1.主流网络设备的快速探测：

快速探测的意义在于，能给出一个较小时间窗口内Internet设备的拓扑快照。ZMAP快速扫描工具，针对上述快速大规模测量而设计，使用随机化探测的技术，并且跳过协议栈直接生成以太栈，在扫描速度上能达到以太网理论上的极限，大大提高了扫描速度。此外ZMAP使用类SYN cookie技术，做到了不保存状态信息，不重传丢包，提高了扫描速度的同时降低了内存资源消耗。此外，ZMAP提供的模块接口，可以支持如TCP SYN scan、ICMP request scan，DNS scan等种单包探测，增加了扫描引擎的复用性和多态性。ZMAP面临的挑战是，其扫描策略是简单随机枚举，对于IPV6的测量，由于其地址空间过于庞大，枚举法不适用。此外，ZMAP的广泛使用，会给网络上的主机较大的负载，所以缺乏一种排除机制，让主机有选择的回复ZMAP探测包。

2.主流网络设备的指纹识别：

指纹识别的意义在于，除了测量网络设备的ip接口拓扑外，还提取设备的操作系统，提供的服务，防火墙类型等描述设备具体属性的设备指纹，对网络设备有更细节的掌握。NMAP工具，提供TCP SYN scan，Xmas scan等多种端口扫描技术的实现，结合社区维护的保存有主流的2200多个服务的namp-services数据库，进行服务探测。NMAP使用nmap-service-probes数据库，针对不同的服务，发送相应探测包，以进行进一步的服务版本探测，发现服务背后的协议类型，实现版本，版本号等，还有服务所反映的设备信息如主机名称，设备类型，操作系统信息等。对于在测量中发现的设备，使用TCP ISN采样，IPID采样，TCP选项支持，初始窗口大小检测等多种探测设备特征行为的方法，结合保存有2600多个主流OS指纹的nmap-os-db数据库，给出设备的操作系统零售商，操作系统类型，操作系统版本，还有设备本身的设备类型，在线时间，ip序列号的可预测性强弱等多种设备指纹信息。

3.大规模低感知网络探测技术：

比较著名的隐蔽端口扫描方法有SYN 扫描，如基于SYN scan修改了TCP三次握手的Half open scan，还有通过构造异常TCP选项搭配，根据回复行为进行端口开放情况判断的异常扫描，如FIN scan，Xmas Tree scan，Null scan。还有针对防火墙的ACK扫描，向目的主机端口发送ACK包，伪装成应答包骗过防火墙，如果收到RST则认为防火墙开放了该端口。

诱饵地址，发送大量假造ip给目的主机，用以混淆日志系统和管理员，使其难以在众多地址中发现自己的地址。

空闲主机扫描技术，通过一台没有其他流量的空闲主机与目标主机进行通信，根据空闲主机的IPID判断目的主机的行为，推断端口开放情况。这样简洁扫描，完全隐藏了自己的ip。

ip分片隐藏技术，发送很小的ip分片，来隐藏自己的扫描意图试图骗过防火墙和IDS。

适用于局域网环境的两种欺骗技术：ip地址复用欺骗，攻击者使用随机的ip地址伪造扫描包的源地址，在包的必经网关进行嗅探，判断端口开放情况。ARP欺骗，通过修改自己的MAC地址和上构造假的ARP应答，污染主机的ARP表，达到伪装的目的。

代理反弹技术，利用一些支持代理的协议如FTP proxy，Finger等，通过代理服务器间接扫描目的主机实现自身隐藏，如果代理在防火墙内，还能够绕过防火墙进行更多的隐蔽操作。

NMAP实现了上述大部分技术，能够做到隐蔽扫描。

此外还有Hping2工具，向第三方主机发送ping包，通过观察TCP ISN，构造扫描包使得目的主机相信扫描者是第三方主机。

5.大规模拓扑探测：

大规模拓扑探测最早是从几个观测点出发进行的探测，例如法国UoS Pansiot等人进行的研究。

专用大规模拓扑探测平台，CAIDA的Skitter利用web服务器，以及Skitter的后继Arc。一般意义的分布式测量平台还有，Planet Lab，iPlane，和UW的RocketFuel。

全球有近千个Traceroute server，作为拓扑探测的窥镜(looking glass)，由于其测量点的分布覆盖范围广，能够保证较好的完全性。

此外还有crowd sourcing测量，不再适用专用的测量平台，而是利用Internet大量的用户基础，通过在浏览器安装插件，让终端用户执行测量工作，如Scriptroute，Dimes，Bitprobe等。这种利他主义的方法，需要额外的设计权衡，和安全性考虑。

在大规模拓扑探测中，有两个科学问题：首先观察点的选取问题，有的观察点很难发现一些如AS间的p2p路径。相关研究使用了Targeted Probing技术，利用专家的领域知识，有根据的进行探测。其次，大规模traceroute测量平台要有合理的协作机制，如果不对冗余测量进行控制，和观察点拓扑距离较小的路由器将会有较大负载。针对该问题，通常在监控点内采用“远探针”手段，监控点间采用“协作监测”手段，去除冗余测量，做到高发现率的同时，降低负载。