

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2014年10月16日 (16.10.2014)



(10) 国际公布号
WO 2014/166065 A1

- (51) 国际专利分类号:
H04L 12/26 (2006.01) H04L 12/70 (2013.01)
H04L 12/24 (2006.01)
- (21) 国际申请号: PCT/CN2013/073973
- (22) 国际申请日: 2013年4月9日 (09.04.2013)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。
- (72) 发明人: 胡杰晖 (HU, Jiehui); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 杨杰 (YANG, Jie); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 吴小前 (WU, Xiaoqian); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王

歆平 (WANG, Xinping); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

- (74) 代理人: 北京中博世达专利商标代理有限公司 (BEIJING ZBSD PATENT&TRADEMARK AGENT LTD.); 中国北京市海淀区大柳树路 17 号富海大厦 B 座 501 室, Beijing 100081 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA,

[见续页]

(54) Title: METHOD AND DEVICE FOR PROTECTING SERVICE RELIABILITY, AND NETWORK VIRTUALIZATION SYSTEM

(54) 发明名称: 保护业务可靠性的方法、设备及网络虚拟化系统

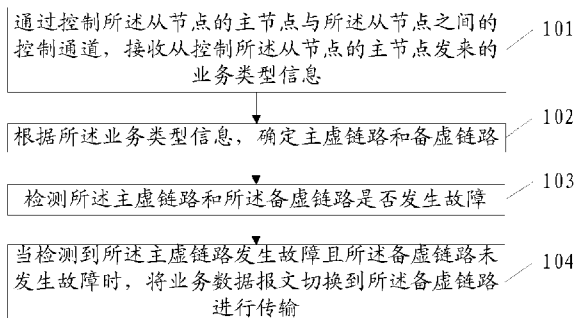


图 2 /Fig.2

- 101 Receiving service type information sent from a master node for controlling a slave node through a control passage between the master node and the slave node
- 102 Determining a main virtual link and a standby virtual link in accordance with the service type information
- 103 Detecting whether the main virtual link and the standby virtual link have failed or not
- 104 When it is detected that the main virtual link has failed and the standby virtual link has not failed, switching a service data message to the standby virtual link for transmission

(57) Abstract: Disclosed are a method and device for protecting service reliability, and a network virtualization system, relating to the technical field of communications and being capable of ensuring the protection of the service reliability in the network virtualization system provided in the present invention. In one embodiment of the present invention, a master node with a control function acquires current service type information and informs a slave code of the current service type information so that the slave code can determine a main virtual link and a standby virtual link in accordance with the service type information and conduct failure detection. When it is detected that the main virtual link has failed and the standby virtual link has not failed, a service data message is switched to the standby virtual link for transmission, in order to ensure that the uninterrupted transmission of the service data message is realized in a brand new system framework provided in the present invention, thus ensuring the service reliability.

(57) 摘要:

[见续页]

WO 2014/166065 A1



RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG,

CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明公开了一种保护业务可靠性的方法、设备以及网络虚拟化系统，涉及通信技术领域，能够保证在本发明提供的网络虚拟化系统中的业务可靠性保护。在本发明一种实施方式中具有控制功能的主节点获取当前业务类型信息并将当前业务类型信息告知从节点以使得从节点能够根据业务类型信息来确定主虚链路和备虚链路并进行故障检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输，用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输，进而保证了业务可靠性。

保护业务可靠性的方法、设备及网络虚拟化系统

技术领域

本发明涉及通信技术领域，尤其涉及一种保护业务可靠性的方法、设备及网络虚拟化系统。

背景技术

基站回传是指集中在基站(BTS)与基站控制器(BSC)之间的传送网络，称之为 RAN(Radio Access Network)。IPRAN 是针对基站回传应用场景进行优化定制的路由器/交换机整体解决方案，具备电路仿真、同步等能力。IPRAN 承载方案是在城域内汇聚层（汇聚层也可以叫做核心层）采用 IP/MPLS 技术，接入层主要采用增强以太技术或与 IP/MPLS 技术相结合的方案。核心汇聚节点采用的设备为支持 IP/MPLS 的路由器，基站接入节点采用的设备为路由器或三层交换机。

目前 IPRAN 的解决方案配置管理复杂，因此需要较多的初始配置，并在业务发放前进行针对诸如 CSG 的业务 IP，IGP 域的规划；在日常的维护中，仍然需要依靠人工干预来完成设备配置调整，尚无法实现自动化。随着网络规模、业务量和用户数的不断增长，这方面的问题会愈加突出。将网络虚拟化应用于 IPRAN 可以简化配置和管理，快速开通业务，同时，也需要为 IPRAN 提供相应的业务可靠性保护方案。

发明内容

本发明的实施例提供一种保护业务可靠性的方法、设备及网络虚拟化系统，实现对业务的可靠性保护。

为达到上述目的，本发明的实施例采用如下技术方案：

第一方面，本发明实施例提供一种保护业务可靠性的方法，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的

主主节点之间设置有第一虚链路,所述从节点和控制所述从节点的备主节点之间设置有第二虚链路,该方法包括:

所述从节点通过控制所述从节点的主节点与所述从节点之间的控制通道,接收从控制所述从节点的主节点发来的业务类型信息,所述业务类型信息包括 L2VPN 和 L3VPN;

所述从节点根据所述业务类型信息,确定主虚链路和备虚链路;其中,所述主虚链路为所述第一虚链路和第二虚链路中的一条虚链路,所述主虚链路用于传输业务数据报文的虚链路,所述备虚链路为所述第一虚链路和第二虚链路中除所述主虚链路之外的另一条虚链路;

所述从节点检测所述主虚链路和所述备虚链路是否发生故障;

当检测到所述主虚链路发生故障且所述备虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路进行传输。

结合第一方面,在第一种可能的实现方式中,所述根据业务类型信息,确定主虚链路和备虚链路包括:

当业务类型为 L2VPN 时,所述从节点将所述第一虚链路设置为主虚链路,并将所述第二虚链路设置为备虚链路;

或者,当业务类型为 L2VPN 时,所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息,确定主虚链路和备虚链路;

或者,当业务类型为 L3VPN 时,所述从节点将所述第一虚链路设置为主虚链路,并将所述第二虚链路设置为备虚链路;

或者,当业务类型为 L3VPN 时,所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息,确定主虚链路和备虚链路,所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由状态信息,所述外连接接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

结合第一方面的第一种可能的实现方式，在第二种可能的实现方式中，所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点发送的状态信息，确定主虚链路和备虚链路包括：

通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的状态信息；

通过所述备注节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的状态信息；

当接收到从所述主主节点发送的状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，当接收到从所述备主节点发来的状态信息为 Standby 待机状态时，则所述从节点将所述第二虚链路设置为备虚链路；

或者，当接收到从所述主主节点发送的状态信息为 Standby 时，则所述从节点所述第一虚链路设置为备虚链路，当接收到从所述备主节点发来的状态信息为 Active 时，则所述从节点所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

结合第一方面的第一种可能的实现方式，在第三种可能的实现方式中，所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路包括：

通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的接口路由状态信息；

通过所述备主节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的接口路由状态信息；

当接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文；当接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态，则所述从节点将第二虚链路设置为备虚链路；

或者，当接收到从所述主主节点发送的接口路由状态信息为 Standby

待机状态时,所述从节点将所述第一虚链路设置为备虚链路,当接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态,则所述从节点所述第二虚链路设置为主虚链路,并在所述第二虚链路上传输业务数据报文。

结合第一方面或第一方面的前三种可能的实现方式,在第四种可能的实现方式中,还包括:

当检测到所述主虚链路故障恢复正常时,所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

结合第一方面的第四种可能的实现方式,在第五种可能的实现方式中,所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输包括:在预设时间内,所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文,并通过所述备虚链路传输上行业务数据报文,在所述预设时间后,所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

结合第一方面或第一方面的前五种可能的实现方式,在第六种可能的实现方式中,所述从节点检测所述主虚链路和所述备虚链路是否发生故障包括:

当所述业务类型信息为 L2VPN 时,所述从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路,以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路;相应地,当检测到所述主虚链路发生故障且所述备虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路进行传输包括:当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路传输;

或者,当所述业务类型信息为 L3VPN 时,所述从节点启动对网络虚拟

化系统内部的虚链路进行故障检测,所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路;相应地,当检测到所述主虚链路发生故障且所述备虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路进行传输包括:当检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路传输。

结合第一方面或第一方面的前五种可能的实现方式,在第七种可能的实现方式中,所述从节点检测所述主虚链路和所述备虚链路是否发生故障包括:

当所述业务类型信息为 L2VPN 时,所述从节点通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令,所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路,以及与控制所述从节点的主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路;

所述从节点根据所述使能故障检测配置命令,启动对端到端虚链路进行故障检测;相应地,当检测到所述主虚链路发生故障且所述备虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路进行传输包括:当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路传输。

第二方面,本发明实施例提供了一种保护业务可靠性的方法,应用于基于控制和转发分离的网络虚拟化系统中,所述网络虚拟化系统包括主节点和从节点,从节点被一对互为主备的主节点控制,所述一对互为主备的主节点包括一个主主节点和一个备主节点,所述从节点和控制所述从节点

的主主节点之间设置有第一虚链路,所述从节点和控制所述从节点的备主节点之间设置有第二虚链路,该方法包括:

主节点获取业务类型信息,所述业务类型信息包括 L2VPN 和 L3VPN;

通过主节点以及所述主节点控制的从节点之间的控制通道,向所述主节点控制的从节点发送业务类型信息,以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路,并对确定好的主虚链路和备虚链路进行故障检测。

结合第二方面,在第一种可能的实现方式中,所述主节点获取业务类型信息包括:

为所述主节点控制的从节点的外连接接口建立对应的虚拟远端逻辑接口,所述外连接接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口;

在所述虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务,并获取与配置的业务相应的业务类型信息。

结合第二方面的第一种可能的实现方式,在第二种可能的实现方式中,在向所述从节点发送业务类型信息之后,还包括:

向所述主节点控制的从节点发送使能故障检测配置命令,以使得所述主节点控制的从节点根据所述使能故障检测配置命令,启动对端到端虚链路进行故障检测;其中,所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指从节点到主节点之间的在网络虚拟化系统内部的虚链路,以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

结合第二方面或第二发明的前两种可能的实现方式,在第三种可能的实现方式中,在向所述主节点控制的从节点发送业务类型信息之后,还包括:

所述主节点接收 RSG 发送的状态信息,所述状态信息包括 Active 和 Standby;

所述主节点将所述状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

结合第二方面或第二发明的前两种可能的实现方式，在第四种可能的实现方式中，在向所述从节点发送业务类型信息之后，还包括：

当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时，则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低，并获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级，所述另一个主节点和所述主节点互为主备关系；

当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过与所述主节点控制的从节点之间的控制通道，发送至所述主节点控制的从节点。

第三方面，本发明提供一种从节点，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，所述从节点包括：

接收单元，用于通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；

确定单元，用于根据所述接收单元接收的业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路与所述第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路与所述第二虚链路中除所述主虚链路之外的另一条虚链

路；

检测单元，用于检测所述确定单元确定的主虚链路和备虚链路是否发生故障；

切换单元，用于当所述检测单元检测到所述主虚链路发生故障且所述备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输。

结合第三方面，在第一种可能的实现方式中，所述确定单元用于当业务类型为 L2VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；还用于当业务类型为 L2VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息，确定主虚链路和备虚链路；还用于当业务类型为 L3VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；还用于当业务类型为 L3VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路，所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由状态信息，所述外连接接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

结合第三方面的第一种可能的实现方式，在第二种可能的实现方式中，所述确定单元包括：

第一接收模块，用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的状态信息；

所述第一接收模块，还用于通过所述备注节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的状态信息；

确定模块，当所述第一接收模块接收到从所述主主节点发送的状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，并当所述第一接收模块接收到从所述备主节点发来的状态信息为 Standby 待机状态时，则将所述第二虚

链路设置为备虚链路;还用于当所述第一接收模块接收到从所述主主节点发送的状态信息为 Standby 时,则将所述第一虚链路设置为备虚链路,并当所述第一接收模块接收到从所述备主节点发来的状态信息为 Active 时,则将所述第二虚链路设置为主虚链路,并在所述第二虚链路上传输业务数据报文。

结合第三方面的第一种可能的实现方式,在第三种可能的实现方式中,所述确定单元包括:

第二接收模块,用于通过所述主主节点和所述从节点之间的控制通道,所述从节点接收所述主主节点发送的接口路由状态信息;

所述第二接收模块,还用于通过所述备主节点和所述从节点之间的控制通道,所述从节点接收所述备主节点发送的接口路由状态信息;

设置模块,用于当所述第二接收模块接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时,所述从节点将所述第一虚链路设置为主虚链路,并在所述第一虚链路上传输业务数据报文,并当所述第二接收模块接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态,则将第二虚链路设置为备虚链路;还用于当接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时,将所述第一虚链路设置为备虚链路;并当所述第二接收模块接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态,则将所述第二虚链路设置为主虚链路,并在所述第二虚链路上传输业务数据报文。

结合第三方面或第三方面的前三种可能的实现方式,在第四种可能的实现方式中,所述切换单元还用于当所述检测单元检测到所述主虚链路故障恢复正常时,将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

结合第三方面的第四种可能的实现方式,在第五种可能的实现方式中,所述切换单元用于在预设时间内,所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文,并通过所述备虚链路传输

上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

结合第三方面或第三方面的前五种可能的实现方式，在第六种可能的实现方式中，所述检测单元用于当所述接收单元接收到的业务类型信息为L2VPN时，启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关RSG之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；

则所述切换单元，用于当所述检测单元检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输；

或者，所述检测单元用于当所述接收单元接收到的业务类型信息为L3VPN时，启动对网络虚拟化系统内部的虚链路进行故障检测，所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路。

则所述切换单元，用于当所述检测单元检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

结合第三方面或第三方面的前五种可能的实现方式，在第七种可能的实现方式中，所述检测单元用于当所述接收单元接收到的业务类型信息为L2VPN时，通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令，所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内

部的虚链路,以及与控制所述从节点的主节点到RSG之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路;根据所述接收单元接收到的使能故障检测配置命令,启动对端到端虚链路进行故障检测;

则所述切换单元,用于当所述检测单元检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时,所述从节点将业务数据报文切换到所述备虚链路传输。

第四方面,本发明实施例提供了一种主节点,应用于基于控制和转发分离的网络虚拟化系统中,所述网络虚拟化系统包括主节点和从节点,从节点被一对互为主备的主节点控制,所述一对互为主备的主节点包括一个主主节点和一个备主节点,所述从节点和控制所述从节点的主主节点之间设置有第一虚链路,所述从节点和控制所述从节点的备主节点之间设置有第二虚链路,,其中,所述主节点包括:

第一获取单元,用于获取业务类型信息,所述业务类型信息包括L2VPN和L3VPN;

发送单元,用于通过主节点以及所述主节点控制的从节点之间的控制通道,向所述主节点控制的从节点发送所述第一获取单元获取到的业务类型信息,以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路,并对确定好的主虚链路和备虚链路进行故障检测。

结合第四方面,在第一种可能的实现方式中,所述第一获取单元包括:

建立模块,用于所述主节点控制的从节点的外接口建立对应的虚拟远端逻辑接口,所述外接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口;

配置模块,用于在所述建立模块建立的虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务;

获取模块,用于获取与配置的业务取相应的业务类型信息。

结合第四方面的第一种可能的实现方式,在第二种可能的实现方式

中,所述发送单元还用于向所述主节点控制的从节点发送使能故障检测配置命令,以使得所述主节点控制的从节点根据所述使能故障检测配置命令,启动对端到端虚链路进行故障检测;其中,所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指从节点到主节点之间的在网络虚拟化系统内部的虚链路,以及与主节点到RSG之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

结合第四方面或第二发明的前两种可能的实现方式,在第三种可能的实现方式中,还包括:

接收单元,用于接收RSG发送的状态信息,所述状态信息包括Active和Standby;

所述发送单元,用于将所述接收单元接收到的状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

结合第四方面或第二发明的前两种可能的实现方式,在第四种可能的实现方式中,还包括:

设置单元,用于当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时,则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低;

第二获取单元,用于获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级,所述另一个主节点和所述主节点互为主备关系;

所述发送单元,用于当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时,将Standby状态携带在接口路由状态信息中,通过所述与所述主节点控制的从节点之间的控制通道,发送至所述主节点控制的从节点。

第五方面,本发明提供了一种网络虚拟化系统,所述网络虚拟化系统

包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路；

其中，所述主节点获取业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送业务类型信息；

所述从节点通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；根据所述业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路和第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路和第二虚链路中除所述主虚链路之外的另一条虚链路；检测所述主虚链路和所述备虚链路是否发生故障；当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，将业务数据报文切换到所述备虚链路进行传输。

本发明实施例提供的一种保护业务可靠性的方法、设备及网络虚拟化系统，在基于控制与转发分离的网络虚拟化系统中，具有控制功能的主节点获取当前业务类型信息并将当前业务类型信息告知从节点以使得从节点能够根据业务类型信息来确定主虚链路和备虚链路并进行故障检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输，用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输，进而保证了业务可靠性。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员

来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例提供的一种基于控制和转发分离的网络虚拟化系统的架构示意图；

图 2 为本发明实施例提供的一种保护业务可靠性的方法流程图；

图 3 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 4 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 5 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 6 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 7 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 8 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 9 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 10 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 11 为通过 L2VPN 承载 TDM 或 ATM 业务的可靠性场景示意图；

图 12 为通过 L3VPN 承载 ETH 业务的可靠性场景示意图；

图 13 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 14 为本发明实施例提供的另一种保护业务可靠性的方法流程图；

图 15 为本发明实施例提供的一种从节点的组成框图；

图 16 为本发明实施例提供的另一种从节点的组成框图；

图 17 为本发明实施例提供的另一种从节点的组成框图；

图 18 为本发明实施例提供的一种主节点的组成框图；

图 19 为本发明实施例提供的另一种主节点的组成框图；

图 20 为本发明实施例提供的另一种主节点的组成框图；

图 21 为本发明实施例提供的另一种主节点的组成框图；

图 22 为本发明实施例提供的另一种从节点的组成框图；

图 23 为本发明实施例提供的另一种主节点的组成框图。

具体实施方式

下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

本发明提供了一种基于控制和转发分离的网络虚拟化系统,图 1 为该系统实体架构的示意图,在此网络虚拟化系统中包括若干个主节点(图 1 中为 A, B, C, D 共四个主节点)和若干个从节点(图 1 中共 13 个从节点),各个主节点和从节点可按照如图 1 所示的连接方式通过实际物理信道进行连接通信。只有主节点可以设置有控制功能以及转发功能,而从节点则只具有转发功能。当然,为了控制方便,每个主节点的控制功能可以集成在同一个高层设备中进行统一管理。

每个从节点都被一对互为主备的主节点控制,在图 1 中表示为 A/B, B/C, B/D 和 A/D。分别表示由主节点 A 和 B 进行控制,由主节点 B 和 C 进行控制,由主节点 B 和 D 进行控制,由主节点 A 和 D 进行控制。所述一对互为主备的主节点包括一个主主节点和一个备主节点,所述从节点和控制所述从节点的主主节点之间设置有第一虚链路,所述从节点和控制所述从节点的备主节点之间设置有第二虚链路。第一虚链路和第二虚链路均为虚拟逻辑信道,在图 1 中并未示出。其中,可将第一虚链路的转发优先级初始化高于第二虚链路的转发优先级,其目的在于从节点在确定当前业务类型进行主、备虚链路初始化时,可以优先选择第一虚链路为主虚链路,选择第二虚链路为备虚链路。当然,这种初始化设定可以根据实际需要另行设置。在此网络虚拟化系统中并不限定每个从节点必须要设置有独立的主主节点和备主节点,也就是说,同一个主节点既可以作为一个从节点的主主节点,同时也可以作为另一个从节点的备主节点。

基于上述基于控制和转发分离的网络虚拟化系统,本发明实施例提供了一种保护业务可靠性的方法,如图 2 所示,可由从节点来实现,包括:

101、所述从节点通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息。

其中，所述业务类型信息包括 L2VPN (layer 2 virtual private network, 二层虚拟私有网络) 和 L3VPN (layer 3 virtual private network, 三层虚拟私有网络)。

102、所述从节点根据所述业务类型信息，确定主虚链路和备虚链路。

其中，所述主虚链路为所述第一虚链路与所述第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路与所述第二虚链路中除所述主虚链路之外的另一条虚链路。

值得说明的是，为方便从节点后续工作，在本实施例中，一般会使用激活状态 Active 来标识第一虚链路为主虚链路，使用待机状态 Standby 来标识第二虚链路为备虚链路。

针对不同的业务类型信息，本发明实施例对如何实现步骤 102、根据业务类型信息，确定主虚链路和备虚链路提供了相应的具体实施方式，具体如下：

针对 L2VPN 这种业务类型信息，本发明实施例提供了两种具体实施方式，包括：

第一种实施方式：将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路。

第二种实施方式：根据控制所述从节点的主节点和控制所述从节点的备主节点各自发送的状态信息，确定主虚链路和备虚链路。

针对 L2VPN 的第一种实施方式一般可以作为初始化设置，应用在网络虚拟化系统组网时期。而针对 L2VPN 的第二种实施方式可以使用在网络虚拟化系统运行的各个阶段。

其中，上述针对 L2VPN 的第二种实施方式的具体实现步骤可参照如图 3 所示的方法流程，具体包括；

A1021、通过所述主节点和所述从节点之间的控制通道，所述从节

点接收所述主主节点发送的状态信息。

其中,所述主主节点和从节点之间的控制通道是独立于主主节点和从节点之间的业务数据信道外的另一个信道。

A1022、通过所述备注节点和所述从节点之间的控制通道,所述从节点接收所述备主节点发送的状态信息。并执行 A1023 或者执行 A1024。

其中,所述备主节点和从节点之间的控制通道是独立于备主节点和从节点之间的业务数据信道外的另一个信道

A1023、当接收到从所述主主节点发送的状态信息为 Active 激活状态时,所述从节点将所述第一虚链路设置为主虚链路,并在所述第一虚链路上传输业务数据报文,当接收到从所述备主节点发来的状态信息为 Standby 待机状态时,则将所述第二虚链路设置为备虚链路。

A1024、当接收到从所述主主节点发送的状态信息为 Standby 时,则所述从节点将所述第一虚链路设置为备虚链路,当接收到从所述备主节点发来的状态信息为 Active 时,则将所述第二虚链路设置为主虚链路,并在所述第二虚链路上传输业务数据报文。

在上述步骤 A1023 和 A1024 中,Active 激活状态用于表示发送此状态信息的主节点处于正常运行状态。Standby 待机状态用于表示发送此状态信息的从节点处于暂停工作状态。

而针对 L3VPN 这种业务类型信息,本发明实施例提供了两种具体实施方式,包括:

第一种实施方式:所述从节点将所述第一虚链路设置为主虚链路,并将所述第二虚链路设置为备虚链路。

第二种实施方式:根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息,所述从节点确定主虚链路和备虚链路。

其中,所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由信息,所述

外连接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的其它网络设备相连接的接口。

针对 L3VPN 的第一种实施方式一般可以作为初始化设置, 应用在网络虚拟化系统组网时期。而针对 L3VPN 的第二种实施方式可以使用在网络虚拟化系统运行的各个阶段, 当然在在网络虚拟化系统运行 L3VPN 的各个阶段中, 也可以按照初始化设置维持主虚链路和备虚链路的配置不变。

其中, 针对 L3VPN 的上述第二种实施方式的具体实现步骤可参照如图 4 所示的方法流程, 具体包括;

B1021、通过所述主主节点和所述从节点之间的控制通道, 所述从节点接收所述主主节点发送的接口路由状态信息。

B1022、通过所述备主节点和所述从节点之间的控制通道, 所述从节点接收所述备主节点发送的接口路由状态信息。并执行步骤 B1023 或步骤 B1024。

B1023、当接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时, 所述从节点将所述第一虚链路设置为主虚链路, 并在所述第一虚链路上传输业务数据报文; 当接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态, 则所述从节点将第二虚链路设置为备虚链路。

其中, 值得说明的是, 当某一主主节点的接口路由状态信息为 Active 激活状态表示所述主主节点上的虚拟远端逻辑接口的路由优先级高于与所述主主节点对应的备主节点上的虚拟远端逻辑接口的路由优先级。

当某一备主节点的接口路由状态信息为 Standby 待机状态表示所述备主节点上的虚拟远端逻辑接口的路由优先级低于与所述备主节点对应的主主节点上的虚拟远端逻辑接口的路由优先级。

B1024、当接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时, 所述从节点将所述第一虚链路设置为备虚链路, 当接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态, 则

将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

103、所述从节点检测所述主虚链路和所述备虚链路是否发生故障。

其中，从节点检测所述主虚链路和所述备虚链路是否发生故障的方法可以使用对主虚链路和备虚链路进行 BFD (Bidirectional Forwarding Detection, 双向转发检测) 检测来实现。

104、当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输。

本发明实施例提供了一种保护业务可靠性的方法，在本发明提供的基于控制与转发分离的网络虚拟化系统中，从节点通过对已确定好的主虚链路和备虚链路进行检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输，用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输，进而保证了业务可靠性。

进一步值得说明的是，如图 5 所示，在执行了步骤 104 之后，还可以执行步骤 105、当检测到所述主虚链路故障恢复正常时，所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

进一步的，在执行上述步骤 105 时，从节点不需要经过主节点或备主节点的同意，可根据自己做出的判断直接进行主、备虚链路之间的切换，但是当主虚链路回复正常时，此时备虚链路也处于正常工作状态，因此，这两个虚链路可以同时传输下行业务数据报文。

为了保证业务数据报文传输不中断和不丢失，当业务数据报文传输量较少，从节点可以直接将业务数据报文切换回主虚链路进行传输。

当业务数据报文传输量较多时，在预设时间内，所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文，并通过所述备虚链路传输上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

其中，预设时间为经验值，例如 300ms 等，可以预先设定。

值得说明的是，在执行所述步骤 103 时，本发明实施例针对不同的业务类型信息还提供了以下三种故障检测的启动方法，包括：

第一种启动方法：当所述业务类型信息为 L2VPN 时，所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

相应地，所述步骤 104 当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输的实现方法包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

第二种启动方法：当所述业务类型信息为 L3VPN 时，所述从节点启动对网络虚拟化系统内部的虚链路进行故障检测，所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路。

相应地，所述步骤 104 当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输的实现方法包括：当检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

第三种启动方法：当所述业务类型信息为 L2VPN 时，从节点通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令，所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到主节点之间的在网络虚拟化系统内部的虚链路，以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；根据所述使能

故障检测配置命令，启动对端到端虚链路进行故障检测。

相应地，所述步骤 104 当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输的实现方法包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

基于上述基于控制和转发分离的网络虚拟化系统，本发明实施例提供了一种保护业务可靠性的方法，如图 6 所示，可由主节点来实现，包括：

201、获取业务类型信息。

其中，所述业务类型信息包括 L2VPN 和 L3VPN。

其中，主节点获取业务类型信息的方法可由如图 7 所示的方法流程实现，具体包括：

2011、为所述主节点控制的从节点的外连接接口建立对应的虚拟远端逻辑接口。

其中，所述外连接接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

2012、在所述虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务，并获取与配置的业务相应的业务类型信息。

202、通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送业务类型信息，以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路，并对确定好的主虚链路和备虚链路进行故障检测。

本发明实施例提供了一种保护业务可靠性的方法，在本发明提供的基于控制与转发分离的网络虚拟化系统中，具有控制功能的主节点获取当前业务类型信息并将当前业务类型信息告知从节点以使得从节点能够根据业务类型信息来确定主虚链路和备虚链路并进行故障检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚

链路进行传输,用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输,进而保证了业务可靠性。

可选的是,在执行所述步骤 202 之后,如图 8 所示,本发明实施例提供的方法还包括:

203、向所述主节点控制的从节点发送使能故障检测配置命令,以使得所述主节点控制的从节点根据所述使能故障检测配置命令,启动对端到端虚链路进行故障检测。

其中,所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指所述主节点控制的从节点到所述主节点之间的在网络虚拟化系统内部的虚链路,以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

通过执行步骤 203,本发明实施例提供的方法能够对从节点的故障检测的启动进行控制。值得说明的是,该步骤也可以设置为优先有主主节点来完成。

进一步的,在 L2VPN 业务类型下,为了能够对基于控制和转发分离的网络虚拟化系统外部的出现的问题进行响应,以保证业务数据报文的正常传输,如图 9 所示,该方法还包括:

204、所述主节点接收 RSG 发送的状态信息,所述状态信息包括 Active 和 Standby。

205、将所述状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

进一步的,在 L3VPN 业务类型下,若在主节点上的所述主节点控制的从节点对应的路由接口出现故障时,则需要告知所述主节点控制的从节点,以保证所述主节点控制的从节点及时调整主、备虚链路,如图 10 所示,该方法还包括:

206、当主节点检测到与所述主节点控制的从节点对应的接口路由发

生故障时,则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低,并获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级,所述另一个主节点和所述主节点互为主备关系。

其中,主节点降低优先级的方法,可以使用将接收对应的路由权值降低即可。

207、当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时,将 Standby 状态携带在接口路由状态信息中,通过与所述主节点控制的从节点之间的控制通道,发送至所述主节点控制的从节点。

另外,在此之后,若主节点检测到与所述从节点对应的接口路由之间的故障恢复,还可以将所述从节点在所述主节点上的虚拟远端逻辑接口的路由优先级提高,并将 Active 状态携带在接口路由状态信息中,通过所述与从节点之间的控制通道,发送至所述从节点。

基于前述如图 2 至图 5 所示的从节点方法以及如图 6 至图 10 所示的主节点的方法,本发明实施例在此结合如图 11 所示的通过 L2VPN 承载 TDM 或 ATM 业务的可靠性场景,以及如图 12 所示的通过 L3VPN 承载 TDM 或 ATM 业务的可靠性场景,分别具体描述本发明提供的技术方案。

在如图 11 所示的通过 L2VPN 承载 TDM (time division multiplexing, 时分复用) 或 ATM (asynchronous transfer mode, 异步传输模式) 业务的可靠性场景中,设置有一个从节点,负责控制该从节点的主主节点和备主节点,两个 RSG (如图 11 所示的 RSG1 和 RSG2), 一个 RNC, 从节点与主主节点和备主节点通过伪线进行业务数据传输, 主主节点与 RSG1 通过伪线连接, 备主节点与 RSG2 通过伪线连接, 两个 RSG 都与 RNC 相连。

在如图 12 所示的通过 L3VPN 承载 ETH (ethernet, 以太网) 业务的可靠性场景中,设置有一个从节点,负责控制该从节点的主主节点和备主

节点，两个 RSG（如图 12 所示的 RSG1 和 RSG2），一个 RNC，从节点与主主节点和备主节点通过伪线进行业务数据传输，主主节点和备主节点分别于 RSG1 和 RSG2 通过三层路由网络进行通信，两个 RSG 都与 RNC 相连。

结合图 11 所示的具体应用场景，本发明实施例提供了一种保护业务可靠性的方法，如图 13 所示，包括：

301、主主节点和备主节点分别为从节点的外连接口创建虚拟远端逻辑接口，并将网络虚拟化系统外 L2VPN 业务配置在该虚拟远端逻辑接口上。

302、主主节点和备主节点分别建立虚拟远端逻辑接口和从节点的外连接口之间点到点虚链路。

303、主主节点通过主主节点与所述从节点之间的控制通道，将业务类型发送至从节点。

304、所述从节点将所述第一虚链路设置为主虚链路，将所述第二虚链路设置为备虚链路，并启动对 RSG1 到所述主主节点之间的虚链路和 RSG2 到所述备主节点之间的虚链路以及所述主主节点与所述从节点之间的虚链路和所述备主节点与所述从节点之间的虚链路进行故障检测。

305、当 RSG1 检测到与 RNC 之间的链路发生故障，则向所述主主节点发送 Standby 状态信息，并向所述备主节点发送 Active 状态信息。

306、所述主主节点收到 Standby 状态信息后，通过控制信道向所述从节点发送 Standby 状态信息。所述备主节点收到 Active 状态信息后，通过控制信道向所述从节点发送 Active 状态信息。

307、所述从节点接收到所述主主节点发送的 Standby 状态信息和所述备主节点发送的 Active 状态信息后，将当前主虚链路设置为备虚链路，当前备虚链路设置为主虚链路。

此时，上行流量传输途径为：从节点将收到的业务数据报文传输至备主节点。再由备主节点发送至 RSG2，继而传送到 RNC。

下行流量传输途径为：RSG2 接收 RNC 发来的业务数据报文，发送至

备主节点，再由备主节点发送至从节点。

值得说明的是，在上述步骤 304 中，从节点根据业务类型为 L2VPN，直接启动对对 RSG1 到主主节点之间的虚链路和 RSG2 到备主节点之间的虚链路以及主主节点与从节点之间的虚链路和备主节点与从节点之间的虚链路进行故障检测。本发明实施例还提供了一种方法，在执行 304 之前，还可以由主主节点向从节点发送使能故障检测配置命令，从节点接收到此命令后，才启动故障检测。

结合图 12 所示的具体应用场景，本发明实施例提供了一种保护业务可靠性的方法，如图 14 所示，包括：

401、在所述主主节点和所述备主节点上分别为所述从节点的外连接接口创建虚拟远端逻辑接口，并将网络虚拟化系统外 L3VPN 业务配置在该虚拟远端逻辑接口上。

402、所述主主节点和所述备主节点分别建立虚拟远端逻辑接口和所述从节点的外连接接口之间点到点虚链路。

403、所述主主节点通过所述主主节点与所述从节点之间的控制通道，将业务类型发送至所述从节点。

此时，所述备注节点也可以发送相同的业务类型信息至所述从节点，所述从节点仍然根据所述主主节点发送的业务类型信息进行后续处理。

404、所述从节点将所述第一虚链路设置为主虚链路，将所述第二虚链路设置为备虚链路，并启动所述主主节点与所述从节点之间的虚链路和所述备主节点与所述从节点之间的虚链路进行故障检测。

405、当所述主主节点检测到与所述从节点对应接口路由发生故障，则将所述从节点与所述主主节点之间的虚拟远端逻辑接口的路由优先级降低。

406、确定降低后的路由优先级低于所述备主节点与所述主主节点之间的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过所述与从节点之间的控制通道，发送至所述从节点。

407、当所述备主节点确定从节点与所述主节点之间的虚拟远端逻辑接口的路由优先级低于自身与所述主节点之间的虚拟远端逻辑接口的路由优先级时，将 Active 状态携带在接口路由状态信息中，通过所述与从节点之间的控制通道，发送至所述从节点。

408、将第一虚链路设置为备虚链路，将第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

此时，上行流量传输途径为：从节点将收到的业务数据报文传输至备主节点。再由备主节点经过三层路由网络发送至 RSG1 或 RSG2，继而传送到 RNC。

下行流量传输途径为：RSG1 或 RSG2 接收 RNC 发来的业务数据报文，通过三层路由网络将接收到的业务数据报文发送至备主节点，再由备主节点发送至从节点。

值得说明的是，所述步骤 407 确定所述主虚链路的路由优先级低于所述备虚链路的路由优先级，可以不将当前主虚链路设置为备虚链路，当前备虚链路设置为主虚链路，而只是将上行业务数据报文发送至备主节点即可。

在执行所述步骤 407 之后，若主主节点上对应于所述从节点的接口路由恢复正常，则主主节点会重新对该接口路由的路由优先级进行设置，以使得其路由优先级能够重新高于或等于所述备主节点上的路由优先级，但在此过程中，主节点与 RSG 之间的三层路由网络的路由表等信息需要根据主主节点的路由优先级重新更新，这一过程需要一段时间。因此，为保证下行业务数据报文不中断，在此提供以下业务数据报文传输路径回切的步骤，包括：

上行业务数据报文传输路径回切：从节点等待 300s 后将上行业务数据报文从向备主节点发送变更为向主主节点发送。

下行业务数据报文传输路径回切，从节点同时主、备主节点发送的下行业务数据报文。在 300s 后将仅接收主主节点发送过来的下行业务数据

报文。

本发明实施例提供了一种保护业务可靠性的方法，在本发明提供的基于控制与转发分离的网络虚拟化系统中，具有控制功能的主节点获取当前业务类型信息并将当前业务类型信息告知从节点，从节点能够根据业务类型信息来确定主虚链路和备虚链路并进行故障检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输，用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输，进而保证了业务可靠性。

本发明实施例提供了一种从节点，可用于实现如图 2 至图 14 所示的所有从节点侧的方法流程，具体应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，其中，如图 15 所示，所述从节点包括：

接收单元 51，用于通过主节点与从节点之间的控制通道，接收从主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN。

确定单元 52，用于根据所述接收单元 51 接收的业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路与所述第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路与所述第二虚链路中除所述主虚链路之外的另一条虚链路。

检测单元 53，用于检测所述确定单元 52 确定的主虚链路和备虚链路是否发生故障。

切换单元 54，用于当所述检测单元 53 检测到所述主虚链路发生故障且所述备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输。

可选的是，所述确定单元 52 用于当业务类型为 L2VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；还用于当业务类型为 L2VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息，确定主虚链路和备虚链路；还用于当业务类型为 L3VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；还用于当业务类型为 L3VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路，所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由状态信息，所述外连接接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

可选的是，如图 16 所示，所述确定单元 52 包括：

第一接收模块 521，用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的状态信息。

所述第一接收模块 521，还用于通过所述备注节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的状态信息。

确定模块 522，当所述第一接收模块 521 接收到从所述主主节点发送的状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，并当所述第一接收模块 521 接收到从所述备主节点发来的状态信息为 Standby 待机状态时，则将所述第二虚链路设置为备虚链路；还用于当所述第一接收模块 521 接收到从主主节点发送的状态信息为 Standby 时，则将所述第一虚链路设置为备虚链路，当所述第一接收模块 521 接收到从所述主主节点发送的状态信息为 Standby 时，则将所述第一虚链路设置为备虚链路，并当所述第一接收模块 521 接收到从所述备主节点发来的状态信息为 Active 时，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

可选的是，如图 17 所示，所述确定单元 52 包括：

第二接收模块 523，用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的接口路由状态信息。

所述第二接收模块 524，还用于通过所述备主节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的接口路由状态信息。

设置模块 524，用于当所述第二接收模块 524 接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，并当所述第二接收模块 524 接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态，则将第二虚链路设置为备虚链路；还用于当所述第二接收模块接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时，将所述第一虚链路设置为备虚链路；并当所述第二接收模块 524 接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

可选的是，所述切换单元 54 还用于当所述检测单元检测到所述主虚链路故障恢复正常时，将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

可选的是，所述切换单元 54 用于在预设时间内，所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文，并通过所述备虚链路传输上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

可选的是，所述检测单元 53 用于当所述接收单元 51 接收到的业务类型信息为 L2VPN 时，启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

则所述切换单元 54, 用于当所述检测单元 53 检测到所述主虚链路发生故障且所述备虚链路未发生故障时, 所述从节点将业务数据报文切换到所述备虚链路进行传输包括: 当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时, 所述从节点将业务数据报文切换到所述备虚链路传输。

可选的是, 所述检测单元 53 用于当所述接收单元 51 接收到的业务类型信息为 L3VPN 时, 启动对网络虚拟化系统内部的虚链路进行故障检测, 所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路。

则所述切换单元 54, 用于当所述检测单元 53 检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时, 所述从节点将业务数据报文切换到所述备虚链路传输。

可选的是, 所述检测单元 53 用于当所述接收单元 51 接收的业务类型信息为 L2VPN 时, 通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令, 所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测, 所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路, 以及与控制所述从节点的主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路; 根据所述接收单元 51 接收到的使能故障检测配置命令, 启动对端到端虚链路进行故障检测。

则所述切换单元 54, 用于当所述检测单元 53 检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时, 所述从节点将业务数据报文切换到所述备虚链路传输。

本发明实施例还提供了一种主节点, 可用于实现如图 2 至图 14 所示的所有主节点侧的方法流程, 具体应用于基于控制和转发分离的网络虚拟化系统中, 所述网络虚拟化系统包括主节点和从节点, 从节点被一对互为

主备的主节点控制,所述一对互为主备的主节点包括一个主主节点和一个备主节点,所述从节点和控制所述从节点的主主节点之间设置有第一虚链路,所述从节点和控制所述从节点的备主节点之间设置有第二虚链路,,其中,如图 18 所示,所述主节点包括:

第一获取单元 61,用于获取业务类型信息,所述业务类型信息包括 L2VPN 和 L3VPN。

发送单元 62,用于通过主节点以及所述主节点控制的从节点之间的控制通道,向所述主节点控制的从节点发送所述第一获取单元 61 获取到的业务类型信息,以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路,并对确定好的主虚链路和备虚链路进行故障检测。

可选的是,如图 19 所示,所述第一获取单元 61 包括:

建立模块 611,用于为所述主节点控制的从节点的外连接口建立对应的虚拟远端逻辑接口,所述外连接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

配置模块 612,用于在所述建立模块 612 建立的虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务。

获取模块 613,用于获取与配置的业务相应的业务类型信息。

可选的是,所述发送单元 62 还用于向所述主节点控制的从节点发送使能故障检测配置命令,以使得所述主节点控制的从节点根据所述使能故障检测配置命令,启动对端到端虚链路进行故障检测;其中,所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测,所述端到端虚链路是指所述主节点控制的从节点到主节点之间的在网络虚拟化系统内部的虚链路,以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

可选的是,如图 20 所示,还包括:

接收单元 63,用于接收 RSG 发送的状态信息,所述状态信息包括

Active 和 Standby。

所述发送单元 62，用于将所述接收单元 63 接收到的状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

可选的是，如图 21 所示，还包括：

设置单元 64，用于当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时，则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低。

第二获取单元 65，用于获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级，所述另一个主节点和所述主节点互为主备关系。

所述发送单元 62，用于当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过所述与所述主节点控制的从节点之间的控制通道，发送至所述主节点控制的从节点。

本发明实施例还提供了一种从节点，如图 22 所示，包括至少一个中央处理器 71 和存储器 72，所述存储器 72 被配置代码，所述中央处理器 71 可以读取所述存储器 72 中的代码，用于实现如图 2 至图 14 所示的所有主节点侧的方法流程。所述中央处理器 71 和存储器 72 之间通过总线通信。

其中，所述中央处理器 71 用于通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；根据所述业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路与所述第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路与所述第二虚链路中除所述主虚链路之外的

另一条虚链路；检测所述主虚链路和所述备虚链路是否发生故障；当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输。

所述存储器 72，还用于存储业务类型信息。

所述中央处理器 71，还用于当业务类型为 L2VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路。

还用于当业务类型为 L2VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息，确定主虚链路和备虚链路。

还用于，当业务类型为 L3VPN 时，将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路。

还用于，当业务类型为 L3VPN 时，根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路，所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由状态信息，所述外连接接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

所述存储器 72，还用于存储状态信息和接口路由状态信息。

所述中央处理器 71，还用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的状态信息；通过所述备注节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的状态信息；当接收到从所述主主节点发送的状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，当接收到从所述备主节点发来的状态信息为 Standby 待机状态时，则将所述第二虚链路设置为备虚链路；以及用于当接收到从所述主主节点发送的状态信息为 Standby 时，则将所述第一虚链路设置为备虚链路，当接收到从所述备主节点发来的状态信息为 Active

时，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

所述中央处理器 71，还用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的接口路由状态信息；通过所述备主节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的接口路由状态信息；当接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文；当接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态，则所述从节点将第二虚链路设置为备虚链路；以及用于当接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时，所述从节点将所述第一虚链路设置为备虚链路，当接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

所述中央处理器 71，还用于当检测到所述主虚链路故障恢复正常时，所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

所述中央处理器 71，还用于在预设时间内，所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文，并通过所述备虚链路传输上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

所述中央处理器 71，还用于当所述业务类型信息为 L2VPN 时，所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故

障时，所述从节点将业务数据报文切换到所述备虚链路传输。

所述中央处理器 71，还用于当所述业务类型信息为 L3VPN 时，所述从节点启动对网络虚拟化系统内部的虚链路进行故障检测，所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路；当检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

所述中央处理器 71，还用于当所述业务类型信息为 L2VPN 时，所述从节点通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令，所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；根据所述使能故障检测配置命令，启动对端到端虚链路进行故障检测；当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

本发明实施例还提供了一种从节点，如图 23 所示，包括至少一个中央处理器 81 和存储器 82，所述存储器 82 被配置代码，所述中央处理器 81 可以读取所述存储器 82 中的代码，用于实现如图 2 至图 14 所示的所有从节点侧的方法流程。所述中央处理器 81 和存储器 82 之间通过总线通信。

其中，所述中央处理器 81 用于获取业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送业务类型信息，以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路，并对确定好的主虚链路和备虚链路进行故障检测。

所述存储器 82 还用于存储业务类型信息。

可选的是，所述中央处理器 81 用于为所述主节点控制的从节点的外连接接口建立对应的虚拟远端逻辑接口，所述外连接接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口；在所述虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务，并获取与配置的业务相应的业务类型信息。

可选的是，所述中央处理器 81 用于在所述向所述从节点发送业务类型信息之后，还执行向所述主节点控制的从节点发送使能故障检测配置命令，以使得所述主节点控制的从节点根据所述使能故障检测配置命令，启动对端到端虚链路进行故障检测；其中，所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述主节点控制的从节点到所述主节点之间的在网络虚拟化系统内部的虚链路，以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

可选的是，所述中央处理器 81 用于在所述向所述从节点发送业务类型信息之后，还执行接收 RSG 发送的状态信息，所述状态信息包括 Active 和 Standby；将所述状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

可选的是，所述中央处理器 81 用于，当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时，则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低，并获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级，所述另一个主节点和所述主节点互为主备关系；当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过与所述主节点控制的从节点之间的控制通道，发送至所述主节点控制的从节点。

本发明实施例还提供了一种网络虚拟化系统，包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路。可实现如图 2 至图 13 所示的所有方法流程。

本发明实施例提供的一种主节点、从节点及网络虚拟化系统，在基于控制与转发分离的网络虚拟化系统中，具有控制功能的主节点获取当前业务类型信息并将当前业务类型信息告知从节点以使得从节点能够根据业务类型信息来确定主虚链路和备虚链路并进行故障检测，当检测到所述主虚链路发生故障且备虚链路未发生故障时，将业务数据报文切换到备虚链路进行传输，用以保证业务数据报文在本发明提供的全新系统架构中实现不中断传输，进而保证了业务可靠性

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例所述的方法。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

权利要求书

1、一种保护业务可靠性的方法，其特征在于，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，该方法包括：

所述从节点通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；

所述从节点根据所述业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路和第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路和第二虚链路中除所述主虚链路之外的另一条虚链路；

所述从节点检测所述主虚链路和所述备虚链路是否发生故障；

当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输。

2、根据权利要求 1 所述的方法，其特征在于，所述根据业务类型信息，确定主虚链路和备虚链路包括：

当业务类型为 L2VPN 时，所述从节点将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；

或者，当业务类型为 L2VPN 时，所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息，确定主虚链路和备虚链路；

或者，当业务类型为 L3VPN 时，所述从节点将所述第一虚链路设置为主虚链路，并将所述第二虚链路设置为备虚链路；

或者，当业务类型为 L3VPN 时，所述从节点根据控制所述从节点的主

主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路，所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外接口具有对应关系的虚拟远端逻辑接口的路由状态信息，所述外接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

3、根据权利要求 2 所述的方法，其特征在于，所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点发送的状态信息，确定主虚链路和备虚链路包括；

通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的状态信息；

通过所述备注节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的状态信息；

当接收到从所述主主节点发送的状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，当接收到从所述备主节点发来的状态信息为 Standby 待机状态时，则将所述第二虚链路设置为备虚链路；

或者，当接收到从所述主主节点发送的状态信息为 Standby 时，则所述从节点将所述第一虚链路设置为备虚链路，当接收到从所述备主节点发来的状态信息为 Active 时，则所述从节点将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

4、根据权利要求 2 所述的方法，其特征在于，所述从节点根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息，确定主虚链路和备虚链路包括：

通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的接口路由状态信息；

通过所述备主节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的接口路由状态信息；

当接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文；当接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态，则所述从节点将第二虚链路设置为备虚链路；

或者，当接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时，所述从节点将所述第一虚链路设置为备虚链路，当接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态，则所述从节点将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

5、根据权利要求 1-4 任意一项所述的方法，其特征在于，还包括：

当检测到所述主虚链路故障恢复正常时，所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

6、根据权利要求 5 所述的方法，其特征在于，所述从节点将业务数据报文从所述备虚链路切换回所述主虚链路进行传输包括：在预设时间内，所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文，并通过所述备虚链路传输上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

7、根据权利要求 1-6 任意一项所述的方法，其特征在于，所述从节点检测所述主虚链路和所述备虚链路是否发生故障包括：

当所述业务类型信息为 L2VPN 时，所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；相应地，当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在

的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输；

或者，当所述业务类型信息为 L3VPN 时，所述从节点启动对网络虚拟化系统内部的虚链路进行故障检测，所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路；相应地，当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输包括：当检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

8、根据权利要求 1-6 任意一项所述的方法，其特征在于，所述从节点检测所述主虚链路和所述备虚链路是否发生故障包括：

当所述业务类型信息为 L2VPN 时，所述从节点通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令，所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；

所述从节点根据所述使能故障检测配置命令，启动对端到端虚链路进行故障检测；相应地，当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

9、一种保护业务可靠性的方法，其特征在于，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从

节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，该方法包括：

主节点获取业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；

通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送业务类型信息，以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路，并对确定好的主虚链路和备虚链路进行故障检测。

10、根据权利要求 9 所述的方法，其特征在于，所述主节点获取业务类型信息包括：

为所述主节点控制的从节点的外连接接口建立对应的虚拟远端逻辑接口，所述外连接接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口；

在所述虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务，并获取与配置的业务相应的业务类型信息。

11、根据权利要求 10 所述的方法，其特征在于，在向所述从节点发送业务类型信息之后，还包括：

向所述主节点控制的从节点发送使能故障检测配置命令，以使得所述主节点控制的从节点根据所述使能故障检测配置命令，启动对端到端虚链路进行故障检测；其中，所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述主节点控制的从节点到所述主节点之间的在网络虚拟化系统内部的虚链路，以及与主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

12、根据权利要求 9-11 任意一项所述的方法，其特征在于，在向所述主节点控制的从节点发送业务类型信息之后，还包括：

所述主节点接收 RSG 发送的状态信息，所述状态信息包括 Active 和 Standby；

所述主节点将所述状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

13、根据权利要求 9-11 任意一项所述的方法，其特征在于，在向所述从节点发送业务类型信息之后，还包括：

当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时，则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低，并获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级，所述另一个主节点和所述主节点互为主备关系；

当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过与所述主节点控制的从节点之间的控制通道，发送至所述主节点控制的从节点。

14、一种从节点，其特征在于，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，所述从节点包括：

接收单元，用于通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；

确定单元，用于根据所述接收单元接收的业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路和第二虚链路中的

一条虚链路,所述主虚链路用于传输业务数据报文的虚链路,所述备虚链路为所述第一虚链路和第二虚链路中除所述主虚链路之外的另一条虚链路;

检测单元,用于检测所述确定单元确定的主虚链路和备虚链路是否发生故障;

切换单元,用于当所述检测单元检测到所述主虚链路发生故障且所述备虚链路未发生故障时,将业务数据报文切换到备虚链路进行传输。

15、根据权利要求 14 所述的从节点,其特征在于,所述确定单元用于当业务类型为 L2VPN 时,将所述第一虚链路设置为主虚链路,并将所述第二虚链路设置为备虚链路;还用于当业务类型为 L2VPN 时,根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的状态信息,确定主虚链路和备虚链路;还用于当业务类型为 L3VPN 时,将所述第一虚链路设置为主虚链路,并将所述第二虚链路设置为备虚链路;还用于当业务类型为 L3VPN 时,根据控制所述从节点的主主节点和控制所述从节点的备主节点各自发送的接口路由状态信息,确定主虚链路和备虚链路,所述接口路由状态信息为在所述主主节点或备主节点上的与所述从节点的外连接接口具有对应关系的虚拟远端逻辑接口的路由状态信息,所述外连接接口指所述从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口。

16、根据权利要求 15 所述的从节点,其特征在于,所述确定单元包括:

第一接收模块,用于通过所述主主节点和所述从节点之间的控制通道,所述从节点接收所述主主节点发送的状态信息;

所述第一接收模块,还用于通过所述备注节点和所述从节点之间的控制通道,所述从节点接收所述备主节点发送的状态信息;

确定模块,当所述第一接收模块接收到从所述主主节点发送的状态信息为 Active 激活状态时,所述从节点将所述第一虚链路设置为主虚链路,并在所述第一虚链路上传输业务数据报文,并当所述第一接收模块接收到从所述备主节点发来的状态信息为 Standby 待机状态时,则将所述第二虚

链路设置为备虚链路；还用于当所述第一接收模块接收到从所述主主节点发送的状态信息为 Standby 时，则将所述第一虚链路设置为备虚链路，并当所述第一接收模块接收到从所述备主节点发来的状态信息为 Active 时，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

17、根据权利要求 15 所述的从节点，其特征在于，所述确定单元包括：第二接收模块，用于通过所述主主节点和所述从节点之间的控制通道，所述从节点接收所述主主节点发送的接口路由状态信息；

所述第二接收模块，还用于通过所述备主节点和所述从节点之间的控制通道，所述从节点接收所述备主节点发送的接口路由状态信息；

设置模块，用于当所述第二接收模块接收到从所述主主节点发送的接口路由状态信息为 Active 激活状态时，所述从节点将所述第一虚链路设置为主虚链路，并在所述第一虚链路上传输业务数据报文，并当所述第二接收模块接收到从所述备主节点发来的接口路由状态信息为 Standby 待机状态，则将第二虚链路设置为备虚链路；还用于当所述第二接收模块接收到从所述主主节点发送的接口路由状态信息为 Standby 待机状态时，将所述第一虚链路设置为备虚链路；并当所述第二接收模块接收到从所述备主节点发来的接口路由状态信息为 Active 激活状态，则将所述第二虚链路设置为主虚链路，并在所述第二虚链路上传输业务数据报文。

18、根据权利要求 14-17 任意一项所述的从节点，其特征在于，所述切换单元还用于当所述检测单元检测到所述主虚链路故障恢复正常时，将业务数据报文从所述备虚链路切换回所述主虚链路进行传输。

19、根据权利要求 18 所述的从节点，其特征在于，所述切换单元用于在预设时间内，所述从节点同时接收在所述主虚链路和所述备虚链路上传输的下行业务数据报文，并通过所述备虚链路传输上行业务数据报文，在所述预设时间后，所述从节点将上行业务数据报文和下行业务数据报文都切换到所述主虚链路上传输。

20、根据权利要求 14-19 任意一项所述的从节点，其特征在于，所述检测单元用于当所述接收单元接收到的业务类型信息为 L2VPN 时，启动对端到端虚链路进行故障检测，所述端到端虚链路是指所述从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到远程信令网关 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；

则所述切换单元，用于当所述检测单元检测到所述主虚链路发生故障且所述备虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路进行传输包括：当检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输；

或者，所述检测单元用于当所述接收单元接收到的业务类型信息为 L3VPN 时，启动对网络虚拟化系统内部的虚链路进行故障检测，所述网络虚拟化系统内部的虚链路是指从节点到主节点的网络虚拟化系统内部的虚链路；

则所述切换单元，用于当所述检测单元检测到所述主虚链路所在的网络虚拟化系统内部的虚链路发生故障且所述备虚链路所在的网络虚拟化系统内部的虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

21、根据权利要求 14-19 任意一项所述的从节点，其特征在于，所述检测单元用于当所述接收单元接收的业务类型信息为 L2VPN 时，通过与控制所述从节点的主节点之间的控制通道接收控制所述从节点的主节点发送的使能故障检测配置命令，所述使能故障检测配置命令用于控制所述从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到控制所述从节点的主节点之间的在网络虚拟化系统内部的虚链路，以及与控制所述从节点的主节点到 RSG 之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路；根据所述接收单元接收到的使能故障检测配置命令，

启动对端到端虚链路进行故障检测；

则所述切换单元，用于当所述检测单元检测到所述主虚链路所在的端到端虚链路发生故障且所述备虚链路所在的端到端虚链路未发生故障时，所述从节点将业务数据报文切换到所述备虚链路传输。

22、一种主节点，其特征在于，应用于基于控制和转发分离的网络虚拟化系统中，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路，其中，所述主节点包括：

第一获取单元，用于获取业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；

发送单元，用于通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送所述第一获取单元获取到的业务类型信息，以使得所述主节点控制的从节点能够根据接收到的业务类型信息确定主虚链路和备虚链路，并对确定好的主虚链路和备虚链路进行故障检测。

23、根据权利要求 22 所述的主节点，其特征在于，所述第一获取单元包括：

建立模块，用于所述主节点控制的从节点的外连接接口建立对应的虚拟远端逻辑接口，所述外连接接口指所述主节点控制的从节点与基于控制和转发分离的网络虚拟化系统外的网络设备相连接的接口；

配置模块，用于在所述建立模块建立的虚拟远端逻辑接口上配置基于控制和转发分离的网络虚拟化系统外的业务；

获取模块，用于获取与配置的业务相应的业务类型信息。

24、根据权利要求 23 所述的主节点，其特征在于，所述发送单元还用于向所述主节点控制的从节点发送使能故障检测配置命令，以使得所述主

节点控制的从节点根据所述使能故障检测配置命令，启动对端到端虚链路进行故障检测；其中，所述使能故障检测配置命令用于控制所述主节点控制的从节点启动对端到端虚链路进行故障检测，所述端到端虚链路是指从节点到主节点之间的在网络虚拟化系统内部的虚链路，以及与主节点到RSG之间的在网络虚拟化系统外部的虚链路拼接起来形成的虚链路。

25、根据权利要求 21-24 任意一项所述的主节点，其特征在于，还包括：

接收单元，用于接收 RSG 发送的状态信息，所述状态信息包括 Active 和 Standby；

所述发送单元，用于将所述接收单元接收到的状态信息通过与所述主节点控制的从节点之间的控制通道发送至所述主节点控制的从节点。

26、根据权利要求 21-24 任意一项所述的主节点，其特征在于，还包括：

设置单元，用于当主节点检测到与所述主节点控制的从节点对应的接口路由发生故障时，则将所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级降低；

第二获取单元，用于获取所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级，所述另一个主节点和所述主节点互为主备关系；

所述发送单元，用于当确定所述主节点控制的从节点在所述主节点上的虚拟远端逻辑接口的路由优先级低于所述主节点控制的从节点对应的另一个主节点上的虚拟远端逻辑接口的路由优先级时，将 Standby 状态携带在接口路由状态信息中，通过所述与所述主节点控制的从节点之间的控制通道，发送至所述主节点控制的从节点。

27、一种网络虚拟化系统，其特征在于，所述网络虚拟化系统包括主节点和从节点，从节点被一对互为主备的主节点控制，所述一对互为主备的主节点包括一个主主节点和一个备主节点，所述从节点和控制所述从节

点的主主节点之间设置有第一虚链路，所述从节点和控制所述从节点的备主节点之间设置有第二虚链路；

其中，所述主节点获取业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；通过主节点以及所述主节点控制的从节点之间的控制通道，向所述主节点控制的从节点发送业务类型信息；

所述从节点通过控制所述从节点的主节点与所述从节点之间的控制通道，接收从控制所述从节点的主节点发来的业务类型信息，所述业务类型信息包括 L2VPN 和 L3VPN；根据所述业务类型信息，确定主虚链路和备虚链路；其中，所述主虚链路为所述第一虚链路与所述第二虚链路中的一条虚链路，所述主虚链路用于传输业务数据报文的虚链路，所述备虚链路为所述第一虚链路与所述第二虚链路中除所述主虚链路之外的另一条虚链路；检测所述主虚链路和所述备虚链路是否发生故障；当检测到所述主虚链路发生故障且所述备虚链路未发生故障时，将业务数据报文切换到所述备虚链路进行传输。

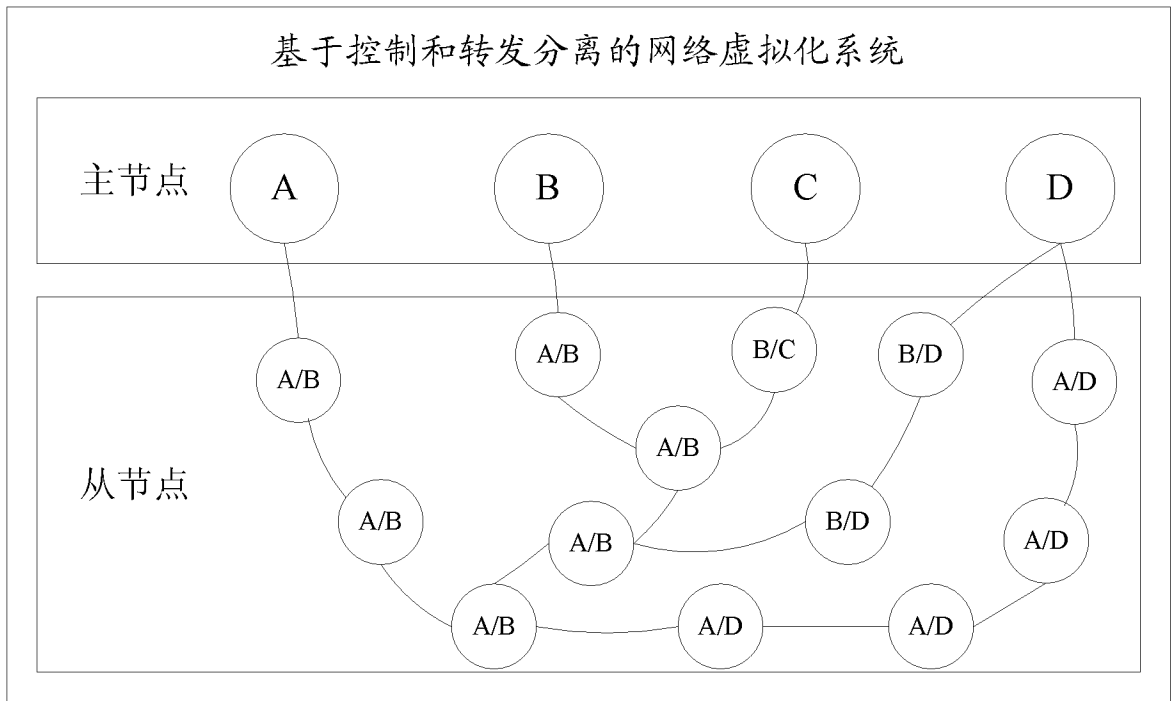


图 1

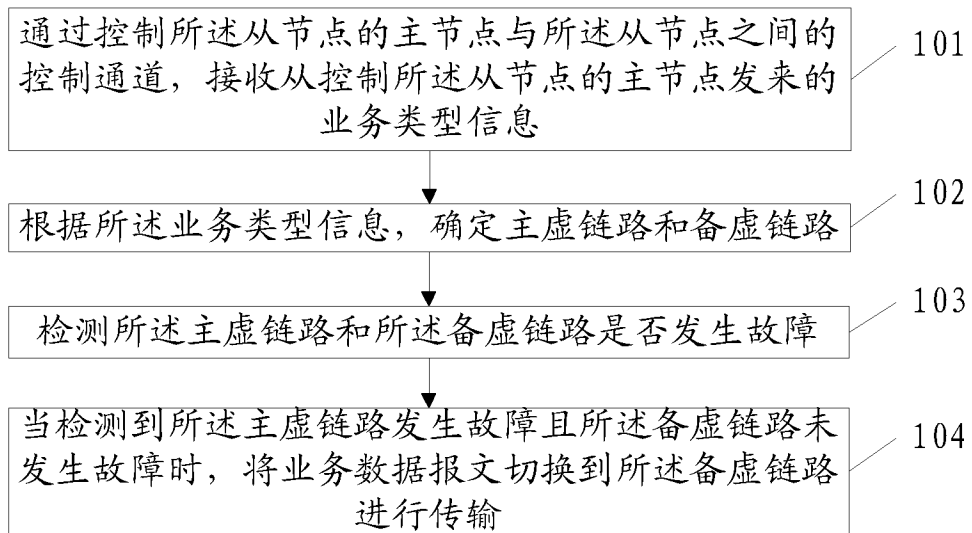


图 2

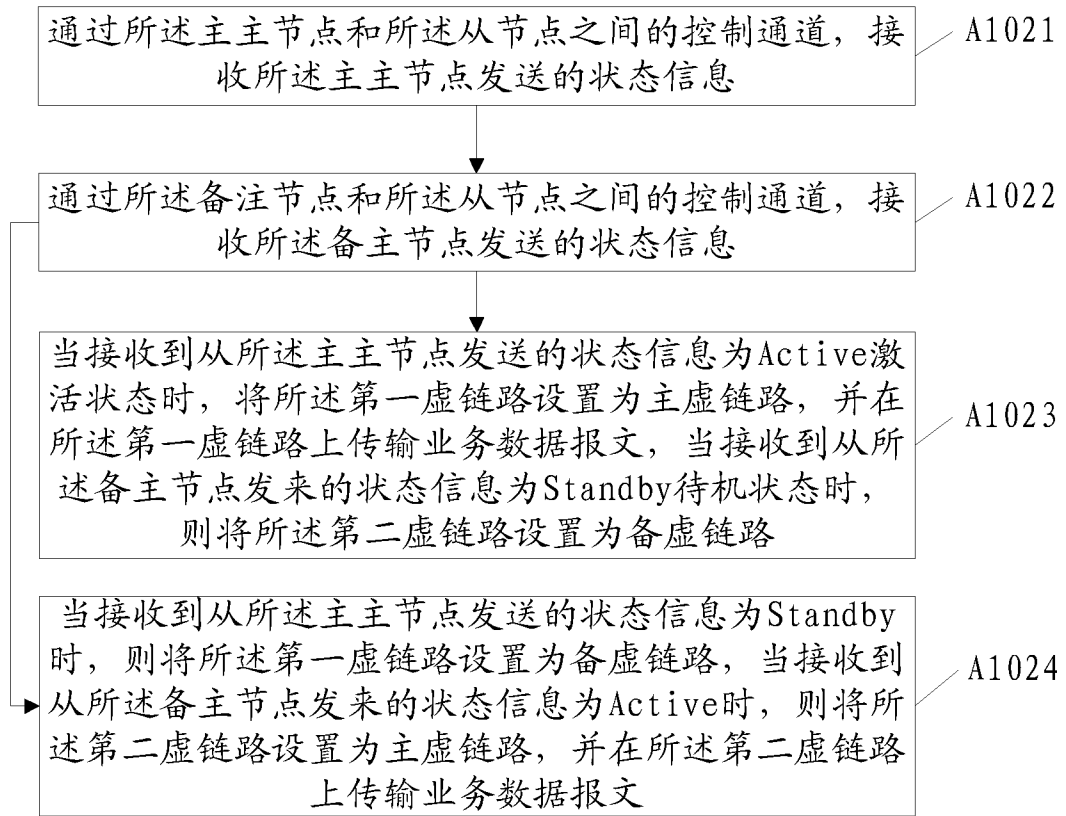


图 3

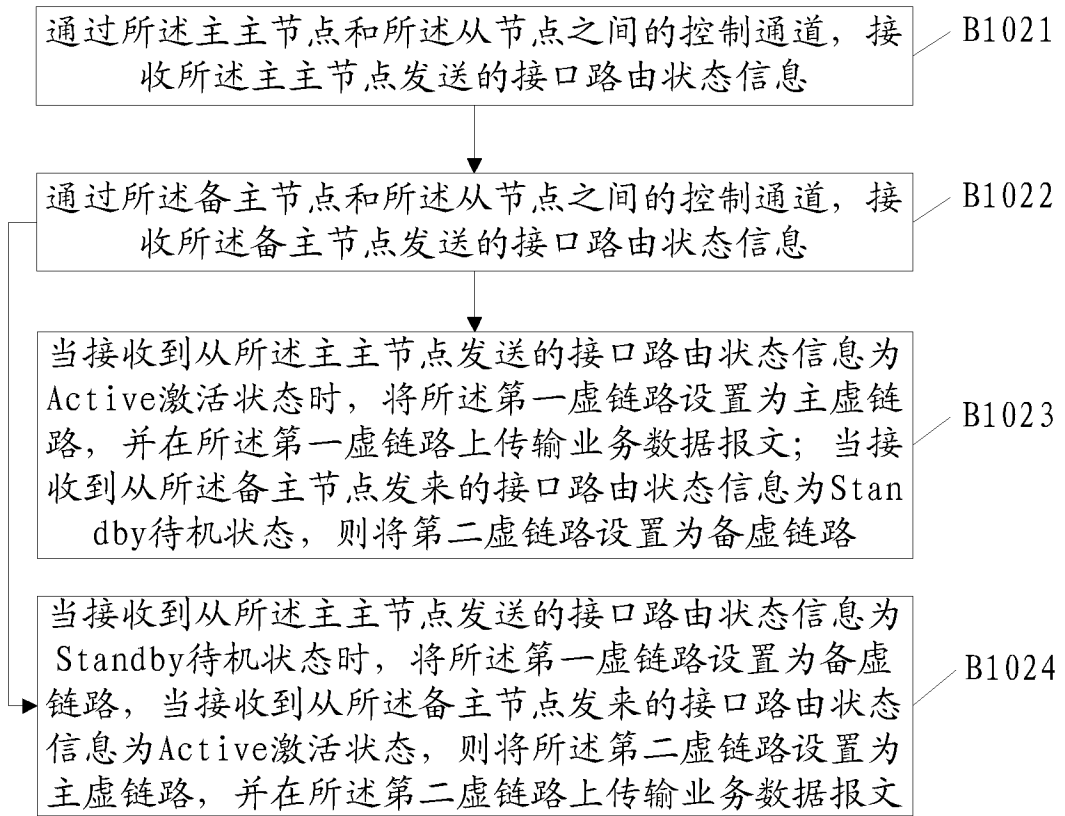


图 4

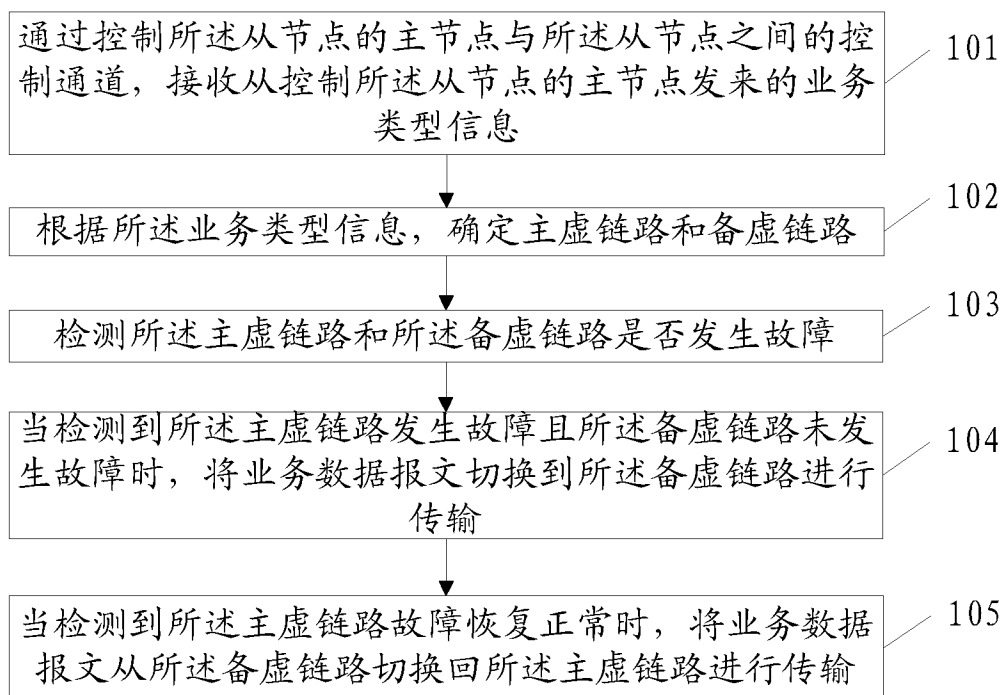


图 5

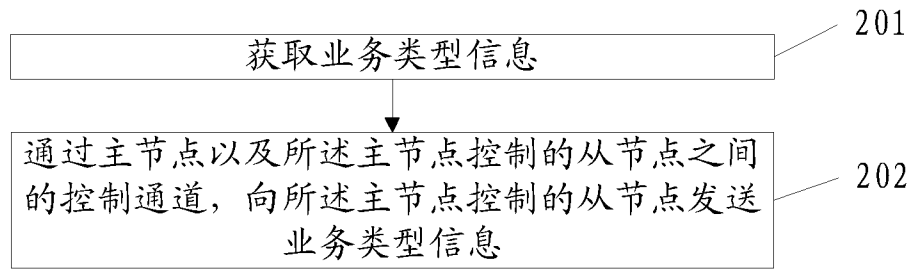


图 6

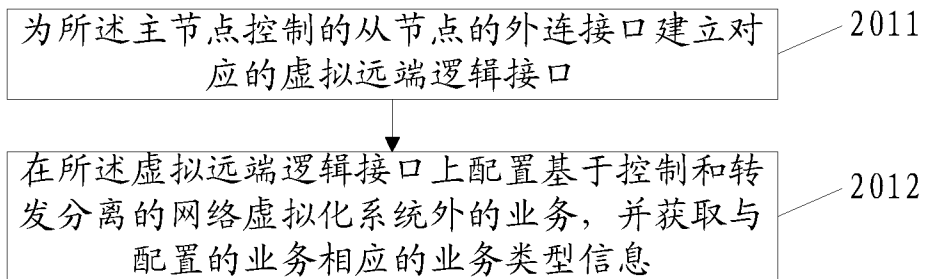


图 7

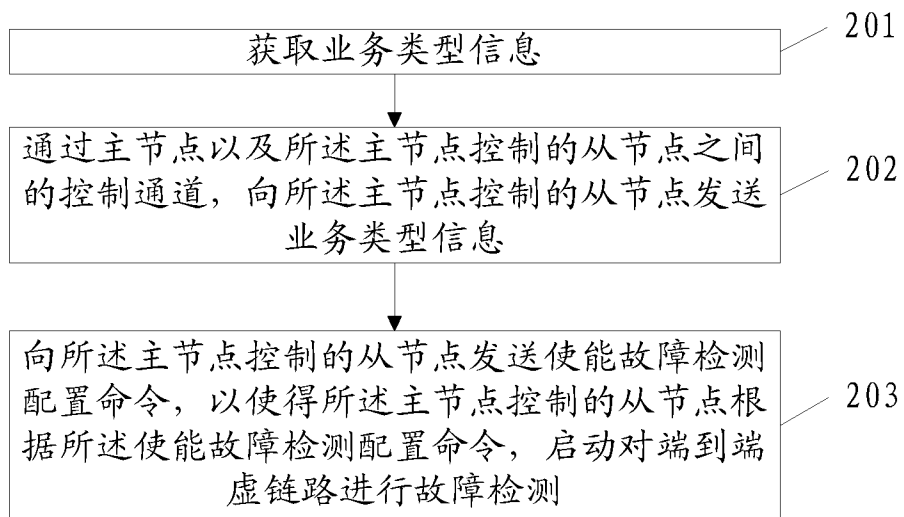


图 8

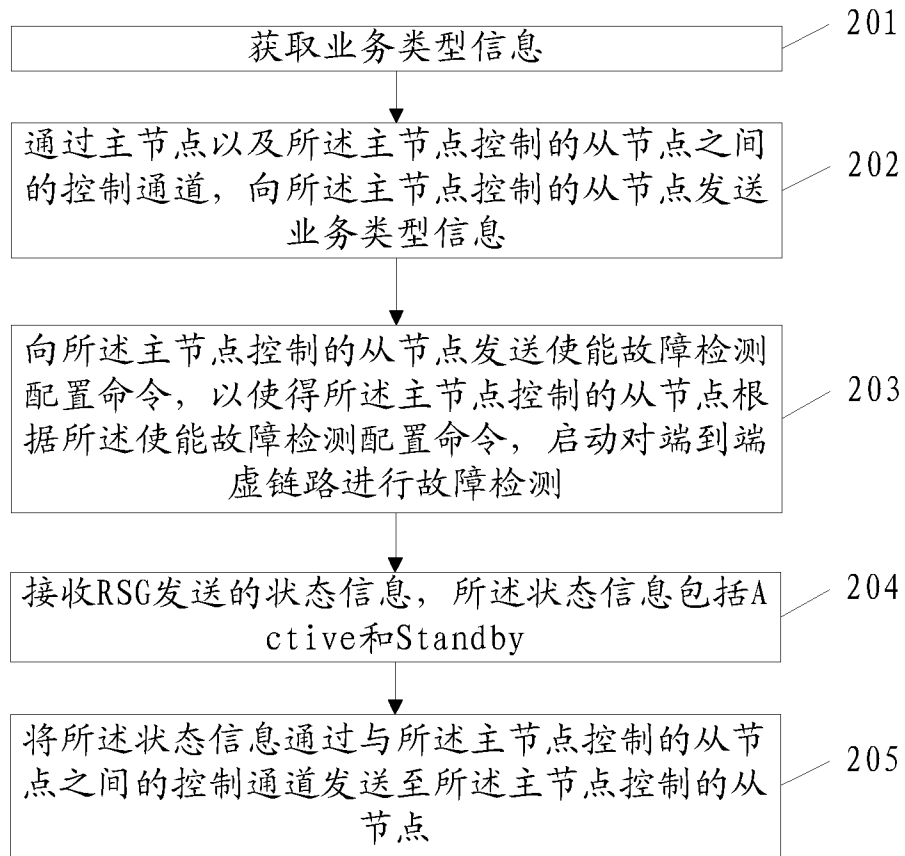


图 9

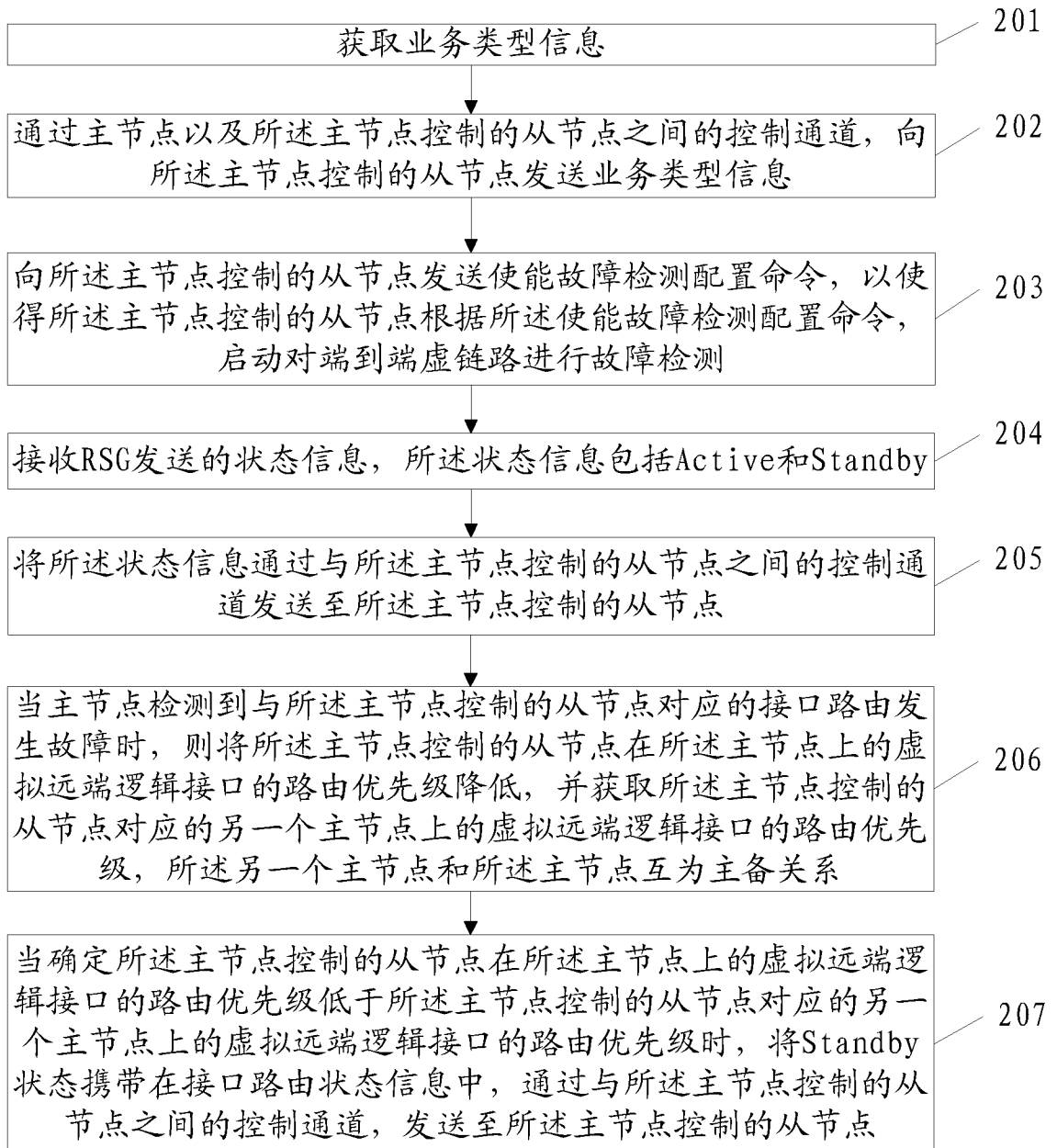


图 10

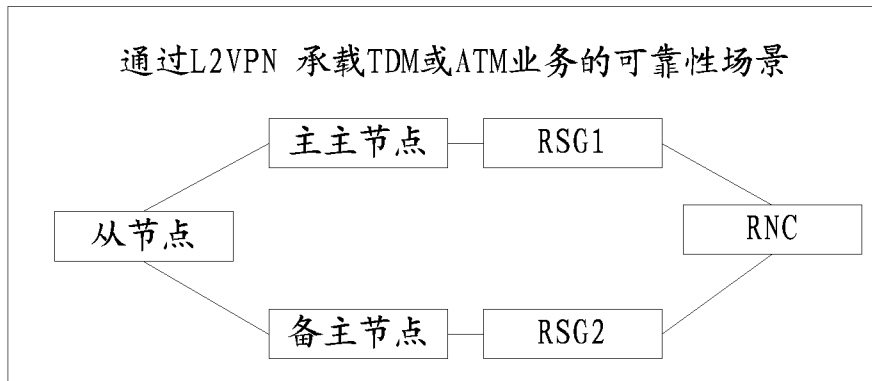


图 11

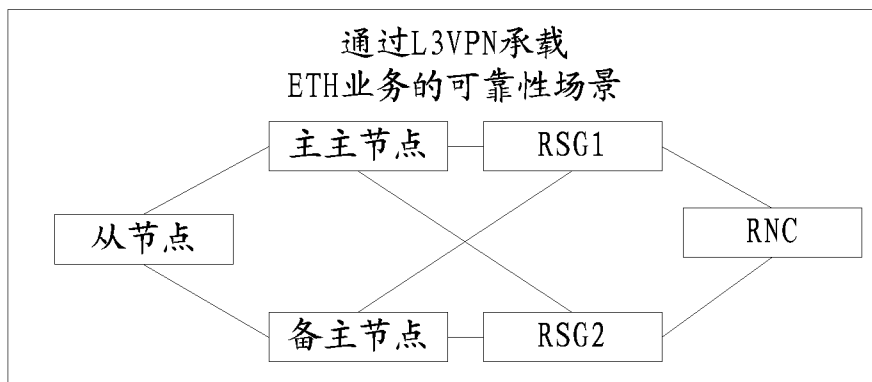


图 12

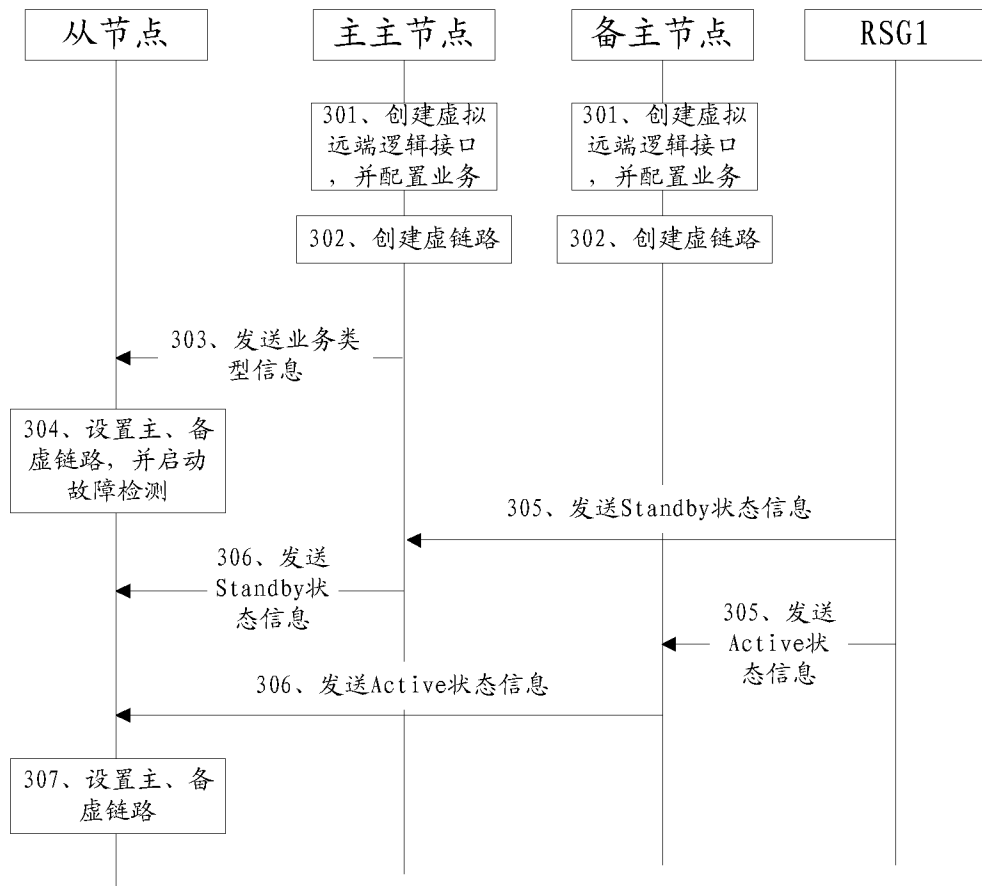


图 13

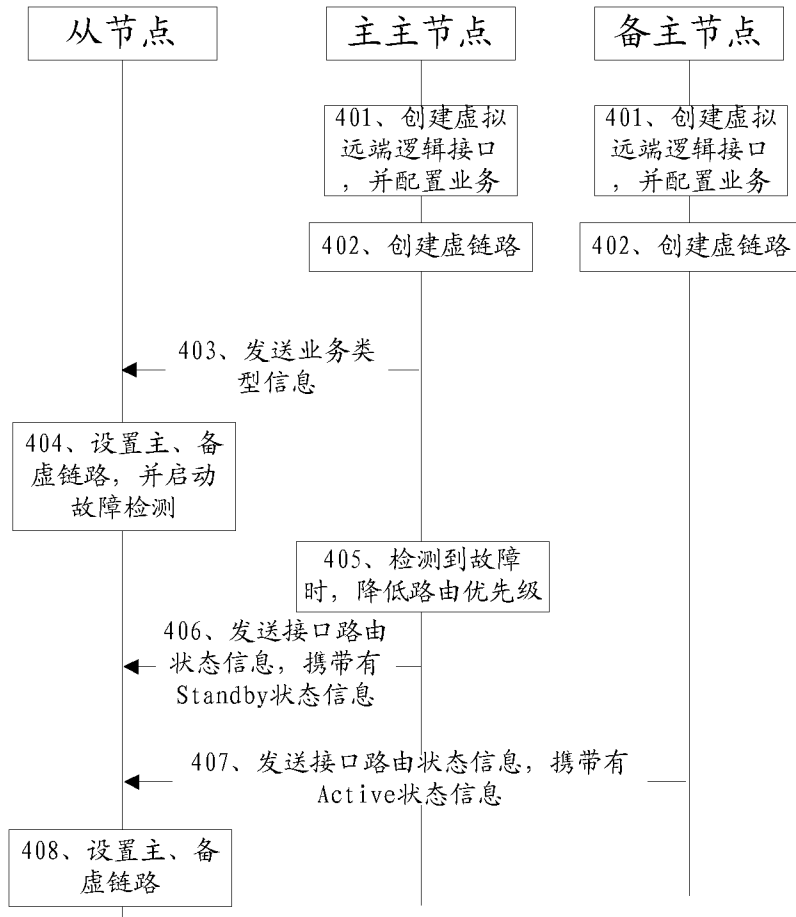


图 14

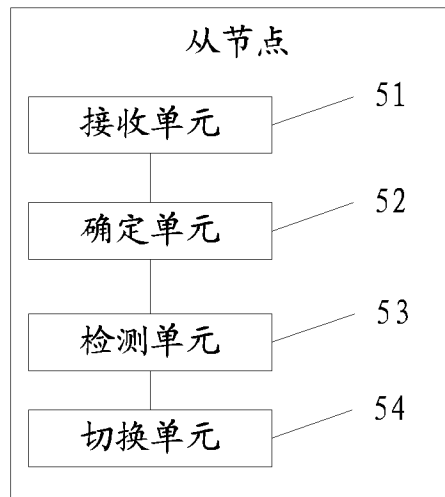


图 15

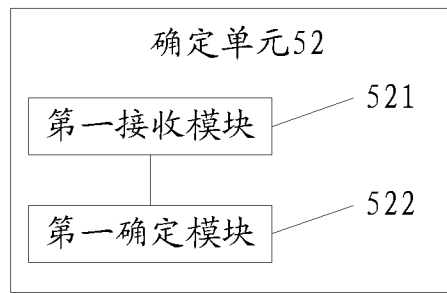


图 16

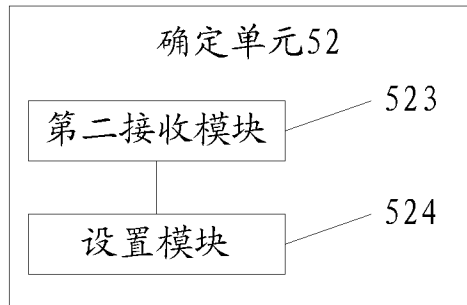


图 17

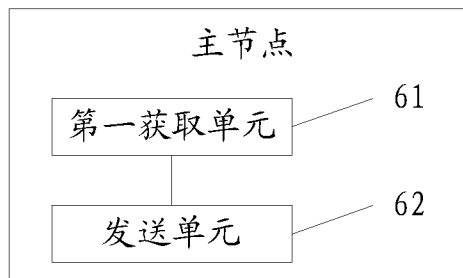


图 18

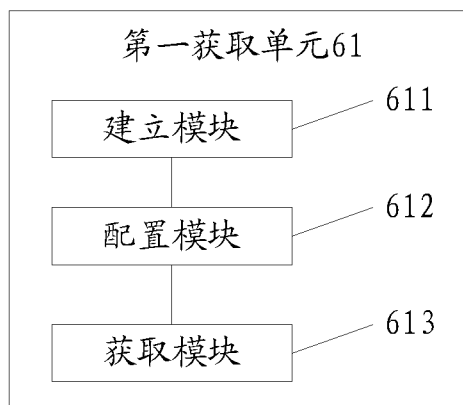


图 19

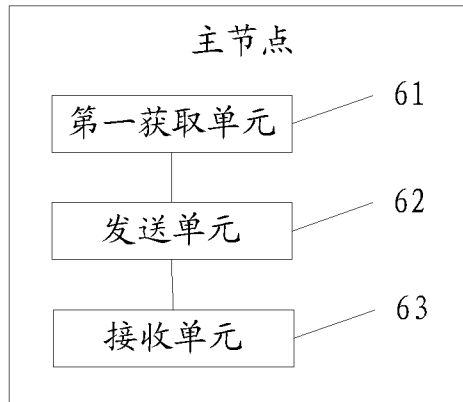


图 20

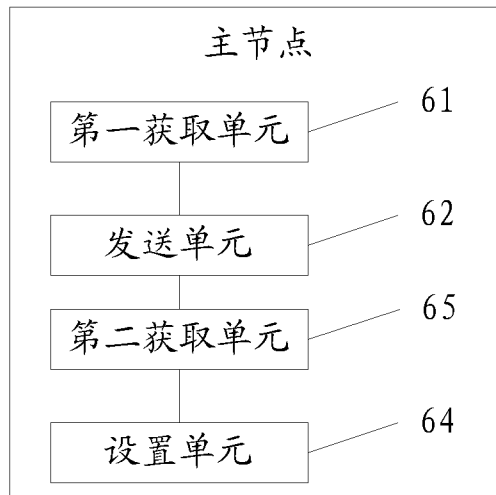


图 21

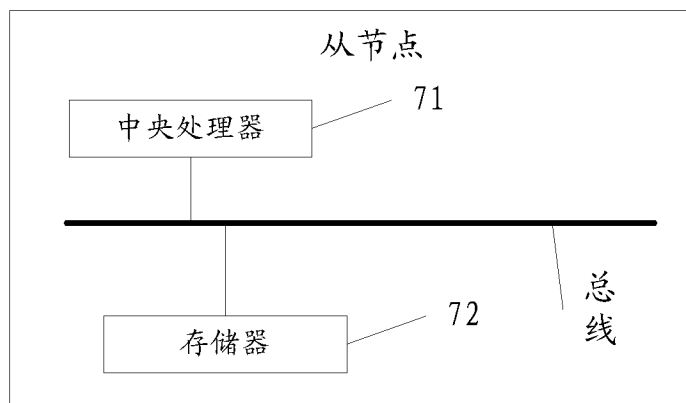


图 22

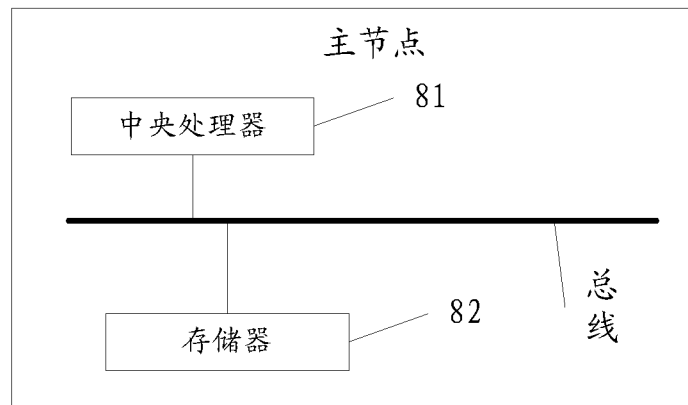


图 23

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/073973

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT, CPRSABS, CNKI, VEN, USTXT, WOTXT: service type, virtual link, PW, node, L2VPN, L3VPN, system, service, type, determin+, virtual, link, connect+, pseudo 1w wire, main, standby, secondary, point, peer, layer, vpn, virtualization, network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102377607 A (HUAWEI TECHNOLOGIES CO., LTD.), 14 March 2012 (14.03.2012), see abstract, description, page 1, paragraphs [0005]-[0009]	1-27
A	CN 102098231 A (H3C TECHNOLOGIES CO., LIMITED), 15 June 2011 (15.06.2011), the whole document	1-27
A	CN 1863069 A (HUAWEI TECHNOLOGIES CO., LTD.), 15 November 2006 (15.11.2006), the whole document	1-27

Further documents are listed in the continuation of Box C.

See patent family annex.

<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p>	<p>“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>“&” document member of the same patent family</p>
---	---

<p>Date of the actual completion of the international search</p> <p style="text-align: center;">06 January 2014 (06.01.2014)</p>	<p>Date of mailing of the international search report</p> <p style="text-align: center;">23 January 2014 (23.01.2014)</p>
<p>Name and mailing address of the ISA/CN:</p> <p>State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451</p>	<p>Authorized officer</p> <p style="text-align: center;">HE, Liliang</p> <p>Telephone No.: (86-10) 62411216</p>

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/073973

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102377607 A	14.03.2012	WO 2012016458 A1	09.02.2012
CN 102098231 A	15.06.2011	US 2012236868 A1	20.09.2012
		CN 102098231 B	11.09.2013
CN 1863069 A	15.11.2006	EP 1909435 A1	09.04.2008
		EP 1909435 B2	06.03.2013
		EP 1909435 B1	28.07.2010
		US 7782764 B2	24.08.2010
		CN 100362810 C	16.01.2008
		US 2009154339 A1	18.06.2009
		DE 602006015814 D1	09.09.2010
		WO 2007012239 A1	01.02.2007

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2013/073973

CONTINUATION OF BOX A ON SECOND SHEET: CLASSIFICATION OF SUBJECT MATTER

H04L 12/26 (2006.01) i

H04L 12/24 (2006.01) n

H04L 12/70 (2013.01) n

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2013/073973

检索报告中引用的 专利文件	公布日期	同族专利	公布日期
CN 102377607 A	14.03.2012	WO 2012016458 A1	09.02.2012
CN 102098231 A	15.06.2011	US 2012236868 A1	20.09.2012
		CN 102098231 B	11.09.2013
CN 1863069 A	15.11.2006	EP 1909435 A1	09.04.2008
		EP 1909435 B2	06.03.2013
		EP 1909435 B1	28.07.2010
		US 7782764 B2	24.08.2010
		CN 100362810 C	16.01.2008
		US 2009154339A1	18.06.2009
		DE 602006015814 D1	09.09.2010
		WO 2007012239 A1	01.02.2007

续第 2 页:

A. 主题的分类

H04L 12/26 (2006.01) i

H04L 12/24 (2006.01) n

H04L 12/70 (2013.01) n