**大作业事项**

1. 分数占比

大作业分数占期末总评的30%。大作业内分数分为基础分+附加分两部分，基础分占比75%，附加分占比25%。

1. 开展形式

同学们自由组队，推荐为3-4人每组。本次大作业共10个题目，每个题目供2个组选择，选题链接模板：<https://kdocs.cn/l/cq4tC30lKlYk> ，16周课上poster展示，现场打分。

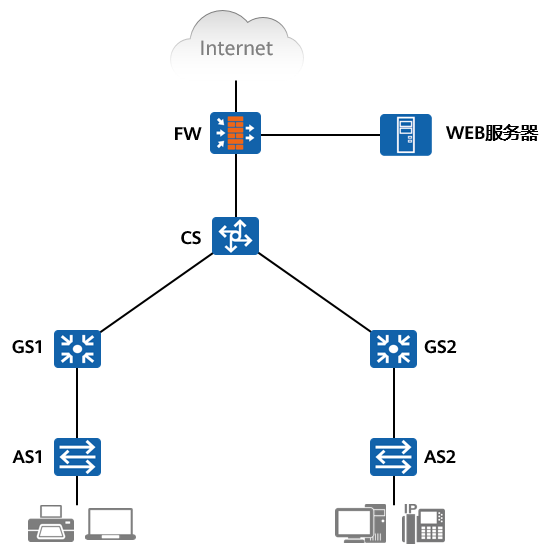
1. 提交内容

主要分为两部分。

1. 项目海报。参照给出的学术会议poster形式，总结自己组的工作内容，制作一份海报。
2. 一份提交文件，包括项目报告文档，代码，以及可能有的演示材料，如截图、视频等。

# IPv6在园区网络中的方案设计

课题描述



在如图所示的组网中，AS1、AS2为接入层交换机，GS1、GS2为汇聚层交换机，CS为核心层交换机，FW为出口防火墙。AS1、AS2连接着终端设备，GS1、GS2充当终端设备的网关设备，FW连接着园区网络与Internet，并连接WEB服务器，该服务器用于对Internet用户提供服务。

用于针对网络提出了如下要求，请给出相应的方案设计，详细描述方案的原理、设计意图以及该方案如何满足用户需求。

基本要求：

1. 要求AS1及AS2下联的终端之间能够相互通信，使用动态路由协议完成路由信息通告，最终实现终端之间的数据互通。
2. 在防火墙上分别完成适当的安全区域规划，使得园区网络内部不受来自Internet的网络攻击；通过适当防火墙技术允许来自Internet的用户访问WEB服务器的HTTP服务（TCP8080端口）。
3. AS1下联的部分终端支持DHCPv6，用户希望通过该方式实现终端地址自动配置，并且计划将DHCPv6服务器旁路连接在CS上，那么为了实现终端的地址自动获取，网络中还需要考虑什么技术点？
4. AS2下联的部分终端不支持DHCPv6，并且这部分终端数量较多，用户表示无需对终端的地址进行强管理，并且希望通过自动化的方式实现终端地址自动配置，请给出建议方案。

高级要求：使用华为eNSP网络模拟器模拟并展示你的方案设计

参考资料

* S5700, S6700系列以太网交换机 产品文档

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&lang=zh&idPath=24030814%7C21782164%7C21782167%7C22318564%7C6691579>

重点参考本文档中的如下章节（主要查阅文档中关于技术原理部分的描述）：

* + OSPFv3章节：

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_TASK_0177105218&lang=zh>

* + DHCPv6章节：

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_TASK_0176372350&lang=zh>

* + DHCPv6 Snoping章节：<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_CONCEPT_0176367279&lang=zh>
  + IPv6基础配置章节：

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_TASK_0177104314&lang=zh>

* + ND Snooping章节：

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_CONCEPT_0176370423&lang=zh>

* HiSecEngine USG6000F 产品文档

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100231714&lang=zh&idPath=24030814%7C9856724%7C21430823%7C253423179%7C22914752>

重点参考本文档中的如下章节（主要查阅文档中关于技术原理部分的描述）：

* + 安全区域原理描述

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100231714&id=ZH-CN_CONCEPT_0000001125008874&lang=zh>

* + 安全策略

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100231714&id=ZH-CN_TASK_0000001125007228&lang=zh>

* + NAT与IPv6过渡技术

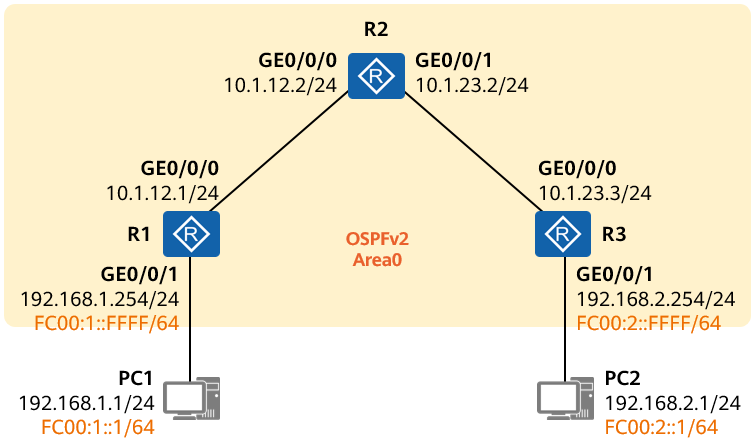
<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100231714&id=ZH-CN_TOPIC_0000001125010674&lang=zh>

* 华为eNSP网络模拟器安装详细教程（2024）

<https://bbs.huaweicloud.com/blogs/422935>

# IPv6网络过渡方案设计

课题描述



如上图所示，用户通过R1、R2及R3构建了一个简单的路由器组网，其中R1及R3分别接入了一些终端，当前整个网络是纯IPv4的网络，但是PC与网络设备都支持IPv6功能，现在用户需要在PC1及PC2上部署一些软件应用，并且计划使用IPv6实现应用信息交互。

1. 演进初期：不对网络的IPv4部分进行变更，确保IPv4流量的正常传输。
2. 演进中期：PC1和PC2之间的IPv4和IPv6流量交互都能同时正常进行，网络部分逐步变为纯IPv6网络，PC1与PC2之间IPv6业务逐渐成熟。
3. 演进后期：将终端的IPv4地址删除，整网平滑地演进到纯IPv6状态，终端PC之间的IPv6流量能够直接在网络中进行转发。

基本要求：请给出一套可供用户分期执行的IPv6网络演进方案，并描述方案设计的原则以及涉及的关键技术。

高级要求：使用华为eNSP网络模拟器模拟并展示你的方案设计

参考资料

* AR系列接入路由器产品文档

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=AR_Series_Access_Routers_ARM>

重点参考本文档中的如下章节（主要查阅文档中关于技术原理部分的描述）：

* + IPv6 over IPv4隧道

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_ipv6tunnel_cfg_0001>

* + OSPFv3

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_cfg_ospfv3_0000>

* OSPF（OSPFv2）

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_cfg_ospf_0000>

* 华为eNSP网络模拟器安装详细教程（2024）

<https://bbs.huaweicloud.com/blogs/422935>

# IPv6网络路由策略设计

课题描述

在如图所示的网络中，R3是一台边缘路由器，它连接着终端PC所在网段，并上联出口路由器R1及R2，R1、R2及R3运行着OSPFv3动态路由协议。

SW1、SW2及SW3构成一个小型数据中心网络，其中SW1及SW2是核心交换机，SW3是服务器接入交换机，SW1、SW2并不运行任何动态路由协议。上述三台交换机构成了一个二层冗余环境。

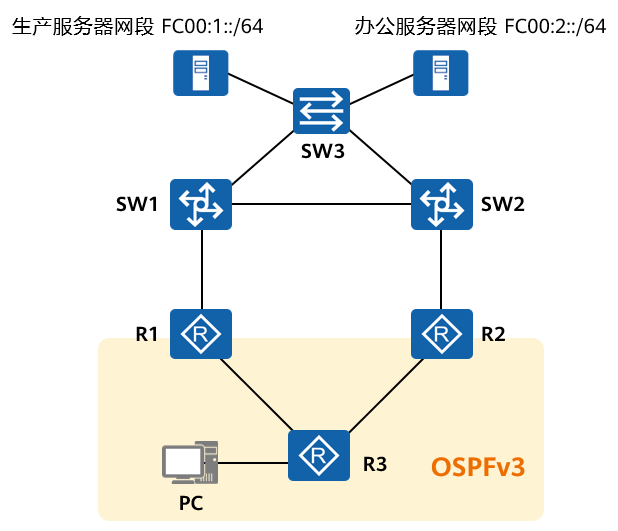
现在，用户要求对网络进行设计，使得当网络正常时，PC访问生产服务器网段的去向流量通过R3-R1-SW1-SW3这段路径进行转发；PC访问办公服务器网段的去向流量则通过R3-R2-SW2-SW3这段路径进行转发。当R1或SW1发生故障时，PC访问生产服务器网段的去向流量可自动切换至R3-R2-SW2-SW3这条路径，同理，当R2或SW2发生故障时，PC访问办公网段服务器的流量则自动切换至R3-R1-SW1-SW3这条路径。针对上述情况，要求PC均可正常与生产服务器及办公服务器通信。

基本要求：

请给出方案设计，包括R1、R2及R3路由器上的网络技术方案，以及SW1、SW2及SW3上的网络技术方案，设计覆盖整网的流量引导策略、流量切换保护策略，分析当网络发生以上提及的故障时，所使用的方案是如何保证数据流量按照用户需求进行转发。

高级要求：

使用华为eNSP网络模拟器模拟并展示你的方案设计



参考资料

* AR系列接入路由器产品文档

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=AR_Series_Access_Routers_ARM>

重点参考本文档中的如下章节（主要查阅文档中关于技术原理部分的描述）：

* + 静态路由

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_cfg_static-route_0000>

* + OSPFv3

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_cfg_ospfv3_0000>

* + 路由策略

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100007338&id=dc_cfg_route-policy_0000>

* S5700, S6700系列以太网交换机 产品文档

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&lang=zh&idPath=24030814%7C21782164%7C21782167%7C22318564%7C6691579>

重点参考本文档中的如下章节（主要查阅文档中关于技术原理部分的描述）：

* + MSTP

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_TASK_0177103197&lang=zh>

* + VRRP

<https://support.huawei.com/hedex/hdx.do?docid=EDOC1100247312&id=ZH-CN_CONCEPT_0177109806&lang=zh>

* 华为eNSP网络模拟器安装详细教程（2024）

<https://bbs.huaweicloud.com/blogs/422935>

# 综述IPv6+技术体系

课题描述

2021年，我国颁布《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》，着力解决关键问题，深化部署加速推进IPv6规模部署和应用；《通知》从政策驱动转向应用需求驱动，鼓励开展“IPv6＋”产业创新引领全球发展方向，要求到2025年末，全面建成领先的IPv6技术、产业、设施、应用和安全体系，我国IPv6网络规模、用户规模、流量规模位居世界第一位，成为全球“IPv6＋”技术和产业创新重要推动力量。

基本要求：请综述IPv6+的技术体系创新，概述其中的关键技术，例如分段路由SRv6、业务随流检测iFIT、网络切片、新型组播BIERv6等的技术创新、产业应用、技术价值。

高级要求：SRv6工作模式分为两种：SRv6 BE和SRv6 TE Policy，请分析介绍两者的差异。

其他要求：正文页数为8-10页，英文写作要求字体为Times New Roman；中文写作要求字体为宋体。字号为小四，行距为1.2倍。页边距选择“适中”。引用采用尾注形式。 报告末尾需附有各位组员明确的贡献度，由组员之间讨论决定。

参考资料

1. 什么是IPv6+？

<https://info.support.huawei.com/info-finder/encyclopedia/zh/IPv6---.html>

1. 什么是SRv6？

<https://info.support.huawei.com/info-finder/encyclopedia/zh/SRv6.html>

1. 什么是iFIT？

<https://info.support.huawei.com/info-finder/encyclopedia/zh/IFIT.html>

1. 什么是BIERv6？

<https://info.support.huawei.com/info-finder/encyclopedia/zh/detail?action=queryEntityDetail&keyword=BIERv6>

1. IP新技术基础

<https://info.support.huawei.com/network/ptmngsys/Web/OnlineCourse_NE/zh/mooc_IPV6.html>

1. IPv6+ A New Era of IP Networks for 5G and Cloud

<https://www.ipv6plus.net/>

1. IP网络系列丛书

<https://e.huawei.com/cn/solutions/enterprise-networks/ip-ebook>

# 基于socket的聊天软件实现

课题描述

在这个实验中，我们将实现一个即时聊天软件。

Socket网络编程原理：以 TCP 服务器为例说明， UDP 服务器略有不同。客户端也是如此。

服务器：服务器先创建一个套接字（Socket），并将该套接字和特定端口绑定，然后服务器开始在此套接字上监听，直到收到一个客户端的连接请求，然后服务器与客户端建立连接，连接成功后和该客户端进行通信（相互接收和发送数据），进行用户信息验证，并返回验证信息。最后，服务器和客户端断开连接，继续在端口上监听。

客户端：客户端创建一个套接字，里面包含了服务器的地址和端口号，客户端的端口号由系统自动分配，不需要指明。和服务器建立连接，如果连接成功则Socket创建成功。然后客户端发送用户名和密码，等待验证。通信结束后主动断开连接，释放资源。

基本要求：

1.在这个聊天软件中，不限具体的通信模式，可以是单纯的客户机/服务器（C/S）模式，也可以是混合 C/S 和 P2P 模式； 具体协议不限，可以是基于 TCP 的实现，也可以是混合 TCP 和 UDP 协议的实现。需要实现的基本功能包括①验证用户登录②两用户之间的文字聊天③用户之间的文件传输，包括二进制的大文件(比如100MB)。

高级要求：

2.除了基本要求外，你可以为你的软件加入①支持NAT穿透②离线文件和断点续传的支持③语音或视频聊天。此实验较为开放，你可以向你的聊天软件中加入一切你想加入的功能，来丰富你的软件。

# 流式存储视频传输

课题描述

流式存储视频应用在我们生活中有着广泛的应用，预先录制的视频放置在服务器上，用户向这些服务器发送请求 按需观看这些视频。首先了解流式视频的原理、客户端使用的实时流协议(Real-Time Streaming Protocol, RTSP)以及服务器使用的实时传输协议(Real-Time Transfer Protocol, RTP)

基本要求：

1)实现一个流式视频的服务器和客户端，即补全相应的代码，具体待补全的类见VideoStreaming.pdf的Code模块要求

高级要求：

2)实现对当前会话信息(丢包率，视频码率等)进行统计和展示的功能；（(参考VideoStreaming.pdf→附加练习-1)）

3)优化SETUP按钮和TEARDOWN指令的处理逻辑(参考VideoStreaming.pdf→附加练习-2)或者实现DESCRIBE功能，服务器收到该请求后能返回对当前会话的描述（(参考VideoStreaming.pdf→附加练习-3），练习2或3中选其中一个即可

参考资料

VideoStreaming.pdf及相应的待补全的代码（请在canvas上进行下载）

# P2P网络拓扑结构

课题描述

P2P网络系统经过了早期的诸如Napster、Guntella、Freenet等框架的实践后，逐步形成了一种统一的设计模式： Overlay Network模型，即以物理层面的互联网为基础构建逻辑层的网络模型（也被称为第二代和第三代P2P网络）。课程中介绍的Chord模型就是三种经典P2P拓扑模型之一。

基本要求：

1)从CAN、Chord、Pastry三种经典P2P逻辑层网络拓扑模型中选择一种，深入学习其细节，包括原理思路、模型架构、负载均衡方法、路由寻址模式等。

2)通过数学推理，给出该网络模型路由寻址的时间复杂度、空间复杂度。

3)任选语言/工具，模拟复现该网络模型，实现节点加入与退出、路由寻址等基本功能。

4)在节点数目>1000的情况下，验证你复现的模型性能（各种情况下的路由寻址平均跳数）是否与原文接近。

高级要求：

5)将网络模型和路由寻址过程可视化；

6)在原有模型的基础上，在提出你的一些改进方法，可以是参数、机制改进，也可以是某（几）类特殊情况的针对性优化。在节点数目>1000的情况下，设计实验（可参考原论文），评估改进后模型的路由寻址平均跳数。

注意，因为讨论的模型只是逻辑层模型，本实验的性能关注点主要在于路由寻址跳数，不需要考虑物理网络中的通信延迟、丢包等问题，也不要求在现实网络中复现，所以即使节点数目>1000，在本地计算机串行执行也是没有压力的。

参考资料（canvas）

* Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications (Chord.pdf)
* A Scalable Content-Addressable Network (CAN.pdf)
* Pastry: Scalable, Decentralized Object Location, and Routing for Large Scale Peer-to-Peer Systems (Pastry.pdf)

# 计算机网络安全

课题描述

利用kali虚拟机、wireshark、ettercap等工具，模拟体验网络攻击，并理解攻击的原理。

基本要求：

1. ARP 攻击：

利用kali，实现简单的arp断网攻击。攻击者与被攻击者均可使用虚拟机实现，也可利用自己的物理机作为被攻击方。利用wireshark抓包，查看攻击过程并理解原理。

利用kali和ettercap等工具进行网络攻击，实现窃听图片信息，(窃听密码等攻击)。并利用 wireshark抓包，查看攻击过程并理解原理。

1. SYN泛洪(DoS)：

利用kali，实现简单的SYN泛洪攻击，并用wireshark抓包，查看并分析攻击过程，解释其中原理。

1. 尝试实现DDoS攻击，即分布式DoS攻击，一种通过使用更多IP发起的更具威胁的DoS攻击。在实验中，IP的数量只需量力而行。与你实现DoS攻击对比攻击效果。

高级要求：

1. 基于恶意请求拦截的泛洪攻击防御：若泛洪攻击来自同一IP，则只需检测出该恶意IP地址，拦截所有来自该IP的请求即可。在你的设备上模拟该过程，并评估该防御方式的针对DoS攻击有效性。若有效，验证你的DDoS攻击是否能突破该防御。
2. 尝试你了解的更多攻击方式；也可针对本实验中你使用的攻击方式，寻找其他有效的防御方式，并设计实验验证该防御方式的有效性。

注意：实验对象请选择自己的设备或是知情且同意者的设备，切勿攻击无关人员/组织。

参考资料

* [Kali官网](https://www.kali.org/)
* [kali虚拟机安装教学](https://zhuanlan.zhihu.com/p/162161429)
* [ettercap安装地址](https://www.ettercap-project.org/downloads.html)
* [ARP攻击](https://blog.csdn.net/weixin_39190897/article/details/104569308?csdn_share_tail=%7B%22type%22%3A%22blog%22%2C%22rType%22%3A%22article%22%2C%22rId%22%3A%22104569308%22%2C%22source%22%3A%22qq_52463707%22%7D&ctrtid=aihhW)
* [wireshark监听ARP攻击](https://blog.csdn.net/qq_35733751/article/details/104786319?csdn_share_tail=%7B%22type%22%3A%22blog%22%2C%22rType%22%3A%22article%22%2C%22rId%22%3A%22104786319%22%2C%22source%22%3A%22qq_52463707%22%7D&ctrtid=LRKhN)
* [SYN的DOS攻击](https://blog.csdn.net/qq_35733751/article/details/104786319?csdn_share_tail=%7B%22type%22%3A%22blog%22%2C%22rType%22%3A%22article%22%2C%22rId%22%3A%22104786319%22%2C%22source%22%3A%22qq_52463707%22%7D&ctrtid=LRKhN)

# SDN+Ryu网络控制应用

课题描述

SDN(Soft Defined Network) 将网络的控制层与转发层进行分离，对整个网络进行集中控制，从而大大简化了对网络的控制和管理，能够快速响应业务需求的变化，迅速灵活地进行部署。

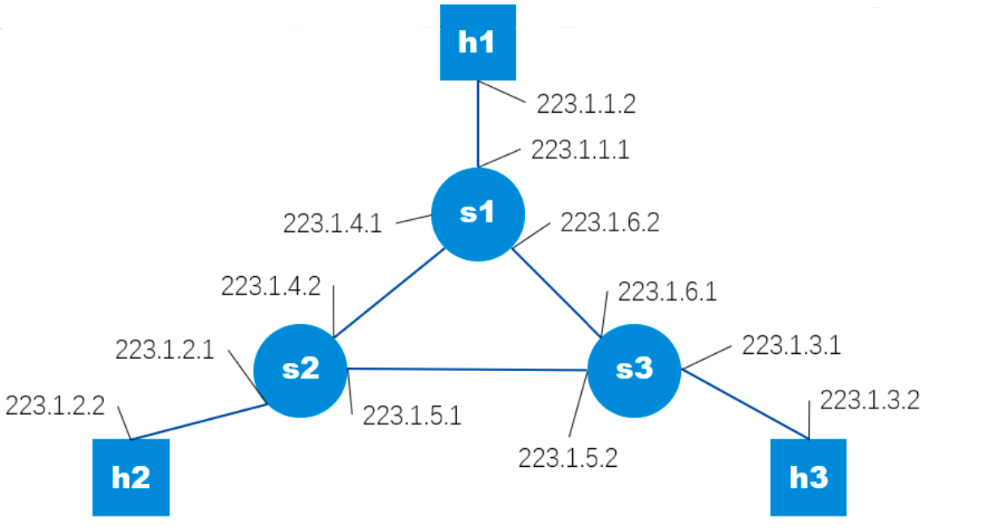
该实践需要基于mininet和ryu (基于python的SDN控制器框架) 编程实现一个SDN网络控制应用程序。

Ryu安装：

pip3 install ryu

前3个要求直接运行如下命令来启动SDN控制器

ryu-magager ryu.app.rest\_router ryu.app.ofctl\_rest ryu.app.rest\_topology ryu.app.ws\_topology --observe-links

运行 python3 net\_start.py 启动如上图的网络拓扑结构

基本要求：

1. 通过SDN控制器北向API，使用LS算法，实现静态路由选择功能，并为给定拓补图上的交换机更新流表信息。
2. 在第一问的基础上，实现动态更新流表功能，要求在第一问给定拓补图中，若链路状态发生改变时，可以动 态更新流表信息。(可以尝试使用link s1 s2 down指令断开交换机s1和s2的链接)
3. 在第二问的基础上，请尝试配置s2的流表，实现如下行为：

a) 仅有TCP流量被允许传递到主机h2(即UDP流量被阻塞)

b) 所有从h2发出的流量目的地址均被改为h1。

高级要求（两者任选其一）：

1. 如何在复杂多变的网络环境下保证网络服务的稳定性和效率，是负载均衡机制需要解决的一个重要问题。在上述实践中，我们已经熟悉了如何调用北向API实现对交换机的控制。请尝试在SDN架构下为该网络应用 程序加入负载均衡策略，以期提高网络性能。
2. 随着信息技术和产业的高速发展和广泛应用，人类社会进入信息化时代，信息安全已成为影响国家经济社 会发展的关键问题之一。请参考实际应用场景来完善SDN控制器，实现防火墙和入侵检测功能，如拒绝来自 某IP地址的数据包、拒绝试图访问某个主机的数据包、禁止包含某些关键字的数据包等。

参考资料

* [ryu安装](https://blog.csdn.net/qq_34415266/article/details/92795959)
* [mininet官网](http://mininet.org/)
* [ryu tutorial](https://ryu.readthedocs.io/en/latest/)
* [ryu book](https://book.ryu-sdn.org/en/html/)
* net\_start.py (canvas给出)

# BitTorrent

BitTorrent是一种用于文件分发的流行P2P协议，广泛应用于一些下载软件如比特彗星，Azereus等。

基本要求:

1. 了解BitTorrent协议，并实现一个简单的BitTorrent客户端。
2. 设计一个场景，如3个peer进行文件传输，peer3同时从peer1和peer2下载同一个文件A，并使用mininet构造多个peer。
3. 进行模拟实验并展示效果。需要实现以下功能:

* 种子的生成 :发布者要按照一定算法生成torrent
* 种子的上传 :发布者要向Tracker服务器上传种子，tracker进行相应的动作
* p2p文件传输 :任何获得种子的对等下载方，需要解析种子，然后向tracker请求下载，并进行后续交互。

高级要求：

1. 尝试实现以下三种性能优化策略。

* 疏通(unchocking): 详见BitTorrent协议说明11.5节”Chocking and Optimistic Unchocking
* 最稀缺优先策略（rarest-first）：详见BitTorrent协议说明11.3节“Piece Downloading Strategy"
* 收尾模式(endgame): 详见BitTorrent协议说明11.4节“End Game”

参考资料

* [基于Python实现的P2P通信](https://www.writebug.com/code/0c4f04d7-c792-11ed-bf4e-6479f0e5e323/)
* [Bittorrent协议说明](https://wiki.theory.org/BitTorrentSpecification)
* [BT种子原理简介](https://blog.csdn.net/qq_33850438/article/details/80514813)
* [P2P通信原理与实现](https://www.cnblogs.com/pannengzhi/p/4800526.html)
* [mininet官网](http://mininet.org/)