# 用于单点检测子网连通性的优化方法

赵昕[1, 2]，程光[1, 2]

（1.东南大学计算机科学工程学院，南京，211189；2.计算机网络与信息集成教育部重点实验室，南京，211189）

**摘　要：**网络可达性是网络测量与分析中的一项重要指标，本文介绍的是一种在单一主机上主动检测子网可达性的方法。相较于传统的利用 SNMP 基于路由表的网络可达性检测方法不需要获取网络中各主要节点路由器的信息，更加灵活简单。本文结合了在单点通过对目标地址采用 ICMP PING 方法和 TCP 端口发现的方法，通过网络层和传输层的连接确保了结果的准确性。对于子网地址过多而使得资源消耗大、检测效率低这个问题，本文介绍了一种基于子网中的地址在时间上会表现出一定规律性，通过将全地址检测中得到的可达地址放入一个队列，再从队列中抽取以后该子网的检测地址的方法，在保证了一定的准确率的情况下减少子网的检测地址数量，提高检测效率。

**关键词：**子网可达性；单点检测；ICMP 与 TCP；减少子网检测地址

# An Optimized Method for Large-Scaled Network Connectivity Detection

ZHAO Xin[1, 2], CHENG Guang[1, 2]

(1. School of Computer Science & Engineer, Southeast University, Nanjing, 211189;

2. Key Laboratory of Computer Network and Information Integration, Ministry of Education, Nanjing, 211189)

**Abstract:** Network reachablity is an important aspect in measuring and analyzing network. The article introduces a method to detect reachablity of subnets on one machine. Compared with methods that analyse routing tables of routeres based on SNMP, the method has no need for information of routers so that it is simple and quick. The article combine ICMP PING and TCP port detecting to the target IP addresses on one machine. The link on network layer and transport layer ensure the accuracy of result. The article also introduces a method based on regularity of existing addresses of a subnet during a period of time to optimize the source utilize and efficiency. To detect all addresses of a subnet first and record addresses that can be reached each time and put them in a queue, then select some addresses in the queue to build a list for the subnet and regard addresses in the list as addresses that would be detected of the subnet. It reduces the number of addresses to detect as well as ensure the accuracy.

**Key words:** Reachablity of subnet; One-point detecting; ICMP and TCP; reduce detecting addresses of a subnet

## 1 引言

本文的研究的背景是教育网子网的可视化中的一部分，对于教育网中大量的子网数量，怎样才能有效率且较准确的检测出其可达性成为研究中的一个严峻的问题。

网络可达性作为网络测量与性能分析中的一项重要的指标，是进行其他性能指标测量或分析拓扑测量的前提。传统的方式有根据 SNMP 协议，分析路由器中的路由表，通过路由表的信息来构建网络拓扑，还有常见的方法是在网络中的边界路由器获取 BGP 报文，对报文进行解析，解析 BGP UPDATE 报文中的 acknowledge 或者 withdraw 消息[1]中的地址和路径进行提取，也有对 ARP 表进行解析，还有的通过 DNS 服务器寻找对应域名的 IP 等等。

现有的单点主动检测网络可达性的方法中，比较多的采用了网络层协议以及传输层协议。常被用于在主机上做网络可达性检测和网络拓扑发现的是基于 ICMP 的 PING 和 TRACEROUTE。对于复杂的网络环境，有时更要综合考虑有连接和无连接的传输协议、无状态/有状态路由（或防火墙）、静态/动态 NAT、PAT 等因素。

SNMP 协议虽然准确且效率高，但是通用性较差，在无法实时获得边界路由器路由表的情况下不

**作者简介：**赵昕，（1988-），男，硕士研究生，E-mail: xiaoxian1412@foxmail.com；程光，（1973-）男，教授，博导，E-mail: gcheng@seu.edu.cn.

实际，而且本文注重的是子网地址是否存在，更多地偏重于的是地址的发现而不在于得知 IP 地址的拓扑，或者是说子网中的地址能否被扫描到存在。由于无法获得路由器的数据，所以使用主动检测连通性的一些方法在主机上更易实现和灵活。ARP 协议比较常用于局域网中的地址发现，故而也不实际。BGP 的方法需要获取很多边界路由器的 BGP 报文，故而灵活性也很低。

由于实验中已知了子网的划分结果，即地理位置、分配给的单位等信息，实验的着眼点在于子网是否存在与网络上，那么通过主机能够到达子网中的某地址就可以简单而有效的达到目的。由于需要每隔一段时间要对可达性进行更新，所以就需要每次检测需要简单快速而有效地进行。

最常见用于主机上检测目标 IP 地址是否可达的是直接使用 Windows 或 Linux 操作系统中的 ping[4]，它的本质是使用 ICMP 报文。但是由于 PING 的原理是对单一目标地址的发包和等待回应，所以在目标地址数量很多的情况下效率很低，实用价值不高。故而像 FPING 这样使用对多地址并发和异步收发 ICMP 报文的工具被开发出。

由于 ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。例如大量的 ICMP 数据包会形成“ICMP 风暴”，使得目标主机耗费大量的 CPU 资源处理，最终瘫痪。现在许多防火墙都具有 ICMP 过滤的功能，使用 ICMP 的方法去检测网络的连通性并不再是一种很准确很全面的方式。所以有很多方法也采用传输层协议报文作为辅助。

以上介绍的是检测地址可达性的方法，但是由于检测的对象是子网，所以对子网中所有的地址一一检测虽然是最为常见也是最为准确的方法，就算使用并发的方式，在子网地址多（如：/17 的子网具有 32768 个地址），子网数量大（教育网的所有子网 4028 个）的情况下，所耗费的时间和空间是相当巨大的，而且对于一个地址的发送报文不可能只有一个，有些时候为了防止丢包、延迟等现象发送至少 4 个请求报文是必要的。可想而知对每个地址进行检测需要耗费相当的资源。

本文介绍了一种在单一主机上通过网络层 ICMP 和传输层的 TCP 连接作为检测可达性的手段，同时采用社会工程学规律，即教育网子网中的地址可达性在时间上会呈现出一些规律这样的手段去缩减子网中需要检测的地址数量的方法，在保证一定准确率的情况下，加快在单一主机上定期检测子网可达性的效率。

## 2 相关工作

文献[2]介绍的就是传统的利用 SNMP，通过获取路由器的路由表和地址表中 ipRouteDest、ipRouteNextHop、ipRouteMask，进行网络拓扑发现算法。文献[3]也提到了关于使用 ping、traceroute（发现主机到目的主机的路径）和 DNS 的域名转换（发现域内主机和路由器）的方法进行地址发现。

文献[4] 具体介绍了 ping 的的原理即 ICMP ECHO 和回应报文。也使用 Winsock 编程自己构造 ICMP 数据报而收包通过 WinPcap 来实现，自己构造了 ICMP 报文。此外，其中还运用相同的方法构造 TCP SYN 利用回复的 ACK 和 RST 报文进行 IP 发现和 UDP 作为提高检测准确率的手段。Linux 下则可以通过 libnet 构造 TCP 报文发送，通过 libpcap 实现异步的接收。

武汉大学的李莉[5]等运用 Java 远程方法调用类 RMI 构建了一个远程调用的框架，远程调用目标主机上的 ping 程序，测试任意两台主机间的网络连通性。他们的方法是采用远程调用 ping，用于端到端连通性的检测。

很多的网络开源工具被开发出用来对多目标进行检测和网络发现如上文提到的 FPING。

FPING[6]的原理是以轮转方式并行地发出大量的 PING 请求。由于这样的特性，用 FPING 工具去扫描多个 IP 地址的速度要比单纯的 ping 命令快很多。FPING 工具既可以通过标准输入向它提供一系列 IP 地址作为输入，也可以让它直接读取文件中的 IP 地址序列。其结果也相当简便易读。

总结来看，目前用于单点进行可达性检测的方法比较集中在利用 ping 或者是自主构造 ICMP 或 TCP 协议数据包。在多目标地址的时候，通常采用并行发送和异步收发的方法来提高效率，但是却没能够将子网中的目标地址减少来提高效率的方法。

## 3 方法分析与实现

根据上述的相关工作中提出的方法的一些优劣性以及可行性，本文设计的方法是针对网络可视化中所要呈现的教育网网络的连通性测试，基于可视化的这个大前提，除了子网数量多，还要定期对测

试结果进行更新和显示。

现有的是子网的分配归属信息，即每个机构所被分配到的子网。本文的目的是要高效率的知道所有这些子网在某一测量的时间是否是连通的，所以本文采用的是一种抽样的方法去实现。

### 3.1 子网分析

现拥有子网和它们的归属地址。各个子网是由网络号+子网掩码构成，如：1.184.0.0/17，归属于暨南大学，由华南理工大学管理并分配；1.184.192.0/18 归属于深圳教育和科研主干网，由深圳大学管理和分配等等。

拿 1.184.0.0/17 为例，它的子网掩码是 17，IPv4 的地址是 32 位，也就是说，在这个子网中若不划分为更多层次的子网，最多可以容纳 2 的 15 次方减去 3 的主机数量，即 IP 地址的数量。

表 1 1.184.0.0/17 地址分析

| 子网 | 可用 IP（不再划分子网） | 广播地址 | 可用 IP 总数 |
|---|---|---|---|
| 1.184.0.0/17 | 1.184.0.1~ 1.184.127.254 | 1.184.127.255 | 32765 |

教育网的子网信息中显示，有 4028 个子网划分给了不同的学校和地区，它们平均子网掩码的大小在 20 左右，如果对所有的地址进行检测，效率会非常低且十分浪费资源，因为子网与地点是一一对应的关系，在一个子网中，只要有一台主机（一个 IP）是可达的，就可以判断出这个地点的子网是可达的。每个子网的每一个 IP 地址（除去全 1 和全 0 的地址）进行连通性的检测是较为准确的做法，但显然代价是相当高昂的。

### 3.2 对单个子网需要检测的 IP 地址进行抽样

可以看到，在 1.184.0.0/17 这个子网中，如果不再向下划分更细的子网，则有 32765 个可作为主机用的 IP 地址。论文的目的是减少需要检测的 IP 地址数目以达到更高的速度和效率。但是，减少检测的地址数会带来结果的不准确，所以，如何合理而准确的精简出需要检测的地址成为本文的主要思考问题。

首先，必须从零开始，对一个子网中的所有地址进行检测。通过一段时间的内不同时间点的检测，不难发现，一个子网中的可用 IP 地址有些可以被检测到可达，有些不可以。在被检测到可达的地址中，有些在多次的检测中均能连通，而有些只是在一些检测的时间点能够连通。

那么第一次想到的方法是，记录下每个子网每隔一段时间能够检测可达的地址，根据这些结果计算出的平均可连通的地址占所有地址的百分比，按照这个百分比对这个子网所有地址进行随机的抽取，对抽取得到的地址列表进行之后每次的测试。但是这种方法所带来的随机性反而使得准确率下降。

那么如何来排除由随机性带来的不准确呢？本文使用的方法是构造一个用于抽取地址的地址队列，记录下每次检测中可以连通的地址，并把它乘以一定的权重（在队列中插入加权系数那么多的此地址编号）放入队列。最后，为了获取之后需要检测的地址列表，之后可以在这个构造好的地址队列中随机抽取这个子网地址总数次，抽到的不重复的地址所构成的就为这个子网之后的检测地址列表。

### 3.3 连接性检测方法

#### 3.3.1 基于 ICMP 的 FPING

通过调用使用 FPING 工具（Linux 下）实现 ICMP 的检测方式。前文也有提到 FPING 的一些特点，如采用并发，速度快，此外它还提供了一些自定义的方法对子网和地址列表文件都有比较好的支持。

#### 3.3.1 网络扫描工具 NMAP

基于 TCP 连接的网络扫描作为加大准确率的方法同样被加入到检测的方法中。本文使用的是 Linux 下的 NMAP，即 Network Mapper，一种知名的开源的网络扫描和嗅探工具来实现 TCP 检测的方法。

NMAP 的基本功能有三个，一是探测一组主机是否在线；其次是扫描主机端口，嗅探所提供的网络服务；还可以推断主机所用的操作系统[7]。此外，NMAP 还允许用户定制扫描技巧。实验中用到的是 NMAP 中默认发送的 TCP SYN 报文中提供的选项来对目标地址和固定端口进行探测，不对所有的端口进行扫描，对返回的结果进行分析即可知道某主机（地址）是不是开启的，方可知道这个主机属于

的这个子网能否连通。

### 3.4 方法详细分析

下面通过对一个具体的子网进行方法的描述。所用到的子网是 1.185.0.0/18，算上全 0 与全 1 的地址，这个子网共包含 16384 个 IPv4 地址。下图是时间间隔 30 分钟，对 1.185.0.0/18 的所有地址进行 FPING 的 21 组结果中能连通的 IP 地址数表示。

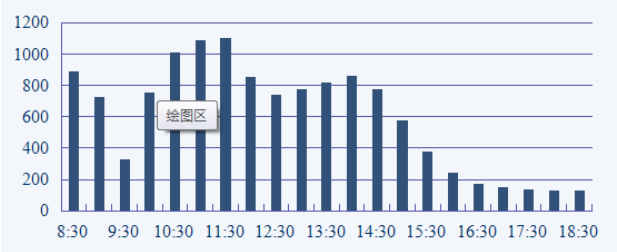


图 1 1.185.0.0/18 于 10 小时的检测结果

从上图可以看到，一个子网中的可连通地址数也会随着时间产生有规律的变化。但在这里为了简化过程提高效率，本文暂时忽略这样一种时间段上的规律。将所有测得可达的地址乘以权重 pri，并插入候选队列（出现一次就插入 pri 次）。当最后需要一个检测列表的时候，再从候选队列抽取 16381 次（子网地址总数次）。所抽到的不重复的地址便为最终检测列表中的地址。之后对于该子网的检测都只需要使用该地址文件即可。

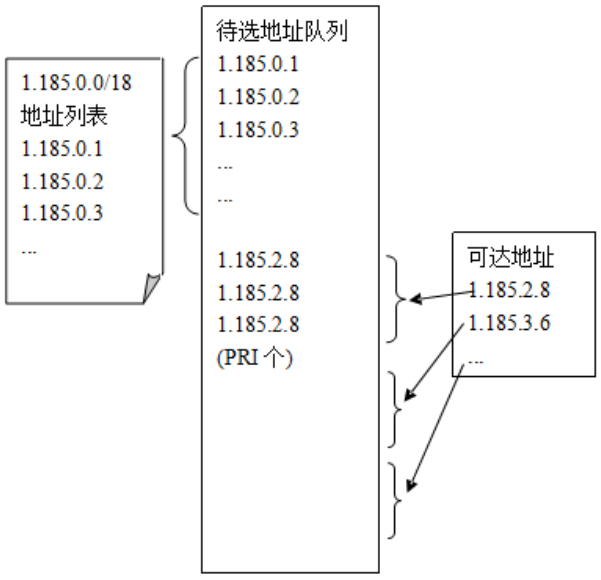


图 2 待选队列构成

这里只选用 FPING 来做测试实验。下表为权重 pri 为 1、2、3、4、5、6 时抽取出的地址数和用 FPING 能够可达的地址数。实验的时间点对整个子网所有地址检测的结果是 672 个地址可达，可达地址数占地址总数的 4.1%。

表 2 不同的权重值抽到地址与可达地址

| 权重 pri | 抽中地址数 | 可达地址数 | 可达百分比 |
|---|---|---|---|
| 1 | 8072 | 487 | 6.0% |
| 2 | 6863 | 223 | 3.2% |
| 3 | 5189 | 100 | 1.9% |
| 4 | 3541 | 76 | 2.1% |
| 5 | 1853 | 31 | 1.6% |
| 6 | 492 | 1 | 0.2% |

下图用曲线表现了三者的变化关系。

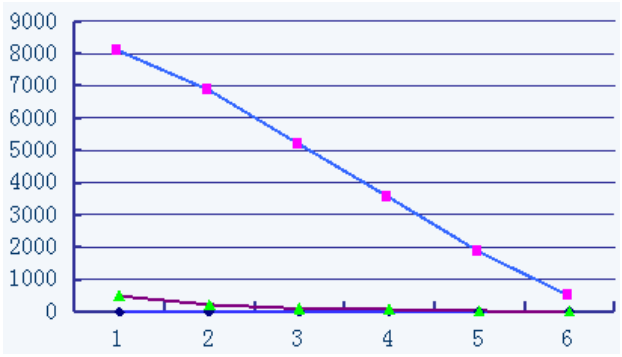


图 3 权重值抽到地址与可达地址变化曲线

由此发现当权重较大时，所抽取到的地址数会减少，故而将权重取 3 或 4 较为适宜。

## 4 实验分析

### 4.1 FPING 与 NMAP 的结合

FPING 与 ping 不同的地方在于，它提供了很多方法，除了可以单独对一个 IP 地址进行 ping 操作，还可以指定要 ping 的主机数量范围或是列表，甚至可以指定一个子网。FPING 给一个主机发送完数据包之后，马上给下一个发送，做到发和收的异步进行，和多地址的并发测试。如果某一地址被 ping 通，则此地址将被打上标记，并从等待列表中移除，如果没有 ping 通，说明主机无法到达，主机仍然留在等待列表中，等待后续操作。

同样的，实验中同时也多线程的进行 NMAP 的调用。NMAP 提供的 sP 选项，发送一个 ICMP echo

请求，对端口 443 发送 TCP SYN，对端口 80 发送 TCP ACK。这个选项跳过了对目标地址的端口扫描，只做主机发现。

论文使用了 Pthread 多线程的方式，抽取了 50 个子网并行的调用 FPING 和 NMAP 生成结果，对同一子网 FPING 测试和 NMAP 测试的时间间隔为 30 分钟，再间隔 30 分钟后重复调用。两种方法各测试了 24 次，并将结果写入不同的文件。由于本身采用异步的方式收发，再加上使用多线程，保证了结果的生成速度。实验共测试了 50 个随机抽取出的子网，每个子网 FPING（间隔 1 小时）结果 24 组，NMAP（间隔 1 小时）结果 24 组。

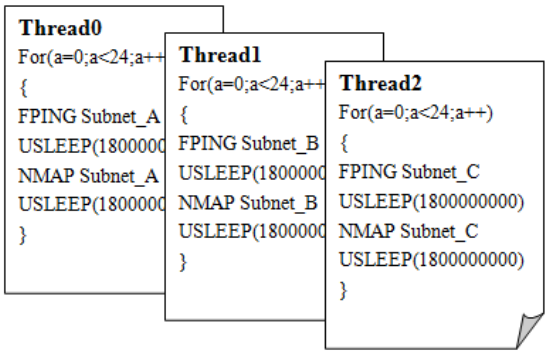


图 4 多线程调用 FPING 和 NMAP

## 4.2 FPING 和 NMAP 的结果统计

用 FPING 和 NMAP 测试得到的结果需要进行统计来观察它们各自的效果。下图是 50 个子网 IP 地址数、每次 FPING 所得可达的平均地址数以及每次 NMAP 所得可达的平均地址数的关系柱状图。

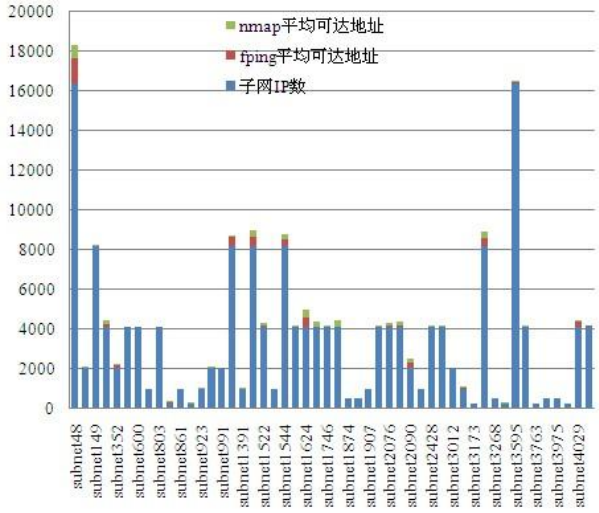


图 5 FPING、NMAP 结果统计

从结果来看，可达的地址都只占子网所有地址的很少一部分，甚至是 0。FPING 和 NMAP 检测的结果不尽相同，其中，FPING 所得结果，50 个子网被测试可达的有 28 个，而 NMAP 测试可达的子网 50 中有 31 个。FPING 可达 NMAP 不可达的子网有 1 个，NMAP 可达而 FPING 没有可达结果的子网有 4 个。但是，在可达的子网中，能够被 FPING 探测到的地址总数有 118896 个，而 NMAP 只有 92544 个。

由此得到这样的结论：FPING（基于 ICMP）和 NMAP（基于 ICMP/TCP）二者的结果可以相互补充，由于 FPING 速度更快更加简单（只基于 ICMP），可以在 FPING 对这个子网的结果是不可达时用 NMAP 进行验证，获得比较好的准确性。

## 4.3 按概率抽取减少需要检测的地址数

### 4.3.1 FPING 可连通的子网

首先是对 FPING 有结果的子网（平均每次测试可达地址数超过 1）单独分析。如果 FPING 检测有结果，则可跳过 NMAP 检测，所以当子网中每次平均测试可达地址超过 1 的子网，论文就只针对 FPING 的结果进行抽取。如第三章所述，将可达的地址乘以权重插入待选队列，这里将权重设为 4，即若出现一次可达，则在队列中插入 4 次。

待选队列建立完成后，下面的工作是要从中抽取具体的 IP 地址。实验中用以系统时间为种子的随机函数从队列中随机选出 IP 地址，再将以抽取出的地址打上标记以免重复抽取，一共抽取该子网所拥有地址数那么多次。最后输出抽取的地址列表。

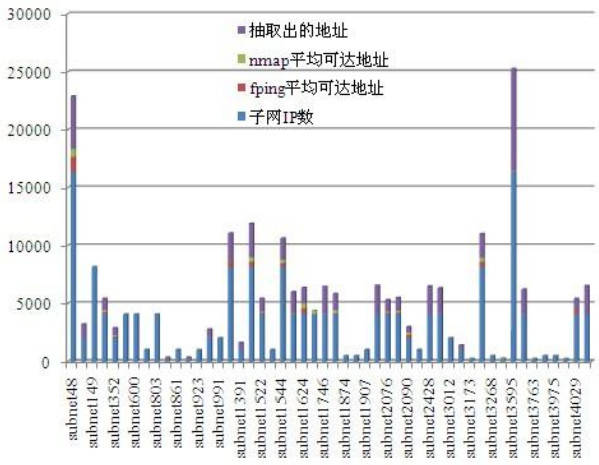

图 6 抽取的地址数与前三者的数量比较

根据图 6 和图 5 的比较，可以看到，抽取的地址数与子网的地址总量还有经测试可达的地址数有关。

至此，得到的是在测试阶段 FPING 有可达性结果的一些子网的简化测试地址列表。有了这些列表，下面就需要测试它们的有效性，有效性包括准确度和速度。

速度自不必说，抽取出的地址数量与权重、子网总地址数和测试可连通地址数三者有关，由图可以看到，抽取出的地址数基本占总地址数的 1/2 至 1/4 之间。

下面是准确度。对测试中可用 FPING 连通的 28 个子网，根据抽取出的地址，进行 FPING 检测。27 个子网被检测是可达的。没有被连通的子网经过全子网地址的 FPING 验证也无可达地址，故而对于这 28 个子网，抽取出的地址结果的准确率达到了 100%。下图是抽取出的地址和其中 FPING 可达地址的比较。

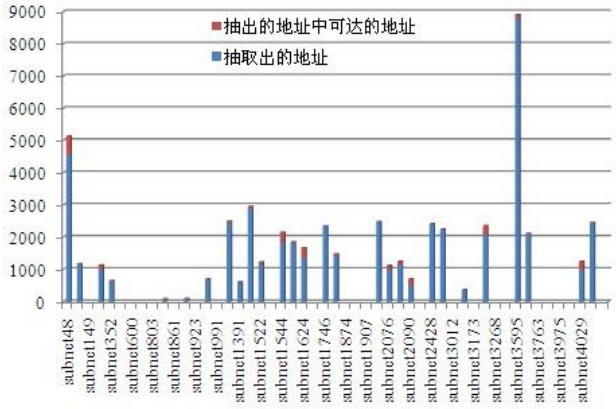


图 7 抽取的地址数与其中可达的地址数量比较

### 4.3.2 FPING 不可连通的子网

对于在子网全地址测试中 FPING 不可连通的子网，需要对它们使用 NMAP 的结果进行补充。根据测试中 NMAP 的结果对它们采用与 4.3.1 中相同的方法。抽取的 50 个子网中，22 个 FPING 不可达的子网中，只有 3 个可被 NMAP 检测可达。也就是说 19 个子网 FPING 和 NMAP 都没有可达的地址结果。

那么首先来处理这 19 个子网，对于他们的处理就很简单，之后对它们的测试将继续使用全网地址。采用 FPING 与 NMAP 相结合的模式。

至于 3 个只可被 NMAP 连通的子网，由于本身可达的地址较少，所以抽取的地址数量在原本的 3/5 至 2/5 左右。经测试 3 个子网均可被连通。

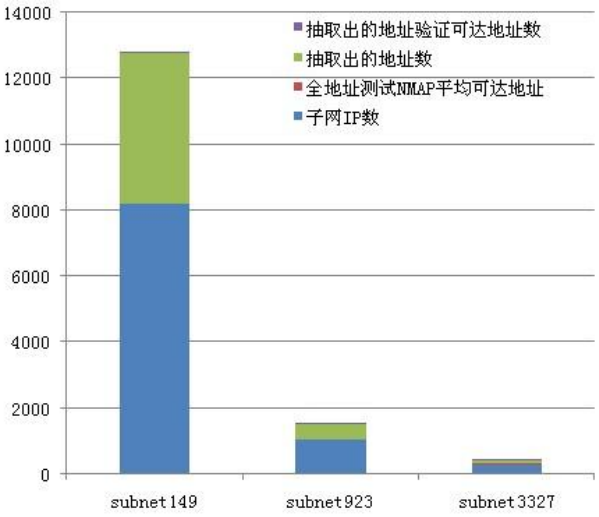


图 8 NMAP 方法的四项数据的比较

## 5 总结

最后总结一下本文所提出的方法。首先对于子网的所有地址进行 FPING 的检测，有可达地址结果的子网将结果乘以权重放入待选队列，通过在队列中随机抽取与子网总地址数相同次数，获得检测地址列表，之后一段时间内可用此列表作为检测的目标。对于 FPING 检测不可达的子网，用 NMAP 进行重复验证，若有可达地址，则采用相同的方法获得检测地址列表，若无可达地址，则以后还是进行全地址的检测。

本文主要运用的是子网中一些地址存在具有规律性，故而利用这样的特性，可以减少一个子网中需要检测的 IP 地址数以加快检测的速度。从教育网中随机抽取的 50 个子网所得到的结果来看，这样的方法是行之有效的。

对于被抽取出的地址列表，也不能是永久性的，要定期对它们进行重新的全地址检测以便对抽取的地址更新。

当然，这个方法也只是对特定的子网进行检测，本文的实验是建立在知晓教育网的 IP 子网划分的情况下。当子网的划分发生变化，需要重新收集子网划分的信息数据。

由于进行本实验的是单一的主机，所以对于不可达的子网，并不能肯定它们没有接入互联网或者

不存在，因为防火墙或网关路由器等会对某些协议的报文进行过滤或对源地址不明的报文进行丢弃或拒绝应答。

还有一点就是可达的地址会随一天中不同的时间段产生变化，例如，工作时间可达的地址较多，深夜就会比较少。工作日可达地址较多，节假日可达地址比较少等等这方面的影响因素也很多。故而本文虽说暂时还有很多因素没有考虑进去，但是提供了这样一种优化的解决方法。未来的工作也可以围绕这些因素慢慢改进。

## 参考文献

[1] Douglas E.Comer. Internetworking With TCP/IP Principles, Protocols, and Architectures Fifth Edition[M]. 北京: 电子工业出版社, 2007.

[2] 李天剑, 曾文方, 李天翼. 基于 SNMP 网络拓扑自动构造的一种实现[J]. 计算机系统应用, 2000.

[3] 田慧, 裴昌幸. 一种改进的 IP 网络拓扑发现算法[J]. 网络技术与应用, 2002.

[4] 傅佳芳, 赵保华. Ping 技术研究[J]. 微型电脑应用, 2007.

[5] 李莉, 徐宁, 曹阳. 用远程方法调用（RMI）实现 IP 连通性测试[J]. 计算机应用研究, 2000.

[6] FPING (Maintained by Thomas Dzubin): http://FPING.sourceforge.net/.

[7] NMAP Free Security Scanner For Network Exploration & Hacking: NMAP.org/.