

(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 23 日 (23.10.2014)



WIPO | PCT



(10) 国际公布号
WO 2014/169765 A1

- (51) 国际专利分类号:
H04L 12/26 (2006.01)
- (21) 国际申请号: PCT/CN2014/074848
- (22) 国际申请日: 2014 年 4 月 4 日 (04.04.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201310138033.8 2013 年 4 月 19 日 (19.04.2013) CN
- (71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 孟伟 (MENG, Wei); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (74) 代理人: 北京派特恩知识产权代理有限公司 (普通合伙) (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (CN)。

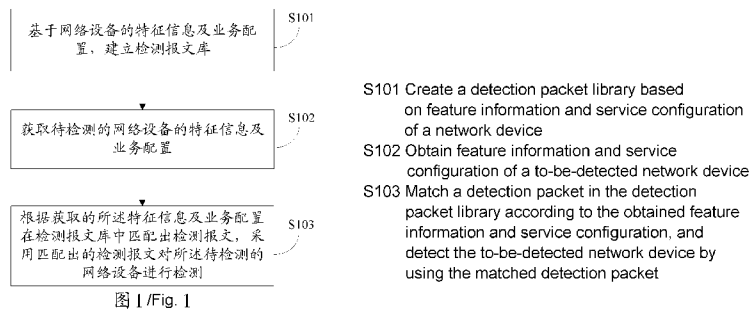
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, KM, 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))。

(54) Title: NETWORK DEVICE DETECTING METHOD AND APPARATUS, AND CLOUD DETECTION SYSTEM

(54) 发明名称: 一种网络设备检测方法、装置及云检测系统



(57) Abstract: Disclosed are a network device detecting method and apparatus, and a cloud detection system. The method comprises: creating a detection packet library based on feature information and service configuration of a network device; obtaining feature information and service configuration of a to-be-detected network device; and matching a detection packet in the detection packet library according to the obtained feature information and service configuration of the to-be-detected network device, and detecting the to-be-detected network device by using the matched detection packet.

(57) 摘要: 本发明公开了一种网络设备检测方法、装置及云检测系统, 该方法包括: 基于网络设备的特征信息及业务配置, 建立检测报文库; 获取待检测的网络设备的特征信息及业务配置; 根据获取的所述待检测的网络设备的特征信息及业务配置在检测报文库中匹配出检测报文, 采用匹配出的检测报文对所述待检测的网络设备进行检测。

WO 2014/169765 A1

一种网络设备检测方法、装置及云检测系统

技术领域

本发明涉及互联网设备技术领域，尤其涉及一种网络设备检测方法、装置及云检测系统。

5 背景技术

网络设备检测和故障发现技术是一种能够有效发现当前运行的网络设备潜在缺陷和隐藏后门的技术，目前已经成为网络安全研究的热点之一，针对发现的缺陷和后门的网络设备检测的安全技术进行分析和研究，具有重要的现实意义。

10 网络设备检测是进行远程或本地系统性能测试的一种技术。其基本原理是：采用模拟构造各类报文对目标路由器、交换机或防火墙进行发送的方式，对目标网络设备可能存在的缺陷进行逐项检测，以便对路由器、交换机、防火墙等对象进行系统可靠性评估。借助于基于报文的检测技术，人们可以发现网络和主机存在的对外开放的端口、提供的服务、某些系统
15 信息、错误的配置、已知的漏洞、未知的漏洞、后门等。因此网络设备检测技术是一种极为有效的自动测试技术，能够发现用户购买、测试、现网运行中的设备隐患，为用户采购、评估网络设备的可靠性，提供强有力的技术支持。

 目前在多数网络设备的扫描客户端或网络设备检测的客户端中，多数
20 只安装一种或固定的几种检测软件，这样的话，就没有任何一种检测软件可以扫描和测试所有网络设备的缺陷。同时，大多数测试用例，尤其是新技术新标准的检测用例需要用户手动添加，增加了维护和开发的难度和成本，并且不能完整的补充案例和报文库。

另外，现有的网络扫描技术目标不单一，目的不明确，并不能全面、有效地发现路由器、交换机或防火墙的漏洞。并且现有的网络扫描技术没有和网络中存在的业务，例如路由协议、多协议标签交换（MPLS，Multi-Protocol Label Switching）、因特网协议安全性（IPsec，Internet Protocol Security）等相关联，因此不能有针对性的发现业务的漏洞和缺陷。

发明内容

为解决现有存在的技术问题，本发明实施例提供一种网络设备检测方法、装置及云检测系统。

本发明实施例提供了一种网络设备检测方法，包括：

10 基于网络设备的特征信息及业务配置，建立检测报文库；

获取待检测的网络设备的特征信息及业务配置；

根据获取的所述待检测的网络设备的特征信息及业务配置，在检测报文库中匹配出检测报文，利用匹配出的检测报文对所述待检测的网络设备进行检测。

15 所述方法还包括：基于网络设备的特征信息及业务配置，建立与检测报文库对应的响应行为库；

相应地，对所述待检测的网络设备进行检测时，将所述待检测的网络设备的响应在响应行为库中进行比对，判断网络设备行为是否合法。

20 通过简单网络管理协议（SNMP，Simple Network Management Protocol）或者网络配置（NETCONF）协议或者用户端设备广域网管理协议 TR-069 获取所述待检测的网络设备的特征信息及业务配置。

所述网络设备的特征信息包括：网络设备的类型和型号；建立检测报文库时，网络设备的业务配置的类型至少包括以下之一：接口信息、互联网协议（IP，Internet Protocol）地址配置、虚拟局域网（VLAN，Virtual Local Area Network）配置、路由配置、MPLS 配置、以及协议配置。

所述检测报文库包括与网络设备的类型对应的通用及随机检测报文库；

所述方法还包括：采用通用及随机检测报文库中的报文对所述待检测的网络设备进行检测，根据所述待检测的网络设备的响应判断所述待检测
5 的网络设备是否存在漏洞和后门。

所述方法还包括：当网络设备的特征信息及业务配置发生变化时，对所述检测报文库进行维护更新。

本发明实施例还提供了一种网络设备检测装置，包括：检测处理模块及检测接口模块；其中，

10 所述检测处理模块，配置为基于网络设备的特征信息及业务配置，建立检测报文库；根据所述检测接口模块获取的所述待检测的网络设备的特征信息及业务配置在检测报文库中匹配出检测报文，并发送给所述检测接口模块，通过所述检测接口模块对所述待检测的网络设备进行检测；

所述检测接口模块，配置为获取所述待检测的网络设备的特征信息及
15 业务配置，并发送给所述检测处理模块。

所述检测处理模块，还配置为：基于网络设备的特征信息及业务配置建立与检测报文库对应的响应行为库；对所述待检测的网络设备进行检测时，将所述待检测的网络设备的响应在响应行为库中进行比对，判断网络设备行为是否合法；

20 相应地，所述检测接口模块，还配置为将所述待检测的网络设备的响应告知所述检测处理模块。

所述检测接口模块，配置为：通过 SNMP 或者 NETCONF 协议或者用户端设备广域网管理协议 TR-069 获取所述待检测的网络设备的特征信息及业务配置。

25 所述网络设备的特征信息包括：网络设备的类型和型号；建立检测报

文库时，网络设备的业务配置的类型至少包括以下之一：接口信息、IP 地址配置、VLAN 配置、路由配置、MPLS 配置、以及协议配置。

所述检测报文库包括与网络设备的类型对应的通用及随机检测报文库；

- 5 相应地，所述检测处理模块，还配置为采用通用及随机检测报文库中的报文对所述待检测的网络设备进行检测，根据所述待检测的网络设备的响应判断所述待检测的网络设备是否存在漏洞和后门；

所述检测接口模块，还配置为将所述待检测的网络设备的响应告知检测处理模块。

- 10 所述检测处理模块，还配置为当网络设备的特征信息及业务配置发生变化时，对所述检测报文库进行维护更新。

本发明实施例又提供了一种采用上述网络设备检测装置的云检测系统，包括云检测数据中心、检测客户端、以及网络设备，其中，

- 15 所述云检测数据中心，配置为基于各网络设备的特征信息及业务配置，建立检测报文库；根据所述检测客户端获取的所述特征信息及业务配置在检测报文库中匹配出检测报文，并发送给所述检测客户端，通过检测所述客户端对待检测的网络设备进行检测；

所述检测客户端，配置为获取待检测的网络设备的特征信息及业务配置，发送给所述云检测数据中心。

- 20 检测处理模块位于所述云检测数据中心中，检测接口模块位于所述检测客户端；

- 25 所述检测处理模块，配置为基于网络设备的特征信息及业务配置，建立检测报文库；根据所述检测接口模块获取的所述待检测的网络设备的特征信息及业务配置在检测报文库中匹配出检测报文，并发送给所述检测接口模块，通过所述检测接口模块对所述待检测的网络设备进行检测；

所述检测接口模块，配置为获取所述待检测的网络设备的特征信息及业务配置，并发送给所述检测处理模块。

本发明实施例又提供了一种计算机存储介质，所述计算机存储介质包括一组指令，当执行所述指令时，引起至少一个处理器执行所述如权利要求5 求上述的网络设备检测方法。

采用上述技术方案，本发明实施例至少具有下列优点：

本发明实施例所述网络设备检测方法、装置及云检测系统，能够有针对性的发现网络设备的业务漏洞和缺陷。

附图说明

10 在附图（其不一定是按比例绘制的）中，相似的附图标记可在不同的视图中描述相似的部件。具有不同字母后缀的相似附图标记可表示相似部件的不同示例。附图以示例而非限制的方式大体示出了本文中所讨论的各个实施例。

- 图 1 为本发明第一实施例的网络设备检测方法流程图；
- 15 图 2 为本发明实施例的检测报文库建立情况示意图；
- 图 3 为本发明第二实施例的网络设备检测方法流程图；
- 图 4 为本发明实施例的响应行为库建立情况示意图；
- 图 5 为本发明第三实施例的网络设备云检测方法流程图；
- 图 6 为本发明第四、五实施例的网络设备检测装置组成示意图；
- 20 图 7 为本发明第六实施例的网络设备云检测系统组成示意图；
- 图 8 为本发明应用实例的网络设备云检测系统的拓扑结构示意图；
- 图 9 为本发明应用实例中对路由器检测的流程图。

具体实施方式

为更进一步阐述本发明为达成预定目的所采取的技术手段及功效，以

下结合附图及较佳实施例，对本发明进行详细说明如后。

本发明第一实施例，一种网络设备检测方法，如图 1 所示，包括以下具体步骤：

步骤 S101，基于网络设备的特征信息及业务配置，建立检测报文库。

5 具体地，网络设备的特征信息可以包括：网络设备的类型和型号，网络设备的种类可以根据特征信息来划分，建立检测报文库时，每种网络设备的业务配置的类型至少包括以下之一：接口信息、IP 地址配置、VLAN 配置、路由配置、MPLS 配置、以及协议配置等。其中，所述协议配置包括：IPsec 配置、远程接入拨入用户服务（RADIUS，Remote Authentication Dial
10 In User Service）配置、以太网上点到点连接协议（PPPoE，Point to Point Protocol over Ethernet）配置等。

网络设备的类型包括：交换机、路由器和防火墙等。图 2 给出了检测报文库建立情况示意图，对于路由器类型的网络设备，为路由器下面每一种型号创建该型号路由器的业务配置所对应的检测报文库，例如，A 型号
15 路由器对应的检测报文库包括：开放式最短路径优先（OSPF，Open Shortest Path First）协议检测报文库、IPsec 应用检测报文库、基于 MPLS 网络的二层虚拟专用网服务（L2VPN，Layer2 Virtual Private Network）应用检测报文库、PPPoE 检测报文库等，每个与业务配置相关的检测报文库中又包含有若干检测报文。对于交换机类型的网络设备，为交换机下面每一种型号创
20 建该型号交换机的业务配置所对应的检测报文库，例如，A 型号交换机对应的检测报文库包括：VLAN 协议检测报文库、连接故障管理（CFM，Connectivity Fault Management）应用检测报文库、窥探（Snooping）检测报文库等。对于防火墙类型的网络设备，为防火墙下面每一种型号创建该型号防火墙的业务配置所对应的检测报文库，例如，A 型号防火墙对应的检
25 测报文库包括：网络地址转换（NAT，Network Address Translation）应用检

测报文库、访问控制列表（ACL，Access Control List）应用检测报文库、策略模块检测报文库等。

本实施例的检测报文库可以是比较全面的覆盖目前本领域所出现的网络设备种类及相应的业务配置情况，优选地，当网络设备的特征信息及业务配置发生变化时，可以对所述检测报文库进行维护更新，比如：当有新的网络设备及其业务配置出现时，或者目前建立的检测报文库中所涉及的某种网络设备的业务配置发生变化时，对所述检测报文库中的检测报文进行相应的增加和/或删除。

步骤 S102，获取待检测的网络设备的特征信息及业务配置。

具体地，主要是通过 SNMP 或者 NETCONF 协议或者用户端设备广域网管理协议 TR-069 获取待检测的网络设备的特征信息及业务配置，还可以通过人工获取、或者基于 WebGUI 管理方式（即网站公开源码的管理系统）获取。实现时，以 SNMP 方式为例，将网络设备的 SNMP 端口和服务打开，通过向网络设备发送 SNMP 报文来获取该网络设备的特征信息和业务配置。

步骤 S103，根据获取的所述特征信息及业务配置，在检测报文库中匹配出检测报文，利用匹配出的检测报文对所述待检测的网络设备进行检测。

此时可以根据网络设备的响应判断其行为是否合法。待检测网络设备的业务配置通常与检测报文库中该网络设备检测报文所涉及的业务配置有交集，即可匹配出检测报文，若没有交集，则需要对检测报文库进行更新，以补充新的业务配置检测报文。

本发明第二实施例，一种网络设备检测方法，如图 3 所示，包括以下具体步骤：

步骤 S201，基于网络设备的特征信息及业务配置，建立检测报文库及其对应的响应行为库。

具体地，本实施例中建立检测报文库的过程与第一实施例中相同。

更具体地，网络设备的特征信息可以包括：网络设备的类型和型号，网络设备的种类可以根据特征信息来划分，建立检测报文库时，每种网络设备的业务配置的类型至少包括以下之一：接口信息、IP 地址配置、VLAN 配置、路由配置、MPLS 配置、以及协议配置等。其中，所述协议配置包括：IPsec 配置、RADIUS 配置、PPPoE 配置等。

网络设备的类型包括：交换机、路由器和防火墙等。图 2 给出了检测报文库建立情况示意图，对于路由器类型的网络设备，为路由器下面每一种型号创建该型号路由器的业务配置所对应的检测报文库，例如，A 型号路由器对应的检测报文库包括：OSPF 协议检测报文库、IPsec 应用检测报文库、L2VPN 应用检测报文库、PPPoE 检测报文库等，每个与业务配置相关的检测报文库中又包含有若干检测报文。对于交换机类型的网络设备，为交换机下面每一种型号创建该型号交换机的业务配置所对应的检测报文库，例如，A 型号交换机对应的检测报文库包括：VLAN 协议检测报文库、CFM 应用检测报文库、Snooping 检测报文库等。对于防火墙类型的网络设备，为防火墙下面每一种型号创建该型号防火墙的业务配置所对应的检测报文库，例如，A 型号防火墙对应的检测报文库包括：NAT 应用检测报文库、ACL 应用检测报文库、策略模块检测报文库等。

本实施例的检测报文库可以是比较全面的覆盖目前本领域所出现的网络设备种类及相应的业务配置情况，优选地，当网络设备的特征信息及业务配置发生变化时，可以对所述检测报文库进行维护更新，比如：当有新的网络设备及业务配置出现时，或者目前建立的检测报文库中所涉及的某种网络设备的业务配置发生变化时，对所述检测报文库中的检测报文进行相应的增加和/或删除。

图 4 给出了响应行为库建立情况示意图，响应行为库中的响应行为记

录是与具体的报文对应的，以交换机类型的网络设备为例，A 型号的交换机下有 n 个报文的响应行为记录，报文 1~3 可能属于 VLAN 协议检测报文库，因此报文 1~3 响应行为记录分别与 VLAN 协议检测报文库中的报文 1~3 对应，而报文 4~6 可能属于 CFM 应用检测报文库，所以报文 4~6 响应行为记录分别与 CFM 应用检测报文库中的报文 4~6 对应。再以路由器类型的网络设备为例，A 型号的路由器下有 m 个报文的响应行为记录，报文 1~4 可能属于 OSPF 协议检测报文库，所以报文 1~4 响应行为记录分别与 OSPF 协议检测报文库中的报文 1~4 对应，A 型号路由器与 A 型号交换机下面的报文的响应行为记录的个数也可以不同。

10 步骤 S202，获取待检测的网络设备的特征信息及业务配置。

具体地，主要是通过 SNMP 或者 NETCONF 协议或者用户端设备广域网管理协议 TR-069 获取待检测的网络设备的特征信息及业务配置，还可以通过人工获取、或者基于 WebGUI 管理方式（即网站公开源码的管理系统）获取。

15 步骤 S203，根据获取的所述特征信息及业务配置，在检测报文库中匹配出检测报文，利用匹配出的检测报文对所述待检测的网络设备进行检测。

具体地，对所述待检测的网络设备进行检测时，将所述待检测的网络设备的响应在响应行为库中进行比对，以判断网络设备行为是否合法。

本实施例中根据响应行为库的不同组成，介绍三种比对流程：

20 第一种：响应行为库中包括：人工设置的第一响应行为记录和检测开始后保存的第二响应行为记录；

将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，则判定行为合法，否则判定行为不合法；这里，响应行为记录中的多数是指响应行为记录中
25 相同响应数量最多的那种响应记录。

当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，将待检测的网络设备的响应与第一响应行为记录进行比对，若与第一响应行为记录一致，则判定行为合法，否则判定行为不合法；

5 第二种：响应行为库中包括：检测开始后保存的第二响应行为记录；

将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，则判定行为合法，否则判定行为不合法；

10 当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，直接将比对结果判定为行为合法；

第三种：响应行为库中包括：人工设置的第一响应行为记录；

将待检测的网络设备的响应与所述匹配的检测报文对应的第一响应行为记录进行比对，若与第一响应行为记录一致，则判定行为合法，否则判定行为不合法。

15 优选地，在步骤 S201 中，检测报文库还包括：与网络设备的类型对应的通用及随机检测报文库。如图 2 所示，通用及随机检测报文库按照网络设备的类型划分。承接步骤 S201，本实施例的所述方法还包括：

步骤 S204，采用通用及随机检测报文库中的报文，对所述网络设备进行检测，根据所述网络设备的响应判断其是否存在漏洞和后门。

20 具体地，按照待检测的网络设备的不同类型，采用相应的通用及随机检测报文库中的报文，对所述网络设备进行检测，对于通用检测报文库，可以具备相应的响应行为库，后续将该网络设备的响应，在该通用检测报文库的响应行为库中进行比对，以判断网络设备行为是否合法。

25 对于采用随机检测报文库中的报文进行检测的情况，根据所述网络设备的响应判断其是否存在漏洞和后门。比如：有些网络设备可能在收到某

条随机检测报文后，会出现向指定端口发送本机信息的行为，这就是一种网络设备的后门。

本发明第三实施例，本实施例是在第二实施例的基础上引入云检测数据
5 中心和检测客户端，使它们按照本实施例的步骤执行检测流程，可以作为本发明的最佳实施例，即一种网络设备检测方法，如图 5 所示，包括以下具体步骤：

步骤 S301，在云检测数据中心中基于网络设备的特征信息及业务配置，建立检测报文库及其对应的响应行为库。

10 本步骤将检测报文库和响应行为库建立在云检测数据中心中，便于对检测报文进行编辑和维护。

步骤 S302，检测客户端获取待检测的网络设备的特征信息及业务配置。

具体地，检测客户端主要是通过 SNMP 或者 NETCONF 协议或者用户
设备广域网管理协议 TR-069 获取待检测的网络设备的特征信息及业务配
15 置，还可以通过人工获取、或者基于 WebGUI 管理方式（即网站公开源码
的管理系统）获取。实现时，以 SNMP 方式为例，网络设备与检测客户端
的物理连接的接口需要打开 SNMP 端口和服务，通过向网络设备发送 SNMP
报文来获取该网络设备的特征信息和业务配置。

步骤 S303，云检测数据中心根据获取的所述特征信息及业务配置，在
20 检测报文库中匹配出检测报文，并发送给检测客户端，通过检测客户端对
所述待检测的网络设备进行检测。

具体地，对所述待检测的网络设备进行检测时，检测客户端将匹配出
的检测报文发送给待检测的网络设备，并将该待检测的网络设备的响应告
知云检测数据中心，云检测数据中心将该待检测的网络设备的响应，在响
25 应行为库中进行比对，以判断网络设备行为是否合法，若行为合法，则输
出日志至检测客户端，若行为不合法，则在输出日志至检测客户端的同时，

追加告警。

本实施例中根据在云检测数据中心中建立的响应行为库的不同组成，介绍三种比对流程：

第一种：响应行为库中包括：人工设置的第一响应行为记录和检测开始5 始后保存的第二响应行为记录；

云检测数据中心将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，则判定行为合法，否则判定行为不合法；这里，响应行为记录中的多数是指响应行为记录中相同响应数量最多的那种响应记录。

10 当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，云检测数据中心将待检测的网络设备的响应与第一响应行为记录进行比对，若与第一响应行为记录一致，则判定行为合法，否则判定行为不合法；

第二种：响应行为库中包括：检测开始后保存的第二响应行为记录；

15 云检测数据中心将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，则判定行为合法，否则判定行为不合法；

当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，云检测数据中心直接将比对结果判定为行为合法；

20 第三种：响应行为库中包括：人工设置的第一响应行为记录；

云检测数据中心将待检测的网络设备的响应与所述匹配的检测报文对应的第一响应行为记录进行比对，若与第一响应行为记录一致，则判定行为合法，否则判定行为不合法。

25 优选地，在步骤 S301 中，检测报文库还包括：与网络设备的类型对应的通用及随机检测报文库。如图 2 所示，通用及随机检测报文库按照网络

设备的类型划分。承接步骤 S301，本实施例的所述方法还包括：

步骤 S304，云检测数据中心采用通用及随机检测报文库中的报文对所述网络设备进行检测，根据所述网络设备的响应判断其是否存在漏洞和后门。

5 具体地，云检测数据中心按照待检测的网络设备的不同类型，采用相应的通用及随机检测报文库中的报文对该待检测的网络设备进行检测。该通用及随机检测报文库中的报文还是由检测客户端发送给待检测的网络设备，对于通用检测报文库，可以为其建立相应的响应行为库，后续云检测数据中心将该待检测的网络设备的响应，在该通用检测报文库的响应行为
10 库中进行比对，以判断网络设备行为是否合法，若行为合法，则输出日志至检测客户端，若行为不合法，则在输出日志至检测客户端的同时，追加告警。

对于采用随机检测报文库中的报文进行检测的情况，后续根据所述待检测的网络设备的响应判断其是否存在漏洞和后门。

15

本发明第四实施例，一种网络设备检测装置，如图 6 所示，包括以下组成部分：

检测处理模块 100，优选地，位于云检测数据中心，配置为基于网络设备的特征信息及业务配置，建立检测报文库；根据检测接口模块 200 获取
20 的所述特征信息及业务配置在检测报文库中匹配出检测报文，并发送给检测接口模块 200，通过检测接口模块 200 对待检测的网络设备进行检测；

检测接口模块 200，优选地，位于检测客户端中，配置为获取待检测的网络设备的特征信息及业务配置，并发送给检测处理模块 100。

具体地，检测接口模块 100 主要是通过 SNMP 或者 NETCONF 协议或者
25 用户端设备广域网管理协议 TR-069 获取待检测的网络设备的特征信息及业务配置，还可以通过人工获取、或者基于 WebGUI 管理方式（即网站公

开源码的管理系统)获取。网络设备的特征信息可以包括:网络设备的类型和型号,网络设备的种类可以根据特征信息来划分,建立检测报文库时,每种网络设备的业务配置的类型至少包括以下之一:接口信息、IP地址配置、VLAN配置、路由配置、MPLS配置、以及协议配置等。其中,所述协议配置包括:IPsec配置、RADIUS配置、PPPoE配置等。

实际应用时,本实施例的检测处理模块100可以由网络设备检测装置中的中央处理器(CPU, Central Processing Unit)、数字信号处理器(DSP, Digital Signal Processor)或可编程逻辑阵列(FPGA, Field-Programmable Gate Array)实现;本实施例的检测接口模块200可以由网络设备检测装置中的接口实现。

本发明第五实施例,一种网络设备检测装置,如图6所示,包括以下组成部分:

检测处理模块100,优选地,位于云检测数据中心中,配置为基于网络设备的特征信息及业务配置,建立检测报文库及其对应的响应行为库;根据检测接口模块200获取的所述特征信息及业务配置在检测报文库中匹配出检测报文,并发送给检测接口模块200,通过检测接口模块200对待检测的网络设备进行检测;

检测接口模块200,优选地,位于检测客户端中,配置为获取待检测的网络设备的特征信息及业务配置,发送给检测处理模块100。

对待检测的网络设备进行检测时,检测接口模块200还配置为:将检测报文发送给待检测的网络设备,并将待检测的网络设备的响应告知检测处理模块100;

相应地,检测处理模块100还配置为:将所述待检测的网络设备的响应在响应行为库中进行比对以判断网络设备行为是否合法;

本实施例中根据响应行为库的不同组成,介绍三种可选的比对方式:

第一种：响应行为库中包括：人工设置的第一响应行为记录和检测开始后保存的第二响应行为记录；

检测处理模块 100 将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，
5 则判定行为合法，否则判定行为不合法；这里，响应行为记录中的多数是指响应行为记录中相同响应数量最多的那种响应记录。

当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，检测处理模块 100 将待检测的网络设备的响应与第一响应行为记录进行比对，若与第一响应行为记录一致，则判定行为合法，
10 否则判定行为不合法；

第二种：响应行为库中包括：检测开始后保存的第二响应行为记录；

检测处理模块 100 将待检测的网络设备的响应与所述匹配的检测报文对应的第二响应行为记录进行比对，若与第二响应行为记录中的多数一致，
则判定行为合法，否则判定行为不合法；

15 当所述匹配的检测报文对应的第二响应行为记录中不能区分出多数一致的响应行为记录时，检测处理模块 100 直接将比对结果判定为行为合法；

第三种：响应行为库中包括：人工设置的第一响应行为记录；

检测处理模块 100 将待检测的网络设备的响应与所述匹配的检测报文对应的第一响应行为记录进行比对，若与第一响应行为记录一致，则判定
20 行为合法，否则判定行为不合法。

检测报文库的创建情况如图 2 所示，优选地，检测报文库还包括与网络设备的类型对应的通用及随机检测报文库；

相应地，检测处理模块 100 还配置为：采用通用及随机检测报文库中的报文对所述网络设备进行检测，根据所述网络设备的响应判断其是否存在
25 在漏洞和后门。

具体地，检测处理模块 100 按照待检测的网络设备的不同类型，采用相应的通用及随机检测报文库中的报文对所述待检测的网络设备进行检测。该通用及随机检测报文库中的报文还是由检测接口模块 200 发送给所述待检测的网络设备，对于通用检测报文库，可以具备相应的响应行为库，
5 后续检测处理模块 100 将该待检测的网络设备的响应，在该通用检测报文库的响应行为库中进行比对，以判断网络设备行为是否合法若行为合法，则输出日志至检测客户端，若行为不合法，则在输出日志至检测客户端的同时，追加告警。

对于采用随机检测报文库中的报文进行检测的情况，后续根据所述待
10 检测的网络设备的响应判断其是否存在漏洞和后门。

实际应用时，本实施例的检测处理模块 100 可以由网络设备检测装置中的 CPU、DSP 或 FPGA 实现；本实施例的检测接口模块 200 可以由网络设备检测装置中的接口实现。

本发明第六实施例，一种网络设备云检测系统，如图 7 所示，包括云
15 检测数据中心 10、检测客户端 20、以及网络设备 30；其中，

云检测数据中心 10，配置为基于各网络设备 30 的特征信息及业务配置，建立检测报文库；根据检测客户端 20 获取的所述特征信息及业务配置在检测报文库中匹配出检测报文，并发送给检测客户端 20，通过检测客户端 20 对待检测的网络设备 30 进行检测；

20 检测客户端 20，配置为获取待检测的网络设备 30 的特征信息及业务配置，发送给云检测数据中心 10。

这里，检测处理模块 100，位于云检测数据中心 10 中，配置为基于各网络设备 30 的特征信息及业务配置，建立检测报文库；根据检测接口模块 200 获取的所述特征信息及业务配置在检测报文库中匹配出检测报文，并
25 发送给检测接口模块 200，通过检测接口模块 200 对待检测的网络设备 30 进

行检测;

检测接口模块 200, 位于检测客户端 20 中, 配置为获取待检测的网络设备 30 的特征信息及业务配置, 发送给检测处理模块 100。

5 下面基于第一至第六实施例, 介绍一个本发明的应用实例。

图 8 为本发明应用实例的网络设备云检测系统的拓扑结构示意图。以网络设备为路由器的情况为例, 图 9 为本发明应用实例中的路由器、检测客户端与云检测数据中心报文交互过程示意图。

如图 9 所示, 本发明应用实例中对路由器的检测过程, 包括以下步骤:

10 101, 建立云检测数据中心, 并配置相关的网络设备库、检测报文库、报文的响应行为库;

102, 配置检测客户端 A, 被检测路由器 R1, IP 地址为 192.168.1.1。

103, 检测客户端 A 向路由器 R1 发送 SNMP 请求报文, 路由器 R1 返回相关的配置信息至检测客户端 A。

15 104, 检测客户端 A 获取了路由器 R1 的型号为 X 型号系列路由器、配置了 NAT、OSPF、LSP 协议等业务配置。

105, 检测客户端 A 将获取的路由器 R1 的特征信息及业务配置告知云检测数据中心。

20 106, 云检测数据中心对路由器 R1 特征信息及业务配置分析并进行检测报文库的匹配。

107, 云检测数据中心通知检测客户端 A 准备完毕。

108, 检测客户端 A 通知云检测数据中心, 获取第 1 条检测报文。

109, 云检测数据中心根据路由器 R1 相关 MAC、IP 等配置信息, 封装完整的一条检测报文, 并发送给检测客户端 A。

25 110, 检测客户端 A 收到检测报文后, 将该检测报文发送至被检测路由器 R1, 路由器 R1 做出响应, 并回复响应报文至检测客户端 A。

111, 检测客户端 A 收到响应报文后, 发送响应报文至云检测数据中心。

112, 云检测数据中心将响应报文与响应行为库中的记录进行比对, 若行为合法, 则输出日志至检测客户端 A; 若行为不合法, 则在输出日志至检测客户端 A 的同时追加告警;

5 113, 检测客户端 A 对日志和告警进行处理; 并请求第 2 条检测报文, 重复如上步骤。

114, 当第 2 条检测报文从检测客户端 A 发送至路由器 R1 时, 路由器 R1 没有响应。

115, 检测客户端 A 等待设定的时间 T 之后, 通知云检测数据中心路由
10 器 R1 “无响应”。

116, 云检测数据中心根据路由器 R1 “无响应” 的行为, 和响应行为库中的记录进行比对, 若行为合法, 则输出日志至检测客户端 A; 若行为不合法, 则在输出日志至检测客户端 A 的同时追加告警。

15 本发明实施例的网络设备检测方法、装置及云检测系统, 能够有针对性的发现网络设备的业务漏洞和缺陷。

本发明实施例的网络设备检测方法、装置及云检测系统, 在采用通用及随机检测报文进行检测的情况下, 通过判断检测结果可以发现网络设备的漏洞和后门, 进而实现全面有效的对网络设备进行检测。

20 本发明实施例所述网络设备云检测系统, 将检测报文库创建于云检测数据中心的, 便于编辑与维护, 且与现有技术中将测试用例、报文库、漏洞库、插件库等扫描素材定制化、安装在检测客户端装置中相比, 本发明实施例的检测客户端可以与云检测数据中心中进行实时连接进行检测, 检测结果实时性与交互性较好。

25 本领域内的技术人员应明白, 本发明的实施例可提供为方法、系统、或计算机程序产品。因此, 本发明可采用硬件实施例、软件实施例、或结

合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器和光学存储器等）上实施的计算机程序产品的形式。

5 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现
10 在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个
15 流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功
20 能的步骤。

通过具体实施方式的说明，应当可对本发明为达成预定目的所采取的技术手段及功效得以更加深入且具体的了解，然而所附图示仅是提供参考与说明之用，并非用来对本发明加以限制。

权利要求书

1、一种网络设备检测方法，包括：

基于网络设备的特征信息及业务配置，建立检测报文库；

获取待检测的网络设备的特征信息及业务配置；

5 根据获取的所述待检测的网络设备的特征信息及业务配置，在检测报文库中匹配出检测报文，利用匹配出的检测报文对所述待检测的网络设备进行检测。

2、根据权利要求1所述的网络设备检测方法，其中，所述方法还包括：
基于网络设备的特征信息及业务配置，建立与检测报文库对应的响应行为
10 库；

相应地，对所述待检测的网络设备进行检测时，将所述待检测的网络设备的响应在响应行为库中进行比对，判断网络设备行为是否合法。

3、根据权利要求1所述的网络设备检测方法，其中，通过简单网络管理协议 SNMP 或者网络配置 NETCONF 协议或者用户端设备广域网管理协
15 议 TR-069 获取所述待检测的网络设备的特征信息及业务配置。

4、根据权利要求1所述的网络设备检测方法，其中，所述网络设备的特征信息包括：网络设备的类型和型号；

建立检测报文库时，网络设备的业务配置的类型至少包括以下之一：
接口信息、互联网协议 IP 地址配置、虚拟局域网 VLAN 配置、路由配置、
20 多协议标签交换 MPLS、以及协议配置。

5、根据权利要求4所述的网络设备检测方法，其中，所述检测报文库包括与网络设备的类型对应的通用及随机检测报文库；

所述方法还包括：采用通用及随机检测报文库中的报文对所述待检测的网络设备进行检测，根据所述待检测的网络设备的响应判断所述待检测
25 的网络设备是否存在漏洞和后门。

6、根据权利要求 1-5 中任一项所述的网络设备检测方法，其中，所述方法还包括：当网络设备的特征信息及业务配置发生变化时，对所述检测报文库进行维护更新。

7、一种网络设备检测装置，包括：检测处理模块及检测接口模块；其中，

所述检测处理模块，配置为基于网络设备的特征信息及业务配置，建立检测报文库；根据所述检测接口模块获取的所述待检测的网络设备的特征信息及业务配置在检测报文库中匹配出检测报文，并发送给所述检测接口模块，通过所述检测接口模块对所述待检测的网络设备进行检测；

10 所述检测接口模块，配置为获取所述待检测的网络设备的特征信息及业务配置，并发送给所述检测处理模块。

8、根据权利要求 7 所述的网络设备检测装置，其中，所述检测处理模块，还配置为：基于网络设备的特征信息及业务配置，建立与检测报文库对应的响应行为库；对所述待检测的网络设备进行检测时，将所述待检测的网络设备的响应在响应行为库中进行比对，判断网络设备行为是否合法；

15 相应地，所述检测接口模块，还配置为将所述待检测的网络设备的响应告知所述检测处理模块。

9、根据权利要求 7 所述的网络设备检测装置，其中，所述检测接口模块，配置为：通过 SNMP 或者 NETCONF 协议或者用户端设备广域网管理协议 TR-069 获取所述待检测的网络设备的特征信息及业务配置。

10、根据权利要求 7 所述的网络设备检测装置，其中，所述网络设备的特征信息包括：网络设备的类型和型号；

建立检测报文库时，网络设备的业务配置的类型至少包括以下之一：接口信息、IP 地址配置、VLAN 配置、路由配置、MPLS 配置、以及协议配置。

11、根据权利要求 10 所述的网络设备检测装置，其中，所述检测报文库包括与网络设备的类型对应的通用及随机检测报文库；

相应地，所述检测处理模块，还配置为采用通用及随机检测报文库中的报文对所述待检测的网络设备进行检测，根据所述待检测的网络设备的
5 响应判断所述待检测的网络设备是否存在漏洞和后门；

所述检测接口模块，还配置为将所述待检测的网络设备的响应告知检测处理模块。

12、根据权利要求 7-11 中任一项所述的网络设备检测装置，其中，所述检测处理模块，还配置为当网络设备的特征信息及业务配置发生变化时，
10 对所述检测报文库进行维护更新。

13、一种网络设备云检测系统，包括云检测数据中心、检测客户端、以及网络设备；其中，

所述云检测数据中心，配置为基于各网络设备的特征信息及业务配置，建立检测报文库；根据所述检测客户端获取的所述特征信息及业务配置在
15 检测报文库中匹配出检测报文，并发送给所述检测客户端，通过检测所述客户端对待检测的网络设备进行检测；

所述检测客户端，配置为获取待检测的网络设备的特征信息及业务配置，发送给所述云检测数据中心。

14、根据权利要求 13 所述的网络设备云检测系统，其中，检测处理模块位于所述云检测数据中心中，检测接口模块位于所述检测客户端；
20

所述检测处理模块，配置为基于网络设备的特征信息及业务配置，建立检测报文库；根据所述检测接口模块获取的所述待检测的网络设备的特征信息及业务配置在检测报文库中匹配出检测报文，并发送给所述检测接口模块，通过所述检测接口模块对所述待检测的网络设备进行检测；

25 所述检测接口模块，配置为获取所述待检测的网络设备的特征信息及

业务配置，并发送给所述检测处理模块。

15、一种计算机存储介质，所述计算机存储介质包括一组指令，当执行所述指令时，引起至少一个处理器执行所述如权利要求 1 至 6 任一项所述的网络设备检测方法。

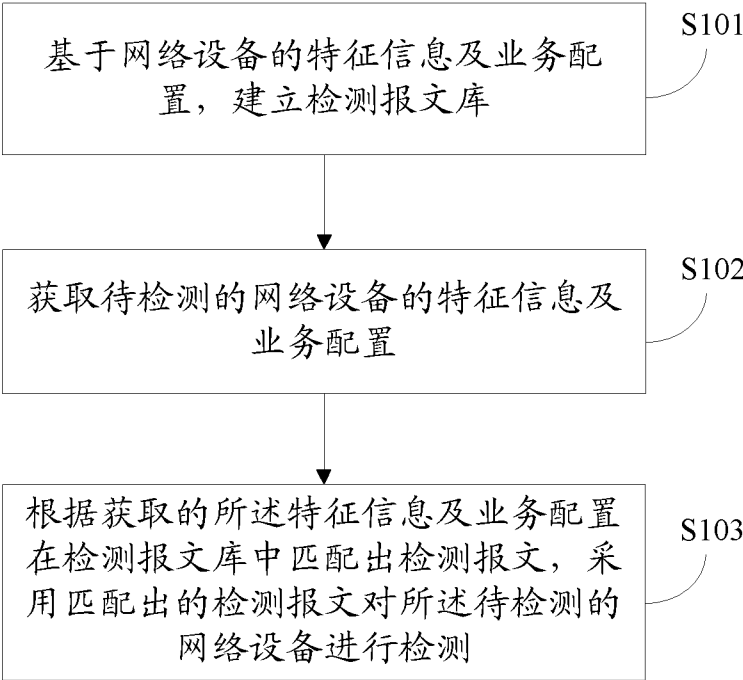


图 1

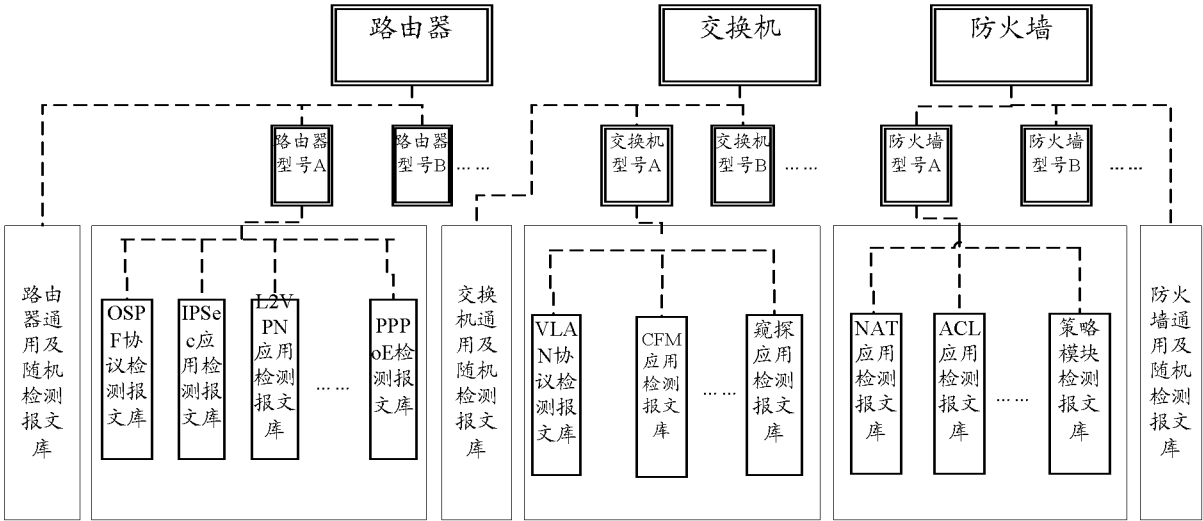


图 2

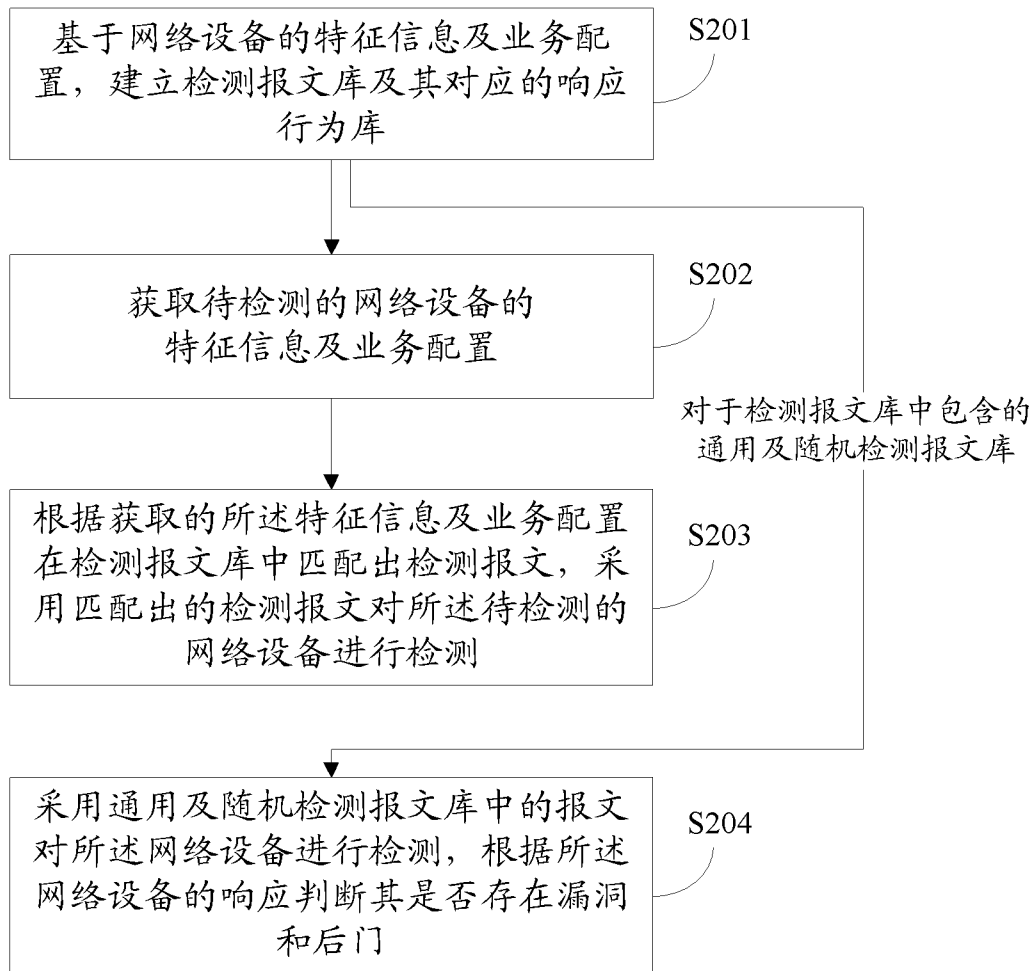


图 3

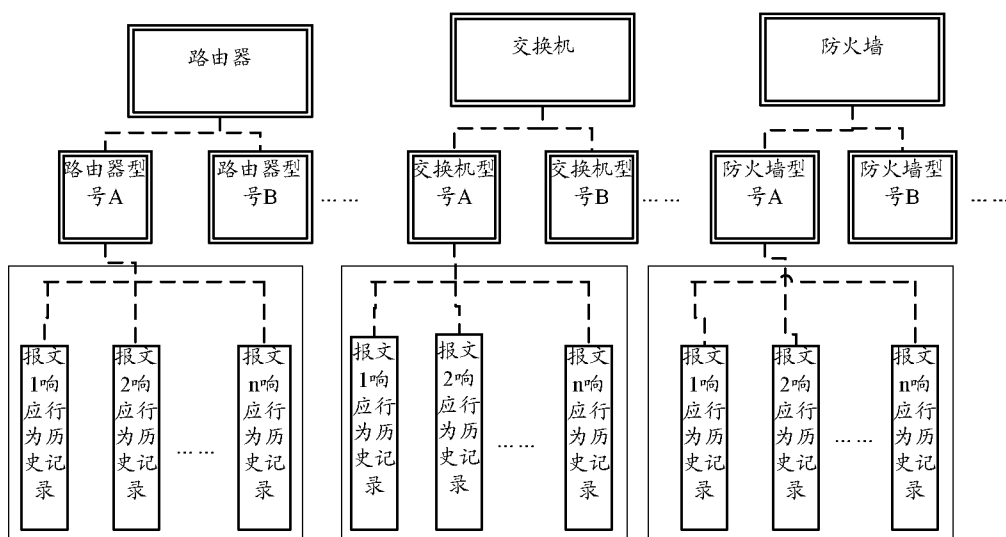


图 4

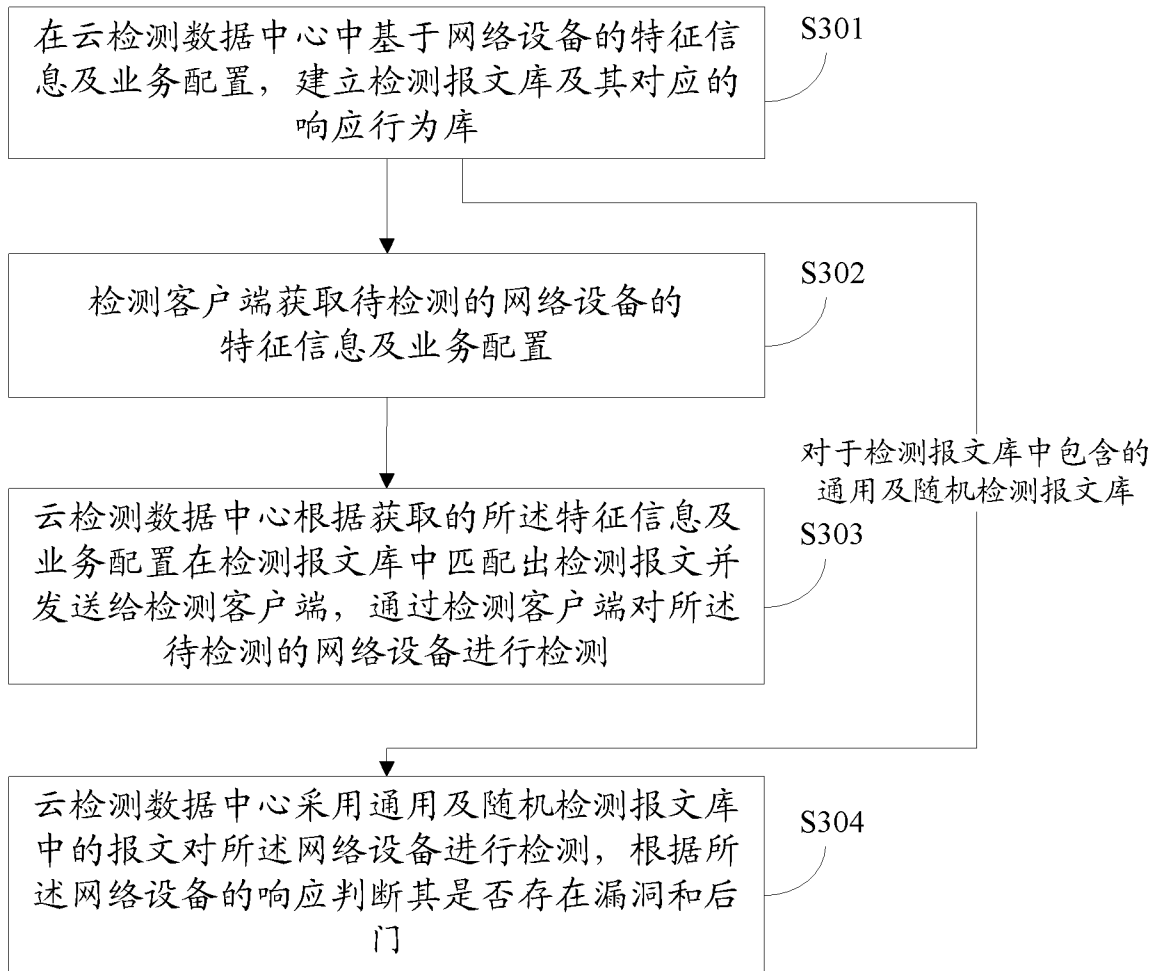


图 5

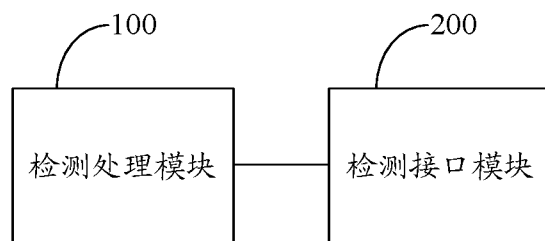


图 6

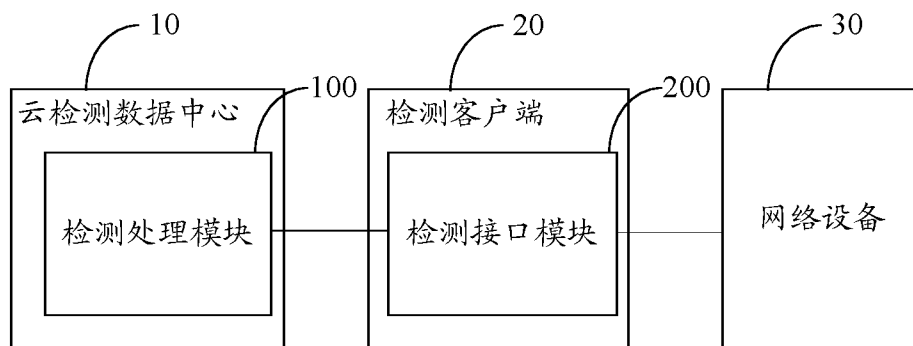


图 7

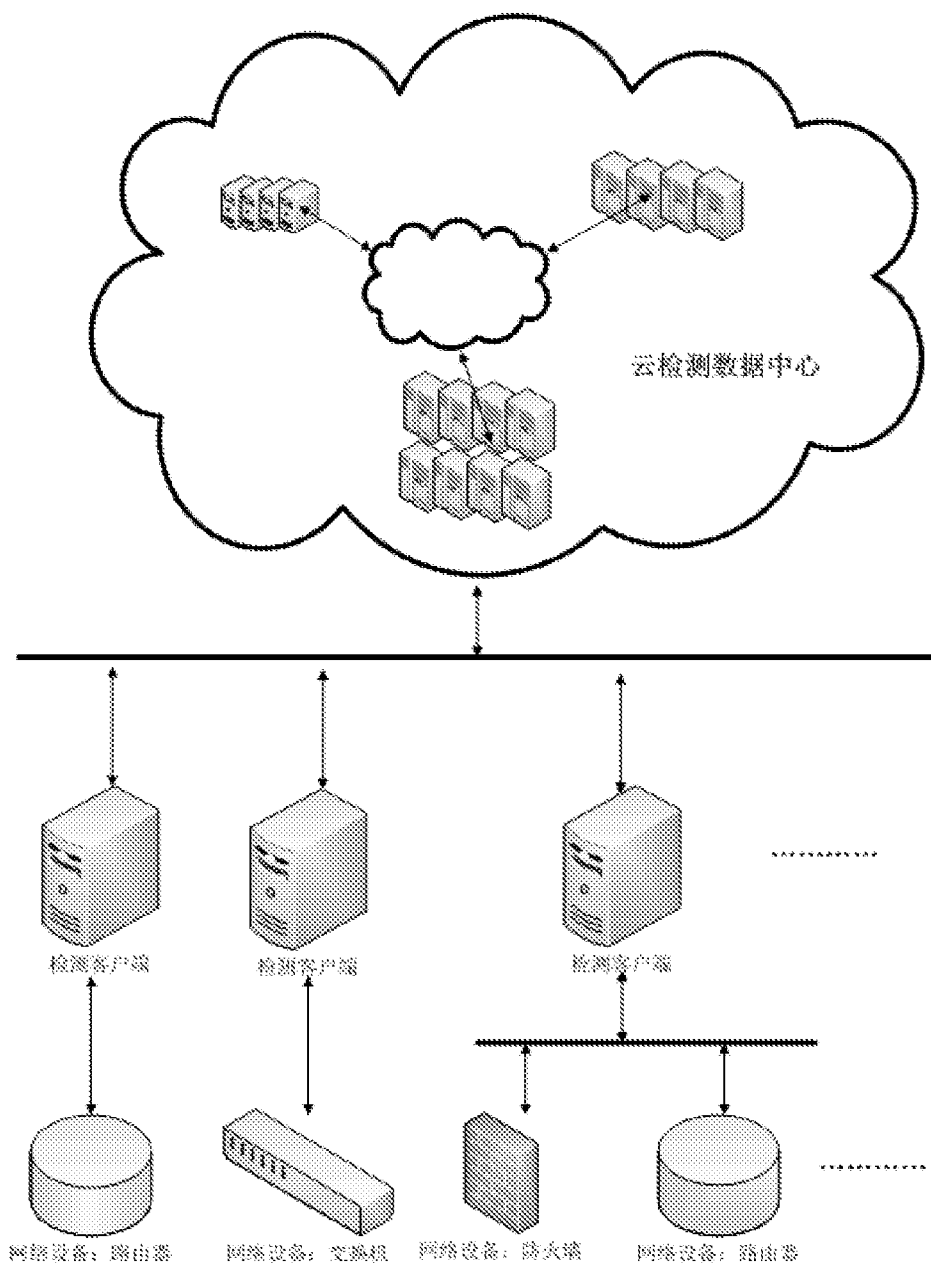


图 8

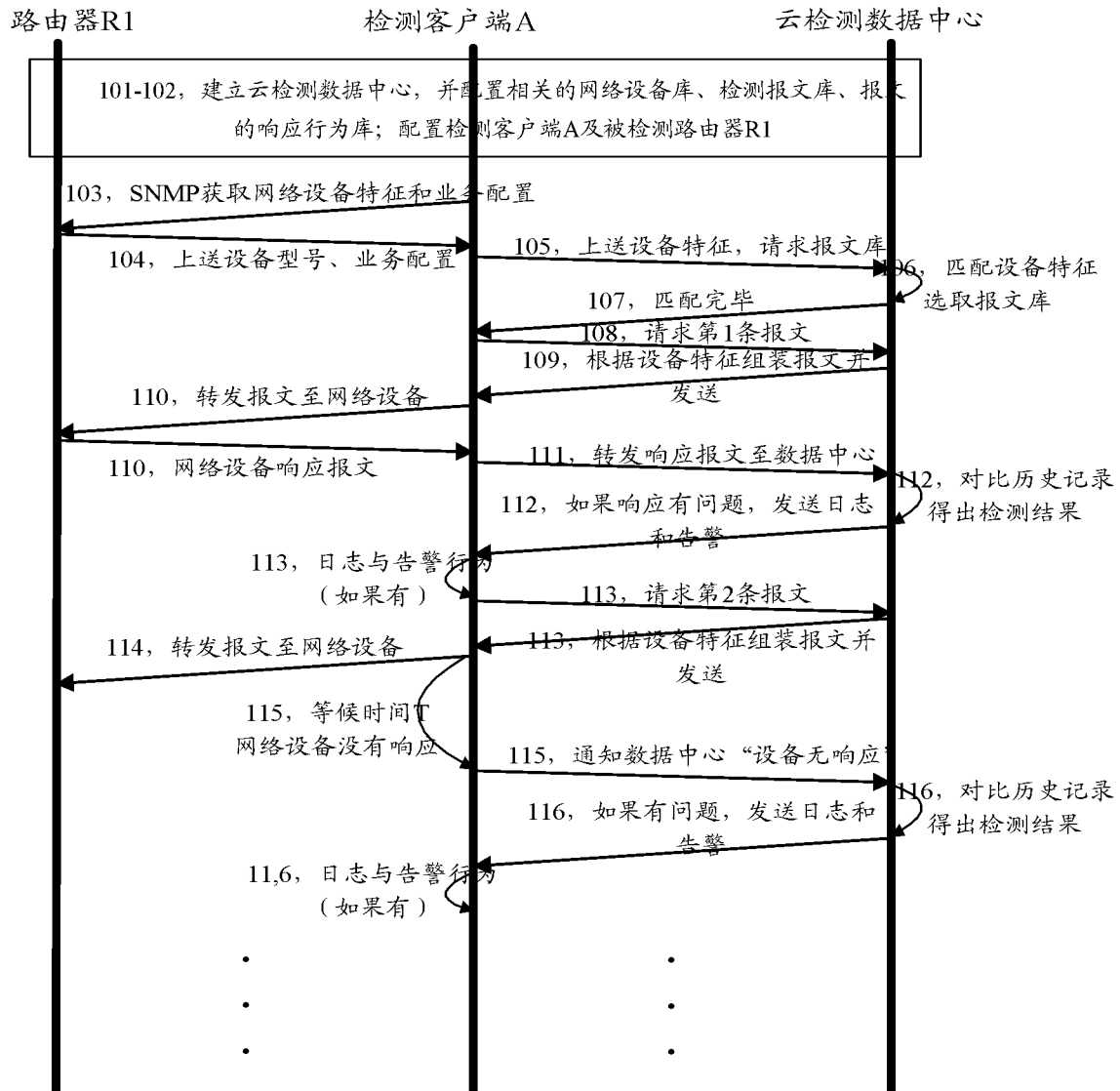


图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/074848

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/26 (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)

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)

WPI, EPODOC, CNKI, IEEE, CNPAT: detecting message, testing message, search+, match, data base, packet, datagram, network device, cloud detection, service, feature, type, parameter, generate, structure, set up, establish, general random detection packet, detecting, packet, query+, modal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 102843269 A (ZTE CORPARATON) 26 December 2012 (26.12.2012) description, paragraphs [0039] to [0050] and figures 1 and 5	1-15
Y	CN 101996451 A (INDUSTRIAL AND COMMERCIAL BANK OF CHINA CO., LTD.) 30 March 2011 (30.03.2011) description, paragraphs [0061] to [0092] and figure 1	1-15
A	US 7821937 B1 (SYMANTEC CORPORATION) 26 October 2010 (26.10.2010) the whole document	1-15
A	CN 102523221 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTR) 27 June 2012 (27.06.2012) the whole document	1-15

☐ 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 20 June 2014	Date of mailing of the international search report 08 July 2014
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer ZHANG, Kaijia Telephone No. (86-10) 61648250

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2014/074848

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 102843269 A	26 December 2012	None	
CN 101996451 A	30 March 2011	CN 101996451 B	25 July 2012
US 7821937 B1	26 October 2010	None	
CN 102523221 A	27 June 2012	None	

国际检索报告

国际申请号

PCT/CN2014/074848

A. 主题的分类

H04L 12/26(2006.01) i

按照国际专利分类(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)

H04L

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))

WPI; EPODOC; CNKI; IEEE; CNPAT: 检测报文, 测试报文, 查询, 匹配, 检索, 数据库, 库, 报文, 数据报, 网络设备, 云检测, 业务, 服务, 特征, 型号, 参数, 生成, 构建, 建立, 创建, 类型, 型号, 通用随机检测报文, detecting, packet, service, search+, query+, feature, type, modal

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
Y	CN 102843269A (中兴通讯股份有限公司) 2012年 12月 26日 (2012 - 12 - 26) 说明书第[0039]-[0050]段、附图1, 5	1-15
Y	CN 101996451A (中国工商银行股份有限公司) 2011年 3月 30日 (2011 - 03 - 30) 说明书第[0061]-[0092]段、附图1	1-15
A	US 7821937B1 (SYMANTEC CORPORATION) 2010年 10月 26日 (2010 - 10 - 26) 全文	1-15
A	CN 102523221A (国家计算机网络与信息安全管理中心 等) 2012年 6月 27日 (2012 - 06 - 27) 全文	1-15

☐ 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	“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
“E” 在国际申请日的当天或之后公布的在先申请或专利	“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
“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 (如具体说明的)	“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
“O” 涉及口头公开、使用、展览或其他方式公开的文件	“&” 同族专利的文件
“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	

国际检索实际完成的日期

2014年 6月 20日

国际检索报告邮寄日期

2014年 7月 08日

ISA/CN的名称和邮寄地址

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

传真号 (86-10) 62019451

授权官员

张嘉凯

电话号码 (86-10) 61648250

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/074848

检索报告引用的专利文件		公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	102843269A	2012年 12月 26日	无	
CN	101996451A	2011年 3月 30日	CN 101996451B	2012年 7月 25日
US	7821937B1	2010年 10月 26日	无	
CN	102523221A	2012年 6月 27日	无	