(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
2020 年 10 月 15 日 (15.10.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/207051 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2019/127244

(22) 国际申请日: 2019 年 12 月 21 日 (21.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910290613.6 2019年4月11日 (11.04.2019) CN

(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: 邢 超 (**XING, Chao**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 徐 科 科 (**XU, Keke**); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 陈颖(**CHEN, Ying**); 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, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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,

(54) **Title:** METHOD AND APPARATUS FOR NETWORK VERIFICATION

(54) **发明名称**: 网络验证的方法和装置

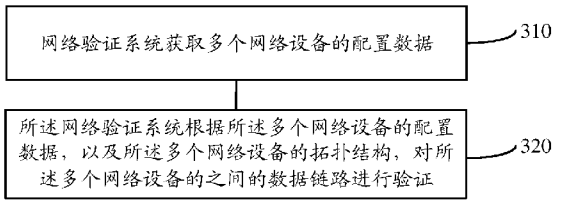


图 3

310 A network verification system obtaining configuration data of a plurality of network devices

320 The network verification system verifying a data link between the plurality of network devices according to the configuration data of the plurality of network devices and the topological structure between the plurality of network devices

(57) **Abstract:** Provided in the present application are a method and apparatus for network verification, the method comprising: a network verification system obtaining configuration data of a plurality of network devices, a data model of the configuration data being described by a general data modeling language unrelated to the network devices; and the network verification system verifying a data link between the plurality of network devices according to the configuration data of the plurality of network devices and the topological structure between the plurality of network devices. In the described method, the network verification system may verify the data link between the plurality of network devices on the basis of the configuration data described by a general data modeling language unrelated to the network devices, and the topological structure of the plurality of network devices. The present application is beneficial for improving the scalability of a network verification system. Moreover, the provision of a template of configuration data for each network device in traditional network simulation software, which leads to poor scalability of network simulation software, is avoided.

(57) **摘要**: 本申请提供了一种网络验证的方法和装置，该方法包括：网络验证系统获取多个网络设备的配置数据，其中，配置数据的数据模型为与网络设备无关的通用数据建模语言描述的；所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证。上述方法中，网络验证系统可以基于与网络设备无关的通用数据建模语言描述的配置数据，以及多个网络设备的拓扑结构，对多个网络设备之间的数据链路进行验证。有利于提高网络验证系统的可扩展性。避免了传统的网络仿真软件中，提供针对每种网络设备的配置数据的模板，导致网络仿真软件的扩展性较差。

WO 2020/207051 A1

[见续页]

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, ST, 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))。

网络验证的方法和装置

技术领域

本申请涉及信息技术领域，并且更具体地，涉及网络验证的方法和装置。

背景技术

网络仿真技术是一种通过建立网络模型，并模拟网络流量的传输，从而获取网络设计或优化所需要的网络性能数据的仿真技术。主要应用在开发和评价新的网络协议和网络设备以及网络规划设计等方面。网络仿真能迅速建立起网络模型，方便地修改模型，适用于预测网络性能、容量规划、故障分析、端到端性能分析、指导新网络建设等。

由于不同厂商生产的网络设备之间配置数据的数据模型存在差异，不同型号的网络设备之间的配置数据的数据模型也可能存在差异，因此，网络仿真软件中通常会提供各种配置数据的数据模型，运维人员可以向配置数据的数据模型中填写待仿真的真实网络的配置数据，以建立网络模型。

然而，上述网络仿真软件的扩展性较差，即网络仿真软件更新配置数据的数据模型的时间比较滞后，通常在新的网络设备投入使用较长的一段时间后。这样，在网络仿真软件添加新的网络设备的配置数据的数据模型天之前，运维人员无法通过网络仿真软件仿真包含新的网络设备的真实网络。

发明内容

本申请提供一种网络验证的方法和装置，以提高网络验证系统的可扩展性。

第一方面，提供了一种网络验证的方法，包括：网络验证系统获取多个网络设备的配置数据，其中，配置数据的数据模型为与网络设备无关的通用数据建模语言描述的；所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证。

上述方法中，网络验证系统可以基于与网络设备无关的通用数据建模语言描述的配置数据，以及多个网络设备的拓扑结构，对多个网络设备之间的数据链路进行验证。有利于提高网络验证系统的可扩展性。避免了传统的网络仿真软件中，提供针对每种网络设备的配置数据的模板，导致网络仿真软件的扩展性较差。

在一种可能的实现方式中，所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证，包括：所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，计算路由得到，所述多个网络设备的路由转发表项；所述网络验证系统根据所述多个网络设备的路由转发表项，对所述多个网络设备之间的数据链路进行验证。

本申请中，基于多个网络设备的配置数据直接生成路由转发表项，并基于路由转发表项对网络的数据链路进行验证，有利于简化得到路由转发表项的过程。避免了传输的数据

链路过程中，网络设备需要基于配置数据（例如，IP 地址）进行路由学习，得到路由转发表项。

在一种可能的实现方式中，所述数据模型包括所述配置数据的通用的数据属性以及所述配置数据的可扩展的数据属性。其中，可扩展的数据属性可以关联数据模型中未添加的数据属性，例如厂商私有属性等。通用的数据属性中包括对常用数据属性，例如，通用的数据属性可以包括以下数据属性中的一个或多个：配置名称、设备类型、设备接口、设备互联网协议地址 IP 地址或虚拟专用网络路由转发表 vrf。

上述方法中，一方面通过在数据模型中增加可扩展的数据属性，有利于提高数据模型的可扩展性。另一方面，通过在一个数据模型中包含配置数据的多个常用数据属性，避免了基于传统的 YANG 模型描述配置数据时，配置数据的不同的数据属性承载于不同的 YANG 模型中，有利于提高数据模型的描述能力。

可选地，所述多个网络设备的配置数据中包括第一网络设备的配置数据，所述方法还包括：所述网络验证系统根据所述第一网络设备的配置数据，对所述第一网络设备进行配置验证，其中，配置验证是指对所述第一网络设备的配置数据的数据模型中的任意一个或多个数据属性进行验证。

上述第一网络设备可以是多个网络设备中的任意一个网络设备。

上述方法中，网络验证系统可以基于第一网络设备的配置数据的数据模型进行配置验证，以简化配置验证的过程。避免了传统的配置验证过程中，由于配置数据中不同的数据属性承载于不同的 YANG 模型，导致要对多个配置数据的数据属性进行验证时，需要基于多个数据属性的 YANG 模型分别进行验证。

可选地，配置数据的数据模型对网络的配置进行验证的所需的配置数据。如此，使得通过一个配置数据的数据模型可以验证进行配置验证所需的，有利于简化获取配置数据的流程。避免了使用传统的 YANG 模型中不同类型的配置数据承载于不同的 YANG 模型中。

可选地，上述通用的数据属性中包括对网络进行数据链路的验证所需的常用数据属性，或者通用的数据属性中包括对网络进行配置验证所需的常用数据属性。

上述方法通过在一个数据模板中集成对数据链路进行验证所需的数据属性，或者配置验证所需的数据属性，以简化网络验证的过程。避免了传统的验证过程中，由于配置数据中不同的数据属性承载于不同的 YANG 模型，导致进行网络验证时通常需要基于多个 YANG 模型进行验证。

在一种可能的实现方式中，所述配置数据的数据模型为树形结构。

本申请通过使用树形结构表示配置数据的数据模型，即使用与 YANG 模型相似结构的数据模型，使得配置数据的数据模型与 Netconf 协议之间的匹配程度，与 YANG 模型与 Netconf 协议之间的匹配程度相似，有利于基于 Netconf 协议推广上述配置数据的数据模型。

另一方面，由于本申请的配置数据的数据模型的结构与 YANG 模型类型，因此可以借用 YANG 模型可以转化 Netconf 报文的性能，将本申请的配置数据的数据模型与 Netconf 报文结合，应用与目前的网络中。上述将配置数据的数据模型转化为 Netconf 报文的过程可以称为“配置数据的数据模型的 YANG 化”。

在一种可能的实现方式中，所述配置数据包括以下任一种：待配置的配置数据；已配置的配置数据；待更新的配置数据。

本申请基于配置数据的类型不同，相应的验证过程可以分为“事前验证过程”以及“事后

验证过程”，使得本申请实施例的方法可以兼容多种场景的验证过程。

在一种可能的实现方式中，所述多个网络设备包括第二网络设备，所述通用数据建模语言为 YANG 模型，所述网络验证系统获取网络中多个网络设备的配置数据，包括：所述网络验证系统接收网络配置协议 NetConf 报文，所述 NetConf 报文中包括所述第二网络设备的配置数据，所述第二网络设备的配置数据用于对所述第二网络设备进行配置，或者对所述第二网络设备的配置进行更新。

上述用于对所述第二网络设备进行配置的配置数据可以理解为上文中待配置的配置数据，上述用于对所述第二网络设备的配置进行更新的配置数据可以理解为上文中待更新的配置数据。

本申请通过 NetConf 报文与配置数据的数据模型结合，有利于借助 Netconf 协议的推广程度，推广本申请的配置数据的数据模型。

第二方面，提供了一种网络验证装置，所述网络验证装置包括用于执行上述方法中各个方面的模块。

第三方面，提供了一种网络验证系统，包括输入/输出接口、处理器和存储器。该处理器用于控制输入/输出接口收发信息，该存储器用于存储计算机程序，该处理器用于从存储器中调用并运行该计算机程序，使得该网络验证系统执行上述第一方面中的各个方法。

第四方面，提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上述第一方面中的各个方法。

需要说明的是，上述计算机程序代码可以全部或者部分存储在第一存储介质上，其中第一存储介质可以与处理器封装在一起的，也可以与处理器单独封装，本申请对此不作具体限定。

第五方面，提供了一种计算机可读介质，所述计算机可读介质存储有程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行上述各方面中的方法。

附图说明

图 1 是本申请实施例适用的 SDN 网络架构的示意图。

图 2 是本申请实施例的网络验证系统 140 的示意性框图。

图 3 是本申请实施例的网络验证方法的示意性流程图。

图 4 是本申请实施例的配置数据的数据模型的组织形式的示意图。

图 5 是本申请实施例的配置数据的数据模型的逻辑结构的示意图。

图 6 是本申请实施例的网络验证方法的示意性流程图。

图 7 是本申请实施例的网络验证方法的示意性流程图。

图 8 是本申请实施例的网络验证装置的示意图。

图 9 是本申请实施例的另一网络验证系统的示意图。

具体实施方式

下面将结合附图，对本申请的技术方案进行描述。

传统的网络验证过程，都是基于网络仿真软件实现的。网络仿真软件中会配置多个配

置数据的数据模型，以对应使用不同配置数据的数据模型的网络设备。然而，这种基于多种配置数据的数据模型以描述不同厂商的网络设备，以实现对真实网络进行仿真的方案，扩展性较差。当网络仿真软件中未添加某一网络设备对应的配置数据的数据模型时，运维人员则无法通过网络仿真软件准确地对包含上述网络设备的网络进行仿真。

为了避免上述问题，本申请提供一种网络验证方法，在该方法中网络验证系统基于通用模型描述不同网络设备的配置数据，解耦配置数据的数据模型与网络设备之间的捆绑关系，以提高网络验证系统的扩展性。

为了便于理解，先结合图 1，以本申请应用于软件定义网络（software defined network，SDN）架构为例，介绍本申请适用的网络架构。需要说明的是，本申请实施例的方法还可以应用其他网络架构。

图 1 是本申请实施例适用的 SDN 网络架构的示意图。图 1 所示的网络架构包括应用层 110，控制层 120，转发层 130 以及网络验证系统 140。

应用层（application layer）110，用于实现对网络业务的呈现。

转发层 130，又称基础设施层（infrastructure layer），用于实现路由、交换功能。具体地，转发层 130 可以包含多个网络设备，网络设备可以是交换机、路由器等。

控制层（control layer）120，用于集中管理转发层 130 中的网络设备，具体地，控制层可以包括 SDN 控制器，由 SDN 控制器为集中管理转发层中的网络设备。例如，由 SDN 控制器为各个网络设备配置相应的配置数据等。

上述控制层可以基于网络配置协议（network configuration protocol，Netconf）为转发层中的网络设备配置、修改、删除配置数据。例如，SDN 控制器中可以设置有网络配置协议客户端（Netconf-Client），网络设备中可以设置有 Netconf 服务端（Netconf-Server），这样，SDN 控制器通过 Netconf-Client 与网络设备中的 Netconf-Server 进行通信，以基于 Netconf 配置、修改、删除网络设备的配置数据。

网络验证系统 140，用于对转发层中的网络设备的配置或者数据链路进行验证。

下文结合图 2，介绍本申请实施例的网络验证系统的架构。需要说明的是，图 2 所示的网络验证系统仅仅为了便于理解方案，并不会对本申请的方案造成限定。网络验证系统还可以是其他形式的，例如，可以根据实际应用，删除网络验证系统中的某些功能，或者合并网络验证系统中的某些功能。

图 2 是本申请实施例的网络验证系统 140 的示意性框图。图 2 所示的网络验证系统 140 包括北向服务应用程序接口（application programming interface，API）层 141，业务层 142，核心算法能力层 143，配置数据的数据模型 144、数据链路模型 145 以及南向采集模块 146。

北向服务 API 层 141，用于对外提供服务化 RESTful（Representational State Transfer）接口供北向用户界面（user interface，UI）或者第三方应用调用。

业务层 142，用于提供配置验证，数据链路验证以及用户扩展业务等功能。

上述配置验证用于对网络设备的配置数据进行验证，具体可以包括配置内容校验，多配置一致性校验、安全策略冗余或冲突验证、IP 冲突检测、规划配置一致性检测等。

其中，配置内容校验，用于验证网络设备的配置数据内容是否符合设备规格/规范要求。

多配置一致性校验，用于验证网络中网络设备配置的多个配置数据是否一致。

安全策略冗余或冲突验证，用于验证网络中各个网络设备相关的安全策略是否存在冲突或者冗余的情况。

IP 冲突检测，用于通过从不同的网络设备上获取配置数据，检测不同的网络设备上的配置数据是否具有相同的 IP 地址，如果具有相同的 IP 地址，那么就认为网络中存在 IP 冲突。

规划配置一致性检测，在数据通信网络（Data Communication Network，DCN）场景中，当零接触供应（Zero Touch Provisioning，ZTP）开局时会根据用户的需求生成一份规划配置，这个规划配置在下发到设备上之后，待配置生效之后需要验证下发的配置和网络设备上生效的配置是否一致，是否符合用户的规划意图。具体包括，比较规划配置数据和生成配置数据是否一样，以及基于生成的配置数据对全网的数据链路进行可达性验证，并将网络中数据链路的通断情况显示给用户。

针对这种验证规划配置一致性检测，还有一个场景，就是网络 CDN 节点选址是否最优的验证，用户规划的 CDN 节点是否是全网最优，在经过验证引擎验证之后更能给出一个结论或者相对于当前用户的规划更加合理高效的节点选址。

上述数据链路验证用于对网络中的数据链路进行验证，具体可以包括数据链路的可达性验证，数据链路的环路检查，数据链路的一致性检测以及数据链路的黑洞检查等。

其中，数据链路的可达性验证用于验证网络中某一数据链路的源网络设备到目标网络设备是否可达。数据链路的一致性检测，用于检测通过某一数据链路传输的数据包中的数据在传输之前与传输之后是否一致。数据链路的黑洞检查，用于检查网络中是否存在黑洞路由器。上述用户扩展功能用于支持用户根据需求扩充验证插件。通常包括需求模型以及结果模型，其中，需求模型用于用户自定义输入待验证的问题，结果模型用于返回验证结果。

核心算法能力层 143，用于提供基础算法能力。通常包括配置校验算法、词语语法解析、路由/拓扑计算引擎，以及可满足性模理论（satisfiability modulo theories，SMT）求解器。

其中，配置校验算法用于对网络中网络设备的配置数据进行校验。即可以理解为，是上述业务层中的配置验证的基础算法。词语语法解析，用于将获取的配置数据的数据模型进行词语语法解析转换成为通用模型。路由/拓扑计算引擎，用于根据网络中网络设备的配置信息，以及网络中的拓扑结构计算中网络传输报文使用的路由转发表项。SMT 求解器，在上述路由转发表项用一组一阶逻辑公式表示时，可以通过 SMT 求解器对网络中的数据链路进行验证。

配置数据的数据模型 144，用于描述网络中网络设备的配置数据。通常包括从网络中采集的配置数据的数据模型，即已为网络中网络设备配置的配置数据的模型，以及待为网络中网络设备配置的配置数据的数据模型。

数据链路模型 145，用于描述网络中数据链路的模型。例如可以是上述一组一阶逻辑公式。

南向采集模块 146，用于采集网络中网络设备的配置数据。通常，上述南向采集模块可以配置有 Netconf-Client，以便南向采集模块 146 可以基于 Netconf 采集网络中网络设备的配置数据。

需要说明的是，网络配置验证系统 140 可以部署在 SDN 控制器中，还可以单独的部署在服务器中，本申请实施例对此不做限定。

下文结合图 3 介绍本申请实施例的网络验证的方法，需要说明的是，该方法可以由图

1 中的网络验证系统 140 执行，图 3 所示的方法涉及数据链路验证的方案，可以由网络验证系统中用于数据链路验证的模块配合执行，例如可以由数据链路验证、路由/拓扑计算引擎、以及数据链路模型 145 等模块配合执行。

图 3 是本申请实施例的网络验证方法的示意性流程图。图 3 所示的方法包括步骤 310 以及步骤 320。

310，网络验证系统获取多个网络设备的配置数据，其中，配置数据的数据模型是通过与网络设备无关的通用数据建模语言描述的。

上述网络设备的配置数据可以包括网络设备的 IP 地址、子网掩码、网关、端口、物理地址以及防火墙（firewall）等。

上述多个网络设备的配置数据可以包括已经为网络设备配置的配置数据，还可以是待为网络设备配置的配置数据以及待为网络设备更新的配置数据。关于网络验证系统获取已配置的配置数据以及待配置的配置数据的具体方式在下文中详细介绍。

需要说明的是，若各个厂商的网络设备使用的配置数据的数据模型都是基于上述数据模型，则网络验证系统可以直接从网络设备中采集配置数据。若各个厂商的网络设备使用的配置数据的数据模型是与网络设备相关的数据模型，或者与厂商相关的数据模型，则需要将上述网络设备相关的数据模型，或者与厂商相关的数据模型转换成上述与网络设备无关的数据模型。其中，上述数据模型之间的转换过程可以由运维人员进行转换，再输入进上述网络验证系统。

上述数据模型的转换过程可以包括：若网络设备是依赖安全外壳（Secure Shell，SSH）协议的，则可以先将网络设备的厂商特性模型转换为基于 SSH 协议的通用模型，在将基于 SSH 协议的通用模型转换为本申请实施例的数据模型。若网络设备是支持 Netconf 协议的，则将网络设备中的配置数据由厂商特性 BA（Binding-Aware）模型转换为 BI YANG 模型，再将 BI（Binding-Independent）YANG 模型转换为本申请实施例的数据模型。其中，BA 模型是指使用根据 YANG 模型定义而自动生成的 Java Bindings 的插件（plugin），BI 模型是指使用文件对象模型（Document Object Model，DOM）格式的应用程序编程接口，（ Application Programming Interface，API）不依赖 Java Bindings 的插件。

可选地，所述配置数据的数据模型包括所述配置数据的通用的数据属性以及所述配置数据的可扩展的数据属性。其中，可扩展的数据属性可以关联数据模型中未添加的数据属性或者网络设备私有属性，例如厂商私有属性等。通用的数据属性包括常用的数据属性。

可选地，通用的数据属性中包括对网络进行数据链路的验证所需的常用数据属性，或者通用的数据属性中包括对网络进行配置验证所需的常用数据属性。

本申请实施例使用的配置数据的数据模型与 YANG 模型的原理相似，但是通过配置数据的数据模型包含了对网络的数据链路进行验证的所需的配置数据，或者包含了对网络的配置进行验证的所需的配置数据，使得通过一个配置数据的数据模型可以获得数据链路验证，或者配置验证所需的配置数据，有利于简化获取配置数据的流程。避免了使用传统的 YANG 模型中不同类型的配置数据承载于不同的 YANG 模型中。例如，传统的 YANG 模型中访问控制列表和设备接口等配置数据使用单独的 YANG 模型。

图 4 是本申请实施例的配置数据的数据模型的组织形式的示意图。图 4 仅仅从便于理解的角度介绍本申请实施例的数据模型，而数据模型的真是逻辑结构请参见图 5 所示。图 4 所示的数据模型包括通用的数据属性 410，以及可扩展的数据属性 420。

其中，通用的数据属性410包括配置名称、设备类型、设备接口、设备IP地址、虚拟专用网路由转发表（virtual private network routing and forwarding table，vrf）、安全域、设备厂商等。

可扩展的数据属性420包括扩展价值属性以及扩展私有属性。其中，扩展价值数据可以理解为具有扩展价值的数据属性，即当前数据模型中未包含，但后续考虑添加至数据模型的数据属性，例如设备认证信息等。扩展私有属性包括设备相关的私有数据属性以及厂商私有的数据属性。

可选地，所述配置数据的数据模型为树形结构。上述数据模型中的配置数据可以存储在该属性结构的节点中。

可选地，图4所示的数据模型的组织形式中，可扩展的数据属性对应可扩展的数据属性的配置数据的路径，该路径指向树形结构中存储可扩展的数据属性的配置数据的节点。例如，可扩展的数据属性为设备的认证信息，则图4所示的组织形式中，可扩展的数据属性可以对应设备认证信息的路径，该路径可以指向在树形结构中存储设备认证信息的节点。

下文结合图5介绍本申请实施例的配置数据的数据模型的逻辑结构的示意图。该数据模型具有树形化层次结构，因此，配置数据的数据模型又被称为“配置树”。配置树包括根节点501以及多个叶子节点502。

其中根节点501用于标识整棵配置树。叶子节点502用于承载数据模板中的所有的原子配置数据。承载有配置名称、设备类型、设备接口、设备IP地址、vrf、安全域、设备厂商等。

在本申请实施例中通过使用树形结构表示配置数据的数据模型，即使用与YANG模型相似的结构数据模型，使得配置数据的数据模型与Netconf协议之间的匹配程度，与YANG模型与Netconf协议之间的匹配程度相似，有利于基于Netconf协议推广上述配置数据的数据模型。

另一方面，由于本申请实施例的配置数据的数据模型的结构与YANG模型类型，因此可以借用YANG模型可以转化Netconf报文的性能，将本申请实施例的配置数据的数据模型与Netconf报文结合，应用与目前的网络中。上述将配置数据的数据模型转化为Netconf报文的过程可以称为“配置数据的数据模型的YANG化”。

320，所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备的拓扑结构，对所述多个网络设备之间的数据链路进行验证。

在本申请实施例中，网络验证系统可以基于与网络设备无关的通用数据建模语言描述的配置数据，以及网络的拓扑结构，对网络进行数据链路验证。有利于提高网络验证系统的扩展性。避免了传统的网络仿真软件中，提供针对每种网络设备的配置数据的模板，导致网络仿真软件的扩展性较差。

可选地，上述步骤320包括：所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，计算路由得到，所述多个网络设备的路由转发表项；所述网络验证系统根据所述多个网络设备的路由转发表项，对所述多个网络设备之间的数据链路进行验证。

本申请中，基于多个网络设备的配置数据直接生成路由转发表项，并基于路由转发表项对网络的数据链路进行验证，有利于简化得到路由转发表项的过程。避免了传输的数据

链路过程中，网络设备需要基于配置数据（例如，IP 地址）进行路由学习，得到路由转发表项。

可选地，上述多个网络设备的路由转发表项可以通过多个一阶逻辑表达式表示。

具体地，可以通过多个一阶逻辑表达式表示网络中传输数据的路由转发表项，对网络的数据链路进行验证的过程，可以理解为将上述多个一阶逻辑表达式描述的路由转发表项作为传输报文的约束条件，再通过状态机模拟报文在网络中的传输状态，以对网络中的数据连链路进行验证。

如上文所述，上述网络设备的配置数据可以已为网络设备配置的配置数据，或者待为网络设备配置的配置数据。其中，基于已配置的配置数据的验证过程可以称为“事后验证”，基于待配置的配置数据或者待更新的配置数据的验证过程可以称为“事前验证”。

下文分别基于“事前验证”的场景以及“事后验证”的场景介绍本申请实施例的方法。

在“事后验证”的场景中，网络验证系统用于对网络中网络设备已配置的配置数据进行验证，下文结合图 6 介绍本申请实施例的方法。图 6 是本申请实施例的网络验证方法的示意性流程图，图 6 所示的方法包括步骤 510 至步骤 540。

510，网络验证系统从网络（或者称“真实网络”）中采集多个网络设备的配置数据。

可选地，网络验证系统可以向网络设备发送 Netconf 获取（Netconf-get）请求，以从网络设备中获取配置数据。基于目前 Netconf 的规定，上述配置数据的格式为 YANG 模型。当然，网络验证系统还可以通过其他命令获取网络设备的配置数据，例如，上述网络支持虚拟系统（Virtual system，Vsys）功能的情况下，还可以通过 Vsys 中的配置数据获取命令（get-config）获取配置数据，本申请实施例对此不做限定。

520，网络验证系统获取多个网络设备的拓扑结构。

需要说明的是，上述拓扑结构可以是由用户手动向网络验证系统输入的，也可以是网络验证系统基于 Netconf 从网络中采集的，本申请实施例对此不做限定。

530，网络验证系统基于多个网络设备的拓扑结构、多个网络设备的配置数据，得到多个网络设备的路由转发表项。

540，网络验证系统根据多个网络设备的路由转发表项，对多个网络设备之间的数据链路进行验证。

在“事前验证”的场景中，网络验证系统用于对网络中网络设备已配置的配置数据进行验证，下文结合图 7 介绍本申请实施例的方法。图 7 是本申请实施例的网络验证方法的示意性流程图，图 7 所示的方法包括步骤 610 至步骤 640。

610，网络验证系统获取待配置的配置数据或待更新的配置数据。

具体地，上述待配置的配置数据可以是待为一个网络设备配置的配置数据，或者待为多个网络设备配置的配置数据。上述待更新的配置数据可以是待为一个网络设备配置的配置数据，或者待为多个网络设备更新的配置数据。

通常，上述待配置的配置数据或者待更新的配置数据可以由网络中的控制器（例如，SDN 控制器）为网络设备配置，网络验证系统可以在控制器为网络设备配置或更新上述配置数据之前，先基于待配置的配置数据或者待更新的配置数据进行数据链路的验证，确定在真实网络中使用上述待配置的配置数据或者待更新的配置数据是否合理。

可选地，控制器基于 Netconf 协议为网络设备配置配置数据，则网络验证系统从控制器中获取的待更新的配置数据或待配置的配置数据为 YANG 模型的。

620，网络验证系统获取多个网络设备的拓扑结构。

需要说明的是，上述拓扑结构可以是由用户手动向网络验证系统输入的，也可以是网络验证系统基于 Netconf 从网络中采集的，本申请实施例对此不做限定。

630，网络验证系统基于多个网络设备的拓扑结构、多个网络设备的配置数据，得到多个网络设备的路由转发表项。

640，网络验证系统根据多个网络设备的路由转发表项，对多个网络设备之间的数据链路进行验证。

基于上文的介绍，本申请实施例的网络验证系统还可以对上述待配置的配置数据，或者网络中已配置的配置数据对网络进行配置验证。即，所述多个网络设备的配置数据中包括第一网络设备的配置数据，图 3 所示的方法还包括：所述网络验证系统根据所述第一网络设备的配置数据，对所述第一网络设备进行配置验证，其中，配置验证是指对所述第一网络设备的配置数据的数据模型中的任意一个或多个数据属性进行验证。

上述第一网络设备可以是多个网络设备中的任意一个。在本申请实施例中，还可以使用上述方法同时验证多个网络设备的配置。由于验证方式与上文验证第一网络设备的配置的方式相类似，为了简洁，在此不再赘述。

同理，基于配置数据是已配置的配置数据还是待配置的配置数据可以分为“事后验证”以及“事前验证”的场景。在事前验证或者事后验证的场景中，配置数据的获取方式可以参见图 6 和图 7 中的介绍，为了简洁，在此不再赘述。

上文主要结合图 6，图 7 介绍了本申请实施例的数据链路的验证过程，需要说明的是，承载于本申请实施例的配置数据的数据模型的配置数据还可以用于网络的配置验证，具体地配置验证类型可以参见图 1 中相关介绍，为了简洁，在此不再赘述。

需要说明的是，上述配置验证以及数据链路验证可以结合使用，也可以单独使用，本申请实施例对此不做限定。

可选地，上述配置验证的过程可以与上文图 6 以及图 7 所示的“事前验证”以及“事后验证”相结合。并且配置验证的过程可以在数据链路验证之后使用，也可以在数据链路之前使用，或者独立于数据链路验证单独使用。本申请实施例对此不作具体限定。

上文结合图 1 至图 7 介绍本申请实施例的方法，下文结合图 8 至图 9 介绍本申请实施例的装置。应理解，图 8 至图 9 可以执行图 3、图 6 以及图 7 中的部分或全部步骤，为了简洁，在此不再赘述。

图 8 是本申请实施例的网络验证的装置的示意图，图 8 所示装置 800 包括输入输出模块 810 和处理模块 820。

输入输出模块 810，用于获取多个网络设备的配置数据，其中，配置数据的数据模型为与网络设备无关的通用数据建模语言描述的；

处理模块 820，用于根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证。

可选地，作为一个实施例，所述处理模块 820 用于根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，计算路由得到所述多个网络设备的路由转发表项；以及根据所述路由转发表项，对所述多个网络设备之间的数据链路进行验证。

可选地，作为一个实施例，所述配置数据的数据模型包括所述配置数据的通用的数据属性以及所述配置数据的可扩展的数据属性，其中，所述通用的数据属性包括以下数据属

性中的一个或多个：配置名称、设备类型、设备接口、设备互联网协议地址IP地址或虚拟专用网络路由转发表vrf，所述可扩展的数据属性包括私有数据属性。

可选地，作为一个实施例，所述配置数据的数据模型为树形结构，所述数据模型中的可扩展的数据属性为存储所述可扩展的数据属性的路径，所述路径用于指向所述树形结构中存储所述可扩展的数据属性的节点。

可选地，作为一个实施例，所述多个网络设备的配置数据中包括第一网络设备的配置数据，所述处理模块820，还用于根据所述第一网络设备的配置数据，对所述第一网络设备进行配置验证，其中，配置验证是指对所述第一网络设备的配置数据的数据模型中的任意一个或多个数据属性进行验证。

可选地，作为一个实施例，所述配置数据为以下任一种：待配置的配置数据；已配置的配置数据；待更新的配置数据。

可选地，作为一个实施例，所述多个网络设备包括第二网络设备，所述通用数据建模语言为YANG模型，所述输入输出模块还用于：接收网络配置协议NetConf报文，所述NetConf报文中包括所述第二网络设备的配置数据，所述第二网络设备的配置数据用于对所述第二网络设备进行配置，或者对所述第二网络设备的配置进行更新。

在可选的实施例中，所述处理模块810可以为处理器920，所述输入输出模块820可以为输入/输出接口930，所述网络验证系统还可以包括存储器910，具体如图9所示。

图9是本申请实施例的另一网络验证系统的示意图。图9所示的网络验证系统900可以包括：存储器910、处理器920、通信接口930。其中，存储器910、处理器920、输入/输出接口930通过内部连接通路，例如总线，相连。该存储器910用于存储指令，该处理器920用于执行该存储器920存储的指令，通过该通信接口930接收输入的数据和信息，输出操作结果等。

可选地，上述网络验证系统900可以包括一个或者多个服务器，本申请实施例对此不作限定。

在实现过程中，上述方法的各步骤可以通过处理器920中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器910，处理器920读取存储器910中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

处理器920可以为中央处理单元（central processing unit，CPU），还可以是其他通用处理器、数字信号处理器（digital signal processor，DSP）、专用集成电路（application specific integrated circuit，ASIC）、现成可编程门阵列（field programmable gate array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

应理解，本申请实施例中，该存储器可以包括只读存储器和随机存取存储器，并向处理器提供指令和数据。处理器的一部分还可以包括非易失性随机存取存储器。例如，处理器还可以存储设备类型的信息。

应理解，在本申请实施例中，“与A相应的B”表示B与A相关联，根据A可以确定B。但还应理解，根据A确定B并不意味着仅仅根据A确定B，还可以根据A和/或其它信息

确定 B。

应理解，本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

应理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（digital subscriber line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够读取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，数字通用光盘（digital video disc，DVD））或者半导体介质（例如，固态硬盘（solid state disk，SSD））等。

以上所述，仅为本申请的具体实施方式，但本申请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申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求

1、一种网络验证的方法，其特征在于，包括：

网络验证系统获取多个网络设备的配置数据，其中，配置数据的数据模型是通过与网络设备无关的通用数据建模语言描述的；

所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证。

2、如权利要求 1 所述的方法，其特征在于，所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，对所述多个网络设备之间的数据链路进行验证，包括：

所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备之间的拓扑结构，计算路由，得到所述多个网络设备的路由转发表项；

所述网络验证系统根据所述多个网络设备的路由转发表项，对所述多个网络设备之间的数据链路进行验证。

3、如权利要求 1 或 2 所述的方法，其特征在于，所述数据模型包括通用数据属性以及可扩展数据属性，其中，所述通用数据属性包括以下数据属性中的一个或多个：配置名称、设备类型、设备接口、设备互联网协议地址 IP 地址或虚拟专用网络路由转发表，所述可扩展数据属性包括私有数据属性。

4、如权利要求 1-3 中任一项所述的方法，其特征在于，所述多个网络设备的配置数据中包括第一网络设备的配置数据，所述方法还包括：

所述网络验证系统根据所述第一网络设备的配置数据，对所述第一网络设备进行配置验证，其中，配置验证是指对所述第一网络设备的配置数据的数据模型中的任意一个或多个数据属性进行验证。

5、如权利要求 1-4 中任一项所述的方法，其特征在于，所述多个网络设备的配置数据包括：待配置的配置数据，已配置的配置数据，待更新的配置数据。

6、如权利要求 1-5 中任一项所述的方法，其特征在于，所述多个网络设备包括第二网络设备，所述通用数据建模语言为 YANG 模型，所述网络验证系统获取网络中多个网络设备的配置数据，包括：

所述网络验证系统接收网络配置协议 NetConf 报文，所述 NetConf 报文中包括所述第二网络设备的配置数据，所述第二网络设备的配置数据用于对所述第二网络设备进行配置，或者对所述第二网络设备的配置进行更新。

7、一种网络验证的装置，其特征在于，包括：

输入输出模块，用于获取网络中多个网络设备的配置数据，其中，配置数据的数据模型为与网络设备无关的通用数据建模语言描述的；

处理模块，用于根据所述多个网络设备的配置数据，以及所述多个网络设备的拓扑结构，对所述多个网络设备之间的数据链路进行验证。

8、如权利要求 7 所述的装置，其特征在于，所述处理模块，用于：

根据所述多个网络设备的配置数据，以及所述多个网络设备的拓扑结构，计算路由得到，所述多个网络设备的路由转发表项；

根据所述多个网络设备的路由转发表项，对所述多个网络设备之间的数据链路进行验

证。

9、如权利要求 7 或 8 所述的装置，其特征在于，所述配置数据的数据模型包括所述配置数据的通用的数据属性以及所述配置数据的可扩展的数据属性，其中，所述通用的数据属性包括以下数据属性中的一个或多个：配置名称、设备类型、设备接口、设备互联网协议地址 IP 地址或虚拟专用网络路由转发表，所述可扩展的数据属性包括私有数据属性。

10、如权利要求 7-9 中任一项所述的装置，其特征在于，所述多个网络设备的配置数据中包括第一网络设备的配置数据，

所述处理模块，还用于根据所述第一网络设备的配置数据，对所述第一网络设备的进行配置验证，其中，配置验证是指对所述第一网络设备的配置数据的数据模型中的任意一个或多个数据属性进行验证。

11、一种计算机可读介质，其特征在于，所述计算机可读介质存储有程序代码，当所述计算机程序代码在计算机上运行时，使得计算机执行如权利要求 1-6 中任一项所述的方法。

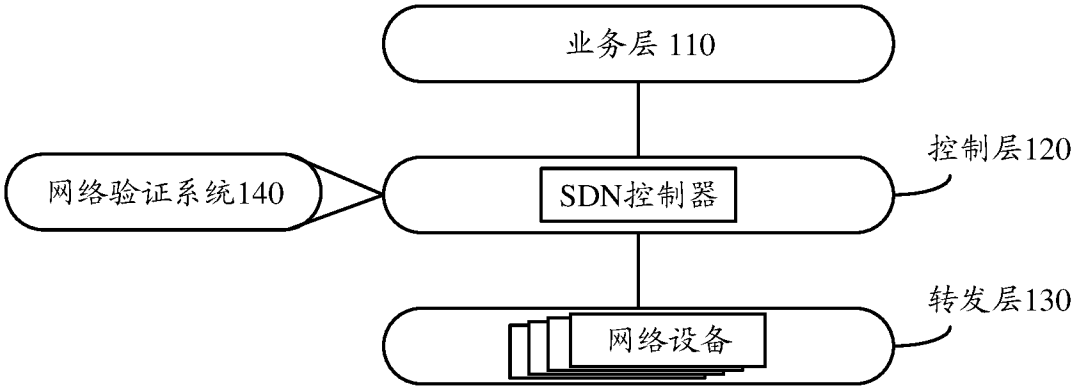


图 1

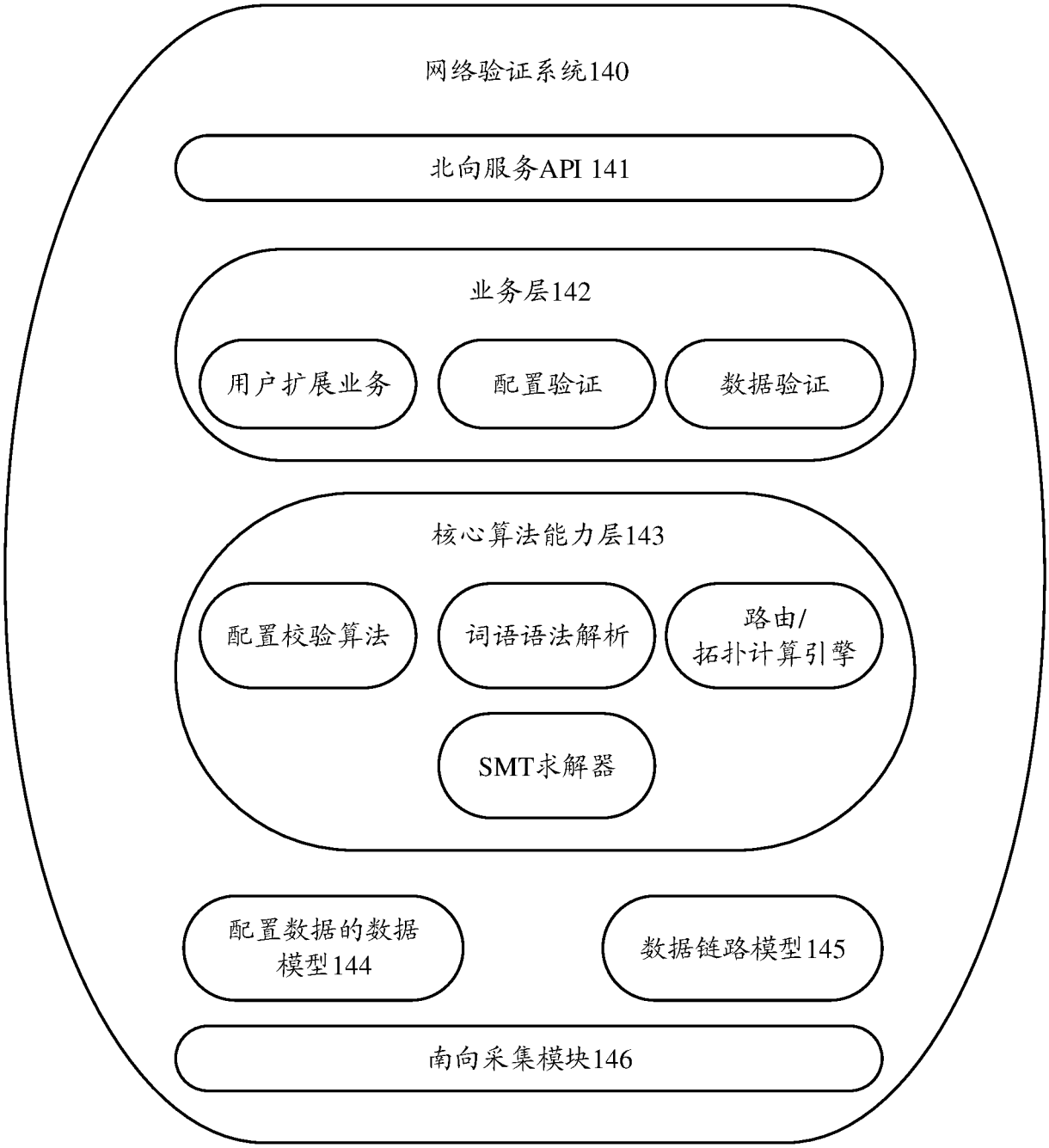

网络验证系统140
北向服务API 141
业务层142
用户扩展业务
配置验证
数据验证
核心算法能力层143
配置校验算法
词语语法解析
路由/
拓扑计算引擎
SMT求解器
配置数据的数据
模型144
数据链路模型145
南向采集模块146

图 2

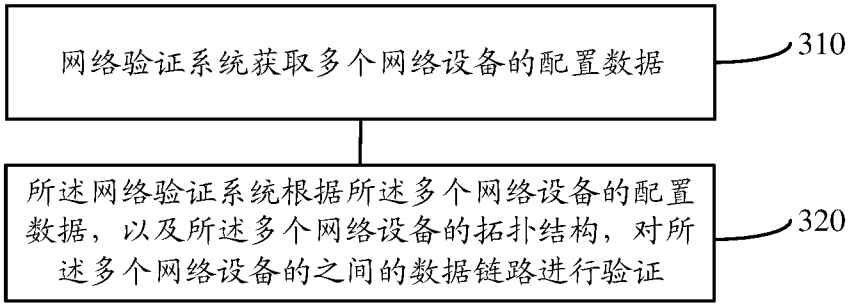

网络验证系统获取多个网络设备的配置数据
310
所述网络验证系统根据所述多个网络设备的配置数据，以及所述多个网络设备的拓扑结构，对所述多个网络设备的之间的数据链路进行验证
320

图 3

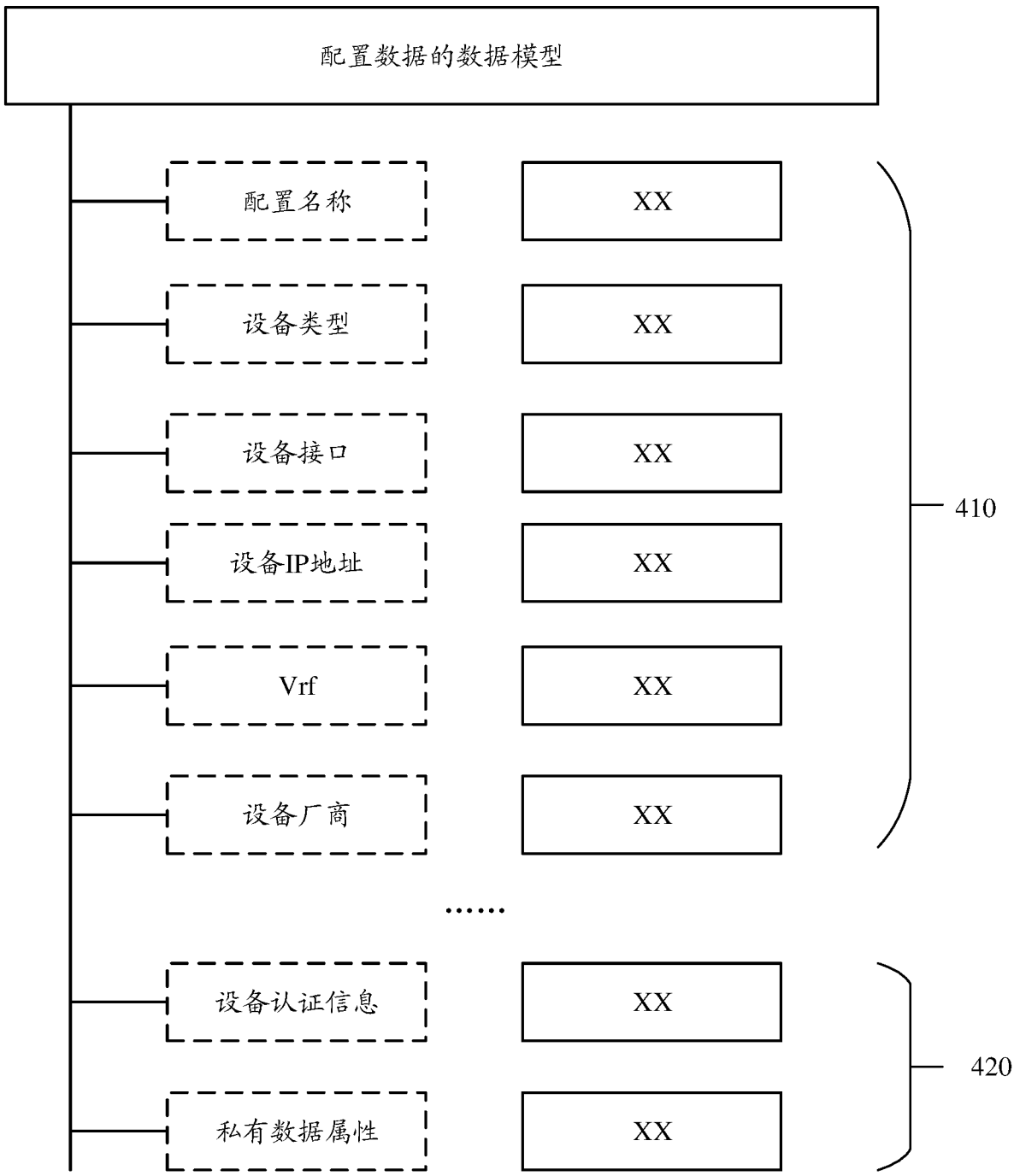

配置数据的数据模型
配置名称
XX
设备类型
XX
设备接口
XX
设备IP地址
XX
Vrf
XX
设备厂商
XX
410
.....
设备认证信息
XX
私有数据属性
XX
420

图 4

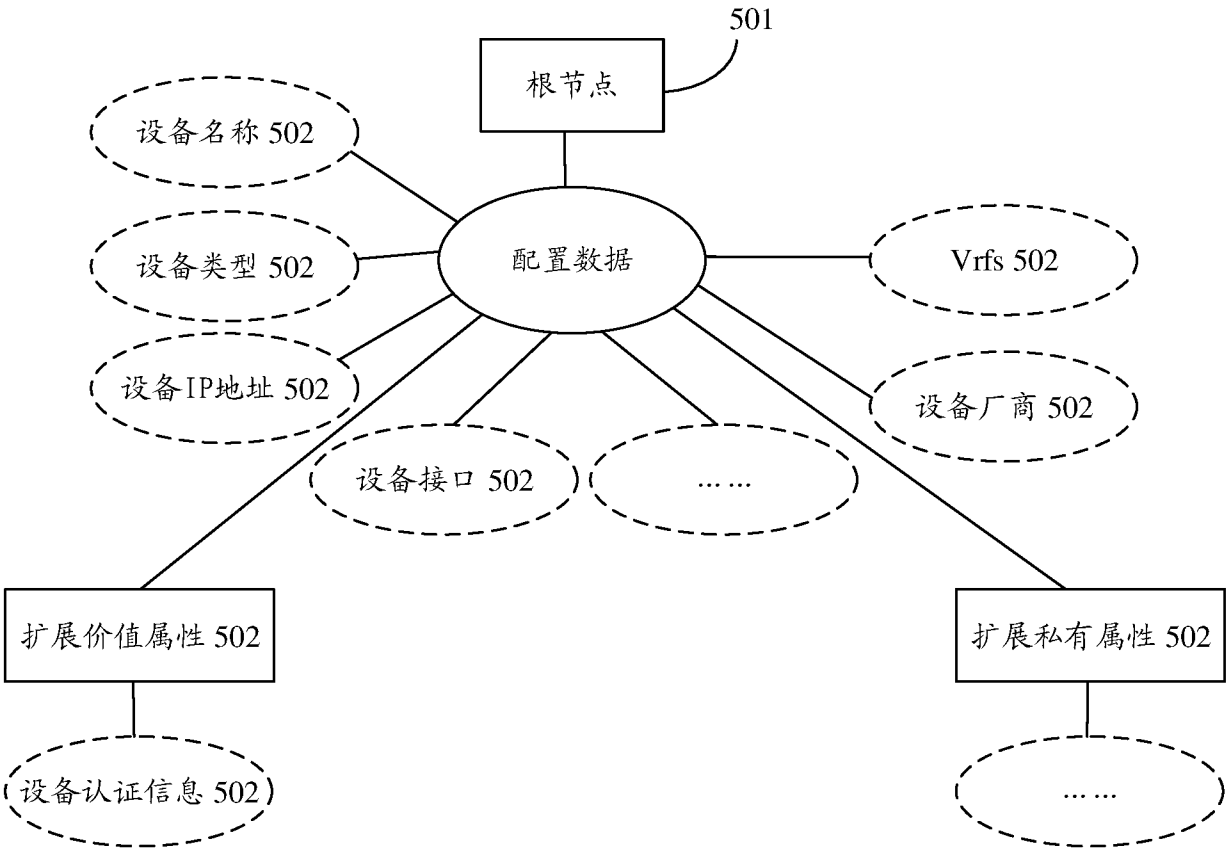

501
根节点
设备名称 502
设备类型 502
设备IP地址 502
配置数据
Vrfs 502
设备厂商 502
设备接口 502
……
扩展价值属性 502
扩展私有属性 502
设备认证信息 502
……

图 5

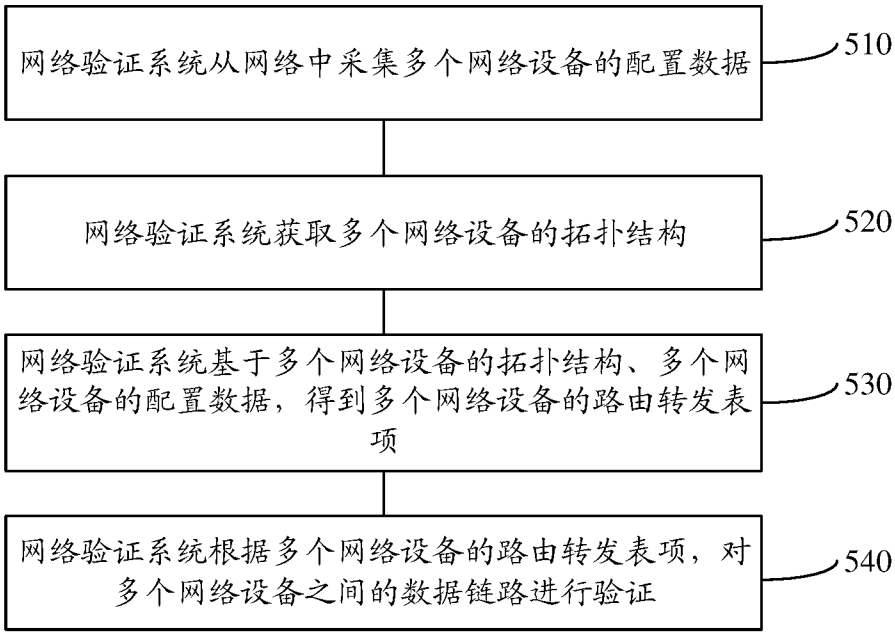

网络验证系统从网络中采集多个网络设备的配置数据
510
网络验证系统获取多个网络设备的拓扑结构
520
网络验证系统基于多个网络设备的拓扑结构、多个网络设备的配置数据，得到多个网络设备的路由转发表项
530
网络验证系统根据多个网络设备的路由转发表项，对多个网络设备之间的数据链路进行验证
540

图 6

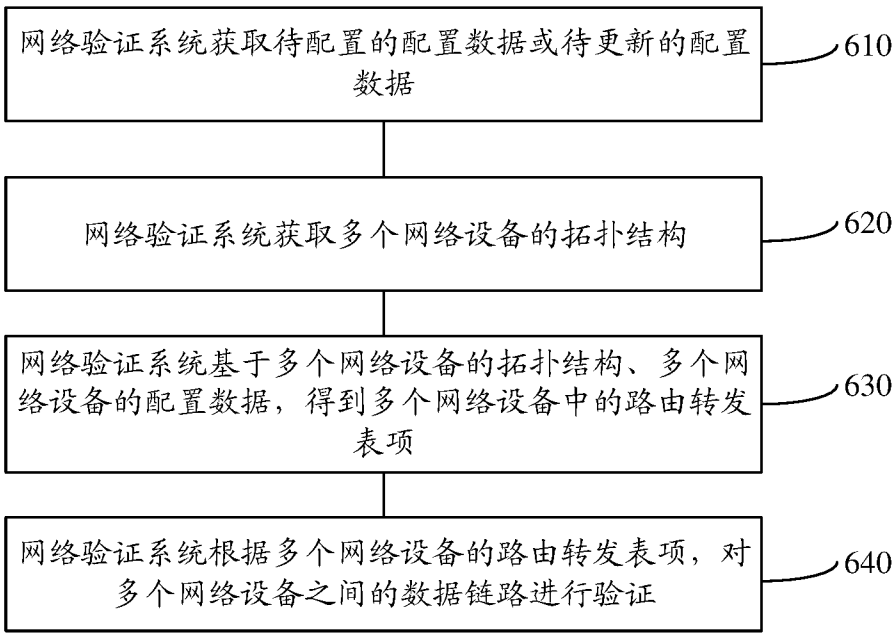

网络验证系统获取待配置的配置数据或待更新的配置数据
610
网络验证系统获取多个网络设备的拓扑结构
620
网络验证系统基于多个网络设备的拓扑结构、多个网络设备的配置数据，得到多个网络设备中的路由转发表项
630
网络验证系统根据多个网络设备的路由转发表项，对多个网络设备之间的数据链路进行验证
640

图 7

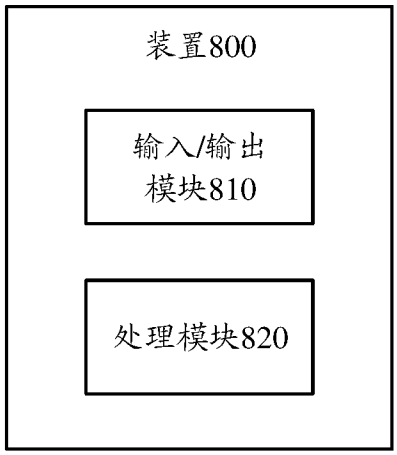

装置800
输入/输出
模块810
处理模块820

图 8

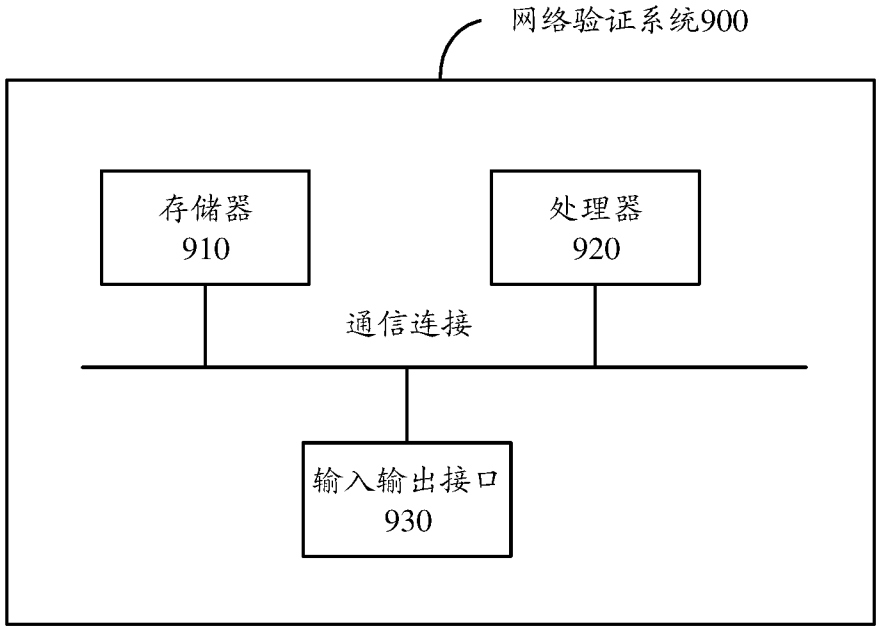

网络验证系统900
存储器
910
处理器
920
通信连接
输入输出接口
930

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/127244

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(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)

CNABS, CNTXT, CNKI, VEN, WOTXT, USTXT, EPTXT: 验证, 配置, 模型, 建模, netconf, YANG, 拓扑, 链路, 路由; verif+, configur+, model+, topology, link, route

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106656792 A (NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY, PLA) 10 May 2017 (2017-05-10) description, paragraphs [0050]-[0076]	1-11
A	CN 109361550 A (NATIONAL COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT CENTER et al.) 19 February 2019 (2019-02-19) entire document	1-11
A	CN 104065514 A (TSINGHUA UNIVERSITY) 24 September 2014 (2014-09-24) entire document	1-11
A	WO 2018231901 A1 (CISCO TECHNOLOGY, INC.) 20 December 2018 (2018-12-20) entire document	1-11

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 March 2020	**13 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/127244

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106656792 A	10 May 2017	CN 106656792 B	28 June 2019
CN 109361550 A	19 February 2019	None	
CN 104065514 A	24 September 2014	None	
WO 2018231901 A1	20 December 2018	US 10462010 B2	29 October 2019
		US 2018359146 A1	13 December 2018

国际检索报告

国际申请号
PCT/CN2019/127244

A. 主题的分类

H04L 12/24(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））

CNABS,CNTXT,CNKI,VEN,WOTXT,USTXT,EPTXT: 验证，配置，模型，建模，netconf，YANG， 拓扑，链路，路由；ve-rif+, configur+, model+, topology, link, route

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
X	CN 106656792 A (中国人民解放军国防科学技术大学) 2017年 5月 10日 (2017-05-10) 说明书50-76段	1-11
A	CN 109361550 A (国家计算机网络与信息安全管理中心等) 2019年 2月 19日 (2019-02-19) 全文	1-11
A	CN 104065514 A (清华大学) 2014年 9月 24日 (2014-09-24) 全文	1-11
A	WO 2018231901 A1 (CISCO TECH INC.) 2018年 12月 20日 (2018-12-20) 全文	1-11

☐ 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（如具体说明的）
“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	国际检索报告邮寄日期
2020年 3月 3日	2020年 3月 13日
ISA/CN的名称和邮寄地址 中国国家知识产权局(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 吴斌 电话号码 86-010-62412115

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/127244

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	106656792	A	2017年 5月 10日	CN	106656792	B	2019年 6月 28日
CN	109361550	A	2019年 2月 19日		无		
CN	104065514	A	2014年 9月 24日		无		
WO	2018231901	A1	2018年 12月 20日	US	10462010	B2	2019年 10月 29日
				US	2018359146	A1	2018年 12月 13日