网络与应用课程设计

一、课设说明

1.1 课程信息

本次课程设计面向北京邮电大学信息与通信工程学院的《计算机网络》 《软件定义网络》两门课程，课设的目的是让同学学会创建真实的网络环境，实践当前网络技术，并初步了解软件定义网络这个网络新技术方向。

课程内容包含基础题和提高题两部分。其中，**基础实验（必修）两道题由学生独立完成，进阶实验（选修）选 2 题即可，进阶实验允许组队完成，队员不超过 6 人**。

1.2 实施方案

本次课设在第三方实验平台上进行，由于实验平台无法满足所有人同时实验，本次课设实验**分两批次进行**：

第一批：2019 课设信息统计表中前 12 组，总共 64 人。**时间为 5.27——7.17（6.8——6.15 期间不能登陆实验平台做实验）。**

第二批：表格中剩下 14 组，总共 63 人。**时间为 7.17——8.31。**

实验过程遇到资源不够的情况，可以先释放之前的实验资源，然后再创建实验，或者小组内部资源调节一下。学生完成所有实验后不需要立即删除实验，可以由后台统一释放。

Linux 以及 SDN 基础比较好的同学，也可以在自己的电脑上搭建环境进行实验，但是要求在实验报告中一定要写明软件环境搭建的过程。

1.3 课设要求

实验报告以小组形式统一提交，将在第二批实验结束后统一收报告，每人一份报告文档，并附上小组成员分工的百分比表格，名称为“**学号-姓名-指导老师**”。基础实验和进阶实验报告提交内容见各实验的“实验要求”。学生尽量将课程设计的操作步骤写的详细一点，每一个步骤附上操作的指令，以及执行结果的截图，相关软件安装的步骤也尽量写一下，也可参考群里上传的《实验教程文档模板.docx》。课设评分将按照实验完成程度，实验结果，以及步骤的详细程度来进行。

所有实验中安装的 mininet 版本最好统一为 2.2.1。

在实验开始前，用户首先访问实验平台首页：http://bupt.51openlab.com。根据表格中的用户名密码登陆之后，点击上方项目案例，点击相应的实验项目即可开始创建实验。群里会先上传第一批同学的账号密码，等第一批实验结束之后再发布第二批同学的账号密码，登陆之后可以根据自己需求改一下密码。

1.4 联系方式

目前实验平台依旧在优化当中，若出现平台使用问题请等待一段时间后再重开，或与助教联系。课设的联系人为：

周宇柯（助教）：bupt_zyk@163.com

曾诗钦（助教）：469265284@qq.com

黄韬老师：htao@bupt.edu.cn

刘江老师：liujiang@bupt.edu.cn

如有问题可以通过课设的 qq 群反映：240798963

二、基础题（必修）

2.1 实验一　TCP 三次握手实验

TCP 协议是面向连接的、端到端的可靠传输协议，它支持多种网络应用程序。TCP 必须解决可靠性，流量控制的问题，能够为上层应用程序提供多个接口，同时为多个应用程序提供数据，TCP 也必须能够解决通信安全性的问题。同时，有多种网络工具可以测试网络性能，比较常用的有 iperf 和 Netperf 两种网络检测工具，可以用于检测网络吞吐量。

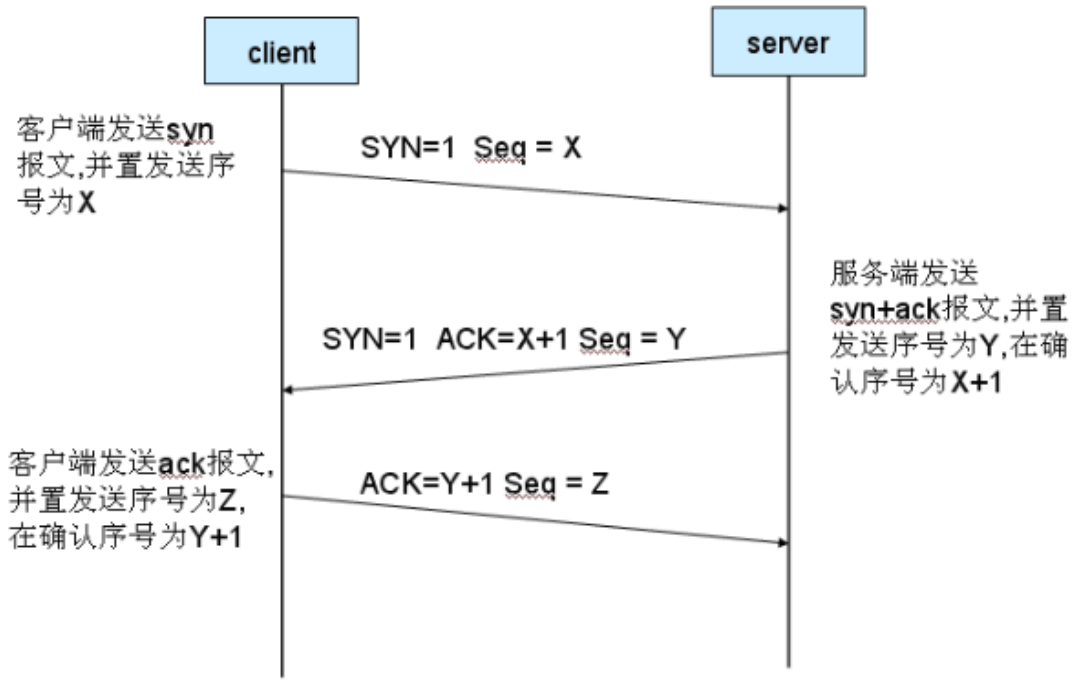
2.1.1 实验目的

- 掌握 TCP 协议建立连接的工作原理；
- 理解 TCP 会话的概念；
- 掌握 TCP 协议的建立连接的过程；
- 掌握常用的网络性能检测工具；

2.1.2 实验原理

TCP 协议属于可靠的、面向连接（利用三次握手）的全双工协议，它在两台设备之间真正传输数据前会交换握手控制信息 。TCP 协议使用称为三段式握手的方式来建立传输。三次握手即对每次发送的数据量是怎样跟踪进行协商使数据段的发送和接收同步，根据所接收到的数据量而确定的数据确认数及数据发送、接收完毕后何时撤消联系，并建立虚连接。为了提供可靠的传送，TCP 在发送新的数据之前，以特定的顺序将数据包的序号，并需要这些包传送给目标机之后的确认消息。

三次握手示意图如下：



TCP 三次握手示意图

iPerf 是一种网络性能测试工具，可以运行于 Linux、BSD、Unix 及 Windows 等操作系统。iPerf 具有多种参数和特性，支持协议、定时、缓冲区等参数的配置调整，能够测试 TCP/UDP 最大带宽、延迟抖动、数据包丢失等统计信息，可以根据需求采用不同的参数从而达到不同的测试目的。

Netperf 是一种网络性能测量工具，主要用于测试 TCP 或 UDP 和 Berkeley 套接字接口的批量数据传输（bulkdatatransfer）和请求/应答（request/reponse）性能。

2.1.3 实验任务

1. 通过访问网站来让主机与网站服务器之间建立 TCP 连接，同时通过抓包分析 TCP 三次握手的建立连接过程，让用户对传输层有更深的认识；
2. 使用 iPerf 测试 SDN 网络的性能，熟悉 iPerf 常用的测试命令；
3. 使用 Netperf 测试 SDN 网络的性能，并且总结 Netperf 与 iPerf 的不同之处；

2.1.4 实验报告要求

1. Wireshark 抓取 TCP 数据包的流程截图；
2. TCP 三次握手过程中产生的数据包的主要字段的截图（至少三张），三次握手过程详细分析报告；
3. iPerf 网络性能测试截图（TCP 和 UDP 至少各一张）；
4. Netperf 网络性能测试截图（TCP 和 UDP 至少各一张）；

2.2 实验二　SDN 路由转发应用开发

2.2.1 实验目的

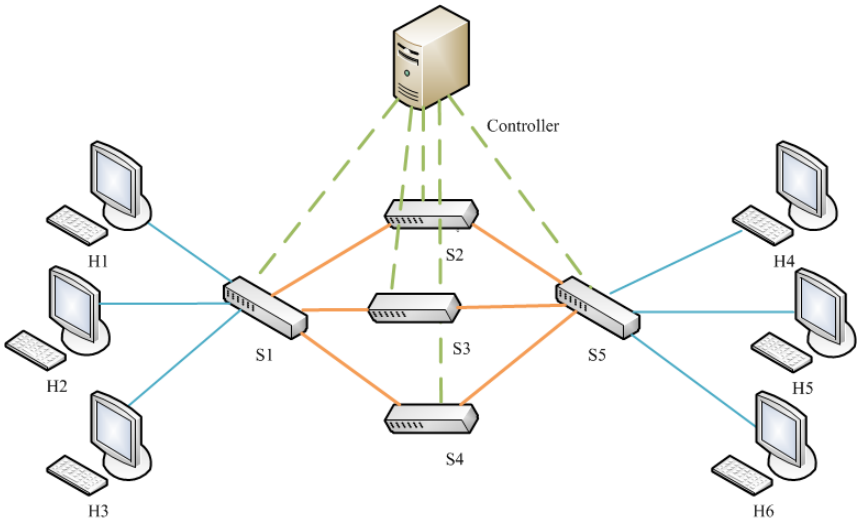
- 掌握 Mininet 的一些基本操作；
- 熟悉 SDN 中的 OpenFlow 协议；
- 理解 SDN 的基本架构；
- 熟悉简单的控制器应用的开发；

2.2.2 实验原理

利用 Mininet 可以构建自己想要的拓扑网络结构，然后和自己要用的控制器相连接，实现一个 SDN 网络，同时通过 openflow 协议下发流表实现网络可达。通过控制器北向 API 开发控制器应用程序，可以实现搭建网络拓扑、修改路由规则等功能。

2.2.3 实验任务

基于北向 API 开发一个简单的路由控制应用，实现动态转发路径规则设置。



1、利用 mininet 部署如图所示拓扑的网络环境。

2、利用北向 API 在控制器上开发路由控制程序，使得在该环境下，假设 H1 ping H4，初始的路由规则是 S1-S2-S5，30 秒后，路由转发规则变为 S1-S3-S5，再过 30 秒，规则变为 S1-S4-S5，然后再回到最初的转发规则 S1-S2-S5。通过这个循环调度的例子动态地改变交换机的转发规则。

3、在完成 2 的基础上，额外开发简单验证程序，使得为程序输入源 IP 地址和目的 IP 地址时，能够根据当前的流表信息分析出传输路径，并输出路径结果。

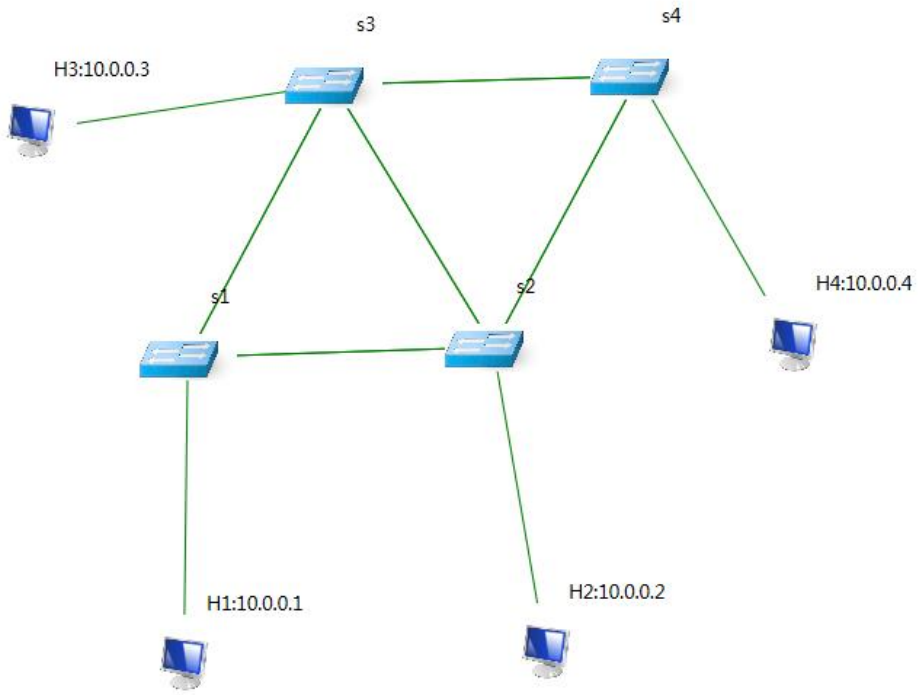
2.2.4 实验要求

1、给出具体的网络拓扑视图截图，并将对应于图中的节点名称标明在图中；
2、给出两步程序的代码；
3、给出程序运行后的结果截图；

三 进阶题（五选二）

3.1 环路广播风暴实验

用 mininet 搭建一个有环网络（网络拓扑可以参考下图），使用 ryu 或者 onos 或者 odl 或者 floodlight 等等控制器中的一种作为 sdn 控制器，实现网络中可以互相通信，避免环路带来的环路风暴或者其他影响。



3.1.1 实验目的

- 掌握 mininet 构建网络 topo 结构图；
- 了解环路风暴的相关知识；
- 熟悉控制器开发 app 的架构与流程；
- 对于 sdn 开发能够有一个大体上的认知，并且能够自己开发一个简单的 app；

3.1.2 实验原理

在传统网络中，存在着一定的广播流量，占据了一部分的网络带宽。同时，在有环的拓扑中，如果不运行某些协议，广播数据还会引起网络风暴，使网络瘫痪，传统解决方案是使用 stp 协议，在 sdn 上则可以采用 ARP 代理请求回复解决环装拓扑风暴的问题。

3.1.3 实验任务

通过本实验来熟悉 mininet 和 sdn 控制器的一些基本操作，以及知道 sdn 控制器中的一些字段及结构，同时通过这个程序的开发来深入理解环状网络风暴的问题，通过上网查阅相关资料和一些自己的操作对于这个问题相信会有更加深入的理解。

通过 mininet 利用 python 语言编写一个 topo 文件或者是利用有界面的 gui 界面构建拓扑。

开发控制器的 app 处理环路风暴的问题，这个问题可以分为几个步骤，从交换机接收到不能匹配的包将消息 packetin 给控制器时，此时有一个学习的过程，而这个过程就会存在广播风暴的问题，此时就需要通过一些手段想办法把环路给封锁掉，然后再进行决策下发流表，具体的实现方式亦是可以去网上查阅相关控制器的开发文档，利用最基本的转发包的 app 去改写实现阻止环路广播的方法。

3.1.4 实验要求

1. mininet 构建的 py 文件截图一张；
2. 控制器开发的代码截图一张；
3. mininet 的主机之间互 ping 的截图一张；
4. 控制器后台信息一张（若没有写明即可）；
5. 前端网络的 topo 结构图一张；

3.2 恶意网站防护

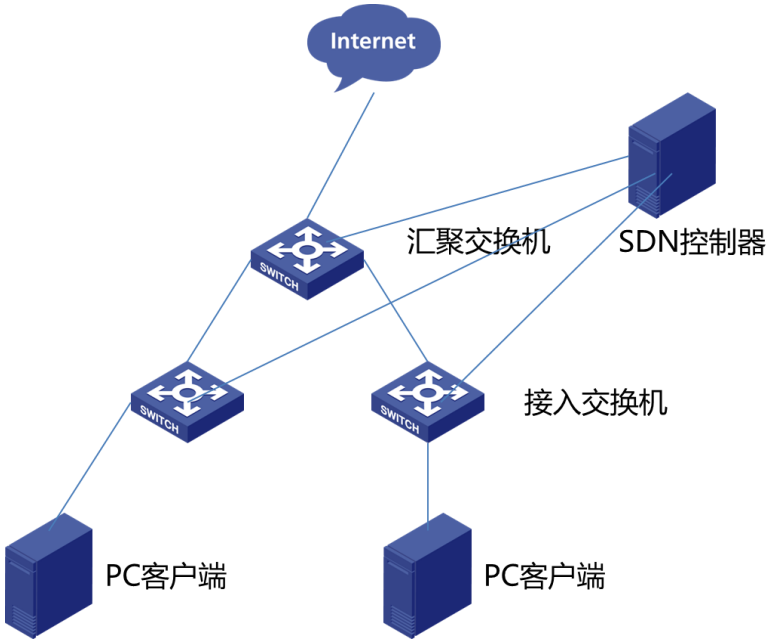
3.2.1 实验目的

互联网中存在恶意网站，严重威胁正常上网，例如：www.1cbc.com，仿冒 www.icbc.com，如果访问可能被套取网银密码，造成资金损失，如何有效进行恶意网站防护非常有意义。

3.2.2 实验原理

传统恶意网站防护一般采用在 PC 客户端上安装杀毒软件或安全浏览器，或者在网络出口端安装流量审计软件，客户端安装软件可能不是所有用户都会安装或使用，网络出口流量审计一般是事后审计，可能用户已经造成了损失，本题目要求利用 SDN 技术设计一种不需

要在客户端安装特定软件，且能够事前防护，即在用户访问恶意网站前进行阻止，防止用户数据传输到恶意网站。可以采用两层网络架构的园区网模型：接入+汇聚设备，接入设备接入 PC，汇聚设备接入 Internet，可以假设某正常网站（例如 www.baidu.com）为恶意网站，这样通过 SDN 技术使得 PC 无法访问该假设恶意网站，而能够访问其他网站。



3.2.3 实验内容

1. 在提交的方案中需要给出实验的网络拓扑，并给出主要核心的操作步骤。对技术实现及其可行性需要作一定的论证，能给出理论分析、仿真结果等论据材料则更佳。

2. 报告文档中的必备内容：设计方案、实现方法、网络拓扑、验证实验设计。报告中的可选内容：实验结果或仿真结果、理论分析、实验数据、其他补充材料。

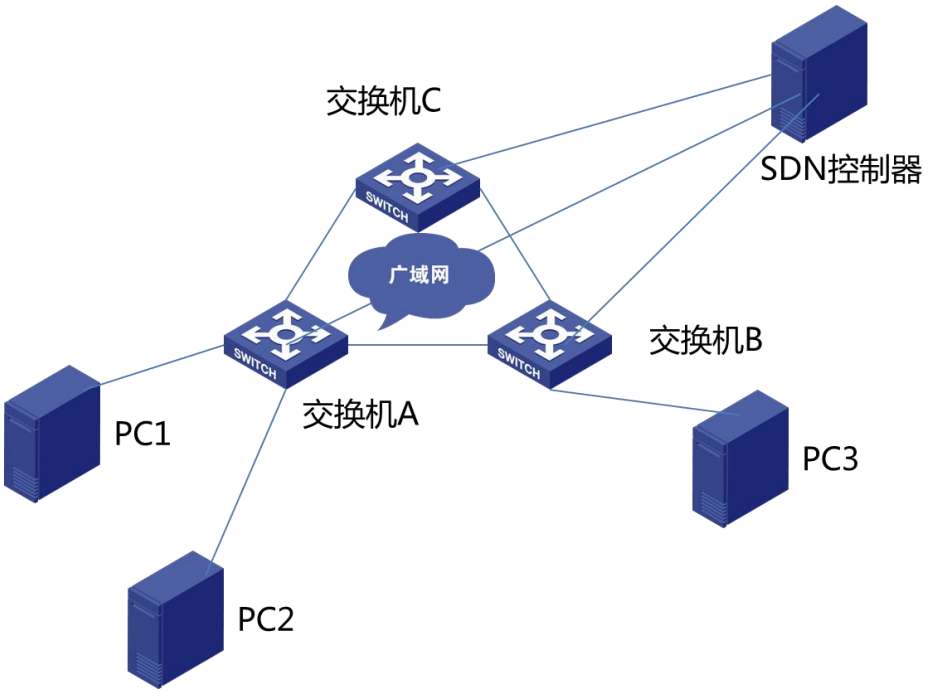
3.3 骨干网/广域网流量工程

3.3.1 实验目的

数据中心之间大量流量通过骨干网/广域网进行互连，由于通信数据的不确定性，一般会为流量可能的峰值做为最高带宽来进行建设，这就带来平时带宽利用率比较低的问题，为了保证数据中心之间传输数据的业务不受影响，骨干网/广域网带宽利用率一般只有 30%左右。分析其原因，主要是传统路由协议只是按照最短路径进行流量路由与转发，当最短路径流量已经满负荷时仍然将新的流量导入，而不会进行分流操作，所以会导致过载的链路无法正常服务，迫使用户不得不进行网络改造与升级。

3.3.2 实验内容

对骨干网/广域网上通信的流量进行分级处理，高优先级流量走最短路径，低优先级流量视最短路径负载动态选择路径，当负载没有超过阈值时同样选择最短路径，当负载超过阈值时选择非最短路径。可以如下组网，模拟三个数据中心之间的互联。PC1 访问 PC3 的流量定义为高优先级，PC2 访问 PC3 定义为低优先级。交换机 A－B 为最短路径，交换机 A-C-B 为非最短路径。



3.3.3 实验要求

1. 在提交的方案中需要给出实验的网络拓扑，并给出主要核心的操作步骤。对技术实现及其可行性需要作一定的论证，能给出理论分析、仿真结果等论据材料则更佳。

2. 报告文档中的必备内容：设计方案、实现方法、网络拓扑、验证实验设计。报告中的可选内容：实验结果或仿真结果、理论分析、实验数据、其他补充材料。

3.4 流量负载均衡调度

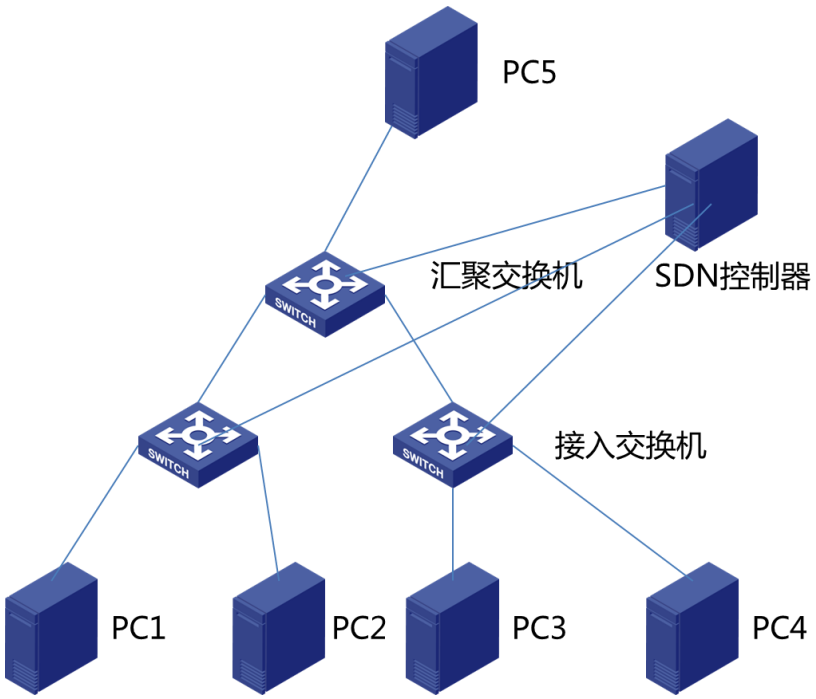
3.4.1 实验背景

数据中心在用户访问量超过单台服务器服务能力时，一般通过增加相同功能的服务器来满足海量用户的访问需求，在这种场景下如何将大量用户的访问流量分担到不同的服务器上成为决定整体业务服务质量的重要指标。目前业界一般采用商用的负载均衡设备或 LVS 等

开源软件来实现。

3.4.2 实验任务

数据中心多台服务器提供相同业务，通过 SDN 网络对访问该业务的流量进行负载均衡，保证每台提供该业务的服务器（或虚拟机）的负载大致相同（或者根据不同服务器的性能等因素进行加权分配）。可以采用如下数据中心组网，其中 PC1 到 PC4 模拟 WEB 服务器，向外提供相同的 WEB 服务（静态 HTML 访问即可），在 PC5 上模拟大量用户访问 WEB 服务。



3.4.3 实验要求

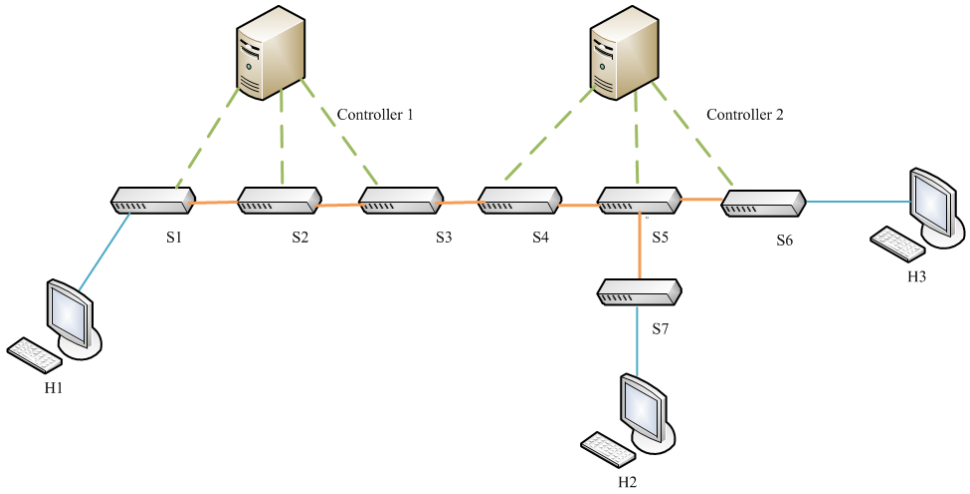
1. 在提交的方案中需要给出实验的网络拓扑，并给出主要核心的操作步骤。对技术实现及其可行性需要作一定的论证，能给出理论分析、仿真结果等论据材料则更佳。

2. 报告文档中的必备内容：设计方案、实现方法、网络拓扑、验证实验设计。报告中的可选内容：实验结果或仿真结果、理论分析、实验数据、其他补充材料。

3.5 基于 LLDP 和 OpenFlow 的网络拓扑检测内容

3.5.1 实验内容

网络拓扑检测对于网络策略的执行十分重要，本题主要考察对拓扑检测原理的理解以及对全局拓扑的检测。



3.5.2 实验要求

1、南向接口采用 OpenFlow 协议；
2、部署如图所示拓扑的网络环境；
3、分析控制器的拓扑发现机制；

3.5.3 实验报告要求

1、搭建上述网络环境，并附加控制器 web 界面拓扑截图，分析搭建上述网络环境中采用的控制器网络拓扑检测原理（例如：LLDP）；
2、在上述网络环境中，给出一种全局拓扑检测方案，用简洁的流程图描述检测拓扑的过程，给出全局拓扑结构化数据。