基于 SDN 的可视化流量分析

详细设计说明书（2014 年 9 月）

文档历史

序号	版本号	修订	作者
1	1.0	起稿	宋剑
2	1.1	简要修改和细化	宋剑
3	1.2	细化 web 设计和功能管理	宋剑
4	1.3	细化数据表设计和流表管理	宋剑

目录

图表

正文

1. 系统介绍与结构

本文档是开发基于 SDN 的可视化流量分析器的设计说明。该应用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可应用性。

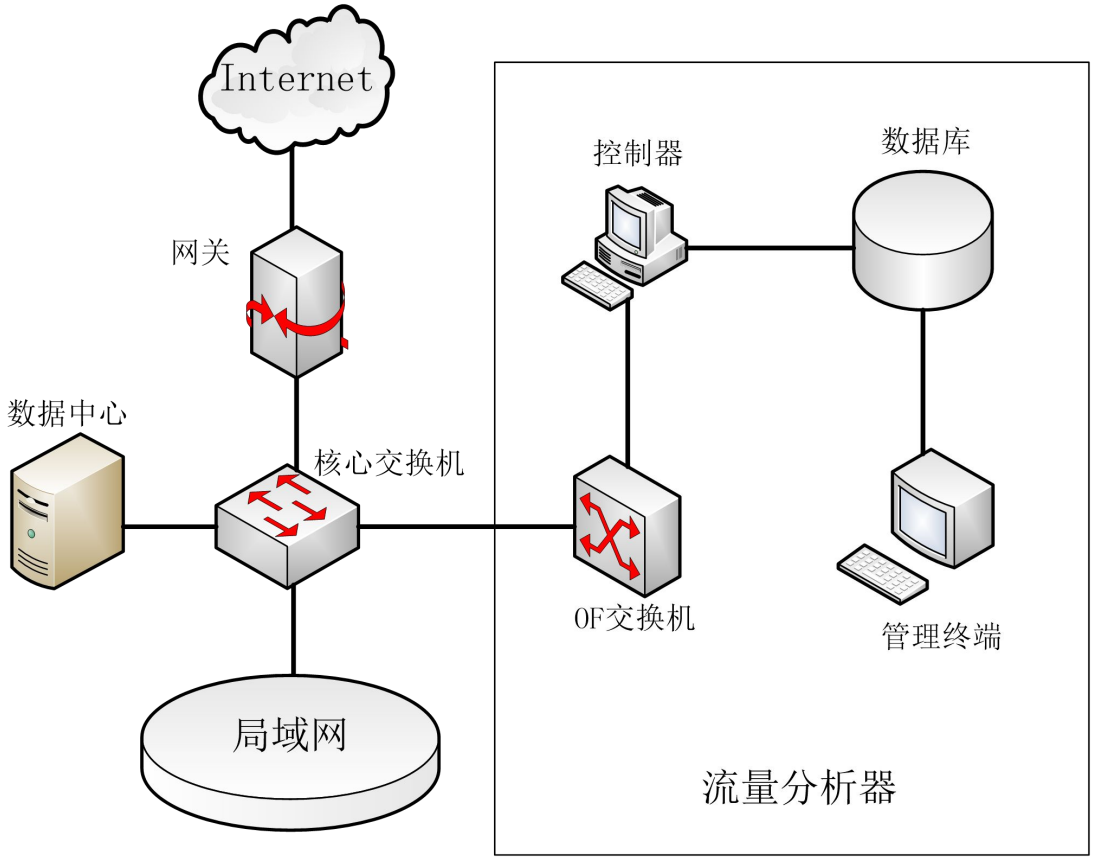
基于 SDN 的可视化流量分析器相对于现有的流量分析工具的优势见如下表格：

	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

开发的设备将以一台 controller 与一台 openflow 交换机组成，设备通过内网核心交换机的

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，本软件系统个在流量分析控制上与传统的网络有根本的区别 。

总而言之，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。

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，内容部分左侧侧边栏（sidebar）为二级标签链接，每个二级标签对应侧边栏右侧内容各不相同，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。

图表 2　系统结构示意图

图表 3　页面布局格式

系统中数据传输以 json 数据包格式传输，定义如下：

Json 数据只用于平台返回给页面 restful 接口查询信息所用，返回的信息都是由数据库中数据打包而成，格式为“[{参数 a: 参数 b，参数 c...}...]”，其中，参数 a 为数据库内数据存储主键（有两个主键时为第一个），参数 b、c、d...为数据库中该项存储的其他参数，数目不确定。每一条数据由中括号包围，相邻中括号间用逗号隔开，数据包由大括号包围。

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，系统提供以下服务：

1. 访问排行统计功能，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
2. 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
3. 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
4. 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
5. 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
6. 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

2. Web 前端设计

2.1 用户管理

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。

用户管理的功能显示区提供如下处理流程：

1、查看用户列表。点击用户管理时，系统调用用户列表查询接口（GET /users/），该接口会调用数据持久层 getUsers 服务方法获取用户信息表中的用户信息，并以列表显示。一条列表用户信息包括用户 ID、角色类型和上次登录时间。若用户数超过 10 个，则分页显示，每页显示 10 位用户。

2、修改用户信息的处理流程如下：

点击某个用户列表项，弹出信息修改对话框，所有用户都只能修改自己的用户名、用户密码；

用户修改完成后，单击确定按钮,将调用用户修改接口（PUT /users/），该接口继续调用数据层 setUser 方法更新数据库。

若接口调用成功，返回修改成功对话框，并刷新列表；

若由于修改数据异常、数据库连接问题等导致修改失败，返回修改失败对话框，并提示错误原因。

3、新建用户的处理流程如下：

点击新建按钮，进入新建用户对话框。只有管理员能够用户，因此其他用户对应的页面上没有新建按钮。

管理员输入用户名、用户初始密码、角色类型（权限），点击确定提交请求；

调用用户新建接口（POST /users/），接口接着调用数据层 addUser 方法更新数据库；

若接口调用成功，直接刷新功能显示区用户列表；

若接口调用失败，返回添加失败对话框，并提示错误原因。

4、删除普通用户，其处理流程主要是通过列表项左边的复选框选中要删除的一个或多个用户，单击删除按钮，系统调用删除用户接口（DELETE /users/），接着调用数据层的 deleteUsers 方法将相关用户删除。若删除失败，返回错误提示对话框。只有管理员有删除用户的权力，但是他不能删除自己。

2.2 访问排行

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。

2.2.1 对外访问排名

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 4 个选项，列表容量分为 10、20、50 和 100 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。

页面加载过程如下：

1. 页面加载时自动调用用户排名查询接口（GET /rank/），时间参数默认当天、列表容量参数默认 20，获取当天内所有地址的对外访问排名信息
2. 后台从数据库中取得数据打包成 Json 数据包返回给页面，如果没有数据返回错误信息
3. 页面解析后将获取结果以列表形式显示在页面上，如果为错误信息则弹出错误报告
4. 当用户选择统计时间段和列表容量信息并单击查询按钮后，页面获取时间参数和列表容量参数后重复步骤 1

2.2.2 被访问排名

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 4 个选项，列表容量分为 10、20、50 和 100 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。

页面加载过程如下：

1. 页面加载时自动调用用户排名查询接口（GET /rank/），地址类型默认为 IPv4、时间参数默认当天、列表容量参数默认 20，获取当天内所有地址的被访问排名信息
2. 后台从数据库中取得数据打包成 Json 数据包返回给页面，如果没有数据返回错误信息

3. 页面解析后将获取结果以列表形式显示在页面上，如果为错误信息则弹出错误报告
4. 当用户选择地址类型、统计时间段和列表容量信息并单击查询按钮后，页面获取地址类型参数、时间参数和列表容量参数后重复步骤 1

2.3 实时监控.

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。当前活跃用户统计页面提供基于源 IP、目的 IP 和类型端口的当前实时数据包数量曲线图。

2.3.1 源 IP 实时监控页面加载流程

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前若干个源 IP（或者类型），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。

页面加载过程如下：

1. 当用户选择要查询的信息时，页面自动调用实时信息查询接口（GET /realtime/）
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面

6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息调用相应控件形成曲线图显示

2.3.2 目的 IP 实时监控页面加载流程

1. 当用户选择要查询的信息时，页面自动调用实时信息查询接口（GET /realtime/）
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息调用相应控件形成曲线图显示

2.3.3 类型端口实时监控页面加载流程

1. 当用户选择要查询的信息时，页面自动调用实时信息查询接口（GET /realtime/）
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上， 否则将获取

的信息调用相应控件形成饼状图或者柱状图显示

2.4 历史查询

历史查询页面提供基于源 IP、目的 IP 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 OF 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 OF 交换机实时监控信息并在页面以饼状图/柱状图显示。

2.4.1 源 IP 历史查询页面加载流程

1. 页面获取用户设置的源 IP 查询选择信息和查询时间范围
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息调用相应控件形成曲线图显示

2.4.2 目的 IP 历史查询页面加载流程

1. 页面获取用户设置的目的 IP 查询选择信息和查询时间范围
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息调用相应控件形成曲线图显示

2.4.3 类型端口历史查询页面加载流程

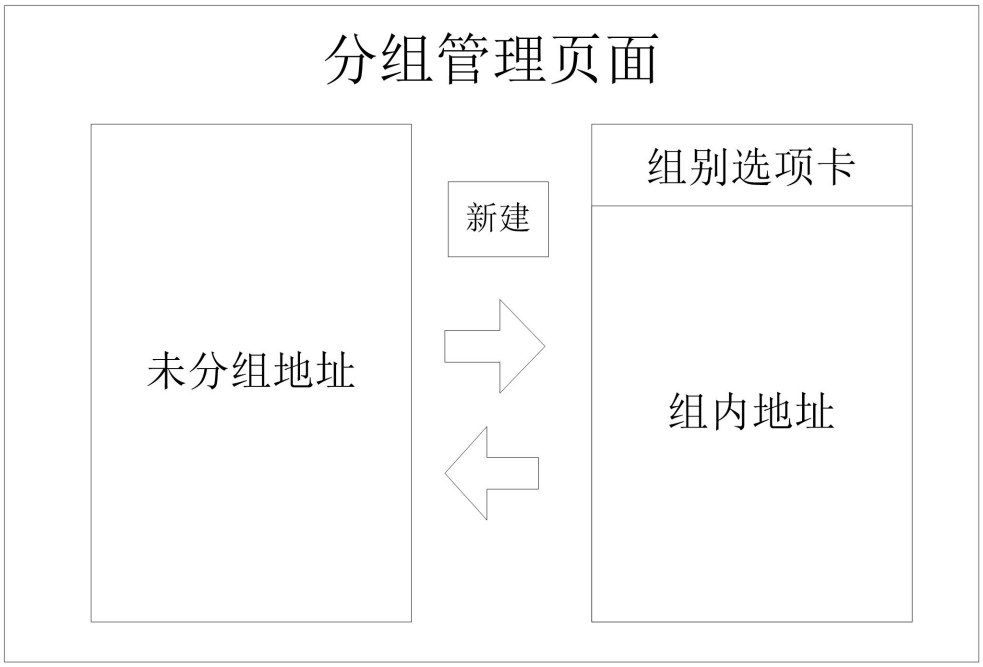
1. 页面获取用户设置的类型端口查询选择信息和查询时间范围
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上， 否则将获取的信息调用相应控件形成饼状图或者柱状图显示

2.5 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分组管理和组别数据查询 2 个子页面。

2.5.1 分组管理页面

该页面提供对局域网内用户的分组服务，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。



图表 4 分组管理页面

如图 4 所示，分组管理页面中，页面加载时自动调用用户分组查询接口（GET/group/），

获取所有的分组信息。

当用户点击组别选项卡时，页面将该组别内的所有地址以列表显示。

当用户点击左右箭头按钮时，页面获取当前左右两侧地址栏信息和组别信息，调用用户分组修改接口（ADD/group/和 DELETE/group/），如果操作成功页面刷新，否则弹出错误报告。

当用户点击新建按钮时，页面调用用户分组增加接口（NEW/group/）添加新的分组信息，后台收到请求后返回操作结果到页面显示。

2.5.2 组别数据查询

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）以及所有现有组别的多选框，当用户选定后在页面中显示相应的曲线图或柱状图。

页面加载过程如下：

1. 当用户选择要查询的信息时，页面自动调用组别数据信息查询接口（GET /groupdata/）
2. 页面形成相应的 form 表单提交给控制器
3. 控制器收到页面发来的 form 表单后解析获取用户请求
4. 控制器查询流表中是否有与用户请求一致的流表项，如果没有添加相应流表项，无法添加则返回错误信息给页面
5. 控制器周期性实时获取用户请求监控的相关信息，并将之打包发送给页面
6. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息调用相应控件形成曲线图或者饼状图显示

2.6 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。

2.6.1 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。

2.6.2 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。

页面加载过程如下：

1. 页面加载时自动调用组别数据信息查询接口（GET /alert/）获取所有报警事件信息
2. 页面形成相应的 form 表单提交给后台

3. 后台收到页面发来的 form 表单后解析获取用户请求，并将结果打包成 Json 数据包返回给页面

4. 页面接收、解析控制器返回的信息，如果是错误提示则显示在页面上，否则将获取的信息以列表形式显示

5. 当用户输入时间信息并单击查询按钮时，页面获取用户填写的信息调用查询接口（GET /alert/）获取相关事件并重复步骤 2

2.7 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数据层 addLogger 方法保存到操作日志表中。当加载该页面时，调用（GET /loggers/）接口，通过 getLoggers 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。

页面同时提供搜索框，用户可以通过输入相关信息的方式提交表单，后台调用（GET /loggers/）接口获取相关信息返回，实现用户的感兴趣的信息查询。

只有系统管理员才能够浏览所有用户的操作信息，其他用户只能查看自己的操作记录。

3. 流表设计

Flow 管理是本系统的核心模块，它负责汇总用户提交的请求，结合自身算法策略，统一部署流表、Meter 表，并能根据网络负载变化动态调度流量。

流表的存储由源 IP、目的 IP、源 MAC、目的 MAC 和类型端口 5 部分确定和组成，因此网络中流表项将会大大超过流表容量，为了保证统计信息尽量准确，采取动态的流表管理方式。

3.1 动态流管理方法

流表的数量是有限的，为了保证流量大的 IP 能够保持持续被统计，同时流表本身又有能力处理所有的其他流信息，因此要对流表进行动态管理。管理的目标是数据包多的 IP 流表项尽可能被保存下来，而流量少的流表项因末尾淘汰而被数据包更多的流表项替代。

流表规模管理规则如下：

1. 流表项数未达到存储总量的 100%时，新的流表项到达后直接被添加进流表
2. 流表项数达到存储总量的 80%时，控制器自动开启流表动态管理功能
3. 在流表动态管理过程中，每过一个周期 T，控制器对流表内流表项数据量大小进行排序，将当前没有流量的数据量最少的 20%流表项删除
4. 当存储总量达到 100%时，新到达的流将被舍弃直至流表项出现空余

3.2 周期 T 的选择

周期 T 是控制器中写定的对流表进行缩减的周期时间，如果 T 取得太大将导致流表太容

易溢出而损失流表统计数据，如果 T 取得太小又会导致控制器频繁地修改流表大大降低系统效率。在当前设计文档中暂定 T 为 5 分钟，视编写完成后具体情况再做相应调整。

3.3 流表更新依据

为了保证软件效率，控制器必须在进入流表动态管理状态后尽快确定要删减的流表项有哪些，根据流表更新规则，当前无流量的通信量最少的 20%流表项被删除，对应操作流程如下：

1. 对历史流量表中的各项以通信数据包数大小由小到大进行排序
2. 顺序对排序后的各项进行检测
3. 如果被删除的项不到 20%且当前检测项当前在实时流量表中流量为 0，则在流表中删除该项
4. 当删除的项达到 20%或者所有数据项都检查完毕后返回。

4. 数据库表设计

系统使用数据库管理存储信息，所有的流信息以源 IP、源 mac、目的 IP、目的 mac 和类型端口号信息作为标识符，当五者全部匹配时才可确认是一个流。数据库设计如下：

4.1 总数据表管理

控制器从 OF 交换机获取的每一条统计信息都将写入总数据表，总数据表存储最近一周内的所有数据，每天自动清除一周前的数据，该表只用做数据存储和提供数据分析的依据，本身不做任何处理。该表格每日凌晨 0 点自动清楚 7 日之前的数据。

该表的数据添加在 ODL 端完成，自动清除维护又数据库工程完成。

数据库存储表项如下，表名 All_data。

字段名	类型	描述	说明
SIP	String	主键	源 IP
DIP	String	主键	目的 IP
SMAC	String	主键	源 mac
DMAC	String	主键	目的 mac
Type	String	主键	数据包类型
Port	int	主键	端口号
Time	String	主键	数据上报时间
Count	int		数据包数
Default	char		备用字段

表格 3　总数据表

4.2　分数据表管理

为了提高系统的相应速度，降低数据处理延迟，系统会每天的进行总数据表数据的维护，将总数据表中的信息进行汇总和处理，分别存储在不同的表里，以满足系统的各项服务需求。

对各个流的相关信息进行的统计和存储在不同粒度的流统计表中完成，针对不同的统计项以及时间粒度分别建立相应的存储表用于存储访问和被访问的相关统计数据。

不同的表中主键依据要统计的对象进行存储，下表中带星号的字段一个表中只存在一个（带双星号的作为一个对象）。表名命名方式为：<统计对象>_<方向>_<时间粒度>，如 IPv4

的对外访问一天统计表名为 IPv4_out_day。

字段名	类型	描述	说明
SIP*	String	主键	源 IP
DIP*	String	主键	目的 IP
SMAC*	String	主键	源 mac
DMAC*	String	主键	目的 mac
Type**	String	主键	数据包类型
Port**	int	主键	端口号
Count	int		总数据包数
Default	char		备用字段

表格 4　数据存储数据表

相应的，还有实时数据表、用户管理表、报警信息存储表和系统日志统计表。

因为实时统计不是对五元组的实时统计，而是对用户的查询进行的统计反馈信息，因此应建立对应的实时统计数据表来便于服务提供和管理。表名 Realtime_data。

字段名	类型	描述	说明
SIP	String	主键	源 IP
DIP	String	主键	目的 IP
SMAC	String	主键	源 mac
DMAC	String	主键	目的 mac
Type	String	主键	数据包类型

Port	int	主键	端口号
Time	String	主键	数据上报时间
Count	int		数据包数
Default	char		备用字段

表格 5　实时数据表

用户数据表存储用户相关信息，表名 User_list。

字段名	类型	描述	说明
ID	String	主键	用户编号
Name	String		用户名
Code	String		密码
Type	int		权限
LastTime	String		上次登录时间
ThisTime	String		本次登录时间
Default	char		备用字段

表格 6　用户信息表

分组功能服务由分组信息表提供技术支持，表名 Group_list。

字段名	类型	描述	说明
MAC	String	主键	主机地址
Name	String		主机名
Group	int		组别编号

Gname	String		组别名称
Default	char		备用字段

表格 7　分组信息表

报警信息表存储当前系统要监控和报警的信息，表名 Warning_list。

字段名	类型	描述	说明
ID	String	主键	建立报警监测的用户
SIP	String		源 IP
DIP	String		目的 IP
SMAC	String		源 mac
DMAC	String		目的 mac
Type	String		数据包类型
Port	int		端口号
Time	String	主键	监测开始时间
Count	int		阈值数据包数
Default	char		备用字段

表格 8　报警信息存储表

系统日志表名为 System_log。

字段名	类型	描述	说明
ID	String	主键	用户
Name	String		用户名

Time	String	主键	事件发生时间
Event	String		事件代码
Default1	String		参数字段 1
Default2	String		参数字段 2
Default3	String		参数字段 3

表格 9　系统日志表

4.3　历史数据存储和获取

由 xml 文件维护和管理。