

# (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  
2012年9月27日 (27.09.2012)



(10) 国际公布号  
WO 2012/126413 A2

- (51) 国际专利分类号:  
H04L 12/24 (2006.01)
- (21) 国际申请号: PCT/CN2012/074963
- (22) 国际申请日: 2012年5月2日 (02.05.2012)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人 (对除美国外的所有指定国): **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: 及
- (75) 发明人/申请人 (仅对美国): **夏寅贲 (XIA, Yinben)** [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)。 **李凤凯 (LI, Fengkai)** [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)。
- (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, 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, 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, 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:

- 根据申请人的请求, 在条约第 21 条(2)(a)所规定的期限届满之前进行。
- 不包括国际检索报告, 在收到该报告后将重新公布(细则 48.2(g))。

(54) Title: METHOD AND APPARATUS FOR CONTROLLING NETWORK DEVICE

(54) 发明名称: 一种控制网络设备的方法和装置

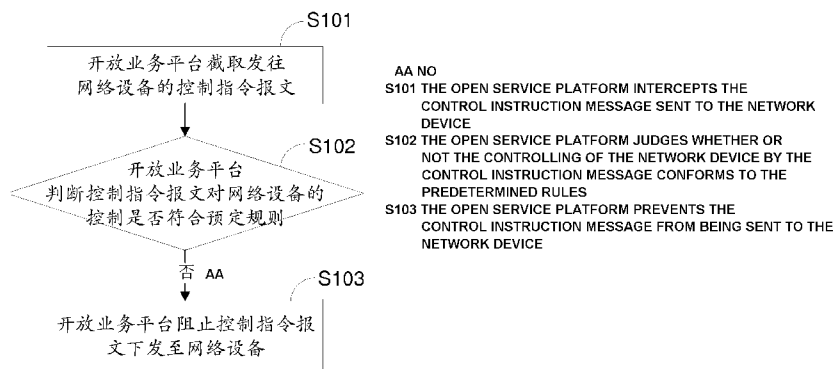


图 1 / Fig. 1

(57) Abstract: The present invention relates to the field of communications, and disclosed are a method and apparatus for controlling a network device. An open service platform is used to intercept the instruction message sent to the network device, identify the rights of the instruction message, judge whether or not the instruction message is in conflict with the previous instruction, and send the instruction message to the network device if the message has the rights and is not in conflict with the previous instruction. The method and apparatus can ensure that the instruction message controls the network device properly and legally.

(57) 摘要:

WO 2012/126413 A2

## 一种控制网络设备的方法和装置

本发明涉及通信领域，特别涉及一种控制网络设备的方法和装置。

### 技术领域

本发明涉及通信技术领域，具体涉及一种建立邻居关系的方法和网络设备。

### 背景技术

随着网络技术的不断发展，网络带宽流量越来越大，但每比特 bit 的收益却越来越低，运营商正在逐步成为了一个管道提供商。运营商迫切需要具备能够与互联网内容提供商（英文全称：Internet Content Provider，简称 ICP）、互联网服务提供商（英文全称：Internet Service Provider，简称 ISP）进行利润分成的能力，对网络的精细化运营便是运营商提升实现该利润分成的途径之一。

通常，会有多个业务同时部署在一台网络设备对应的开放业务平台之上，现有开放业务平台对业务进行分析和统计，而不对数据、控制指令做任何判断与修改，可能会存在恶意、逻辑不健全的业务，这些业务可能会对网络设备的进行错误控制，导致网络设备出现灾难性的后果。

### 发明内容

有鉴于此，本发明实施例提供一种控制网络设备的方法和装置，可以应用于开放的网络设备架构中。

一方面，本发明实施例提供一种控制网络设备的方法，包括：开放业务平台截取发往所述网络设备的第一控制指令报文，开放业务平台判断所述第一控制指令报文对所述网络设备的控制是否符合预定规则；以及如果不符合所述预定规则，开放业务平台阻止所述第一控制指令报文下发至所述网络设备。

另一方面，本发明实施例提供一种控制网络设备的装置，其特征在于所述装置包括鉴权冲突控制模块和数据存储单元；数据存储单元用于存储所截取的发往所述网络设备的第一控制指令报文和预定规则；鉴权冲突控制模块用于用于从数据存储单元读取所述第一控制指令报文和所述预定规则，并根据所述预

定规则判断所述控制指令报文对网络设备的控制是否符合预定规则；以及如果不符合所述预定规则，鉴权冲突控制模块阻止所述第一控制指令报文下发至所述网络设备。

采用本发明实施例的技术方案，保证了业务处理、及控制的正确性，以及防止恶意、逻辑不健全的业务对网络设备的错误控制的技术效果。从而，确保开放业务系统对网络设备控制的正确、合法性，使得网络设备健壮、安全。

## 附图说明

- 图1为本发明实施例的方法的流程图；
- 图2a为本发明实施例的方法的子流程图；
- 图2b为本发明实施例的方法的子流程图；
- 图3a为本发明实施例的方法的子流程图；
- 图3b为本发明实施例的方法的子流程图；
- 图4为本发明实施例的组网示意图；
- 图5a为本发明实施例中的配置文件示意图；
- 图5b为本发明实施例中的配置文件示意图；
- 图6为本发明实施例中的系统示意图；
- 图7为本发明实施例中的装置示意图；
- 图8为本发明实施例中的模块示意图。

## 具体实施方式

为了使本发明实施例的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。本发明的具体实施方式包括控制网络设备的方法和装置。本发明的实施方式所包括的方法可由通用计算机或网络服务器等硬件设备实现。

根据本发明的一个实施方式，如图1所示，控制网络设备的方法包括S101，开放业务平台截取发往网络设备的第一控制指令报文。S102，开放业务平台判

断第一控制指令报文对网络设备的控制是否符合预定规则。S103, 如果不符合预定规则, 开放业务平台阻止第一控制指令报文下发至网络设备。

本发明的一个应用场景如图4所示, 用户A(401)通过互联网(internet)设备访问互联网资源403。用户A的各种不同的请求到达网络设备, 网络设备的示例如图4下部显示的路由器402。用户请求被引流至开放业务平台406, 各种不同的请求可以是语音、视频流下载、访问internet甚至是恶意攻击互联网服务器。开放业务平台406识别和归类用户的请求, 例如: 语音增强业务, 视频增强业务, 带宽控制业务等。实施开放业务平台406上述功能的设备即本发明所涉及的控制网络设备的装置, 该装置实施本发明所涉及的控制方法, 从而过滤不符合预定规则的控制指令。

可选的, 根据本发明的一个实施方式, 判断所述第一控制指令报文对网络设备的控制是否符合预定规则, 可以为: 判断所述第一控制指令报文对网络设备的控制是否具有授权。

进一步可选的, 根据本发明的一个实施方式, 判断所述第一控制指令报文对网络设备的控制是否符合预定规则, 可以包括:

获取与所述第一控制指令报文相对应的业务标识(ID);

利用已授权业务ID表, 判断与所述第一控制指令报文相对应的业务是否有授权;

如果与所述第一控制指令报文相对应的业务没有授权, 则确定所述第一控制指令报文对网络设备的控制不符合预定规则。

可选的, 根据本发明的一个实施方式, 判断所述第一控制指令报文对网络设备的控制是否符合预定规则, 可以为: 判断所述第一控制指令报文对网络设备的控制, 是否与开放业务平台在所述第一控制指令报文之前截取到的控制指令报文对网络设备的控制冲突。

为便于表述,将所述控制指令报文称为第一控制指令报文,将开放业务平台在所述控制指令报文之前截取到的控制指令报文称为第二控制指令报文。

进一步可选的,根据本发明的一个实施方式,如果所述第一控制指令报文对网络设备的控制与所述第二控制指令报文对网络设备的控制冲突,比较所述第一控制指令报文的优先级与第二控制指令报文的优先级;

如果所述第一控制指令报文的优先级低于第二控制指令报文的优先级,则确定所述控制指令报文对网络设备的控制不符合预定规则。

可选的,根据本发明的一个实施方式,如图2a所示,在S201,截取发往网络设备的的第一控制指令报文。S202,判断第一控制指令报文对网络设备的控制是否具有授权。如果没有授权,跳转到S204,阻止第一控制指令报文下发至网络设备;如果第一控制指令报文对网络设备的控制具有授权,S203,进一步判断第一控制指令报文对网络设备的控制是否与第二控制指令报文对网络设备的控制冲突。如果第一控制指令报文对网络设备的控制与第二控制指令报文对网络设备的控制冲突,跳转到S204,阻止第一控制指令报文下发至网络设备。

可选的,根据本发明的另一个实施方式,如图2b所示,S1001,截取发往网络设备的的第一控制指令报文。S1002,判断第一控制指令对网络设备的控制是否与第二控制指令对网络设备的控制冲突;如果有冲突,则转到S1004,阻止第一控制指令报文下发至网络设备。如果没有冲突,则转到S1003。在S1003,判断与所述第一控制指令报文相对应的业务是否具有授权。如果未授权,转到S1004,阻止第一控制指令报文下发至网络设备。

根据本发明的另一个实施方式,如图3a所示,S301,截取发往网络设备的的第一控制指令报文。S302,获取与第一控制指令报文相对应的业务标识ID。业务ID是开放业务平台进行业务部署的编号,主要用于对业务的识别。可以是一个递增的数,1 2 3 4 5...,例如1业务就是一个视频增强的业务;2业务就是一个语音增强的业务;3业务是一个绿色上网的业务。上述业务1、2和3的授权可以是:业务1允许对视频包进行控制;业务2允许对语音报文进行控制;业务3

允许对超文本传送协议http (Hypertext Transfer Protocol) 报文进行控制等。S303, 利用已授权业务ID表, 判断所述与第一控制指令报文相对应的业务是否有授权。

根据本发明的一个实施方式, 已授权业务ID表可以表现为业务权限配置文件。因此, 在S303, 可以利用业务权限配置文件判断所述与第一控制指令报文相对应的业务是否有授权。如图5a所示, 业务权限配置文件中可以包含业务ID和优先级。其中, 业务ID在开放业务平台之上唯一, 是各个业务的唯一标识, 只有业务ID在该业务权限配置文件中, 该业务的控制指令才可以通过开放业务平台下发至网络设备, 业务ID未在该业务权限配置文件中, 则该业务是没有授权下发网络设备控制指令。优先级用于表示该业务对网络设备控制的权限级别, 优先级为一个整数, 优选的, 数值越小, 表明优先级越高。

可选的, 业务权限配置文件可以设置的更为复杂, 比如增加报文业务类型, 以说明该业务可以对哪些业务类型的数据报文进行处理和针对这些业务而对网络设备进行控制指令下发。如图5b所示, 业务ID为12的业务对应的报文业务类型是视频, ID为12的业务的授权是对视频的控制, 如果业务ID为12的业务下发到网络设备的控制指令是对上传ftp (File Transfer Protocol) 数据报文的控制, 则认为该控制指令是一个没有授权的控制指令。同样, 业务ID为20的业务的合法权限是对ftp数据报文的控制, 如果业务ID为20的业务下发到网络设备的控制指令是对点对点P2P数据报文的控制, 则认为该控制指令是一个没有授权的控制指令。

已授权业务ID表包括各个业务ID对应的合法授权权限, 例如, 业务ID为20的业务的合法授权权限是对ftp数据报文的控制。

如果S303的判断结果是与第一控制指令报文相对应的业务没有授权, 在S304, 阻止第一控制指令报文下发至网络设备。可选的, 阻止第一控制指令报文下发至网络设备之后, 向第一控制指令报文的发送方发送error信息。

如果S303的判断结果是与第一控制指令报文相对应的业务有授权,

S305, 遍历全局控制指令列表, 判断第一控制指令报文是否已下发过, 全局控制指令列表是已下发过的控制指令报文的列表。如果S305的判断结果是未曾下发, 在S308, 将第一控制指令报文存入全局控制指令列表。在S309, 将第一控制指令报文下发至网络设备。在S310, 子流程结束。

如果S305的判断结果是曾经下发过, 在S306, 判断第一控制指令报文对网络设备的控制与第二控制指令报文对网络设备的控制是否冲突。例如, 对于一个在线观看的视频的数据报文, 第一控制指令报文是一个保证带宽的指令, 而第二控制指令报文是一个阻止观看的指令, 则这两个控制指令报文对网络设备的控制就存在冲突。如果S306的判断结果是不冲突, 则转到S309, 将第一控制指令报文下发至网络设备。如果S306的判断结果是冲突, 在S307, 比较第一控制指令报文与第二控制指令报文的优先级, 若第一控制指令报文的优先级比第二控制指令报文的优先级低, 则跳转至S304, 阻止第一控制指令报文下发至网络设备。如果第一控制指令报文的优先级不比第二控制指令报文的优先级低, 则跳转至S309, 将第一控制指令报文下发至网络设备。

根据本发明的又一个实施方式, 如图3b所示, 在S901, 截取发往网络设备的第一控制指令报文。在S902, 获取业务ID。在S905, 遍历已经下发全局控制指令列表, 判断第一控制指令报文是否曾经下发。如果第一控制指令报文曾经下发过, 在S906, 判断第一控制指令报文对网络设备的控制是否与第二控制指令报文对网络设备的控制冲突; 如果第一控制指令报文未下发过, 在S908, 将第一控制指令报文存入全局控制指令列表, 跳转至S903。

如果S906的判断结果是有冲突, 则转到S907, 比较第一控制指令报文与第二控制指令报文的优先级, 若第一控制指令报文的优先级比第二控制指令报文的优先级低, 则跳转至S904, 阻止第一控制指令报文下发至网络设备。如果第一控制指令报文的优先级不比第二控制指令报文的优先级低, 则跳转至S903, 判断第一控制指令报文是否具有授权。如果S906的判断结果是没有冲突, 则转到S903。

在S903, 根据业务权限配置文件判断第一控制指令报文是否具有授权。如果没有授权, 跳转至S904, 阻止第一控制指令报文下发至网络设备。可选的, 阻止第一控制指令报文下发至网络设备后, 可以向第一控制指令报文的发送方发送error消息。如果有授权, 在S909, 将第一控制指令报文下发至网络设备。

通过采用本实施方式, 先进行冲突判定再进行授权判断, 可以减少多余的授权判断, 从而加速操作的流程。

可选的, 本发明的方法还包括: 为开放业务平台的管理人员提供一个网络接口平台, 管理人员可以根据业务部署的需要, 随时更改开放业务平台所使用的已授权业务ID表, 例如业务权限配置文件。业务权限配置文件中也可以包括前述S102中所运用的预定规则, 使新增业务配置文件条目满足新增业务的部署需要, 或者更改已部署的业务优先级。如图6所示, 管理人员可以启动新增业务, 并在配置文件中为新增的业务设置业务ID、权限和优先级等参数。

图7是实施本发明的方法的装置的一个简化的例子, 该装置能够执行本发明的方法。可选的, 该装置可以通过例如网络连接与其它装置相连。该装置可以按顺序或并行执行一系列的指令。此外, 尽管图7中只展示了1个装置, 但是应该理解“装置”可以解释为指令执行本发明的方法的单个装置或多个装置的集合。

装置700包括一个处理器702(例如, 中央处理器CPU), 处理器702可以执行计算、选择或比较等功能, 例如, 本发明的方法所包括的S303、S305和S306。主内存704可以存储本发明的方法相关的参数, 例如, 业务权限配置文件和/或全局内部控制指令列表等。静态内存706也可以存储本发明的方法相关的参数, 例如全局内部控制指令列表等。上述处理器702、主内存704和静态内存706通过总线708通信。装置700还可包括磁盘驱动器单元710和网络接口装置712。磁盘驱动器单元710也可以存储本发明的方法相关的参数, 例如全局内部控制指令列表等。网络接口装置712可以使装置700与外部通信, 例如, 步骤S201, 截取发往网络设备的控制指令报文和S309的下发控制指令至网络设备。



磁盘驱动器单元710包括机器可读介质722，机器可读介质722存储一个以上的内部控制指令和执行本发明的方法的数据结构724（例如，软件）。上述内部控制指令也可部分或全部的存储于主内存704或处理器702中。前述的机器可读介质也可以包括内部控制指令和主内存704。此外，前述内部控制指令可以通过网络接口装置712，并利用现有通讯协议，发送至或从网络端726接收。

机器可读介质722可包括存储指令的单介质或多介质（例如，集中或分散式的数据库或与之相关的缓存）。术语“机器可读介质”也可理解为由机器执行的任何可以实施本发明的方法的指令的存储、编码或承载介质。术语“机器可读介质”也可理解为包括固态内存和光磁介质。

根据本发明的一个实施方式，控制网络设备的装置如图8所示，装置800包括数据存储单元801和鉴权冲突控制模块802。其中，数据存储单元801用于存储所截取的发往网络设备的第一控制指令报文和预定规则。鉴权冲突控制模块802可以与数据存储单元801通信，鉴权冲突控制模块802用于从数据存储单元801读取第一控制指令报文和预定规则，并根据预定规则判断第一控制指令报文对网络设备的控制是否符合预定规则，如果不符合预定规则，鉴权冲突控制模块802阻止第一控制指令报文下发至所述网络设备。

可选的，鉴权冲突控制模块802还可以包括鉴权模块804、冲突判断模块803、优先级判断模块806和控制模块807。其中，鉴权模块804用于判断第一控制指令报文对网络设备的控制是否具有授权。冲突判断模块803用于判断第一控制指令报文对网络设备的控制是否与第二控制指令报文对网络设备的控制冲突。当冲突判断模块803判断第一控制指令报文对网络设备的控制与第二控制指令报文对网络设备的控制冲突时，优先级判断模块806用于判断第一控制指令报文的优先级是否比第二控制指令报文的优先级低。当鉴权模块804判断第一控制指令报文对网络设备的控制不具有授权、或者优先级判断模块806判断第一控制指令报文的优先级比第二控制指令报文的优先级低时，控制模块807用于阻止第一控制指令报文下发至所述网络设备。

可选的，数据存储单元801还用于存储已授权业务ID表。鉴权模块804从所述数据存储单元801读取已授权业务ID表，并判断第一控制指令报文相对应的业务是否有授权。

可选的，数据存储单元801还用于存储全局控制指令列表。冲突判断模块803从数据存储单元801读取全局控制指令列表，并判断第一控制指令报文对网络设备的控制是否与第二控制指令报文对网络设备的控制冲突。

可选的，在本发明的实施例中，可以是鉴权模块804确定第一控制指令报文相对应的业务具有授权后，触发冲突判断模块803；也可以是冲突判断模块803确定第一控制指令报文对网络设备的控制与第二控制指令报文对网络设备的控制不冲突后，触发鉴权模块804；也可以是优先级判断模块806判断第一控制指令报文的优先级不比第二控制指令报文的优先级低时，触发鉴权模块804。

进一步可选的，装置800还可以包括转发模块805，当鉴权冲突控制模块802判断第一控制指令报文对网络设备的控制符合预定规则时，转发模块805用于将第一控制指令转发至网络设备。

例如，鉴权模块804确定第一控制指令报文相对应的业务具有授权后，触发冲突判断模块803；如果冲突判断模块803的判断结果为第一控制指令报文对网络设备的控制与第二控制指令报文对网络设备的控制冲突，进一步的优先级判断模块806比较第一控制指令报文的优先级与第二控制指令报文的优先级，如果第一控制指令报文的优先级不低于第二控制指令报文的优先级，触发转发模块805，转发模块805将第一控制指令报文转发至网络设备。

通过以上的实施方式的描述，本领域的普通技术人员可以清楚地了解到本发明实施例可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件来实现。基于这样的理解，本发明实施例的技术方案可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备、或者服务器、或者其他网络设备执行本发明各个实施例或者实施例的某些部分所述的方法。

以上仅为本发明的较佳实施例，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

## 权利要求书

1、一种控制网络设备的方法，其特征在于，包括：

开放业务平台截取发往所述网络设备的第一控制指令报文；

所述开放业务平台判断所述第一控制指令报文对所述网络设备的控制是否符合预定规则；以及

如果不符合所述预定规则，所述开放业务平台阻止所述第一控制指令报文下发至所述网络设备。

2、根据权利要求1所述的方法，其特征在于，所述判断所述第一控制指令报文对所述网络设备的控制是否符合所述预定规则包括：

判断所述第一控制指令报文对所述网络设备的控制是否具有授权；

当所述第一控制指令报文对所述网络设备的控制没有授权时，确定所述第一控制指令报文对所述网络设备的控制不符合预定规则。

3、根据权利要求2所述的方法，其特征在于，所述判断所述第一控制指令报文对所述网络设备的控制是否具有授权包括：

获取与所述第一控制指令报文相对应的业务标识ID；以及

利用已授权业务ID表，判断与所述第一控制指令报文相对应的业务是否有授权。

4、根据权利要求3所述的方法，其特征在于，如果与所述第一控制指令报文相对应的业务没有授权，停止所述第一控制指令报文向所述网络设备的发送。

5、根据权利要求1所述的方法，其特征在于，所述判断所述第一控制指令报文对所述网络设备的控制是否符合预定规则包括：

判断所述第一控制指令报文对所述网络设备的控制是否与第二控制指令报文对所述网络设备的控制冲突；其中，所述第二控制指令报文为所述开放业务平台在所述第一控制指令报文之前截取到的控制指令报文。

6、根据权利要求5所述的方法，其特征在于，

如果所述第一控制指令报文对所述网络设备的控制与所述第二控制指令报文对所述网络设备的控制冲突，比较所述第一控制指令报文的优先级与所述第二控制指令报文的优先级；以及

如果所述第一控制指令报文的优先级低于所述第二控制指令报文的优先级，确定所述第一控制指令报文对所述网络设备的控制不符合预定规则。

7、一种控制网络设备的装置，其特征在于所述装置包括鉴权冲突控制模块和数据存储单元；

所述数据存储单元用于存储所截取的发往所述网络设备的第一控制指令报文和预定规则；

所述鉴权冲突控制模块用于从数据存储单元读取所述第一控制指令报文和所述预定规则，并根据所述预定规则判断所述第一控制指令报文对网络设备的控制是否符合所述预定规则；以及

如果不符合所述预定规则，所述鉴权冲突控制模块阻止所述第一控制指令报文下发至所述网络设备。

8、根据权利要求7所述的装置，其特征在于，所述鉴权冲突控制模块还包括鉴权模块；

所述鉴权模块用于判断所述第一控制指令报文对网络设备的控制是否具有授权。

9、根据权利要求8所述的装置，其特征在于，所述数据存储单元还用于存储已授权业务ID表；

所述鉴权模块用于获取所述第一控制指令报文相对应的业务标识；以及

所述鉴权模块从所述数据存储单元读取所述已授权业务ID表，并利用所述已授权业务表项判断所述的第一控制指令报文相对应的业务是否有授权；

所述鉴权模块判断结果是所述第一控制指令报文相对应的业务没有授权，则所述鉴权模块停止所述第一控制指令报文向所述网络设备的发送。

10、根据权利要求7所述的装置，其特征在于，所述鉴权冲突控制模块还包括冲突控制模块，所述冲突控制模块用于判断所述第一控制指令报文对所述网络设备的控制是否与第二控制指令报文对所述网络设备的控制冲突；以及

所述第二控制指令报文为所述数据存储单元所存储的、在所述第一控制指令报文之前截取到的控制指令报文。

11、根据权利要求10所述的装置，其特征在于，如果所述第一控制指令报文对所述网络设备的控制与所述第二控制指令报文对所述网络设备的控制冲

突,所述冲突控制模块比较所述第一控制指令报文的优先级与所述第二控制指令报文的优先级; 以及

如果所述第一控制指令报文的优先级低于所述第二控制指令报文的优先级,所述冲突控制模块确定所述第一控制指令报文对所述网络设备的控制不符合预定规则。

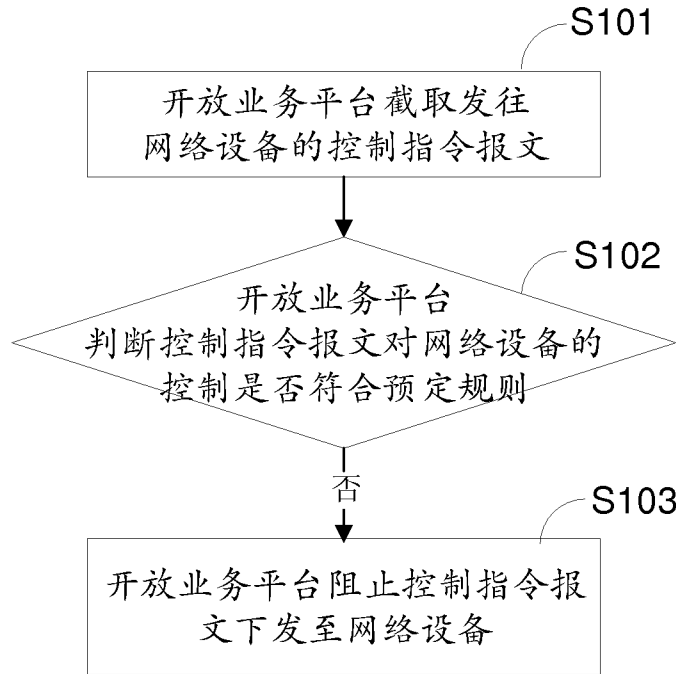


图 1

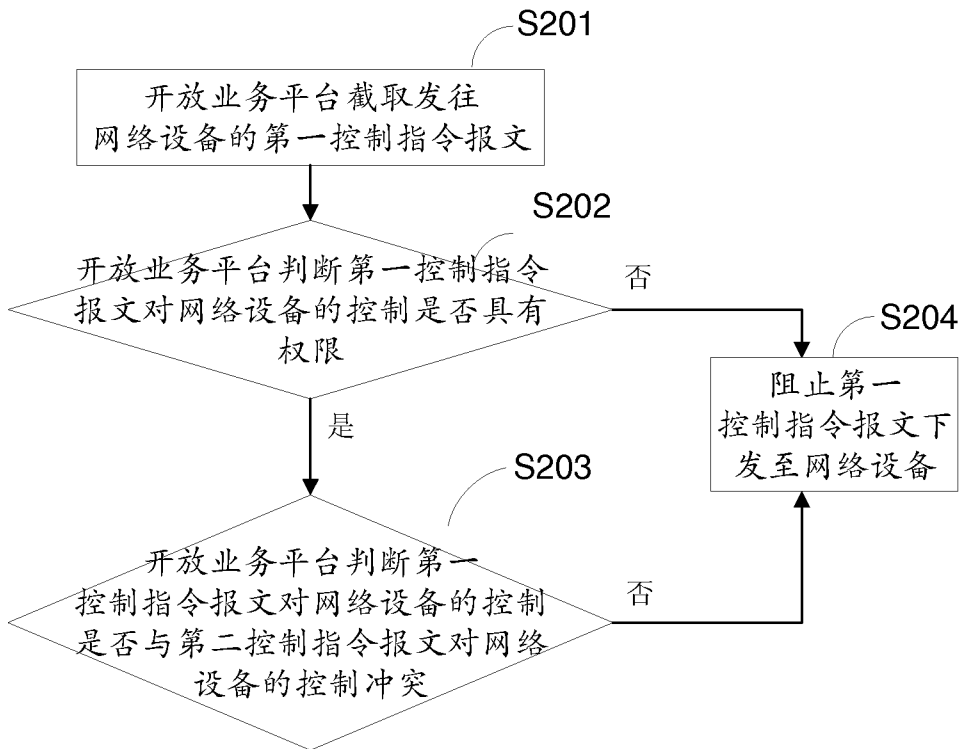


图 2a

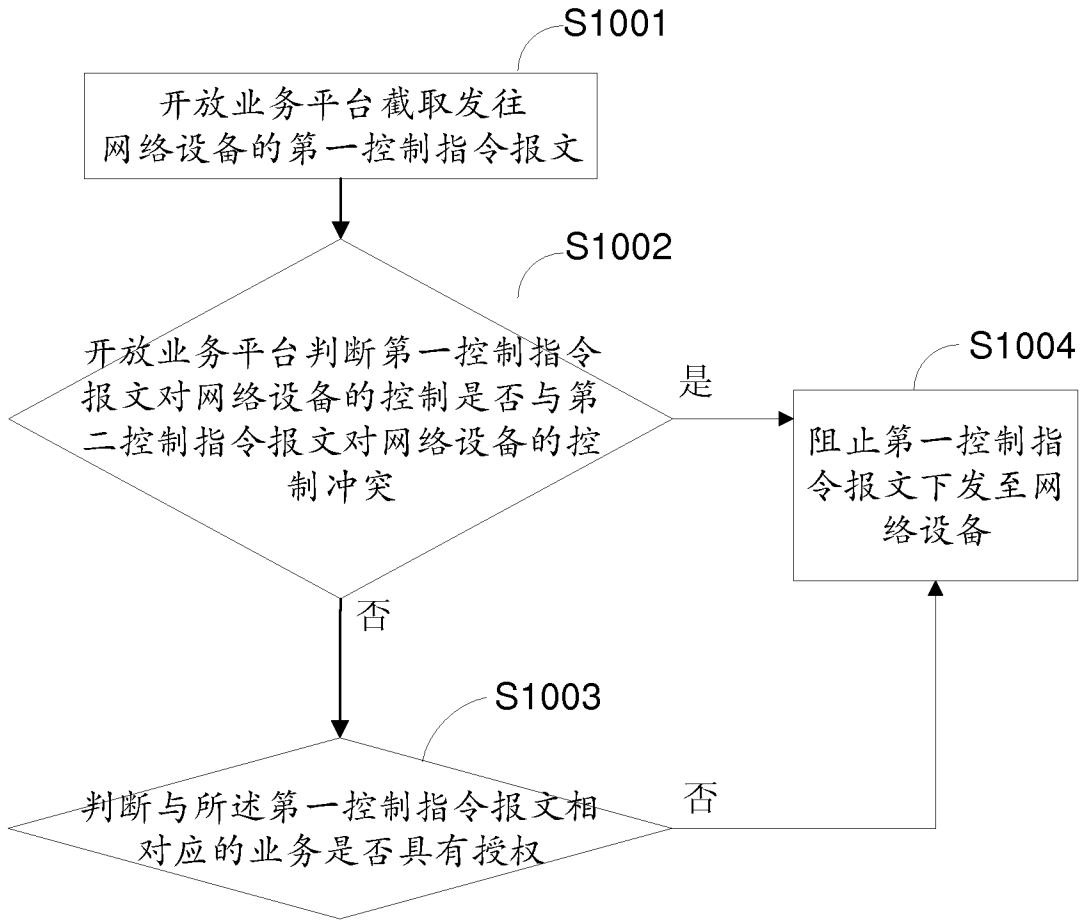


图 2b



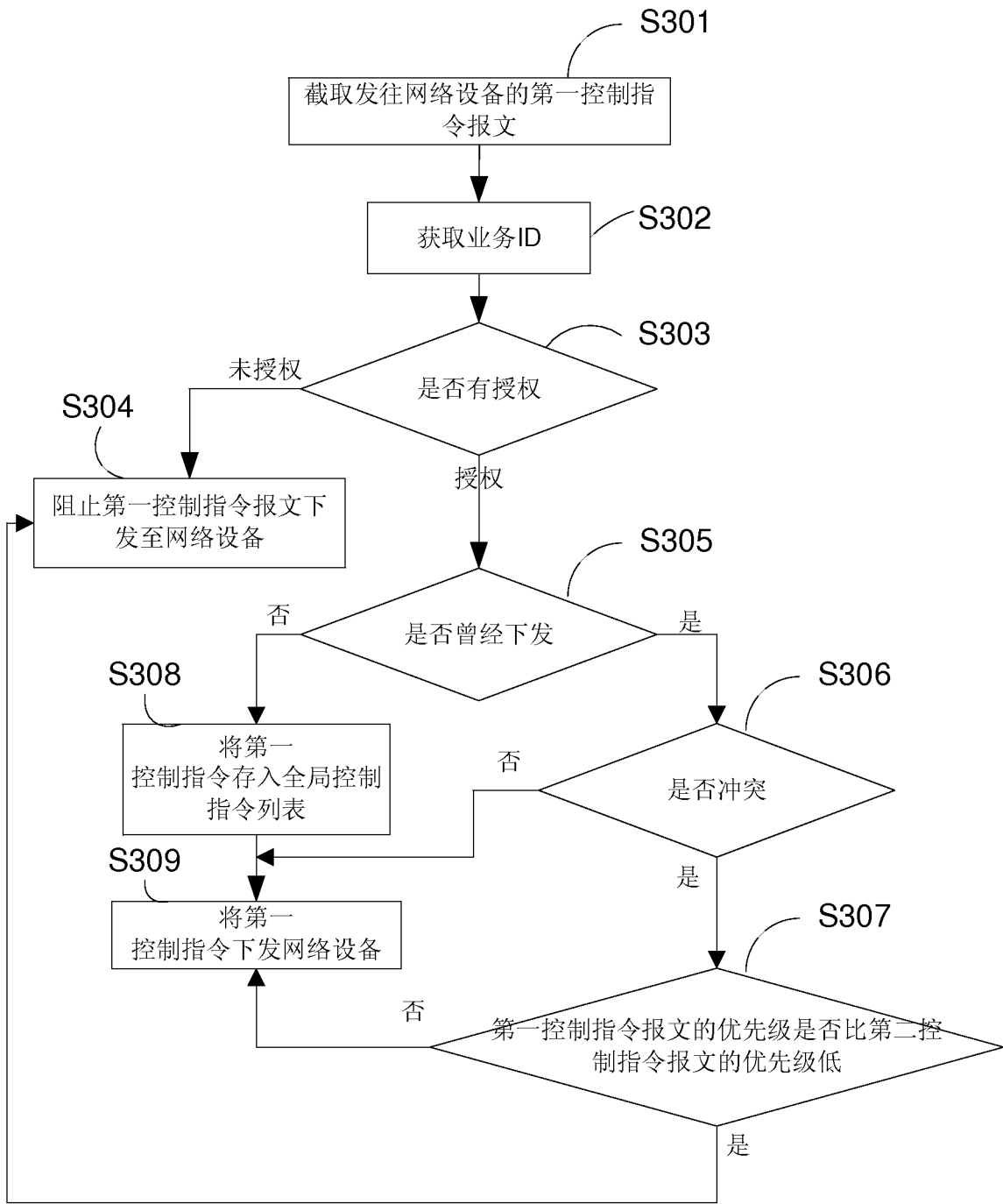


图 3a

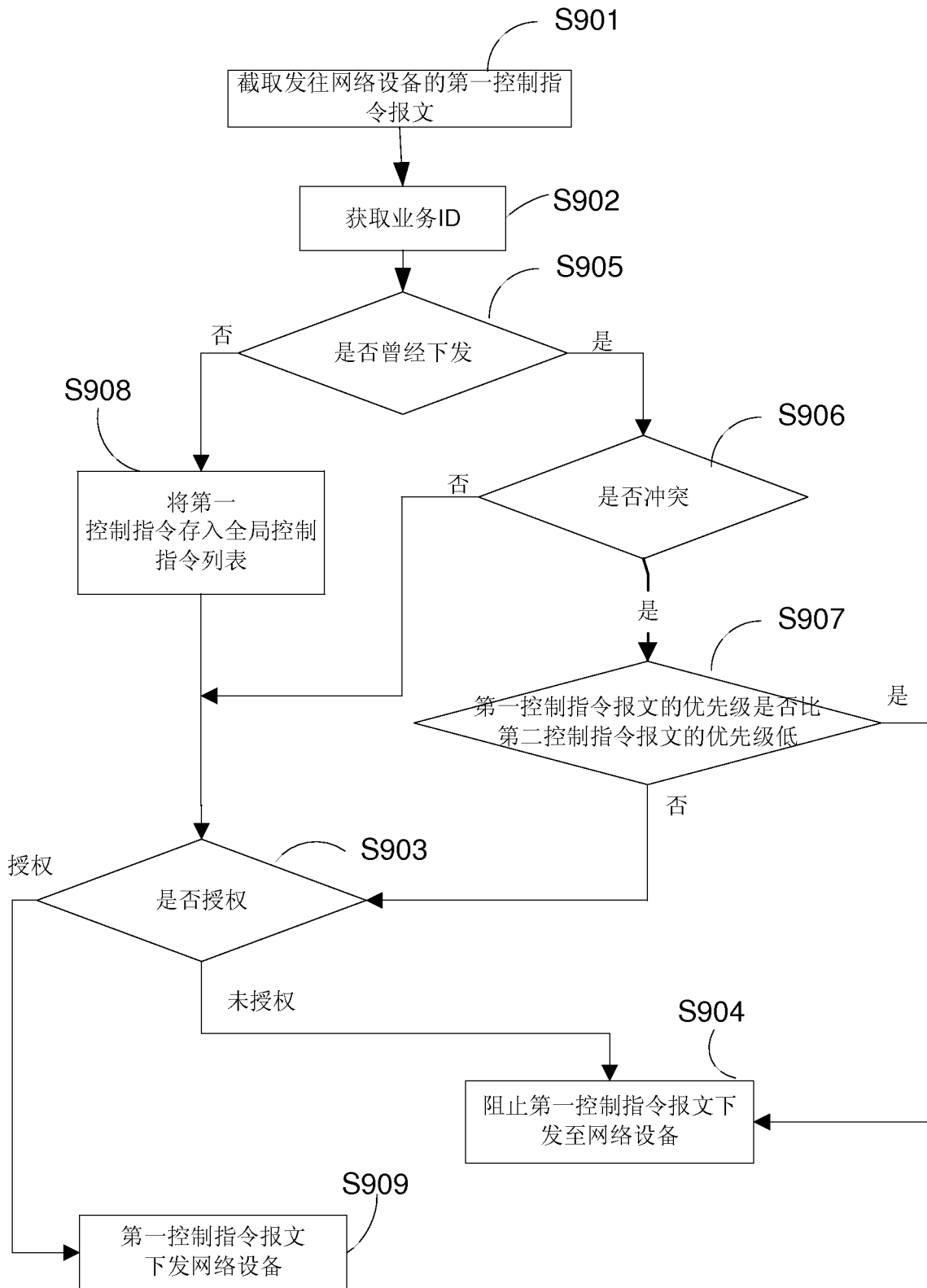


图 3b

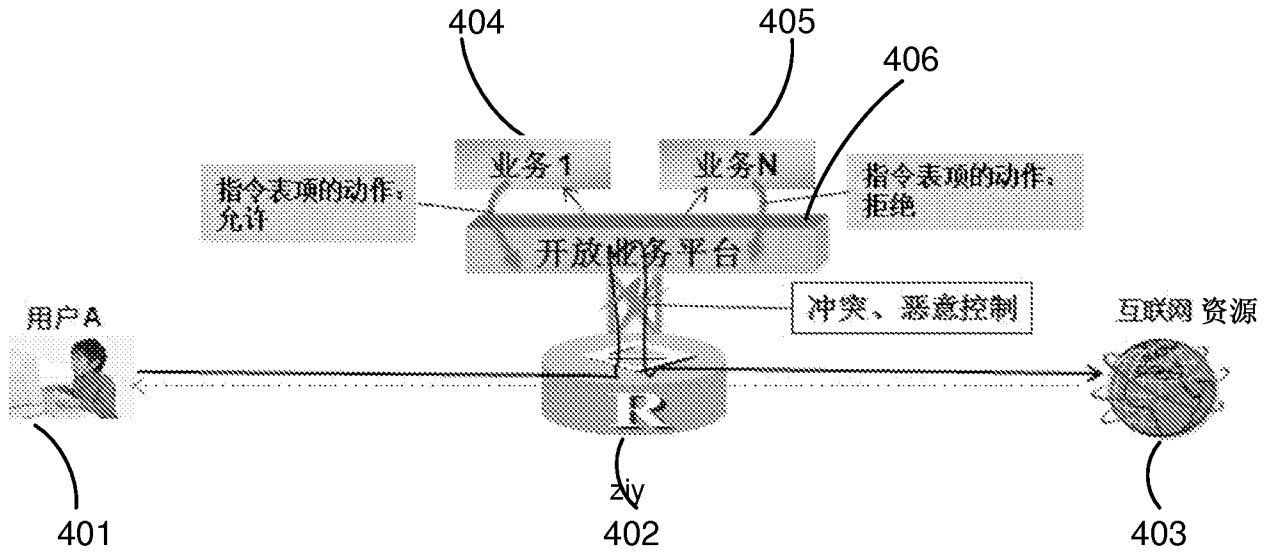


图 4

```
#Service ID, Priority  
  
12, 5,  
  
20, 6
```

图 5a

```
#Service ID, Priority, Packet Service Type  
  
12, 5, video  
  
20, 6, ftp  
  
21, 1, P2P
```

图 5b

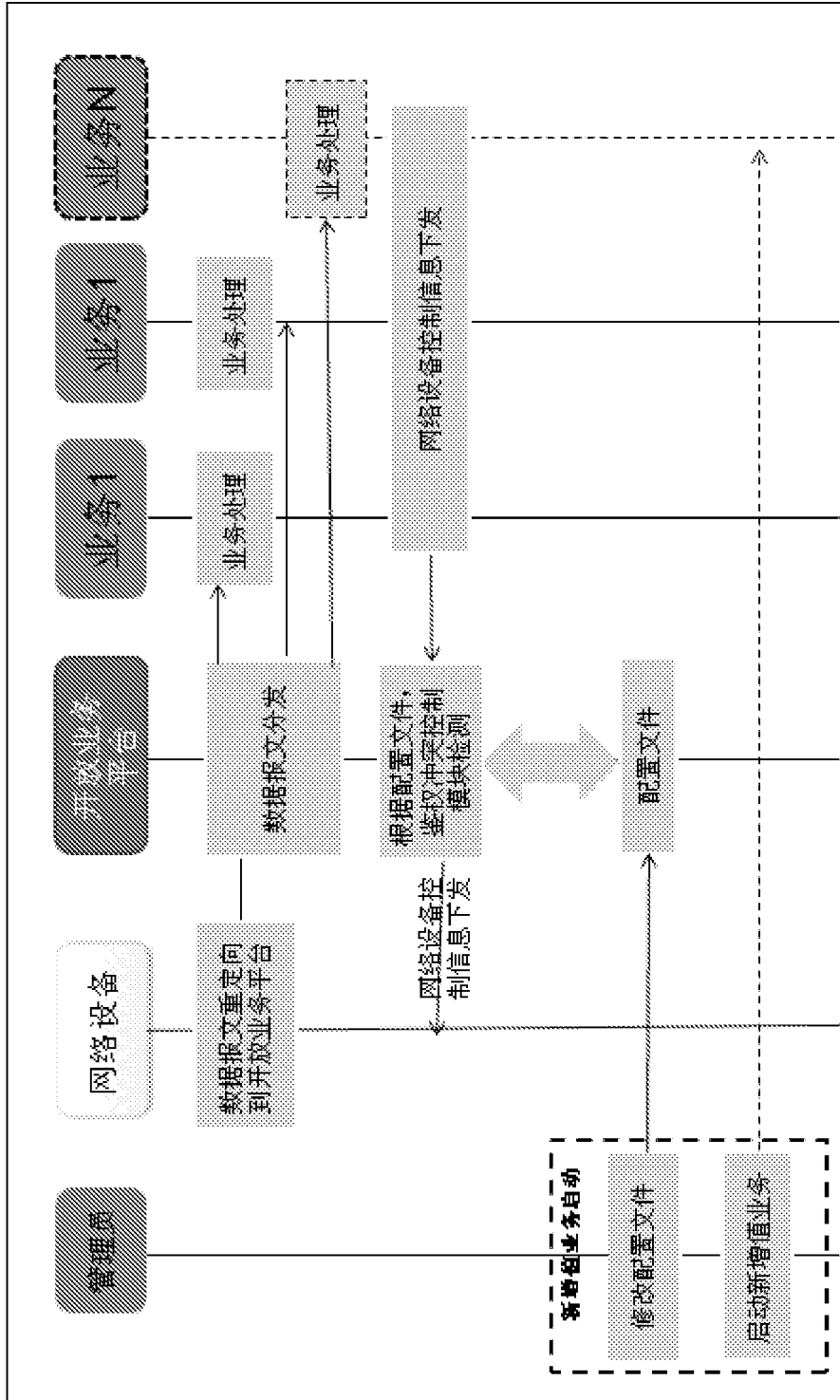


图 6

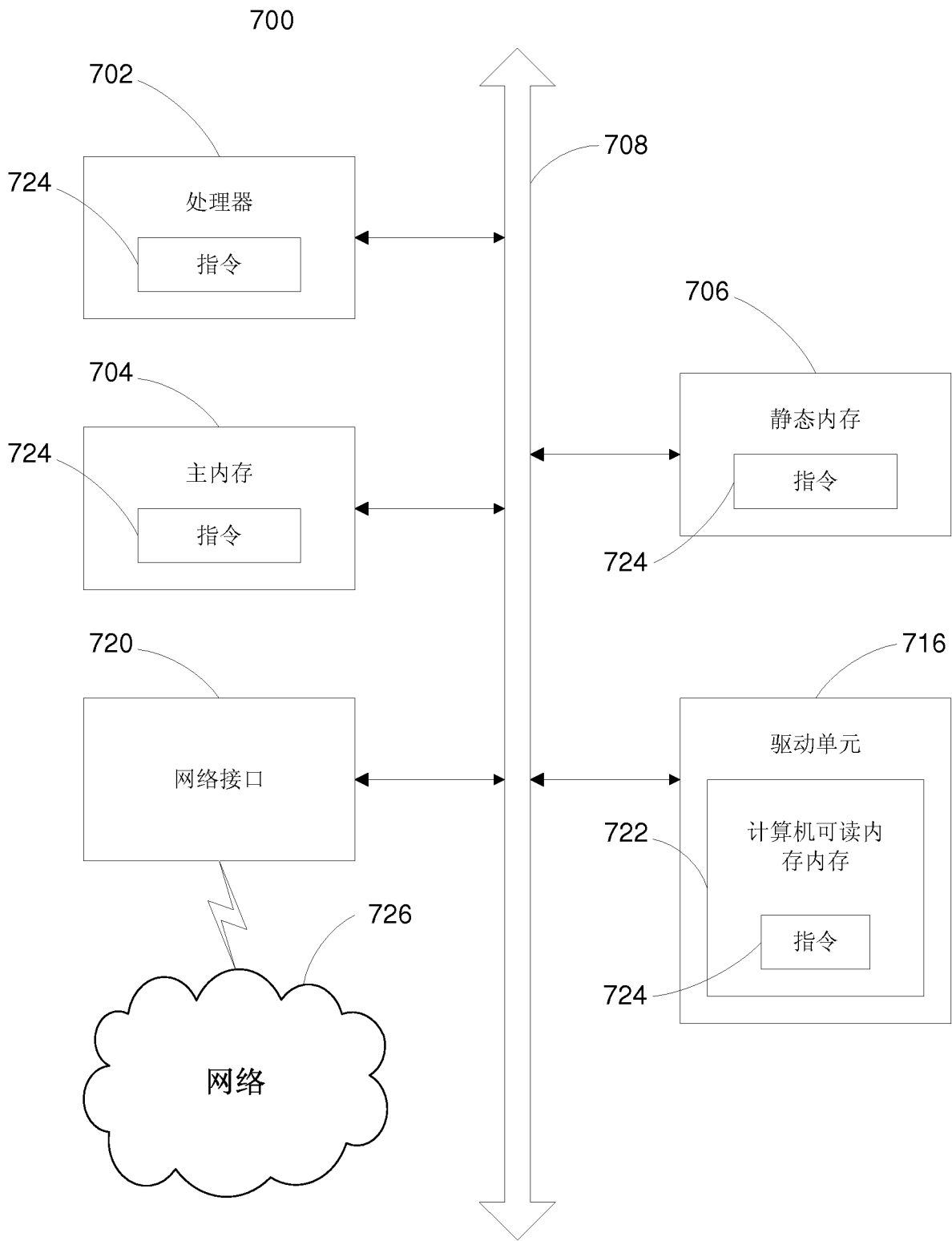


图 7

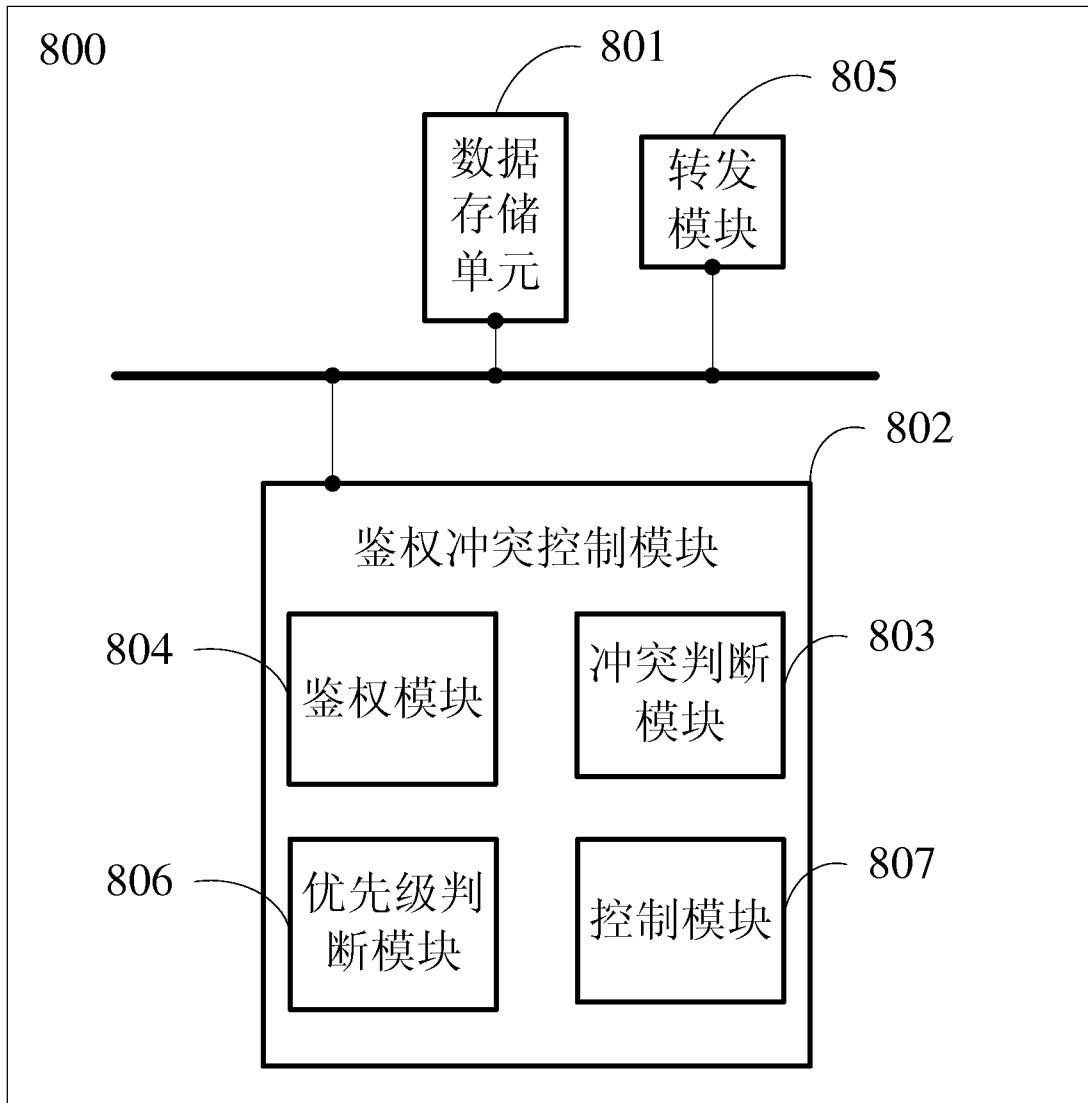


图 8