

(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



PCT



(43) 国际公布日
2008 年 7 月 10 日 (10.07.2008)

(10) 国际公布号
WO 2008/080314 A1

(51) 国际专利分类号:
H04L 12/56 (2006.01)

(21) 国际申请号: PCT/CN2007/070551

(22) 国际申请日: 2007 年 8 月 24 日 (24.08.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200610064671.X
2006 年 12 月 29 日 (29.12.2006) CN

(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): 宋端智(SONG, Du-anzhi) [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)。 杨平安(YANG, Ping'an) [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)。 熊怡(XIONG, Yi) [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)。

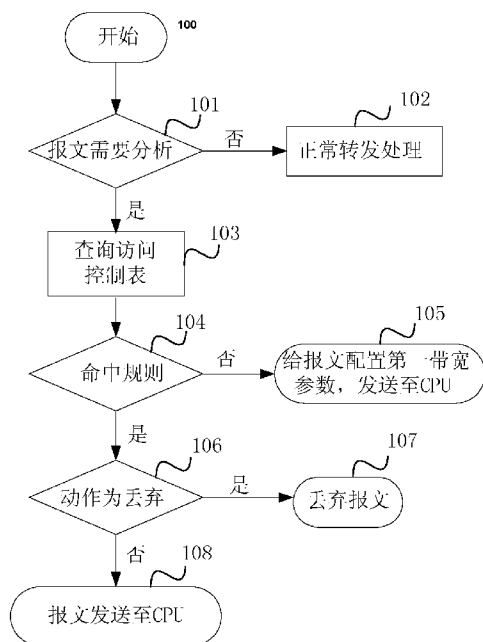
(74) 代理人: 北京集佳知识产权代理有限公司(UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (CN)。

(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, AT, AU, AZ, BA, BB, BG,

[见续页]

(54) Title: A METHOD, FORWARDING ENGINE AND COMMUNICATION DEVICE FOR MESSAGE ACCESS CONTROL

(54) 发明名称: 报文访问控制的方法、转发引擎和通信设备



100 ... START
101 ... MESSAGE NEED BE ANALYZED
102 ... FORWARDED NORMALLY
103 ... INQUIRING THE ACCESS CONTROL LIST
104 ... HITTING THE RULE
105 ... CONFIGURING THE FIRST BANDWIDTH PARAMETER FOR THE MESSAGE
AND TRANSMITTING THE MESSAGE TO CPU
106 ... THE ACTION IS DISCARDING
107 ... DISCARDING THE MESSAGE
108 ... TRANSMITTING THE MESSAGE TO CPU
109 ... YES
110 ... NO

(57) Abstract: A method for message access control is disclosed. Said method comprises the following steps: setting up the first bandwidth parameter in the forwarding engine, and determining whether said message need be retransmitted according to the message information; inquiring the access control list according to the message information if the message need not be retransmitted; executing the corresponding action if the rule is hit, and transmitting the message to the control plane with the first bandwidth parameter if the rule is not hit. Moreover, a message forwarding engine and a communication device are also disclosed. Said method, said message forwarding engine and said communication device can control carefully and guarantee the stable running of service simultaneously, and they can increase the stability of the device and the availability of the whole network.

[见续页]



BH, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

(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, LS, MW, MZ, NA,

本国际公布:

— 包括国际检索报告。

(57) 摘要:

本发明提供了一种报文访问控制的方法, 包括: 在转发引擎设置第一带宽参数, 根据报文信息判断所述报文是否需要转发, 如果不需要转发, 则根据所述报文的信息查询所述访问控制表, 如果命中, 则执行相应动作; 否则, 给所述报文应用第一带宽参数, 发送至控制平面。另外, 本发明还提供了一种报文转发引擎和通信设备, 利用本发明提供的方法、报文转发引擎和通信设备, 均可以同时兼顾精细控制和保证业务运行稳定, 有效地提高设备的稳定性和整个网络的可用性。

报文访问控制的方法、转发引擎和通信设备

本申请要求于 2006 年 12 月 29 日提交中国专利局、申请号为 200610064671.X、发明名称为“报文访问控制的方法、转发引擎和通信设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及通信技术领域，尤其涉及一种报文访问控制的方法、转发引擎和通信设备。

背景技术

10 由于Internet网络流量越来越大，对数据通信网络设备的性能要求越来越高。纯软件转发的网络设备逐渐被淘汰，更多的设备采用硬件转发来提高性能。

相对于软件转发来说，硬件转发的灵活性较差，如果仅仅依靠硬件转发引擎，如专用集成电路（ASIC，Application-Specific Integrated Circuit）和网络处理器（NPU，Network Processing Unit）等，许多功能都将无法实现或很
15 难实现。因此，一般的网络设备在提供硬件转发的同时，还提供CPU等用于完成转发引擎难以完成的功能，以兼顾性能和灵活性。在数据通信设备中，包含有称之为数据平面和控制平面的部分，数据平面主要包含硬件转发引擎和交换网、物理层接口等，用于完成大部分数据报文的转发；控制平面主要包含CPU及其周边设备（如内存等），用于完成设备的管理和控制、
20 需要软件参与的数据报文（如路由协议报文、网管交互报文等）的处理等任务。

如图1所示的典型的集中式数据通信网络设备的结构和如图2所示的典型
的分布式数据通信网络设备的结构，其中实线为数据报文的转发路径，虚线为控制报文/控制消息的通道。

25 一般情况下，网络设备收到的大部分数据报文都会在数据平面内部直接找到目的地并发送出去，但部分数据报文仍需要控制平面的参与，比如：网络设备之间交互的协议报文（最常见的是路由协议报文）；其他终端或设备发给本设备的报文（如网管发过来的配置请求等）和途经本设备，但

-2-

需要特殊处理的报文（如IP报文，TTL（time to live，生存时间）超时报文等）。

这些数据报文在被转发引擎识别出来之后，通过转发引擎和CPU之间的通道(以下简称控制通道)发送给CPU进行处理，同样，CPU也会有一些报文通过该控制通道从转发引擎转发出去。需要说明的是，对图2所示的典型的分布式数据通信网络设备来说，控制平面不仅包括线路卡上的CPU，还包括控制卡上的CPU。因此，控制通道不仅包含线路卡上的转发引擎和CPU之间的通道，还包括线路卡和控制卡CPU之间的通道。

在这样的架构下，由于CPU自身处理能力和控制通道带宽的限制，网络设备很容易受到有意或无意的拒绝服务(Denial of Service, DOS)攻击(无意的攻击可能的来源有蠕虫病毒、网络风暴等)，如果数据平面短时间内发送的流量过大，会造成控制通道拥塞，导致发送的部分报文丢包；如果控制平面发送流量过大，CPU忙于处理发送的某种报文，便会无暇进行其他处理。

上述这两种后果都可能造成设备或网络故障。如何防范此类攻击是网络设备必须要考虑的问题。

通常，转发引擎判断某个报文是否需要发送是基于报文内容的某些字段，比如目的IP地址、协议号、端口号等。但它判断出来需要发送的报文，对于控制平面来说，可能是没用的，也就是说，本来就无需发送(将这种对控制平面无用的报文称为垃圾报文)，但垃圾报文被发送的情况是普遍存在的，在发送报文总流量中占据了较大的比例。

出现这种情况的原因在于：虽然网络设备支持众多功能，但在某个具体的应用场景中，可能仅仅使用了该设备的很小一部分功能，属于其他未用功能的报文发送控制平面后，经过一些处理，最终会发现报文无用而将其丢弃。但这些报文既占用了控制通道的带宽，又占用了CPU的处理时间。一旦这些报文流量过大，就可能造成其他正常报文无法发送或正常业务来不及处理，出现前述的DOS攻击结果。

在现有技术中，有一种做法是转发引擎将可能发送的报文进行分类，在每种报文发送前进行带宽限制，并且该带宽是可配置的。一旦发现某设

-3-

备中某种报文发送流量较大，并且该种报文对于当前业务来说是无用的，这时根据设备当前配置可以通过更改带宽配置限制该种报文的发送，以避免出现DOS攻击。

但是，为了不影响正常业务，针对不同类别的报文设置的缺省带宽参数都比较大，以避免在使用该类报文对应的业务时出现问题。使用缺省参数处理发送报文，仍会出现垃圾报文占用较多控制通道带宽；并且，仅仅根据报文分类，就很难做到精细控制，比如限制只有某个源地址发送过来的某种报文才发送。

针对这一问题，现有技术的另一种做法就是手工配置访问控制列表 (ACL, Access Control List)，在转发引擎将报文送入控制通道前，查询设备配置特定ACL规则，根据命中规则对应的动作进行处理，可能将报文丢弃，也可能限制该类报文的带宽。其中比较常用的做法是在ACL中配置需要丢弃的报文信息，而这种情况下，需要设备维护人员对设备具体实现细节了解较多，配置成本高，且容易出错，往往会使得部分垃圾报文仍然被发送到CPU，仍然难以有效解决垃圾报文过多占用控制通道带宽的问题，难以精细控制；还有一种作法是在ACL中配置需要送给CPU处理的报文信息，未配置的报文则被丢弃，在这种情况下，由于需要手工配置，则对配置者要求较高，一些与业务实现有关的报文可能会被错误地配置，导致错误丢弃，使得业务运行不正常，而在新的业务建立或者连接建立的情况下，如果未事先配置ACL规则，则还需要再次配置ACL，影响了业务运行的效率。

发明内容

本发明提供一种报文访问控制的方法、转发引擎和一种通信设备，能同时兼顾精细控制和保证业务运行稳定。

本发明提供一种报文访问控制的方法，包括：

25 当接收到的报文不需要进行转发处理时，根据所述报文的信息查询访问控制表，如果命中访问控制表规则，则根据所述访问控制表规则对所述报文进行相应操作；

如果没有命中访问控制表规则，应用第一带宽参数所提供的带宽，将所述报文发送给控制平面；

-4-

所述报文的信息包括源 IP 地址、目的 IP 地址、源端口、目的端口、协议号中至少之一。

本发明提供的又一种报文访问控制的方法，包括：

当接收到的报文不需要进行转发处理时，根据所述报文的信息查询访问控制表；

如果没有命中访问控制表规则，应用第一带宽参数所提供的带宽，将所述报文发送给控制平面；

如果命中访问控制表规则，应用第二带宽参数所提供的带宽，将所述报文发送给控制平面；

10 其中，应用所述第二带宽参数所提供的带宽大于应用所述第一带宽参数所提供的带宽。

本发明提供一种报文转发引擎，包括设置模块、存储模块、接收模块、转发判断模块、访问控制模块和处理模块，

设置模块，用于设置带宽参数；

15 存储模块，用于存储并更新访问控制表；

接收模块，用于接收报文；

转发判断模块，用于根据所述接收模块所接收报文的信息，判断所述报文是否需要转发；

20 访问控制模块，用于查询所述控制表中的访问控制规则；当所述转发判断模块判断所述报文不需要转发时，所述访问控制模块根据所述报文的信息，查询所述存储模块中存储的访问控制规则；

25 当所述访问控制模块命中所述访问控制规则时，所述处理模块根据所命中的访问控制规则对所述接收模块接收的报文进行操作；否则，所述处理模块给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数，发送至控制平面。

本发明提供的一种通信设备，包括控制单元和数据单元，

控制单元，用于配置访问控制表和处理报文；

数据单元，用于设置带宽参数，根据所接收报文的信息判断所述报文是否需要转发，如果不需要转发，则根据所述报文的信息查询所述控制单

-5-

元配置的访问控制表，如果命中，则执行相应操作；否则，应用所设置的带宽参数将所述报文发送给所述控制单元。

利用本发明提供的报文访问控制的方法、报文转发引擎和通信设备，由于对报文访问控制采取了事先的配置，并且对未命中访问控制表规则的
5 报文配置一个带宽参数，可以在降低已知垃圾报文对设备控制平面造成影响的同时，防止对业务实现所必需的报文不被遗漏丢弃，保证业务的正常运行，有效地提高设备的稳定性和整个网络的可用性。

附图说明

- 图 1 为现有技术中典型集中式数据通信网络设备结构示意图；
10 图 2 为现有技术中典型分布式数据通信网络设备结构示意图；
图 3 为本发明实施例中提供的报文访问控制方法的流程图；
图 4 为本发明一个实施例中提供的报文转发引擎的示意图；
图 5 为本发明一个实施例中提供的通信设备的示意图。

具体实施方式

- 15 本发明所提供的实施例中，转发引擎根据报文的信息查询访问控制表，如果命中访问控制表规则，就执行相应的动作；否则，就给报文配置一个带宽参数，发送至控制平面，例如 CPU。

- 访问控制表可以包括普通意义上的访问控制列表 ACL 和特殊的 ACL，所谓普通的访问控制列表则是包含五元组信息（源 IP 地址、目的 IP 地址、
20 源端口、目的端口、协议号）的访问控制表，而特殊的访问控制表则是只包含五元组中部分字段的访问控制列表，比如只包含源端口或者源 IP 地址等字段信息。

- 在本发明所提供的的一个实施例中，转发引擎需要设置第一带宽参数，对于未在访问控制表中配置，而对业务实现所必需的报文，可以应用第一
25 带宽参数所提供的带宽发送，因此上述的报文不会因为未命中访问控制表而被错误丢弃，造成业务运行的不正常，其中，该第一带宽参数则可以任意设置，优选的将该参数设置成小于总带宽的一半。此外，还可以设置第二带宽参数，在命中访问控制表并根据控制规则需要发送报文给控制平面的情况下，可以应用第二带宽参数所提供的带宽发送，该第

-6-

二带宽参数可以比第一带宽参数大，以使得命中访问控制表而需要发送的报文比未命中访问控制表的报文获得更大的带宽。

访问控制表的配置可以有多种方法，可以手工配置该访问控制表，也可以在设备的运行过程中，由设备对访问控制表进行再配置或者更新原先的访问控制表。由于未命中访问控制表规则的报文仍然可以获得一个带宽，从而保证了新的业务或者连接成功建立的时候，原先不在访问控制表中配置的报文仍然可以发送到控制平面进行处理，尤其是发送到CPU。例如，该通信设备根据当前配置的业务或者和其他设备或终端之间建立的会话，进行配置访问控制表规则及其动作的发送或删除等处理。

- 10 当设备在配置某种新业务时，如果与新业务相关的报文并没有事先在访问控制表中进行配置，报文会以第一带宽参数所提供的带宽发送到控制平面中进行处理，控制平面判断该新业务相关的种报文是否与特定业务相关，即，是否需要一直由控制平面对该新业务相关的报文进行处理，如果需要，则发送相应的访问控制表规则，或者同时根据该业务的重要性发送该类报文对应的优先级等信息，更新原有的访问控制表。比如，设备可以允许终端通过远程登陆的方式管理该设备，为实现该功能，需要通过配置使能设备的Telnet的服务，并设置登录权限进行限制，只允许某个或某些终端才能登陆设备(防止非法用户登陆)。根据Telnet报文的特点(目的端口号为23，协议号为传输控制协议(TCP, Transfer Control
- 15 Protocol))，以及限制的终端IP地址信息，提取五元组中的三个信息：源IP地址、目的端口、协议号，组成相应的访问控制表规则发送到数据平面。

- 25 在控制平面所在的网络设备和其他设备或终端动态建立会话(如TCP连接)的情况下，如果控制平面根据当前会话的信息分析该会话建立成功，则会发送相应的访问控制规则，或者同时根据该会话的重要性发送该类报文对应的优先级等信息，更新原有的访问控制表。比如，两个路由器A和B通过某种路由协议交互路由信息，在正式交互路由信息之前，需要相互进行认证，以防止其他非法终端仿冒。这个认证的过程一般需要几次握手交互，在这几次握手过程中，A和B相互将自己的信息告

-7-

知对方，可能包括需要认证的密码等加密信息。在相互认可对方后，两个设备之间的会话(连接)才正式建立，在协议连接建立后，设备控制层面将标识连接的元素(比如五元组：源IP地址、目的IP地址、源端口、目的端口、协议号)组成相应的访问控制表规则发送到数据平面。

- 5 在上述配置访问控制表的方法中，五元组中的信息，即源IP地址、目的IP地址、源端口、目的端口、协议号，可以单独或者任意组合，形成普通意义上的访问控制表规则或特殊的访问控制表规则，并根据该访问控制表配置相应的动作，或者同时根据该业务或者会话的重要性下发该类报文对应的优先级等信息，或者还可以配置成只要与访问控制表匹配便丢弃报文。
- 10

为使本发明的目的、技术方案及优点更加清楚明白，以下参照附图并举较佳实施例，对本发明进一步详细说明。

- 在本发明所提供的报文访问控制的方法的一个实施例中，可以事先设置好各种参数和访问控制表，也可以不必事先配置。如图3所示，本发明提供的实施例中报文访问控制的方法流程，包括如下步骤：
- 15

步骤 101：转发引擎根据报文信息判断所述报文是否需要转发，如果不需要转发，则执行步骤 103，否则执行步骤 102。

一般而言，对如下几种情况的报文需要进行分析：

- 20 1) 本设备的报文需要发送，如FTP、Telnet等报文；
- 2) 广播或组播的协议报文需要发送，如路由协议报文、ARP请求报文等；
- 3) 途经本设备的报文在处理过程中发现有错，需通知报文源时需要发送，如目的不可达时。

- 转发引擎通过查询特定表进行判断，如当涉及到IP报文转发时，转发引擎可以查询转发表，如果可以直接转发，执行步骤 102，报文进行正常转发处理，而无需再发送到控制平面，否则执行步骤 103，继续本流程。
- 25

步骤 102：报文进行正常转发处理。

步骤 103：转发引擎根据报文的信息查询访问控制表。

当然，这里也可以再增加一个步骤，即在报文需要发送到控制平面时，先查询一下有无访问控制表存在，如果存在访问控制表，则按照步骤 103 进行查询，如果不存在访问控制表，报文仍然会发送到控制平面，但为了防止占用全部带宽，报文会应用第一带宽参数所提供的带宽发送。

5 步骤 104：根据访问控制表中内容判断是否命中访问控制表规则。

步骤 105：如果没有命中访问控制表规则，则给报文应用第一带宽参数所提供的带宽发送到控制平面，比如 CPU。通常可以将第一带宽参数设置成小于总带宽的一半，也就是给该没有命中访问控制表规则的报文配置的带宽比较小。

10 步骤 106：如果命中访问控制表规则，则判断相应的动作是否是丢弃报文，如果是的话，则执行步骤 107，否则执行步骤 108。当然，如果没有设置丢弃的动作，也可以省略该步骤，只要命中访问控制表规则就执行步骤 108。

步骤 107：丢弃报文。

15 步骤 108：将报文发送至控制平面，比如 CPU。在本步骤中，报文应用第二带宽参数所提供的带宽发送，还可以同时根据设置的优先级进行发送，例如，优先级大的报文优先使用第二带宽参数所提供的带宽发送至 CPU。优选地，第二带宽参数大于第一带宽参数，这样就保证了命中规则的报文可以获得较大的带宽，而未命中规则的报文则获得较小的带宽。

20 如果以第一带宽参数所提供的带宽发送的报文经过控制平面的分析，认为需要继续发送的，则根据报文的信息发送访问控制表规则，同时规定具体的动作，将这些信息再发送到转发引擎中，并更新原有的访问控制表，将报文的相关信息以及所对应的具体动作加入到访问控制表中。尤其是，当原先并不存在访问控制表时，根据控制平面的处理，生成访问控制表并发送到转发引擎。

最后，如果在取消某种业务的配置或拆除会话时，可以相应地删除对应的访问控制表规则。

在本实施例中，步骤序号仅仅是为了介绍本实施例的方便而设置，

并不表示各步骤需按照序号的顺序进行。

在本发明的实施例中，在设备本身未存储访问控制表或未命中访问控制表规则的情况下，报文仍然还可以以第一带宽参数所提供的带宽发送到控制平面处理，这样就可以很好地解决现有技术中不能同时兼顾精细控制和保证业务运行稳定的问题，可以有效地对访问控制表形成补充，防止一些对业务实现所必需的报文不会因为可能未命中访问控制表而被错误丢弃，造成业务运行的不正常，在这个意义上，可以有效地提高设备的稳定性和整个网络的可用性，保证了业务的正常运行。

5 本发明的实施例还提供了一种报文转发引擎，如图4所示。该转发引擎可以包括设置模块、存储模块、接收模块、转发判断模块、访问控制模块和处理模块，

设置模块，用于设置带宽参数，在本发明的实施例中，该设置模块用于设置第一带宽参数和第二带宽参数；具体参数的设置以及目的可以参照前述方法实施例的介绍，在此就不再赘述；

15 存储模块，用于存储并更新访问控制表；

接收模块，用于接收报文；

转发判断模块，用于根据所述接收模块接收的所述报文的报文信息，判断所述报文是否需要转发，

20 一般而言，可以由源IP地址、目的IP地址、源端口、目的端口、协议号中的一个或者多个组成报文信息。

访问控制模块，当所述转发判断模块判断的结果为所述报文不需要转发时，根据所述接收模块接收的所述报文的信息，查询所述存储模块中存储的所述访问控制表规则，

该访问控制模块还包括查询模块和判断模块，

25 查询模块，当所述转发判断模块判断的结果为不需要转发时，用于查询所述存储模块中是否存储有所述访问控制表；在本发明实施例中，并不必然要求对访问控制表进行事先配置，

判断模块，当所述查询模块的查询结果为存在所述访问控制表时，根据所述接收模块接收的报文的信息，查询所述存储模块中存储的所述访问

控制表规则，

当所述查询模块的查询结果为不存在所述访问控制表时，所述处理模块给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数，发送至控制平面。也就是说，在不存在访问控制表的情况下，报文仍然可以直接发送到控制平面，但是会应用一个较小的带宽发送，在发送到控制平面以后，再根据相应的分析，下发访问控制表至转发引擎，该转发引擎可以在降低已知垃圾报文对设备控制平面造成的影响的同时，防止对业务实现所必需的报文不被遗漏丢弃，保证业务的正常运行，有效地提高设备的稳定性和整个网络的可用性，

10 在所述访问控制模块的分析结果为命中所述存储模块中存储的所述访问控制表规则时，发送模块给所述接收模块接收的报文应用所述设置模块设置的第二带宽参数，当然前提是设置模块还设置了第二带宽参数，将所述报文发送至控制平面；

处理模块，当所述访问控制模块的分析结果为命中所述访问控制表规则时，执行相应动作；否则，给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数，发送至控制平面，

处理模块还包括转发模块，在转发判断模块判断的结果为需要转发时，用于正常转发所述接收模块接收的所述报文；

20 处理模块还包括丢弃模块和发送模块，其中丢弃模块，根据所命中的访问控制表规则，丢弃所述接收模块接收的报文；发送模块用于将所述接收模块接收的所述报文发送至所述控制平面。

同时，本发明还公开了一种通信设备，如图5所示，该通信设备包括控制单元和数据单元，其中控制单元，用于配置访问控制表和处理报文；数据单元，用于设置第一带宽参数，在报文到来时，根据报文信息判断所述报文是否需要转发，如果不需要转发，则根据所述报文的信息查询所述控制单元配置并下发的访问控制表，如果命中，则执行相应动作；否则，给所述报文应用第一带宽参数，发送至所述控制单元。

尤其是，数据单元中还可以包括本发明提供的报文转发引擎。而且，如果以第一带宽参数发送的报文经过控制单元的分析，认为在以后还需

要继续发送的，则根据报文的信息下发 ACL 访问控制表规则，同时规定具体的动作，认为不再需要发送的，也可以同样下发 ACL 访问控制表，只是将动作规定为丢弃报文，然后，将这些信息再下发到转发引擎中的存储模块，更新原有存储模块中存储的 ACL 访问控制表，如果原先并不存在 ACL 访问控制表的话，则根据这些信息建立一个 ACL 访问控制表，保存在转发引擎中。

该设备由于包含了本发明实施例所提供的转发引擎，对未命中访问控制表规则的报文配置一个带宽参数，加之对报文访问控制的配置，可以在降低已知垃圾报文对设备控制平面造成的影响的同时，防止对业务实现所必需的报文不被遗漏丢弃，保证业务的正常运行，有效地提高设备的稳定性和整个网络的可用性。

本领域技术人员可以理解，上述实施例中的全部或部分模块（单元）或各步骤可以通过程序来指令相关硬件来实现，所述程序可存储于计算机可读取存储介质中，所述存储介质，如 ROM/RAM、磁盘、光碟等。或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块（单元）或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权 利 要 求

1、一种报文访问控制的方法，其特征在于，包括：

当接收到的报文不需要进行转发处理时，根据所述报文的信息查询访问控制表，如果命中访问控制表规则，则根据所述访问控制表规则对所述
5 报文进行相应操作；如果没有命中访问控制表规则，应用第一带宽参数所提供的带宽，将所述报文发送给控制平面；

所述报文的信息包括源IP地址、目的IP地址、源端口、目的端口、协议号中至少之一。

2、如权利要求1所述的方法，其特征在于，进一步包括：

10 设置第二带宽参数，应用所述第二带宽参数所提供的带宽大于应用所述第一带宽参数所提供的带宽；

当所述根据所述访问控制表规则进行相应操作为：将所述报文丢弃或者将所述报文应用第二带宽参数所提供的带宽发送至控制平面。

3、如权利要求1所述的方法，其特征在于，还包括：

15 根据报文信息判断所述报文是否需要转发，如果确定所述报文不需要转发，判断是否存在访问控制表，如果存在，根据所述报文的信息查询所述访问控制表。

4、如权利要求1、2或3所述的方法，其特征在于，还包括：

20 预先为所述报文配置优先级参数，并根据所述优先级参数对应的优先级，将所述报文发送至所述控制平面。

5、如权利要求1、2或3所述的方法，其特征在于，进一步包括：

若所述报文与转发引擎所在的网络设备所配置的业务相关，则根据与所述业务或者会话相关的报文信息，配置所述报文的访问控制规则，

将所述访问控制规则发送至所述转发引擎，并更新所述访问控制表。

25 6、如权利要求1、2或3所述的方法，其特征在于，进一步包括：

所述转发引擎所在的网络设备与其他网络设备动态建立会话连接后，根据与该会话相关的报文信息配置所述报文的访问控制规则；

将所述访问控制规则发送至所述转发引擎，并更新所述访问控制表。

7、一种报文访问控制的方法，其特征在于，包括：

当接收到的报文不需要进行转发处理时, 根据所述报文的信息查询访问控制表;

如果没有命中访问控制表规则, 应用第一带宽参数所提供的带宽, 将所述报文发送给控制平面;

- 5 如果命中访问控制表规则, 应用第二带宽参数所提供的带宽, 将所述报文发送给控制平面;

其中, 应用所述第二带宽参数所提供的带宽大于应用所述第一带宽参数所提供的带宽。

8、如权利要求7所述的方法, 其特征在于, 还包括:

- 10 预先为所述报文配置优先级参数, 并根据所述优先级参数对应的优先级, 将所述报文发送至所述控制平面。

9、一种报文转发引擎, 其特征在于, 包括设置模块、存储模块、接收模块、转发判断模块、访问控制模块和处理模块,

设置模块, 用于设置带宽参数;

- 15 存储模块, 用于存储并更新访问控制表;

接收模块, 用于接收报文;

转发判断模块, 用于根据所述接收模块所接收报文的信息, 判断所述报文是否需要转发;

- 20 访问控制模块, 用于查询所述控制表中的访问控制规则; 当所述转发判断模块判断所述报文不需要转发时, 所述访问控制模块根据所述报文的信息, 查询所述存储模块中存储的访问控制规则;

- 25 当所述访问控制模块命中所述访问控制规则时, 所述处理模块根据所命中的访问控制规则对所述接收模块接收的报文进行操作; 否则, 所述处理模块给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数, 发送至控制平面。

10、如权利要求9所述的报文转发引擎, 其特征在于, 所述访问控制模块包括查询模块和判断模块,

查询模块, 当所述转发判断模块判断所述报文不需要转发时, 用于查询所述存储模块中是否存储有所述访问控制表;

判断模块，当所述查询模块的查询到所述访问控制表时，根据所述接收模块接收的报文的信息，查询所述存储模块中存储的所述访问控制规则；

当所述查询模块查询后确定不存在所述访问控制表时，所述处理模块给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数发送给
5 控制平面。

11、如权利要求9或10所述的报文转发引擎，其特征在于，所述处理模块包括：

转发模块，在转发判断模块判断需要转发时，转发所述接收模块接收的报文。

10 12、如权利要求9或10所述的报文转发引擎，其特征在于，所述处理模块还包括丢弃模块和发送模块，

丢弃模块，根据所命中的访问控制规则，丢弃所述接收模块接收的所述报文；

15 发送模块，根据所命中的访问控制规则，将所述接收模块接收的所述报文发送至所述控制平面。

13、如权利要求12所述的报文转发引擎，其特征在于，所述设置模块用于设置第二带宽参数；

当根据所命中的访问控制表规则需将所述报文发送给所述控制平面时，所述发送模块采用所述第二带宽参数将所述报文发送给控制平面。

20 14、一种通信设备，其特征在于，包括控制单元和数据单元，
控制单元，用于配置访问控制表和处理报文；

数据单元，用于设置带宽参数，根据所接收报文的信息判断所述报文是否需要转发，如果不需要转发，则根据所述报文的信息查询所述控制单元配置的访问控制表，如果命中，则执行相应操作；否则，应用所设置的
25 带宽参数将所述报文发送给所述控制单元。

15、如权利要求14所述的通信设备，其特征在于，所述数据单元包括报文转发引擎，所述报文转发引擎包括设置模块、存储模块、接收模块、转发判断模块、访问控制模块和处理模块，

设置模块，用于设置带宽参数；

存储模块, 用于存储并更新所述控制单元下发的访问控制表;

接收模块, 用于接收报文;

转发判断模块, 用于根据所述接收模块所接收报文的信息, 判断是否需要转发;

5 访问控制模块, 用于查询所述访问控制表中的访问控制规则;

当所述转发判断模块判定所述报文不需要转发时, 所述访问控制模块根据所述接收模块接收的报文的信息, 查询所述存储模块中存储的所述访问控制表, 所述报文的信息包括源IP地址、目的IP地址、源端口、目的端口、协议号中至少之一;

10 处理模块, 当所述访问控制模块命中所述访问控制表中的规则时, 用于执行相应动作; 否则, 用于给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数, 发送给控制平面。

16、如权利要求15所述的通信设备, 其特征在于, 所述访问控制模块包括查询模块和判断模块,

15 查询模块, 当所述转发判断模块确定所述报文不需要转发时, 用于查询所述存储模块中是否存储有所述访问控制表;

判断模块, 当所述查询模块查询到存在所述访问控制表时, 根据所述接收模块接收的报文的信息, 查询所述存储模块中存储的所述访问控制规则;

20 当所述查询模块的查询后确定不存在所述访问控制表时, 所述处理模块给所述接收模块接收的报文应用所述设置模块设置的第一带宽参数, 并发送给控制平面。

17、如权利要求15或16所述的通信设备, 其特征在于, 所述报文转发引擎还包括:

25 转发模块, 在转发判断模块确定所述报文需要转发时, 用于转发所述接收模块接收的所述报文。

18、如权利要求15或者16所述的通信设备, 其特征在于, 所述处理模块还包括丢弃模块和发送模块,

丢弃模块, 根据所命中的访问控制规则, 丢弃所述接收模块接收的所

述报文;

发送模块, 根据所命中访问控制规则, 将所述接收模块接收的所述报文发送给所述控制平面。

19、如权利要求17所述的通信设备, 其特征在于, 所述设置模块设置

5 第二带宽参数;

当根据所命中的访问控制表规则需将所述报文发送给所述控制平面时, 所述发送模块采用所述第二带宽参数将所述报文发送给控制平面。

— 1/3 —

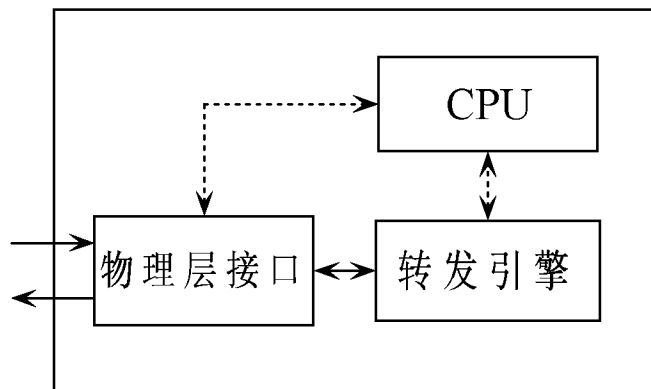


图 1

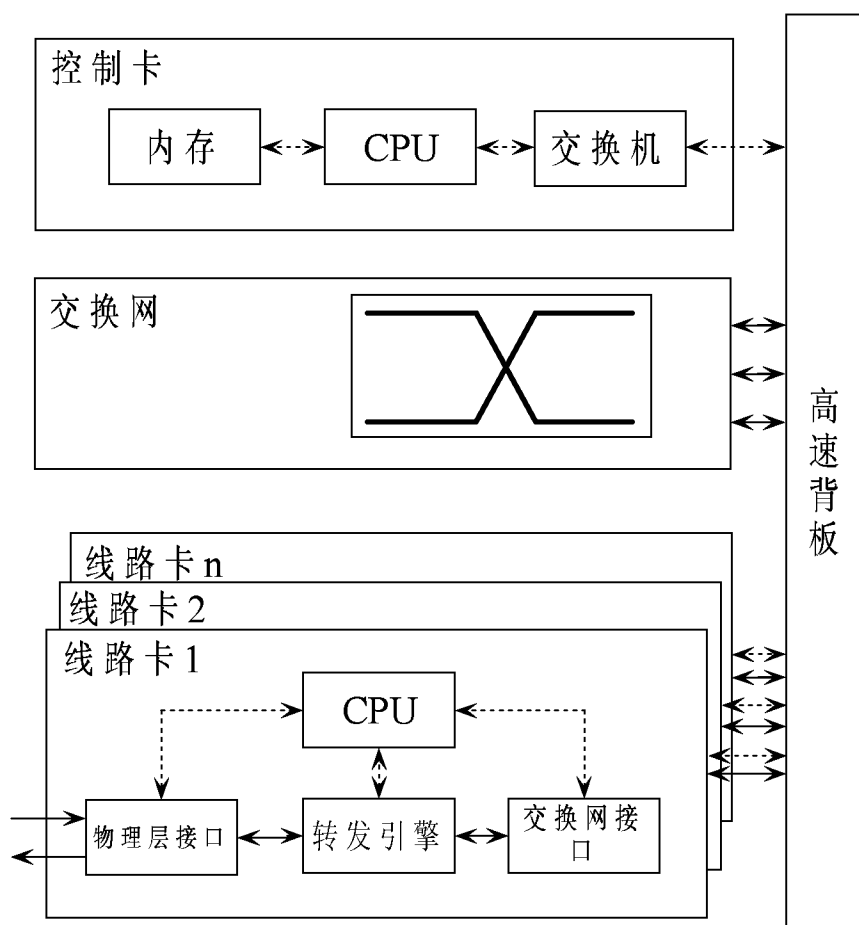


图 2

-2/3-

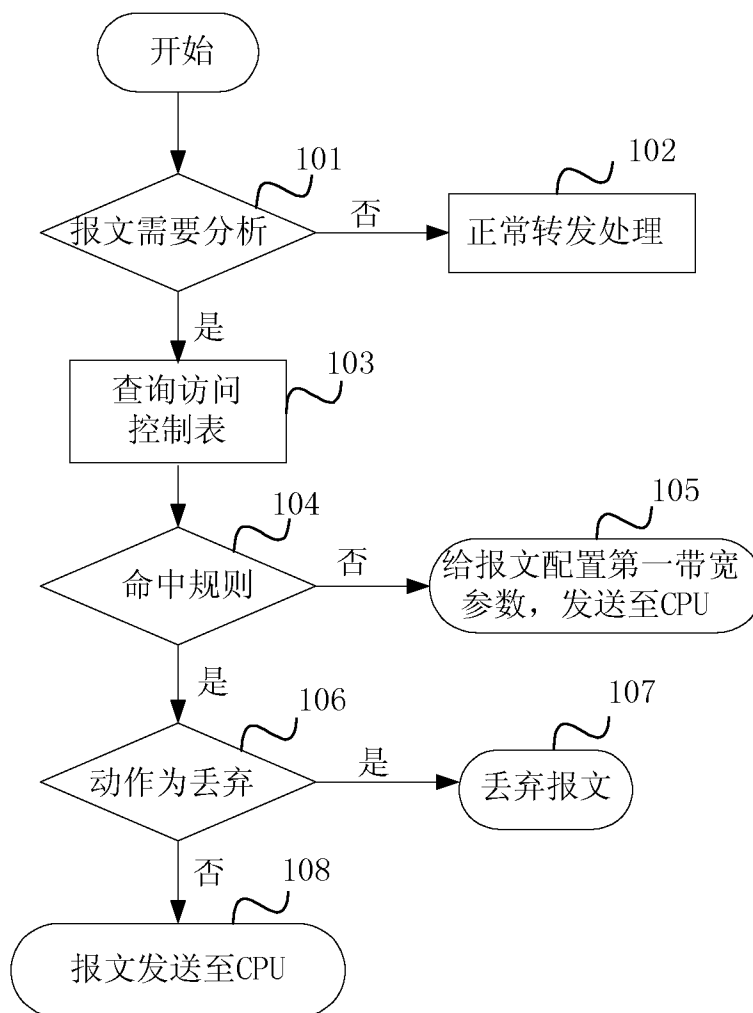


图 3

—3/3—

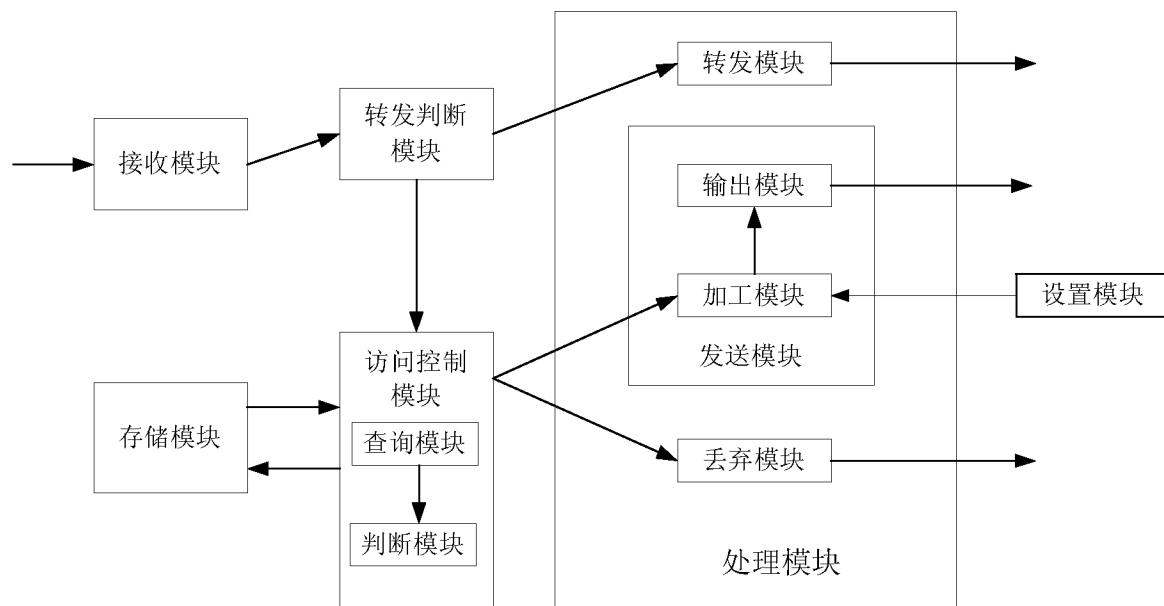


图 4

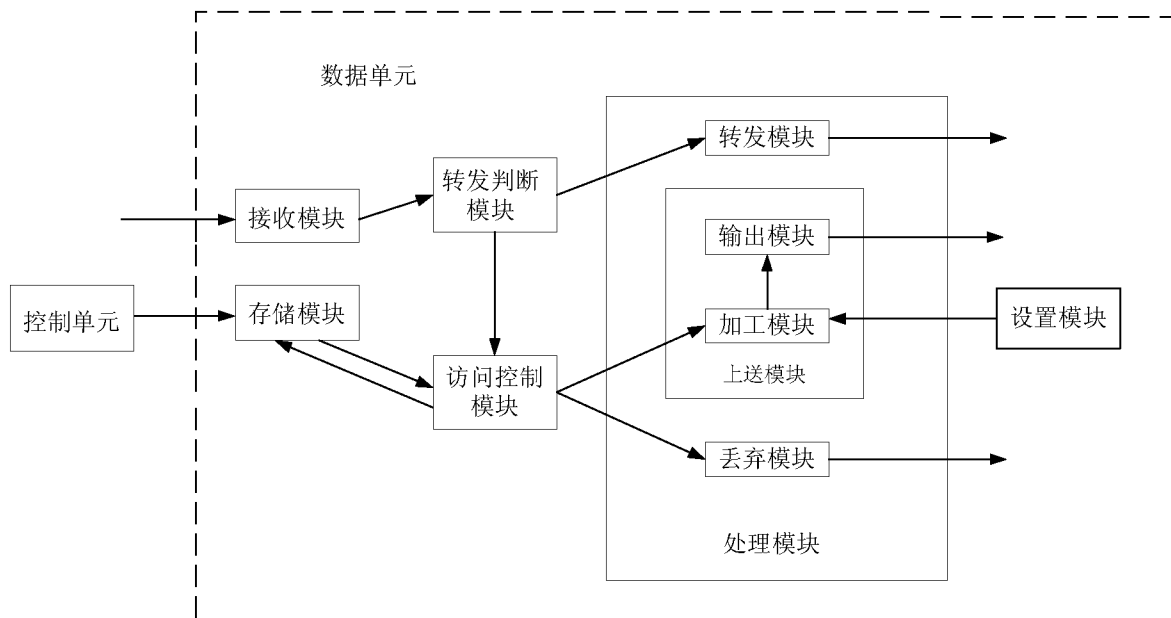


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/070551

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/56(2006.01) i

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: H04L12/00,12/28,12/40,12/54,12/56,H04L5/00,5/02,H04L29/00,29/02,29/06,H04N7/00,7/14,G06F15/-

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)

See the extra sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 1996939 A (HUAWEI TECHNOLOGIES CO., LTD.),11 July 2007 (11.07.2007), Claims 1-16, Page 3 Line 23-Page 11 Line 2 in the description, Fig. 1-5	1-19
A	CN 1738290 A (HUAWEI TECHNOLOGIES CO., LTD.), 22 February 2006 (22.02.2006), the whole document	1-19
A	CN 1859293 A (HUAWEI TECHNOLOGIES CO., LTD.), 08 November 2006 (08.11.2006), the whole document	1-19

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&"document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
30 October 2007(30.10.2007)

Date of mailing of the international search report
29 Nov. 2007 (29.11.2007))

Name and mailing address of the ISA/CN
The State Intellectual Property Office, the P.R.China
6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China
100088
Facsimile No. 86-10-62019451

Authorized officer
GUO,Fengshun
Telephone No. (86-10)82755435

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/070551

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 0235374 A1(CADANT, INC.), 02 May 2002(02.05.002), the whole document	1-19
A	US 5864554 A (LSI LOGIC CORPORATION), 26 January 1999(26.01.1999), the whole document	1-19
A	CN 1863161 A (HUAWEI TECHNOLOGIES CO., LTD.), 15 November 2006(15.11.2006), the whole document	1-19

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/070551

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1996939 A	11.07.2007	NONE	
CN 1738290 A	22.02.2006	NONE	
CN 1859293 A	08.11.2006	NONE	
WO 0235374 A1	02.05.2002	WO 0235374 A1	02.05.2002
		AU 9092101 A	06.05.2002
US 5864554 A	26.01.1999	WO 9511554 A1	27.04.1995
		AU 7981494 A	08.05.1995
		US 5446726 A	29.08.1995
		EP 0724794 A1	07.08.1996
		JP 9504149T T	22.04.1997
		US 5654962 A	05.08.1997
		US 5708659 A	13.01.1998
		US 5856975 A	05.01.1999
		US 5864554 A	26.01.1999
		US 5872784 A	16.02.1999
		US 5887187 A	23.03.1999
		US 5914955 A	22.06.1999
		US 5963543 A	05.10.1999
		US 6016401 A	18.01.2000
		US 6026088 A	15.02.2000
CN 1863161 A	15.11.2006	NONE	

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2007/070551

Continuation of :

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

WPI;EPODOC;PAJ;CNKI;IEE;CPRS.....AND KEYS:

ADDRESS, PORT, POTOCOL, ACL, CONTROL???, DETECT???, INQUIR???, CHECK???,

BAND W WIDTH, BANDWIDTH , MESSAGE, PARAMETER, CHANNEL, TRANSMIT???,TRANSMISSION,

REPEAT???,TRANSLAT???

国际检索报告

国际申请号
PCT/CN2007/070551

A. 主题的分类

H04L12/56(2006.01) i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC: H04L12/00,12/28,12/40,12/54,12/56,H04L5/00,5/02,H04L29/00,29/02,29/06,H04N7/00,7/14,G06F15/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

参见附加页

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 1996939 A(华为技术有限公司),11.7 月 2007(11.07.2007), 权利要求 1-16, 说明书第 3 页第 23 行-第 11 页第 2 行, 附图 1-5	1-19
A	CN 1738290 A(华为技术有限公司), 22.2 月 2006(22.02.2006), 全文	1-19
A	CN 1859293 A(华为技术有限公司), 08.11 月 2006(08.11.2006), 全文	1-19
A	WO 0235374 A1(CADANT, INC.), 02.5 月 2002(02.05.002), 全文	1-19
A	US 5864554 A(LSI LOGIC CORPORATION),26.1 月 1999(26.01.1999), 全文	1-19

☒ 其余文件在 C 栏的续页中列出。

☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇
引用文件的公布日而引用的或者因其他特殊理由而引
用的文件

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了
理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的
发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件
结合并且这种结合对于本领域技术人员为显而易见时,
要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期
30.10 月 2007(30.10.2007)

国际检索报告邮寄日期
29.11 月 2007 (29.11.2007)

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路 6 号 100088
传真号: (86-10)62019451

受权官员
郭风顺
电话号码: (86-10) 82755435

C(续). 相关文件

类 型	引用文件, 必要时, 指明相关段落	相关的权利要求
A	CN 1863161 A(华为技术有限公司), 15.11 月 2006(15.11.2006), 全文	1-19

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/070551

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 1996939 A	11.07.2007	无	
CN 1738290 A	22.02.2006	无	
CN 1859293 A	08.11.2006	无	
WO 0235374 A1	02.05.2002	WO 0235374 A1	02.05.2002
		AU 9092101 A	06.05.2002
US 5864554 A	26.01.1999	WO 9511554 A1	27.04.1995
		AU 7981494 A	08.05.1995
		US 5446726 A	29.08.1995
		EP 0724794 A1	07.08.1996
		JP 9504149T T	22.04.1997
		US 5654962 A	05.08.1997
		US 5708659 A	13.01.1998
		US 5856975 A	05.01.1999
		US 5864554 A	26.01.1999
		US 5872784 A	16.02.1999
		US 5887187 A	23.03.1999
		US 5914955 A	22.06.1999
		US 5963543 A	05.10.1999
		US 6016401 A	18.01.2000
		US 6026088 A	15.02.2000
CN 1863161 A	15.11.2006	无	

国际检索报告

国际申请号

PCT/CN2007/070551

续：在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPI;EPODOC;PAJ;CNKI;IEE;CPRS……和关键词: 报文, 信息, 消息, 源 I P 地址, 源地址, 目的 I P 地址, 目的地, 源端口, 目的端口, 协议, 转发, 路由, 带宽, 控制, C P U, 查询, 检索, 检测, ACL, 访问控制, 存取控制+接入控制, 参数, ADDRESS, PORT ,POTOCOL,ACL,CONTROL???, DETECT???, INQUIR???,CHECK???,BAND W WIDTH,BANDWIDTH ,MESSAGE,PARAMETER,CHANNEL, TRANSMIT???,TRANSMISSION, REPEAT???, TRANSLAT???