应用。

9.根据权利要求8所述的方法,其特征在于,所述检测到所述前台运行的应用满足设定条件包括以下至少之一:

检测到所述前台运行的应用记录在网络加速应用列表中;

检测到所述前台运行的应用消耗的历史数据流量满足第一条件;

检测到所述前台运行的应用的历史使用时长满足第二条件。

10.根据权利要求8所述的方法，其特征在于，所述利用VPN阻断目标应用之外的应用的网络通信，包括：

控制所述目标应用采用物理网卡提供的网络通道进行网络通信；

控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断所述VPN虚拟网卡提供的网络通道。

11.根据权利要求10所述的方法，其特征在于，所述方法还包括：在检测到所述满足设定条件的应用结束前台运行时，恢复所述VPN虚拟网卡提供的网络通道。

12.一种网络控制装置，其特征在于，包括：

第二检测模块，适于检测前台运行的应用是否满足设定条件；

第二控制模块，适于在所述第二检测模块检测到所述前台运行的应用满足设定条件时，利用虚拟专用网络VPN阻断目标应用之外的应用的网络通信；当满足设定条件的应用结束前台运行时，恢复所述目标应用之外的应用的网络通信；其中，所述目标应用至少包括所述前台运行的应用。

13.根据权利要求12所述的装置，其特征在于，所述第二检测模块适于通过以下至少之一方式检测到所述前台运行的应用满足设定条件：

检测到所述前台运行的应用记录在网络加速应用列表中；

检测到所述前台运行的应用消耗的历史数据流量满足第一条件；

检测到所述前台运行的应用的历史使用时长满足第二条件。

14.一种终端设备，其特征在于，包括：存储器、处理器以及存储在所述存储器上并在所述处理器上运行的网络控制程序，所述网络控制程序被所述处理器执行时实现如权利要求1至5中任一项所述的网络控制方法的步骤。

15.一种终端设备，其特征在于，包括：存储器、处理器以及存储在所述存储器上并在所述处理器上运行的网络控制程序，所述网络控制程序被所述处理器执行时实现如权利要求8至11中任一项所述的网络控制方法的步骤。

16.一种计算机可读介质，其特征在于，存储有网络控制程序，所述网络控制程序被处理器执行时实现如权利要求1至5中任一项所述的网络控制方法的步骤。

17.一种计算机可读介质，其特征在于，存储有网络控制程序，所述网络控制程序被处理器执行时实现如权利要求8至11中任一项所述的网络控制方法的步骤。

18.一种网络控制方法，其特征在于，包括：

确定目标软件运行；

根据预设规则，控制所述目标软件之外的软件的网络通信状态，当所述目标软件结束运行时，恢复所述目标软件之外的软件的网络通信状态，其中，所述网络通信状态包括网络通信速度或网络通信开关。

一种网络控制方法及装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种网络控制方法及装置。

背景技术

[0002] 目前，用户在使用终端设备(比如，手机或平板电脑等)进行应用操作时，存在用户体验不高的情况。比如，用户在使用手机进行对战游戏时，若存在多个其他应用处于开启状态，则开启的多个应用会抢占网速，导致游戏网速慢，从而影响用户体验，而且在游戏过程中手机会收到即时通信(IM，Instant Messaging)应用的消息提醒，也会影响到用户的操作体验。

发明内容

[0003] 以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

[0004] 本申请实施例提供一种网络控制方法及装置，能够提高终端设备的用户使用体验。

[0005] 第一方面，本申请实施例提供一种网络控制方法，包括：

[0006] 终端设备检测目标加速应用是否在前台运行；

[0007] 当检测到所述目标加速应用在前台运行时，利用虚拟专用网络(VPN)阻断目标应用之外的应用的网络通信，其中，所述目标应用至少包括：所述目标加速应用。

[0008] 其中，所述目标应用还可以包括：与所述目标加速应用关联的应用。

[0009] 其中，所述利用VPN阻断目标应用之外的应用的网络通信，可以包括：

[0010] 控制所述目标应用采用物理网卡提供的网络通道进行网络通信；

[0011] 控制所述目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断所述VPN虚拟网卡提供的网络通道。

[0012] 其中，上述方法还可以包括：在检测到所述目标加速应用结束前台运行时，恢复所述VPN虚拟网卡提供的网络通道。

[0013] 其中，所述方法还可以包括：在检测到所述目标加速应用在前台运行时，拦截来自拦截列表中记录的号码的电话和短消息；

[0014] 将拦截的电话和短消息的信息以悬浮窗形式显示在显示界面。

[0015] 第二方面，本申请实施例提供一种网络控制装置，包括：

[0016] 第一检测模块，适于检测目标加速应用是否在前台运行；

[0017] 第一控制模块，适于当所述第一检测模块检测到所述目标加速应用在前台运行时，利用VPN阻断目标应用之外的应用的网络通信，其中，所述目标应用至少包括：所述目标加速应用。

[0018] 其中，所述第一控制模块可以适于通过以下方式利用VPN阻断目标应用之外的应用的网络通信：

[0019] 控制所述目标应用采用物理网卡提供的网络通道进行网络通信；

[0020] 控制所述目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断所述VPN虚拟网卡提供的网络通道。

[0021] 第三方面，本申请实施例提供一种网络控制方法，包括：

[0022] 终端设备检测前台运行的应用是否满足设定条件；

[0023] 在检测到所述前台运行的应用满足设定条件时，利用VPN阻断目标应用之外的应用的网络通信；其中，所述目标应用至少包括所述前台运行的应用。

[0024] 其中，所述检测到所述前台运行的应用满足设定条件可以包括以下至少之一：

[0025] 检测到所述前台运行的应用记录在网络加速应用列表中；

[0026] 检测到所述前台运行的应用消耗的历史数据流量满足第一条件；

[0027] 检测到所述前台运行的应用的历史使用时长满足第二条件。

[0028] 其中，所述利用VPN阻断目标应用之外的应用的网络通信，可以包括：

[0029] 控制所述目标应用采用物理网卡提供的网络通道进行网络通信；

[0030] 控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断所述VPN虚拟网卡提供的网络通道。

[0031] 其中，上述方法还可以包括：在检测到所述满足设定条件的应用结束前台运行时，恢复所述VPN虚拟网卡提供的网络通道。

[0032] 第四方面，本申请实施例提供一种网络控制装置，包括：

[0033] 第二检测模块，适于检测前台运行的应用是否满足设定条件；

[0034] 第二控制模块，适于在所述第二检测模块检测到所述前台运行的应用满足设定条件时，利用VPN阻断目标应用之外的应用的网络通信；其中，所述目标应用至少包括所述前台运行的应用。

[0035] 其中，所述第二检测模块可以适于通过以下至少之一方式检测到所述前台运行的应用满足设定条件：

[0036] 检测到所述前台运行的应用记录在网络加速应用列表中；

[0037] 检测到所述前台运行的应用消耗的历史数据流量满足第一条件；

[0038] 检测到所述前台运行的应用的历史使用时长满足第二条件。

[0039] 第五方面，本申请实施例提供一种网络控制方法，包括：

[0040] 确定目标软件运行；

[0041] 根据预设规则，控制所述目标软件之外的软件的网络通信状态，其中，所述网络通信状态包括网络通信速度或网络通信开关。

[0042] 第六方面，本申请实施例还提供一种终端设备，包括：存储器、处理器以及存储在所述存储器上并在所述处理器上运行的网络控制程序，所述网络控制程序被所述处理器执行时实现上述第一方面的网络控制方法的步骤。

[0043] 第七方面，本申请实施例还提供一种终端设备，包括：存储器、处理器以及存储在所述存储器上并在所述处理器上运行的网络控制程序，所述网络控制程序被所述处理器执行时实现上述第三方面的网络控制方法的步骤。

[0044] 此外，本申请实施例还提供一种计算机可读介质，存储有网络控制程序，所述网络控制程序被处理器执行时实现上述第一方面的网络控制方法的步骤。

[0045] 此外，本申请实施例还提供一种计算机可读介质，存储有网络控制程序，所述网络控制程序被处理器执行时实现上述第三方面的网络控制方法的步骤。

[0046] 此外，本申请实施例还提供一种计算机可读介质，存储有网络控制程序，所述网络控制程序被处理器执行时实现上述第五方面的网络控制方法的步骤。

[0047] 在本申请实施例中，终端设备检测目标加速应用是否在前台运行，在检测到目标加速应用在前台运行时，利用VPN阻断目标应用之外的应用的网络通信，其中，目标应用至少包括目标加速应用。如此，通过阻断目标应用之外的应用的网络通信，提高了目标应用占用的带宽，从而达到了目标应用的加速目的；而且，由于目标应用之外的应用处于断网状态，在目标加速应用运行时屏蔽了这些应用的通知消息，从而提高了用户操作体验。

[0048] 进一步地，在检测到目标加速应用在前台运行时，还可以进行电话和短消息拦截，避免了目标加速应用在前台运行时电话和短消息的干扰，从而提高了用户操作体验。而且，可以将拦截的电话和短消息以悬浮窗的形式进行提醒，从而避免用户错过重要事情。

[0049] 当然，实施本申请的任一产品不一定需要同时达到以上所有优点。

附图说明

[0050] 图1为本申请实施例一提供的网络控制方法的流程图；

[0051] 图2为本申请实施例一中利用VPN阻断相关应用的网络通信的示意图；

[0052] 图3为本申请实施例一的示例流程图；

[0053] 图4为本申请实施例二提供的网络控制装置的示意图；

[0054] 图5为本申请实施例三提供的网络控制方法的流程图；

[0055] 图6为本申请实施例三提供的网络控制装置的示意图；

[0056] 图7为本申请实施例四提供的网络控制方法的流程图。

具体实施方式

[0057] 以下结合附图对本申请实施例进行详细说明，应当理解，以下所说明的实施例仅用于说明和解释本申请，并不用于限定本申请。

[0058] 需要说明的是，如果不冲突，本申请实施例以及实施例中的各个特征可以相互结合，均在本申请的保护范围之内。另外，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0059] 一些实施方式中，执行网络控制方法的计算设备可包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存(memory)。

[0060] 内存可能包括计算机可读介质中的非永久性存储器、随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flashRAM)。内存是计算机可读介质的示例。内存可能包括模块1，模块2，……，模块N(N为大于2的整数)。

[0061] 计算机可读介质包括永久性和非永久性、可移动和非可移动存储介质。存储介质可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)，快闪记忆体或其他内存技术、只读光盘只读

存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括非暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0062] 实施例一

[0063] 本申请实施例提供一种网络控制方法，如图1所示，包括：

[0064] S101、终端设备检测目标加速应用是否在前台运行；

[0065] S102、在检测到目标加速应用在前台运行时，利用VPN阻断目标应用之外的应用的网络通信；其中，目标应用至少包括目标加速应用。

[0066] 本实施例中，终端设备可以包括诸如手机、平板电脑、笔记本电脑、掌上电脑、个人数字助理(Personal Digital Assistant，PDA)、便捷式媒体播放器(Portable Media Player，PMP)、可穿戴设备等移动终端，以及诸如数字TV、台式计算机等固定终端。然而，本申请对此并不限定。

[0067] 其中，目标加速应用可以包括配置在网络加速应用列表中的应用，比如，对战游戏应用等。

[0068] 在示例性实施方式中，目标应用可以仅包括：目标加速应用；此时，在检测到目标加速应用在前台运行时，可以利用VPN阻断该目标加速应用之外的应用的网络通信。

[0069] 在示例性实施方式中，目标应用可以包括：目标加速应用以及与目标加速应用关联的应用。此时，在检测到目标加速应用在前台运行时，可以利用VPN阻断目标加速应用和与其关联的应用之外的应用的网络通信。其中，目标加速应用与其他应用之间的关联关系可以由用户设置，或者，可以根据应用之间的调用关系确定。然而，本申请对此并不限定。

[0070] 比如，目标加速应用为应用A，应用A在运行过程中可以跳转至运行应用B，则可以认为应用B为与应用A关联的应用；若当前的已启动应用包括应用A、应用B、应用D及应用E，其中，未启动的应用不进行网络通信，则当应用A在前台运行时，可以利用VPN阻断应用D及应用E的网络通信，使得应用A和应用B保持联网状态，屏蔽了应用A运行过程中应用D和应用E的消息通知。

[0071] 在示例性实施方式中，利用VPN阻断目标应用之外的应用的网络通信，可以包括：

[0072] 控制目标应用采用物理网卡提供的网络通道进行网络通信；

[0073] 控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断VPN虚拟网卡提供的网络通道。

[0074] 其中，本实施例的方法还可以包括：在检测到目标加速应用结束前台运行时，恢复VPN虚拟网卡提供的网络通道。换言之，在目标加速应用结束前台运行时，可以恢复目标应用之外的应用的网络通信。

[0075] 在示例性实施方式中，用户可以预先在终端设备上配置目标应用采用物理网卡提供的网络通道进行网络通信，并配置目标应用外的应用采用VPN虚拟网卡提供的网络通道进行网络通信；终端设备在检测到目标加速应用在前台运行时，基于用户预先的配置暂时阻断VPN虚拟网卡提供的网络通道，即可实现断开目标应用外的应用的联网状态。或者，终端设备在检测到目标加速应用在前台运行时，可以在显示界面提示用户选择并确认需要阻断哪些应用的联网状态，并控制用户选择的应用采用VPN虚拟网卡提供的网络通道进行网

络通信,并暂时阻断VPN虚拟网卡提供的网络通道。然而,本申请对此并不限定。

[0076] 下面参照图2说明利用VPN阻断相关应用的网络通信的过程。

[0077] 如图2所示,可以将终端设备上的应用分成两部分:网络加速应用、非加速应用;其中,可以预先设置网络加速应用列表,用于记录需要进行网络加速的应用的信息(比如,应用标识(ID)、名称等)。例如,网络加速应用可以包括:一种或多种对战游戏应用。其中,不在网络加速应用列表中记录的应用即为非加速应用。或者,用户可以根据实际场景选择哪些应用作为网络加速应用,哪些应用作为非加速应用。然而,本申请对此并不限定。

[0078] 如图2所示,网络加速应用可以直接通过物理网卡提供的网络通道进行网络通信,而非加速应用则设置为采用VPN虚拟网卡提供的网络通道进行网络通信。其中,可以在VPN虚拟网卡的配置信息中添加需要通过VPN虚拟网卡联网的应用的信息(比如,应用ID、应用名称等)。

[0079] 当终端设备的网络加速应用在前台运行时,可以暂时阻断VPN虚拟网卡提供的网络通道,比如,VPN虚拟网卡设置为暂时停用,不进行数据传输处理。如此,通过VPN虚拟网卡进行网络通信的非加速应用处于断网状态,网络加速应用可以独享网络带宽,以达到加速目的。而且,由于非加速应用处于断网状态,在网络加速应用的运行过程中阻隔了非加速应用的消息通知,从而给用户提供了对网络加速应用的纯净操作体验。

[0080] 需要说明的是,当网络加速应用列表中记录有多个网络加速应用,且当前至少有两个网络加速应用(以网络加速应用A和网络加速应用B为例)启动时,若网络加速应用A在前台运行,需要屏蔽网络加速应用B的干扰,则可以将网络加速应用B配置为通过VPN虚拟网卡提供的网络通道进行网络通信,并通过阻断VPN虚拟网卡提供的网络通道使得网络加速应用B断网;若网络加速应用A在前台运行,且网络加速应用B与网络加速应用A存在关联,则网络加速应用A和网络加速应用B都可以配置为通过物理网卡提供的网络通道进行网络通信。

[0081] 如图2所示,终端设备还可以根据当前无线网络(比如,WiFi网络)是否存在风险,确定互联网访问路径。比如,若判断当前连接的WiFi网络存在风险,则通过VPN服务器进行网络访问,若判断当前连接的WiFi网络无风险或风险较低,则可以直接通过路由器路径进行网络访问。

[0082] 在示例性实施方式中,本实施例的网络控制方法还可以包括:

[0083] 在检测到目标加速应用在前台运行时,拦截来自拦截列表中记录的号码的电话和短消息;

[0084] 将拦截的电话和短消息的信息以悬浮窗形式显示在显示界面。

[0085] 在本实施方式中,在拦截列表中可以记录需要拦截的号码。

[0086] 在本实施方式中,悬浮窗可以是半透明的。将拦截的电话和短消息以悬浮窗形式显示在显示界面,既不影响用户在终端设备的当前操作,也可以让用户实时了解已经拦截的电话和短消息,避免用户错过重要事情。其中,悬浮窗可以在显示预定时长之后自动消失,或者,在接收到用户执行相应操作(比如,点击悬浮窗、翻转或摇动终端设备等)之后消失。本申请对此并不限定。

[0087] 在其他实现方式中,可以预先设置号码白名单,此时,在检测到目标加速应用在前台运行时,可以针对来自不在号码白名单中的号码的电话和短消息进行拦截。

[0088] 下面通过一个示例对本申请的方法进行说明。在本示例中，目标加速应用以游戏应用为例进行说明。然而，本申请对此并不限定。在实际场景中，可以根据实际情况确定目标加速应用。

[0089] 如图3所示，本示例包括以下步骤：

[0090] S301、在终端设备上运行一游戏应用；

[0091] S302、终端设备检测该游戏应用是否在终端设备的前台运行；若该游戏应用在前台运行，则执行S303，否则，结束处理；

[0092] S303、在该游戏应用在前台运行时，启用VPN网络控制；比如，终端设备可以直接利用VPN阻断当前游戏应用之外的已启动应用的联网状态，使得当前游戏应用可以独享网络带宽，从而提高游戏应用的网络速度，达到加速游戏应用的目的；或者，终端设备可以提示用户确认需要阻断哪些应用的联网状态，并控制用户选择的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断VPN虚拟网卡提供的网络通道；其中，用户选择的应用可以是已启动应用，也可以是暂未启动的应用，以避免在游戏应用运行过程中启动其他应用影响游戏应用操作的网络速度。关于VPN网络控制的实现方式可以参照图2的说明，故于此不再赘述。

[0093] 其中，由于相关应用在断网之后，无法进行网络通信，不会进行消息通知，避免了用户在游戏过程中被打扰，从而为用户提供纯净的娱乐体验。

[0094] S304、在该游戏应用在前台运行时，启用通话和短消息拦截；其中，用户可以设置拦截列表，对来自拦截列表中号码的来电和短消息进行拦截，从而使得用户在防打扰状态进行游戏操作，为用户提供沉浸式的游戏体验。

[0095] 在示例性实施方式中，在用户进行游戏时将电话和短消息进行拦截之后，可以以悬浮窗的形式进行提醒，以便用户可事后进行处理，避免用户错过重要事情。

[0096] S305、检测游戏应用是否结束前台运行；若检测到游戏应用结束前台运行，则执行S306，否则继续进行VPN网络控制，即返回S303。

[0097] S306、在游戏应用结束前台运行，结束对相关应用的断网控制；即恢复VPN虚拟网卡提供的网络通道。

[0098] 需要说明的是，本申请对于S303和S304的执行顺序并不限定。本示例中，以S303先于S304执行为例。然而，在其他实现方式中，S304可以先于S303执行，或者，同时执行。

[0099] 实施例二

[0100] 本实施例提供一种网络控制装置，如图4所示，包括：

[0101] 第一检测模块401，适于检测目标加速应用是否在前台运行；

[0102] 第一控制模块402，适于当第一检测模块401检测到目标加速应用在前台运行时，利用VPN阻断目标应用之外的应用的网络通信，其中，目标应用至少包括：目标加速应用。

[0103] 其中，第一控制模块402可以适于通过以下方式利用VPN阻断目标应用之外的应用的网络通信：

[0104] 控制目标应用采用物理网卡提供的网络通道进行网络通信；

[0105] 控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断VPN虚拟网卡提供的网络通道。

[0106] 其中，第一控制模块402还适于在第一检测模块401检测到目标加速应用结束前台

运行时，恢复VPN虚拟网卡提供的网络通道。

[0107] 其中，本实施例的网络控制装置还可以包括：通话控制模块，适于在第一侧模块401检测到目标加速应用在前台运行时，拦截来自拦截列表中记录的号码的电话和短消息；并将拦截的电话和短消息的信息以悬浮窗形式显示在显示界面。

[0108] 关于本实施例提供的网络控制装置的相关说明可以参照实施例一的网络控制方法的说明，故于此不再赘述。

[0109] 此外，本申请实施例还提供一种终端设备，包括：存储器、处理器以及存储在存储器上并在处理器上运行的网络控制程序，网络控制程序被处理器执行时实现实施例一所述的网络控制方法的步骤。

[0110] 实施例三

[0111] 本申请实施例提供一种网络控制方法，如图5所示，包括：

[0112] S501、终端设备检测前台运行的应用是否满足设定条件；

[0113] S502、在检测到前台运行的应用满足设定条件时，利用VPN阻断目标应用之外的应用的网络通信；其中，目标应用至少包括前台运行的应用。

[0114] 其中，前台运行的应用指用户在终端设备上正在操作的应用。

[0115] 本实施例中，终端设备可以包括诸如手机、平板电脑、笔记本电脑、掌上电脑、个人数字助理(Personal Digital Assistant，PDA)、便捷式媒体播放器(Portable Media Player，PMP)、可穿戴设备等移动终端，以及诸如数字TV、台式计算机等固定终端。然而，本申请对此并不限定。

[0116] 在示例性实施方式中，检测到前台运行的应用满足设定条件，可以包括以下至少之一：

[0117] 检测到前台运行的应用记录在网络加速应用列表中；

[0118] 检测到前台运行的应用消耗的历史数据流量满足第一条件；

[0119] 检测到前台运行的应用的历史使用时长满足第二条件。

[0120] 其中，可以通过第一条件筛选出数据流量消耗较大的应用，通过第二条件筛选出使用时长较长的应用。比如，第一条件可以包括：大于或等于第一阈值；第二条件可以包括大于或等于第二阈值。然而，本申请对此并不限定。第一条件和第二条件可以根据实际情况进行设置。

[0121] 在示例性实施方式中，在目标应用仅包括前台运行的应用时，在检测到前台运行的应用满足设定条件时，可以利用VPN阻断该前台运行的应用之外的应用的网络通信。

[0122] 在示例性实施方式中，目标应用可以包括：前台运行的应用以及记录在网络加速应用列表中的应用。换言之，在检测到前台运行的应用满足设定条件时，还可以利用VPN阻断网络加速应用列表中应用之外的应用的网络通信。比如，前台运行应用为应用A，网络加速应用列表中记录有应用A、应用B及应用C；在已启动应用包括应用A、应用B、应用D及应用E的情况下，可以利用VPN阻断应用B、应用D及应用E的网络通信，使得应用A可以独享所有带宽；或者，也可以利用VPN仅阻断应用D和应用E的网络通信，使得应用A和应用B分享带宽，避免应用D和应用E对应用A使用过程的干扰。

[0123] 在示例性实施方式中，目标应用可以包括：前台运行的应用以及与前台运行的应用存在关联的应用。其中，可以根据用户设置的信息确定与前台运行的应用存在关联的应

用，或者，可以根据应用之间的调用关系确定与前台运行的应用存在关联的应用。本申请对此并不限定。

[0124] 在示例性实施方式中，利用VPN阻断目标应用之外的应用的网络通信，可以包括：

[0125] 控制目标应用采用物理网卡提供的网络通道进行网络通信；

[0126] 控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断VPN虚拟网卡提供的网络通道。

[0127] 其中，本实施例的方法还可以包括：在检测到满足设定条件的应用结束前台运行时，恢复VPN虚拟网卡提供的网络通道。

[0128] 关于利用VPN阻断相关应用的网络通信的说明可以参照实施例一所述，故于此不再赘述。

[0129] 另外，在本实施例中也可以进行电话和短消息的拦截处理，相关说明可以参照实施例一所述，故于此不再赘述。

[0130] 此外，本实施例还提供一种网络控制装置，如图6所示，包括：

[0131] 第二检测模块601，适于检测前台运行的应用是否满足设定条件；

[0132] 第二控制模块602，适于在第二检测模块601检测到前台运行的应用满足设定条件时，利用VPN阻断目标应用之外的应用的网络通信；其中，目标应用至少包括前台运行的应用。

[0133] 其中，第二检测模块601可以适于通过以下至少之一方式检测到前台运行的应用满足设定条件：

[0134] 检测到前台运行的应用记录在网络加速应用列表中；

[0135] 检测到前台运行的应用消耗的历史数据流量满足第一条件；

[0136] 检测到前台运行的应用的历史使用时长满足第二条件。

[0137] 其中，第二控制模块602可以适于通过以下方式利用VPN阻断目标应用之外的应用的网络通信：

[0138] 控制目标应用采用物理网卡提供的网络通道进行网络通信；

[0139] 控制目标应用之外的应用采用VPN虚拟网卡提供的网络通道进行网络通信，并暂时阻断VPN虚拟网卡提供的网络通道。

[0140] 其中，第二控制模块602还可以适于在第二检测模块601检测到满足设定条件的应用结束前台运行时，恢复VPN虚拟网卡提供的网络通道。

[0141] 关于本实施例提供的网络控制装置的相关说明可以参照本实施例的网络控制方法的说明，故于此不再赘述。

[0142] 此外，本实施例还提供一种终端设备，包括：存储器、处理器以及存储在存储器上并在处理器上运行的网络控制程序，网络控制程序被处理器执行时实现本实施例的网络控制方法的步骤。

[0143] 实施例四

[0144] 本实施例提供一种网络控制方法，如图7所示，包括：

[0145] S701、确定目标软件运行；

[0146] S702、根据预设规则，控制目标软件之外的软件的网络通信状态，其中，网络通信状态包括网络通信速度或网络通信开关。

[0147] 其中，预设规则可以包括：目标软件在前台运行时，控制目标软件之外的软件的网络通信状态。然而，本申请对此并不限定。比如，预设规则可以包括：在目标软件运行时长大于或等于时长阈值时，控制目标软件之外的软件的网络通信状态；或者，在目标软件消耗的数据流量大于或等于流量阈值时，控制目标软件之外的软件的网络通信状态。

[0148] 在示例性实施方式中，S702中，控制目标软件之外的软件的网络通信状态，可以包括：利用VPN控制目标软件之外的软件的网络通信状态。比如，可以采用如实施例一所述的方式利用VPN控制目标软件(比如，实施例一中的目标加速应用)之外的软件的网络通信开关。关于利用VPN控制网络通信开关的实现方式如实施例一所述，故于此不再赘述。

[0149] 在示例性实施方式中，在S702中，还可以控制目标软件之外的软件的网络通信速度，比如，减少或降低目标软件之外的软件占用的网络带宽，以确保目标软件流畅运行。

[0150] 本实施例还提供一种网络控制装置，包括：

[0151] 第三检测模块，适于确定目标软件运行；

[0152] 第三控制模块，适于根据预设规则，控制目标软件之外的软件的网络通信状态，其中，网络通信状态包括网络通信速度或网络通信开关。

[0153] 关于本实施例的网络控制装置的说明可以参照本实施例的方法描述，故于此不再赘述。

[0154] 本实施例还提供一种设备，包括：存储器、处理器以及存储在存储器上并在处理器上运行的网络控制程序，网络控制程序被处理器执行时实现本实施例的网络控制方法的步骤。

[0155] 此外，本申请实施例还提供一种计算机可读介质，存储有网络控制程序，所述网络控制程序被处理器执行时实现上述实施例一或实施例三或实施例四所述的网络控制方法的步骤。

[0156] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块/单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块/单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器，如数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0157] 以上显示和描述了本申请的基本原理和主要特征和本申请的优点。本申请不受上述实施例的限制，上述实施例和说明书中描述的只是说明本申请的原理，在不脱离本申请

精神和范围的前提下,本申请还会有各种变化和改进,这些变化和改进都落入要求保护的本申请范围内。

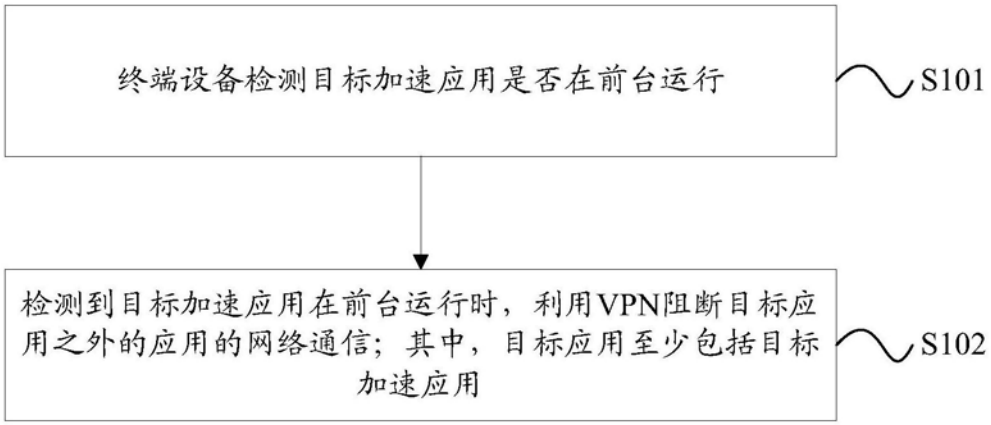

终端设备检测目标加速应用是否在前台运行
S101
检测到目标加速应用在前台运行时，利用VPN阻断目标应用之外的应用的网络通信；其中，目标应用至少包括目标加速应用
S102

图1

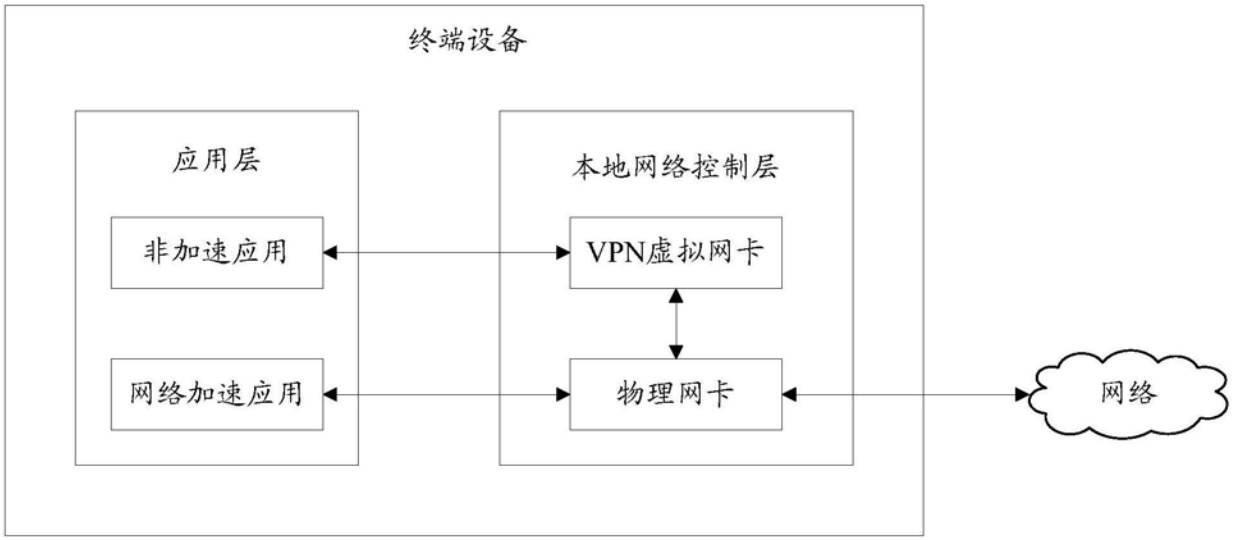

终端设备
应用层
非加速应用
网络加速应用
本地网络控制层
VPN虚拟网卡
物理网卡
网络

图2

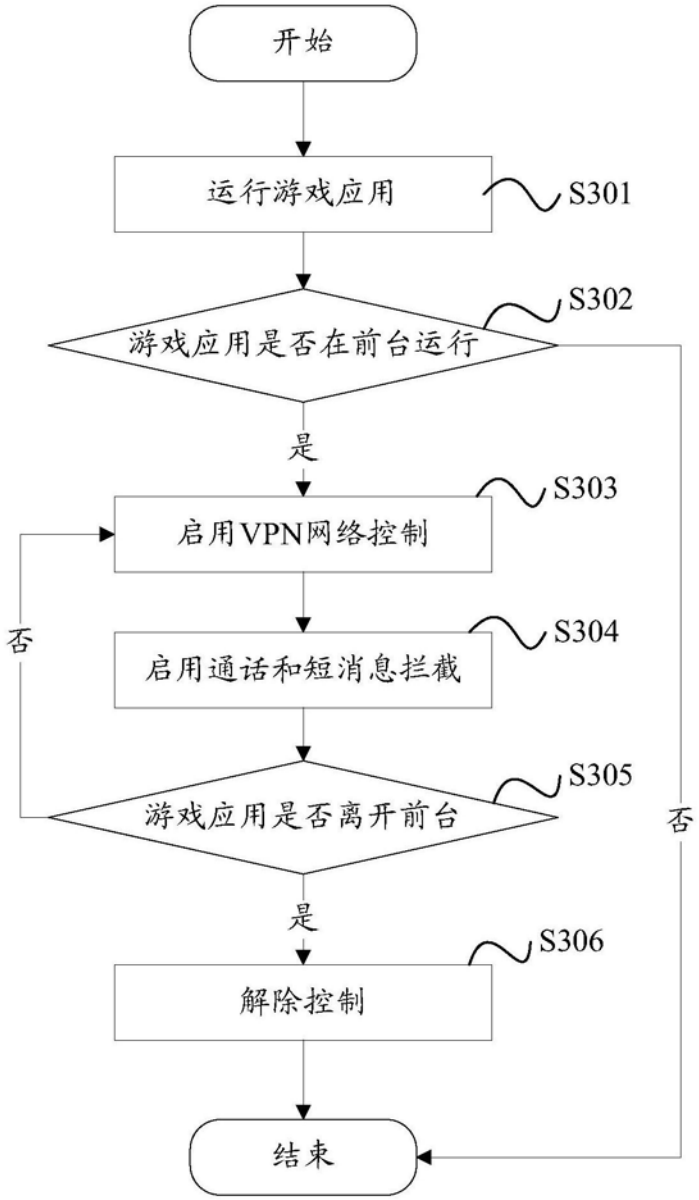

开始
运行游戏应用
S301
游戏应用是否在前台运行
S302
是
否
启用VPN网络控制
S303
启用通话和短消息拦截
S304
游戏应用是否离开前台
S305
是
否
解除控制
S306
结束

图3

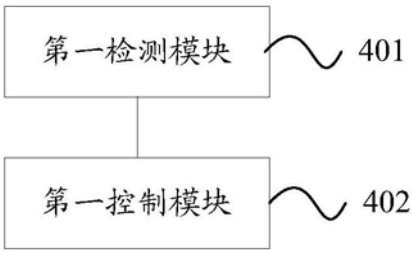

第一检测模块
401
第一控制模块
402

图4

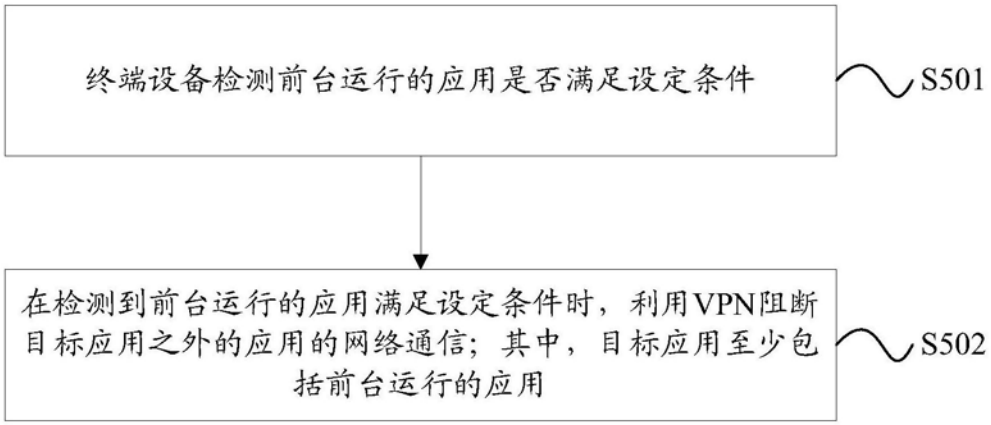

终端设备检测前台运行的应用是否满足设定条件
S501
在检测到前台运行的应用满足设定条件时，利用VPN阻断目标应用之外的应用的网络通信；其中，目标应用至少包括前台运行的应用
S502

图5

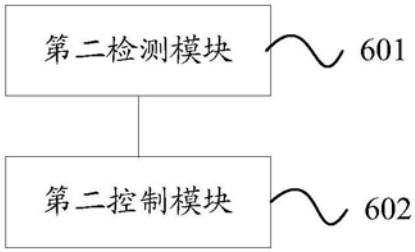

第二检测模块
601
第二控制模块
602

图6

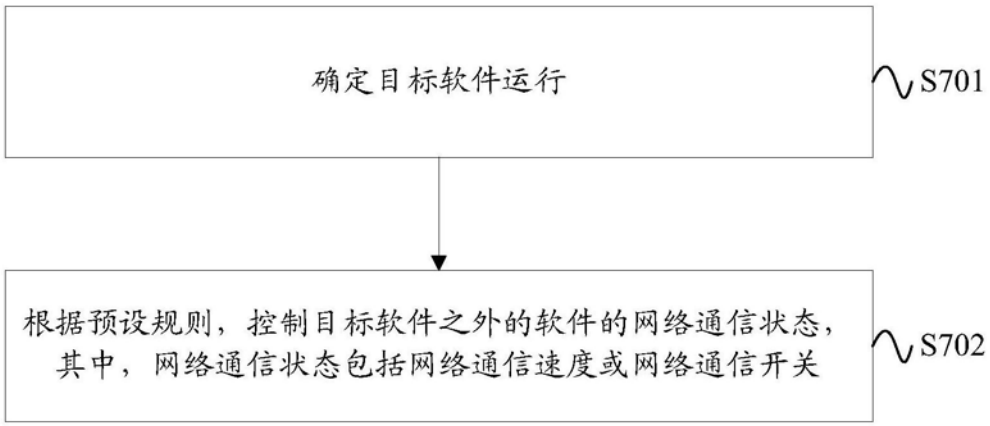

确定目标软件运行
S701
根据预设规则，控制目标软件之外的软件的网络通信状态，其中，网络通信状态包括网络通信速度或网络通信开关
S702

图7