基于 SDN 的可视化流量分析器概要设计说明书

V1.2

2014 年 9 月

文档历史

序号	版本号	作者	修订
1	1.0	兰卫国、曹健、宋剑	起稿
2	1.1	兰卫国、曹健、宋剑	简要修改和细化
3	1.2	兰卫国、曹健、宋剑	细化数据表设计和流表管理

目录

项目意义 3
项目概述 4
系统功能 6
用户管理 6
访问排行统计 6
实时数据包数量监控 6
历史数据包数量统计 6
分组管理服务 7
报警管理 7
日志管理 7
功能模块 7
用户管理模块 7
访问排行模块 8
实时监控模块 8
历史查询 9
分组管理 9
报警设置 10
系统日志 10
参考文献 11

项目意义

基于 SDN 可视化流量分析器可以完成对进入网络的流量的统计分析，不同于传统路由的收集分析功能，而是基于软件定义网络（SDN）控制面与数据面相分离的思想，在支持 OpenFlow 的交换机网络中，布置流量分析工具，通过与 SDN Controller 的交互实现对 OpenFlow 交换机网络中流量的统计分析。

相对于现有的流量分析工具（如 cisco 的 NetFlow），基于 SDN 的可视化流量分析器不仅可以完全继承 NetFlow 关于 IPv4 和 IPv6 的统计分析功能，同时可以应用于纯 SDN 网络或者是含有部分 OpenFlow 交换机的异构网络等其他网络。基于 SDN 的可视化流量分析器所有分析信息只基于网络中的所有流量数据包，与网络通信协议类型、网络构成等无关，避免了 NetFlow 等现有流量分析工具对于网络和硬件条件的依赖性，具有更高的适应性和应用性。

基于 SDN 的可视化流量分析器相对于现有的流量分析工具的优势，如下表所示：

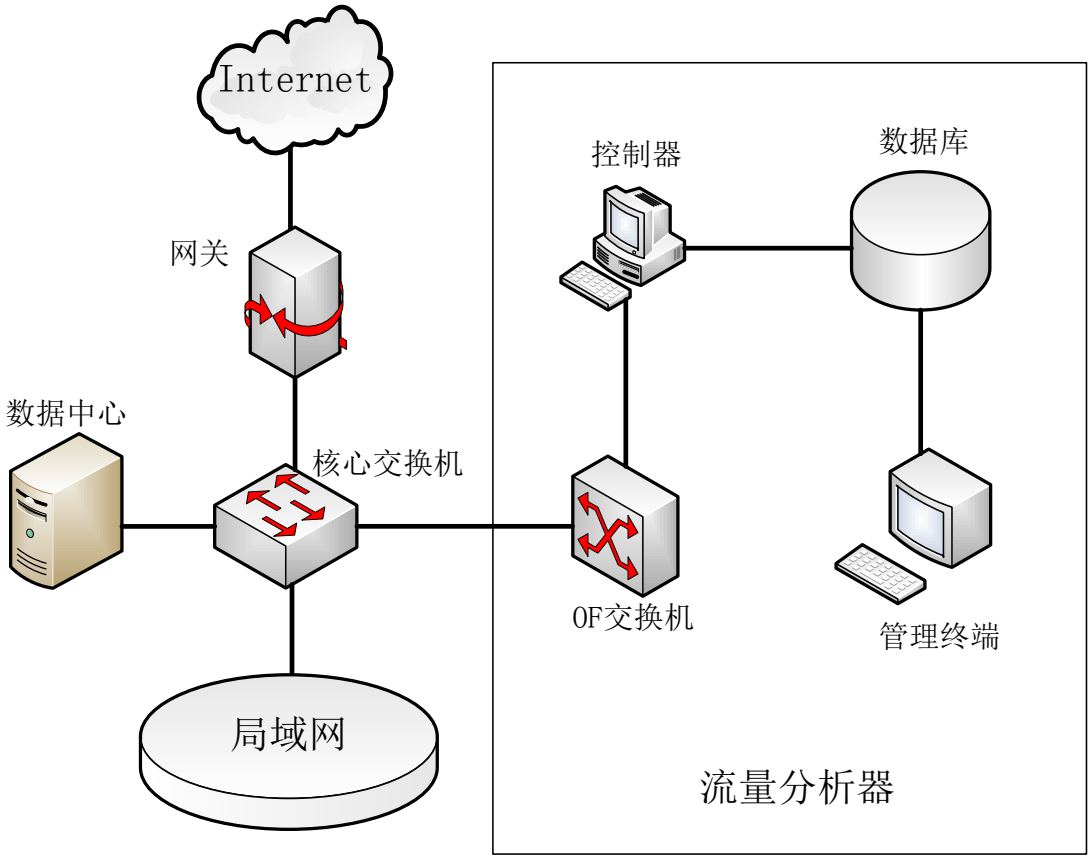
	NetFlow 等现有的流量分析工具	基于 SDN 的可视化流量分析器
设备依赖性	对设备依赖严重，特定工具只能在特定设备上使用，不具有普适性	对局域网内的设备无任何依赖，适用于各类型网络和异构网络
服务灵活性	可提供的服务较为固定，根据用户需求定制分析工具实现困难	SDN 的管理灵活，可针对用户需求灵活提供流量分析监控服务
对网络的干扰	占用交换机一定的 CPU 和缓存资源，对网络性能有影响	对于局域网内现有交换机和终端等均无影响
成本	成本高	成本低

表格 1　基于 SDN 的可视化流量分析器优势对比表

综上，将 SDN 技术用于流量收集和分析中，能够有效的发挥 SDN 可编程性的特点，尤其是它集中控制的特点在流量分析方面有先天优势。同时，可以提高现有网络的灵活性，可扩展性，节约系统的成本。

项目概述

本系统开发的设备将以一台 controller 与一台 OpenFlow 交换机组成，设备通过内部局域网核心交换机的镜像出口获取数据并做监测和检查，如图 1 所示。



图表 1　系统逻辑图

所需硬件如表 2 所示。

设备	数量	用途
OpenFlow 交换机	1 台	流统计，响应控制器的命令
控制器服务器	1 台	

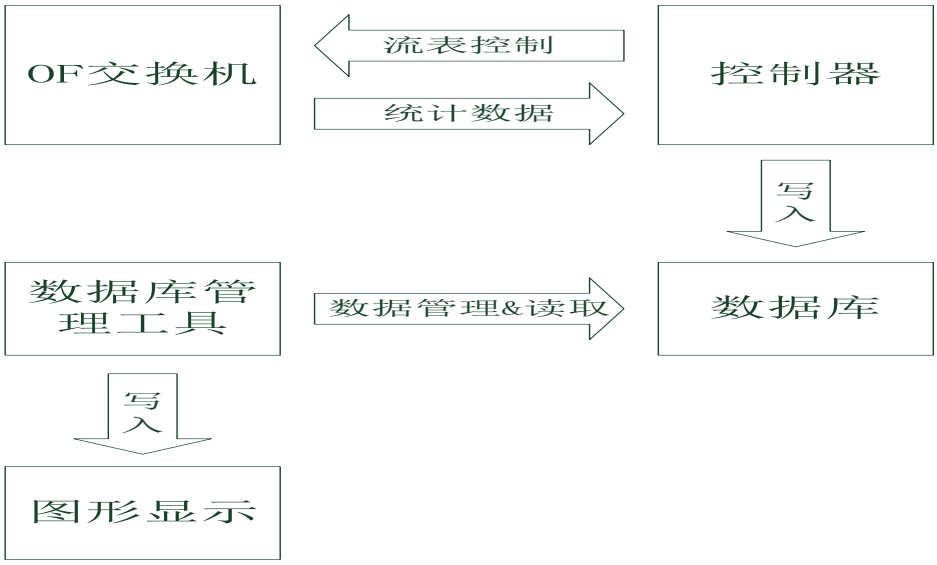
表格 2　系统设备需求表

本软件开发是基于 OpenDaylight 项目下的控制器。OpenDaylight 是一套以社

区为主导的开源框架，旨在推动软件定义网络透明化。该项目的核心是一套模块化、可插拔且极为灵活地控制器，它能够被部署在任何支持 java 平台之上，用户基于它能够开发自己的网络应用管理软件，快速地完成网络任务。由于基于全新的网络架构，本软件系统在流量分析控制上与传统的网络有根本的区别 。

系统采基于 OpenDaylight 进行开发，由控制器负责流表的设计和管理，同时统计由 OpenFlow 交换机记录的相关数据，将其存储入数据库，数据库有一定的管理规则，数据库的数据可以提供读取访问用于信息图形显示。如图 2 所示。

系统页面设计采用两级标签页设计模式，页面上方横排一级标签页，每个标签页对应页面中下方大部分内容各不相同，在每个一级标签页下，内容部分左侧的侧边栏（sidebar）为二级标签链接，每个二级标签所对应的其右侧内容各不相同，由此形成两级标签页目录导航形式网站，各标签页用 frame 标签实现，在各页面切换中网站网址不变。如图 3 所示。在网络正常运行的情况下，网络管理员可以通过 web 接口访问我们的控制器。



图表 2　系统结构示意图

<table>
<tr><td colspan="2">流量分析器</td></tr>
<tr><td>用户管理</td><td rowspan="7">功能区</td></tr>
<tr><td>访问排行</td></tr>
<tr><td>实时监控</td></tr>
<tr><td>历史查询</td></tr>
<tr><td>分组管理</td></tr>
<tr><td>报警设置</td></tr>
<tr><td>系统日志</td></tr>
</table>

图表 3　页面布局格式

系统功能

用户管理

添加用户、修改用户信息和删除用户，以及对用户赋予不同的权限。

访问排行统计

统计局域网内各终端与外部网络数据交互数据包数量排名，并提供分时段查询服务。

实时数据包数量监控

给出当前局域网内各终端实时数据交互数据。

历史数据包数量统计

可以根据用户当前的需求反馈指定时间段指定终端的历史数据包数量服务。

分组管理服务

网络管理员可根据实际情况对局域网内部终端进行分组，显示分组后数据包数量访问或被访问曲线图，可做多组曲线对比。

报警管理

提供对网络性能的具体管理服务，用户可以通过设置报警事件的方式通知系统监控网络流量，如果达到报警条件页面将给出报警信息。用户可以设置针对于数据包数目的报警管理事件，如设定某些特定 IP 的对外访问或被访问数据包频率限制（可用作攻击监测）、系统整体数据包发送频率限制等。

日志管理

记录系统本身的运行日志，以及系统检测到可能网络事件后的日志信息。系统本身的日志包括有用户登录事件等信息，网络事件包括有网络过载，网络节点失效等信息。

功能模块

用户管理模块

用户必须通过登录才能使用本系统，登录后用户可以在用户管理中看到当前系统的用户列表，该页面的主要功能是查看、修改、新建、删除用户。点击选择用户管理，在功能显示区会显示相应的用户列表。普通用户可以查看用户列表、查询流量数据、历史信息和该用户自身的系统日志；网络管理员不仅可以查看用户列表、查询流量数据和历史信息，同时还可以查看所有的网络异常事件和系统操作记录，用户的添加和删除也只能由网络管理员完成。

访问排行模块

访问统计排名页面主要负责提供局域网内用户与外部网络间的数据交互量统计服务，由对外访问排名和被访问排名两个子页面构成。

1. 对内访问排行

页面上方提供两个下拉选项框，分别负责获取访问统计时间段和列表容量，访问统计事件段分为过去 1 小时、1 天、1 周和 1 月这四个选项，列表容量分为 10、20、50 和 100 这四个选项。选定后页面列表显示相应时间段内访问量最多的对应容量地址列表。

2. 对外访问排行

页面内有 3 个选项卡，分别对应 IPv4、IPv6 和 mac 地址的统计信息。任一选项卡内的页面上方提供两个下拉选项框，分别负责获取访问统计时间段和列表容量，访问统计事件段分为过去 1 小时、1 天、1 周和 1 月这四个选项，列表容量分为 10、20、50 和 100 这四个选项。选定后页面列表显示相应时间段内被访问量最多的对应容量局域网地址列表。

实时监控模块

用户（网络管理员或者其他的有权限登录本系统的用户）可以在完成登录之后，点击进入实时监控功能界面，该界面主要用来监测交换机流表的当前实时数据包数量信息。基于当前活跃用户统计，页面提供源 IP 地址、目的 IP 地址和类型端口的当前实时数据包数量曲线图。

1. 源 IP 实时监控

该页面为实时流量统计下的子页面，页面上方提供下拉选项框，选项为 1 个小时内数据包数量，统计源 IP 地址，用户选择后页面通过与控制器的接口调用获取当前查询对象源 IP 地址实时监控信息并在页面以曲线图显示。页面同时提供可输入文本框用以查询任意 IP 的数据包数量曲线图。

2. 目的 IP 实时监控

该页面为实时流量统计下的子页面，页面上方提供下拉选项框，选项为 1 个

小时内数据包数量，统计目的 IP 地址，用户选择后页面通过与控制器的接口调用获取当前查询对象目的 IP 地址实时监控信息并在页面以曲线图显示。页面同时提供可输入文本框用以查询任意目的 IP 的数据包数量曲线图。

3. 类型端口实时监控

该页面为实时流量统计下的子页面，页面上方提供下拉选项框，选项为 1 个小时内数据包数量，统计数据包类型和对应的通信端口号，用户选择后页面通过与控制器的接口调用获取当前查询对象数据包类型和对应的通信端口号实时监控信息并在页面以曲线图显示。页面同时提供可输入文本框用以查询任意数据包类型和对应的通信端口号的数据包数量曲线图。

历史查询

历史查询页面提供源 IP 地址、目的 IP 地址和类型端口的历史流量图，页面上方提供单选按钮或者下拉菜单，可以选择查询特定 IP/类型端口的历史信息，提供地址/端口输入栏（根据类型选择而定），通过与控制器的接口调用获取当前 OpenFlow 交换机实时监控信息并在页面以曲线图显示；也可以选择流量最多的地址/类型端口的历史信息，通过与控制器的接口调用获取当前 OpenFlow 交换机实时监控信息并在页面以饼状图/柱状图显示。

分组管理

网络管理员可根据实际情况对局域网内部终端进行分组，显示分组后数据包数量访问或被访问曲线图，可做多组曲线对比。分组管理服务页面包括成员管理和组别数据查询 2 个子页面。

1. 成员管理

该页面提供对局域网内成员的分组服务，页面初始显示局域网内各组用户列表，其中未分组用户统一归属于未分组组别中。页面中提供分组新建按钮，用于新建不同分组。用户可以通过页面拖拽操作将不同局域网终端在分组中进行切换，每个分组提供删除操作，删除后该分组内终端自动归入未分组组别中，未分组组别不可删除。

2. 组别查询

该页面上方提供曲线图、柱状图下拉单选框、时间段下拉单选框（1 小时、1 天、1 周、1 月和总数据）和组别的多选框，当用户选定后在页面中显示相应的曲线图或柱状图。

报警设置

报警管理页面提供对网络性能的具体管理服务，用户可以通过设置报警事件的方式通知系统监控网络流量，如果达到报警条件页面将给出报警信息。用户可以设置针对于数据包数目的报警管理事件，如设定某些特定 IP 的对外访问或被访问数据包频率限制（可用作攻击监测）、系统整体数据包发送频率限制等。报警管理页面包括报警事件设置页面、报警事件查看页面和报警事件管理页面三个子页面。

1. 报警事件设置

该页面用于设置报警事件的监测数据及阈值，所有用户均可以设置报警事件。用户在页面内选定监测要求（协议类型、地址信息等）并设定相应的阈值，单击确定后页面形成表单发送给后台，后台处理后返回操作结果至页面显示。当网络当前流量数据超过阈值时页面应弹出警告。

2. 报警事件查看

报警事件查看页面以列表形式显示系统内所有的报警事件，页面上方提供事件输入文本框用于获取某段时间间隔内的报警事件。同时提供空白文本框可以查询某个用户的报警事件。

系统日志

该页面按时间倒序依次列出在本系统上登录用户历史操作信息。登录操作、退出操作和对数据层中数据产生实际改变的操作都将通过访问数据层接口保存到操作日志表中。当加载该页面时，调用接口，通过接口方法重新获取操作记录以列表显示。每条记录包括操作时间、用户名、用户编号、操作类型、操作描述。

参考文献

[1] 陆慧梅, 向勇, 史美林. Internet QoS 研究[J]. 小型微型计算机系统, 2002, 23(7): 786-791.

[2] McKeown N, Anderson T, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2): 69-74.

[3] Lantz B, Heller B, McKeown N. A network in a laptop: rapid prototyping for software-defined networks[C]//Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010: 19.

[4] 左青云, 陈鸣, 赵广松, 等. 基于 OpenFlow 的 SDN 技术研究[J].

[5] 张顺淼, 邹复民. 软件定义网络研究综述[J]. 计算机应用研究, 2013, 30(8): 2246-2251