计网第一次实验

目录

[一. 问题描述 1](#_Toc191761587)

[二. 问题分析 2](#_Toc191761588)

[三. 实验过程及代码 4](#_Toc191761589)

[四. 结论 13](#_Toc191761590)

[五. 参考文献 15](#_Toc191761591)

# 问题描述

Assignment :Probe the Internet (lPv4 and |Pv6) (探测互联网（IPv4和IPv6）)

1. Probe and estimate how many addresses are active, explain

your methods and estimates the error bounds

(探测并估算有多少地址是活跃的，解释你的方法并估计误差范围。)

2. Find as many key addresses as possible, and then explain what

are they and why are they important

(尽可能找到尽可能多的关键地址，然后解释它们是什么以及为什么它们重要。)

3.Finish 1 and 2 in both lPv4 and lPv6(在IPv4和IPv6中完成1和2。)

# 问题分析

题目的目的是探测互联网地址活跃度，故我们需要查找相关资料找到探测的方法。整合网上的资料，探测的方式大致分为这几种：Ping探测，网络扫描工具扫描，流量分析等。

实验对象是IPv4和IPv6，我们需要知道什么是IPv4和IPv6。

IPv4：

网际协议版本4（英语：Internet Protocol version 4，又称互联网通信协议第四版）是网际协议开发过程中的第四个修订版本，也是此协议第一个被广泛部署和使用的版本。其后继版本为IPv6，直到2011年，IANA IPv4位址完全用尽时，IPv6仍处在部署的初期。

IPv4在IETF于1981年9月发布的 RFC 791 中被描述，此RFC替换了于1980年1月发布的 RFC 760。

IPv4是一种无连接的协议，操作在使用分组交换的链路层（如以太网）上。此协议会尽最大努力交付数据包，意即它不保证任何数据包均能送达目的地，也不保证所有数据包均按照正确的顺序无重复地到达。这些方面是由上层的传输协议（如传输控制协议）处理的。

IPv6：

网际协议第6版（英语：Internet Protocol version 6，缩写：IPv6）是网际协议的最新版本，用作互联网的协议。用它来取代IPv4主要是为了解决IPv4地址枯竭问题，同时它也在其他方面对于IPv4有许多改进。

IPv6的设计目的是取代IPv4，然而长期以来IPv4在互联网流量中仍占据主要地位，IPv6的使用增长缓慢。在2022年4月，通过IPv6使用Google服务的用户百分率首次超过40%[1]。

现今的互联网络发展蓬勃，截至2018年1月，全球上网人数已达40.21亿，IPv4仅能提供约42.9亿个IP位置。虽然目前的网络地址转换及无类别域间路由等技术可延缓网络位置匮乏之现象，但为求解决根本问题，从1990年开始，互联网工程工作小组开始规划IPv4的下一代协议，除要解决即将遇到的IP地址短缺问题外，还要发展更多的扩展，为此IETF小组创建IPng，以让后续工作顺利进行。1994年，各IPng领域的代表们于多伦多举办的IETF会议中，正式提议IPv6发展计划，该提议直到同年的11月17日才被认可，并于1996年8月10日成为IETF的草案标准，最终IPv6在1998年12月由互联网工程工作小组以互联网标准规范（RFC 2460）的方式正式公布。

IPv6的计划是建立未来互联网扩展的基础，其目标是取代IPv4，虽然IPv6在1994年就已被IETF指定作为IPv4的下一代标准，由于早期的路由器、防火墙、企业的企业资源计划系统及相关应用程序皆须改写，所以在世界范围内使用IPv6部署的公众网与IPv4相比还非常的少[2][3]，技术上仍以双架构并存居多。预计在2025年以前IPv4仍会被支持，以便给新协议的修正留下足够的时间。

因为网络端口数量过多，我们选择抽样调查的方式进行估算总共的活跃端口数量，其中IPv4和IPv6的总端口数量分别为2的32次方以及2的128次方，我们使用nmap来进行网络端口扫描实验。

我们还需要了解什么是关键网络，经过询问deepseek，得到以下回答：

在计算机网络中，关键端口通常指的是那些用于提供核心服务或功能的端口。这些端口通常与特定的服务或协议相关联，且在网络通信中扮演着重要角色。

根据端口号的范围，端口可以分为以下几类：

知名端口（Well-Known Ports）：范围从0到1023，这些端口号通常固定分配给一些服务。例如：

21端口：用于FTP（文件传输协议）服务。

22端口：用于SSH（安全外壳协议）服务。

80端口：用于HTTP（超文本传输协议）服务。

443端口：用于HTTPS（安全的HTTP）服务。

注册端口（Registered Ports）：范围从1024到49151，这些端口号可以由应用程序使用，但通常需要注册以避免冲突。

动态和/或私有端口（Dynamic and/or Private Ports）：范围从49152到65535，这些端口号通常用于客户端与服务器之间的临时连接。

在网络安全和管理中，了解和监控这些关键端口非常重要，因为它们可能成为攻击的目标。例如，攻击者可能会扫描开放的知名端口，以寻找潜在的漏洞。因此，确保这些端口的安全性对于保护网络免受未授权访问和攻击至关重要。

# 实验过程及代码

我们首先在虚拟机中下载kali，在其中打开nmap



图表 1 在kali系统中打开nmap

从网上搜索资料得到其具体的使用方式，使用指令“nmap -sn -iR 10000 -PE -n --min-parallelism 1000 --max-parallelism 10000 -oA report”，意为通过 ICMP ping 扫描 10000 个随机 IP 地址，检测哪些主机在线，并且将扫描结果以三种格式保存到以 report 为前缀的文件中。扫描时会采用较高的并行度，以加快速度。（注意，nmap扫描端口默认为扫描ipv4）其中各个参数的意义如下：

-sn: 这个参数表示只进行 "ping扫描"，即检测哪些主机在线，而不进行端口扫描。

 -iR 10000: 这个参数指定随机选择 10000 个目标进行扫描。-iR 后面跟的是要扫描的目标数量。

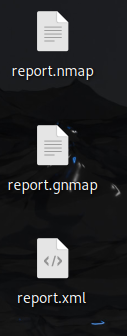
 -PE: 这个参数指定使用 ICMP Echo 请求进行 ping 扫描。即使用标准的 ICMP "ping" 协议来检查主机是否在线。

 -n: 这个参数表示禁用 DNS 解析。通常，nmap 会尝试解析主机的域名，但加上 -n 就意味着不进行 DNS 查询，直接使用 IP 地址。

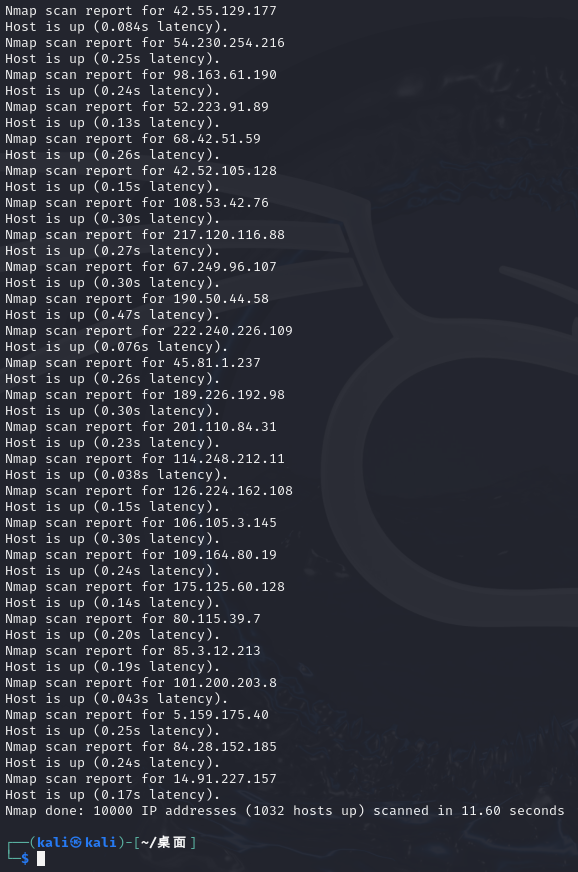
 --min-parallelism 1000: 这个参数设置扫描时的最小并行度为 1000，意味着扫描过程中会同时处理至少 1000 个主机。

 --max-parallelism 10000: 这个参数设置扫描时的最大并行度为 10000，意味着最多可以同时处理 10000 个主机。

 -oA report: 这个参数表示将扫描结果输出到文件，并且输出格式为 -oA（普通格式、XML格式和脚本格式），文件名前缀是 report，所以会生成 report.nmap、report.xml 和 report.gnmap 文件。



图表 2 生成的report文件



图表 3扫描结果

根据图3中的结果，我们得到了10000个地址中有1032个活动端口，根据这个数据，我们可以尝试着估算ipv4的活跃端口数量：

**1. 估计总体中具有活动端口的 IPv4 地址数量：**

在样本中，具有活动端口的比例为：

p=1,032/10,000=0.1032

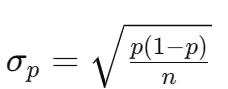
因此，可以估计整个网络中具有活动端口的 IPv4 地址数量为：

N=4,294,967,296×p=4,294,967,296×0.1032≈443,597,568

这意味着，基于样本，估计约有 443,597,568 个 IPv4 地址具有活动端口。

**2. 计算估计的标准误差：**

由于使用了简单随机抽样，估计的标准误差可以通过以下公式计算：



其中，p 是样本中具有活动端口的比例，n 是样本大小。

代入数值：

σp=≈0.00097

**3. 计算总体估计的标准误差：**

总体估计的标准误差可以通过以下公式计算：

σN​=N×σp​

代入数值：

σN=4,294,967,296×0.00097≈4,165,019

**4. 计算置信区间：**

假设以 95% 的置信水平估计总体中具有活动端口的 IPv4 地址数量。 在正态分布下，95% 的置信区间对应的 Z 值约为 1.96。 因此，置信区间的计算公式为：

置信区间=N±Z×σN

代入数值：

置信区间=443,597,568±1.96×4,165,019

置信区间=443,597,568±8,150,838

因此，95% 的置信区间为：

(435446730,451748406)

接着我们计算该估计的误差比例，根据公式：误差比例=估计的总体数量标准误差​×100%，我们得到误差比例=（4165019/443597568）​×100%≈0.94%。

总结：

基于样本数据，估计整个网络中约有 443,597,568 个 IPv4 地址具有活动端口。 在 95% 的置信水平下，实际数量可能在 435,446,730 到 451,748,406 之间。误差比例约为0.94 %

但是注意，这些估计基于样本数据，实际情况可能因网络环境的差异而有所不同。整理网上查找到的资料，发现可能的误差来源大概有以下几种：

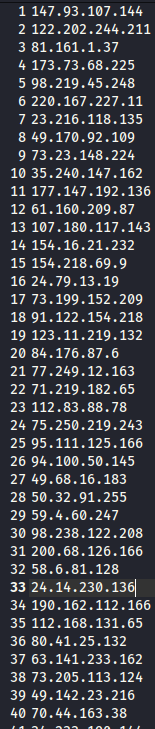
1.网络环境变化：网络中的主机和端口状态可能会随着时间变化，扫描时刻的网络状态可能与实际情况有所差异。

2．防火墙和安全设备的影响：防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）可能会阻止或修改扫描流量，导致扫描结果不准确。

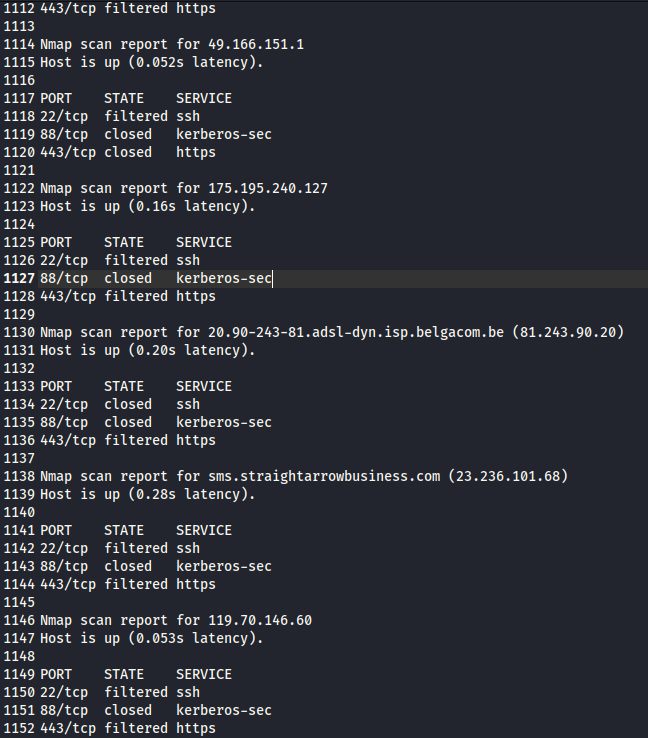
3.扫描方法的局限性：不同的扫描技术（如 SYN 扫描、TCP connect 扫描等）可能对不同类型的主机和网络环境有不同的适用性和准确性。

结合ipv4总地址有2的32次方这么多的实际情况，我认为，活跃的ipv4端口数量应该远高于这个估计数字，但是探测不出来实际相近的结果。

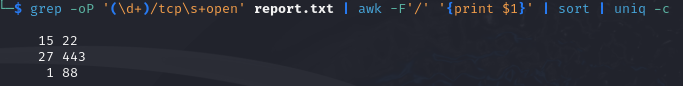
探测关键端口：  
上面问题分析中我们知道了关键端口包含22，80，443等端口，故我们可以指定扫描这些端口。扫描之前，我们需要从原先保存的report文件中提取出IP地址，这需要借用到指令“grep -oP 'Host: \K[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+'report.gnmap > ips.txt”

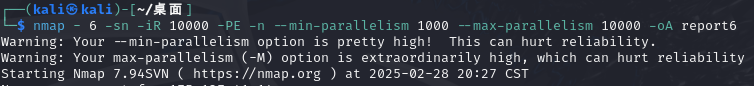


图表 4地址文件 ipx

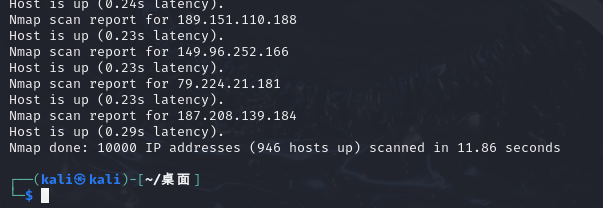
接着使用指令“nmap -p 22,88,443 -iL ips.txt -oN report.txt”扫描ipx中的22，80，443端口。最终得到结果：

再使用指令“grep -oP '(\d+)/tcp\s+open'report.txt | awk -F'/' '{print $1}' | sort | uniq -c”得到结果中每种关键端口的数量：

  
接下来，我们进行IPv6的相关实验，和IPv4的实验步骤大致类似，但是nmap的指令中需要添加参数 “-6”.



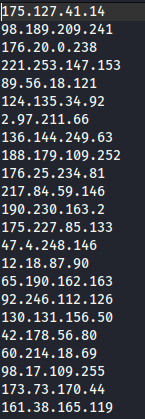
得到扫描结果：



可以看到10000个地址中有946个IPv6地址，我们按照上面IPv4一样的步骤进行估算，得到一下结果：  
估算出的全球IPv6的活跃地址约为189,200,000（这个结果有一个前提是我们估计全球的IPv6地址为20忆个，虽然IPv6理论上能提供2的128次方个地址，但是实际上很多地方并未普及IPv6，故由网上一些基于研究和统计的估计，我们把20忆作为全球的IPv6地址），由此得初的标准误差为171,832 个，误差比例约为0.09%。

然后我们扫描关键端口：  
和ipv4一样，我们得到地址集合文件ipx6.txt.





图表 5 ipx6.txt

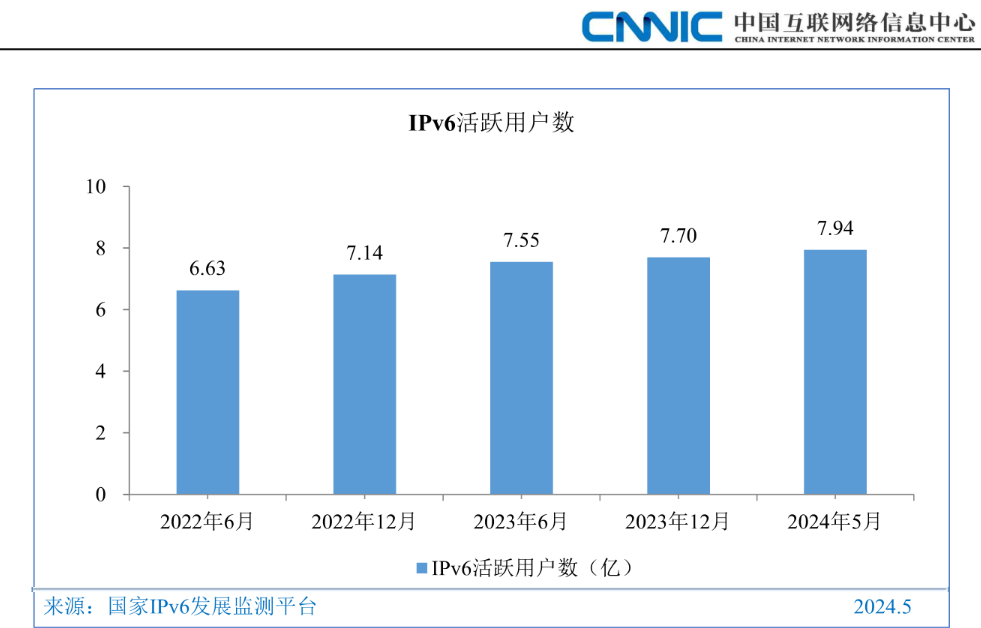
扫描其中的22，80，443端口，得：  

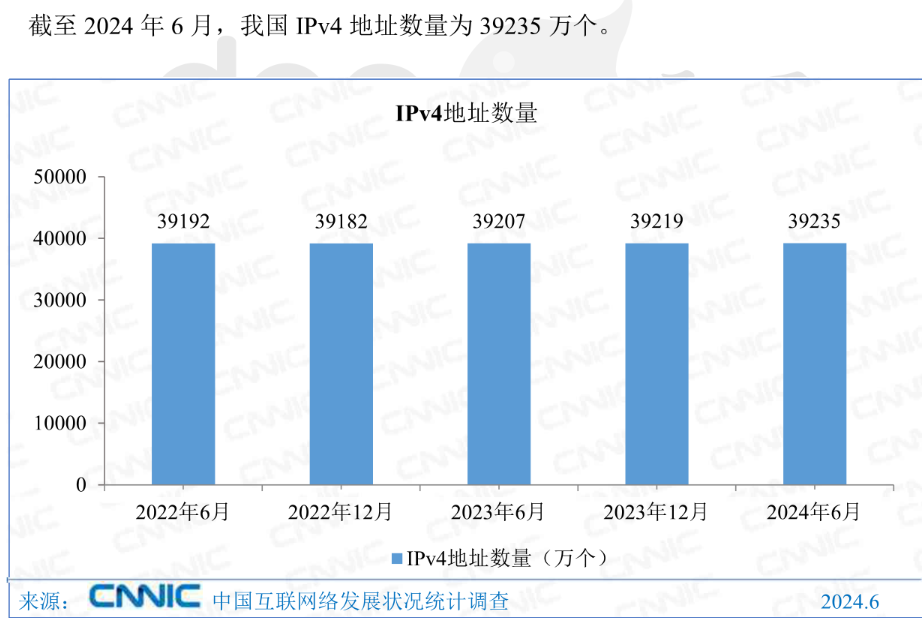

关于关键端口为什么重要，通过询问deepseek，我们得到以下答案：

关键端口的重要性在于它们通常是网络和系统的入口点，攻击者通过这些端口尝试入侵系统。保护这些端口，及时识别潜在的安全风险，是确保网络和服务正常、安全运行的关键措施。因此，了解并监控这些关键端口是网络安全管理的基础。最重点的是，关键端口构成现代网络交互的基础。

# 结论

通过实验，我们得到了估算之后的IPv4和IPv6的活跃端口数量，经过实验认为，活跃的IPv4端口远多于活跃的IPv6端口，同时粗略扫描了关键端口。实验期间遇到许多以前不曾遇到过的困难，诸如nmap的常用命令行，linux系统下文件的编写等等，感谢有deepseek能使其被尽快解决。 同时也感到个人实力的不足，实际上该实验得到的估算结果因为诸如普及程度，防火墙等等现实因素具有较大误差。经过查阅《第54次中国互联网络发展状况统计报告》我看到了一些国内的网络情况：





# 参考文献

[1].维基百科，IPv4词条，IPV6词条

[2].csdn，Ly4j，Nmap扫描结果保存到本地并提取ip，2021.9.14

[3].csdn [Python\_chichi](https://blog.csdn.net/Javachichi) 2025版最新保姆级扫描工具Nmap使用教程图文教程（超详细）零基础入门到精通，收藏这篇就够了，2025.1.14

[4] 中国互联网络信息中心，第54次中国互联网络发展状况统计报告，2024.11.17

[5] IPv4 VS IPv6：what are the different，John Bogna，2023.6.6

[6] 活跃ip地址检测与性质判定研究，丁枫，东南大学，2011.6.6