《计算机网络第二次实验》

班级：信安2302班

学号：202308060227

姓名：石云博

目录

[一. 问题描述 2](#_Toc192274121)

[二. 问题分析 2](#_Toc192274122)

[三. 实验过程及代码 4](#_Toc192274123)

[四. 结论 11](#_Toc192274124)

[五. 参考文献 12](#_Toc192274125)

# 问题描述

任务：测量大学网

1.试着找到我们大学网络的拓扑结构

2.试着找出我们大学网络中有多少信息节点，无论是虚拟的还是物理的

3.试着找出这些节点中有多少是持续活动的、周期性活动的或随机活动的

4.尝试找到尽可能多的多主节点，谈谈你的方法和结果，给出你的方法可以获得结果的理由

# 问题分析

首先第一个问题中，我们需要知道这里的大学网络指的是什么，没有特殊说明所以我们当它是校园网。要找到网络的拓扑结构，我们需要知道拓扑结构这个定义，网上查找相关资料，整理如下：

网络拓扑结构描述了网络中各个设备（如计算机、路由器、交换机等）如何相互连接的整体布局，它既可以指物理上实际的连线方式，也可以指逻辑上数据流转的路径。了解网络拓扑结构有助于设计、管理和维护网络，确保网络的可靠性、可扩展性和高效性。大致能分为以下几个类型：

总线型拓扑，星型拓扑，环型拓扑，树型拓扑，网状拓扑，混合型拓扑。

想要找出校园网的网络拓扑结构，我们需要使用诸如 Traceroute、Nmap、或更专业的网络拓扑发现工具（如 Cisco Discovery Protocol 或 LLDP）扫描校园网各个网段，收集路由器、交换机、服务器等设备之间的连接信息。

第二个问题，找到信息节点，我们可以通过设备扫描即采用端口扫描、主机发现等技术，确定校园网络中在线的物理节点（服务器、路由器、交换机、终端等），然后通过虚拟节点识别： 从虚拟化平台（如 VMware、KVM、Docker 等）中提取虚拟机、容器等信息，或通过 DHCP、DNS 记录结合扫描结果来识别存在的虚拟节点。

第三个问题，确定节点的活跃状态，我们可以用监控数据采集的方式对所有节点进行一段较长时间（如数天或数周）的流量、心跳、SNMP 状态等数据采集，但是这种方式耗费时间过于长，所以我们使用较短时间的结果来进行推断。

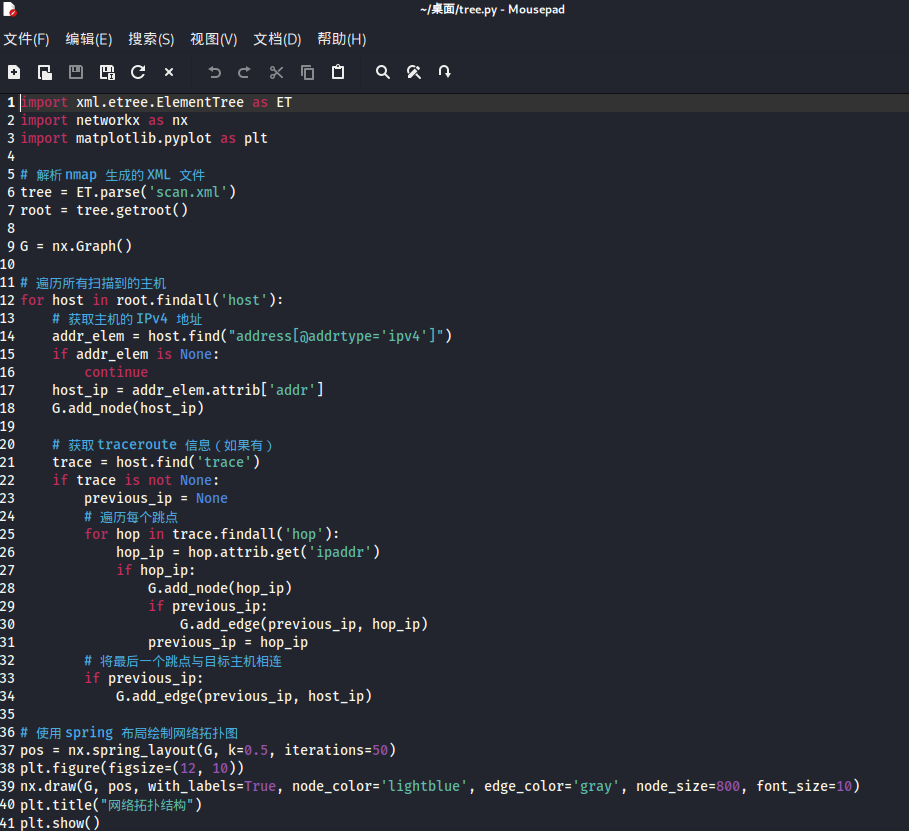
第四个问题，我们首先明确多主节点的定义，查到其值的是承担多个服务、多个控制任务或者在网络中同时扮演多个角色的节点。我们可以建立节点与服务的映射关系，将所有节点的角色、职责进行标签化。交叉统计，得到多主节点的名单及其分布情况。

# 实验过程及代码

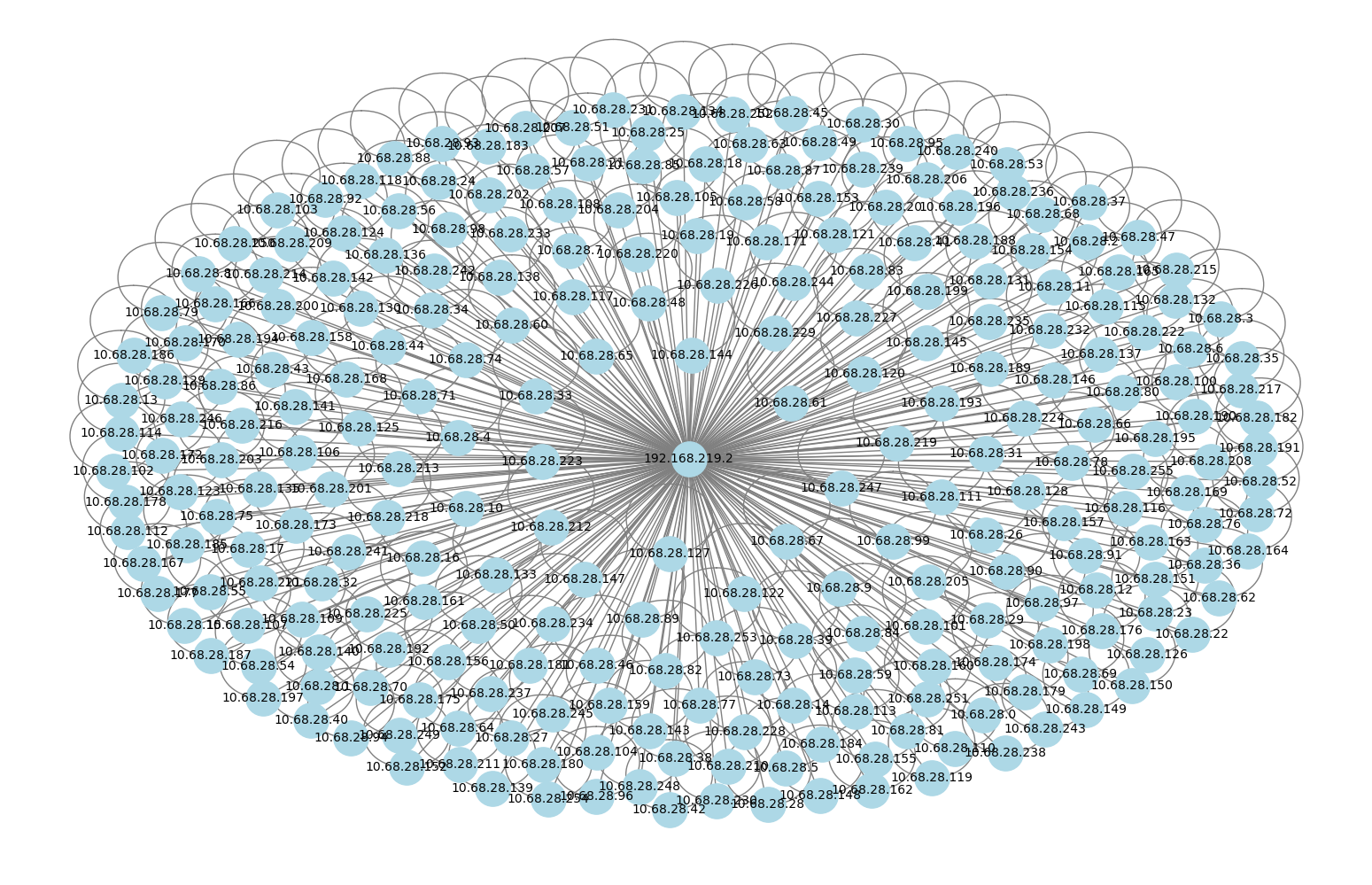
首先来看第一个问题：找出我们学校的网络拓扑结构。这里我们使用namp中traceroute以及网络拓扑图绘制工具networkl来尝试完成这个任务。首先，我们需要先知道校园网的ip，在接入校园网的vpn之后我们在windows命令行中使用“ipconfig”来找到当前ip地址为10.68.28.101（位于天马学生公寓）。

我们利用指令“sudo nmap -sn --traceroute 10.68.28.101/24 -oX scan.xml”来使用nmap扫描校园网ip并将扫描结果放到“scan.xml”中方便后续使用networkl绘制网络拓扑图。

然后使用python调用networkx来绘制网络拓扑图。

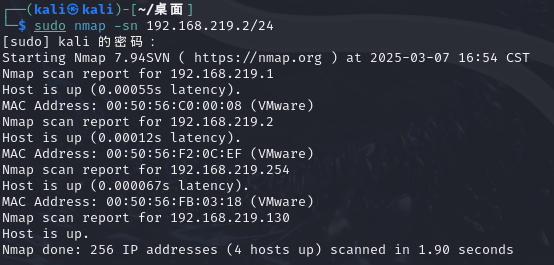


绘制网络拓扑图的代码

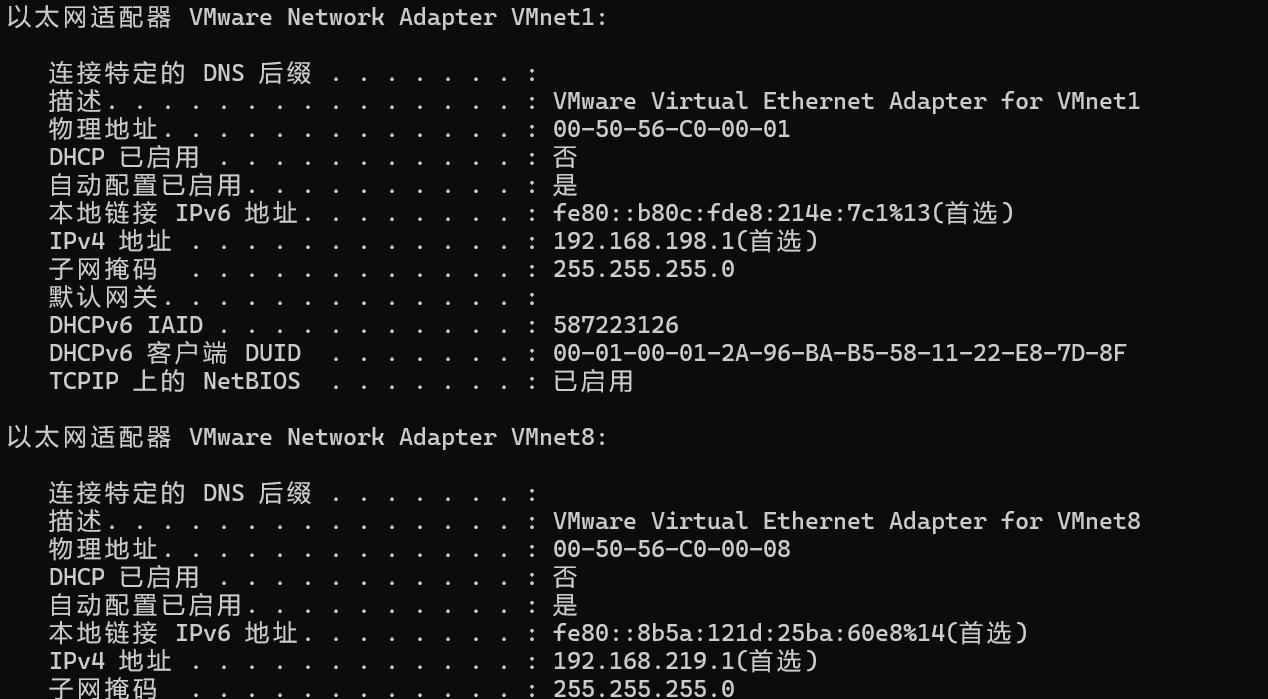


最终得到了上图这样的结果，根据结果我们认为校园网的拓扑结构是星型拓扑结构，中间节点为“192.168.219.2”.当然，由于防火墙等因素，该结果存在偏差。

再来看第二个问题：试着找出我们大学网络中有多少信息节点，无论是虚拟的还是物理的。通过搜索常见的虚拟机网络节点，我们知道有VMware：如 00:50:56, 00:0C:29, 00:05:69VirtualBox：如 08:00:27Hyper-V：如 00:15:5D。KVM/QEMU：常见前缀如 52:54:00。所以我们需要在扫描出来的节点中将这些作为虚拟节点统计。依旧是使用nmap来进行扫描，这次我们直接扫描上面得到的中心地址处的网络，即192.168.219.2。

我们先直接用nmap指令扫描，得到结果如下：

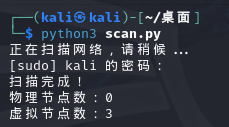
可以看到只有4个活跃地址，其中有三个后面标注了（VMware），是虚拟节点。其中的00-50-56-C0-00-08为本机地址。



我们也可以编写python代码来直接扫描并统计地址个数：



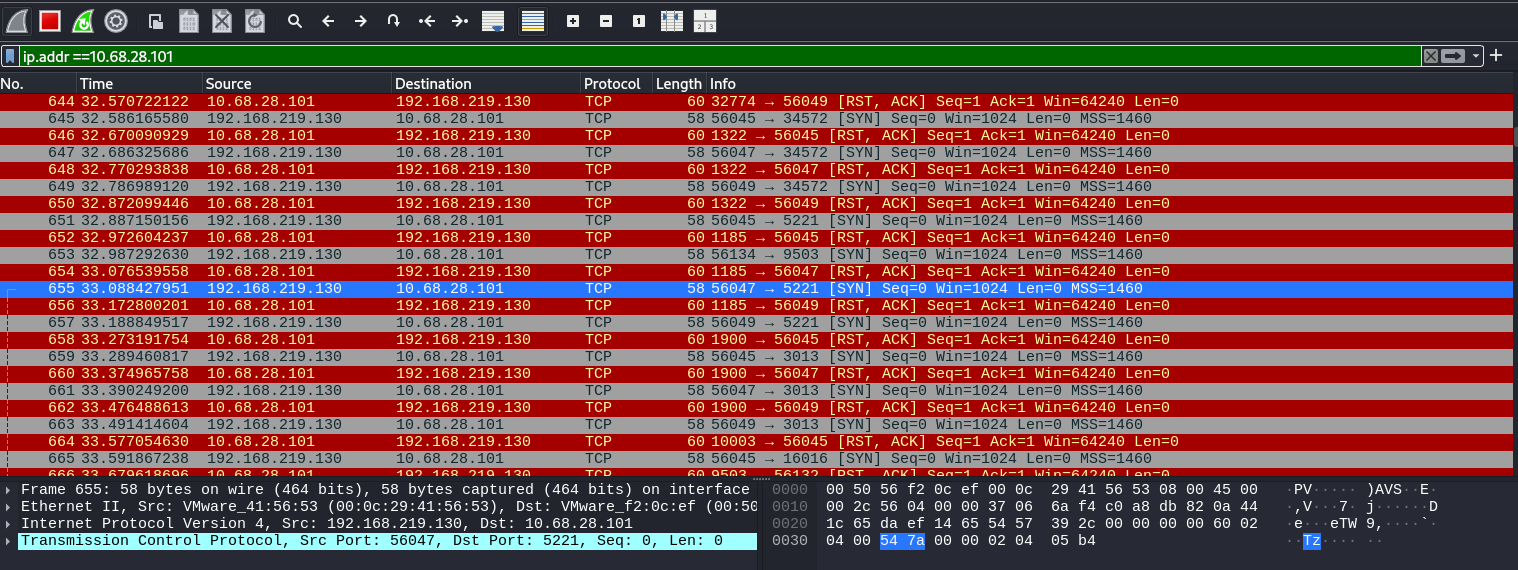
调用该py文件，得到结果：



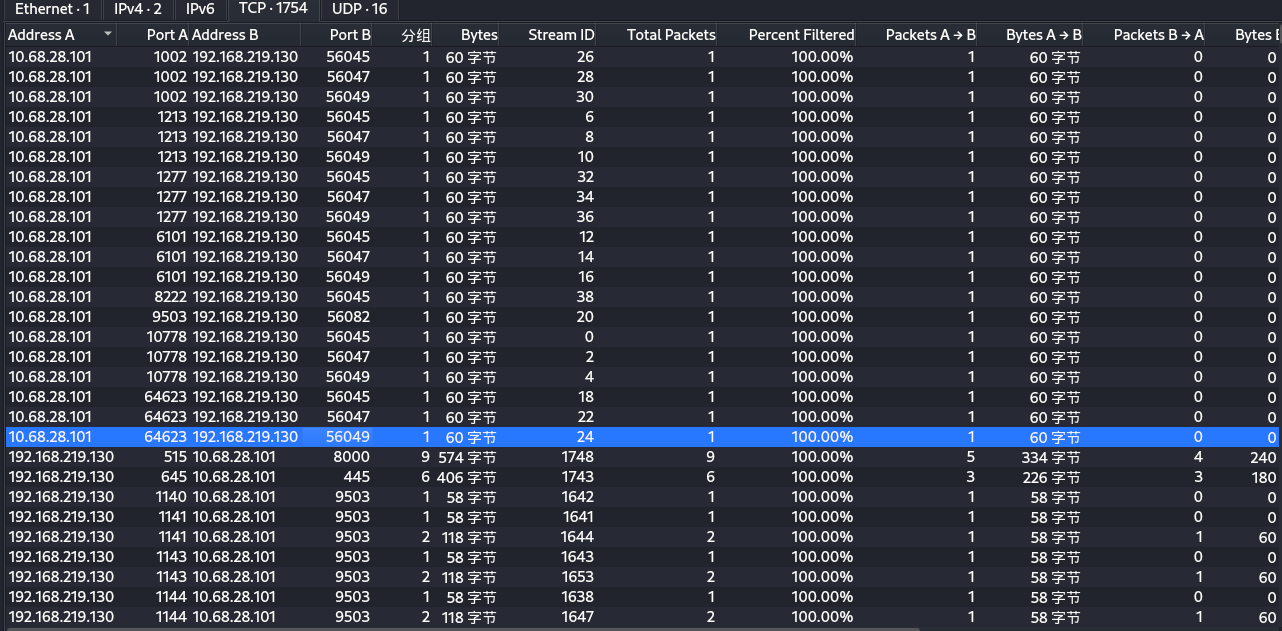
不知道为什么，上面直接扫出来物理节点有1个而这里物理节点只有0个。

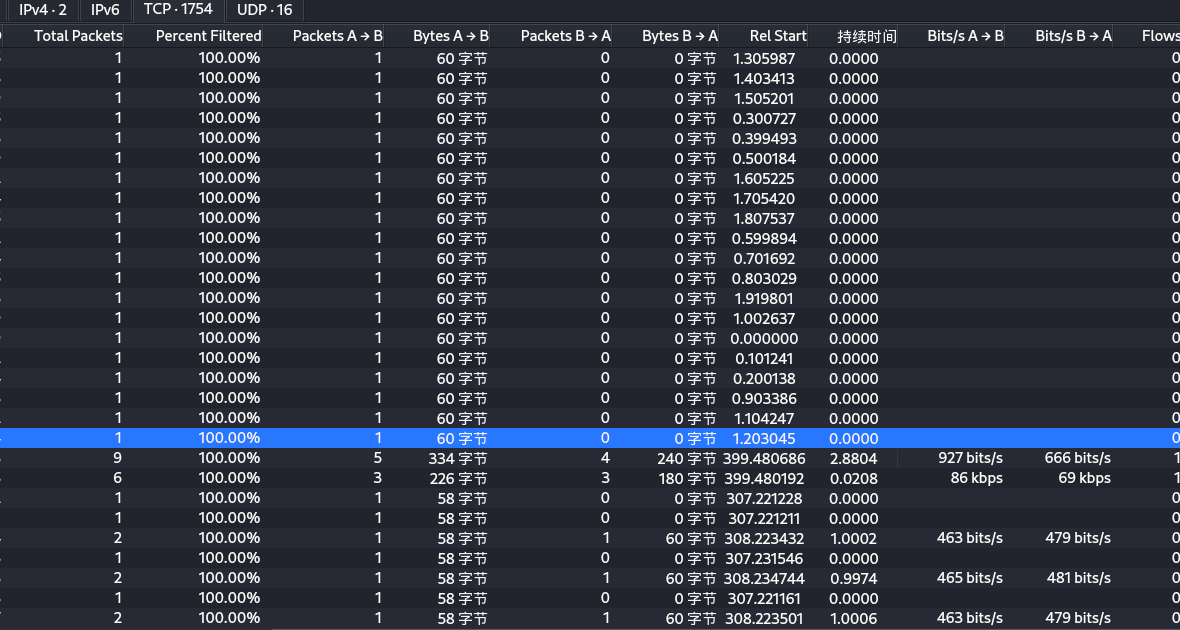
第三个问题：试着找出这些节点中有多少是持续活动的、周期性活动的或随机活动的。我们使用软件wireshark来对节点进行检测，以判断其活跃情况。

首先打开软件，我们需要在过滤设定中输入我们要检测的ip，这样软件就只会返回我们需要的结果。

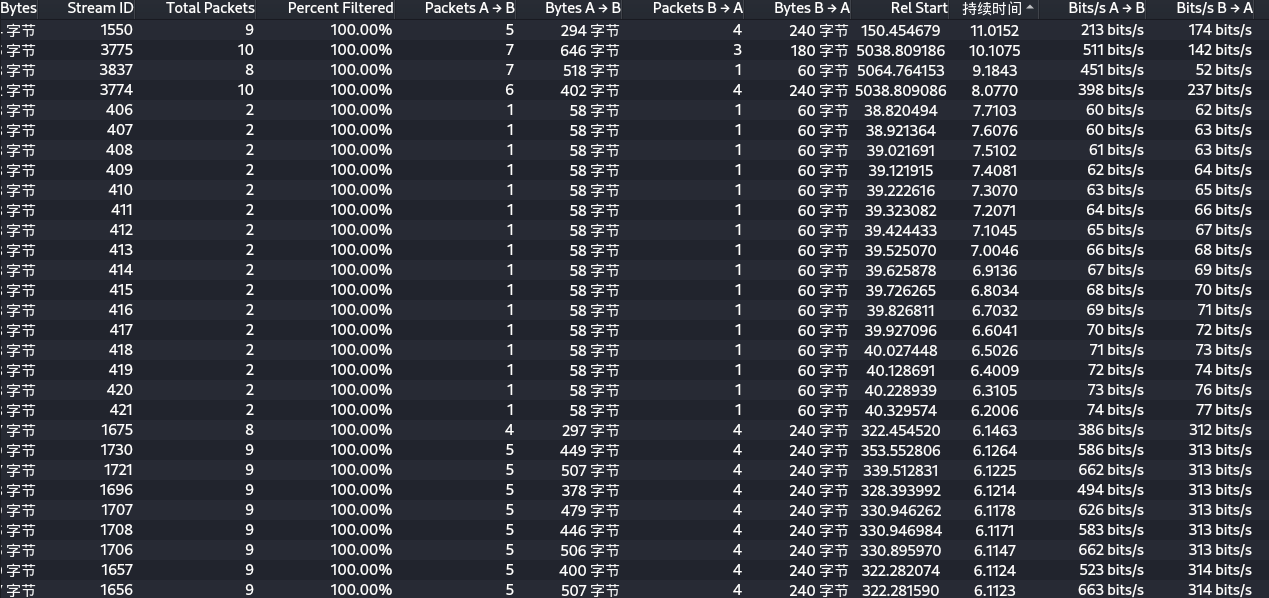


捕获完成之后，我们需要找到持续活动，周期性活动，或者是随机活动，我们通过“统计”，“会话”找到每个节点的统计信息：



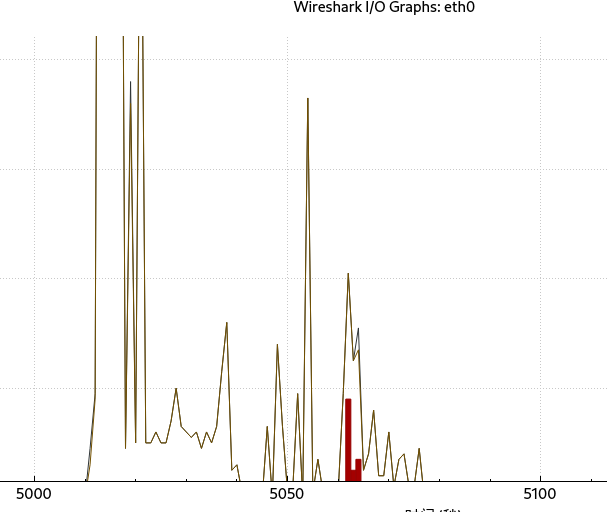


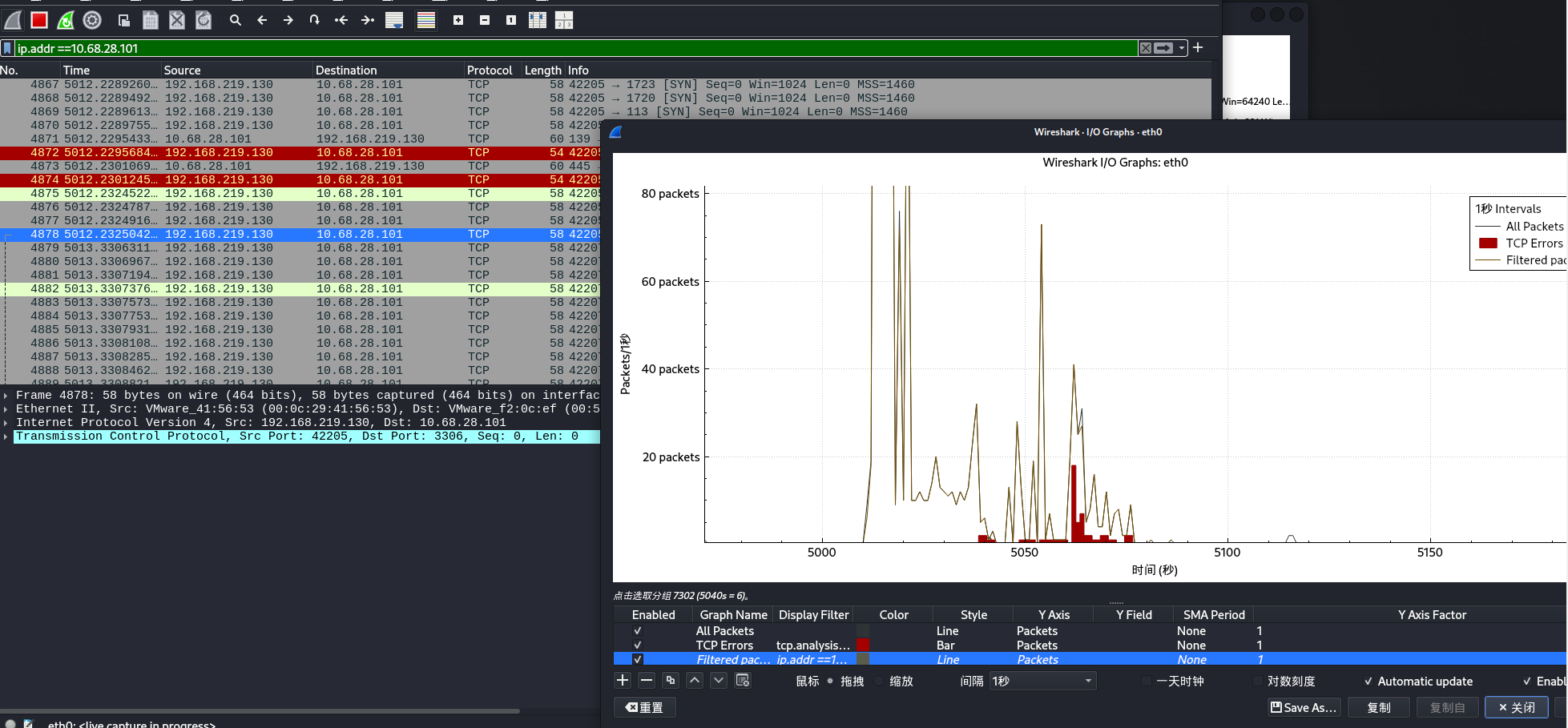
我们可以在这里看到节点的持续连接时间，从而判断出节点的活跃状态。我们选择按照持续时间降序排序：



上面就是持续活跃的节点。

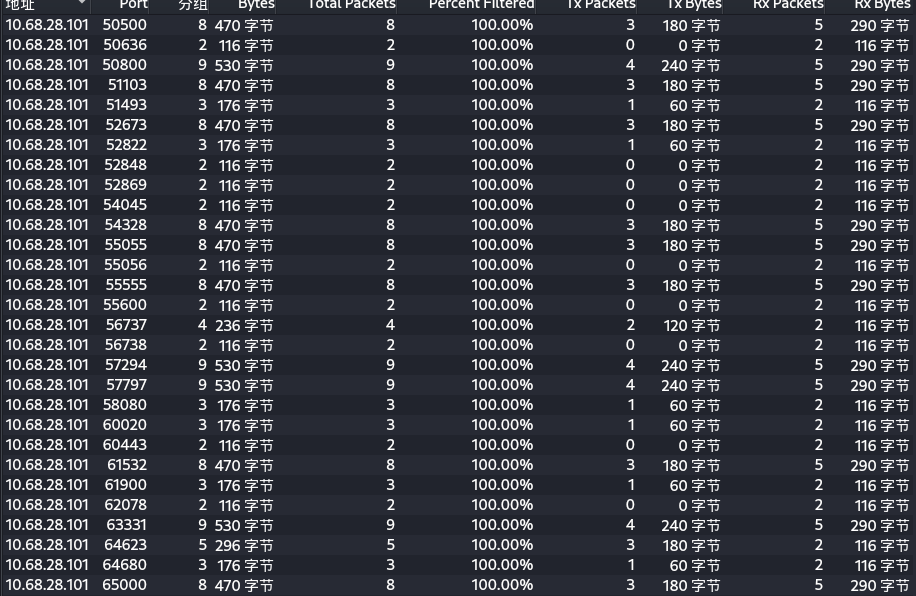
我们点开统计中的io，得到下面的时间图：



这里我们可以找到活跃的周期，可以点击突然跃升的点来看这属于哪些节点应该就是随机活跃的节点：  


第四个问题：

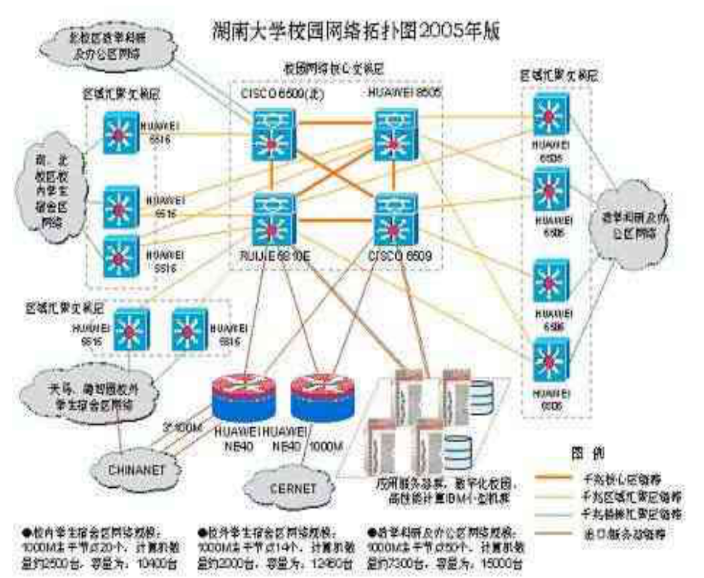
尝试找到尽可能多的多主节点，想要找到多主节点，我们需要找到哪些设备和多个ip有连接行为来判断其为承担多个服务、多个控制任务或者在网络中同时扮演多个角色的节点。这点可以使用wireshark中的端点统计功能来实现：



我们可以看到上图中该地址有多个发送与接收数据包的动作，我们可以据此判断其为一个多主节点。

# 结论

通过这次的实验，我尝试对校园网进行探测，找出其网络拓扑结构，活跃节点，多主节点等。经过实验，我认为我们学校的校园网拓扑结构是星型结构。但是我感觉实验的误差很大，这种感觉的来源是第二个任务中探测大学网络的信息节点我们经实验得到的结果是只有四个活跃的节点，其中一个物理节点，三个虚拟节点，我觉得这个数量应该远小于实际的节点数量，会有这么大的偏差，我认为最大的原因是防火墙。和上一次实验探测节点类似，但是上次实验的样本太多了，这次实验探测的对象本身数量很小，再加上学校校园网本身防火墙更加普遍，所以防火墙的作用表现得更加强烈。对于问题本身，我也去网上搜了搜，得到了下面这张有点年代的校园网拓扑图：



同时找到了一段百度百科上对校园网的描述：

“湖南大学校园网络于1996年开始投资建设，历经多次扩容、升级和改造，已形成核心交换层、区域汇聚交换层、楼栋汇聚层、终端用户接入层四个层次，环形与星型相结合的[网络拓扑结构](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%8B%93%E6%89%91%E7%BB%93%E6%9E%84/4136060?fromModule=lemma_inlink" \t "_blank)。”上面描述其结构为环形与星型相结合。

# 参考文献

1百度百科湖南大学湖南大学校园网络信息中心词条.https://baike.baidu.com/item/湖南大学校园网络信息中心/1234271. 2023.11.25.

[2] https://blog.csdn.net/article/details/128538247?spm=1001.2014.3001.5506. 通过 traceroute 和 networkx 构建网络拓扑图. 哟，又在写bug呢. 2023.03.22.

[3]https://blog.csdn.net/zzwwhhpp/article/details/113077747?spm=1001.2014.3001.550. 0x00dream. 网络分析工具——WireShark的使用（超详细）.2021.01.24.

[4] https://zh.wikipedia.org/wiki/网络拓扑.维基百科.网络拓扑词条.2023.8.15.

[5] https://blog.csdn.net/article/details/123710292. k月光疾风k. 端口扫描工具Zenmap超详细使用方法+使用案例（windows）.2022.3.24

[6] https://docs.pingcode.com/baike/2761362. Edit2. nmap如何全面扫描虚拟机. 2024.9.16.

[7] https://www.zhihu.com/tardis/zm/art/ 亿图图示. 关于网络拓扑图，你想知道的都在这. 2022.8.15.